SND

# Securing Cisco Network Devices

## Volume 1

**Version 2.0**

## Student Guide

Text Part Number: 97-2359-01

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

**European Headquarters**
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

**Asia Pacific Headquarters**
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe





© 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

***Students, this letter describes important course evaluation access information!***

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco Systems is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions; therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. We would appreciate a few minutes of your time to complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,

*Cisco Systems Learning*

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Table of Contents

**Volume 1**


***Course Introduction 1***

Overview 1
Learner Skills and Knowledge 1
Course Goal and Objectives 2
Course Flow 3
Additional References 4
Cisco Glossary of Terms 4
Your Training Curriculum 5

***Introduction to Network Security Policies 1-1***

Overview 1-1
Module Objectives 1-1

**Understanding the Requirement for a Network Security Policy 1-3**

Overview 1-3
Objectives 1-3
Need for Network Security 1-4
Balancing Network Security Requirements 1-9
Assuring the Availability and Protection of Information 1-12
Adversaries, Hacker Motivations, and Classes of Attack 1-14
Classes of Attack 1-15
Information Assurance 1-16
Principles of Defense in Depth 1-20
Network Security Process 1-23
Network Security Design Factors 1-28
Summary 1-30
Additional Resources 1-30

**Introducing Network Attack Mitigation Techniques 1-31**

Overview 1-31
Objectives 1-31
Mitigating Physical and Environmental Threats 1-32
Reconnaissance Attacks and Mitigation 1-38
Access Attacks and Mitigation 1-45
Preventing Buffer Overflows 1-53
IP Spoofing Attacks and Mitigation 1-55
DoS Attacks and Mitigation 1-60
Worm, Virus, and Trojan Horse Attacks and Mitigation 1-66
Application Layer Attacks and Mitigation 1-70
Management Protocols and Vulnerabilities 1-73
Determining Network Vulnerabilities 1-78
Summary 1-79

**Thinking Like a Hacker 1-79**

Overview 1-79
Objective 1-79
How Do Hackers Think? 1-80
Step 1: Footprint Analysis 1-82
Step 2: Enumerate Information 1-85
Step 3: Manipulate Users to Gain Access 1-87
Social Engineering 1-87
Password Cracking 1-88
Step 4: Escalate Privileges 1-89
Step 5: Gather Additional Passwords and Secrets 1-90
Step 6: Install Back Doors and Port Redirectors 1-91
Back Doors 1-91
Port Redirectors 1-92



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Step 7: Leverage the Compromised System 1-93
Best Practices to Defeat Hackers 1-94
Summary 1-95
**Designing a Secure Network Life-Cycle Model 1-97**
Overview 1-97
Objectives 1-97
Components of Network Security Design 1-98
Secure Network Life-Cycle Management 1-100
Planning a Secure Network 1-102
Designing a Secure Network 1-104
Implementing a Secure Network 1-106
Operating a Secure Network 1-107
Optimizing a Secure Network 1-108
Disposing of Secure Network Components 1-109
Principles of Secure Network Design 1-110
Summary 1-117
**Developing a Comprehensive Security Policy 1-119**
Overview 1-119
Objectives 1-119
Why Do You Need a Security Policy? 1-120
Confidentiality, Integrity, and Availability 1-120
What Does a Security Policy Do and Who Uses It? 1-123
Components of a Comprehensive Security Policy 1-125
Developing a Security Policy Using the PDIOO Model 1-133
Developing a Security Policy—Plan Phase 1-134
Developing a Security Policy—Design Phase 1-136
Developing a Security Policy—Implement Phase 1-141
Developing a Security Policy—Operate Phase 1-143
Developing a Security Policy—Optimize Phase 1-148
Managing Change 1-148
Policy Management 1-149
What Makes a Good Security Policy? 1-151
**Building Cisco Self-Defending Networks 1-153**
Objectives 1-153
Changing Threats and Challenges 1-154
Building a Cisco Self-Defending Network 1-159
Adaptive Threat Defense 1-164
Cisco Integrated Security Portfolio 1-166
Endpoint Protection 1-168
Admission Control 1-168
Infection Containment 1-169
In-Line IPS and Anomaly Detection 1-169
Application Security and Anti-X Defense 1-169
Summary 1-170
Module Summary 1-171
References 1-172
Module Self-Check 1-173
Module Self-Check Answer Key 1-183
***Securing the Perimeter 2-1***
Overview 2-1
Module Objectives 2-1
**Applying a Security Policy for Cisco Routers 2-3**
Overview 2-3
Objectives 2-3
Role of Routers in Networks 2-4
Router Security Principles 2-7

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

How Routers Enforce a Perimeter Security Policy 2-8
Filtering with a Router 2-9
Applying Packet Filters 2-9
Local and Remote Administrative Access 2-12
Maintaining the Most Recent Versions of Cisco IOS Software 2-14
Logging 2-16
Conceptual Basis for a Router Security Policy 2-17
Creating a Security Policy for a Router 2-19
Applying Cisco IOS Security Features 2-21
Summary 2-23

**Securing Administrative Access to Cisco Routers 2-25**

Overview 2-25
Objectives 2-25
Configuring Router Passwords 2-26
Setting a Login Failure Rate 2-40
Setting Timeouts 2-41
Setting Multiple Privilege Levels 2-42
Configuring Role-Based CLI 2-44
Securing the Cisco IOS Image and Configuration Files 2-49
Configuring Enhanced Support for Virtual Logins 2-52
Configuring Banner Messages 2-58
Summary 2-60

**Introducing Cisco SDM 2-61**

Overview 2-61
Objectives 2-61
Cisco SDM Overview 2-62
Starting Cisco SDM and Cisco SDM Express 2-64
Additional Preparation for Existing Routers 2-64
Launching Cisco SDM Express 2-67
Launching Cisco SDM 2-68
Navigating the Cisco SDM Interface 2-69
Cisco SDM Wizards 2-71
Summary 2-75

**Configuring AAA Functions on the Cisco IOS Router 2-77**

Overview 2-77
Objectives 2-77
Identification and Authentication 2-78
Introduction to AAA for Cisco Routers 2-79
Authenticating Remote Access 2-80
TACACS+ and RADIUS AAA Protocols 2-82
Authentication Methods 2-83
Point-to-Point Authentication Protocols 2-88
Authenticating Router Access 2-90
Configuring AAA for Cisco Routers 2-92
Troubleshooting AAA for Cisco Routers 2-105
Configuring AAA with Cisco SDM 2-108
Summary 2-109

**Disabling Unused Cisco Router Network Services and Interfaces 2-111**

Overview 2-111
Objectives 2-112
Vulnerable Router Services and Interfaces 2-113
Management Service Vulnerabilities 2-117
Locking Down Your Router with Cisco AutoSecure 2-119
Limitations and Cautions 2-123
Summary 2-125



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

**Implementing Secure Management and Reporting 2-127**
Overview 2-127
Objectives 2-127
Secure Management and Reporting Planning Considerations 2-128
Secure Management and Reporting Architecture 2-130
Using Syslog Logging for Network Security 2-136
Using Logs to Monitor Network Security 2-140
Using SNMPv3 2-141
Configuring an SSH Server for Secure Management and Reporting 2-146
Enabling Management Features 2-148
Summary 2-152
**Defending the Network Perimeter with Cisco Products 2-153**
Overview 2-153
Objectives 2-153
Cisco IOS Security Features 2-154
Introducing the Cisco Integrated Services Router Family 2-155
Cisco 800 Series Routers 2-155
Cisco 1800 Series Integrated Services Routers 2-156
Cisco 2800 Series Integrated Services Routers 2-156
Cisco 3800 Series Integrated Services Routers 2-156
Identity Solutions 2-162
Summary 2-164
References 2-164
Module Summary 2-165
References 2-166
Module Self-Check 2-167
Module Self-Check Answer Key 2-173

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

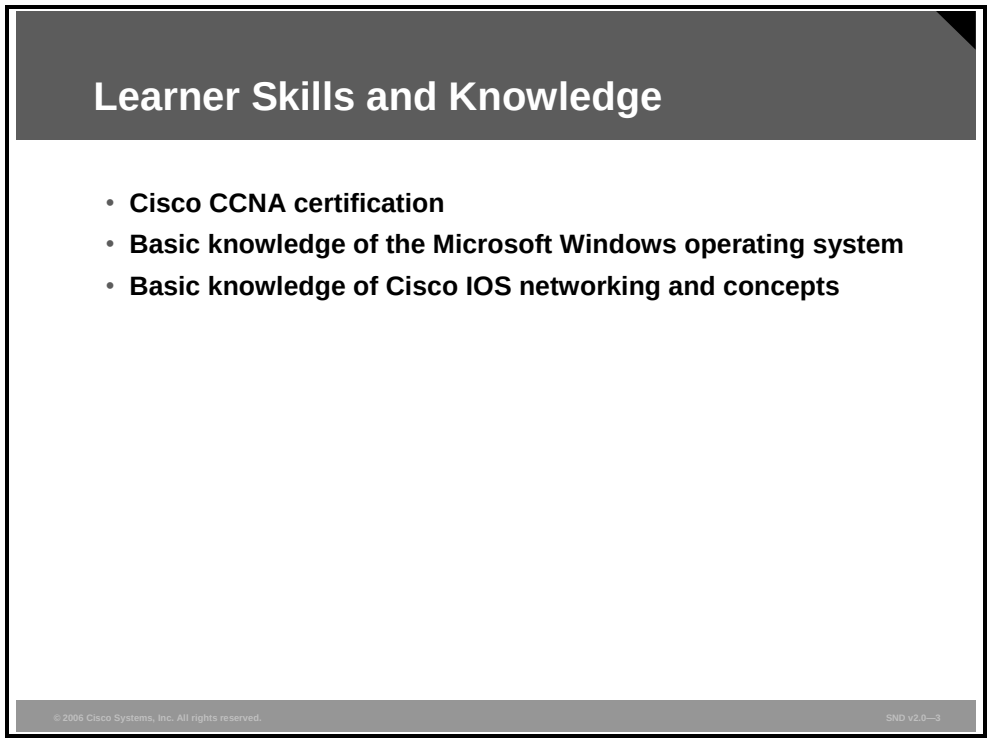
# Course Introduction

## Overview

*Securing Cisco Network Devices* (SND) v2.0 provides an opportunity to learn about a broad range of the components embedded in the Cisco Self-Defending Network. You learn to recognize threats and vulnerabilities to networks and learn how to implement basic mitigation measures.

### Learner Skills and Knowledge

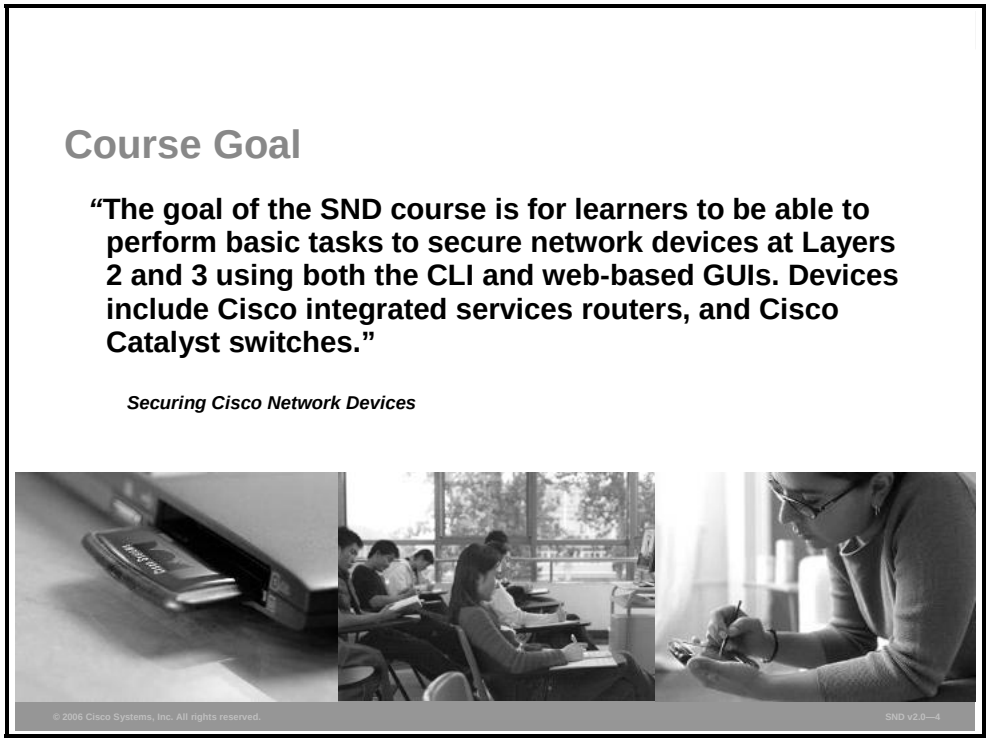
This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.




*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Course Goal and Objectives

This topic describes the course goal and objectives.




Upon completing this course, you will be able to meet these objectives:

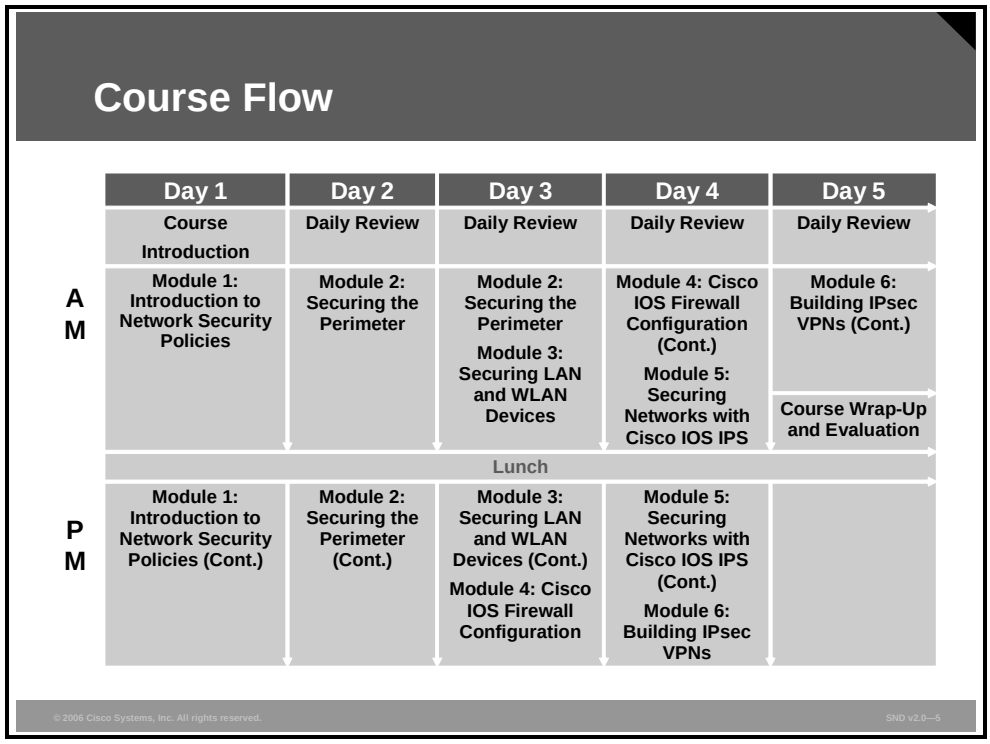
- Develop a comprehensive network security policy to counter threats against information security
- Configure routers on the network perimeter with Cisco IOS software security features
- Configure LAN devices to be secure
- Configure a Cisco IOS Firewall to perform basic security operations on a network
- Configure Cisco IOS IPS on Cisco network routers
- Configure point-to-point and remote-access VPNs using Cisco IOS features



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Course Flow

This topic presents the suggested flow of the course materials.



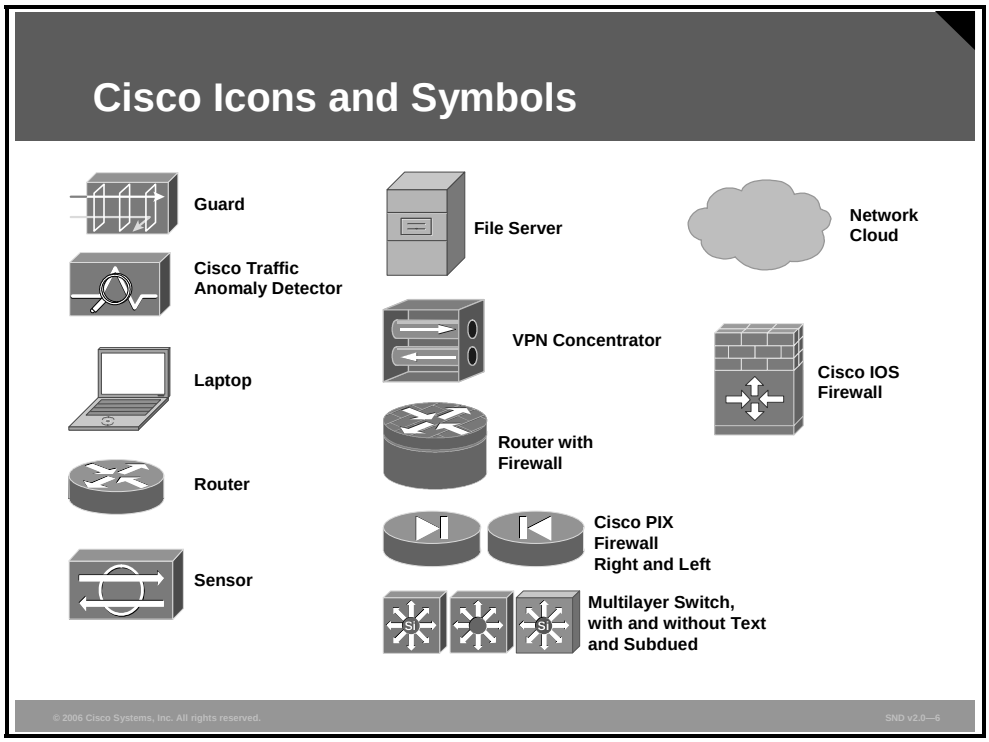

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Additional References

This topic presents the Cisco icons and symbols that are used in this course, as well as information about where to find additional technical references.




## Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Your Training Curriculum

This topic presents the training curriculum for this course.




You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE®, CCNA®, CCDA®, CCNP®, CCDP®, CCIP®, CCVP™, or CCSP™). It provides a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit www.cisco.com/go/certifications.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module 1

# Introduction to Network Security Policies

## Overview

The open nature of the Internet makes it increasingly important for growing businesses to pay attention to the security of their networks. As companies move more of their business functions to the public network, they need to take precautions to ensure that the data is not compromised or that the data does not end up in front of the wrong people.

Unauthorized network access by an outside hacker or disgruntled employee can wreak havoc with proprietary data, negatively affect company productivity, and stunt the ability to compete. Unauthorized network access can also harm relationships with customers and business partners who may question the ability of companies to protect their confidential information.

## Module Objectives

Upon completing this module, you will be able to develop a comprehensive network security policy to counter threats against information security. The module will describe the threat, present and provide an opportunity to practice the process of developing a security policy, and introduce the Cisco Self-Defending Network strategy. This ability includes being able to meet these objectives:

- Explain how increasing network security threats will demand comprehensive network security policies
- Explain the strategies used to mitigate network attacks
- Describe the common methodologies used by hackers to break into and exploit networks
- Describe the main activities in each phase of a secure network life cycle
- Explain how to meet the security needs of a typical enterprise with a comprehensive security policy
- Describe how to implement the Cisco Self-Defending Network strategy by enhancing an existing network infrastructure with Cisco technologies, products, and solutions

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 1

# Understanding the Requirement for a Network Security Policy

## Overview

How important is it to have a strong network security policy? A report from the *2005 Computer Crime and Security Survey* conducted by Computer Security Institute (CSI) with the participation of the San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad provides an updated look at the impact of computer crime in the United States. Based on responses from over 700 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities, the survey confirms that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.

The application of an effective security policy is the most important step that an organization must take to protect itself. An effective security policy is the foundation for all of the activities undertaken to secure network resources.

## Objectives

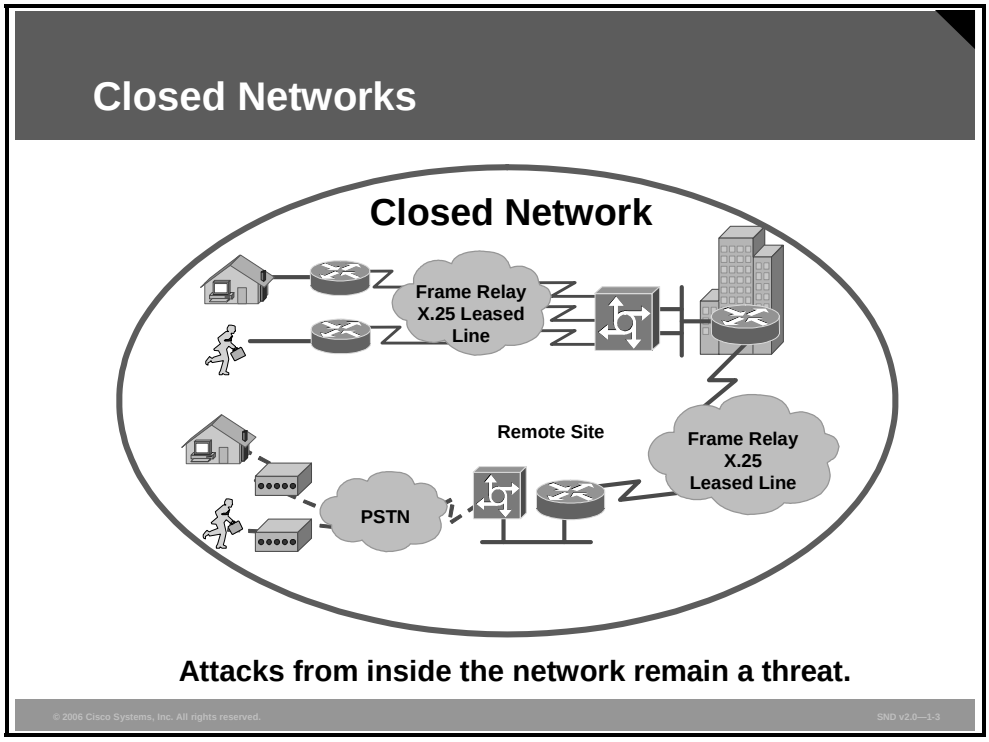
Upon completing this lesson, you will be able to explain the need for a comprehensive network security policy. This ability includes being able to meet these objectives:

- Explain how sophisticated attack tools and open networks have generated an increased need for network security and dynamic security policies
- Describe the challenge of balancing network security needs against e-business processes, legal issues, and government policies
- Describe how information assurance affects network architecture
- Describe network adversaries, hacker motivations, and classes of attack
- Describe how achieving information assurance requires a balanced focus on people, technology, and operations
- Describe the concept of defense in depth
- Describe the factors to consider when designing a secure network infrastructure

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Need for Network Security

This topic explains how sophisticated attack tools and open networks have generated an increased need for network security and dynamic security policies.

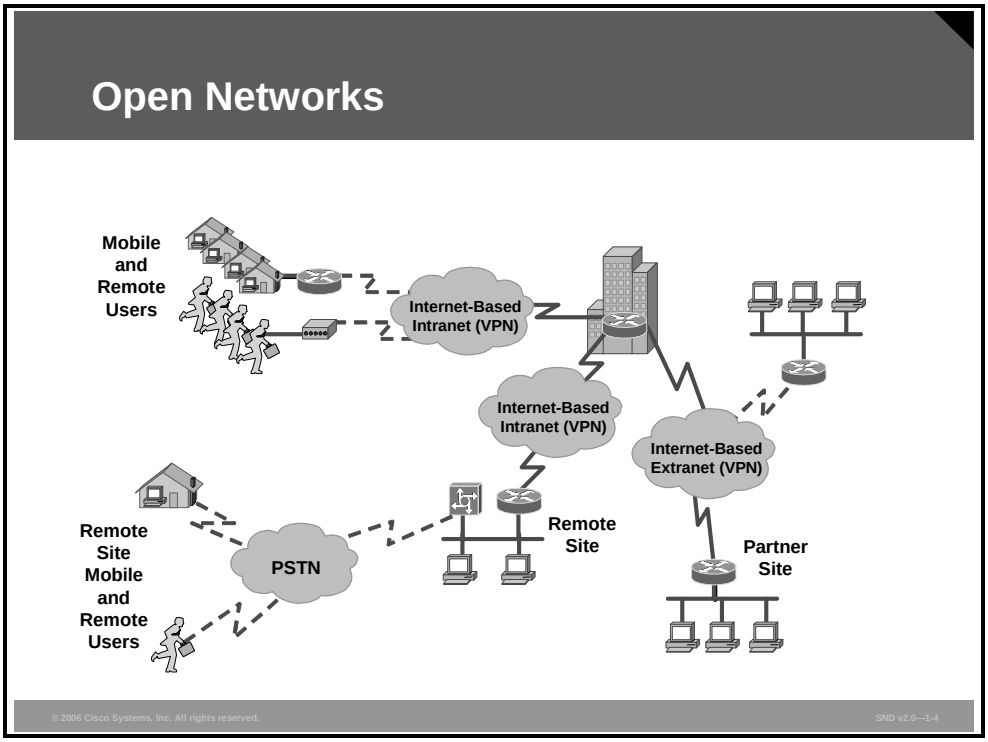



The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.

Because there is no outside connectivity, networks designed in this way can be considered safe from outside attacks. However, internal threats still exist. The CSI in San Francisco, California, estimates that 60 to 80 percent of network misuse comes from inside the enterprise where misuse has taken place.

 © 2006 Cisco Systems, Inc.

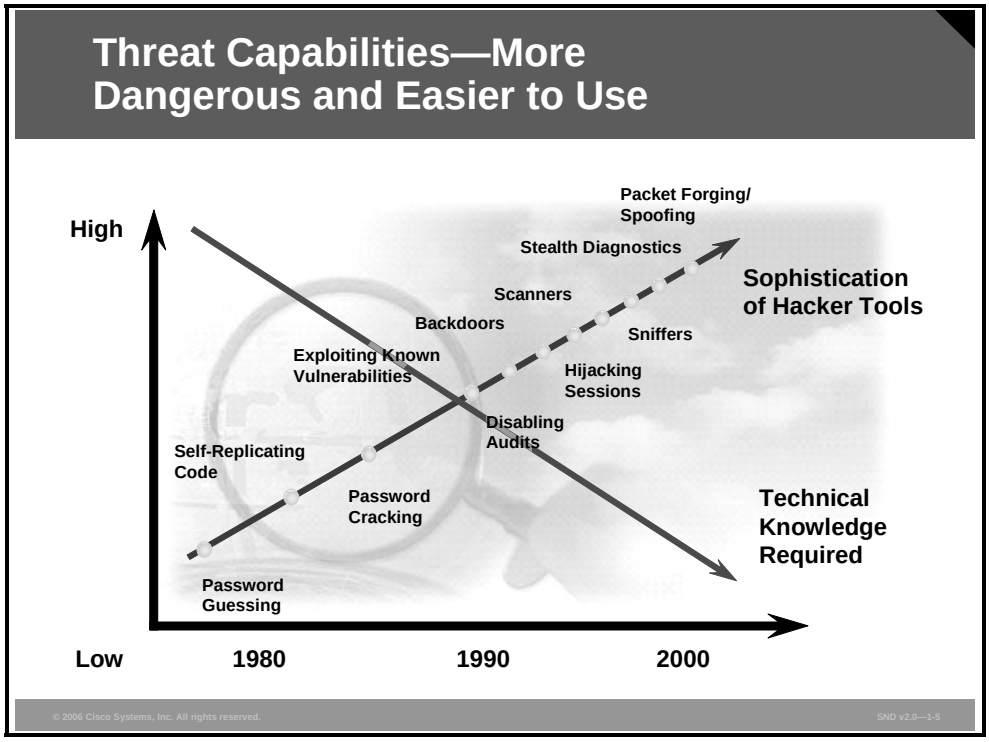
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Today, corporate networks require access to the Internet and other public networks. Most networks have several access points to public and private networks. Securing open networks is extremely important.



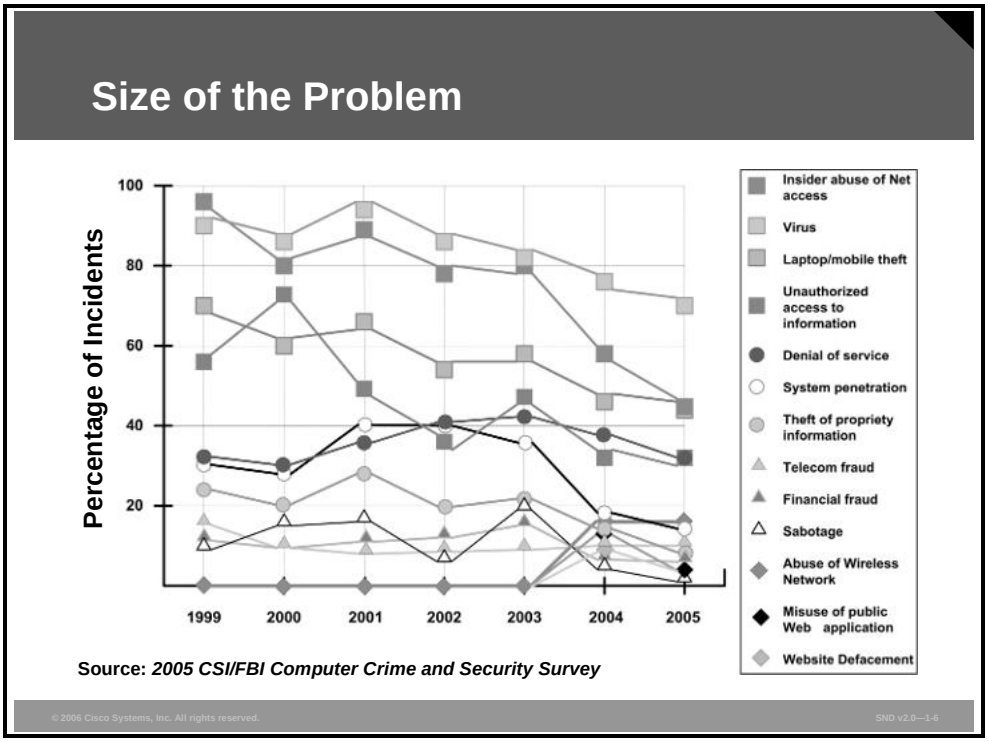
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The figure illustrates how the increasing sophistication of hacking tools and the decreasing skill needed to use these tools have combined to pose increasing threats to open networks. With the development of large open networks, security threats in the past 20 years have increased significantly. Hackers have discovered more network vulnerabilities, and hacking tools have become easier to use. You can now download applications that require little or no hacking knowledge to implement. Troubleshooting applications intended for maintaining and optimizing networks can, in the wrong hands, be used maliciously and pose severe threats.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The threat capabilities just cited add up to a serious situation. The figure here shows the range of security events over the past six years as reported in the *2005 CSI/FBI Computer Crime and Security Survey*. Although it may appear as though the instances are decreasing, keep in mind that security measures continue to improve, and the damage done by the attackers actually costs more all the time.

Here are some additional highlights of the 2005 survey (which is published at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf):

- Virus attacks continued to be the source of the greatest financial losses. Unauthorized access, however, showed a dramatic cost increase and replaced denial of service (DoS) attacks as the second most significant contributor to computer crime-related losses.
- Unauthorized use of computer systems increased slightly according to the survey respondents. However, the survey respondents reported that the total dollar amount of financial losses resulting from cybercrime is decreasing. Given that the total number of respondents to the survey dramatically increased, the survey shows a significant decrease in average total losses per respondent. Two specific areas (unauthorized access to information and theft of proprietary information) showed significant increases in average loss per respondent.
- Website incidents of attacks increased dramatically.
- State governments had the largest information security operating expense and investment per employee of all industry or government segments.
- Use of cyber insurance remains low. That is, the use of cybersecurity insurance is increasing despite the fact that numerous articles have been published that discuss the emerging role of cybersecurity insurance.
- The percentage of organizations reporting computer intrusions to law enforcement continued its multiyear decline. The key reason cited for not reporting intrusions to law enforcement is the concern about negative publicity.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- A significant number of organizations conduct some form of economic evaluation of their security expenditures, with 38 percent using return on investment (ROI), 19 percent using internal rate of return (IRR), and 18 percent using net present value (NPV).
- Over 87 percent of the organizations conduct security audits, up from 82 percent in the 2004 survey.
- The Sarbanes-Oxley Act of 2002 began to have an impact on information security in more industry sectors than in the previous year.
- The vast majority of survey respondents view security awareness training as important. However, on average, respondents from all sectors do not believe that their organization invests enough in this training.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Balancing Network Security Requirements

This topic describes the challenge of balancing network security needs against e-business needs, legal issues, and government policies.

## Network Security Challenge

**As business and management practices become more open and rely more on using Internet-powered initiatives and online collaboration, network security becomes a fundamental part of their survival in an increasingly competitive and threatening world.**



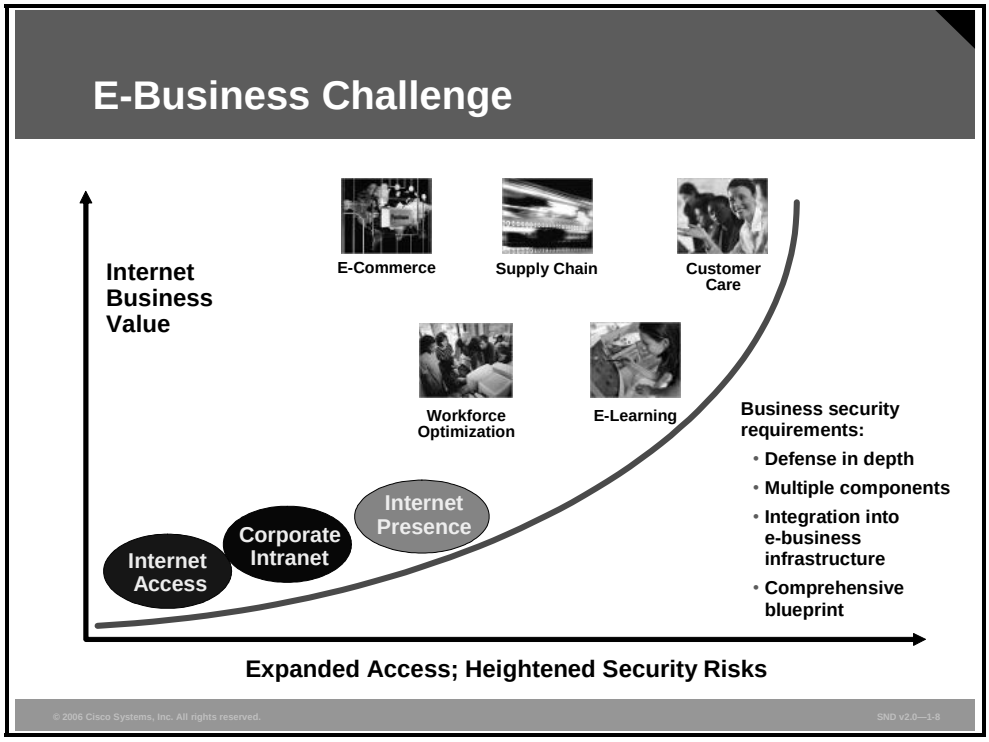

© 2006 Cisco Systems, Inc. All rights reserved.


The overall security challenge is to find a balance between two important needs: the need to open networks to support evolving business requirements and freedom of information initiatives, and the growing need to protect private, personal, and strategic business information.

Security has moved to the forefront of network management and implementation. For the survival of many businesses, it is necessary to allow open access to network resources and to ensure that data and resources are as secure as possible. The increasing importance of e-business and the need for private data to traverse potentially unsafe public networks increases the need for the development and implementation of a corporate-wide network security policy. Establishing a network security policy should be the first step in changing a network over to a secure infrastructure.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The Internet has created expectations for a company to build stronger relationships with customers, suppliers, partners, and employees. E-business challenges companies to become more agile and competitive. The benefit of this challenge is that new applications for e-commerce, supply chain management, customer care, workforce optimization, and e-learning have been created; applications that streamline and improve processes increase turnaround times, lower costs, and increase user satisfaction.

As enterprise network managers open their networks to more users and applications, they also expose the networks to greater risk. The result has been an increase in business security requirements. Security must be included as a fundamental component of any e-business strategy.

E-business requires mission-critical networks that accommodate ever-increasing constituencies and demands for greater capacity and performance. These networks also need to handle voice, video, and data traffic as networks converge into multiservice environments.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Converging Dynamics

- **New laws require organizations to better protect the privacy of sensitive and personal information.**
- **A growing level of terrorist and criminal activity is being directed at communications networks and computer systems.**
- **Cyber attacks and hacking are much easier now than in the past for a larger number of perpetrators.**



© 2006 Cisco Systems, Inc. All rights reserved.


Converging dynamics have raised the risks for organizations that are required to protect the privacy of client information or that have a high political or brand profile. There are three major dynamics that have converged to heighten the need for network and system security.

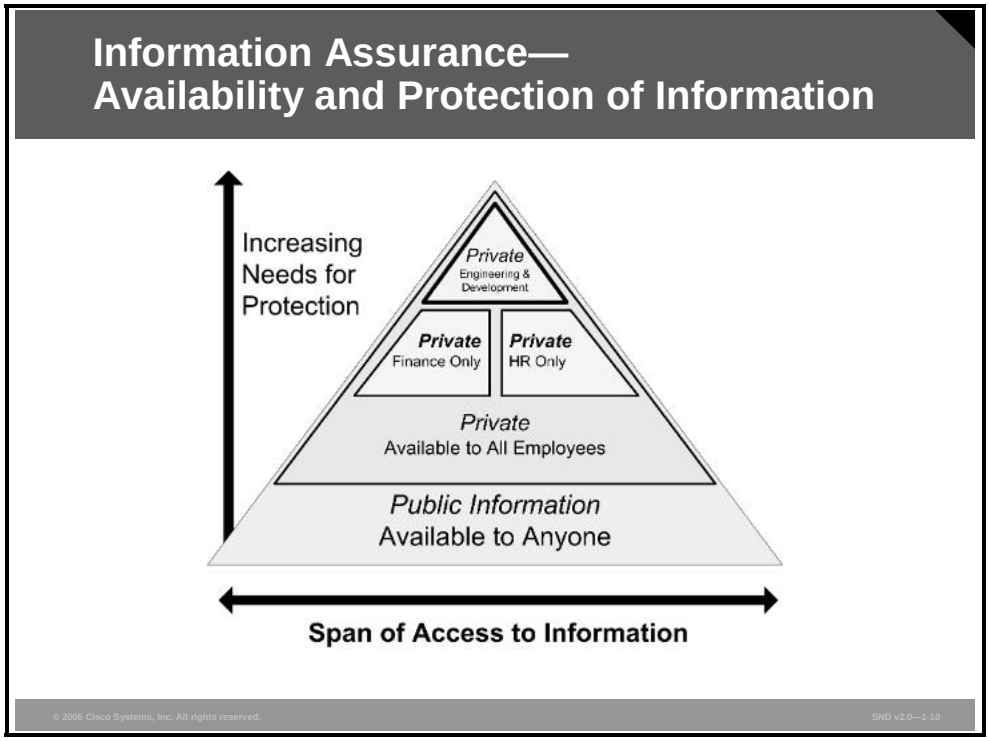
- There are new and pending laws around the world that require organizations to better protect the privacy of sensitive and personal information. Here are some examples of laws and directives that influence network security in the United States:
  - European Union (EU) Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
  - Computer Fraud and Abuse Act.
  - The Digital Millennium Copyright Act of 1998 implements two 1996 World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty and a number of other significant copyright-related issues.
  - Notification of Risk to Personal Data Act.
  - The Gramm-Leach-Bliley Act of 1999, also known as the Financial Services Modernization Act of 1999, includes provisions to protect consumer personal financial information held by financial institutions.
- There is a growing level of terrorist and criminal activity directed at communications networks and computer systems.
- The increased use of Internet technology and connectivity around the world makes cyber attacks and hacking much easier for a larger number of perpetrators.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Assuring the Availability and Protection of Information

This topic describes how information assurance affects network architecture.



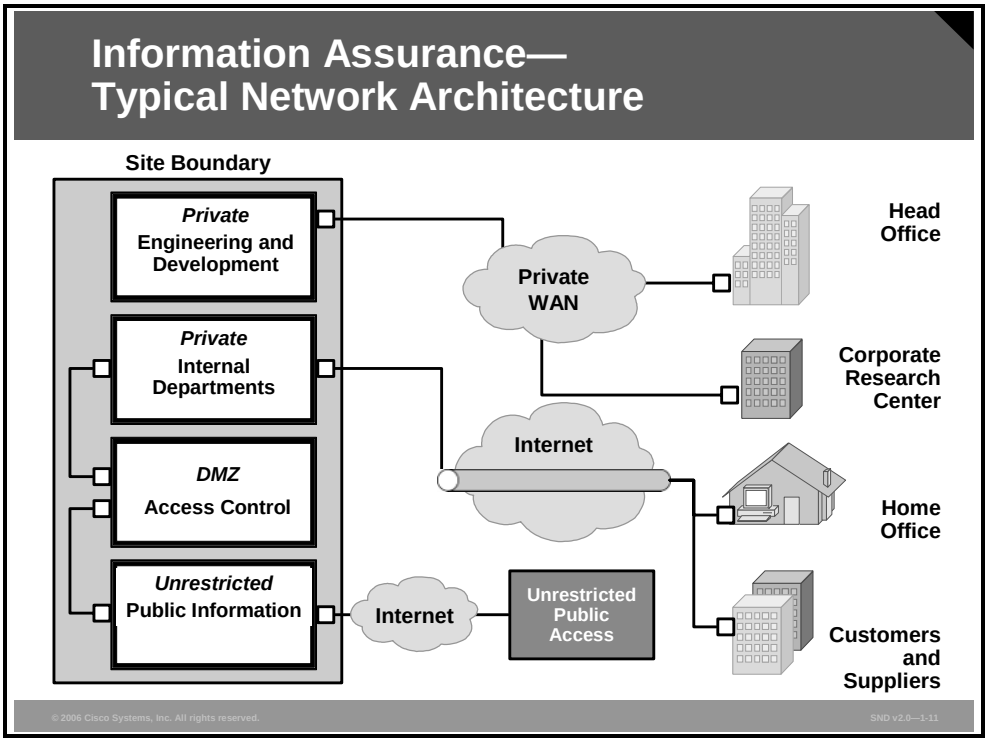

The figure shows how an organization might classify information contained in its network. Organizations assign more rigorous measures to protect their private information than they do for their public information. This diagram is referred to as the Availability and Protection of Information Triangle.

The most important protection measure is access control. According to the example, human resources or finance employees have access to personnel and payroll databases and servers but do not have access to research and development information, which is more sensitive. To limit employee access to a specific body of information, personnel and payroll databases for instance, information assurance assigns different access levels to different people essentially based on need-to-know designations.

In addition to access controls, information assurance implements more robust technical security measures. Organizations acknowledge that the potential loss from exposing private information to the public is high and, therefore, can justify the additional cost of protection. In the figure, information assurance applies the most stringent security measures to the information and to the information infrastructures associated with the top triangle.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




This figure shows a conceptual diagram of a network for a branch location within a large enterprise. The network topology aligns with the Availability and Protection of Information Triangle.

- Information at the bottom is available to the public and corresponds to the base of the Availability and Protection of Information Triangle.
- There is a demilitarized zone (DMZ) that acts as the single point of entry into the site and defends the network perimeter and external connections.
- The network segment serving internal departments is logically isolated from the public by the DMZ.
- The engineering and development segment is physically isolated from all public access.
- All sites are assessable to authorized users through virtual private network (VPN) and remote access connections.

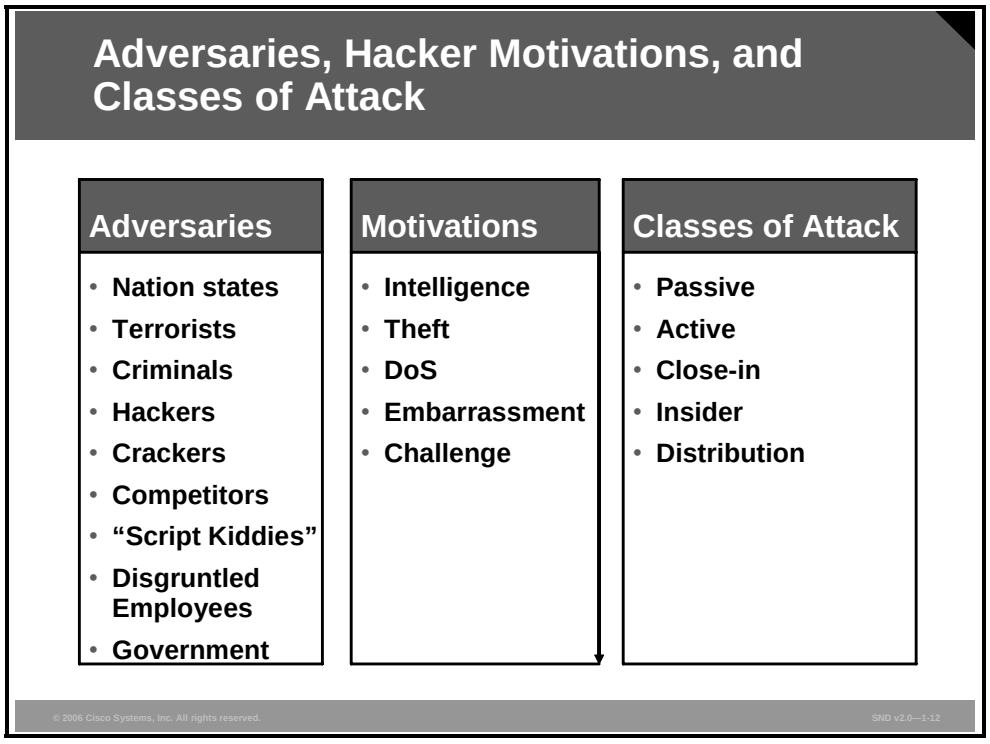
Within the internal corporate networks, VLANs support various corporate functions. Physical separation and isolation of workstations maintain the confidentiality and integrity of classified data. The network also provides carefully controlled connections between the internal networks and the unclassified public network when outside data transfer is required.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Adversaries, Hacker Motivations, and Classes of Attack

This topic describes network adversaries, hacker motivations, and classes of attack.




To defend against attacks on information and information systems, organizations must define the threat in these three terms:

- **Adversaries:** Potential adversaries might include nation states, terrorists, criminals, hackers, and corporate competitors.
- **Motivations:** Motivations may include intelligence gathering, theft of intellectual property, DoS, embarrassment of the company or clients, or pride in exploiting a notable target.
- **Classes of attack:** Classes of attack may include passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through the service provider.

Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation states. A system must be able to limit damage and recover rapidly when attacks occur.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Classes of Attack

There are five classes of attack:

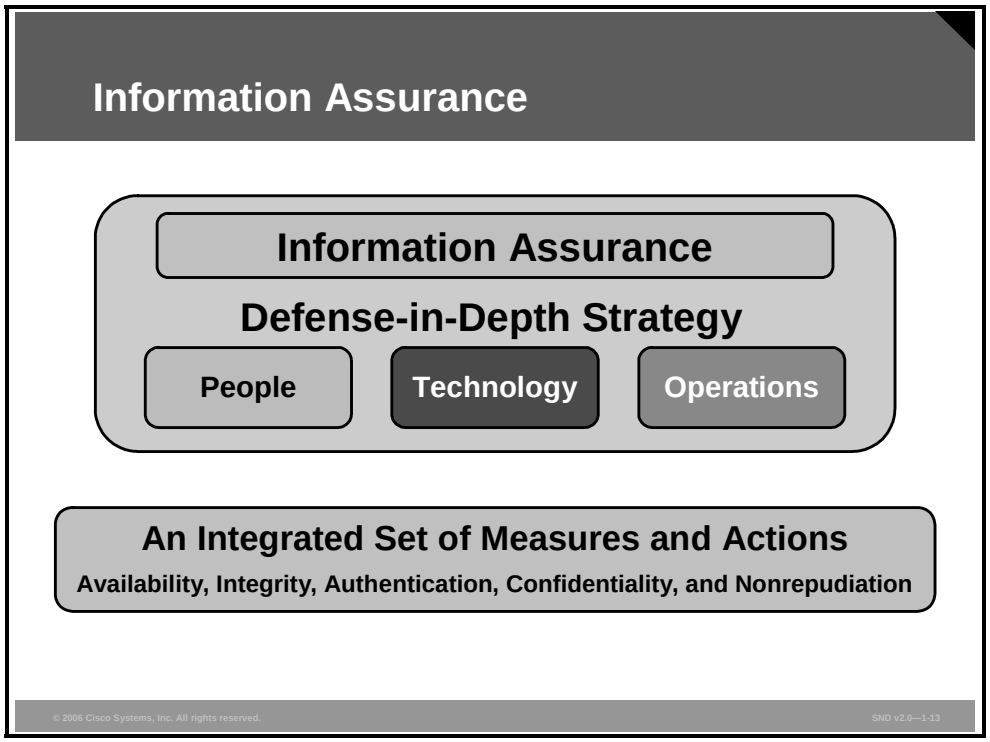
- **Passive:** Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations lets adversaries see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
- **Active:** Active attacks include attempts to circumvent or break protection features, introduce malicious code, and steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.
- **Close-in:** Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry to the network, open access, or both.
- **Insider:** Insider attacks can be malicious or nonmalicious. Malicious insiders intentionally eavesdrop, steal, or damage information, use information in a fraudulent manner, or deny access to other authorized users. Nonmalicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.
- **Distribution:** Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a backdoor to a product to gain unauthorized access to information or to a system function at a later date.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Information Assurance

This topic describes how achieving information assurance requires a balanced focus on people, technology, and operations.




Information assurance ensures that information and information systems are protected against attacks through the application of security services such as availability, integrity, authentication, confidentiality, and nonrepudiation. In addition to incorporating protection mechanisms, organizations need to expect attacks and must include attack detection tools and procedures that allow the organizations to react to and recover from attacks.

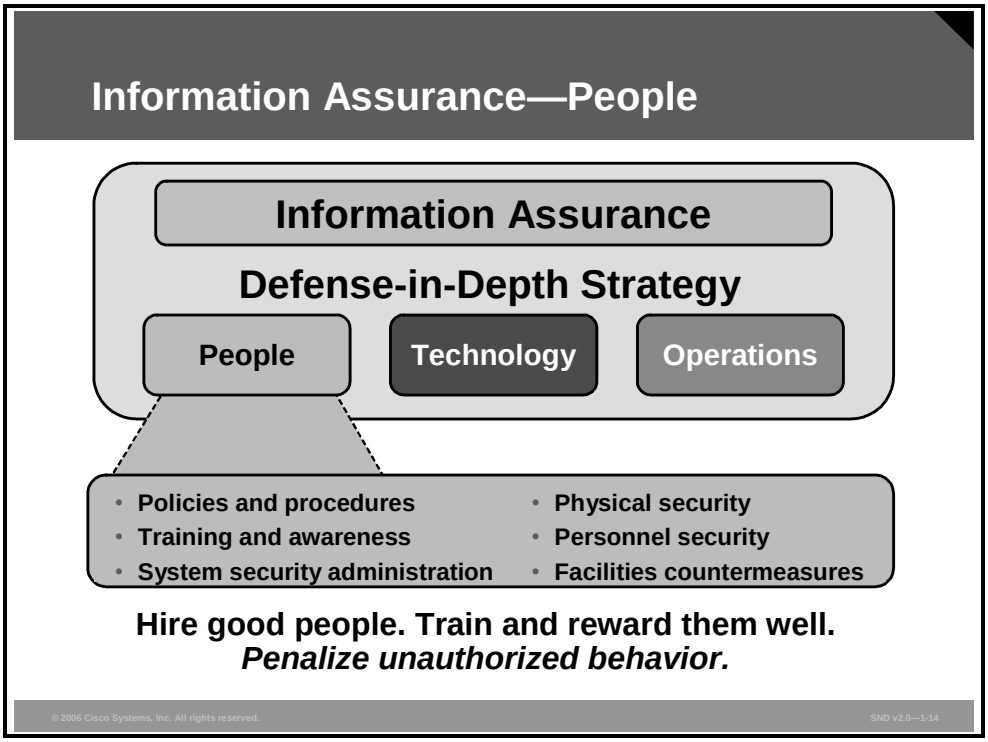
An important principle of the defense-in-depth strategy is that achieving information assurance requires a balanced focus on these three primary elements:

- People
- Technology
- Operations

Managers provide information assurance by protecting information and information systems against attacks. The network security measures taught in this course are part of the information assurance strategy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

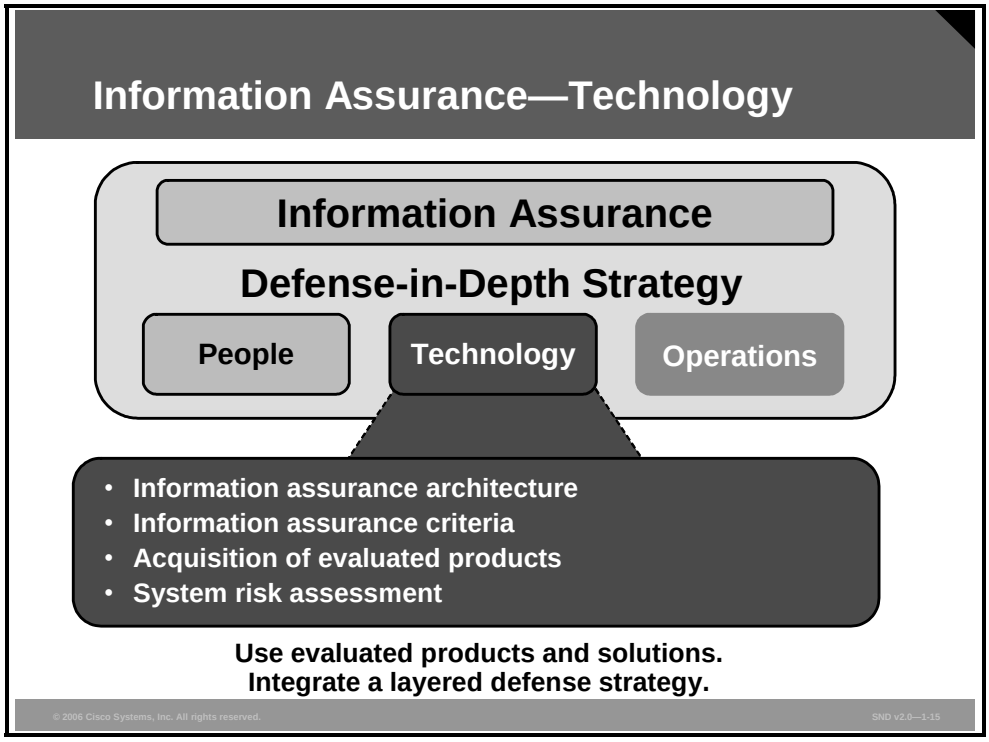



This figure shows some of the disciplines associated with people in the defense-in-depth strategy.

Achieving information assurance begins with a senior-level management commitment (typically at the chief information officer level) based on a clear understanding of the perceived threat. The commitment must be followed by effective information assurance policies and procedures, assignment of roles and responsibilities, commitment of resources, training of critical personnel such as users and system administrators, and personal accountability. Information assurance includes the establishment of physical security and personnel security measures to control and monitor access to facilities and to critical elements of the information technology (IT) environment.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

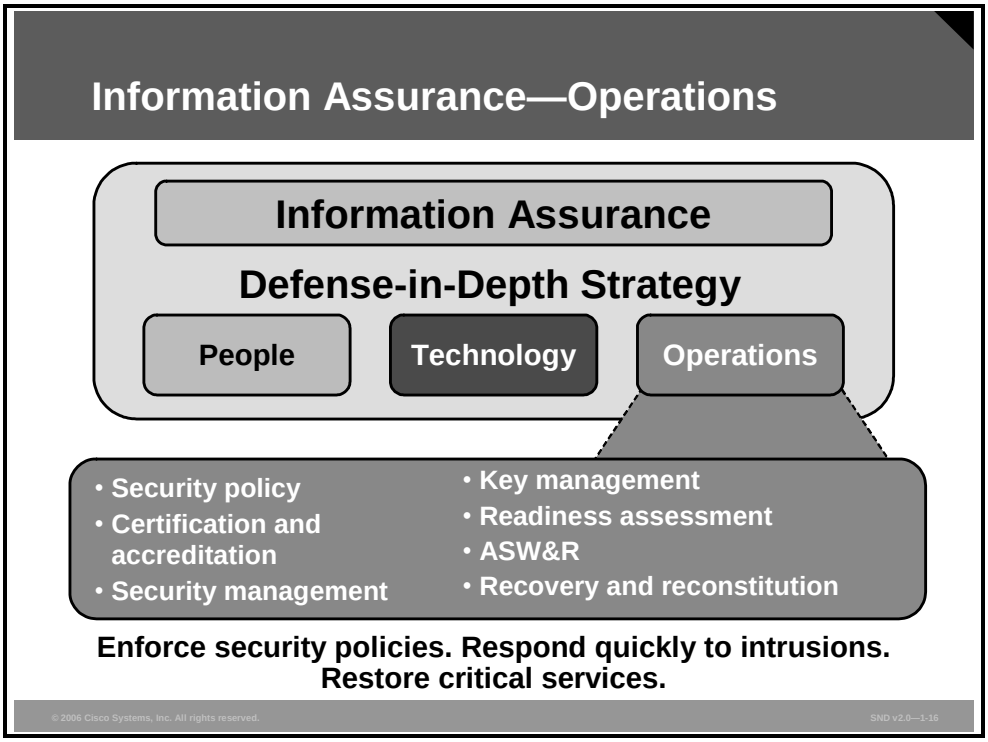



This figure shows some of the technology areas addressed in the defense-in-depth strategy.

A wide range of technologies are available for providing information assurance services and for detecting intrusions. Organizations must establish effective policies and processes for technology acquisition to procure and deploy the right technologies. These policies should include security policies, information assurance principles, system-level information assurance architectures and standards, criteria for needed information assurance products, acquisition of products that have been validated by a reputable third party, configuration guidance, and processes for assessing the risk of the integrated systems.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




This figure lists some of the operational focus areas associated with the defense-in-depth strategy.

The operational element focuses on all of the activities required to sustain the organization security posture on a daily basis. The operational element performs these functions:

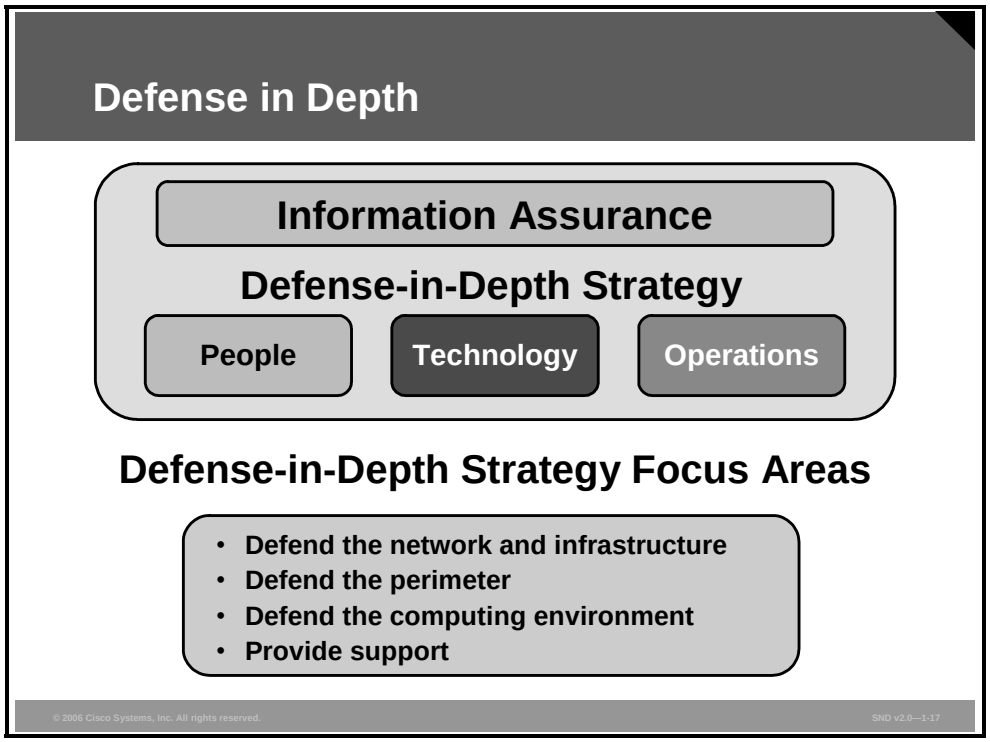
- Maintaining a visible and up-to-date system security policy
- Certifying and accrediting changes to the information technology baseline. (Certification and accreditation processes should provide the data to support risk management-based decisions. These processes should also acknowledge that a risk accepted by one user is a risk shared by many users in an interconnected environment.)
- Managing the security posture of the information assurance technology (for example, installing security patches and virus updates, maintaining access control lists)
- Providing key management services and protecting the lucrative infrastructure
- Performing system security assessments to assess the continued security readiness of the system (For example, using vulnerability scanners or “red teams” are methods of testing system security.)
- Monitoring and reacting to current threats
- Sensing, warning, and responding to attacks
- Recovering and reconstituting the system



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Principles of Defense in Depth

Defense in depth is a practical strategy for achieving information assurance. This topic describes the concept of defense in depth.




Securing information and systems against all threats requires multiple, overlapping protection approaches that address the people, technology, and operational aspects of information technology. Using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will ensure the system is never unprotected.

The defense-in-depth strategy recommends several principles.

- **Defense in multiple places:** Given that insiders or outsiders can attack a target from multiple points, an organization must deploy protection mechanisms at multiple locations to resist all classes of attacks. At a minimum, these three defensive focus areas should be included:
  - **Defend the networks and infrastructure**
    - Protect the local and wide-area communications networks from attacks such as DoS attacks
    - Provide confidentiality and integrity protection for data transmitted over the networks; for example, use encryption and traffic flow security measures to resist passive monitoring
  - **Defend the enclave boundaries**
    - Deploy firewalls and intrusion detection systems (IDS) or intrusion protection systems (IPS) or both to resist active network attacks
  - **Defend the computing environment**
    - Provide access controls and host intrusion prevention systems (HIPS) on hosts and servers to resist insider, close-in, and distribution attacks

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Build layered defenses:** Even the best available information assurance products have inherent weaknesses. Therefore, it is only a matter of time before an adversary will find an exploitable vulnerability. An effective countermeasure is to deploy multiple defense mechanisms between the adversary and the target. Each of these mechanisms must present unique obstacles to the adversary. Further, each should include both protection and detection measures. These measures increase risk of detection for adversaries while reducing their chances of success or by making successful penetrations unaffordable. One example of a layered defense is to have nested firewalls (each coupled with IDS and IPS) deployed at outer and inner network boundaries. The inner firewalls may support more granular access control and data filtering.
- **Use robust components:** Specify the security robustness (that is, strength and assurance) of each information assurance component as a function of the value of what it is protecting and the threat at the point of application. For example, it is often more effective and operationally suitable to deploy stronger mechanisms at the network boundaries than at the user desktop.
- **Employ robust key management:** Deploy robust key management and public key infrastructures that support all of the incorporated information assurance technologies and that are highly resistant to attack. This latter point recognizes that these infrastructures are lucrative targets.
- **Deploy IDS and IPS:** Deploy infrastructures to detect and prevent intrusions and to analyze and correlate the results and react accordingly. These infrastructures should help the operations staff to answer questions such as Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options?



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Layered Defense

| Class of Attack | First Line of Defense | Second Line of Defense |
|---|---|---|
| Passive | Link layer and network layer encryption and traffic flow security | Security-enabled applications |
| Active | Defend the enclave boundaries | Defend the computing environment |
| Insider | Physical and personnel security | Authenticated access controls, audit |
| Close-In | Physical and personnel security | Technical surveillance countermeasures |
| Distribution | Trusted software development and distribution | Run-time integrity controls |

© 2006 Cisco Systems, Inc. All rights reserved.

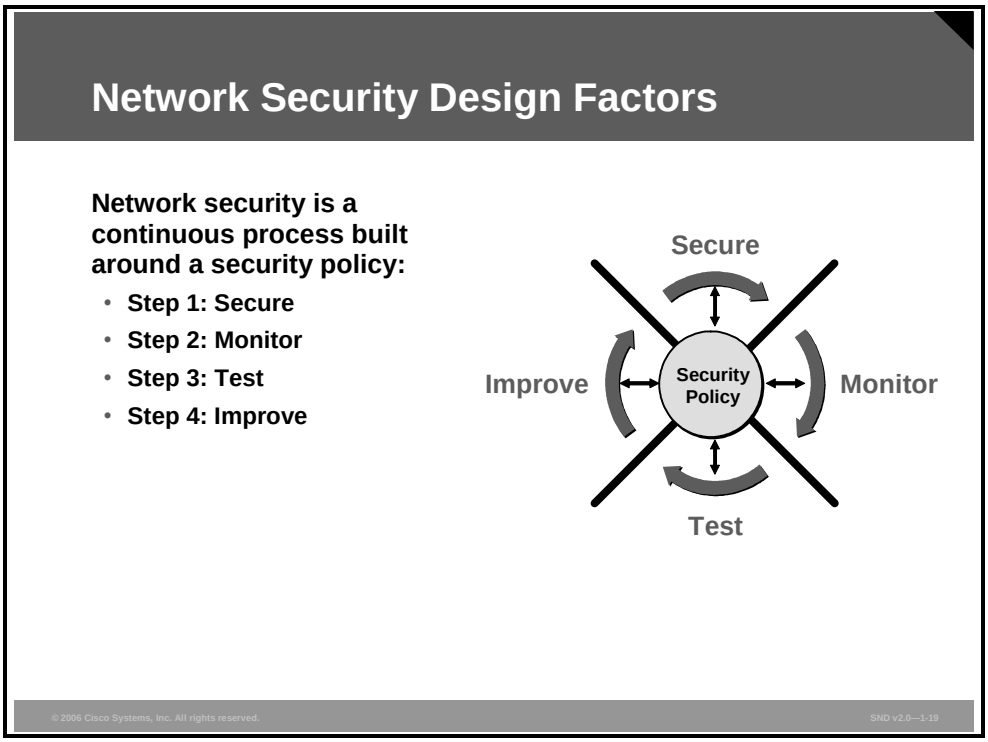

A comprehensive corporate security policy provides in-depth defense. The figure shows the components of a layered defense strategy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Network Security Process

This topic explains the process of maintaining continuous security based on the four sections of the security wheel.




The figure shows the security wheel. This wheel describes the steps that an organization will continuously cycle through to verify the security of the network.

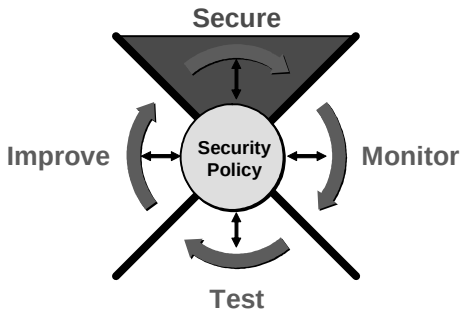


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Secure the Network

**This step involves implementing security solutions to stop or prevent unauthorized access or activities and to protect information. These solutions should be included:**

- **Authentication**
- **Encryption**
- **Firewalls**
- **Vulnerability patching**




© 2006 Cisco Systems, Inc. All rights reserved.


The first step in the security process is to secure the network as described in the figure. When you secure your network, your actions in doing so will be guided by the security policy.

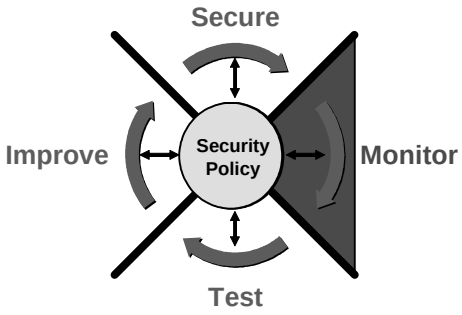


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Monitor Security

**This step involves taking these actions:**

- **Detect violations to the security policy**
- **Involve system auditing and real-time intrusion detection**
- **Validate the security implementation in the previous step where you secured the network**




© 2006 Cisco Systems, Inc. All rights reserved.

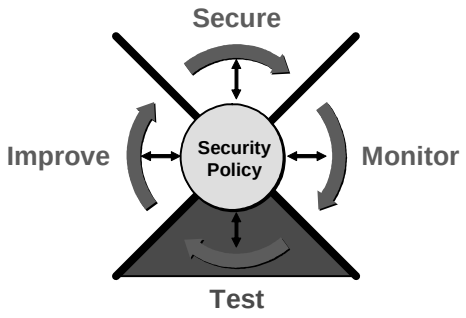

When the network has been secured, you must monitor the network. Failure to monitor the security that you have put in place could result in breaches that go unchallenged by the organization.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Test Security

**This step involves validating the effectiveness of the security policy through system auditing and vulnerability scanning.**




© 2006 Cisco Systems, Inc. All rights reserved.


After monitoring the network, you should further test your systems. Testing ensures that the network security systems are working as they should be, and that any changes (planned or accidental) that may happen in the network are captured and fixed before they can create security problems in the network.

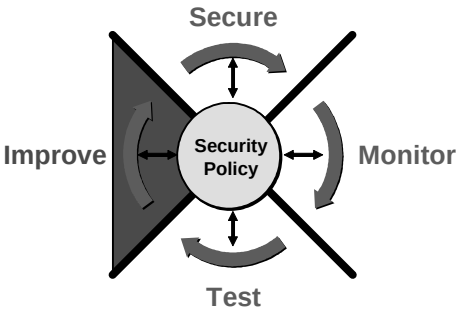


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Improve Security

**This step involves taking these actions:**

- **Use information from the monitor and test phases to make improvements to the security implementation**
- **Adjust the security policy as security vulnerabilities and risks are identified**




© 2006 Cisco Systems, Inc. All rights reserved.

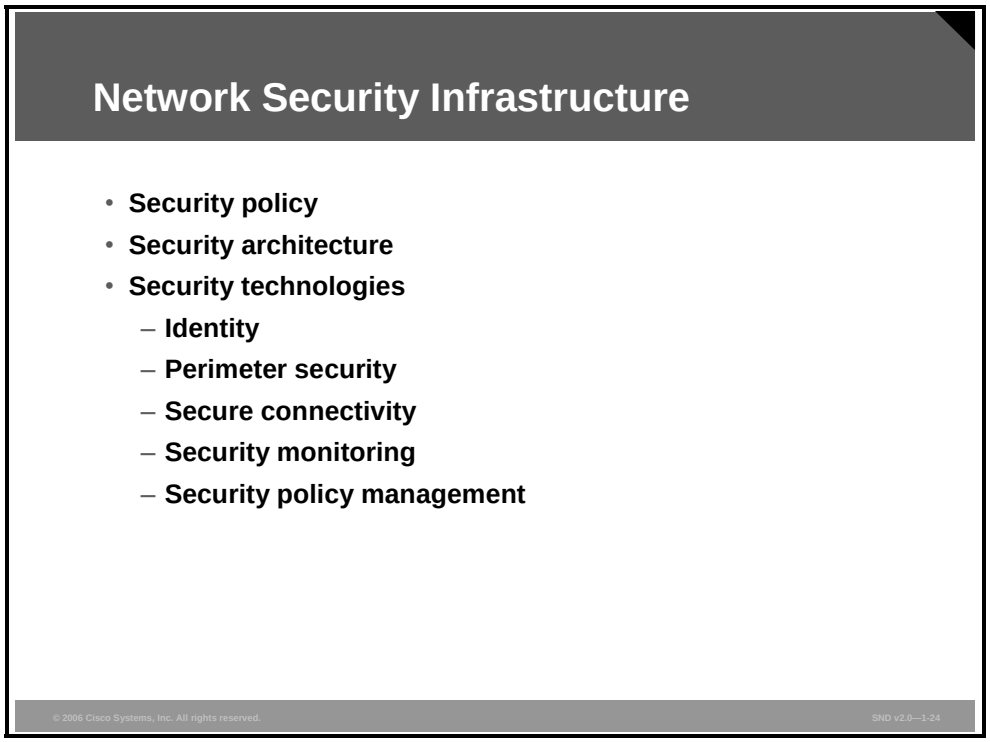

As described in the figure, monitoring and testing of network security may identify aspects of the network that can be improved.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Network Security Design Factors

This topic describes the factors that companies should consider when designing a secure network infrastructure.




The goal of network security is to protect networks and their applications against attack to ensure the availability, confidentiality, and integrity of information. Here are the factors that companies need to consider when building a secure network architecture:

- **Security policy:** A comprehensive security policy is the driver for the security design process. The security policy is a formal statement supported by the leadership of the company. The policy must address these two issues:
  - The security requirements as driven by the business needs of the company
  - The implementation guidelines regarding the available technology

  Because both of these issues change, the security policy is a living document subject to continuing review and revision.
- **Security architecture:** Network design and IT security teams design the security architecture. Their design goal is to ensure efficient user access while building layers of security that will contain attacks to limited parts of the network. Security architectures are typically implemented in phases, addressing the most operationally critical areas first.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

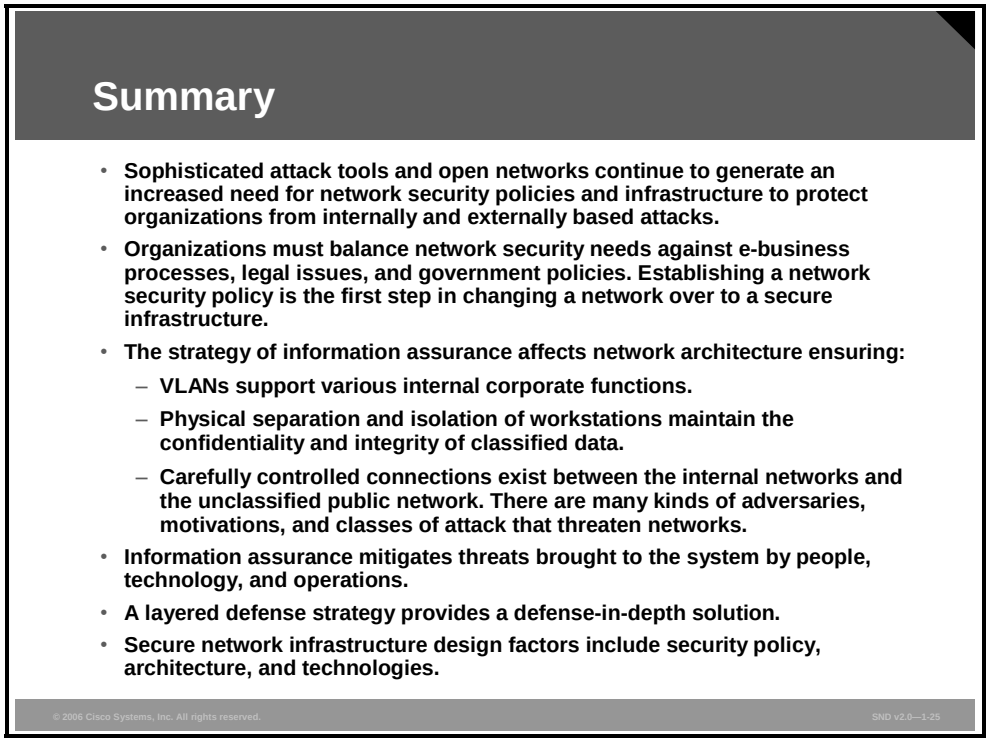
- **Security technologies:** Companies must balance the cost of technology against the benefits of defending their networks. Companies then need to allocate their budgets accordingly. Every design should include components that address each of these factors:
  - Identity
  - Perimeter security
  - Secure connectivity
  - Security monitoring
  - Security policy management



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.




# Additional Resources

Much of the material in this lesson comes from readily available documents provided by many government agencies. The Information Assurance Technical Framework Forum (IATFF) is a National Security Agency (NSA)-sponsored outreach activity created to foster dialog aimed at seeking solutions for information assurance problems. The IATFF website can be found at http://www.iatf.net.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 2

# Introducing Network Attack Mitigation Techniques

## Overview

This lesson describes types of network attacks and provides some techniques for reducing vulnerabilities and determining and mitigating common network attacks.

## Objectives

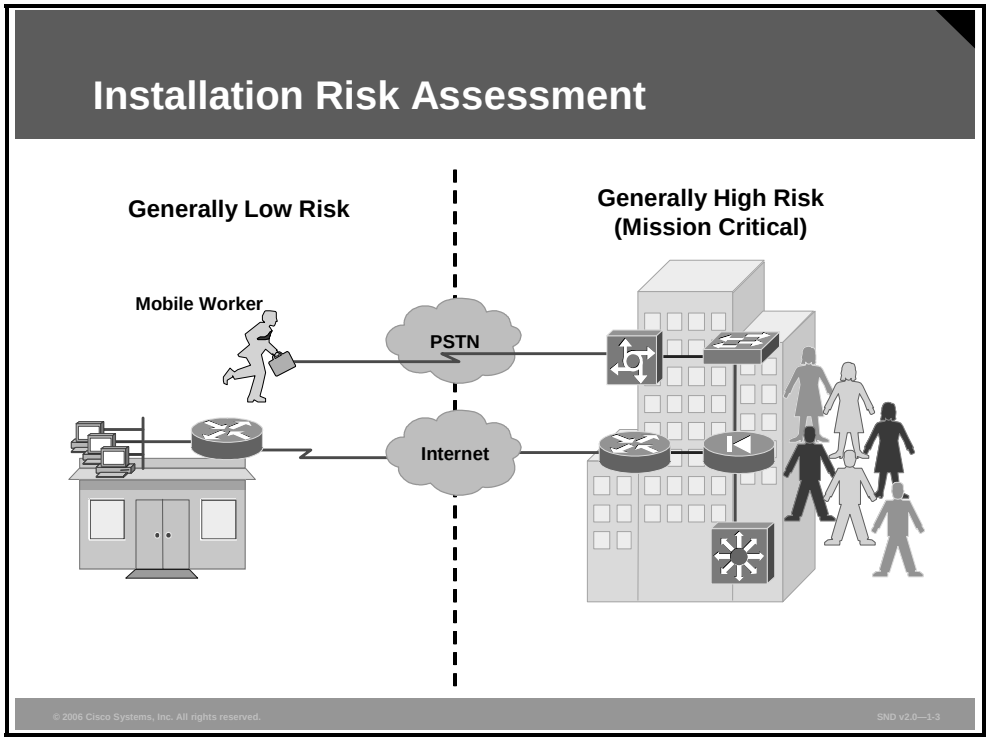
Upon completing this lesson, you will be able to explain the strategies used to mitigate network attacks. This ability includes being able to meet these objectives:

- Describe how to mitigate hardware, environmental, electrical, and maintenance-related security threats to Cisco routers and switches
- Describe the mitigation of reconnaissance attacks including packet sniffers, port scans, ping sweeps, and Internet information queries
- Describe the mitigation of access attacks including password attacks, trust exploitation, port redirection, and man-in-the-middle attacks
- Describe how hackers use IP spoofing to launch various types of attacks
- Describe the mitigation of DoS and DDoS attacks
- Describe the mitigation of worm, virus, and Trojan horse attacks
- Describe the mitigation of application layer attacks
- Describe the vulnerabilities in configuration management protocols and recommendations for mitigating these vulnerabilities
- Describe how to discover network vulnerabilities and threats with GNU Netcat, BluesPortScan, Ethereal, and MBSA

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Mitigating Physical and Environmental Threats

Improper and incomplete network device installation is an often overlooked security threat that, if left unheeded, can have dire results. Software-based security measures alone cannot prevent premeditated or even accidental network damage due to poor installation. This topic describes how to mitigate hardware, environmental, electrical, and maintenance-related security threats to Cisco routers and switches.




Before discussing how to secure Cisco network installations, it is important to make the distinction between low-risk and high-risk devices:

- **Low-risk devices:** These devices are typically low-end, either small office/home office (SOHO) devices. Examples of SOHO devices include the Cisco 800 Series Routers, CiscoPro CPA 900 Series Routers, Cisco 1700 Series Modular Access Routers, Cisco 1800 Series Integrated Services Routers, and Cisco switches in environments where access to the physical devices and cabling does not present a high risk to the corporate network. In these types of installations, it may be physically impossible and too costly to provide a locked wiring closet for physical device security. In these situations, the information technology (IT) manager must decide which devices can be physically secured and which devices cannot be secured and then assess the risk.
- **High-risk (mission-critical) devices:** You will find these devices in larger offices or corporate campuses where tens, hundreds, or even thousands of employees reside, or where the same large numbers of employees remotely access corporate data. These devices are usually Cisco routers, Cisco Catalyst switches, firewalls, and management systems used to route and control large amounts of data, voice, and video traffic. Companies compromise the security of these devices if disgruntled employees have physical access or there are negative environmental conditions.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Common Threats to Physical Installations

- **Hardware threats**
- **Environmental threats**
- **Electrical threats**
- **Maintenance threats**



© 2006 Cisco Systems, Inc. All rights reserved.


There are four classes of insecure installations or physical access threats:

- **Hardware threats:** The threat of physical damage to the router or switch hardware
- **Environmental threats:** Threats such as temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry)
- **Electrical threats:** Threats such as voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
- **Maintenance threats:** Threats such as poor handling of key electronic components (electrostatic discharge), lack of critical spares, poor cabling, poor labeling, and so on

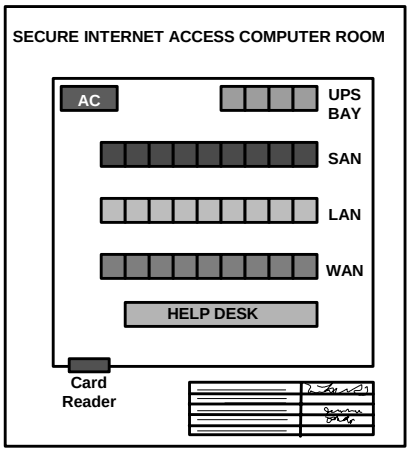


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Hardware Threat Mitigation

**Plan physical security to limit damage to the equipment:**

- **Lock up equipment and prevent unauthorized access from the doors, ceiling, raised floor, windows, ducts, or vents**
- **Monitor and control closet entry with electronic logs**
- **Use security cameras**




SAN = Storage Area Network

© 2006 Cisco Systems, Inc. All rights reserved.


Mission-critical Cisco network equipment should be located in wiring closets or in computer or telecommunications rooms that meet these minimum requirements:

- The room must be locked with only authorized personnel allowed access.
- The room should not be accessible via a dropped ceiling, raised floor, window, ductwork, or point of entry other than the secured access point.
- If possible, use electronic access control with all entry attempts logged by security systems and monitored by security personnel.
- If possible, security personnel should monitor activity via security cameras with automatic recording.

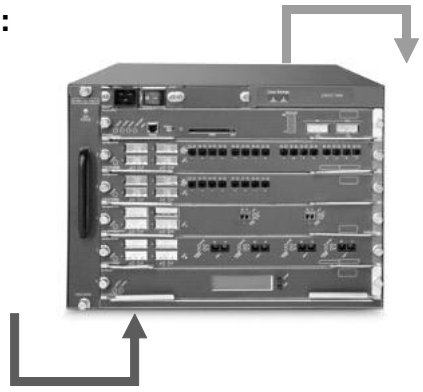


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Environmental Threat Mitigation

**Limit damage by creating a proper operating environment:**

- **Temperature control**
- **Humidity control**
- **Positive air flow**
- **Remote environmental alarming, recording, and monitoring**



© 2006 Cisco Systems, Inc. All rights reserved.


Take these actions to limit environmental damage to Cisco network devices:

- Supply the room with dependable temperature and humidity control systems. Always verify the recommended environmental parameters of the Cisco network equipment with the supplied product documentation.
- Remove any sources of electrostatic and magnetic interferences in the room.
- If possible, remotely monitor and alarm the environmental parameters of the room.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Electrical Threat Mitigation

**Limit electrical supply problems:**

- **Install UPS systems**
- **Install generator sets**
- **Follow a preventative maintenance plan**
- **Install redundant power supplies**
- **Perform remote alarming and monitoring**



© 2006 Cisco Systems, Inc. All rights reserved.


Electrical supply problems can be limited by adhering to these guidelines:

- Install uninterrupted power supply (UPS) systems for mission-critical Cisco network devices.
- Install backup generator systems for mission-critical supplies.
- Plan for and initiate regular UPS or generator testing and maintenance procedures based on the manufacturer suggested preventative maintenance schedule.
- Install redundant power supplies on critical devices.
- Monitor and alarm power-related parameters at the power supply and device levels.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Maintenance-Related Threat Mitigation

**Limit maintenance-related threats:**

- **Use neat cable runs**
- **Label critical cables and components**
- **Use electrostatic discharge procedures**
- **Stock critical spares**
- **Control access to console ports**



© 2006 Cisco Systems, Inc. All rights reserved.


Maintenance-related threats compose a broad category of threats that include many items. Follow the general rules listed here to prevent these types of threats:

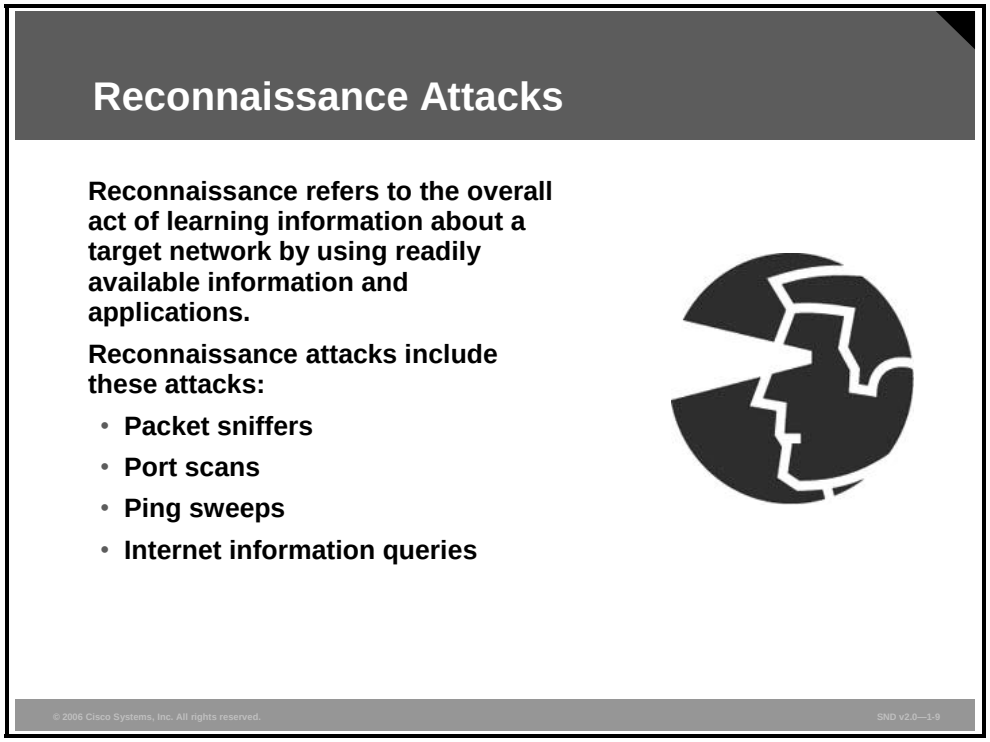
- Clearly label all equipment cabling and secure the cabling to equipment racks to prevent accidental damage, disconnection, or incorrect termination.
- Use cable runs, raceways, or both, to traverse rack-to-ceiling or rack-to-rack connections.
- Always follow electrostatic discharge procedures when replacing or working with internal router and switch device components.
- Maintain a stock of critical spares for emergency use.
- Do not leave a console connected to and logged into any console port. Always log off administrative interfaces when leaving a station.
- Do not rely upon a locked room as the only necessary protection for a device. Always remember that no room is ever totally secure. After intruders are inside a secure room, there is nothing to stop them from connecting a terminal to the console port of a Cisco router or switch.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Reconnaissance Attacks and Mitigation

This topic describes the mitigation of reconnaissance attacks including packet sniffers, port scans, ping sweeps, and Internet information queries.




Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. Reconnaissance is also known as information gathering, and in most cases, precedes an actual access or denial of service (DoS) attack. First, the malicious intruder typically conducts a ping sweep of the target network to determine which IP addresses are alive. Then the intruder determines which services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the type and version of the application and operating system running on the target host.

Reconnaissance is somewhat analogous to a thief investigating a neighborhood for vulnerable homes, such as an unoccupied residence or a house with an easy-to-open door or window to break into. In many cases, intruders look for vulnerable services that they can exploit later when there is less likelihood that anyone is looking.

Reconnaissance attacks can consist of these types of attacks:

- Packet sniffers
- Port scans
- Ping sweeps
- Internet information queries

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Packet Sniffers




**A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets. There are packet sniffer features:**

- **Packet sniffers exploit information passed in clear text. Protocols that pass information in clear text are Telnet, FTP, SNMP, Post Office Protocol (POP), and HTTP.**
- **Packet sniffers must be on the same collision domain as the machine that they are targeting.**
- **Packet sniffers can be used legitimately or can be designed specifically for attack.**

© 2006 Cisco Systems, Inc. All rights reserved.


In an Ethernet LAN, promiscuous mode is a mode of operation in which a network adapter can receive and read every data packet transmitted. Promiscuous mode is the opposite of nonpromiscuous mode. When devices transmit data packets in nonpromiscuous mode, all other LAN devices “listen” to the data to determine if the network address included in the data packet is theirs.

A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets sent across a LAN. Packet sniffers can only work in a single collision domain. Promiscuous mode is a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing.

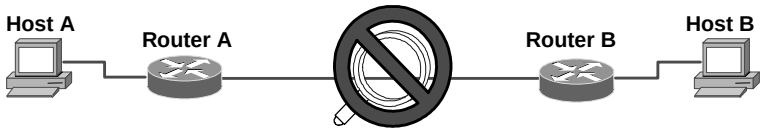
Several network applications distribute network packets in clear text. Clear text is information sent across the network without encryption. Sending clear text in network packets is problematic because if the network packets are intercepted an attacker can easily read the packet contents.

A network protocol specifies the format and protocol operations. Because the specifications for network protocols, such as TCP/IP, are widely published, a third party can easily interpret the network packets and develop a packet sniffer. Numerous freeware and shareware packet sniffers are available that do not require the user to understand anything about the underlying protocols.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Packet Sniffer Attack Mitigation




**Here are some packet sniffer mitigation techniques and tools:**

- **Authentication**
- **Switched infrastructure**
- **Antisniffer tools**
- **Cryptography**

© 2006 Cisco Systems, Inc. All rights reserved.


Use these techniques and tools to mitigate packet sniffer attacks:

- **Authentication:** Using strong authentication is a first option for defense against packet sniffers. In general, strong authentication is a way to authenticate users and is not easily circumvented. A common example of strong authentication is a one-time password (OTP).

  An OTP is a type of two-factor authentication. Two-factor authentication involves using something that you have combined with something that you know. ATMs use two-factor authentication. A customer needs both an ATM card and a PIN to make transactions. With OTPs, you need a PIN and your token card to authenticate to a device or software application. A token card is a hardware or software device that generates new, seemingly random passwords at specified intervals (usually 60 seconds). A user combines the current password with a PIN to create a unique password that works only for one instance of authentication. If a hacker learns that password by using a packet sniffer, the information is useless because the password has already expired. Note that this mitigation technique is effective only against a sniffer implementation designed to grab passwords. Sniffers deployed to learn sensitive information (such as e-mail messages) will still be effective.

- **Switched infrastructure:** This technique counters the unauthorized use of packet sniffers in your network environment. For example, if an entire organization deploys switched Ethernet, hackers can gain access only to the traffic that flows on the specific port to which they connect. A switched infrastructure obviously does not eliminate the threat of packet sniffers, but it can greatly reduce their effectiveness.

- **Antisniffer tools:** Use software and hardware designed to detect the use of sniffers on a network. Such software and hardware reduce the threat, but like many network security tools, they are part of the overall system. Antisniffer tools detect changes in the response time of hosts to determine whether the hosts are processing more traffic than their own traffic loads would indicate. One such network security software tool, AntiSniff, is available from Security Software Technologies.



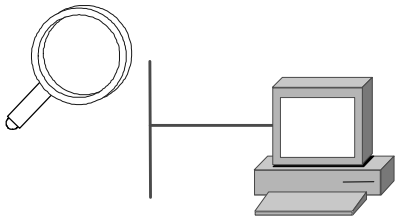
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Cryptography:** Rendering packet sniffers irrelevant is the most effective method for countering packet sniffers. Cryptography is even more effective than preventing or detecting packet sniffers. If a communication channel is cryptographically secure, the only data that a packet sniffer detects is cipher text (a seemingly random string of bits) and not the original message. Cisco Systems bases the deployment of network-level cryptography on IPsec, which is a standard method for networking devices to communicate privately using IP. Other cryptographic protocols for network management include Secure Shell (SSH) and Secure Sockets Layer (SSL).



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Port Scans and Ping Sweeps



**Port scan and ping sweep attacks:**

- **Identify all services on the network**
- **Identify all hosts and devices on the network**
- **Identify the operating systems on the network**
- **Identify vulnerabilities on the network**

© 2006 Cisco Systems, Inc. All rights reserved.

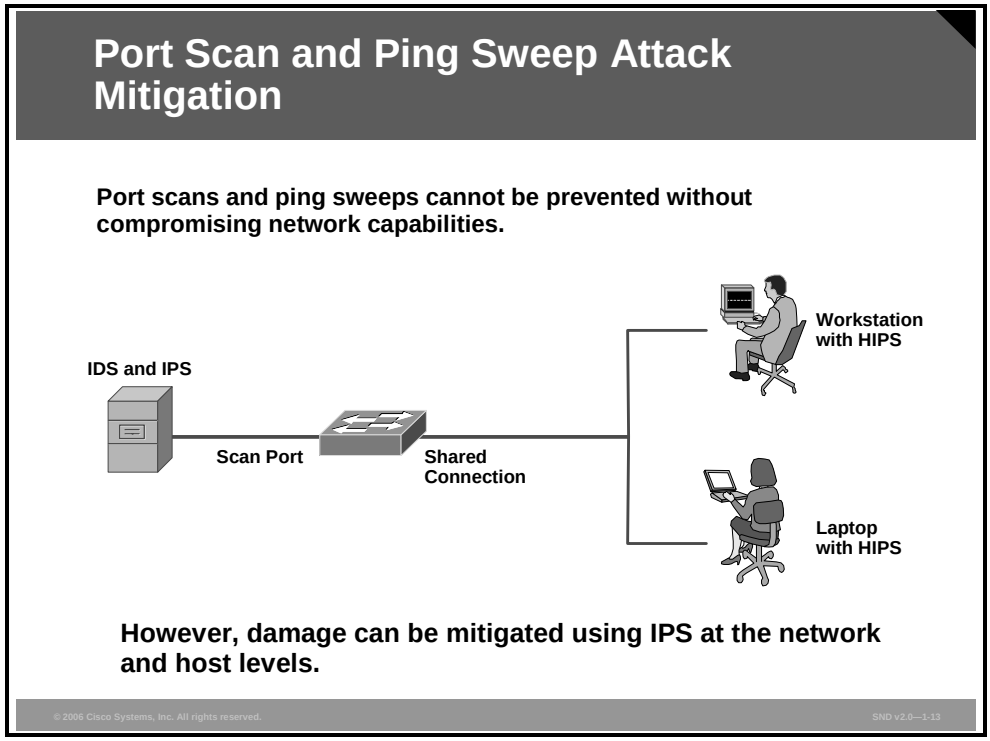

As legitimate tools, port scan and ping sweep applications run a series of tests against hosts and devices to identify vulnerable services needing attention. IP addressing and port or banner data from both TCP and UDP ports are examined to gather information.

In an illegitimate situation, a port scan can be a series of messages sent by someone attempting to break into a computer to learn which computer network services (each service is associated with a well-known port number) the computer provides. Port scanning can be an automated scan of a range of TCP or UDP port numbers on a host to detect listening services. Port scanning, a favorite computer hacker approach, provides information to the assailant about where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is being used and needs probing.

A ping sweep (also known as an Internet Control Message Protocol [ICMP] sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers). A ping sweep consists of ICMP echo-requests (pings) sent to multiple hosts, whereas a single ping will tell you whether one specified host computer exists on the network. If a given address is live, that host will return an ICMP echo-reply. Ping sweeps are among the older and slower methods used to scan a network. As an attack tool, a ping sweep sends ICMP echo-requests to a range of IP addresses, with the goal of finding hosts to probe for vulnerabilities.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Port scanning and ping sweeping are not crimes, and there is no way to prevent these tools from being used on Internet-connected devices. Accessing an Internet server opens a port, which opens a door to the computer. However, there are ways to prevent damage to the system from an open port.

Blocking ICMP echo and echo-reply on edge routers stops ping sweeps. However, network diagnostic data is lost for legitimate uses.

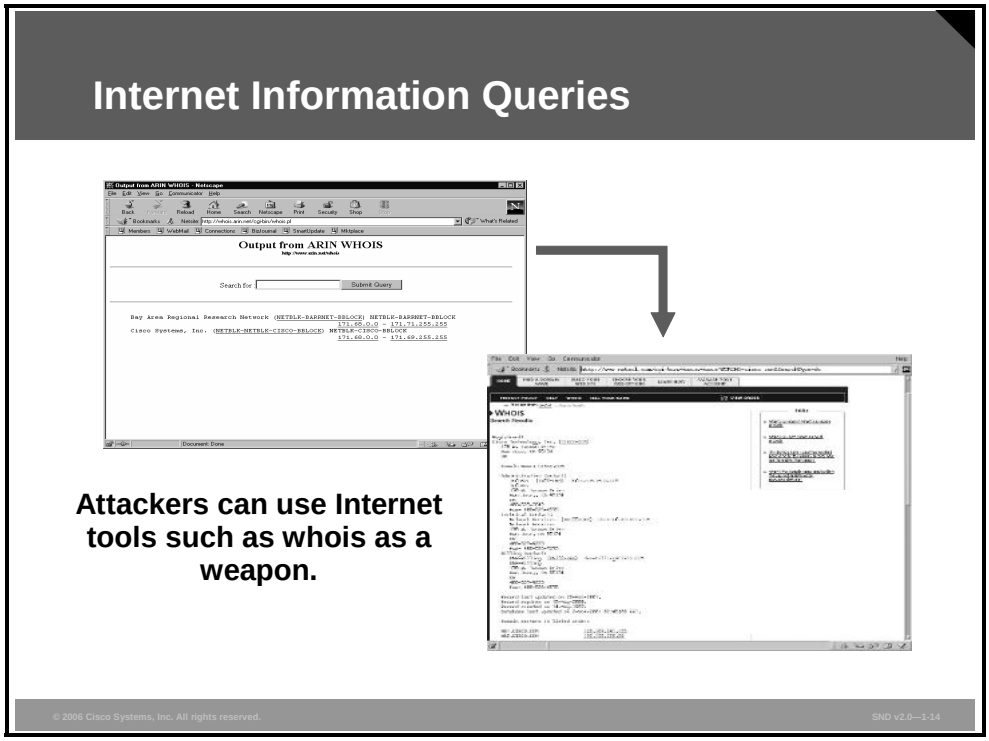
Network intrusion prevention systems and host intrusion prevention systems (HIPS) can usually notify an administrator when a reconnaissance attack is under way. This warning allows the administrator to prepare for the coming attack or to notify the Internet service provider (ISP) that is hosting the system launching the reconnaissance probe.

ISPs compare incoming traffic to the intrusion detection system (IDS) signatures and intrusion prevention system (IPS) signatures or both signatures in the ISP database. Signatures are characteristics of particular traffic patterns. A signature such as “several packets to different destination ports from the same source address within a short period of time” might detect port scans. Another such signature could be “SYN to a nonlistening port.”

Stealth scan is a technique that relies on bugs in networking code. It is difficult, but not impossible to execute a stealth scan on Cisco IOS software. A stealth scan has the advantages of being difficult to detect, and many intrusion detection and prevention systems allow it to go unnoticed. Discovering stealth scans requires kernel-level work.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




This figure demonstrates how to use Internet tools for network reconnaissance.

Domain Name System (DNS) queries can reveal such information as who owns a particular domain and its addresses. Ping sweeps of the addresses revealed by DNS queries can present a picture of the live hosts in a particular environment. After generating the list, port scanning tools can cycle through all well-known ports to provide a complete list of all services running on the hosts discovered by the ping sweep. Finally, the hackers can examine the characteristics of the applications that are running on the hosts. This step can lead to specific information that is useful when the hacker attempts to compromise the service.

IP address queries can reveal information such as who owns a particular IP address or range of addresses and what domain is associated with those addresses.

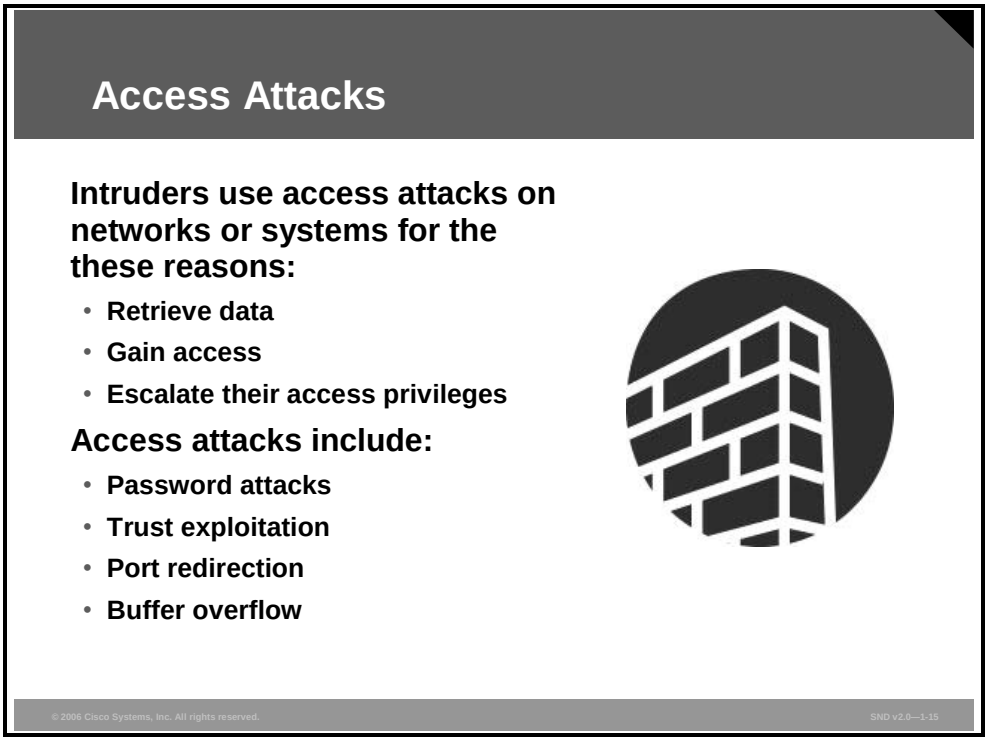
| | |
|---|---|
| **Note** | Organizational websites are archived at http://www.archive.org. Archived versions may include instances of a website that breach good security practices for today. |

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Access Attacks and Mitigation

This topic describes how to mitigate access attacks.




Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. Access attacks can consist of these types of attacks:

- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle attacks
- Buffer overflow

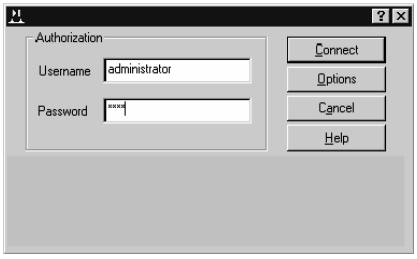


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Password Attacks

**Hackers implement password attacks using:**

- **Brute-force attacks**
- **Trojan horse programs**
- **IP spoofing**
- **Packet sniffers**




© 2006 Cisco Systems, Inc. All rights reserved.


Password attacks are implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are the brute-force attacks discussed earlier.

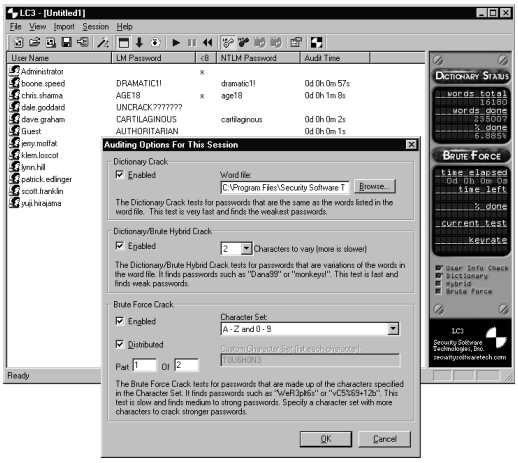
To execute a brute-force attack, an attacker can use a program that runs across the network and attempts to log in to a shared resource, such as a server. When an attacker gains access to a resource, the attacker has the same access rights as the rightful user. If this account has sufficient privileges, the attacker can create a backdoor for future access, without concern for any status and password changes to the compromised user account.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Password Attack Example

- **L0phtCrack can take the hashes of passwords and generate clear text passwords from them.**
- **Passwords are computed using two methods:**
  - **Dictionary cracking**
  - **Brute-force computation**




© 2006 Cisco Systems, Inc. All rights reserved.


Just as with packet sniffer and IP spoofing attacks, a brute-force password attack can provide access to accounts that attackers then use to modify critical network files and services. For example, an attacker compromises your network integrity by modifying your network routing tables. This trick reroutes all network packets to the attacker before transmitting them to their final destination. In such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle.

A security risk lies in the fact that passwords are stored as clear text. You need to encrypt passwords to overcome risks. On most systems, passwords are processed through an encryption algorithm that generates a one-way hash on passwords. You cannot reverse a one-way hash back to its original text. Most systems do not decrypt the stored password during authentication—they store the one-way hash. During the login process, you supply an account and password, and the password encryption algorithm generates a one-way hash. The algorithm compares this hash to the hash stored on the system. If the hashes are the same, the algorithm assumes that the user supplied the proper password.

Remember that passing the password through an algorithm results in a password hash. The hash is not the encrypted password, but rather a result of the algorithm. The strength of the hash is that the hash value can only be recreated using the original user and password information, and that it is impossible to retrieve the original information from the hash. This strength makes hashes perfect for encoding passwords for storage. In granting authorization, the hashes, rather than the plain password, are calculated and compared.

L0phtCrack is a Microsoft Windows NT password-auditing tool used to compute Microsoft Windows NT user passwords from the cryptographic hashes that are stored in the system registry. L0phtCrack computes the password from a variety of sources using a variety of methods. The result is a state of the art tool for recovering the passwords that users use.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

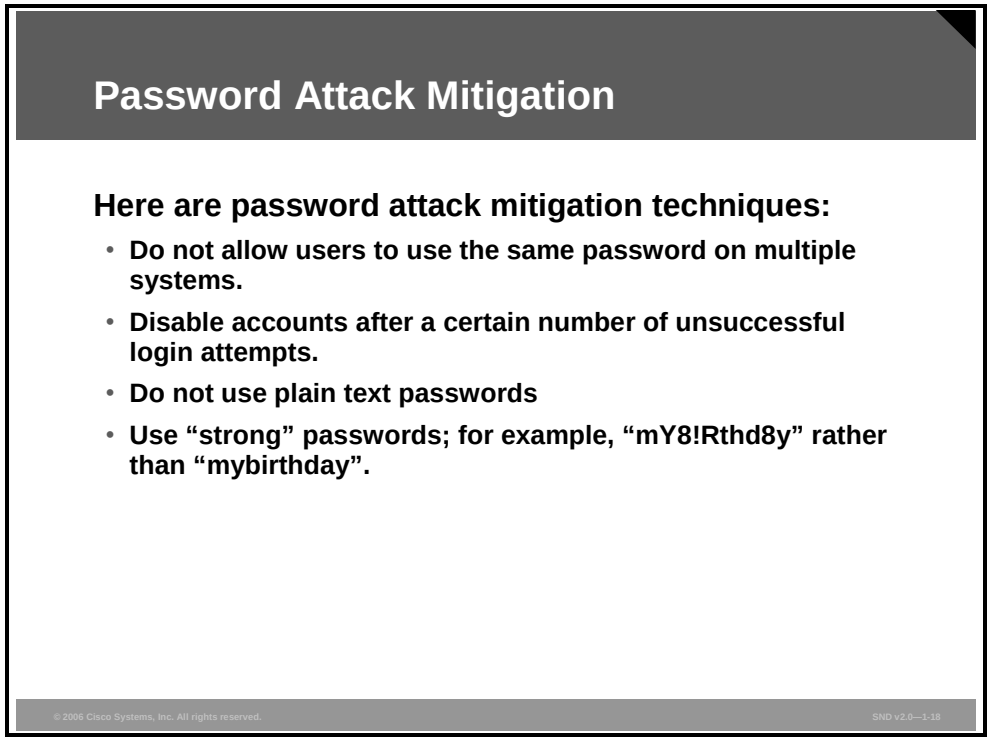
Here are the two methods for computing passwords with L0phtCrack:

- **Dictionary cracking:** The program computes and compares the password hashes for all of the words in a dictionary file against all the password hashes for the users. This method is extremely fast and finds very simple passwords.
- **Brute-force computation:** This method uses a particular character set, such as A to Z, or A to Z plus 0 to 9, and computes the hash for every possible password made up of those characters. Brute-force compilation always computes the password if that password is made up of the character set you have selected to test. The problem for the attacker is that time is required to complete this type of attack.

| | |
|---|---|
| **Note** | RainbowCrack is a compilation of hashes that provide crackers with a list that they can use to attempt to match hashes that they capture with sniffers. |


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Password attack mitigation techniques are as follows:

- Do not allow users to have the same password on multiple systems. Most users use the same password for each system they access, and often personal system passwords are also the same.
- Disable accounts after a specific number of unsuccessful logins. This practice helps to prevent continuous password attempts.
- Do not use plain text passwords. Use either an OTP or encrypted password.
- Use strong passwords. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters. Many systems now provide strong password support and can restrict a user to the use of strong passwords only.



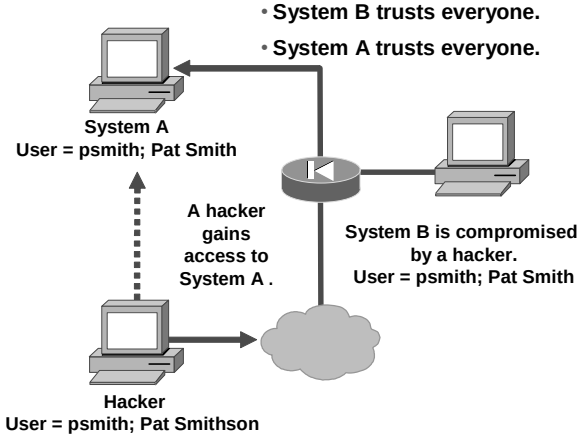
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Trust Exploitation

- **A hacker leverages existing trust relationships.**
- **Several trust models exist:**
  - **Microsoft Windows:**
    - **Domains**
    - **Active directory**
  - **Linux and UNIX:**
    - **NIS**
    - **NIS+**

**Trust relationships:**

- **System A trusts System B.**
- **System B trusts everyone.**
- **System A trusts everyone.**




© 2006 Cisco Systems, Inc. All rights reserved.

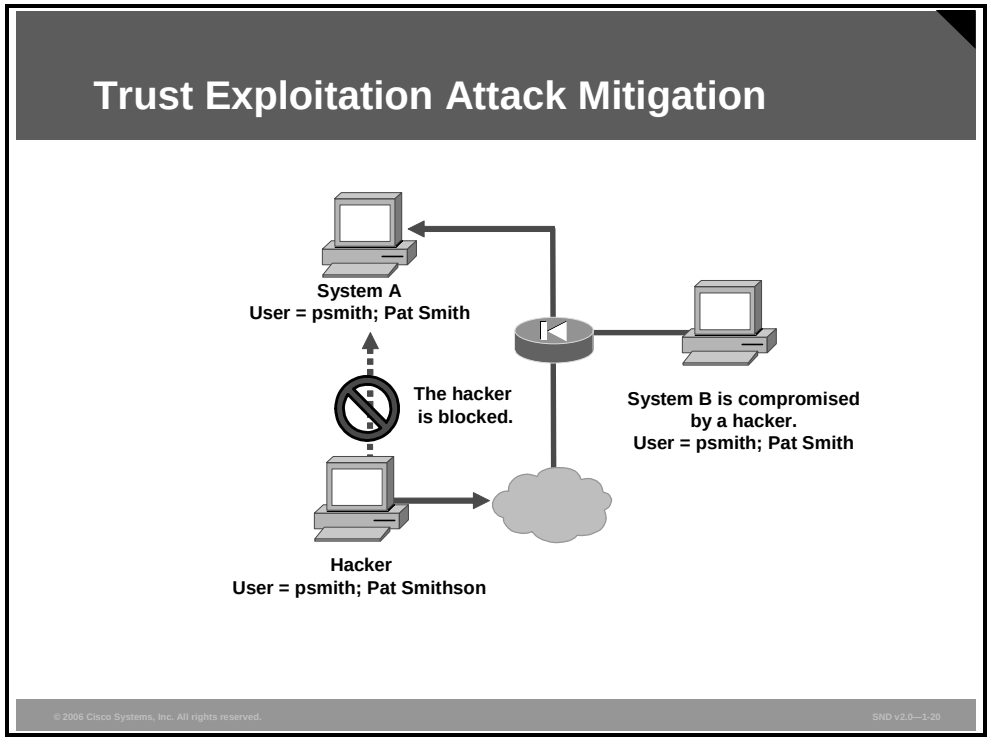

Although it is not an attack in itself, trust exploitation refers to an individual taking advantage of a trust relationship within a network.

An example of trust exploitation occurs when a perimeter network is connected to a corporate network. These two network segments often house DNS, Simple Mail Transfer Protocol (SMTP), and HTTP servers. Because these servers all reside on the same segment, a compromise of one system can lead to the compromise of other systems if those other systems trust systems that are attached to the same network.

Another example of trust exploitation occurs when a system on the demilitarized zone (DMZ) side (System B in the figure) of a firewall that has a trust relationship with a system on the inside (System A in the figure) of a firewall. When the system on the DMZ side is compromised, the attacker can leverage the trust relationship to attack the inside network.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

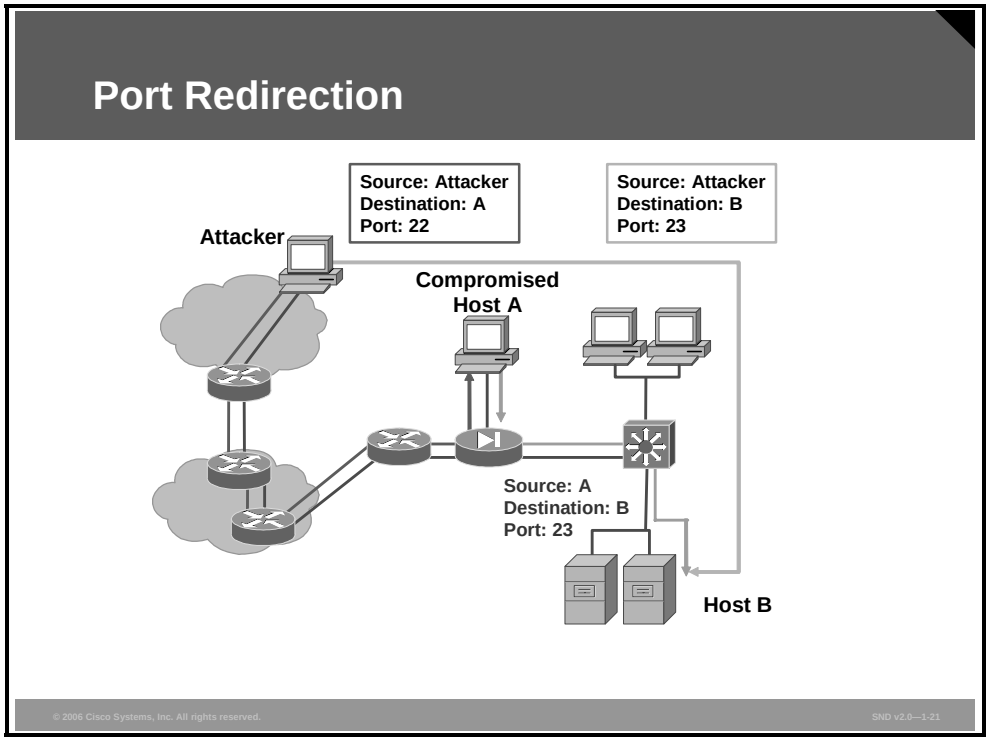



You can mitigate trust exploitation-based attacks through tight constraints on trust levels within a network.

Systems inside the firewall should never assume absolute trust of systems outside the firewall. Such trust should be limited to specific protocols and, where possible, should be validated by something other than an IP address. To prevent giving full trust from the DMZ to the inside network, set up the firewall to limit DMZ access to the inside network.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




A port redirection attack is a type of trust exploitation-based attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. Consider a firewall with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment (the DMZ) (Host A in the slide), but not the host on the inside (Host B in the slide). The host on the public services segment can reach the host on both the outside and the inside of the network. If hackers are able to compromise the public services segment host, they can install software to redirect traffic from the outside host directly to the inside host. Though neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of an application that can provide this type of access is Netcat.

Netcat is a featured networking utility that reads and writes data across network connections using the TCP/IP protocol. Netcat is a reliable back-end tool that can be used directly or that can easily be driven by other programs and scripts. At the same time, Netcat is a feature-rich network debugging and exploration tool because it can create almost any kind of connection that you would need and has several interesting built-in capabilities.

Port redirection can be mitigated primarily using proper trust models that are network specific. Assuming a system is under attack, a HIPS can help detect a hacker and prevent installation of such utilities on a host.

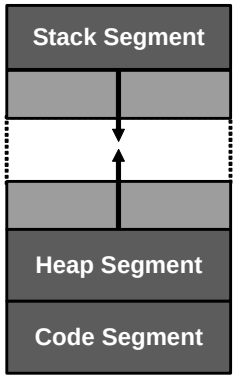


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Buffer Overflow Attack Mitigation

**Buffer overflows are used to execute arbitrary codes or to crash the system (DoS).**

- **Buffer overflow exploits**
  - **Code Red**
  - **SQLSlammer**
- **Heap-based overflows**
- **Prevention**
  - **IDS and IPS**
  - **Stack-smashing protection**
  - **Executable space protection**
  - **Safe libraries**




© 2006 Cisco Systems, Inc. All rights reserved.


A buffer overflow is an anomalous condition in which a program writes data beyond the allocated end of a buffer in memory. Buffer overflows usually arise from a bug and the improper use of languages such as C or C++ that are not memory-safe. One consequence of the overflow is the overwriting of valid data.

Buffer overflows are a commonly exploited computer security risk. Because program control data often sits in the memory areas adjacent to data buffers by means of a buffer overflow condition, the computer can be made to execute arbitrary (and potentially malicious) code that is fed back to the program as data.

A variant of a buffer overflow is a so-called “heap overflow.” The heap is a stack dynamically allocated by the application at run time and typically contains program data.

# Preventing Buffer Overflows

These techniques reduce the possibility of buffer overflows:

- **IPS:** IPS detects remote attempts to use buffer overflows; however, as a sole defense, IPS is not completely effective. Hackers can write code using a large variety of assembly instructions using alphanumeric, polymorphic, and self-modifying shell codes to slip through.

- **HIPS:** HIPS used on end hosts and servers detects buffer overflow attacks.

- **Stack-smashing protection:** Stack-smashing protection detects the most common buffer overflows by checking that an attacker did not alter the stack. If the stack was altered, the program exits with a segmentation fault. Two such systems are StackGuard and ProPolice.

- **Executable space protection for UNIX and Linux systems:** Protecting the executable space may soften the blow of buffer overflow exploits by making most of their operations impossible. This technique randomizes the address space and makes sure that memory is not writable and executable. A nonexecutable stack will stave off most shell code exploits.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Executable space protection for Microsoft Windows systems:** Microsoft Windows customers can choose from a wide variety of Microsoft and third-party executable space protection solutions providing features aimed at preventing the execution of malicious code.

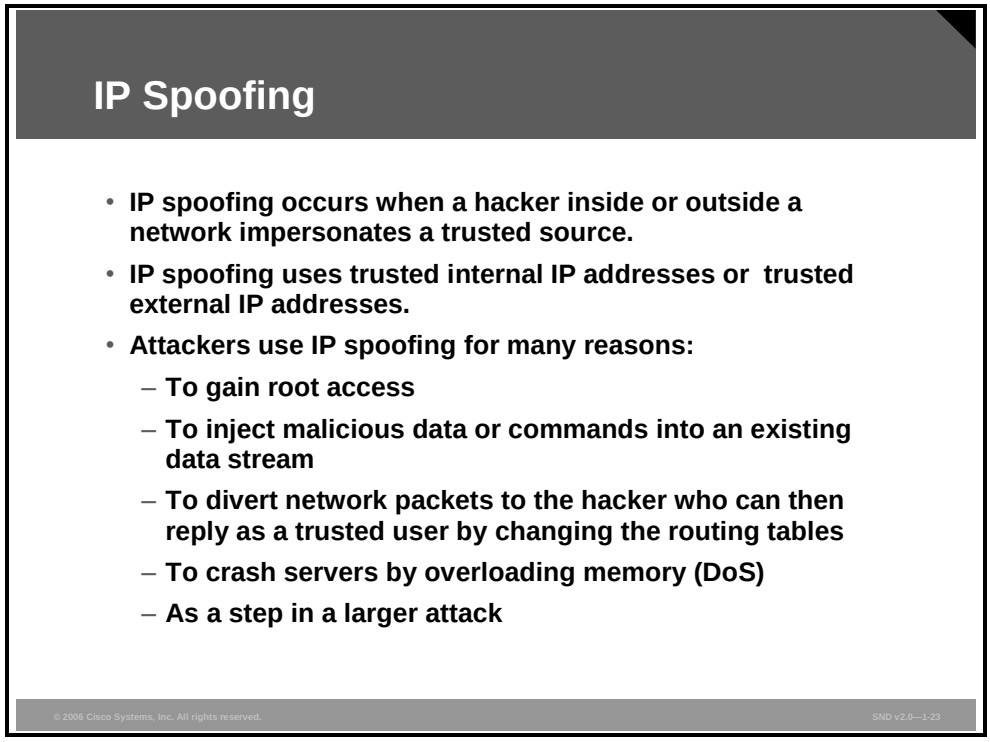
- **Using safe libraries:** C and C++ language applications are susceptible to buffer overflows because they expose low-level representational details of buffers as containers for data types. Avoid buffer overflows by maintaining a high degree of correctness in code that performs buffer management. One engineering approach to reduce the occurrence of buffer overflows is well-written and tested abstract data type libraries that centralize and automatically perform buffer management and include overflow testing.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# IP Spoofing Attacks and Mitigation

This topic describes how hackers use IP spoofing to launch various types of attacks.




The prime goal of an IP spoofing attack is to establish a connection that allows the attacker to gain root access to the host and to create a backdoor entry path into the target system.

IP spoofing is a technique used to gain unauthorized access to computers whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. The attacker learns the IP address of a trusted host and modifies the packet headers so that it appears that the packets are coming from that host.

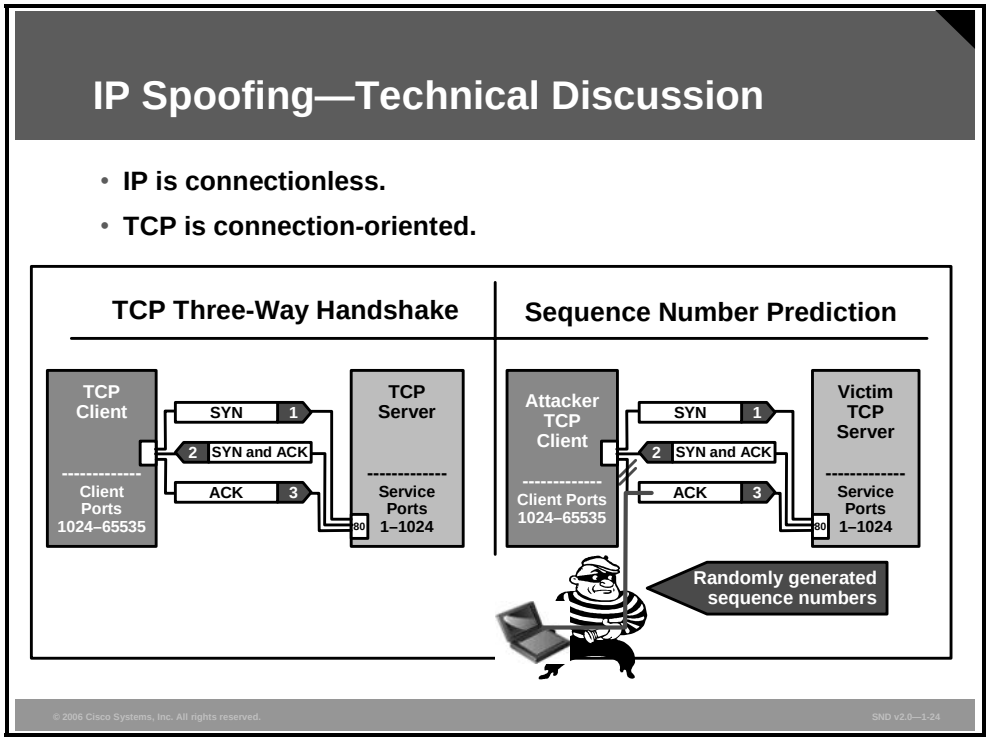
At a high level, the concept of IP spoofing is easy to comprehend. Routers determine the best route between distant computers by examining the destination address, ignoring the source address. In a spoofing attack, an attacker outside your network pretends to be a trusted computer using a trusted internal IP address or a trusted external IP address.

If an attacker manages to change the routing tables to divert network packets to the spoofed IP address, the attacker can receive all the network packets addressed to the spoofed address and reply just as any trusted user can.

IP spoofing can also provide access to user accounts and passwords. For example, an attacker can emulate one of your internal users in ways that prove embarrassing for your organization. The attacker could send e-mail messages to business partners that appear to have originated from someone within your organization. Such attacks are easier to perpetrate when an attacker has a user account and password, but they are also possible when attackers combine simple spoofing attacks with their knowledge of messaging protocols.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Recall that the TCP/IP works at Layer 3 and Layer 4, respectively. IP is a connectionless model, which means that packet headers contain no information regarding the transaction state used to route packets on a network. There is no method in place to ensure proper delivery of a packet to the destination.

The IP header contains the source and destination IP addresses. Using one of several tools, an attacker can easily modify the source address field. Note that in IP, each datagram is independent of all others because of the stateless nature of IP. To engage in IP spoofing, hackers find the IP address of a trusted host and modify their own packet headers to appear as though packets are coming from that trusted host (source address).

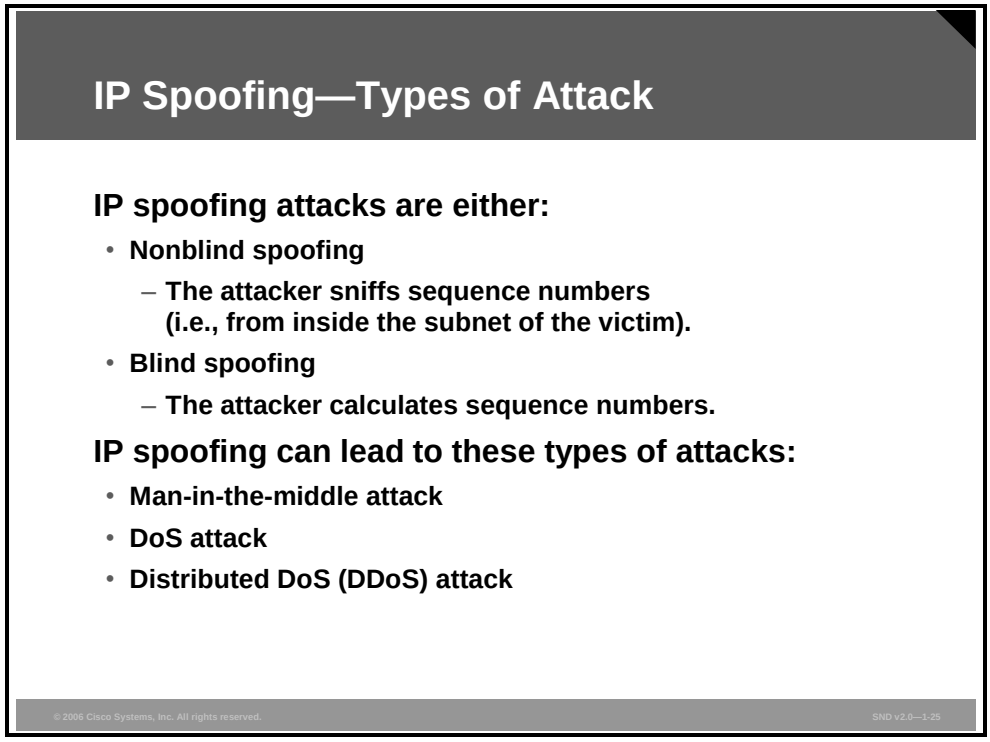
TCP uses a connection-oriented design. This design means that the participants in a TCP session must first build a connection using the three-way handshake. After the connection is established, TCP assures data reliability by applying the same process to every packet as the two machines update one another on progress. The sequence and acknowledgements take place as follows:

- The client selects and transmits an initial sequence number.
- The server acknowledges the initial sequence number and sends its own sequence number.
- The client acknowledges the server sequence number, and the connection is open to data transmission.

The basis of IP spoofing lies in an inherent security weakness in TCP known as sequence prediction. Hackers can guess or predict the TCP sequence number to construct a TCP packet without receiving any responses from the server. Their prediction allows them to spoof a trusted host on a local network. To mount an IP spoofing attack, the hacker listens to communications between two systems. The hacker sends packets to the target system with the source IP address of the trusted system. If the packets from the hacker have the sequence numbers that the target system is expecting, and if these packets arrive before the packets from the trusted system, the hacker becomes the trusted host.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




To engage in IP spoofing, hackers must first use a variety of techniques to find an IP address of a trusted host and then modify their packet headers to appear as though packets are coming from that trusted host. Further, the attacker can engage other unsuspecting hosts to generate traffic that appears as though it too is coming from the trusted host, thus flooding the network.

IP spoofing attacks fall into one of these two categories:

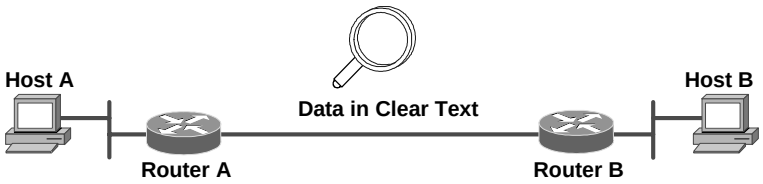
- **Nonblind spoofing:** This type of attack takes place when the attacker is on the same subnet as the victim. The attacker sniffs the sequence and acknowledgement numbers to eliminate the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. The attacker corrupts the datastream of an established connection, and then re-establishes the datastream with the attack machine using the correct sequence and acknowledgement numbers. Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection.
- **Blind spoofing:** This type of attack is a more sophisticated attack because the sequence and acknowledgement numbers are unreachable. To circumvent this issue, the attacker sends several packets to the target machine to sample sequence numbers. This is a difficult task, but not impossible.

Both types of IP spoofing are forms of a common security violation known as a man-in-the-middle attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by “spoofing” the identity of the original sender, who is presumably trusted by the recipient.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Man-in-the-Middle Attacks




- **A man-in-the-middle attack requires that the hacker has access to network packets that come across a network.**
- **A man-in-the-middle attack is implemented using the following:**
  - **Network packet sniffers (nonblind attack)**
  - **Routing and transport protocols (blind attack)**

© 2006 Cisco Systems, Inc. All rights reserved.

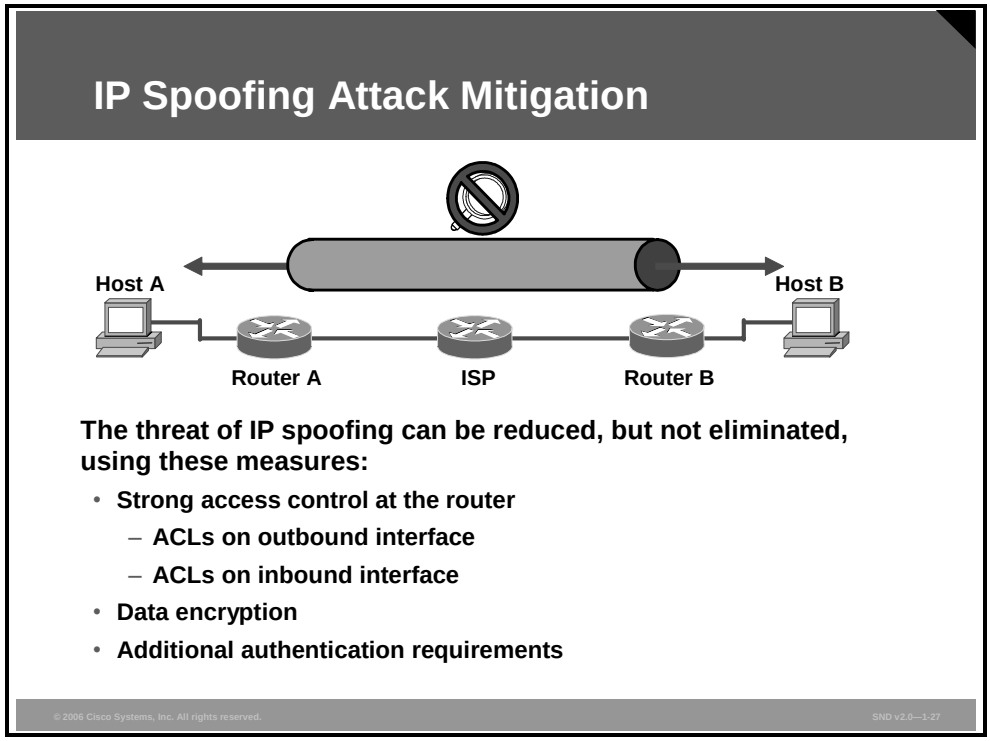

Hackers use man-in-the-middle attacks to perform these violations:

- Theft of information
- Hijacking of an ongoing session to gain access to your internal network resources
- Analysis of traffic to derive information about your network and its users
- DoS
- Corruption of transmitted data
- Introduction of new information into network sessions

TCP session hijacking is a common variant of the man-in-the-middle attack. The attacker sniffs to identify the client and server IP addresses and relative port numbers. The attacker then modifies his or her packet headers to spoof TCP/IP packets from the client. The attacker then waits to receive an ACK packet from the client communicating with the server. The ACK packet contains the sequence number of the next packet that the client is expecting. The attacker replies to the client using a modified packet with the source address of the server and the destination address of the client. This results in a reset that disconnects the legitimate client. The attacker takes over communications with the server by spoofing the expected sequence number from the ACK that was previously sent from the legitimate client to the server.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The measures listed here can reduce the threat of IP spoofing:

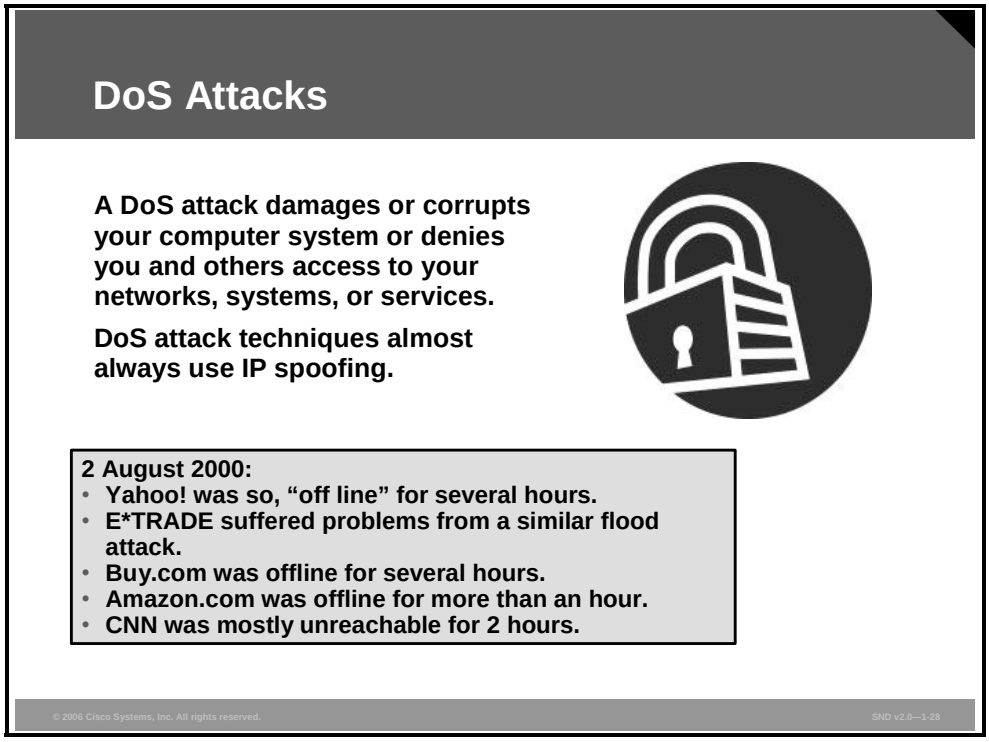
- **Access control at the router:** Properly configured access controls reduce the effectiveness of IP spoofing.
  - **Inbound interface:** If your internal addresses are the only trusted addresses, access control lists (ACLs) should deny any traffic from the external network using an internal source address. If some external addresses are trusted, the ACL needs to block private IP addresses on your inbound (downstream) interface. Additionally, this interface should not accept addresses with your internal range as the source, because this is a common spoofing technique used to circumvent firewalls.
  - **Outbound interface:** You can prevent your network users from spoofing other networks (and be a good Internet citizen at the same time) by preventing any outbound traffic on your network that does not have a source address in the IP range of your organization.
- **Data encryption:** Encryption also reduces spoofing threats. Ensure that the proper authentication measures are in place and carried out over a secure (encrypted) channel. Encrypting traffic in an IPsec tunnel mitigates man-in-the-middle attacks, as shown in the figure. Encryption allows the hacker to see only cipher text.
- **Additional authentication:** The most effective method for mitigating the threat of IP spoofing is the same as the most effective method for mitigating the threat of packet sniffers. Cryptographic authentication is the best form of additional authentication. However, when cryptographic authentication is not possible, strong two-factor authentication using OTPs can also be effective. Additionally, you should eliminate all host-based authentication measures, which are sometimes common for machines on the same subnet.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# DoS Attacks and Mitigation

This topic describes the mitigation of DoS and distributed denial of service (DDoS) attacks.



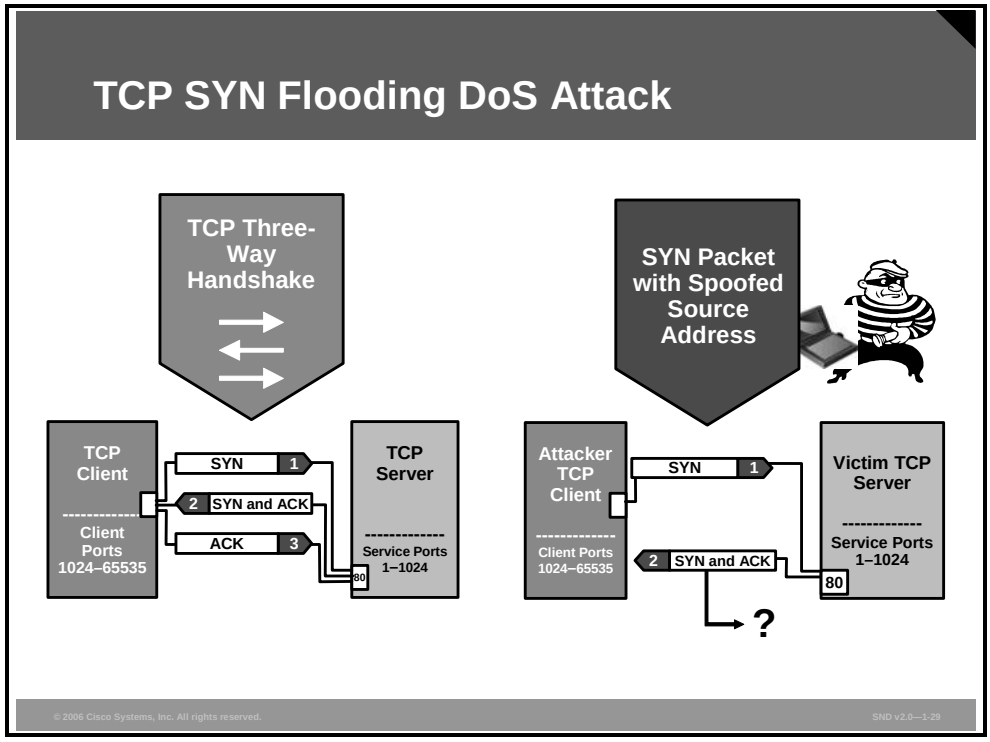

DoS attacks are the most publicized form of attack. They are also among the most difficult to eliminate. A DoS attack on a server sends an extremely large volume of requests over a network or the Internet. These large volumes of requests cause the attacked server to slow down dramatically. As a consequence, the attacked server becomes unavailable for legitimate access and use.

DoS attacks are different from most other attacks because DoS attacks do not aim at gaining access to your network or the information on your network. These attacks focus on making a service unavailable for normal use. Attackers typically accomplish this by exhausting some resource limitation on the network or within an operating system or application. These attacks require little effort to execute because they typically take advantage of protocol weaknesses or because the attacks use traffic normally allowed into a network. DoS attacks are among the most difficult to completely eliminate because of the way that they use protocol weaknesses and accepted traffic to attack a network. There are hackers who regard DoS attacks as trivial and in bad form because they require so little effort to execute. Still, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. However, as with viruses, hackers constantly develop new DoS attacks.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




DoS attacks are most often initiated using IP spoofing. The figure shows how a TCP connection is established between a client and server. After the connection between the client and the server is open, the client and server can send service-specific data.

An avenue of attack exists at the point where the server has sent the SYN-ACK to the client but has not yet received the ACK message. This condition is a half-open connection.

Now consider that the server has built in its system memory a data structure describing all pending connections. This data structure is of finite size and can overflow if there are too many half-open connections created.

Hackers use IP spoofing to create half-open connections. The attacker sends SYN messages to the victim server. These messages appear to be legitimate but, in fact, refer to a client system that is unable to respond to the SYN-ACK messages. This means that the client never sends a final ACK message to the victim server and the connection remains half-open.

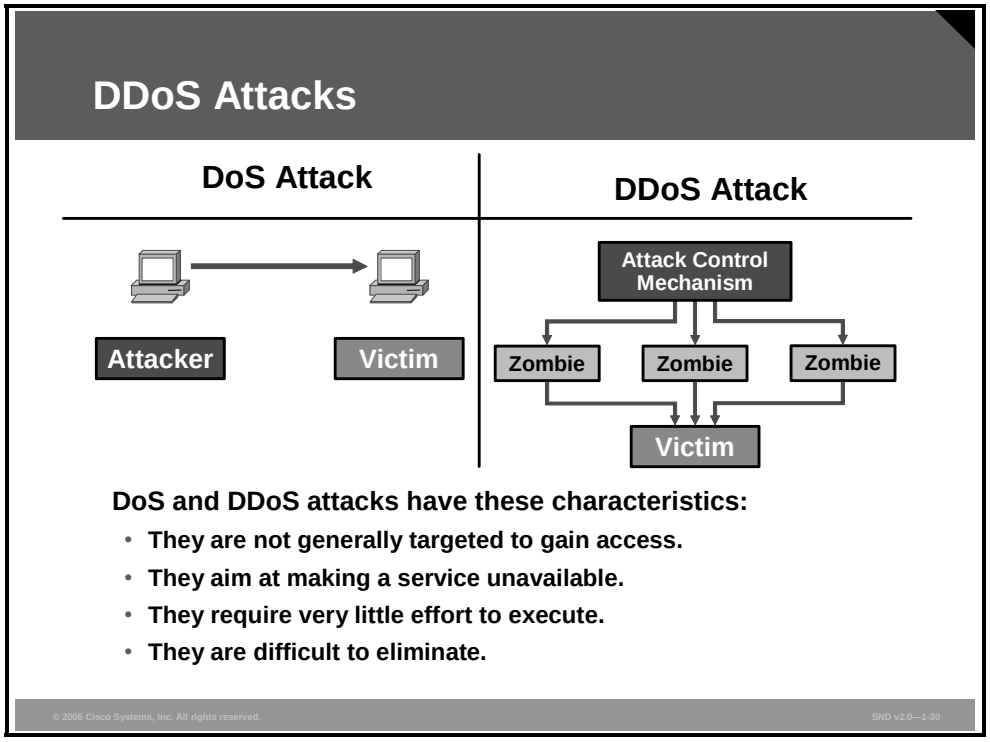
The half-open connection data structure on the victim server eventually fills with messages, and the system is unable to accept any new incoming connections. Normally, there is a timeout period associated with any pending connection. Half-open connections eventually expire, and the victim server recovers. However, the attacking system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system can empty the table.

In most cases, the victim of such an attack will have difficulty accepting any new incoming network connection. In these cases, the attack does not affect existing incoming connections or the ability to originate outgoing network connections. However, in some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

The attacker obscures his or her location by making the source addresses in the SYN packets implausible. When the packet arrives at the victim server, there is no way to determine its true source. Because the network forwards packets based on destination address, the only way to validate the source of a packet is to use input source filtering.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



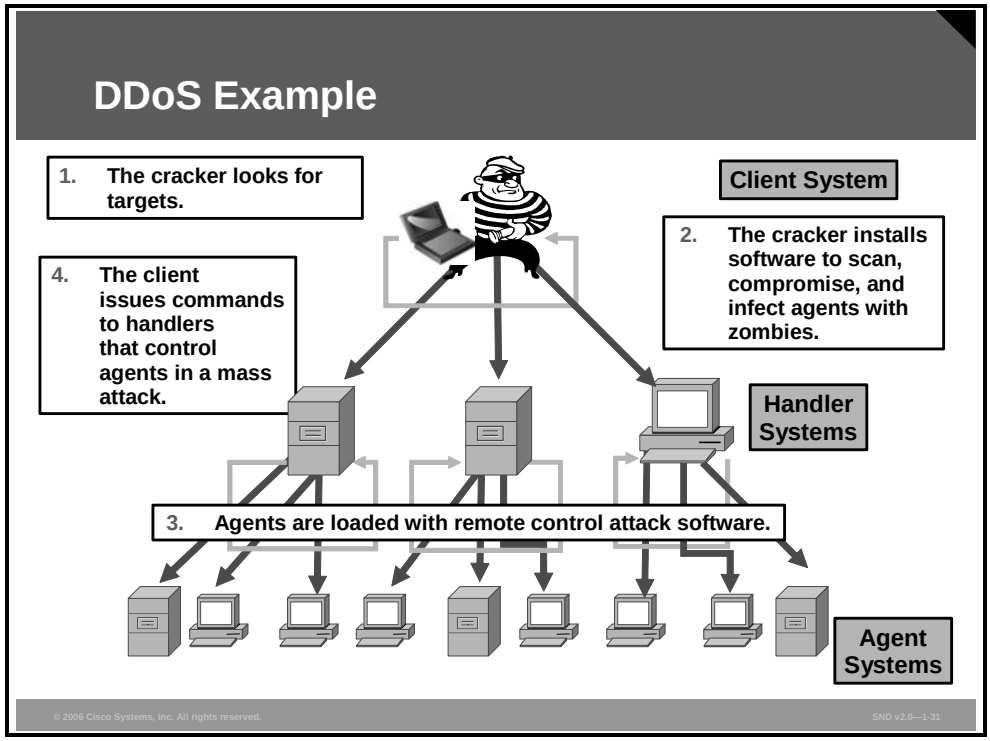

The left side of the figure shows a typical DoS attack architecture. The right side shows a typical DDoS attack architecture. DoS and DDoS attacks share many of the same characteristics.

A DDoS attack generates much higher levels of flooding traffic using the combined bandwidth of multiple machines to target a single machine or network. The DDoS attack enlists a network of compromised machines containing a remotely controlled agent, or zombie, attack program. A master control mechanism provides direction and control. When the zombies receive instructions from the master agent, they each begin generating malicious traffic aimed at the victim.

DDoS attacks are the “next generation” of DoS attacks on the Internet. This type of attack is not new. UDP and TCP SYN flooding, ICMP echo-request floods, and ICMP directed broadcasts (also known as smurf attacks) are similar to DDoS attacks; however, the scope of the attack is new. Victims of DDoS attacks experience packet flooding from many different sources, possibly spoofed IP source addresses that bring their network connectivity to a grinding halt. In the past, the typical DoS attack involved a single attempt to flood a target host with packets. With DDoS tools, an attacker can conduct the same attack using thousands of systems.



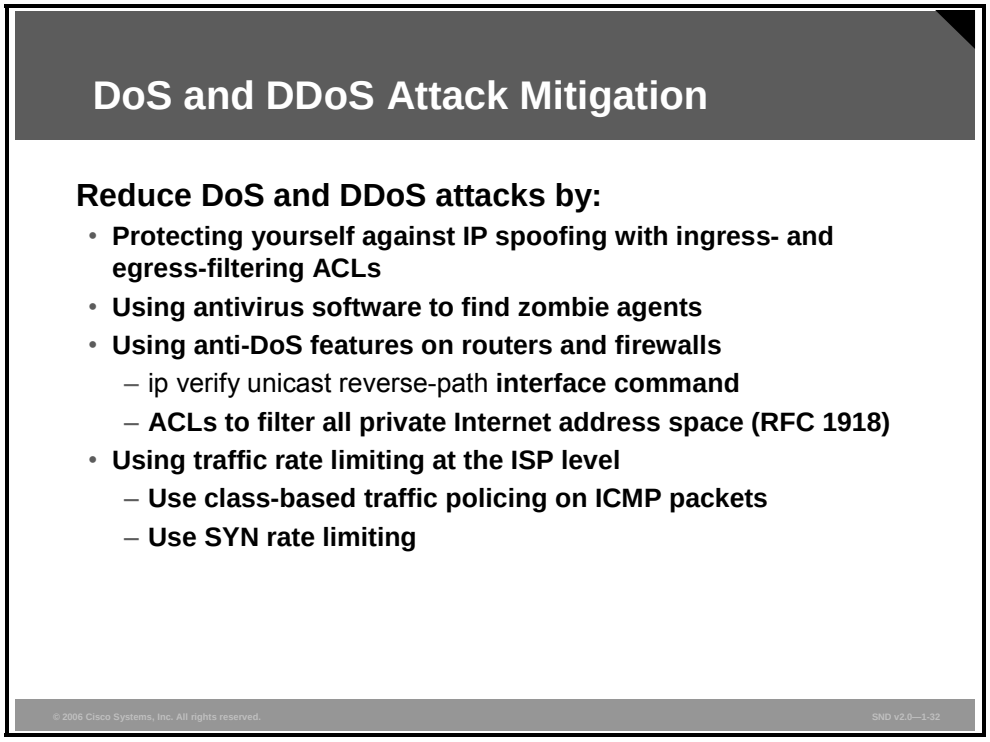
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




This figure shows the process of a DDoS attack. In the figure, the hacker uses a terminal to scan for systems to hack. After the hacker accesses handler systems, the hacker installs zombie software on them. The zombies aim to scan, compromise, and infect agent systems. When the hacker accesses agent systems, the hacker then loads remote control attack software to carry out the DDoS attack.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




When attacks involve specific network server applications, such as an HTTP server or an FTP server, the attacker focuses on acquiring and keeping all the available connections supported by that server open. This strategy effectively locks out valid users of the server or service.

DoS attacks can also be implemented using common Internet protocols, such as TCP and ICMP. For example, ping of death and teardrop attacks exploit limitations in the TCP/IP protocols. While most DoS attacks exploit a weakness in the overall architecture of the attacked system rather than any software bugs or security holes, some attacks compromise the performance of your network by flooding the network with undesired, and often useless, network packets and by providing false information about the status of network resources.

Here are the four methods to reduce the threat of DoS and DDoS attacks:

- **Protect against IP spoofing:** Preventing IP spoofing reduces the effects of a DoS and DDoS attack. If hackers cannot mask their identities, they might not attack. For example, you can use ACLs to apply ingress and egress filtering as described in RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*.
- **Use antivirus software to find zombie agents:** Antivirus software detects viruses; it does not detect DoS attacks. However, antivirus software can play an important role in detecting zombie agents.
- **Use Cisco IOS anti-DoS features:** Proper configuration of Cisco IOS anti-DoS features on routers and firewalls can help limit the effectiveness of an attack. These features often involve limits on the amount of half-open TCP connections that a system allows at any given time. Two suggested measures are as follows:
  - Use the **ip verify unicast reverse-path** interface command on the input interface of the router at the upstream end of the connection. The interface will then examine each packet it receives as input. If the source IP address does not have a route in the Cisco Express Forwarding (CEF) tables that points back to the same interface on which the packet arrived, the router drops the packet.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Use ACLs to filter all private Internet address space (see RFC 1918, *Address Allocation for Private Internets*).

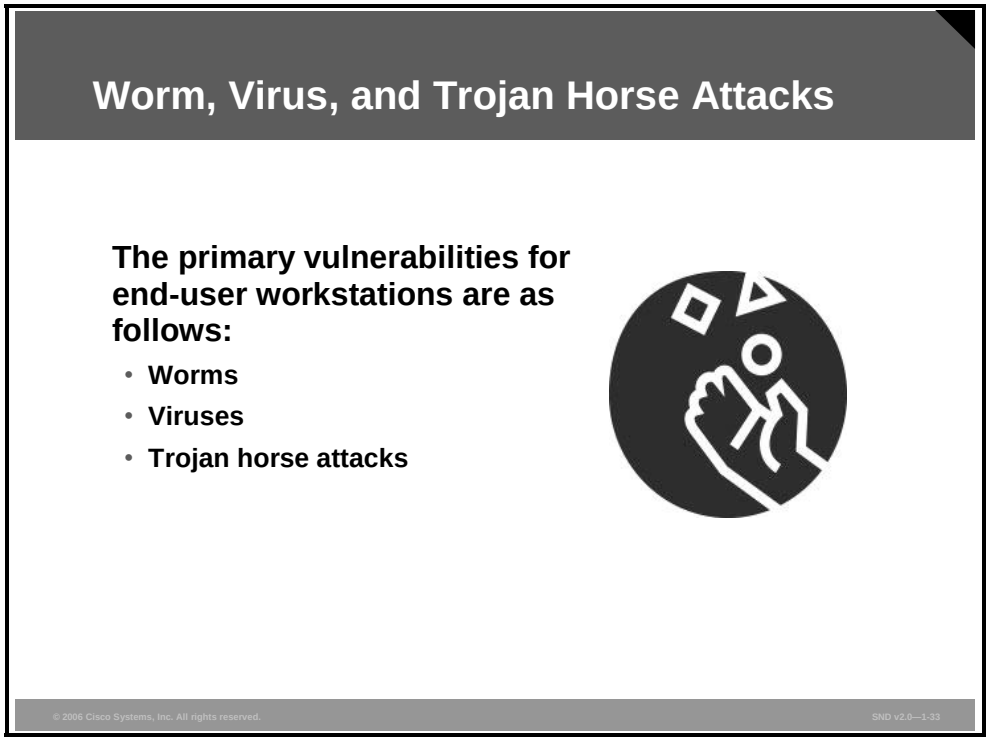
- **Traffic rate limiting:** An organization can implement traffic rate limiting with its ISP. This type of filtering limits the amount of nonessential traffic that crosses network segments at a certain rate and can be done in more than one way.
  - A common approach is to limit the amount of ICMP traffic allowed into a network only for diagnostic purposes. ICMP-based DDoS attacks are common.
  - Another approach is to configure rate limiting for SYN packets. However, this approach can be tricky. Setting the rate limit too high may drop legitimate SYN packets. If an attacker aims a SYN attack against a particular host, consider installing an IP filtering package on that host.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Worm, Virus, and Trojan Horse Attacks and Mitigation

This topic describes the mitigation of worm, virus, and Trojan horse attacks.




A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The worm can then infect other hosts from the infected computer. A worm is also a program that propagates itself. A worm can spread itself automatically over the network from one computer to the next without user intervention. Worms are not clever or evil, they just take advantage of automatic file sending and receiving features found on many computers.

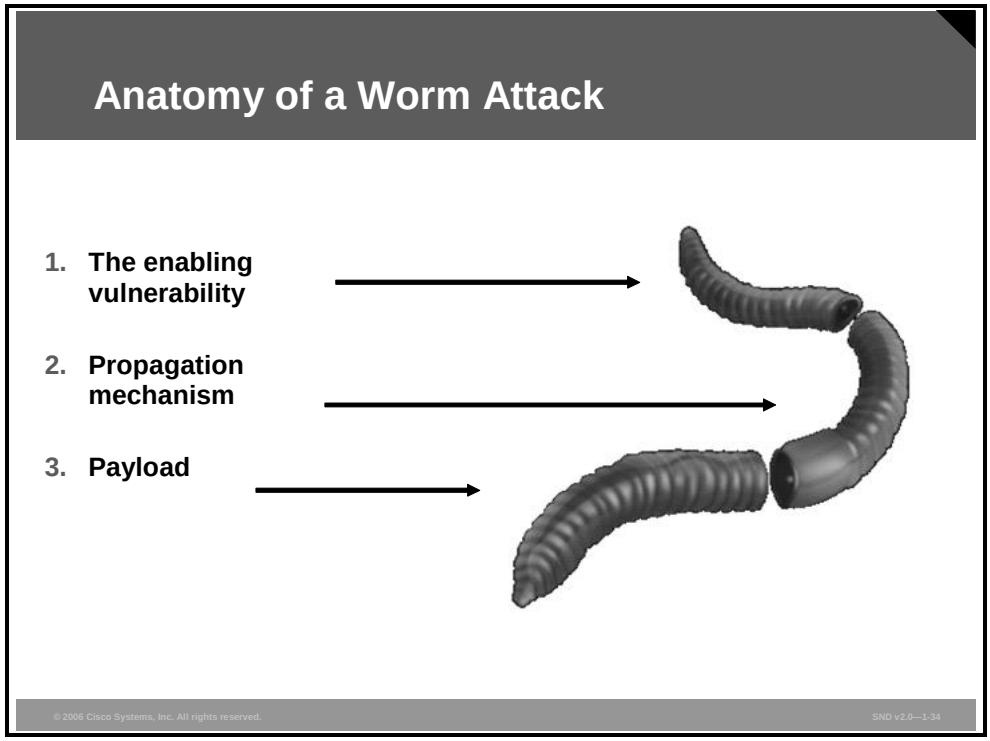
A virus is malicious software that attaches to other programs and executes a particular unwanted function on a user workstation. A virus propagates itself by infecting other programs on the same computer. Viruses can do serious damage, such as erasing files or erasing an entire disk. They can also be a simple annoyance such as popping up a window that says, for example, “Ha ha, you are infected!” True viruses cannot spread to a new computer without human assistance, such as opening an infected file on a floppy disk or an e-mail attachment or through file sharing.

Trojan horse is a general term referring to programs that appear desirable but actually contain something harmful. For example, a downloaded game could erase files. The contents could also hold a virus or a worm.

A Trojan horse can attack on three levels. A virus known as the Love Bug is an example of a Trojan horse because it pretended to be a love letter when it actually carried a harmful program. The Love Bug was a virus because it infected all image files on the attacked disk, turning them into new Trojan horses. Finally, the Love Bug was a worm because it propagated itself over the Internet by hiding in the Trojan horses that it sent out using addresses in the attacked e-mail address book.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The anatomy of a worm attack is as follows:

- **The enabling vulnerability:** A worm installs itself on a vulnerable system.
- **Propagation mechanism:** After gaining access to devices, a worm replicates and selects new targets.
- **Payload:** After the worm infects the device, the attacker has access to the host—often as a privileged user. Attackers use a local exploit to escalate their privilege level to the administrator level.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Mitigating Worm Attacks

**Four recommended steps to mitigate worm attacks:**

- **Step 1: Containment**
- **Step 2: Inoculation**
- **Step 3: Quarantine**
- **Step 4: Treatment**



© 2006 Cisco Systems, Inc. All rights reserved.


Worm attack mitigation requires diligence on the part of system and network administration staff. Coordination between system administration, network engineering, and security operations personnel is critical in responding effectively to a worm incident. There are four recommended steps for worm attack mitigation:

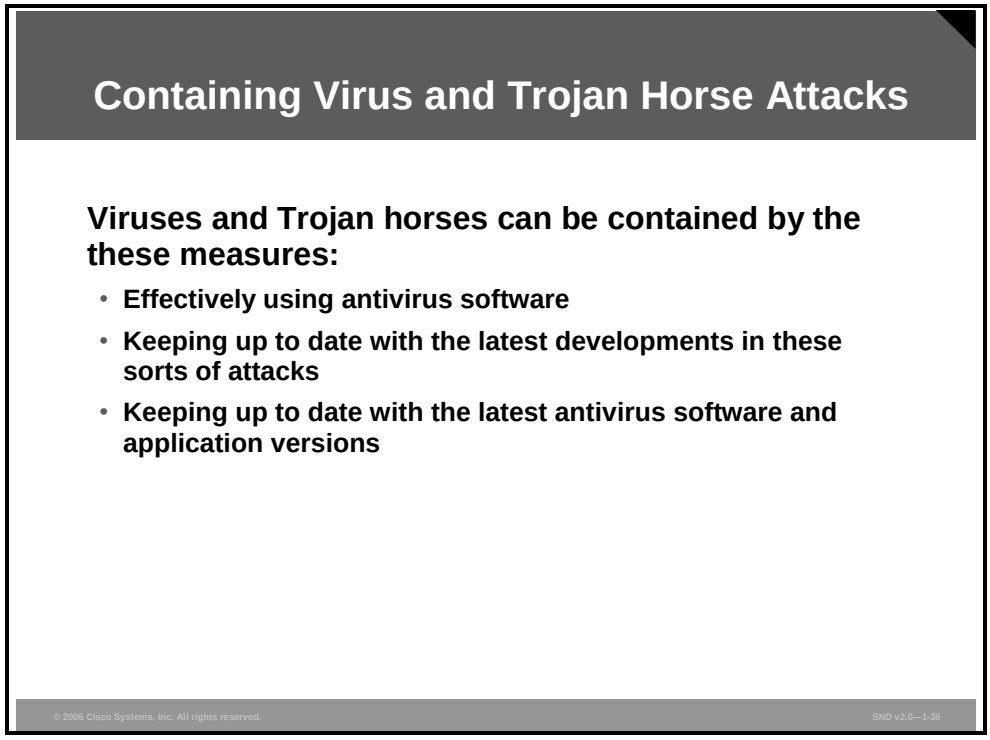
- **Containment:** Contain the spread of the worm inside your network and within your network. Compartmentalize uninfected parts of your network.
- **Inoculation:** Start patching all systems and, if possible, scanning for vulnerable systems.
- **Quarantine:** Track down each infected machine inside your network. Disconnect, remove, or block infected machines from the network.
- **Treatment:** Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.

The network service provider security (NSP-SEC) forum incident response methodology subdivides common incident response methodologies into these six major categories:

- **Preparation:** Acquire the resources to respond
- **Identification:** Identify the worm
- **Classification:** Classify the type of worm
- **Traceback:** Trace the worm back to its origin
- **Reaction:** Isolate and repair the affected systems
- **Post mortem:** Document and analyze the process used for the future



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



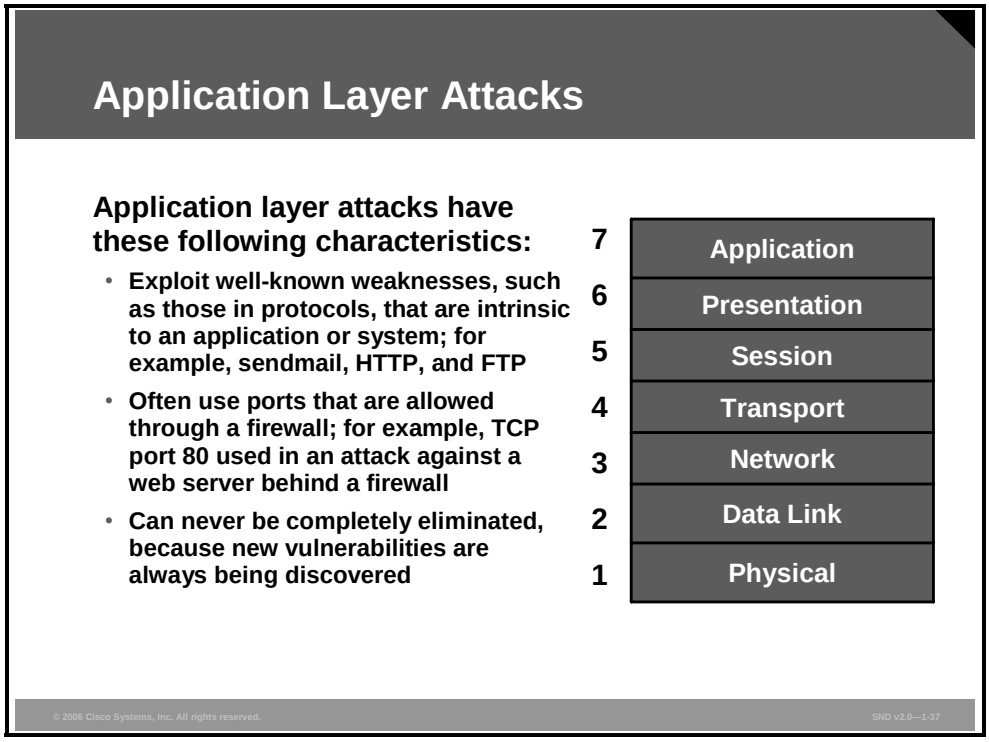

Viruses and Trojan horse attacks can be contained through the effective use of antivirus software at the user level and potentially at the network level. Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. As hackers release new viruses or Trojan horse applications, enterprises need to keep up to date with the latest antivirus software and application versions and patches. Keeping up to date with the latest developments in viruses and Trojan attacks also leads to a more effective posture against the attacks.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Application Layer Attacks and Mitigation

This topic describes the mitigation of application layer attacks.




There are several methods of executing an application layer attack:

- **Exploiting well-known weaknesses:** One of the most common methods of implementing application layer attacks is exploiting well-known weaknesses in software commonly found on servers, such as sendmail, HTTP, and FTP. By exploiting these weaknesses, attackers can gain access to a computer with the permission of the account running the application. The account is usually a privileged, system-level account.
- **Trojan horse programs:** Trojan horse program attacks are implemented using programs that an attacker substitutes for common programs. These programs may provide all the functionality that the normal program provides, but may also include other tactics that the attacker knows and uses. These tactics include monitoring login attempts to capture user account and password information. These programs can capture sensitive information and distribute it back to the attacker. They can also modify application functionality, such as applying a blind carbon copy to all e-mail messages so that the attacker can read all the e-mails from the organization.
- **Password stealing:** One of the oldest forms of application layer attacks is a Trojan horse program that displays a screen, banner, or prompt that the user believes is the valid login sequence. The program then captures the information that the user enters and stores or e-mails it to the attacker. Next, the program either forwards the information to the normal login process (normally impossible on modern systems) or simply sends an expected error to the user (for example, “Bad Username,” “Bad Password,” or a combination), exits, and starts the normal login sequence. The users believe that they have incorrectly entered the password, they re-enter the information, and then gain access.

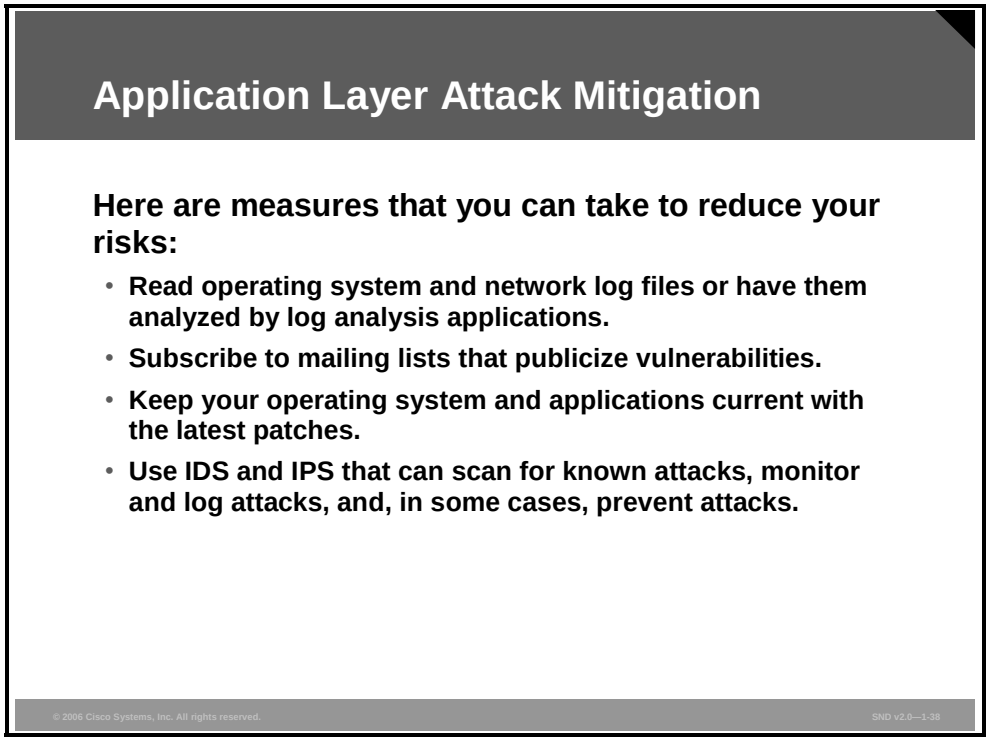

© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Java and ActiveX:** One of the newest forms of application layer attacks exploits the openness of several new technologies: the HTML specification, web browser functionality, and HTTP. These attacks, which include Java applets and ActiveX controls, involve passing harmful programs across the network and loading them through the active browser.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Here are measures that you can take to reduce your risks of application layer attacks:

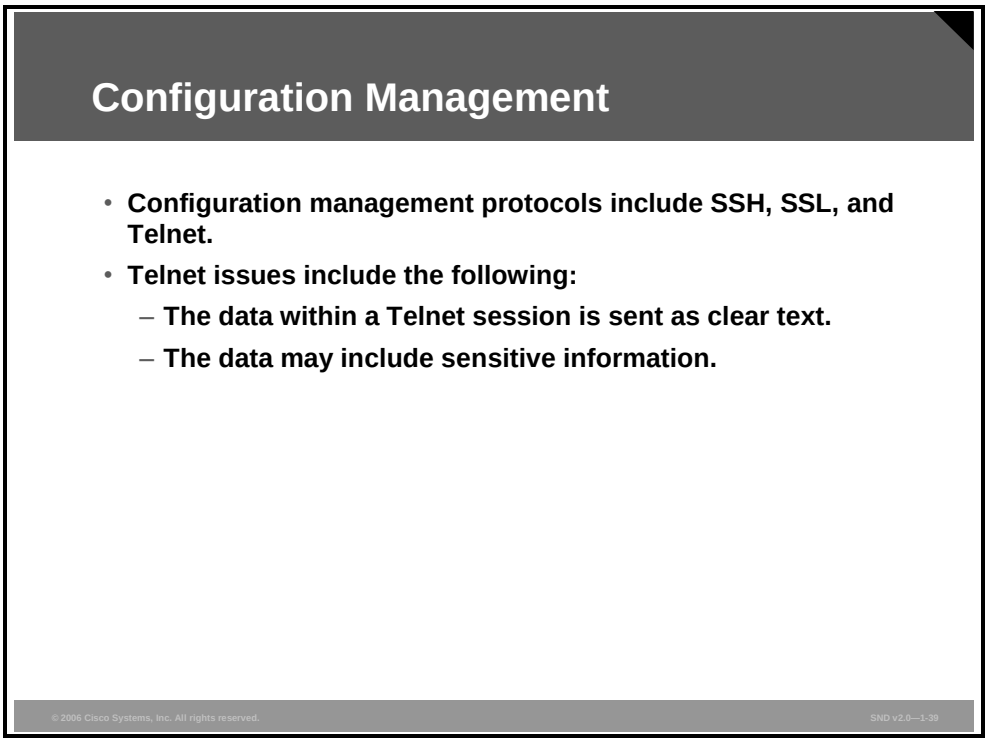
- Read operating system and network log files or have them analyzed. It is important to review all logs and take action accordingly.
- Subscribe to mailing lists that publicize vulnerabilities. There are many Internet resources published by industry, government, and user groups.
- Keep your operating system and applications current with the latest patches. Always test patches and fixes in a nonproduction environment. This practice prevents downtime and generating unnecessary errors.
- Use IDS or IPS or both IDS and IPS to scan for known attacks, to monitor and log attacks, and to ultimately prevent attacks. These systems are essential to identifying security threats and mitigating some of these threats. In most cases, mitigation is automatic.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Management Protocols and Vulnerabilities

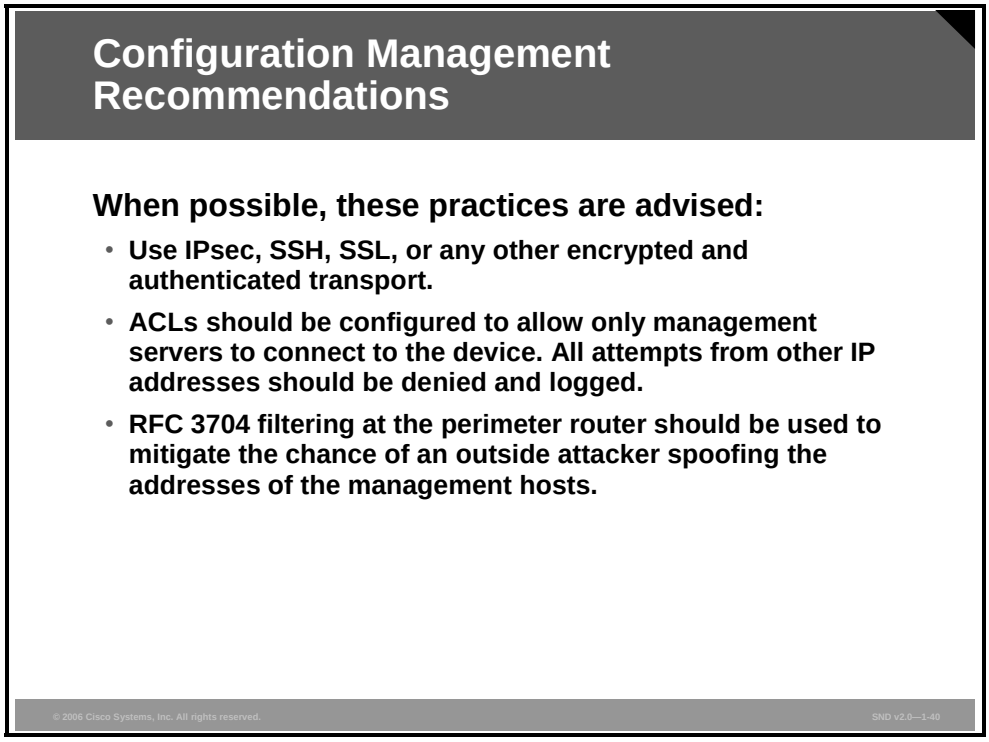
The protocols used to manage your network can be a source of vulnerability. This topic describes vulnerabilities in configuration management protocols and recommendations for mitigating these vulnerabilities.




If the managed device does not support any of the recommended protocols, such as SSH and SSL, Telnet (not recommended) may have to be used. When the inventers of the Internet developed Telnet, security was not an issue. Modern network administrators should recognize that a Telnet session transmits data as clear text that anyone with a packet sniffer along the data path between the managed device and the management server can intercept. The clear text may include important or sensitive information, such as the configuration of the device itself, passwords, or other sensitive data.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



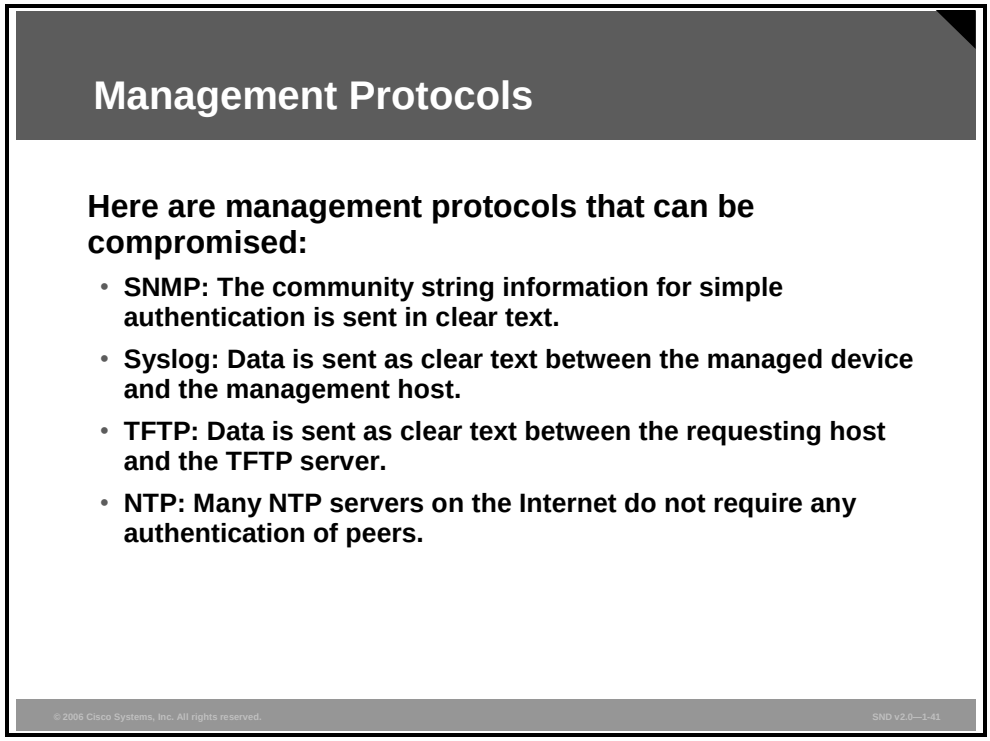

The first recommendation is to use IPsec, SSH, or SSL to encrypt management traffic to protect sensitive information such as the device configuration, passwords, and other sensitive data.

Regardless of whether you use SSH, SSL, or Telnet for remote access to the managed device, you should also configure ACLs to allow only management servers to connect to the device. Deny and log all attempts from other IP addresses logged. Implement RFC 3704 filtering at the ingress router to reduce the chance of an attacker from outside the network spoofing the addresses of the management hosts.

| | |
|---|---|
| **Note** | RCF 3704 covers ingress filtering for multihomed networks. RCF 3704 updates RFC 2827. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Use Simple Network Management Protocol (SNMP) to remotely retrieve information from a network device (commonly referred to as read-only access) or to configure parameters on the device (commonly referred to as read-write access). SNMP uses passwords (called community strings) within each message as a very simple form of security. Unfortunately, most implementations of SNMP on networking devices today send the community string in clear text along with the message. Just like Telnet, anyone with a packet sniffer located along the data path between the device and the management server can intercept SNMP.

Syslog, which is information generated by a device that has been configured for logging, is sent as clear text between the managed device and the management host. Syslog does not have packet-level integrity checking to ensure that nothing alters the packet contents in transit. An attacker may alter syslog data to confuse a network administrator during an attack.

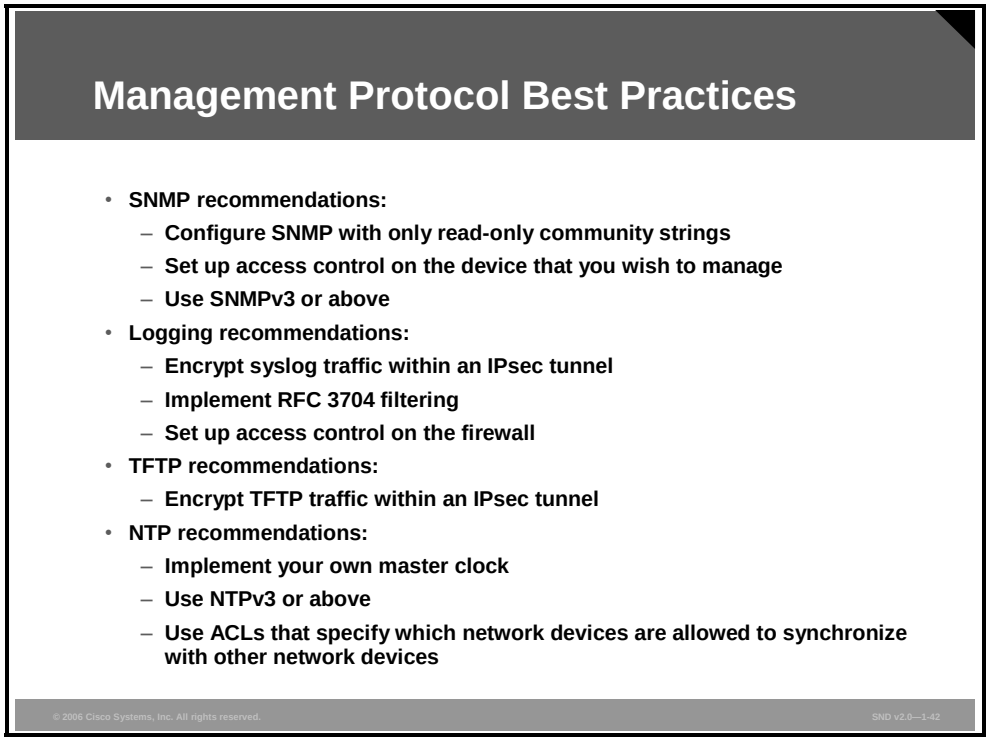
Administrators use TFTP to transfer configuration or system files across the network. TFTP uses UDP for the data stream between the requesting host and the TFTP server. Similar to other management protocols that send data in clear text, the network administrator should recognize that the data within a TFTP session is as vulnerable to intercept as Telnet and SNMP messages.

Networks use Network Time Protocol (NTP) to synchronize the clocks of various devices across a network. Clock synchronization within a network is critical for digital certificates and for correct interpretation of events within syslog data. A secure method of providing clocking for the network is for network administrators to implement their own private network master clocks synchronized to Coordinated Universal Time (UTC) using satellite or radio. However, if network administrators do not wish to implement their own master clocks because of cost or other reasons, other clock sources are available through the Internet.

An attacker could attempt a DoS attack on a network by sending bogus NTP data across the network in an attempt to change the clocks on a network. Changing the clocks can make digital certificates appear invalid. An attacker could also attempt to confuse a network administrator during an attack by disrupting the clocks on network devices. This scenario makes it difficult for the network administrator to determine the order of syslog events on multiple devices.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Here are three recommendations for the correct use of SNMP tools:

- Configure SNMP with only read-only community strings
- Set up access control on the device that you wish to manage via SNMP to allow access only by the appropriate management hosts
- Use SNMP version 3 (SNMPv3) (This version provides secure access to devices through a combination of authenticating and encrypting management packets over the network.)

Use these management logging practices where possible:

- Encrypt syslog traffic within an IPsec tunnel
- Implement RFC 3704 filtering at the perimeter router when allowing syslog access from devices on the outside of a firewall
- Implement ACLs on the firewall to allow syslog data from only the managed devices themselves to reach the management hosts
- When possible, encrypt TFTP traffic within an IPsec tunnel to reduce the chance of interception

Here are recommendations to follow when using NTP:

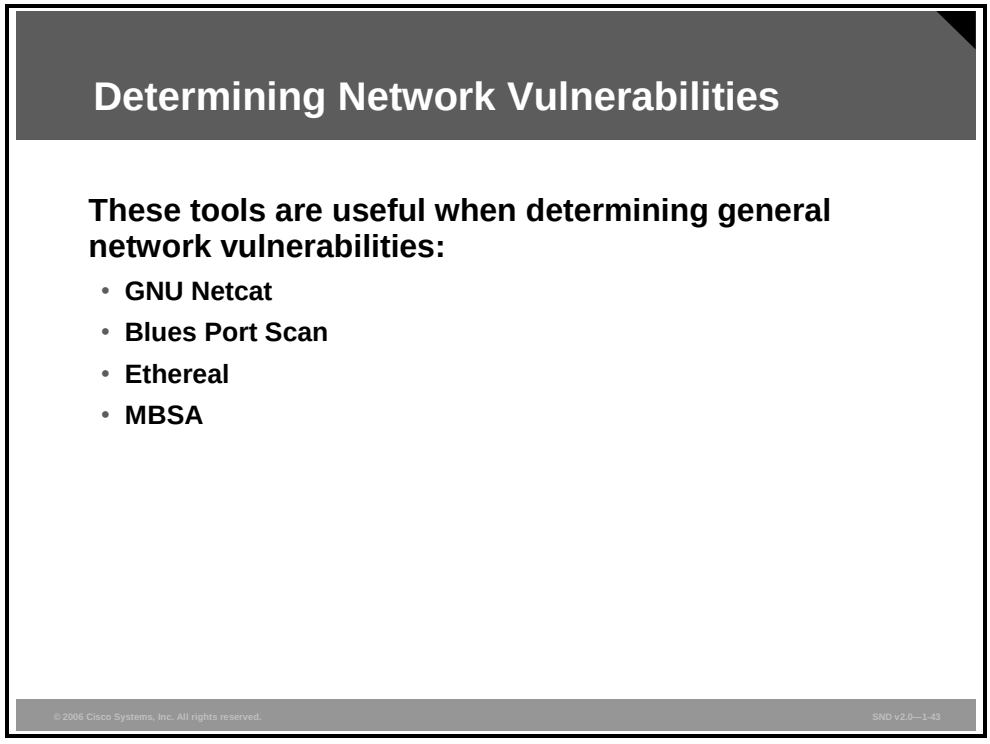
- Implement your own master clock for private network synchronization
- Use NTP version 3 (NTPv3) or above (This is recommended because these versions support a cryptographic authentication mechanism between peers.)
- Use ACLs that specify which network devices may synchronize with other network devices



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Determining Network Vulnerabilities

This topic describes how to discover network vulnerabilities and threats with GNU Netcat, BluesPortScan, Ethereal, and Microsoft Baseline Security Analyzer.




You can use a number of the tools and techniques to find vulnerabilities in your network. You will use some of these tools in the lab exercise for this lesson. Once you identify the vulnerabilities, you can consider and implement mitigation steps as appropriate:

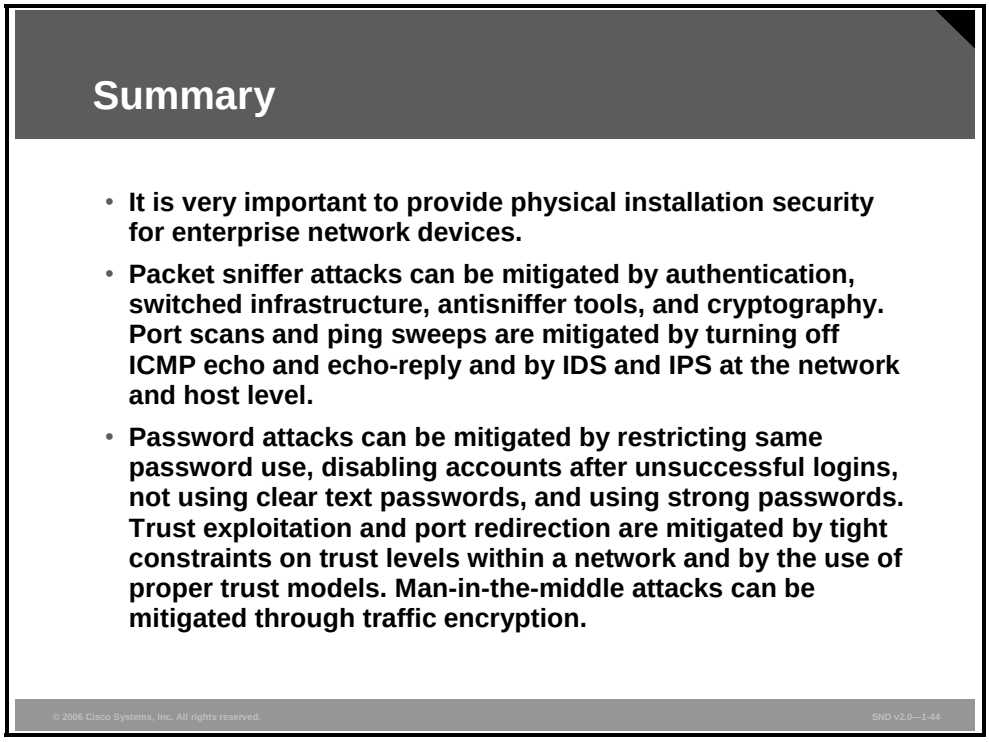
- **GNU Netcat:** Netcat is a featured networking utility that reads and writes data across network connections using the TCP/IP protocol.
- **BluesPortScan:** The BluePortScan scans 300 ports per second on a Microsoft Windows NT or Microsoft Windows 2000 machine.
- **Ethereal:** Network professionals around the world use Ethereal for troubleshooting, analysis, software and protocol development, and education. Ethereal has all of the standard features that you would expect in a protocol analyzer and has several features not seen in any other product. The Ethereal open source license allows talented experts in the networking community to add enhancements to a system. Ethereal runs on all popular computing platforms, including UNIX, Linux, and Microsoft Windows.
- **Microsoft Baseline Security Analyzer (MBSA):** MBSA is a free best practices vulnerability assessment tool for the Microsoft platform. MBSA is a tool designed for the IT professional who helps with the assessment phase of an overall security management strategy. MBSA includes a graphic and command-line interface (CLI) that can perform local or remote scans of Microsoft Windows systems.

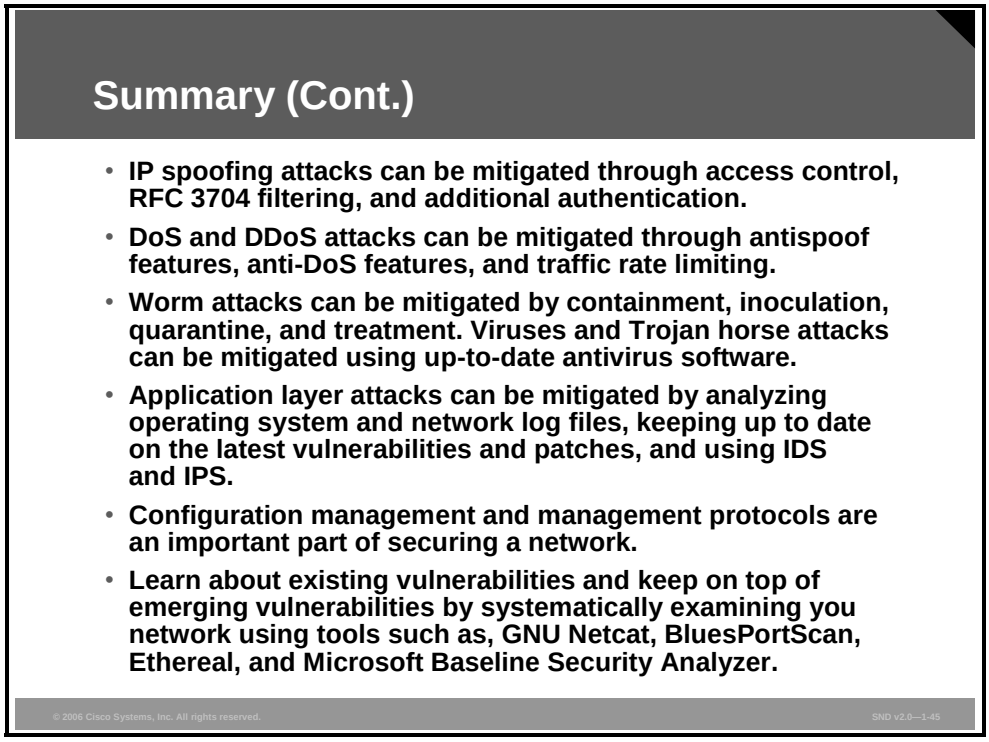


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 3

# Thinking Like a Hacker

## Overview

In many ways, hackers and software developers think very much alike. They both follow a specific methodology and both carefully document their work. Thinking like a successful hacker is not much different from thinking like a good software developer. However, the goals of a hacker are quite different from those of a software developer. Knowing the methodologies that hackers use will help you to develop an effective security policy.

## Objective

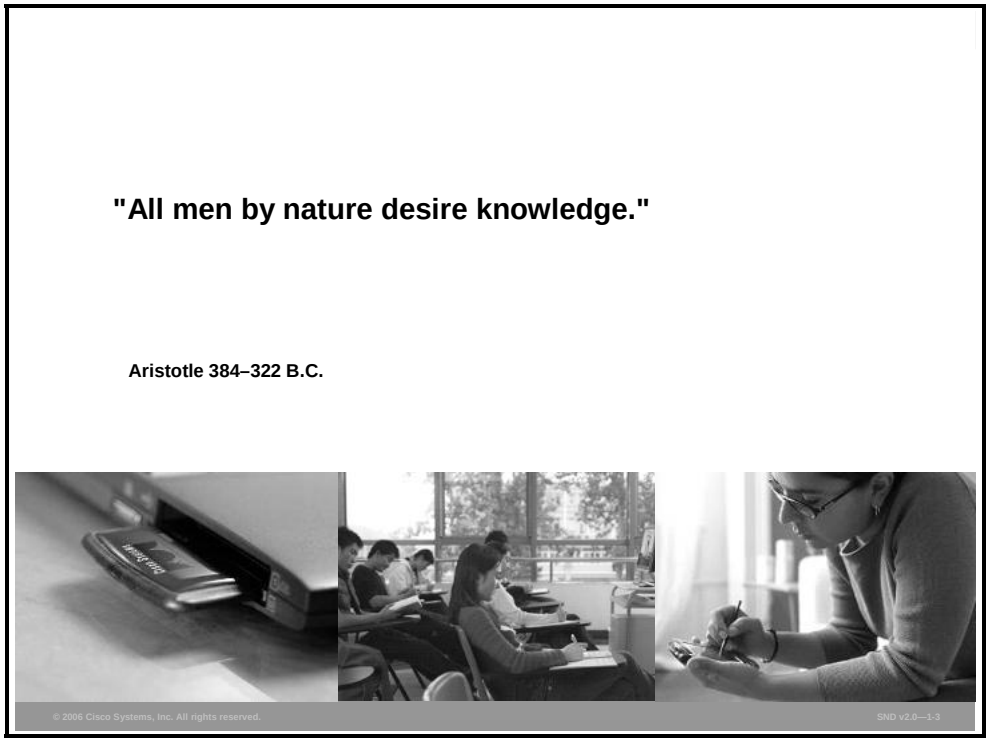
Upon completing this lesson, you will be able to describe the common methodologies used by hackers to break into and exploit networks. This ability includes being able to meet these objectives:

- Describe how hackers work so that you will have a better appreciation of the threats that they pose
- Describe how hackers build a footprint of an organization from which they can launch an attack
- Describe how hackers enumerate information
- Describe how hackers manipulate users to gain access
- Describe how hackers attempt to escalate their privileges
- Describe common ways that hackers gather system passwords and secrets
- Describe how hackers install back doors and port redirectors
- Describe how hackers take advantage of compromised systems
- Describe some best practices that can help defend your network from hackers

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# How Do Hackers Think?

This topic describes how hackers work so that you will have a better appreciation of the threats they pose.




Hackers comprise the most well-known outside threat to information systems. They are not geniuses, but they are persistent people who have taken a lot of time to learn their craft.

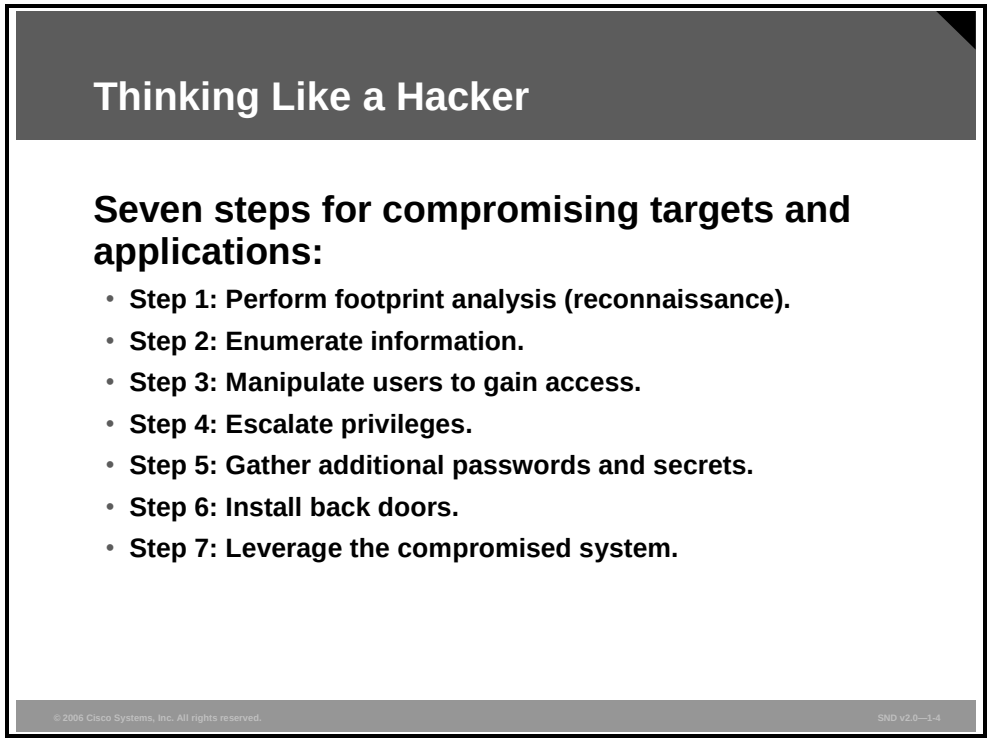
There are many titles assigned to hackers.

- Hackers break into computer networks to learn more about them. Some hackers generally mean no harm and do not expect financial gain. Unfortunately, hackers may unintentionally pass valuable information on to people who do intend to harm the system.
- Crackers (*cr*iminal h*ackers*) are hackers with a criminal intent to harm information systems. Crackers are generally working for financial gain and are sometimes called black hat hackers.
- Phreakers (*ph*one br*eakers*) pride themselves on compromising telephone systems. Phreakers reroute and disconnect telephone lines, sell wiretaps, and steal long-distance services.

| | |
|---|---|
| **Note** | When describing individuals whose intent is to exploit a network maliciously, they are often incorrectly referred to as hackers. In this lesson, the term hacker is used, but may refer to someone more correctly referred to as a cracker, or black hat hackers. |

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



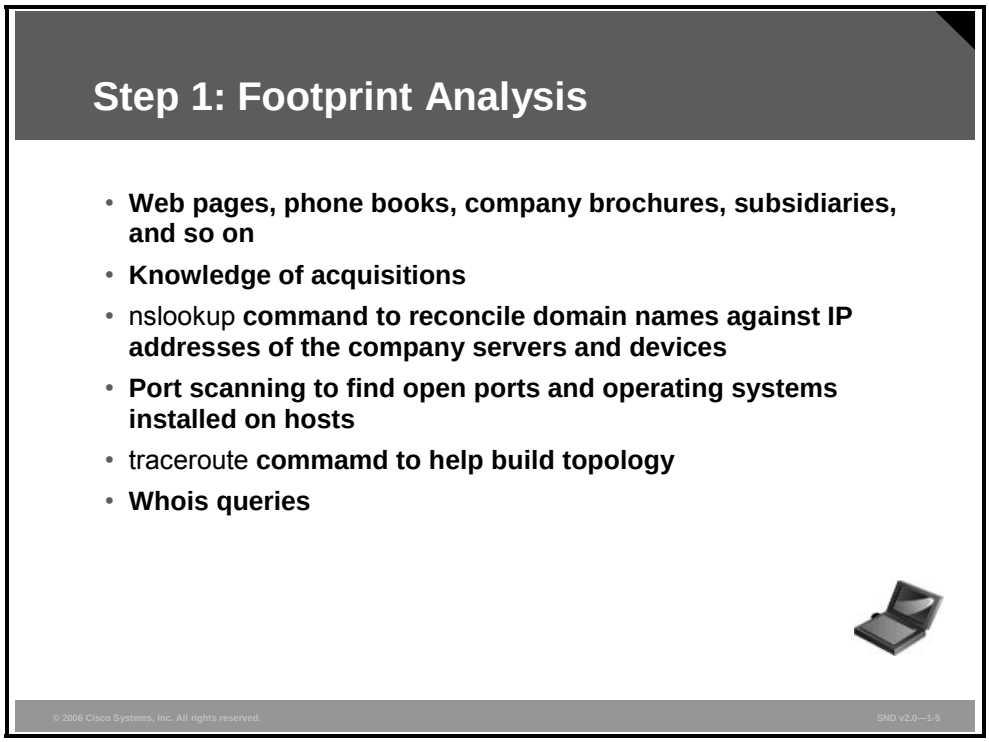

The goal of any hacker is to compromise the intended target or application. Hackers begin with little or no information about the intended target, but by the end of their analysis, they will have accessed the network and will have begun to compromise their target. Their approach is always careful and methodical—never rushed and never reckless. The seven-step process outlined in the figure is a good representation of the method that hackers use.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Step 1: Footprint Analysis

To hack into a system successfully, hackers want to know as much as they can about the system. This topic describes how hackers build a footprint of an organization from which they can launch an attack. By following some simple advice, network administrators can make footprinting more difficult.




Hackers can build a complete profile or "footprint" of the company security posture. Using a range of tools and techniques, an attacker can discover the company domain names; network blocks; IP addresses of systems, ports and services used; and many other details pertaining to the company security posture as related to the Internet, an intranet, remote access, and an extranet.

In a simple scenario, an attacker might start with the company web page. A web page can lead to other sources of information. After the hacker has the company domain name (an easy thing to find), determining the IP addresses of servers and devices is relatively easy.

In another scenario, assume that the footprint reveals a recently acquired startup company. Assume further that this startup company has weaker security than the new parent company. The attacker may be able to use this weakness, possibly through poorly protected virtual private network (VPN) links.

Building a footprint, or "footprinting," is an iterative process. Initially, footprinting provides a number of hostnames, their IP addresses, and a basic picture of the network topology. Hackers can use the whois databases maintained by the InterNIC and domain name registrars to build on this information.

Whois databases contain name server, registrar, and, in some cases, full contact information about a domain name. The InterNIC maintains a central registry whois database containing only registrar and name server information for all .com, .net, and .org domains. However, each registrar must maintain a whois database containing all of the contact information for the domains that they host. Try a whois lookup at http://www.whois.net/.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

These are some of the tools used in footprinting:

- **Commands:** Using the information revealed by the whois effort, the hacker can execute more searches using these commands to develop a more detailed footprint:
  - **nslookup:** Performs Domain Name System (DNS) queries and zone transfers
  - **traceroute (tracert):** Helps build network maps of the target network presence
- **Programs and utilities:**
  - **Uwhois:** The http://www.uwhois.com/ web interface performs whois lookups, forward and reverse DNS searches, and traceroutes.
  - **Nmap:** Network Mapper (Nmap) is a free open source utility for network exploration or security auditing. Nmap rapidly scans large networks and single hosts. Go to http://www.insecure.org/nmap/.
  - **Foundstone ScanLine:** Foundstone ScanLine is a Microsoft Windows NT-based port scanner.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Defeat Footprinting

- **Keep all sensitive data off line (business plans, formulas, and proprietary documents).**
- **Minimize the amount of information on your public website.**
- **Examine your own website for insecurities.**
- **Run a ping sweep on your network.**
- **Familiarize yourself with ARIN to determine network blocks.**



© 2006 Cisco Systems, Inc. All rights reserved.


These are some basic steps to take to make footprinting more difficult:

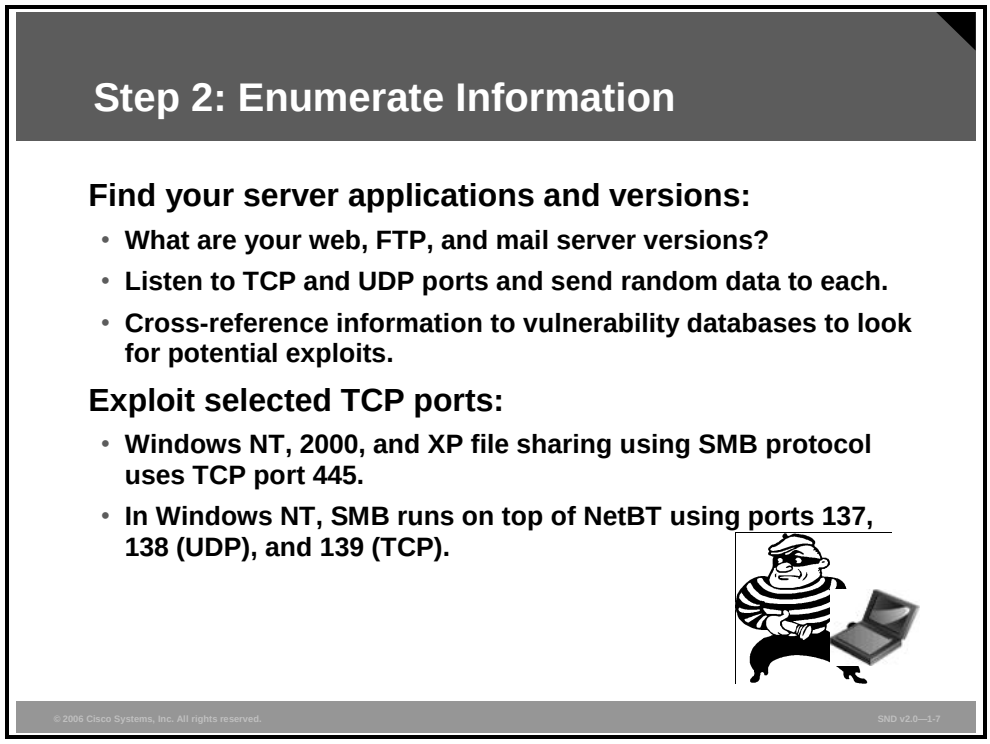
- Keep all information that has the potential to identify and compromise the security of your organization off line. This includes access to business plans, formulas, and proprietary documents.
- In determining how much corporate information to provide the public, balance business needs against security and privacy. Generally, a minimum amount of information is all that you require.
- Audit your organization website from the point of view of a hacker to reveal any potential insecurity.
- Run a ping sweep on your network and carefully examine the results from the point of view of a hacker.
- Familiarize yourself with the American Registry for Internet Numbers (ARIN) to determine network blocks.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Step 2: Enumerate Information

Footprinting generates a map of the target network. Enumeration is the effort aimed at building on the footprint and compiling more specific network data. This topic describes how hackers enumerate information.




Hackers are now interested in finding this information:

- **Server applications and versions:** Hackers find out what web, FTP, and mail server versions you are running by listening to TCP and UDP ports and sending random data to each. Hackers cross-reference this information using vulnerability databases to look for potential exploits. The SecurityFocus website at http://www.securityfocus.com/ provides an index of exploits and vulnerabilities.
- **Exploiting selected TCP ports:** Hackers select TCP ports based on the sensitive information contained on known ports. For example, file sharing using Server Message Block (SMB) protocol in Microsoft Windows NT, 2000, and XP uses TCP port 445. In Windows NT, SMB runs on top of NetBIOS over TCP/IP (NetBT) ports 137 (TCP and UDP), 138 (UDP), and 139 (TCP). If hackers are able to contact the host on these ports, they attempt to enumerate anonymously sensitive information from the system including user names, last login dates, password change dates, and group memberships.

Hackers look for information from listening ports and estimate the level of permission that is required to enumerate this information. They also want to know if a login is required to determine if someone has enumerated this information. Hackers also look to see if a potential exists for an authenticated user to view security-sensitive data or personally identified information that might compromise privacy concerns.

Hackers use the tools listed here. All of these tools are readily available to download, and security staff should know how these tools work.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

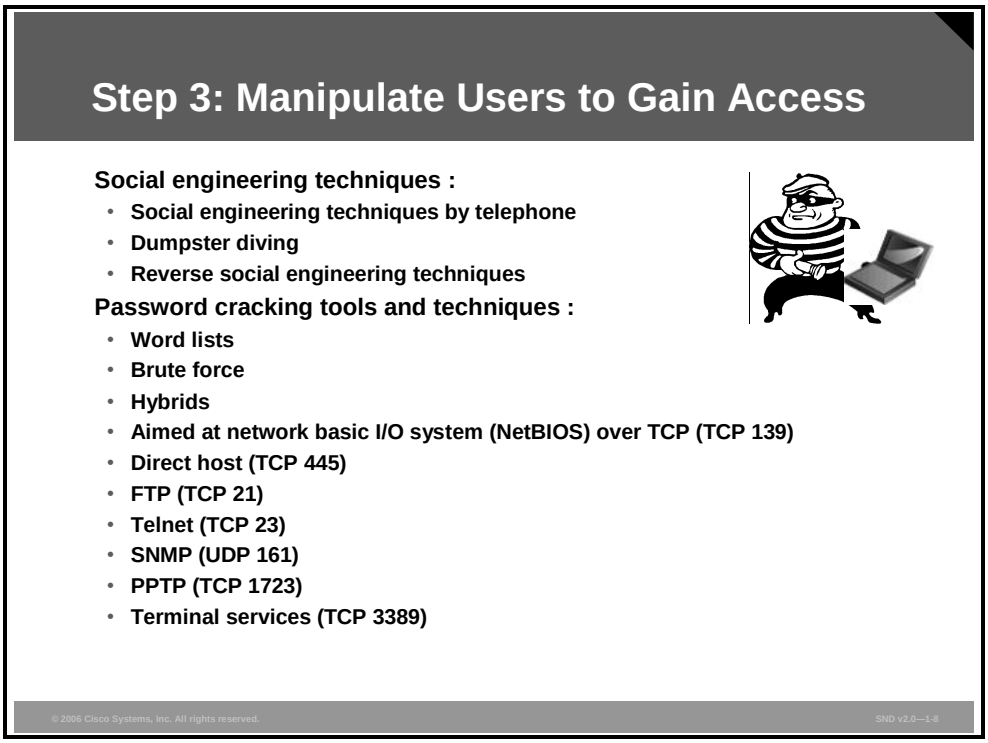
- **Netcat:** Netcat is a featured networking utility that reads and writes data across network connections using the TCP/IP protocol. You can use Netcat directly or driven by other programs and scripts as a reliable back-end tool. Netcat is a feature-rich network debugging and exploration tool because it can create almost any kind of connection you would need and has several interesting built-in capabilities. Hackers use Netcat to grab banners and to scan ports. You will use it in an upcoming lab exercise to find vulnerabilities in your own network. You will find Netcat at http://netcat.sourceforge.net/.
- **Microsoft EPDump and Microsoft Remote Procedure Call (RPC) Dump:** These tools provide information about Microsoft RPC services on a server:
  - The **Microsoft** EPDump application shows what is running and waiting on dynamically assigned ports. For more information, see http://www.security-solutions.net/download/index.html.
  - The RPC Dump (rpcdump.exe) application is a command-line tool that queries RPC endpoints for status and other information on RPC. For more information, see http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/rpcdump-o.asp.
- **GetMAC:** This application provides a quick way to find the MAC (Ethernet) layer address and binding order for a computer running Microsoft Windows 2000 locally or across a network. This application is useful when you want to enter the address into a sniffer, or if you need to know what protocols are currently in use on a computer. For more information, see http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/getmac-o.asp.
- **DumpSec by SomarSoft:** This application is a security auditing program for Microsoft Windows NT, XP, and 2000 or later systems. SomarSoft DumpSec enumerates user and group details from a chosen system. This is the audit and enumeration tool of choice for hackers. For more information, see http://www.somarsoft.com/.
- **Software development kits (SDKs):** SDKs provide hackers with the basic tools that they need to learn more about systems. The Microsoft Windows SDK provides the documentation, samples, header files, libraries, and tools that you need to develop applications that run on Microsoft Windows. See the Microsoft site at http://www.microsoft.com/downloads/details.aspx?FamilyId=A55B6B43-E24F-4EA3-A93E-40C0EC4F68E5&displaylang=en.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Step 3: Manipulate Users to Gain Access

There are countless cases of unsuspecting employees providing information to unauthorized people simply because the requesters appear innocent or to be in a position of authority. Hackers find names and telephone numbers on websites or domain registration records (footprints). Hackers then contact these people directly by phone and convince them to reveal passwords. Hackers do this without raising any concern or suspicion. This topic describes how hackers manipulate users to gain access.




When the hacker knows some basic information about their target, they attempt to masquerade as authorized users. The first thing that hackers need is a password. There are two common ways to get that password: through social engineering or brute-force attack.

## Social Engineering

Our natural human willingness to accept people at their word leaves many of us vulnerable to attack. As a general statement, this trait is the weakest link in the security chain.

Social engineering is a way to manipulate people inside the network to provide the information needed to access the network. A computer is not required.

Here are some social engineering techniques:

- Help desks have responded to calls for forgotten passwords. Help desk operators sometimes feel that their job is to help and not ask questions to verify the identity of the caller. By playing telephone tricks, hackers can appear to be calling from inside the company.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Dumpster diving means exactly what it says. People actually search through company dumpsters or trash cans looking for information. Phone books, organization charts, manuals, memos, charts, and other documentation can provide a valuable source of information for hackers. There have even been cases where hackers have found very sensitive information such as system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware to use in their attacks.
- Reverse social engineering is an interesting twist on the theme. In this case, the hacker appears to be in a position of authority and employees actually ask the hacker for information. Consider a situation in which a hacker causes problems by sabotaging the network. The hacker then appears as the person to fix the problem and, in so doing, requests, and receives, important bits of information from the people the hacker has come to help. The hacker appears to solve the problem and everyone is happy. A well-developed reverse social engineering plan can offer hackers almost limitless chances to find the key information that they need—valuable data from the employees. However, this strategy requires a great deal of preparation, research, and "prehacking" to be successful.

## Password Cracking

Hackers use many tools and techniques to crack passwords:

- **Word lists:** These programs use lists of words, phrases, or other combinations of letters, numbers, and symbols that computer users often use as passwords. Hackers enter word after word, at high speed, until they find a match.
- **Brute force:** This approach relies on power and repetition. It compares every possible combination and permutation of characters until it finds a match. Using brute force will eventually crack any password, but it may take a long, long time. Using brute force is an extremely slow process because it uses every conceivable character combination.
- **Hybrid crackers:** Some password crackers mix the two techniques. This combines the best of both methods and is highly effective against poorly constructed passwords.

Password cracking attacks any application or service that accepts user authentication, including those listed here:

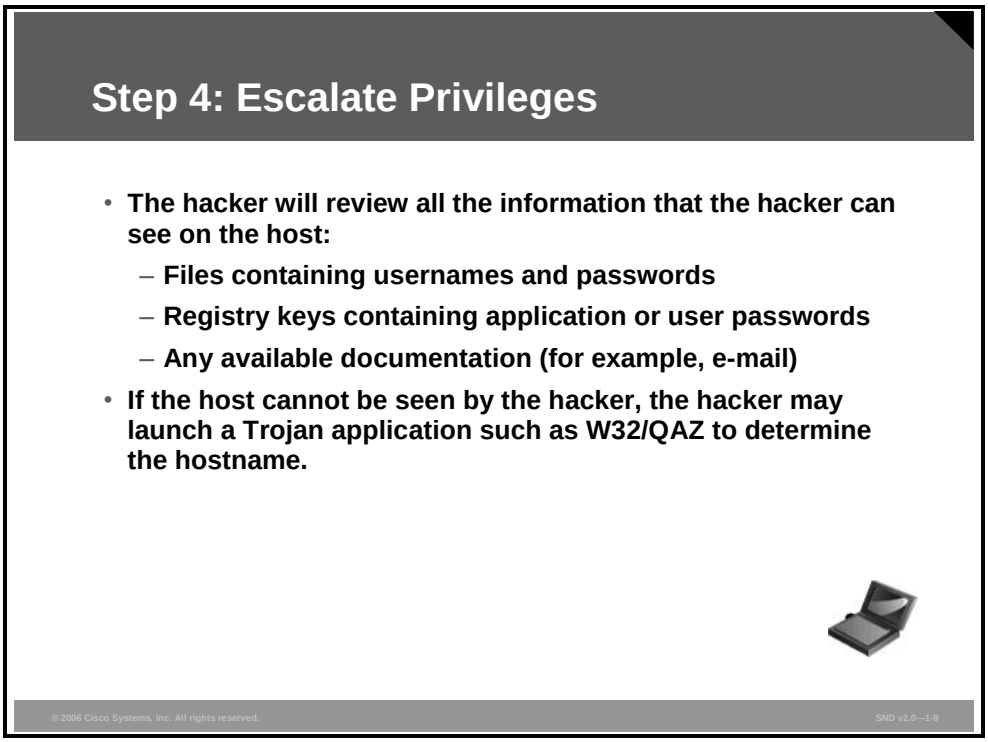
- Network basic I/O system (NetBIOS) over TCP (TCP 139)
- Direct host (TCP 445)
- FTP (TCP 21)
- Telnet (TCP 23)
- Simple Network Management Protocol (SNMP) (UDP 161)
- Point-to-Point Tunneling Protocol (PPTP) (TCP 1723)
- Terminal services (TCP 3389)

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Step 4: Escalate Privileges

This topic describes how hackers attempt to escalate their privileges after they secure a password for a user account and user-level privileges to a host.




The first step is to review all the information on the host that the hacker has collected; for example, files containing usernames and passwords and registry keys containing application or user passwords. (Any available documentation, including e-mails and other documents, may also be of assistance.)

If this step does not succeed, the hacker may launch a Trojan horse attack. This type of attack usually means copying malicious code to the user system and giving it the same name as a frequently used piece of software.

A simple example might have the hacker replace the Microsoft Notepad application (notepad.exe) of the victim with a doctored Trojan horse Notepad. This happened in 2000 when a large corporation experienced an attack by the W32/QAZ, a Trojan horse and an Internet worm that acts as a back door. When it is running, it listens on TCP port 7597 for instructions from a client component. The Trojan horse also communicated with the IP address 202.106.185.107, physically located somewhere in China. The back door allows the remote user to upload and run any program. At this point in the attack, the hacker can install a more complex back door or password-stealing program.

As a worm, W32/QAZ browses network connections to spread to other machines that allow passwordless write access to their Microsoft Windows folders over NetBIOS. W32/QAZ copies itself as “notepad.exe” and renames the existing notepad.exe to note.com.

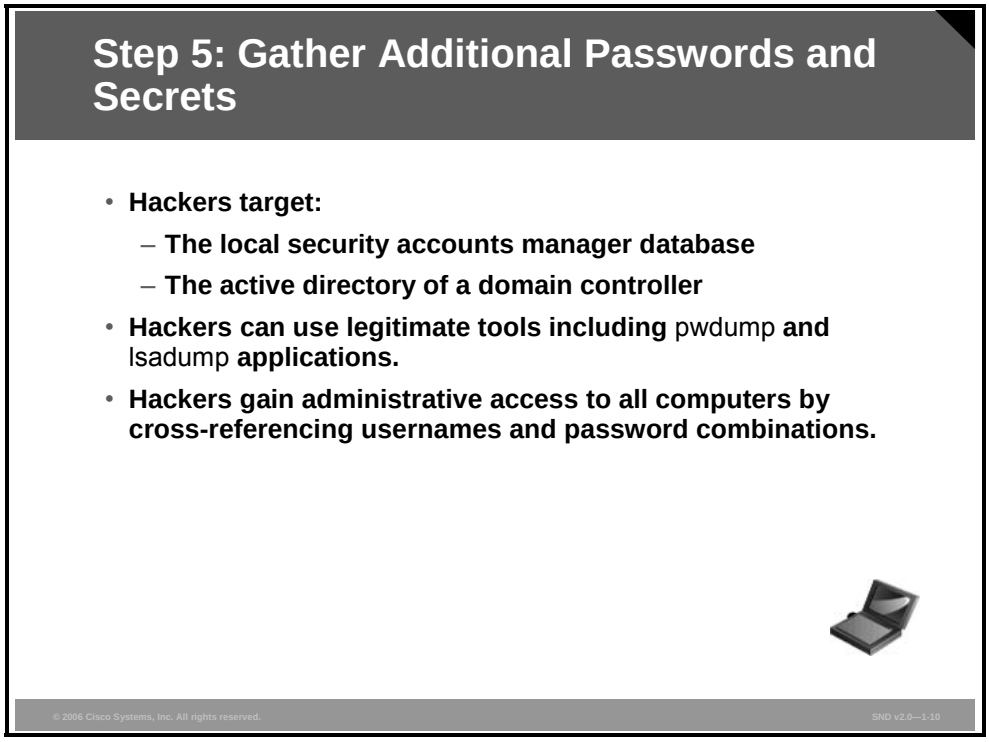
W32/QAZ can give access to the host system that allows a hacker or group of hackers to install other malicious software programs if desired. When the victim opens the Microsoft Notepad application, the Trojan horse makes the victim an administrator on the system before the program launches Microsoft Notepad. This is transparent to the victim, but by logging in as the victim, the hacker now has administrator privileges.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Step 5: Gather Additional Passwords and Secrets

After the hacker has higher network administrator privileges, the next task is to gather more passwords and other sensitive data. This topic describes the common ways that hackers gather system passwords and secrets.



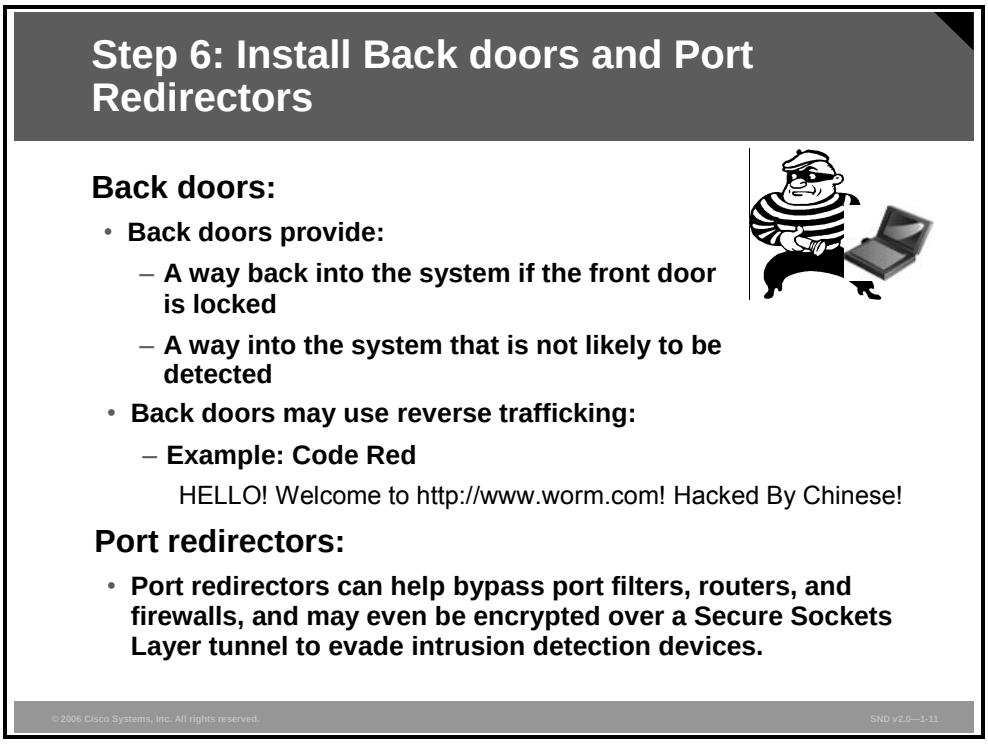

The targets now include such things as the local security accounts manager database or the active directory of a domain controller, where hackers use legitimate tools including pwdump and lsadump applications. By cross-referencing username and password combinations, the hacker is able to obtain administrative access to all computers in the network.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Step 6: Install Back Doors and Port Redirectors

Legitimate users enter systems through the "front door" and abide by the rules assigned to their privilege level. Hackers often build "back doors" to avoid any impediments in their quest to control the network. This topic describes how hackers install back doors and port redirectors.




## Back Doors

Back doors provide hackers with a way into the system if they are detected trying to enter through the front door, or if they want to enter the system without being detected. The most common backdoor point is a listening port that provides remote access to the system for users (hackers) who do not have, or do not want to use, access or administrative privileges.

Firewalls or router filtering may prevent the hacker from later accessing these ports. However, common router filtering may not block high-numbered TCP ports (or any UDP ports). In addition, firewalls and filters may allow traffic originating on a source port such as TCP 20, 53, or 8 to pass. When these ports are blocked, back doors that are more complex are necessary.

Reverse trafficking is a complex backdoor point that enables the attacker to bypass the existing security mechanisms. While routers and firewalls may prevent all unsolicited packets from entering the network from the outside, a client inside the firewall can still initiate a connection on a specified port number to any host on the outside.

Assume that a hacker installs a reverse trafficking Trojan horse to use TCP port 80 to contact computer of the hacker on a regular basis. Because the client computer "pushes" a system-level command shell to the hacker, the hacker can execute code on the "protected" computer.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

The Code Red worm is an example of a backdoor approach. The Code Red worm used reverse trafficking. When installed, Code Red used TCP port 80 to instruct unpatched web servers to execute a TFTP connection from the server to a randomly chosen host on the Internet where it obtained a piece of rogue code. Because the initiating traffic to the web server was legitimate, it passed the firewall. Subsequently, firewalls and routers allowed the web server to initiate a TFTP (UDP 69) connection to the computer belonging to the hacker. If the exploit is successful, the victim host will experience this defacement on all web pages requested from the web server:

**HELLO! Welcome to http://www.worm.com! Hacked By Chinese!**

# Port Redirectors

Port redirectors can help bypass port filters, routers, and firewalls, and can evade intrusion detection. For example, assume that a firewall has ports 80 (HTTP) and 443 (HTTPS) open by default, but port 443 is unused. Assume that there is a database server on port 3389 (ms-wbt-server).

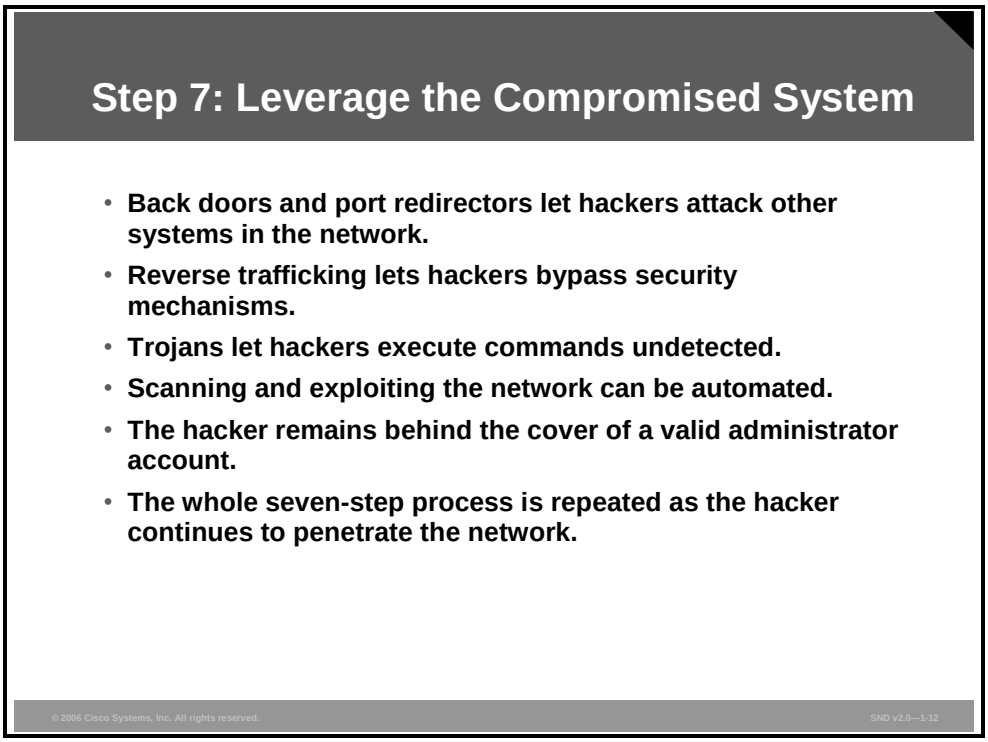
A hacker can select port 443 as a listening port and remain undetected. The hacker can then set up a port redirector without disrupting operations. A port redirector takes traffic coming in on one port and directs it to another host on another port. In this example, the port redirector on the web server takes incoming traffic on port 443 and sends it out to port 3389 on the database server.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Step 7: Leverage the Compromised System

The hacker is now in control of the system. This topic describes how hackers take advantage of compromised systems.




After installing back doors and port redirectors, hackers try to attack other systems after fully hacking the local system.

Recall that reverse trafficking enables hackers to bypass security mechanisms. Trojan horses help hackers execute commands undetected.

If the target host enables failed login auditing or runs a third-party intrusion detection system (IDS), it will record the IP address or computer name of the host running the port redirector and not the system used by the hacker. This makes it difficult to identify the attacker directly.

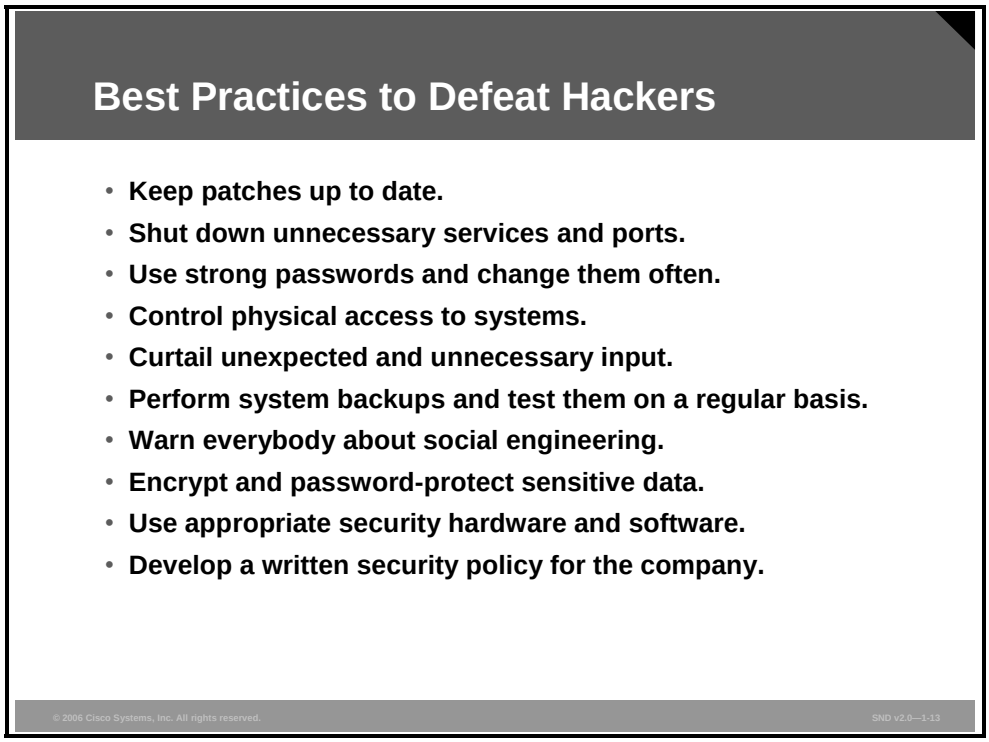
After hackers gain administrative access, they enjoy hacking other systems on the network. As each new system is hacked, the attacker performs the steps outlined previously to gather additional system and password information. Hackers will try to scan and exploit a single system or a whole set of networks. The whole process can be made automated. It is difficult to identify this type of activity because the attacker is usually operating under the guise of a valid administrator account. Unless you catch the attacker before the person gains administrator access, it may be nearly impossible to flush the attacker from the network.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Best Practices to Defeat Hackers

This topic describes some best practices to help defend your network against hackers.




Defending your network against attack requires constant vigilance and education. These 10 practices represent the best insurance for your network:

- Keep patches up to date by installing them weekly or daily, if possible, to prevent buffer overflow and privilege escalation attacks.
- Shut down unnecessary services and ports.
- Use strong passwords and change them often.
- Control physical access to systems.
- Avoid unnecessary web page inputs. Some websites allow users to enter usernames and passwords. A hacker can enter more than just a username. For example, entering “jdoe; rm -rf /”might allow an attacker to remove the root file system from a UNIX server. Programmers should limit input characters and not accept invalid characters such as | ; < > as possible input.
- Perform backups and test the backed up files on a regular basis.
- Educate employees about the risks of social engineering and develop strategies to validate identities over the phone, via e-mail, or in person.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software such as firewalls, intrusion prevention systems (IPSs), antivirus software, and content filtering.
- Develop a written security policy for the company.

These methods are only a starting point for sound security management. Organizations must remain vigilant at all times to defend against continually evolving threats.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- Hackers generally follow a systematic and rigorous seven-step process to break into networks.
- Hackers start by building a footprint. Common sense steps are required to frustrate footprinting.
- Hackers discover exploits and vulnerabilities by learning what server and application versions you are running.
- Social engineering, dumpster diving, and plain hard work allow hackers to discover usernames and passwords.
- Once they have gained access to a network, hackers escalate their user privileges to administrator levels.

© 2006 Cisco Systems, Inc. All rights reserved.


## Summary (Cont.)

- Posing as administrators, hackers gather additional passwords and secrets and exploit more devices.
- Back doors and port redirectors allow hackers to come and go as they like.
- Once they have free rein, hackers can attack other parts of your network.
- There are some best practices to help you defend your network from hackers.

© 2006 Cisco Systems, Inc. All rights reserved.




*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 4

# Designing a Secure Network Life-Cycle Model

## Overview

Building a secure network requires proactive thought and action to handle unforeseen security issues when your network is in operation. Good network design requires you to consider the entire life cycle of the network and, in particular, the security aspects of your network design.

Cisco Systems uses the planning, designing, implementing, operating, and optimizing (PDIOO) network life-cycle model to assist in the design of a secure network. While it does not matter what life model you use, you must design your network in a structured, planned, and modular fashion. You also need feedback and experience from users to control enhancement or redesign projects.

This lesson provides a secure network design model that uses the PDIOO approach. Learning the steps in a PDIOO approach is important if you are studying for Cisco design certification.

## Objectives

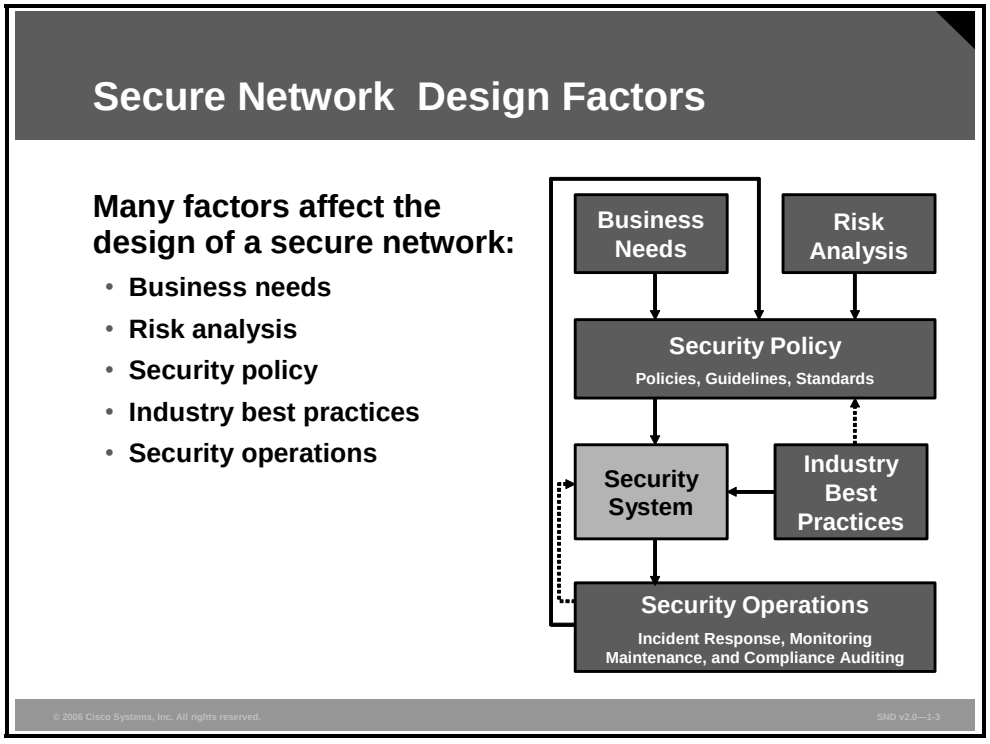
Upon completing this lesson, you will be able to describe the main activities in each phase of a secure network life cycle. This ability includes being able to meet these objectives:

- Describe the factors that you need to consider when designing a network security system
- Describe the PDIOO approach that is used to design a secure network life-cycle management process
- Describe the activities included in the plan phase of the secure network life cycle
- Describe the activities included in the design phase of the secure network life cycle
- Describe the activities included in the implement phase of the secure network life cycle
- Describe the activities included in the operate phase of the secure network life cycle
- Describe the activities included in the optimize phase of the secure network life cycle
- Describe the measures that you follow in the dispose phase of the secure network life cycle
- Describe the system-level security principles that you consider throughout the life cycle of a secure network

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Components of Network Security Design

This topic describes the factors that you need to consider when designing a network security system.




Business goals and risk analysis drive the need for network security. Regardless of the security implications, business needs must come first. If your business cannot function because of security concerns, you have a problem. The security system design must accommodate the goals of the business, not hinder them. Risk analysis includes these two key elements:

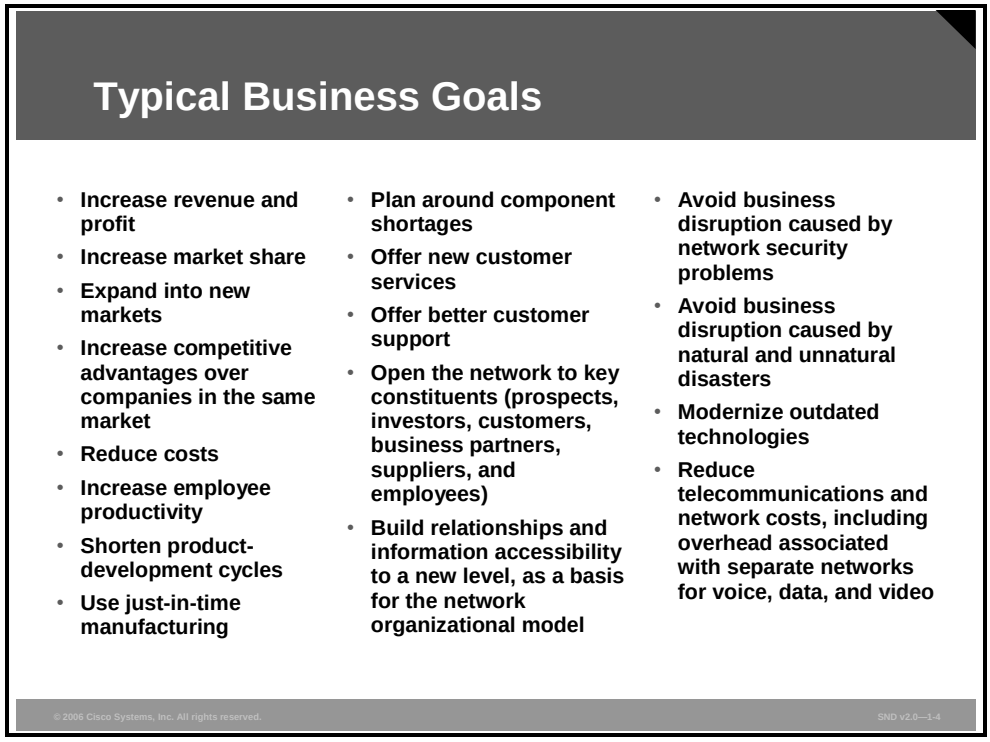
- What does the cost-benefit analysis of your security system tell you?
- How will the latest attack techniques play out in your network environment?

These are the key factors to consider when designing a secure network:

- **Business needs:** What does your organization want to do with the network?
- **Risk analysis:** What is the risk and cost balance?
- **Security policy:** What are the policies, standards, and guidelines needed to address business needs and risks?
- **Industry best practices:** What are the reliable, well-understood, and recommended security best practices?
- **Security operations:** These operations include incident response, monitoring, maintenance, and compliance auditing of the system.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



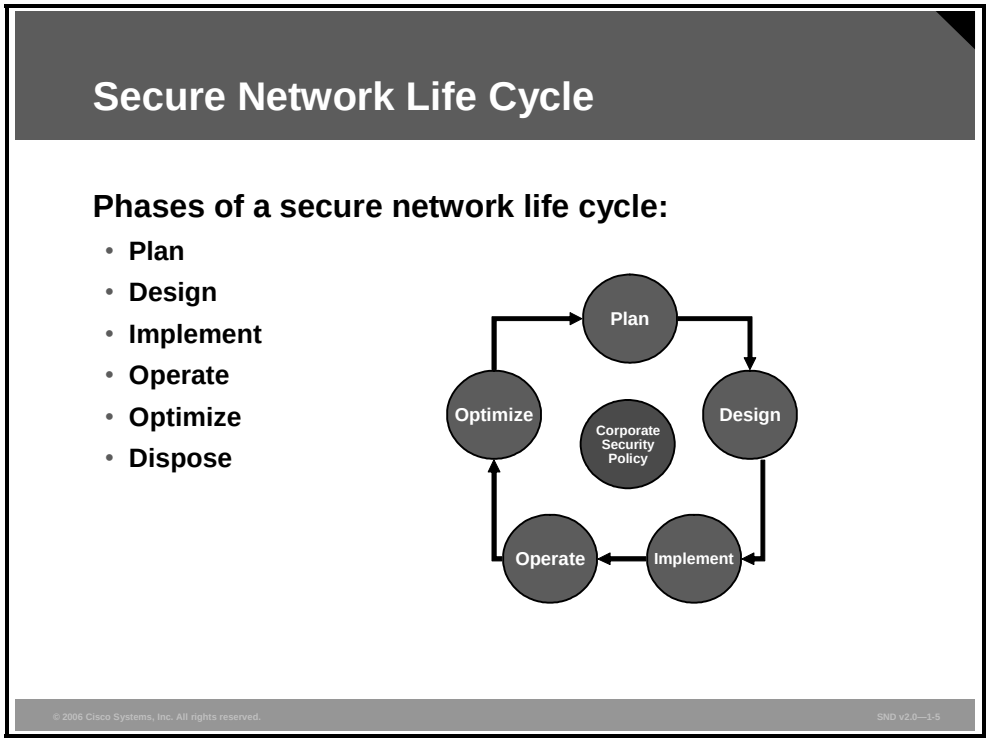

The figure lists typical business goals that may influence a security policy. When you create or review the security policy of your organization, you should consider the impact that organizational goals may have on that policy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Secure Network Life-Cycle Management

This topic describes the PDIOO approach used to design a secure network life-cycle management process.

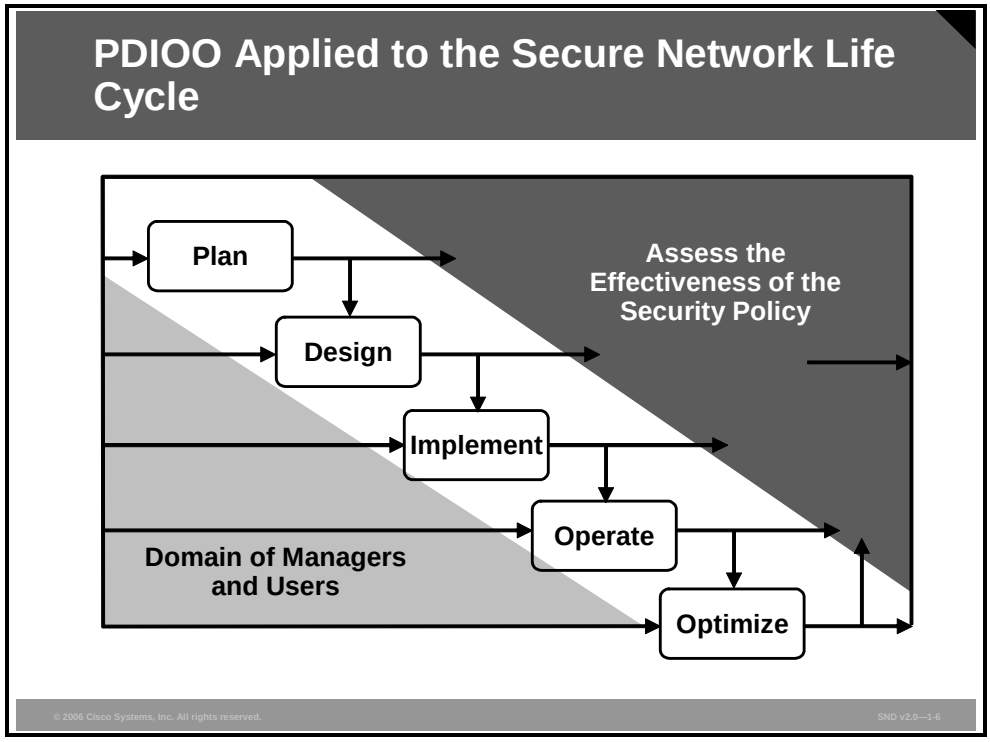



Network security is a process based on security policy. The life cycle of network security consists of these six phases:

- **Plan:** The network designers identify network requirements in this phase. The plan includes analyzing the places where the network will be installed and identifying the people and processes that need network services.
- **Design:** In this phase, the network designers accomplish the bulk of the logical and physical design according to the requirements gathered during the plan phase.
- **Implement:** After management approves the design, implementation begins according to the design specifications. Implementation also serves to verify the design.
- **Operate:** Operation is the final test of the effectiveness of the design. The network is monitored for faults and performance problems during this phase to provide input into the optimize phase of the network life cycle.
- **Optimize:** The optimize phase uses proactive network management techniques to identify and resolve problems before network disruptions arise. The optimize phase may lead to a network redesign if too many problems arise because of design errors or as network performance degrades over time as actual use and capabilities diverge. Redesign may also be required when requirements change significantly.
- **Dispose:** When the network, or a part of the network, is out of date, management may take the out-of-date components out of production. Although Cisco does not include this phase in the life cycle (PDIOO), it is nonetheless an important phase.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



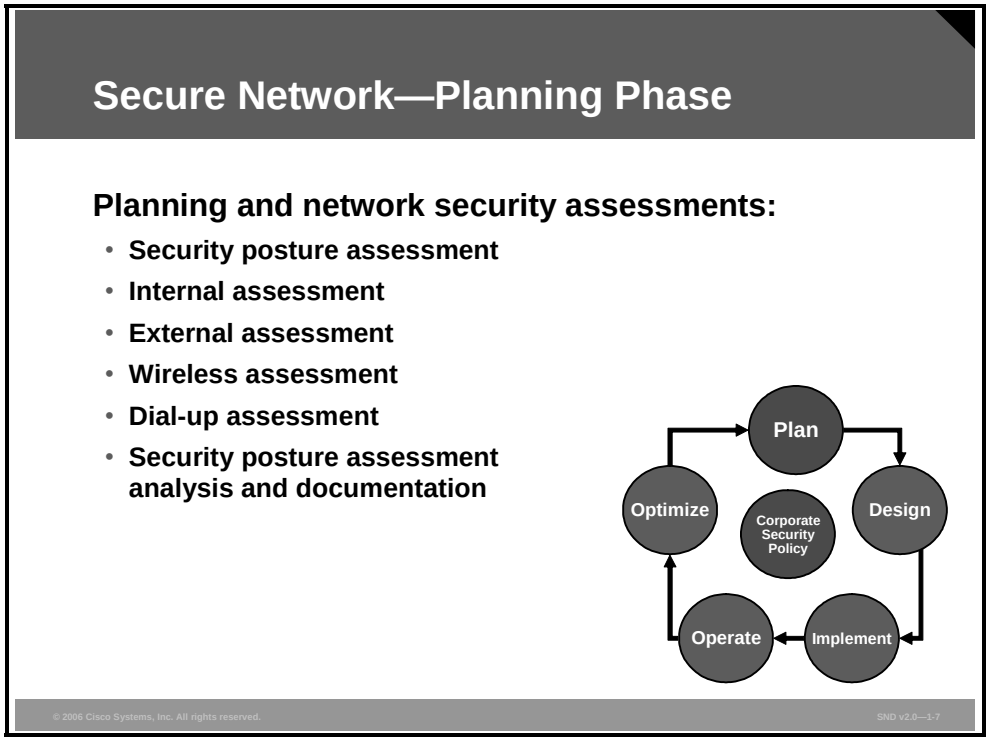

The figure shows the life cycle of a secure network and the dependencies and directions of the information flow between these life-cycle activities. Arrows indicate the flow of information between the activities but not necessarily their sequence or timing. Although not representing an activity, the label “Domain of Managers and Users” is a reminder that throughout the process, there is continual interaction and feedback between the systems engineer or information systems security engineer and the users.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Planning a Secure Network

This topic describes the activities included in the plan phase of the secure network life cycle.




By assessing all aspects of the networked business environment, it is possible to determine the ability of the organization to detect, defend against, and respond to network attacks. These are the key activities:

- **Security posture assessment:** The first step in planning network security requires an evaluation of the network security posture of the organization. The security posture assessment provides a snapshot of the security state of the network by conducting a thorough assessment of the network devices, servers, desktops, and databases.

  Analyze the effectiveness of the network security against recognized industry best practices to identify the relative strengths and weaknesses of the environment and document specific vulnerabilities that could threaten the business. Because network security involves all aspects of the business, it is necessary to assess security from a variety of perspectives, including the internal, external, dial-up, and wireless networks, and to provide recommendations on how to improve overall network security.

- **Internal assessment:** With so much attention devoted to threats and incidents by hackers, administrators may overlook the security of the internal trusted network. The internal assessment is a controlled network attack simulation used to gauge the exposure present on internal systems, applications, and network devices. The assessment identifies the steps needed to thwart intentional attacks or unintentional mistakes from trusted insiders to effectively secure valuable information assets.

  To go beyond automated detection of vulnerabilities, you could simulate a real intruder in a controlled, safe manner to confirm vulnerabilities manually. The assessment provides a more structured approach to identifying vulnerabilities that may go undetected. This secondary exploitation may include attempting to exploit trusted relationships between hosts, exploiting password weakness, or gaining administrative access to systems.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **External assessment:** The goal of an external assessment is to quantify the security risk associated with Internet-connected systems. After researching and confirming the registration of Internet devices, assessors scan the device for external visibility. Because most services have inherent and well-known vulnerabilities, it must be determined whether the services offered are potentially vulnerable.
- **Wireless assessment:** The wireless assessment provides an evaluation of the security posture of the wireless network within the organization and identifies risks and exposures associated with a wireless deployment.

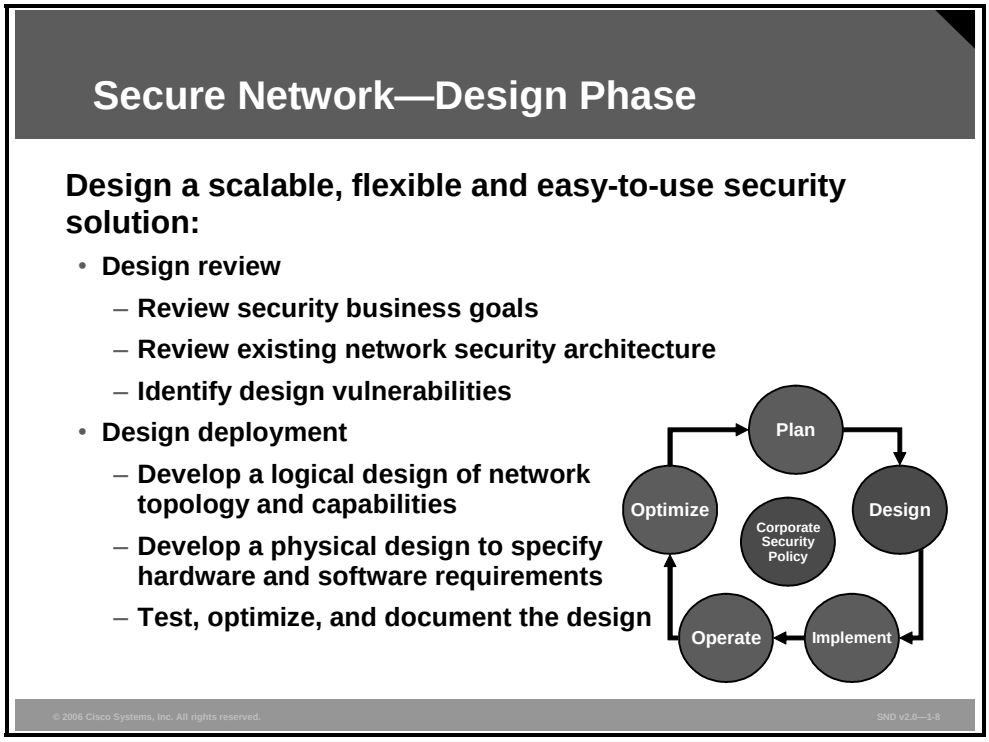
  Assessors analyze the wireless technology architecture and configurations to identify authorized and unauthorized access points and to recommend solutions to strengthen the security of the wireless infrastructure. Assessors also check outside customer buildings to find wireless network traffic leaking from the buildings.
- **Dial-up assessment:** The goal of dial-up assessment is to determine the security risks associated with remote-access services. Dial-up services can provide an attacker with an easy back door into a customer network, bypassing otherwise effective security measures such as firewalls.
- **Security posture assessment analysis and documentation: This assessment** quantifies the security posture of the organization network by using metrics and graphs. The report should also provides technical details, including analysis of each IP address, an explanation of methods used to compromise network devices and systems, and a description of the likelihood that an attacker will use that same approach. The report then prioritizes the vulnerabilities, recommends actions to correct the security risks, and details remediation steps that will prevent future exploitation.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Designing a Secure Network

This topic describes the activities included in the design phase of the secure network life cycle.




After assessing the security state of the network, it is possible to develop a strong security design. The design methodology should consider all aspects of network security and its integration with the core network infrastructure. Use an in-depth, system-wide approach based on industry standards to develop a multilayer defense against directed attacks from hackers or an indiscriminate attack from viruses and worms.

- **Network security design review:** You need a strong security design from both an operational and technical perspective. Conduct a collaborative review of the organization business strategy and related security goals, requirements, and standards. It is possible to recommend protocol, policy, and feature improvements for individual security components after considering all aspects of network security such as scalability, performance, and manageability.
- **Network security design development:** This step develops a strategy, plan, and design for integrating a new security solution into the core network infrastructure. The design team reviews the security goals of the organization and defines an in-depth analysis of the technical, procedural, and resource requirements for a customized security deployment that meets these goals. You will also make decisions on the hardware, software, and sample configurations for the intended solution. Here are the key steps:
  - **Develop the logical design:** This activity deals with a logical topology for the new or enhanced network, network layer addressing, naming, and switching and routing protocols. Logical design also includes security planning, network management design, and the initial investigation into which service providers can meet WAN and remote-access requirements.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

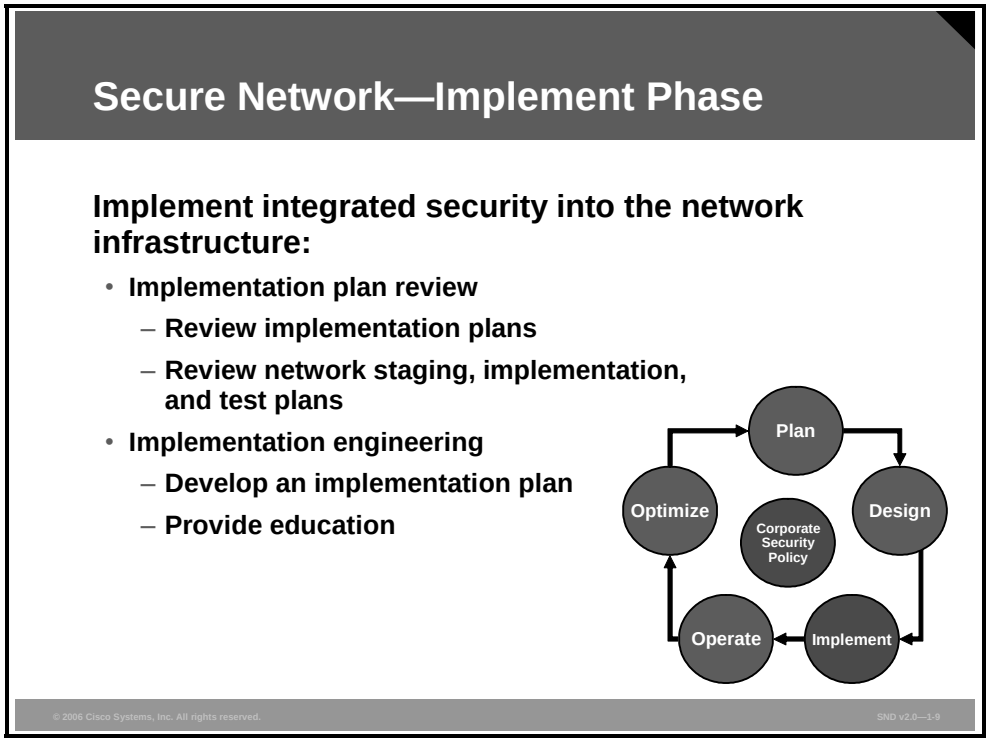
- **Develop the physical design:** You will select specific technologies and products required by the logical design during the physical design activity. You will also complete the selection of service providers.
- **Test, optimize, and document the design:** The final activity is to write and implement a test plan, build a prototype or pilot, optimize the network design, and document your work with a network design proposal.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Implementing a Secure Network

This topic describes the activities included in the implement phase of the secure network life cycle.




When your security solution design is complete, you must define the implementation and deployment activities. During the implement phase, the team uses sound security design principles and assistance provided during the plan and design phases to strengthen their ability to meet aggressive deployment schedules and to help minimize costly disruptions to the existing network infrastructure.

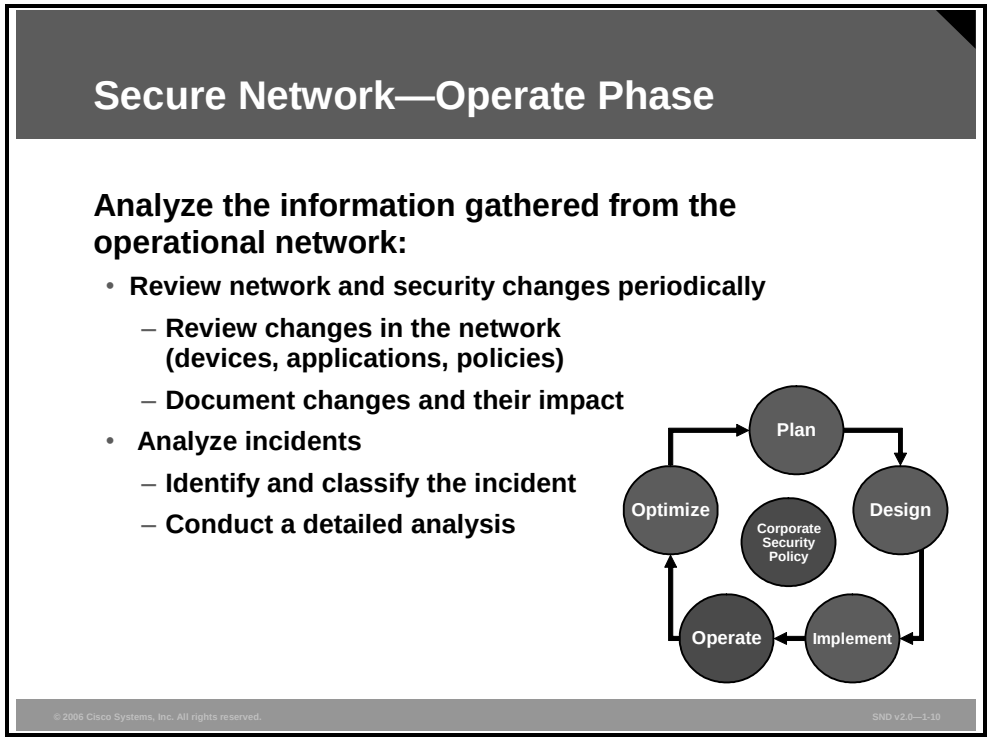
- **Network security implementation plan review:** Begin with a thorough understanding of the objectives and scope of the deployment project. The next step is to review the plan that analyzes the technical requirements, procedures, and resources.
- **Network security implementation engineering:** To be fully effective, you must not only strategically plan your security solution but also make certain that you deploy, configure, tune, and integrate your security solution into the network infrastructure. Educate the users and administrators about your solution to help maintain a secure network and increase the acceptance.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Operating a Secure Network

This topic describes the activities included in the operate phase of the secure network life cycle.




After the network security design is implemented and operational, it is important to review the network periodically to determine if any changes are occurring. These changes might involve new devices that were added, additional applications that were installed, or a change in the security policy. You must document these changes and evaluate their impact on network security.

Conducting follow-up network security audits is an important part of the operations step. The frequency of these security audits is part of the planning step. As the expected losses because of threat changes and new threats begin to surface, new security solutions also become available, and existing solutions become more affordable. Analysis of the audit results, updated expected loss computations, and updated security solution reviews help adjust the security policy with each round of planning. The result of each planning process is an appropriate update to the policy, which includes the timing of the next audit and security policy re-evaluation.

Whenever an incident occurs while the network is operational, it must be identified and classified. This process helps mitigate incidents that may occur in the future and eases the prevention of similar incidents.

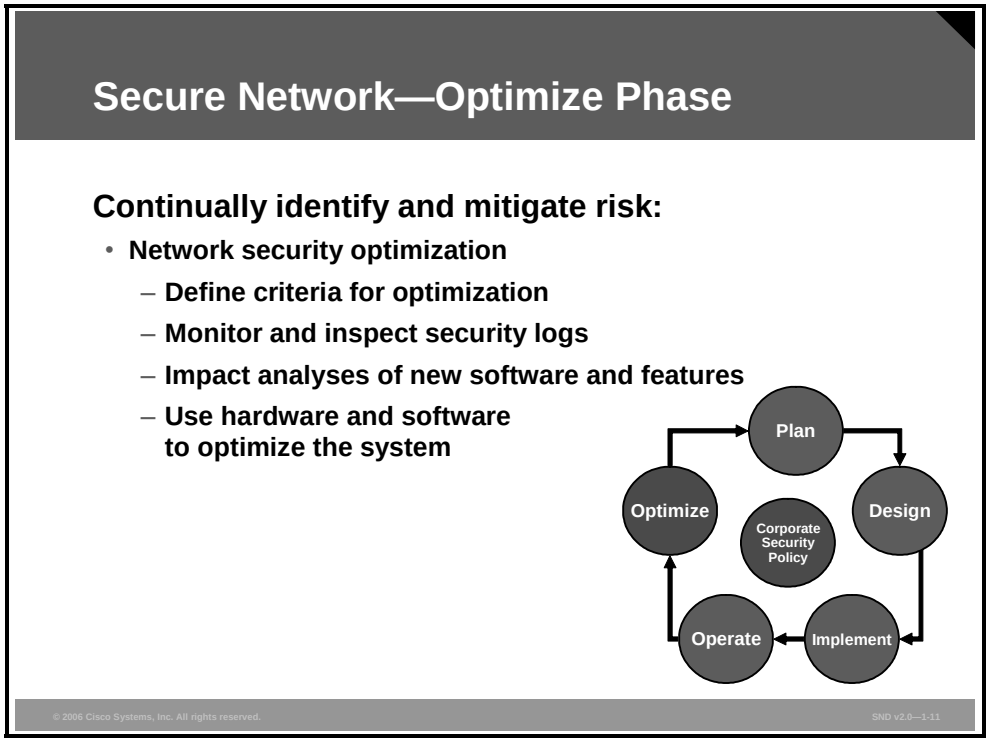
It is important for you to conduct a detailed analysis of incidents and document lessons that you have learned as soon as possible.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Optimizing a Secure Network

This topic describes the activities included in the optimize phase of the secure network life cycle.



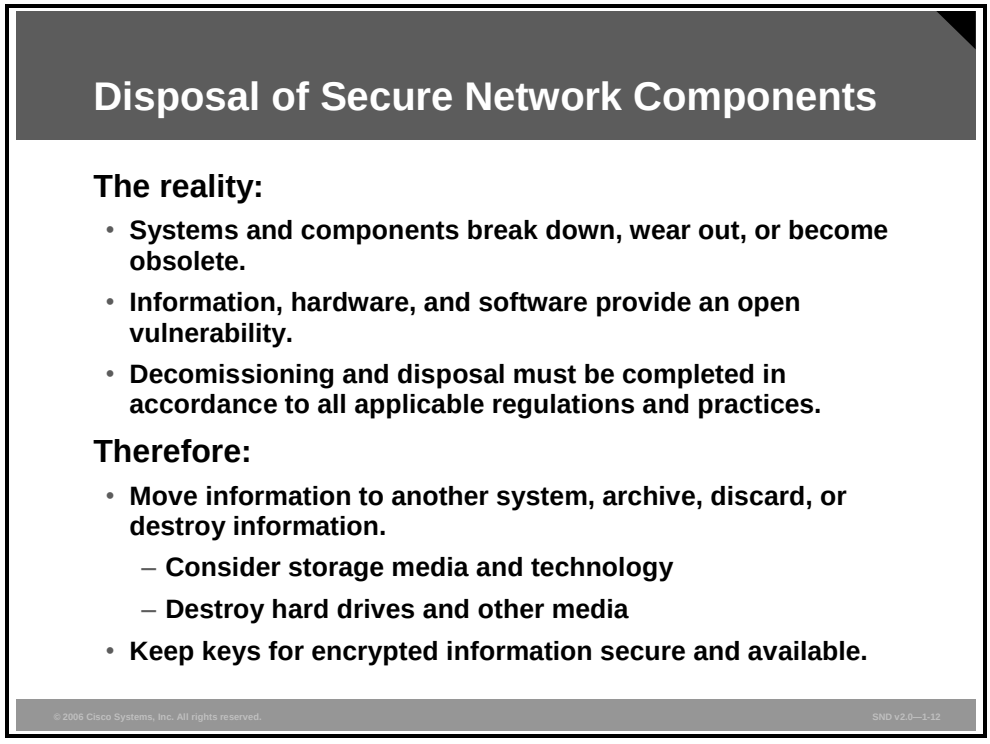

After you deploy the security solution, the network infrastructure is ready to support increased demands that may arise from changing business dynamics and growing network requirements. As network conditions change, perform optimization checks to help ensure that the network security infrastructure continues to meet performance objectives.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Disposing of Secure Network Components

This topic describes the measures that you follow in the dispose phase of the secure network life cycle.




Every system eventually reaches its end of life, and components within the system break down or simply wear out. The disposal phase of the system life cycle involves the state of information, hardware, and software no longer required or of use. Activities include moving, archiving, discarding or destroying information, and sanitizing the media. Disposal activities must meet all applicable regulations and directives.

The disposal phase of the network life cycle involves the state of information, hardware, and software. Your choices include those listed here:

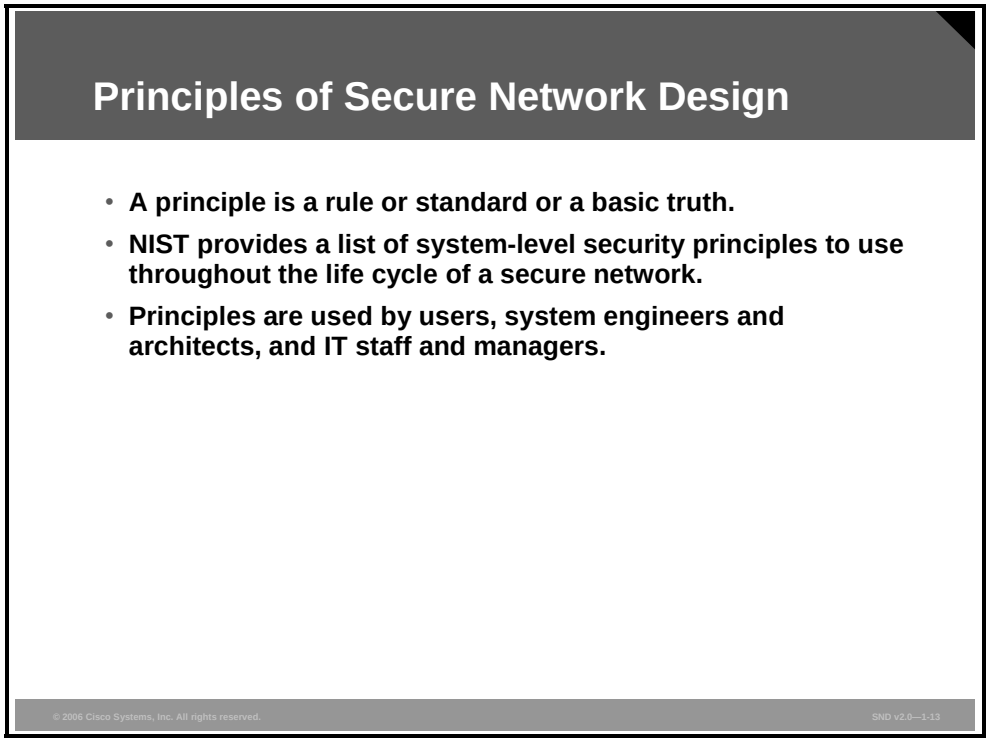
- You can move information to another system, archive it, discard it, or destroy it. When you archive information, consider how to retrieve it in the future. The media and storage technologies available now may not be readily available in the future. For example, Betamax and 5 ¼-inch floppy disks are no longer used.
- You can sell, give away, or discard hardware and software. Sanitize or destroy hard disks and other media before disposal. Review software licenses before disposal.
- Ensure that the encryption keys for encrypted data are securely stored and readily available in case you need to retrieve archived material.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Principles of Secure Network Design

This topic describes system-level security principles that you consider throughout the life cycle of a secure network.




The National Institute of Standards and Technology (NIST) compiled a set of engineering principles for network security to aid in designing a secure information system. These principles provide a foundation for a consistent and structured approach to the design, development, and implementation of network security capability.

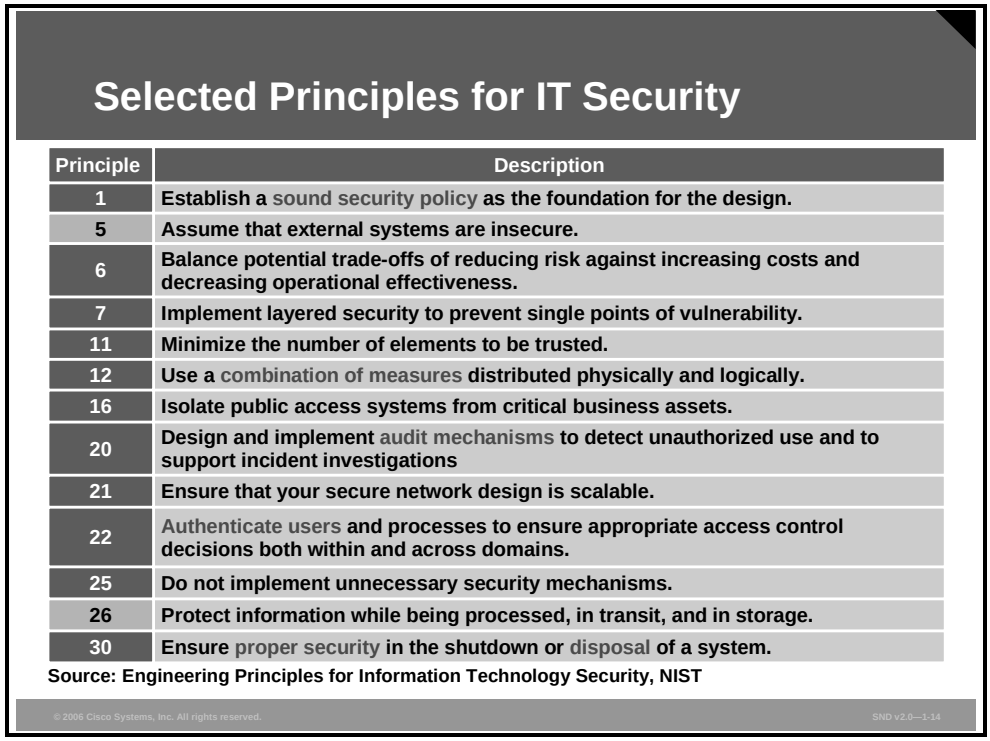
Ideally, network designers apply these principles from the planning phase of any program, or at least during the design phase. However, they are also useful in affirming and confirming the security posture of existing networks and the late development of life-cycle management policies.

Different people use the principles for different reasons as follows:

- **Users:** When developing and evaluating functional requirements or when operating networks within their organizations
- **System engineers and architects:** When designing, implementing, or modifying a network
- **Network specialists:** During all phases of the system life cycle
- **Program managers and security officers:** To ensure that they have implemented adequate security measures for all phases of the system life cycle


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Here are the 33 principles:

- **Principle 1—Establish a sound security policy as the foundation for the design:** The security policy represents the information security commitment of the organization. Leadership and management apply the security policy to all aspects of the system design solution. The policy identifies security goals that the network must support, such as confidentiality, integrity, availability, accountability, and assurance. These goals guide the procedures, standards, and controls used in the design of the security architecture. The policy also defines critical assets, the threat, and security-related roles and responsibilities.
- **Principle 2—Treat security as an integral part of the overall system design:** Network designers must include security in their design from the outset. It is difficult to implement security measures properly and successfully after system development. Designers must integrate security fully into the system life-cycle process. This process includes establishing security policies, identifying the resulting security requirements, participating in the evaluation of security products, and, finally, in the engineering, design, implementation, operation, and optimization of the system.
- **Principle 3—Delineate the physical and logical security boundaries governed by associated security policies:** Information technology exists in physical and logical locations, and boundaries exist between these locations. Designers need to know what to protect from external factors to ensure application of adequate protective measures where they will be most effective. Sometimes people, information, and information technology (IT) associated with one physical location define the boundary. Other times, the security policy defines a boundary that governs a specific set of information and IT that can cross physical boundaries. A further complication exists when a single machine or server may house both public access and sensitive unclassified information. As a result, multiple security policies may apply to a single machine or within a single system.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Principle 4—Reduce risk to an acceptable level:** Risk is the probability that a particular threat source will exploit or trigger system vulnerability. In the past, total risk avoidance was a common design goal. However, elimination of all risks is no longer cost-effective. Designers now conduct a cost-benefit analysis to determine an acceptable level of risk.
- **Principle 5—Assume that external systems are insecure:** The term "information domain" arises from the practice of partitioning information resources according to access control, need, and levels of protection required. An external domain is one that is not under your control. In general, consider external systems as being insecure. Until system engineers, architects, and IT specialists deem an external domain to be "trusted," you should presume that the security measures of an external system are different from those of a trusted internal system and then design the system security features accordingly.
- **Principle 6—Balance potential trade-offs of reducing risk against increasing costs and decreasing operational effectiveness:** A systems designer, architect, or security practitioner must identify and address all competing operational needs to meet the security requirements of the corporate security policy. It may be necessary to modify or adjust security goals to find a balance with other operational requirements. In modifying or adjusting security goals, an acceptance of greater risk and cost may be inevitable. By identifying and addressing these trade-offs as early as possible, decision makers have greater latitude and are able to achieve systems that are more effective.
- **Principle 7—Implement layered security to prevent single points of vulnerability:** A layered approach protects against specific threats and reduces overall vulnerability. For example, using a packet filtering router in conjunction with an application gateway and an intrusion detection system (IDS) increase the work that an attacker must expend to attack the system successfully. Adding good password controls and adequate user training also improves the security posture of the system.
- **Principle 8—Tailor your security measures to meet your organizational security goals:** Designers should tailor security designs to the unique needs of the organization or business. The fundamental consideration is to protect the business from the negative effects of an attack. Security needs vary from business to business and from department to department within the business. This variation means that trust levels also vary, and system designers and security practitioners must consider the level of trust when connecting to other external networks and internal subdomains. A tailored approach to each system allows designers to implement lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only in the most critical areas.
- **Principle 9—Keep it simple:** The more complex the mechanism, the more likely that it may possess exploitable flaws. Simple mechanisms tend to have fewer exploitable flaws and require less maintenance. Also, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.
- **Principle 10—Design and operate the network to resist and recover:** Information systems should be resistant to attack, should limit damage, and should recover rapidly when attacks do occur. This principle recognizes the need for adequate protection technologies in all three areas to ensure that you can counter any potential cyber attack effectively. There are vulnerabilities that you cannot fix, vulnerabilities that you have not fixed yet, vulnerabilities that you do not know about, and vulnerabilities that you could fix but have not fixed. An example of the latter might be risky services allowed through firewalls to allow increased operational capabilities. In addition to achieving a secure initial state, secure systems should have a well-defined status after failure, either to a secure failure state or via a recovery procedure to a known secure state. Organizations should establish detect-and-respond capabilities, manage single points of failure in their systems, and implement a reporting strategy.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Principle 11—Minimize the number of elements to be trusted:** Security measures include people, operations, and technology. Where technology is used, hardware, firmware, and software should be designed and implemented so that a minimum number of system elements need to be trusted to maintain protection. Further, to ensure cost-effective and timely certification of system security features, it is important to minimize the amount of software and hardware expected to provide the most secure functions for the system.
- **Principle 12—Use a combination of measures distributed physically and logically:** Often, a single security service cooperating with network components existing on separate machines provide a single security service. For example, network components ranging from the user interface on a workstation, through the network hardware and software components, to an application on an authentication server often cooperate to provide system authentication. It is important to associate all elements with the security service that they provide. Designers share these components across systems to achieve security because infrastructure resources come under more senior budget and operational control.
- **Principle 13—Assure users that the system will always be resilient:** Assurance comes from the confidence that a system meets its security expectations. In summary, these expectations provide sufficient resistance to both direct penetration and attempts to circumvent security controls. Knowing the threat environment, evaluating network performance requirements, mastering hardware and software engineering disciplines, and evaluating products and systems are primary measures used to achieve this assurance.
- **Principle 14—Limit or contain vulnerabilities:** Design systems to limit or contain vulnerabilities to allow other information system elements to function properly. Limiting and containing insecurities also helps to focus response and reconstitution efforts to information system areas most in need.
- **Principle 15—Attend to overlapping information domains:** An efficient and effective security capability can enforce multiple security policies to protect multiple information domains without needing physical separation. This principle argues for moving away from the traditional practice of creating separate LANs and infrastructures for various sensitivity levels and moving toward solutions to enable the use of common, shared, public infrastructures with appropriate protections at the operating system, application, and workstation level.
- **Principle 16—Isolate public access systems from critical business assets:** Design trends favoring shared infrastructure are not universally applicable. In cases where the sensitivity or criticality of the information is high, businesses may want to limit the number of systems on which that data is stored through physical or logical separation.
  - — Physical isolation may include ensuring that no physical connection exists between the public access information resources of the organization and critical information of the organization.
  - — Logical isolation may include layers of security services and mechanisms between public systems and secure systems responsible for protecting mission-critical resources.

  Security layers may include using network architecture designs such as demilitarized zones (DMZs) and screened subnets. Finally, system designers and administrators should enforce organizational security policies and procedures regarding the use of public access systems.
- **Principle 17—Separate computing systems and network infrastructure:** To control the flow of information and access across network boundaries in computing and communications infrastructures, and to enforce the proper separation of user groups, a suite of access control devices and accompanying access control policies should be used.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

To determine which communications you need across the network boundaries, ask these questions:

- What external interfaces are required?
- Is information being pushed or pulled?
- What ports, protocols, and network services are required?
- What do system information exchanges need? (For example, trust relationships, database replication services, and domain name resolution processes)

- **Principle 18—Base security on open standards for portability and interoperability:** Most businesses depend on distributed information systems that distribute information across their own organization and to customers, suppliers, and others. Security program designers must, therefore, incorporate interoperability and portability into all hardware, software, and implementation practices.
- **Principle 19—Use common language:** Use a common language when developing security requirements to allow people to evaluate and compare security policies, products, and features more efficiently. This commonality provides a level of confidence that helps ensure that product security functions conform to the security requirements of the company.
- **Principle 20—Design and implement audit mechanisms to detect unauthorized use and to support incident investigations:** Organizations should monitor, record, and periodically review audit logs to identify unauthorized use and to ensure that system resources are functioning properly. In some cases, organizations may be required to disclose information obtained through auditing mechanisms to appropriate third parties, including law enforcement authorities or U.S. Freedom of Information Act (FOIA) applicants. Many organizations have implemented consent to monitor policies, which state that evidence of unauthorized use (for example, audit trails) may be used to support administrative or criminal investigations.
- **Principle 21—Ensure that your secure network design is scalable:** You need to adapt your security requirements and technical protection methods to meet changing business needs. Your design must include periodic assessments over the system life cycle to allow system administrators and managers to make informed decisions and risk assessments. Consistent security solution re-evaluation and reaction to changing and evolving vulnerabilities reinforces trust and reduces risk. The ability to migrate every security feature to new and more effective technologies is a defining and important design goal. Modular designs are more flexible in this regard. Also, consider that technology migration affects build-or-buy decisions.
- **Principle 22—Authenticate users and processes to ensure appropriate access control decisions both within and across domains:** Authentication is the process whereby a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action. It is essential to ensure that authentication is adequate to implement security policies and achieve security goals. Also consider that the level of trust is always an issue in cross-domain transactions.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Principle 23—Use unique identities to ensure accountability:** An identity may represent an actual user or a process with its own identity (for example, a program making a remote access). Unique identities are a required element because they provide these accountability features:
  - Maintain accountability and traceability of a user or process
  - Assign specific rights to an individual user or process
  - Provide for nonrepudiation
  - Enforce access control decisions
  - Establish the identity of a peer in a secure communications path
  - Prevent unauthorized users from masquerading as authorized users
- **Principle 24—Implement least privilege:** The concept of least privilege aims to provide no more authorizations than necessary to perform required functions. System administrators use least privilege regularly. Consider privilege levels in Cisco IOS software as an example. A recommended network security practice is to have several administrators with limited access to security resources rather than having one person with super user permissions.

  Use role-based access controls for functions other than system administration. The system security policy should identify and define user and process roles so that security designers can assign permissions specific to the function of that role.
- **Principle 25—Do not implement unnecessary security mechanisms:** Every security mechanism must support a required security service or set of services. Every security service should support one or more security goals. Do not implement any measures that do not support a recognized service or security goal. Such implementations may lead to unneeded complexity and are potential sources of vulnerability.
- **Principle 26—Protect information while being processed, in transit, and in storage:** The risks of unauthorized modification or destruction of data, disclosure of information in storage or being processed, and denial of access to data while in transit, are risks that need consideration. Security designs must, therefore, preserve the integrity, confidentiality, and availability of data, including application software.
- **Principle 27—Make the security system easy to use:** The more difficult it is to maintain and to operate, the less effective a security mechanism becomes. Ease of use is an important design consideration. Training and training costs must be included in design estimates.
- **Principle 28—Develop and exercise contingency and disaster recovery plans:** Business and operational continuity is a key business driver. Businesses must recover from disasters or prolonged service interruptions. Complete network security designs include roles, responsibilities, and procedures for emergency response, recovery, and return to normal operations. Companies should exercise and review such plans on a regular basis.
- **Principle 29—Consider custom products to achieve adequate security:** Standard solutions do not always meet your requirements. Designers can choose to augment such products or build their own solutions.
- **Principle 30—Ensure proper security in the shutdown or disposal of a system:** Unauthorized users may be able to retrieve sensitive information that resides on inactive systems or on systems sent for disposal. Procedures must be implemented to ensure that system hard drives, volatile memory, and other media are purged to an acceptable level and so that they do not retain residual information.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Principle 31—Protect against all likely classes of attack:** Security designers must consider multiple classes of attack and mitigate all unacceptable risks.
- **Principle 32—Identify and prevent common errors and vulnerabilities:** Many errors reoccur with disturbing regularity. These errors include buffer overflows, race conditions, format string errors, failing to check input for validity, and programs having more privileges than they need. Learn from the past to improve future results.
- **Principle 33—Train developers to develop secure software:** It is unwise to assume that developers know how to develop secure software. Companies must train developers to develop secure software.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- **Building secure networks requires proactive thought and action to deal with unforeseen security issues after the network is in operation.**
- **Use the PDIOO network life-cycle model to assist in secure network design. Balance business and operation needs against the provisions of security policies.**
- **The plan phase helps identify network requirements.**
- **The design phase provides the logical and physical design based on requirements gathered during the plan phase.**

© 2006 Cisco Systems, Inc. All rights reserved.


## Summary (Cont.)

- **The implement phase builds the network and verifies the design.**
- **The operate phase is the final test of the effectiveness of the design and provides input into the optimize phase of the network life cycle.**
- **The optimize phase uses proactive network management techniques to identify and resolve problems before network disruptions arise.**
- **Final disposal of network components is an activity that needs attention from the very beginning of the network life cycle.**
- **NIST engineering principles for network security aid in designing a secure information system.**

© 2006 Cisco Systems, Inc. All rights reserved.




*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 5

# Developing a Comprehensive Security Policy

## Overview

This lesson is based on open-source materials available from industry and government sources. Key documents are listed in the References section of the Module Summary, and you are encouraged to review those documents as part of your continuing professional development effort.

It is important to know that the security policy developed in any organization drives all the steps taken to secure network resources. The development of a comprehensive security policy prepares you for the rest of this course.

## Objectives

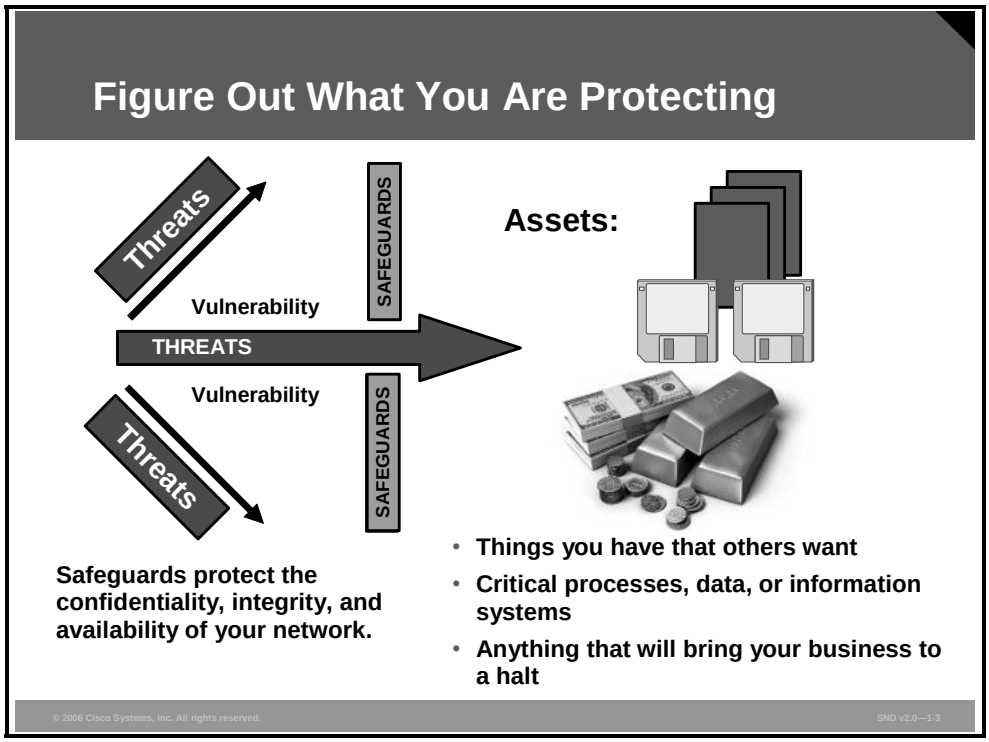
Upon completing this lesson, you will be able to explain how to meet the security needs of a typical enterprise with a comprehensive security policy. This ability includes being able to meet these objectives:

- Explain the goals of a security policy
- Describe the essential functions of a security policy
- Describe the components of a comprehensive security policy
- Describe the process of developing a security policy within a typical corporate environment
- Describe the activities included in the plan phase of a security policy life cycle
- Describe the activities included in the design phase of a security policy life cycle
- Describe the activities included in the implement phase of a security policy life cycle
- Describe the activities included in the operate phase of a security policy life cycle
- Describe the activities included in the optimize phase of a security policy life cycle
- Describe the general characteristics of an effective security policy

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Why Do You Need a Security Policy?

This topic explains the goals of a security policy.




Every organization has something that someone else wants. Someone may want that something for themselves, or they may want the satisfaction of denying something to its rightful owner. Your assets are what need the protection of a security policy.

Consider your assets by asking these questions:

- What do you have that others want?
- What processes, data, or information systems are critical to you, your company, or your organization?
- What would stop your company from doing business or your organization from fulfilling its mission?

The answers identify assets ranging from critical databases, vital applications, vital company customer and employee information, classified commercial information, shared drives, e-mail servers, and web servers.

## Confidentiality, Integrity, and Availability

Your security policy has three goals: confidentiality, integrity, and availability.

- **Confidentiality:** Confidentiality refers to limiting information disclosure to authorized users and preventing access by or disclosure to unauthorized users. Authentication methods that identify systems users, and access control mechanisms that limit use by each user, underpin the goal of confidentiality. Security specialists classify information in increasing levels from restricted distribution to secret. Allowing such information to get into the wrong hands (even within the organization) affects operations. Confidential information is information that should remain private to the company and that should be available only to certain employees within the company.

 © 2006 Cisco Systems, Inc.

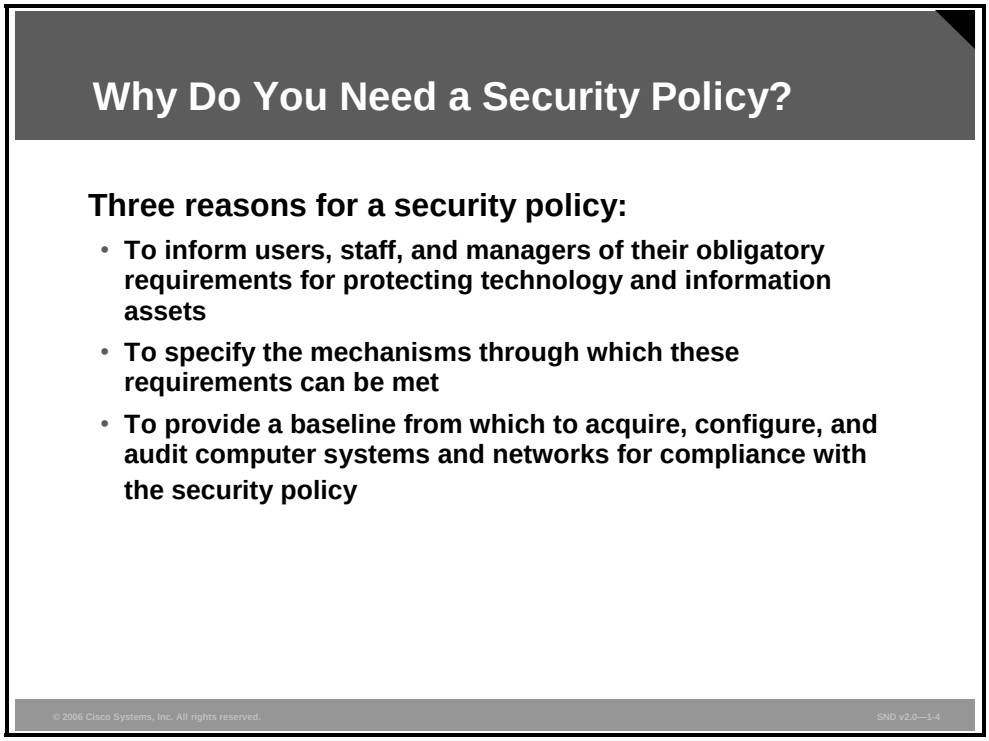
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Integrity:** Integrity refers to the trustworthiness of information resources. Integrity includes the concept of “data integrity,” which means that data have not been changed inappropriately, whether by accident or by deliberate activity. Integrity also includes “origin,” or “source integrity,” which means that the data actually came from the person or entity you think it did, rather than from an imposter. Users must keep information accurate and up to date, but more importantly, information must be protected to prevent unauthorized people or agencies from tampering with it.
- **Availability:** Availability refers to the accessibility of company information and resources. It is vital that company information and resources be readily available to those who need it. In most cases, the unavailability of information is a severe business concern.

Efforts to assure confidentiality, integrity, and availability are focused on prevention or detection. In all cases, appropriate or adequate levels of confidentiality, integrity, and availability depend on the context. Context also applies to balancing prevention and detection. The nature of the business activities that the information systems support, the risks to those activities, and the business standards applied to those activities all contribute to how your security policy will achieve the goals of confidentiality, integrity, and availability in your organization.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




A security policy is a set of objectives for the company, rules of behavior for users and administrators, and requirements for system and management that collectively ensure the security of network and computer systems in an organization. A security policy is a "living document," meaning that the document is never finished and is continuously updated as technology and employee requirements change.

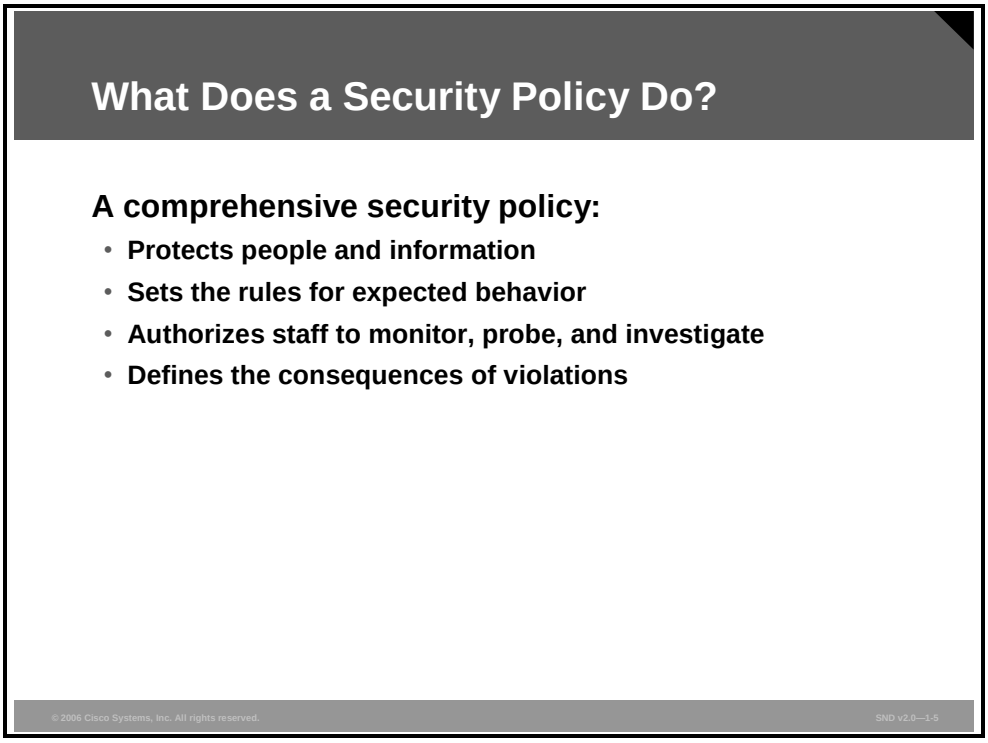
The security policy translates, clarifies, and communicates the management position on security as defined in high-level security principles. The security policies act as a bridge between these management objectives and specific security requirements. The security policy informs users, staff, and managers of their obligatory requirements for protecting technology and information assets. The security policy should specify the mechanisms needed to meet these requirements. Another purpose is to provide a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the security policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# What Does a Security Policy Do and Who Uses It?

This topic describes the essential functions of a security policy.

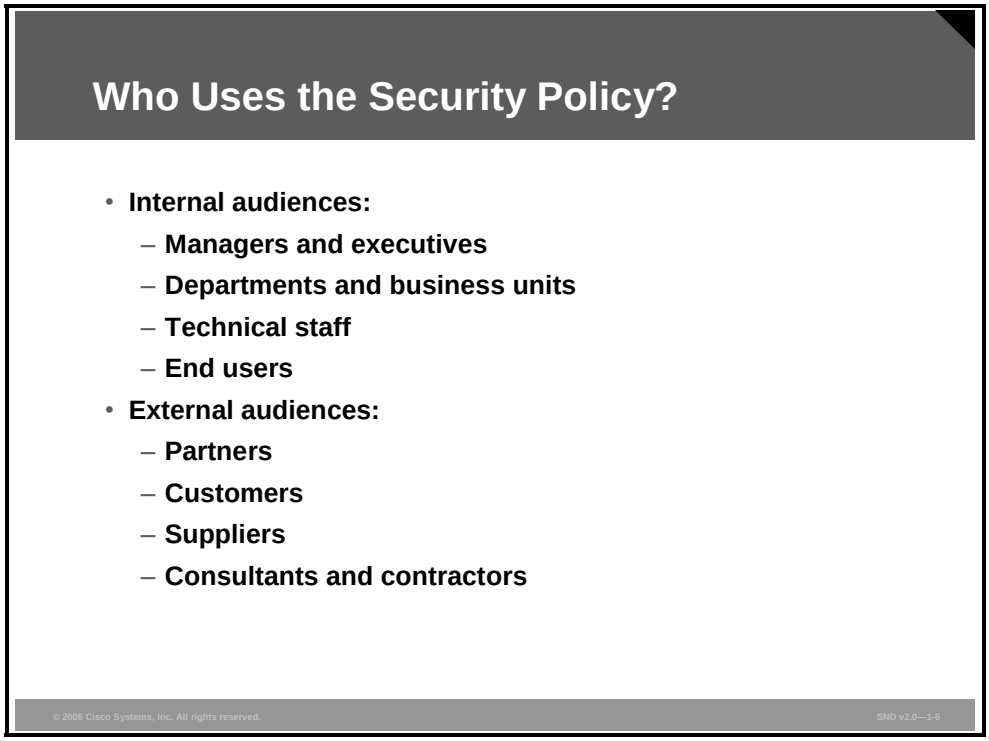



A comprehensive security policy fulfills these essential functions:

- Protects people and information
- Sets the rules for expected behavior by users, system administrators, management, and security personnel
- Authorizes security personnel to monitor, probe, and investigate
- Defines and authorizes the consequences of violations



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The audience for the security policy should be anyone including employees, contractors, suppliers, or customers who may have access to your network. The security policy should treat each of these groups differently.

The audience determines the content of the policy. For example, you probably do not need to include a description of *why* something is necessary in a policy that is intended for the technical staff. You can assume that the technical staff already knows why a particular requirement is included. Managers are also not likely to be interested in the technical aspects of why a particular requirement is required; they may want the high-level overview or the principle supporting the requirement. However, when end users know why a particular security control has been included, they are more likely to comply with the policy.

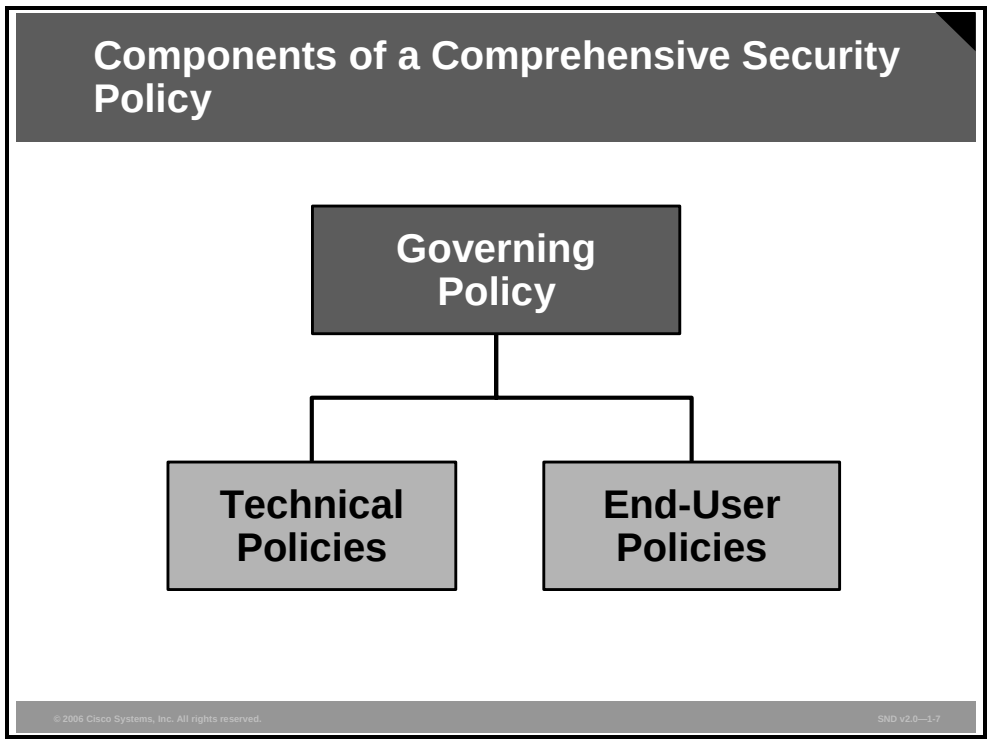
One document is not likely to meet the needs of the entire audience of a large organization. The goal is to ensure that the information security policy documents are coherent with audience needs.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Components of a Comprehensive Security Policy

This topic describes the components of a comprehensive a security policy.



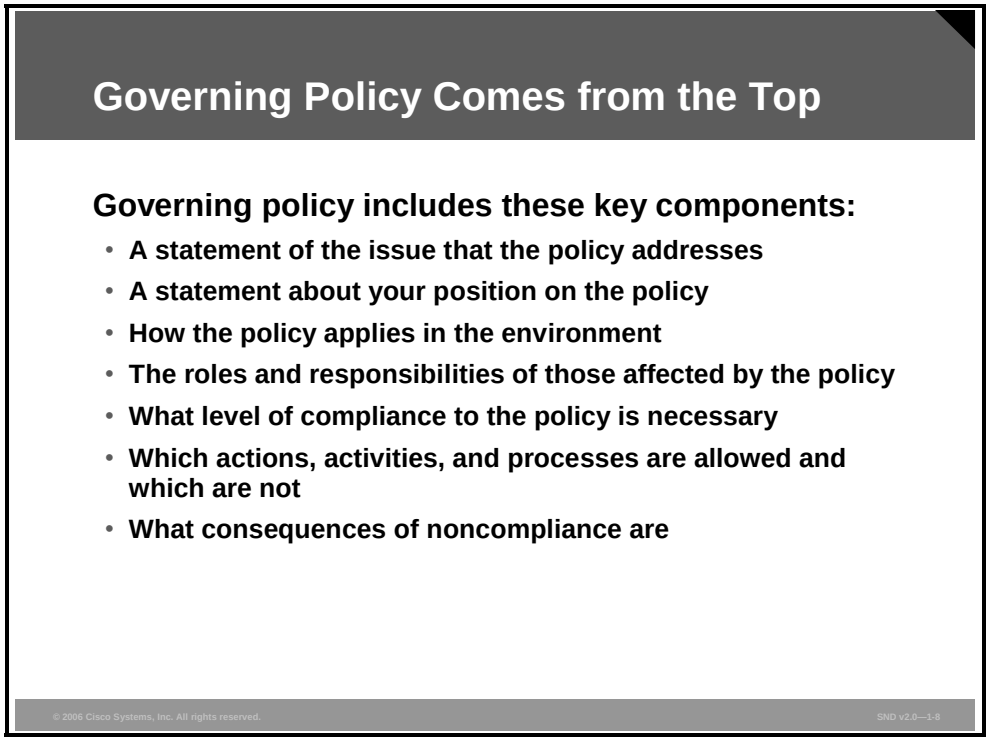

The figure shows the hierarchy of a corporate policy structure aimed at effectively meeting the needs of all audiences. Most corporations should use a suite of policy documents to meet their wide and varied needs.

- **Governing policy:** This policy is a high-level treatment of security concepts that are important to the company. Managers and technical custodians are the intended audience. The governing policy controls all security-related interaction among business units and supporting departments in the company. In terms of detail, the governing policy answers the "what" security policy questions.
- **Technical policies:** Security staff members use technical policies as they carry out their security responsibilities for the system. These policies are more detailed than the governing policy and are system- or issue-specific (for example, access control or physical security issues). In terms of detail, technical policies answer the "what," the "who," the "when," and the "where" security policy questions.
- **End-user policies:** This document covers all security topics important to end users. In terms of detail level, end-user policies answer the "what," "who," "when," and "where" security policy questions at an appropriate level of detail.

Most of the discussion in this course will focus on the specific needs met by technical policies.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The governing policy outlines the security concepts that are important to the company for managers and technical custodians.

- The governing policy controls all security-related interactions among business units and supporting departments in the company.
- The governing policy aligns closely with existing company policies, especially human resource policies, but also any other policy that mentions security-related issues such as e-mail, computer use, or related information technology (IT) subjects.
- The governing policy is placed at the same level as all company-wide policies.
- The governing policy supports the technical and end-user policies.

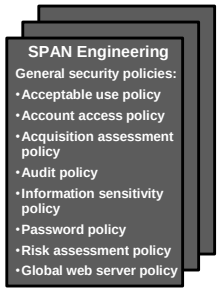
The figure lists the key components of the governing policy.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Technical and User Policies

- **Categories of technical policies describe the duties of the security staff in specified technical areas:**
  - **General policies**
  - **E-mail policies**
  - **Remote access policies**
  - **Telephony policies**
  - **Application policies**
  - **Network policies**
  - **DMZ policies**
  - **Lab policies**
- **User policies detail specific duties and responsibilities for end users.**



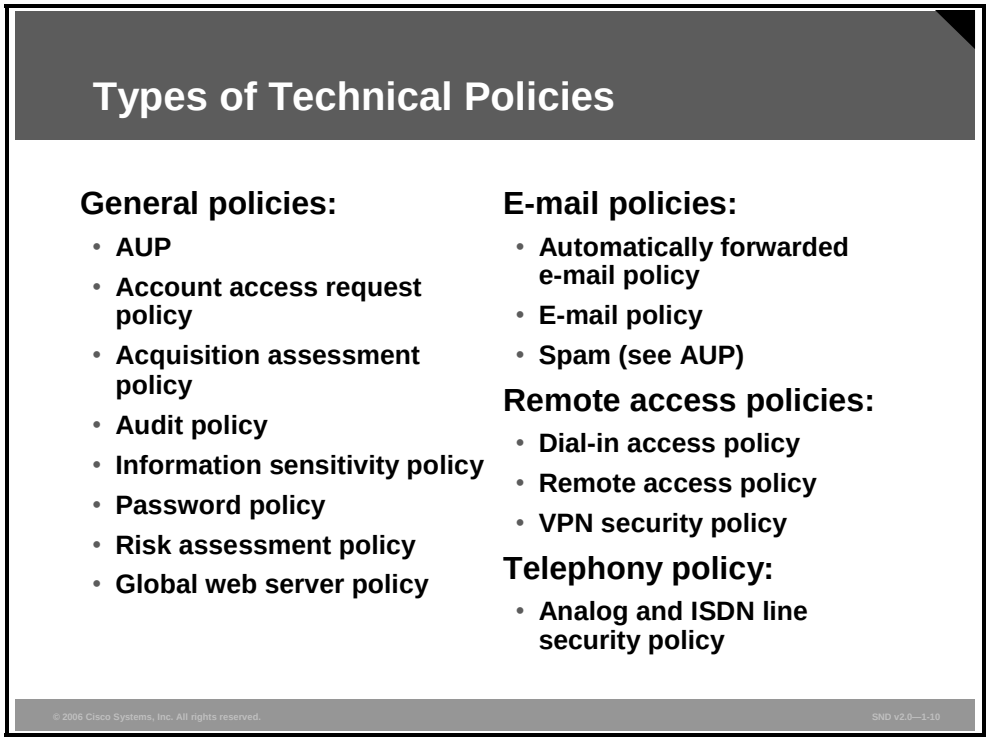

© 2006 Cisco Systems, Inc. All rights reserved.


Security staff members use the technical policies in the conduct of their daily security responsibilities. These policies are more detailed than the governing policy and are system- or issue-specific (for example, router security or physical security issues). These policies are essentially security handbooks that describe what the security staff does, but not how the security staff performs its functions.

The end-user policy is a single policy document that covers all the policy topics pertaining to information security that end users should know about, comply with, and implement. This policy may overlap with the technical policies and is at the same level as a technical policy. Grouping all end-user policies together means that users have to go only to one place and read one document to learn everything that they need to do to ensure compliance with the company security policy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The figure shows some of the security policies used by Cisco Systems. The SANS Institute (http://www.sans.org) lists similar policies and provides many templates for these policies that you can adopt for your own organizational requirements. Not all organizations need all of these policies. One of your first tasks will be to select and adopt these policies templates as applicable:

- **Here is a list of** general policies:
  - **Acceptable use policy (AUP):** Defines the acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization corporate resources and proprietary information
  - **Account access request policy:** Formalizes the account and access request process within the organization (Users and system administrators who bypass the standard processes for account and access requests can lead to legal action against the organization.)
  - **Acquisition assessment policy:** Defines the responsibilities regarding corporate acquisitions and defines the minimum requirements of an acquisition assessment that the information security group must complete
  - **Audit policy:** Conducts audits and risk assessments to ensure integrity of information and resources, investigates incidents, ensures conformance to security policies, or monitors user and system activity where appropriate
  - **Information sensitivity policy:** Defines the requirements for classifying and securing information in a manner appropriate to its sensitivity level
  - **Password policy:** Defines the standards for creating, protecting, and changing strong passwords
  - **Risk assessment policy:** Defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the information infrastructure associated with conducting business
  - **Global web server policy:** Defines the standards required by all web hosts

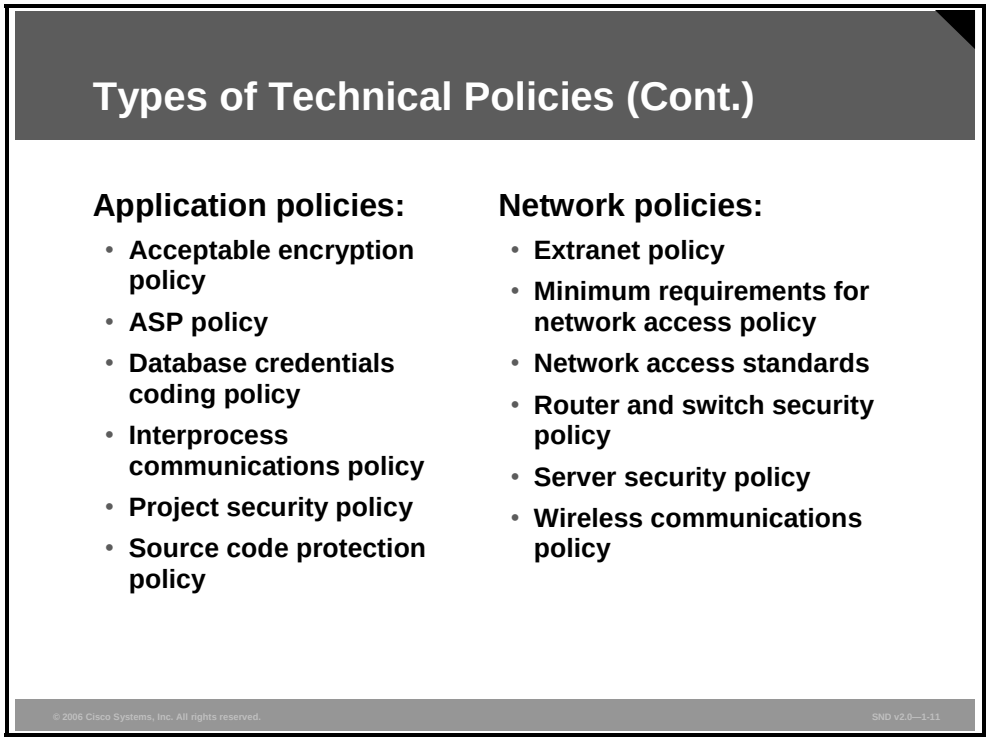

© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Here is a list of e-mail policies:
  - **Automatically forwarded e-mail policy:** Documents the policy restricting automatic e-mail forwarding to an external destination without prior approval from the appropriate manager or director
  - **E-mail policy:** Defines the standards to prevent tarnishing the public image of the organization
  - **Spam policy:** (Spam is covered in the AUP.)
- Here is a list of remote access policies:
  - **Dial-in access policy:** Defines the appropriate dial-in access and its use by authorized personnel
  - **Remote access policy:** Defines the standards for connecting to the organization network from any host or network external to the organization
  - **Virtual private network (VPN) security policy:** Defines the requirements for remote access IPsec or Layer 2 Tunneling Protocol (L2TP) VPN connections to the organization network
- Here is a type of telephony policy:
  - **Analog and ISDN line policy:** Defines the standards for use of analog and ISDN lines for sending and receiving faxes and for connection to computers



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




These policy templates will also need to be selected and adopted:

- **Application policies:** There is a wide range of application policies. Here are some of the listings:
  - **Acceptable encryption policy:** Defines the requirements for encryption algorithms used within the organization
  - **Application service provider (ASP) policy:** Defines the minimum security criteria that an ASP must execute before the organization uses them on a project
  - **Database credentials coding policy:** Defines the requirements for securely storing and retrieving database usernames and passwords
  - **Interprocess communications policy:** Defines the security requirements that any two or more processes must meet when they communicate with each other using a network socket or operating system socket
  - **Project security policy:** Defines requirements for project managers to review all projects for possible security requirements
  - **Source code protection policy:** Establishes minimum information security requirements for managing product source code
- **Network policies: There are many network policies as well. Here are some of the listings:**
  - **Extranet policy:** Defines the requirement that third-party organizations requiring access to the organization networks must sign a third-party connection agreement
  - **Minimum requirements for network access policy:** Defines the standards and requirements for any device requiring connectivity to the internal network
  - **Network access standards:** Defines the standards for secure physical port access for all wired and wireless network data ports

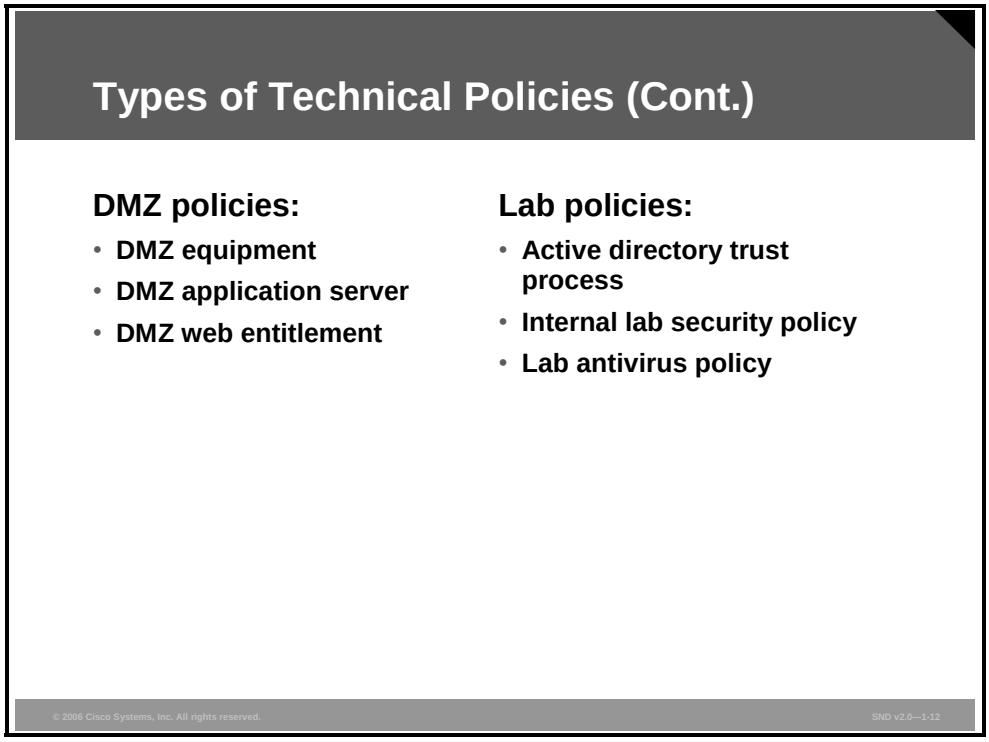
 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Router and switch security policy:** Defines the standards for minimal security configuration for routers and switches inside a company production network or used in a production capacity
- **Server security policy:** Defines the standards for minimal security configuration for servers inside a company production network or used in a production capacity
- **Wireless communication policy:** Defines standards for wireless systems used to connect to the organization networks



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




These policy templates will also need to be selected and adopted.

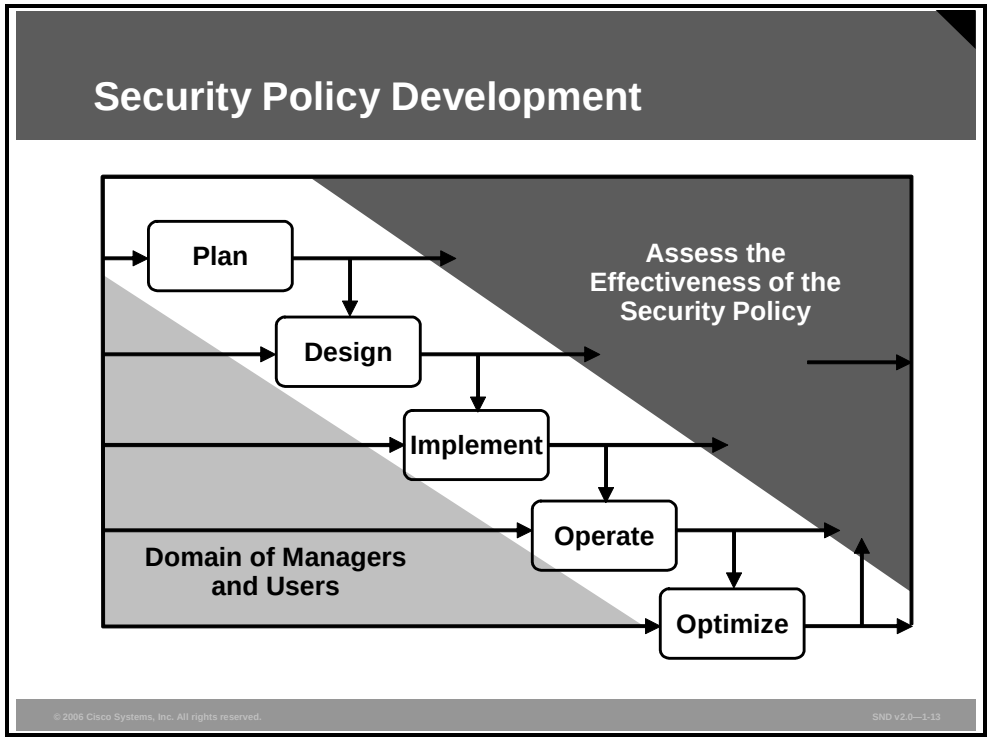
- Here is a list of demilitarized zone (DMZ) policies:
  - **DMZ equipment:** Defines the standards that all equipment in the organization in the DMZ must meet
  - **DMZ application server:** Defines the standards required that all application servers in the organization in the DMZ must meet
  - **DMZ web entitlement:** Defines the minimum authentication standards required by all applications that run on any web infrastructure in the organization in the DMZ must meet
- Here is a list of lab policies:
  - **Active directory trust process:** Defines the process used to grant a security trust with the production active directory
  - **Internal lab security policy:** Defines the requirements for internal labs to ensure that lab use does not compromise confidential information and technologies and that lab activities do not compromise production services and the interests of the organization
  - **Lab antivirus policy:** Defines the requirements that all computers connected to the organization lab networks must meet to ensure effective virus detection and prevention


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Developing a Security Policy Using the PDIOO Model

Developing a security policy is a major undertaking, and you should approach it in the same way as you would any major project. This topic describes the process of developing a security policy within a typical corporate environment.



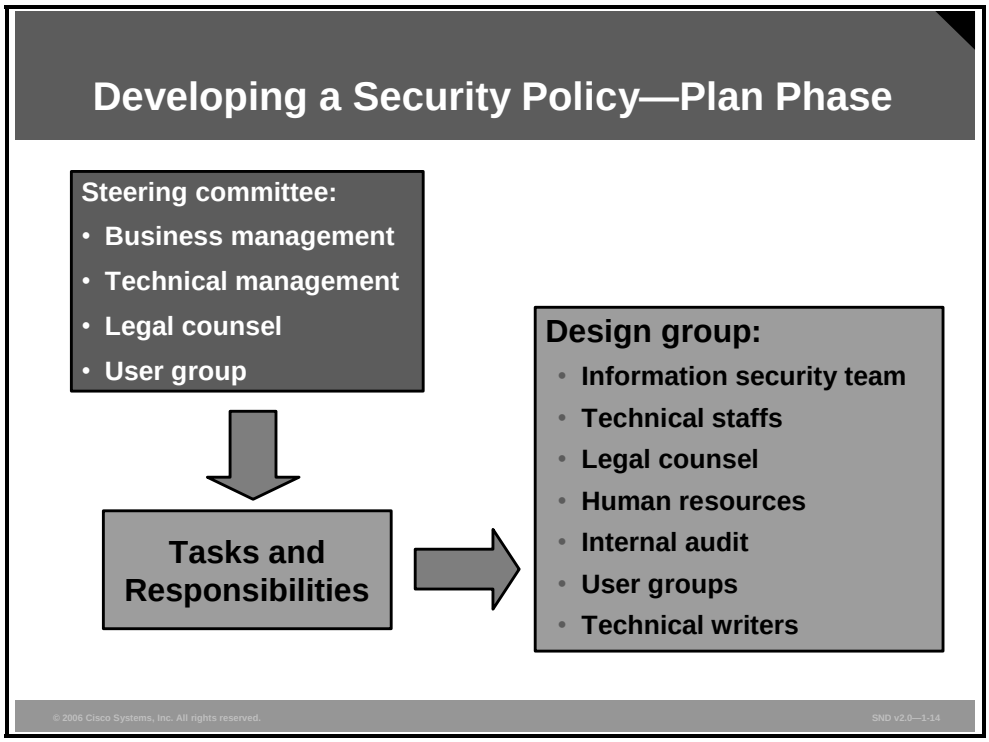

There are many references describing the way to build an effective security policy. A good approach is to use the planning, designing, implementing, operating, and optimizing (PDIOO) methodology.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Developing a Security Policy—Plan Phase

This topic describes the activities included in the plan phase of a security policy life cycle.




The goal of the plan phase is to assemble a team and assign tasks. An appropriate and effective security policy needs the acceptance and support of all employees in the organization. At the top, corporate management must give full support to the policy process or the policy will have little chance of being effective.

Companies should follow a formal policy design process for the development of all security policies. After the need for a security policy is identified, it is important to determine, at an early stage, who is going to be involved in the actual design and implement phases of the policy. Company leadership should form a steering group. Ideally, steering group members are the same company officers who own and enforce the policy in the long term. The steering group outlines these specifications:

- The members who will develop the initial draft of the policies
- The groups that will review each policy
- The approval process for each policy
- The implementation process for each policy

Ideally, the steering committee develops a governing policy to guide further effort. The steering group should include these individuals:

- A senior-level administrator to represent company concerns regarding protecting information and the associated cost of developing and implementing the policy
- A member of management to implement, manage, and enforce the policy
- A representative from the legal staff to ensure that policies do not infringe on privacy laws
- A representative from the internal audit staff to protect the company reputation and ensure responsibility to the company clients, customers, and employees

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- A representative from the user community (because policies affect users the most)

The size of the policy design group depends on the size and scope of the policy. The policy design group will include members from some of or all of these categories:

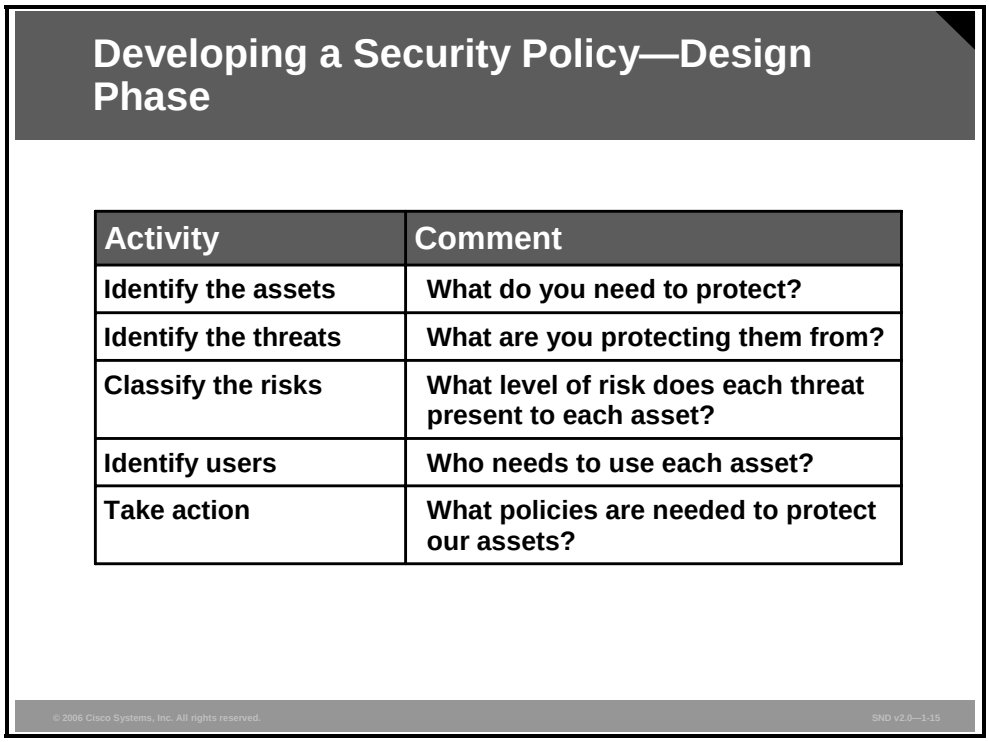
- **Information security team:** Management assigns overall responsibility for developing the policy documents to a team from this group. Management may give one person overall control with others in a supporting role. This team guides each policy document through development and revision.
- **Technical staffs:** In addition to staff on the security team, you may need to call upon the expertise of specific technical staff with specific security and technical knowledge. These people are familiar with the day-to-day use of the technology or system that your policy covers and will help you balance what is good security with what is feasible for business.
- **Legal counsel:** Your legal department should review the policy documents after they are complete. This counsel can provide advice on current relevant legislation and contractual agreements requiring certain types of information needing protection in specific ways and on other legal issues. There may be regulatory requirements, such as line monitoring, that affect some aspects of your security policy. The creators of the security policy should consider seeking legal assistance in the creation of the policy. As a minimum, legal counsel should review all security policies.
- **Human resources:** The human resources department may need to review and approve your policy in terms of how it relates to existing company policies. If your policy touches on topics covered by existing human resources policy, including such things as e-mail use and physical security, you must ensure that both sets of policies say the same thing.
- **Internal audit:** The internal audit department will take interest in monitoring company-wide compliance with the policy after it is in force. The internal audit department should be involved in the development and review processes to ensure that the policy is enforceable in terms of their procedures and best practices.
- **User groups:** User groups can help you determine the success of your policy and whether you need to change it to make it more useable.
- **Technical writers:** An in-house technical writer is a valuable resource to help with planning your policy project, determining an appropriate style and formatting structure for your documents, and editing and proofreading your policy drafts.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Developing a Security Policy—Design Phase

This topic descries the activities included in the design phase of a security policy life cycle.

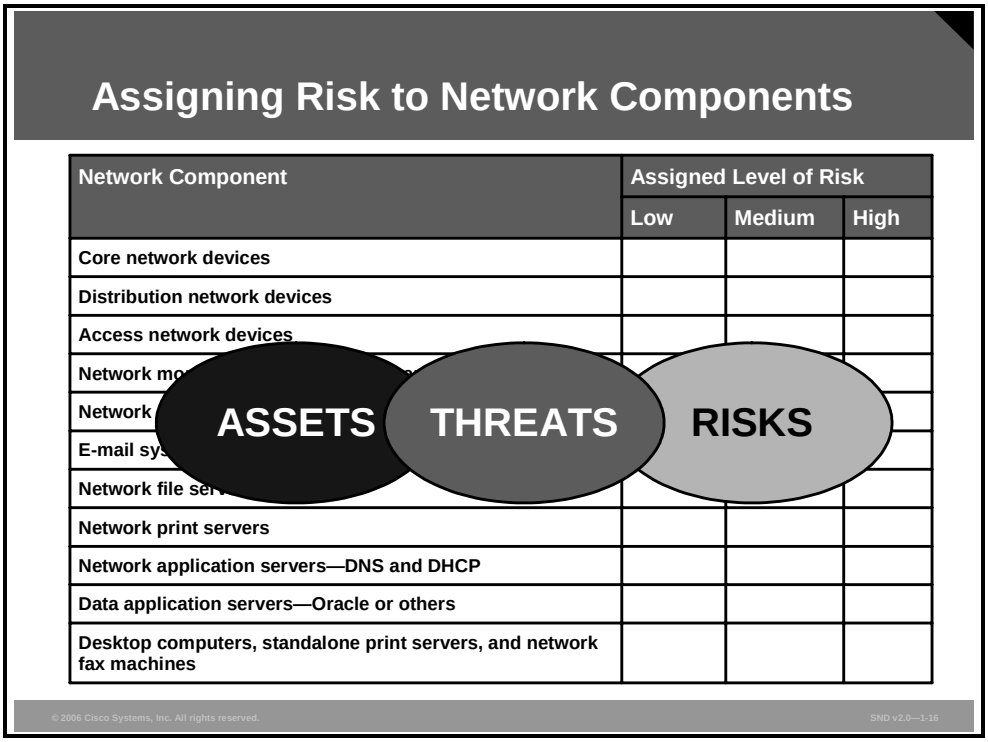



Design activities include these steps:

- Identify the assets that you are trying to protect.
- Identify the threats to those assets.
- Assess the level of risk to each asset.
- Determine who needs to use each asset.
- Draft appropriate security policies.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




An efficient security policy is one in which the effort spent on security yields cost benefits. Although most of the focus will be on network intruders, evidence and experience show that significant threat comes from within the organization. In many cases, the threat from insiders is even greater than from outside intrusion.

Risk analysis determines what you need to protect, what you need to protect it from, and how to protect it. Complete a risk analysis to identify the risks to your network, network resources, and data. This analysis does not mean that you should identify every possible entry point to the network, nor every possible means of attack. The intent of a risk analysis is to identify portions of your network, assign a threat rating to each portion, and apply an appropriate level of security. This process helps maintain a workable balance between security and required network access.

There are two elements of risk analysis that should be considered:

- **Identifying the assets:** A basic goal of your security policy is to assure the availability, confidentiality, and integrity of your assets. The first step then is to identify all of the things that you need to protect. The figure lists the network components that should be included in your analysis.
- **Identifying the threats:** Examine each threat in terms of how each threat could affect the availability, confidentiality, and integrity of each network component. Determine what potential for loss exists from each threat. Loss can come from unauthorized access to resources and information, disclosure of information, or denial of service (DoS). Recall that threats can originate from hackers, viruses, Trojan horses, and worms; DoS attacks; social engineering; inside threats; and natural disasters such as floods, tornadoes, and fire.

You can simplify matching assets to threats by assigning a level of risk to each network component. Use one of these classifications:

- **Low risk:** This classification refers to systems or data that if compromised (viewed by unauthorized personnel, corrupted, or lost) would not disrupt the business or cause legal or financial ramifications. These systems do not permit further access of other systems, and the network security staff can easily restore these systems if compromised.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Medium risk:** The medium risk classification refers to systems or data that if compromised (viewed by unauthorized personnel, corrupted, or lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore, or the restoration process is disruptive to the system.
- **High risk:** The high risk classification refers to systems or data that if compromised (viewed by unauthorized personnel, corrupted, or lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore, or the restoration process is disruptive to the business or other systems.

Network equipment such as switches, routers, Domain Name System (DNS) servers, and DHCP servers can allow further access into the network and are, therefore, either medium- or high-risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. Such a failure can be extremely disruptive to a business.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Identify Types of Users

| Type of User | Description |
|---|---|
| Administrators | Internal users responsible for network resources |
| Privileged users | Internal users with a need for greater access |
| General users | Internal users with general access |
| Partners | External users with a need to access some resources |
| Others | Access granted as required and appropriate |

© 2006 Cisco Systems, Inc. All rights reserved.


After you have assigned a risk level, it is necessary to identify the types of users of that system. The figure shows the five most common types of users.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Security Analysis Matrix

| Network Component | Description | Risk Level | Types of Users |
|---|---|---|---|
| ATM switches | Core network device | High | Administrators for device configuration (support staff only); all others for use as a transport |
| Network routers | Distribution network device | High | Administrators for device configuration (support staff only); all others for use as a transport |
| Closet switches | Access network device | Medium | Administrators for device configuration (support staff only); all others for use as a transport |
| ISDN or dial-up servers | Access network device | Medium | Administrators for device configuration (support staff only); partners and privileged users for special access |
| Firewall | Access network device | High | Administrators for device configuration (support staff only); all others for use as a transport |

© 2006 Cisco Systems, Inc. All rights reserved.


Matching risk levels and the type of access required of each network system component against the user forms the basis of the security matrix. The security matrix provides a quick reference for each system and a starting point for further security measures, such as creating an appropriate strategy for restricting access to network resources.

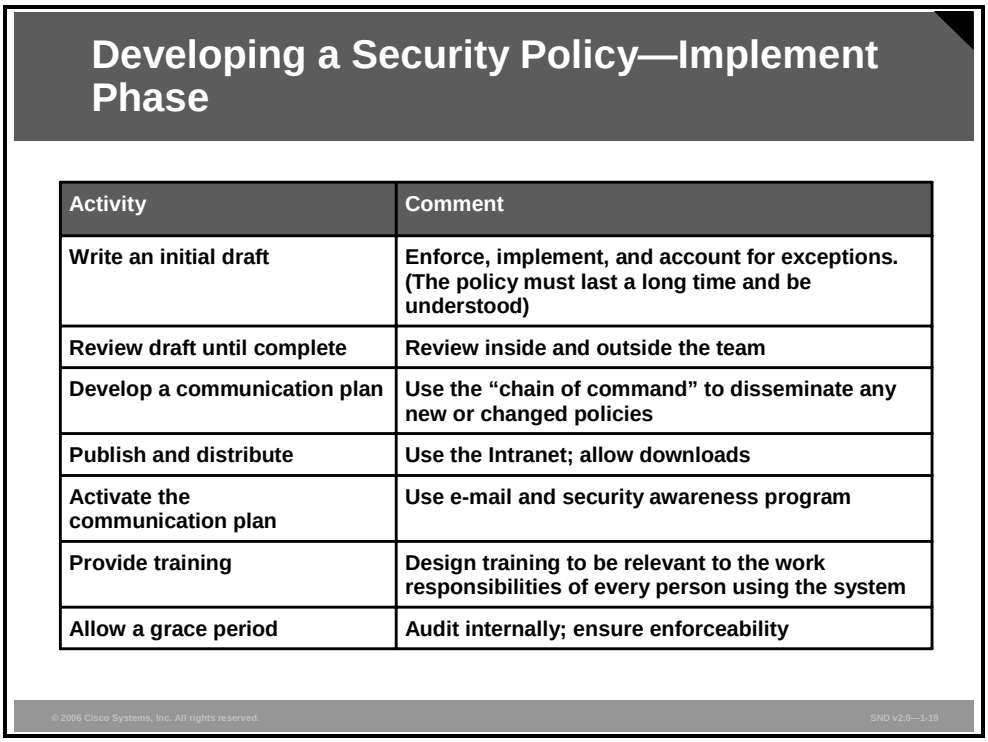
The figure shows some of the system components. Other devices and applications that you would include are DNS and DHCP servers, external e-mail servers, internal e-mail servers, and such things as Oracle databases.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Developing a Security Policy—Implement Phase

This topic describes the activities included in the implement phase of a security policy life cycle.




The implement phase moves the process from design to operations. During implementation, the team drafts, reviews, and distributes the policies and provides training to users. The implementation phase is complete when the steering committee confirms that the policies meet the requirements specified by the steering committee and gives final approval for implementation.

The implementation phase includes these activities:

- **Write the initial draft:** The team writes an initial draft of each policy. You must be able to enforce and implement each policy. You must have a mechanism to account for exceptions, and you must write the policy so that the policy will have lasting value. Everyone must understand the policy.
- **Review the draft until it is complete:** Review the initial draft inside and outside the team. The review must look at all interfaces within the system. The review must consider the people, tools, facilities, schedule, and any monetary resources required to test individual policies. The review must also ensure that all the policies work well together and do not conflict with each other. The reviews must document positive and negative results.
- **Develop a communication plan:** It is important to the success of the security policy process that you inform everyone about how policies will affect their work before you publish, distribute, and put policies into effect. Your communication plan should include management groups to help disseminate the policies in their own areas of responsibility. An effective security awareness strategy will ensure that these requirements are met:
  - Your audience is aware of the organization security policy.
  - The audience knows where to find the policy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- The audience knows how to comply with the policy.
- The audience knows the consequences of noncompliance.

A security awareness program should teach policy stakeholders about the policy and their role in maintaining it. This awareness will help make the policy an integral part of the job.

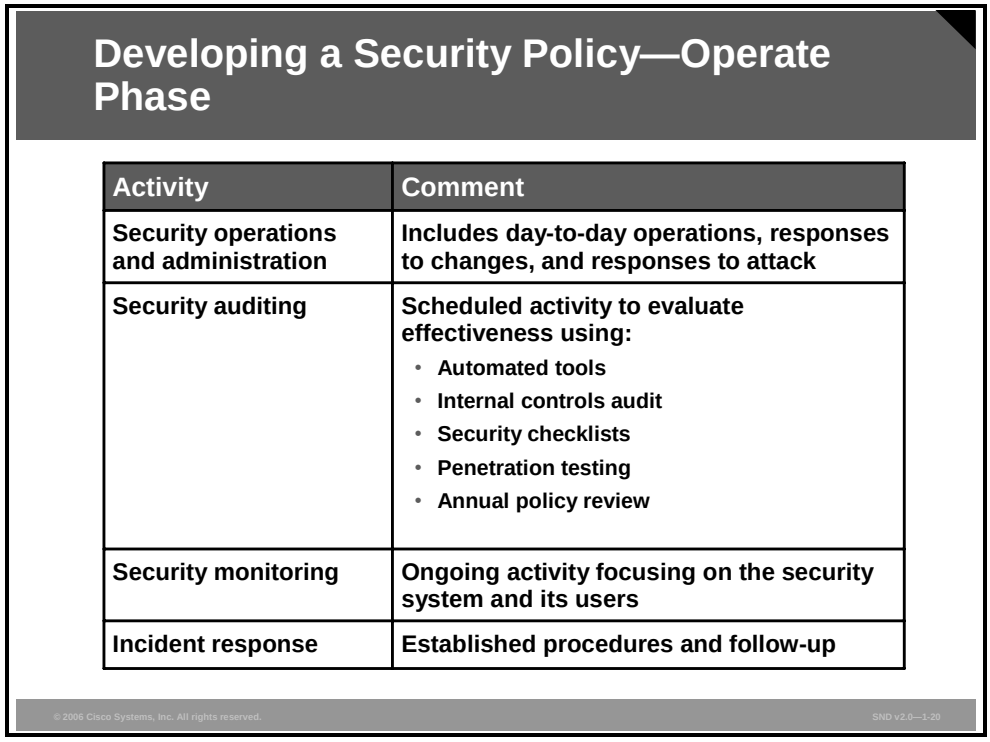
- **Publish and distribute the policies:** After you review and finalize your policies, publish and distribute them so that they are available to everyone concerned. Use your own intranet sites to make the documents accessible and available for download, printing, and saving.
- **Activate the communication plan:** Use internal e-mail to inform employees quickly and effectively about the policy and any changes to the policy. Other company communication channels, such as newsletters and the security awareness program, are also useful.
- **Provide training:** You can use the design documentation, the policies themselves, and your experience as sources of training content. Training programs should aim at performance expectations as they pertain to each user.
- **Set a grace period:** At the beginning of the design phase, the internal audit group needs to determine how soon after policy publication they will perform an audit based on the policy. By allowing a grace period for compliance, you help to ensure that the policies will be enforceable.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Developing a Security Policy—Operate Phase

This topic describes the activities included in the operate phase of the security policy life cycle.




During the operate phase, the system performs its work. However, during this stage, networks change. System administrators add, remove, and upgrade hardware and software components and they add, delete, and modify user privileges. Other events, including corporate acquisitions, attacks, and errors in administrative and operation procedures introduce change.

The operation phase includes security operations and administration, operational assurance, and periodic reanalysis arising from these changes. Here are the four activities that take place during this phase:

- **Security operations and administration:** Systems operation is a big activity that includes backups, training, managing cryptographic keys, keeping up with user administration and access privileges, and updating IT security software. However, there are always vulnerabilities and risks. Network operators do not always keep security and risk foremost on their minds. Users may attempt to bypass security measures and procedures. Changes in the system or the environment can create vulnerabilities. Procedures become outdated.
- **Security auditing:** Audits determine whether the security policy is meeting its goals. Audits can be self-administered or independently administered to provide information about technical, procedural, managerial, or other aspects of security policy effectiveness. Both approaches are effective. However, self-administered audits done by system management staff have an inherent conflict of interest; they should be augmented by independent audits conducted by internal audit staff or unbiased outside contractors. These are the tools and methods used to audit:
  - Automated tools
  - Internal controls audit
  - Security checklists



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Penetration testing
- Annual policy review

- **Security monitoring:** Security monitoring is similar to network monitoring, except security monitoring focuses on detecting changes in the network that indicate a security violation. Ongoing security monitoring looks for vulnerabilities and security problems. Some of the methods are similar to those used for audits, but are done more regularly. There are automated tools that monitor in real time.
- **Incident response:** When security auditing and monitoring expose a security breach, the organization must have a plan in place for immediate response. A good way to approach incident response is to categorize known or expected attacks and devise standard responses that can be used as guides to tailor a rapid incident response.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

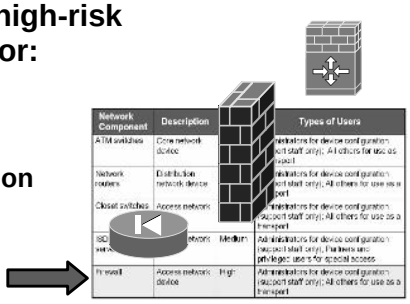
## Operate Phase—Security Monitoring

**Create a monitoring policy based on the security analysis matrix to monitor:**

- **Low-risk equipment weekly**
- **Medium-risk equipment daily**
- **High-risk equipment hourly**

**Example: Because firewalls are high-risk components, set SNMP to monitor:**

- **Failed login attempts**
- **Unusual traffic**
- **Changes to the firewall configuration**
- **Access granted to the firewall**
- **Connections setup through the firewall**



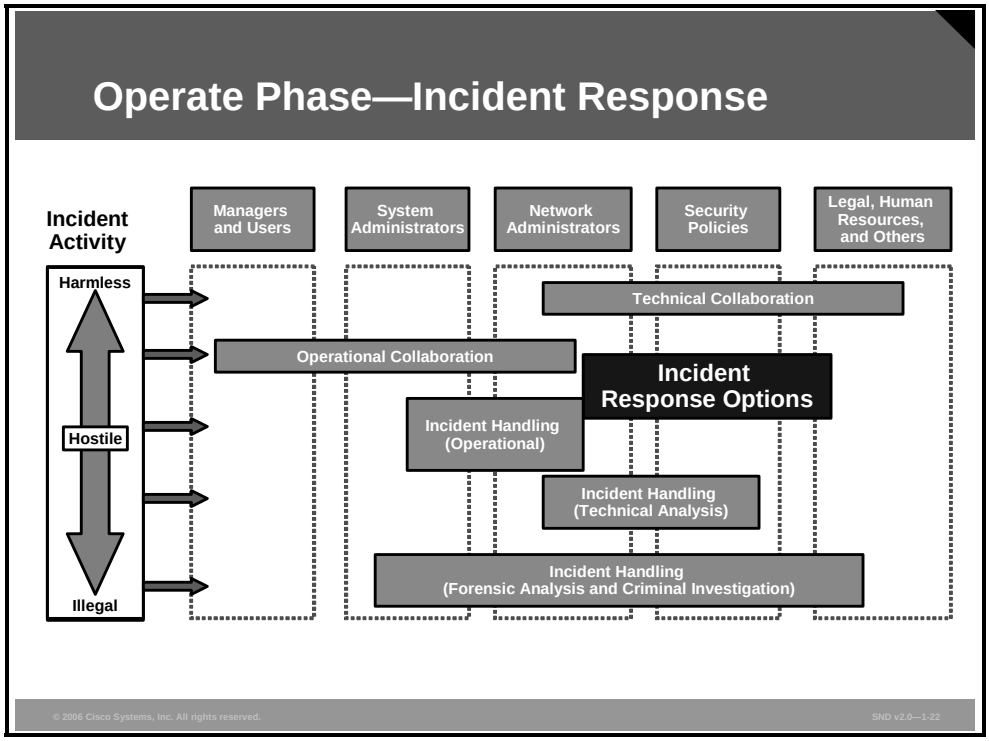

© 2006 Cisco Systems, Inc. All rights reserved.


Recall that in the risk analysis matrix, the firewall is a high-risk network device. This risk indicates a real-time monitoring requirement. You must also monitor any changes to the firewall configuration. Set the Simple Network Management Protocol (SNMP) polling agent to monitor such things as failed login attempts, unusual traffic, changes to the firewall, access granted to the firewall, and connections setup through the firewall.

In a similar fashion, create a monitoring policy for each area identified in the risk analysis matrix. You may want to monitor low-risk equipment weekly, medium-risk equipment every day, and high-risk equipment hourly. If you require more rapid detection, you should monitor more frequently.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Your security policy should define how to notify the security team of security violations. Often, your network monitoring software will be the first to detect the violation. The policy should trigger a notification to the operations center, which, in turn, should notify the security team, using a pager if necessary.

When someone detects a violation, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable.

The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to apply the correct response. You must define a procedure in your security policy that is available 24 hours a day, 7 days a week.

Next, you need to define the level of authority given to the security team to make changes and in what order they will make the changes. These are some possible corrective actions:

- Implementing changes to prevent further access to the violation
- Isolating the violated systems
- Contacting the carrier or Internet service provider (ISP) in an attempt to trace the attack

The figure shows how stakeholders contribute to the incident response, as discussed here:

- Managers and users must know how the incident response team supports their business processes. Managers enter agreements with the incident response team concerning authority over business systems and decision making if critical business systems need to be shutdown or disconnected.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- System and network administrators provide the technical backbone of the team, but not the whole system. The organization must develop procedures to define how staff will work with the incident response team during an emergency or exercise. Agreements define what actions the day staff will take, and what actions the incident response team will take during a response operation. Staff must give the team easy access to network and systems logs for analysis. The team must be able to make recommendations to improve the security of the organizational infrastructure.
- The legal department must also be involved in incident response efforts. This department must review nondisclosure agreements, develop appropriate wording for contacting other sites and organizations, and determine site liability for computer security incidents.
- The human resources department must develop job descriptions and policies and also procedures for removing internal employees found engaging in unauthorized or illegal computer activity.
- The public relations staff must handle any media inquiries and help develop information disclosure policies and practices.
- Other security groups in the organization, especially physical security staff, must exchange information with the team. These other security groups may share responsibility with the team for resolving issues involving computer or data theft.
- Audit and risk management specialists help develop threat metrics and vulnerability assessments, along with encouraging computer security best practices across the constituency or organization.
- Finally, all users provide insight into their needs and requirements.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Developing a Security Policy—Optimize Phase

This topic describes the activities included in the optimize phase of the security policy life cycle.

## Developing a Security Policy—Optimize Phase

| Activity | Comment |
|---|---|
| Managing change | Organizations deal with changes in features and services, new threats and vulnerabilities, increasing need for interconnections, new user groups, and upgrades to software, hardware, and services. |
| Major change | You should analyze changes from a security standpoint and use the PDIOO process. |
| Minor change | You should complete the necessary analysis and modify as necessary. |
| Policy management | You should review policies to ensure that they remain current. |

© 2006 Cisco Systems, Inc. All rights reserved.


## Managing Change

In response to various events, such as user complaints, availability of new features and services, or the discovery of new threats and vulnerabilities, IT system managers and users modify the system and incorporate new features, new procedures, and software updates.

The environment also changes. Networking and interconnections increase. Administrators add new users and user groups including internal users, partners, acquisitions, and others. New threats may emerge. Software, hardware, and services are upgraded.

Companies can deal with change by classifying the change as major or minor, as described here:

- **Major change:** A major change requires analysis to determine any resulting security requirements. Major change usually requires application of the PDIOO process.
- **Minor change:** Many of the changes made to an IT system do not require the extensive analysis performed for major changes but do require some analysis. Each change can involve a limited risk assessment that weighs the benefits and costs.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

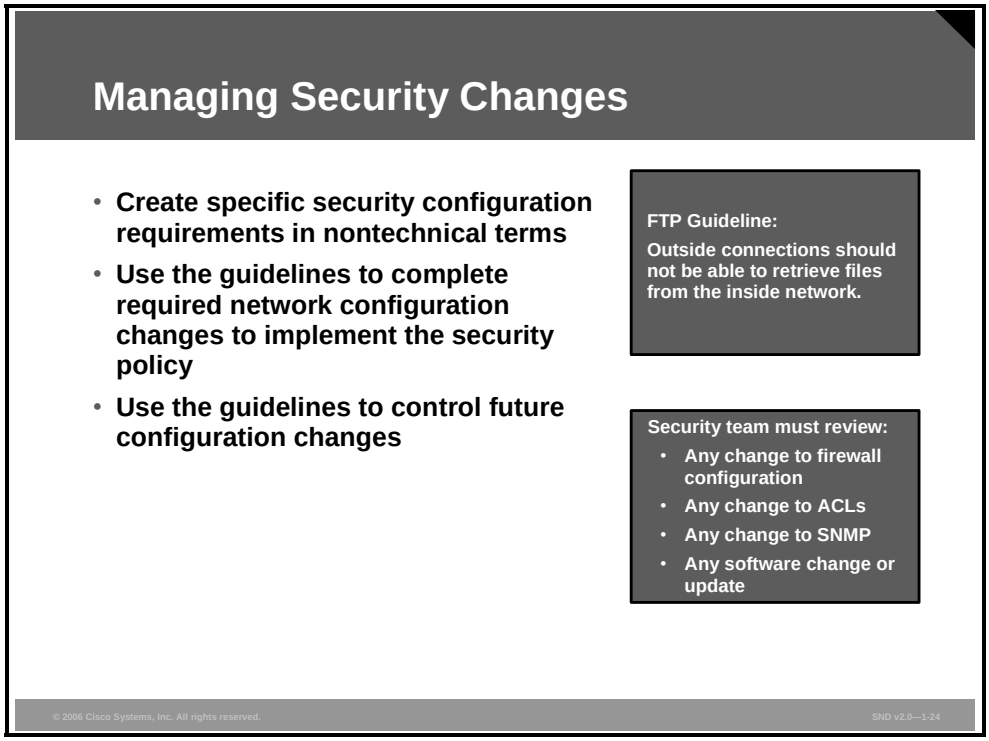
# Policy Management

To ensure that your policies do not become obsolete, you should implement a regular review process. The review process should include some form of update mechanism to translate any changes in the organizational operating environment into your security policy as quickly as possibly.

You must identify and charter a specific department or group, such as the data security department, with the custodianship of the security policy. This organization should also be responsible for conducting a regular review, and, as applicable, updating your security policy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Security changes are changes to network equipment that potentially affect the overall security of the network. Your security policy should identify specific security configuration requirements in nontechnical terms. For example, rather than defining a requirement as "No outside source FTP connections will be permitted through the firewall," define it as "Outside connections should not be able to retrieve files from the inside network." You will need to define a unique set of requirements for your organization.

The security team should review the list of plain language requirements to identify specific network configuration or design issues that meet the requirements. After the team has created the required network configuration changes to implement the security policy, you can apply these to any future configuration changes. Although it is possible for the security team to review all changes, this process allows them to review changes that pose enough risk to warrant special treatment.

The security team should review these types of changes:

- Any change to the firewall configuration
- Any change to access control lists (ACLs)
- Any change to SNMP configuration
- Any change or update in software that differs from the approved software revision level list

It is important to adhere to these guidelines:

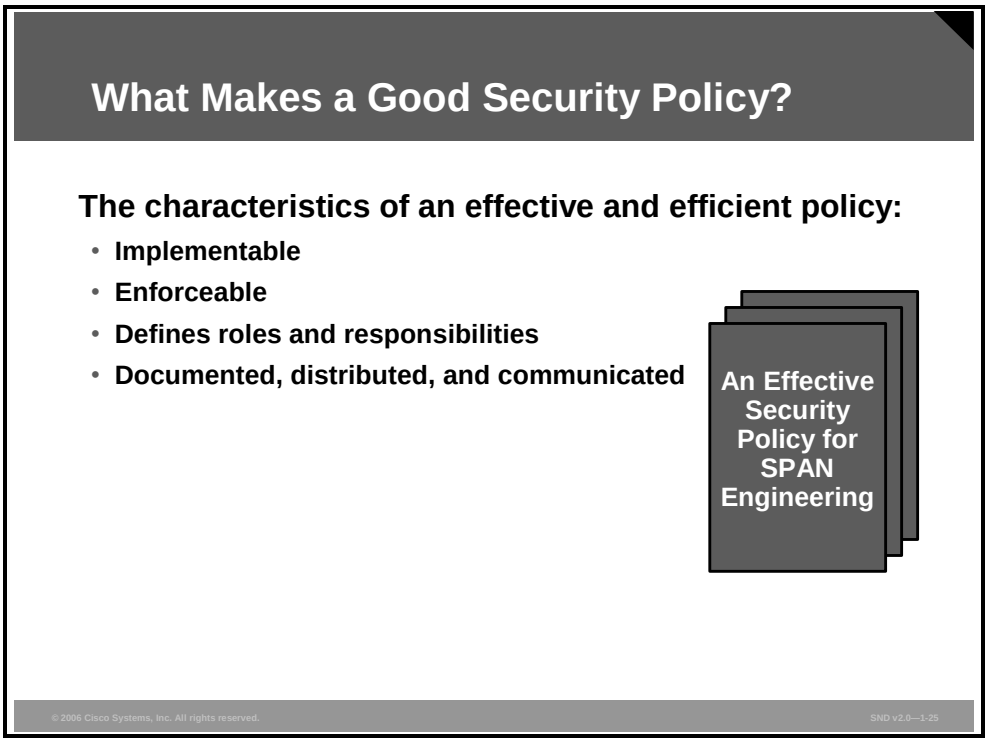
- Change passwords to network devices on a regular basis
- Restrict access to network devices to an approved list of personnel
- Ensure that the current software revision levels of network equipment and server environments comply with security configuration requirements
- Make no network changes without security team approval


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# What Makes a Good Security Policy?

After you put your security policy in place, its effectiveness and efficiency will soon become obvious. This topic describes the general characteristics of an effective security policy.




A good security policy must be effective and efficient. An effective policy does what it is intended to do. An efficient policy does what it is supposed to do in the most cost-effective manner. The characteristics of a good security policy are as follows:

- The policy must be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.
- The policy must be enforceable with security tools, where appropriate, and with sanctions where actual prevention is not technically feasible.
- The policy must clearly define the areas of responsibility for the users, administrators, and management.
- Policies must be documented, distributed, and communicated.

After you establish your security policy, clearly communicate the policy to users, staff, and management. Having all personnel sign a statement indicating that they have read, understood, and agreed to abide by the policy is an important part of the process.

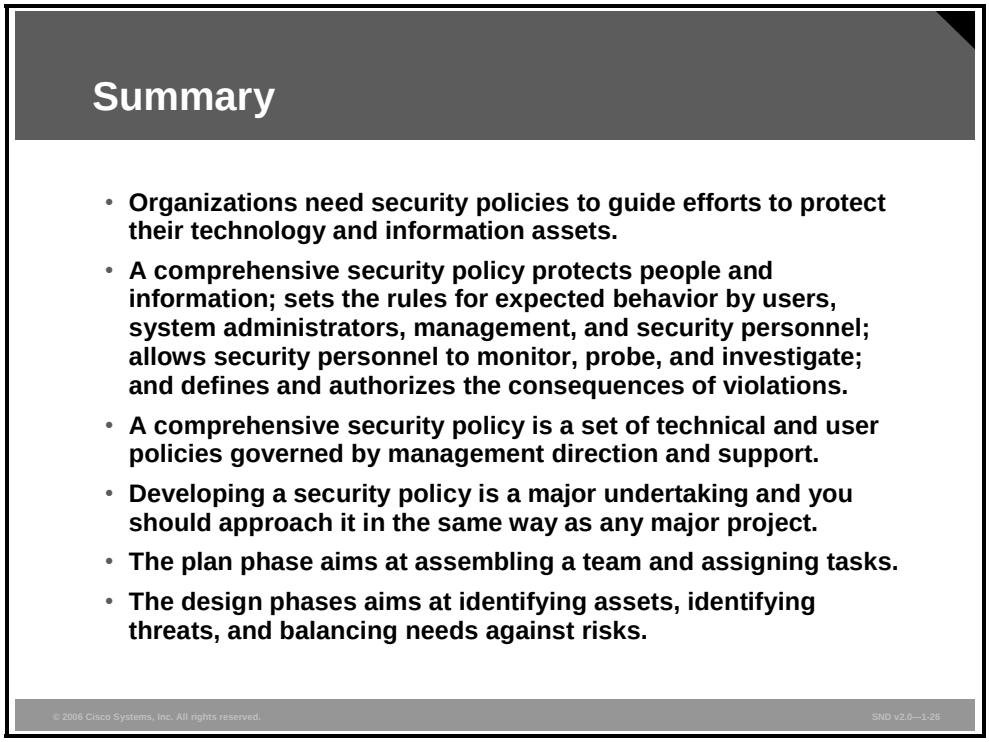
Review your policy on a regular basis to see if the policy is successfully supporting your security needs.

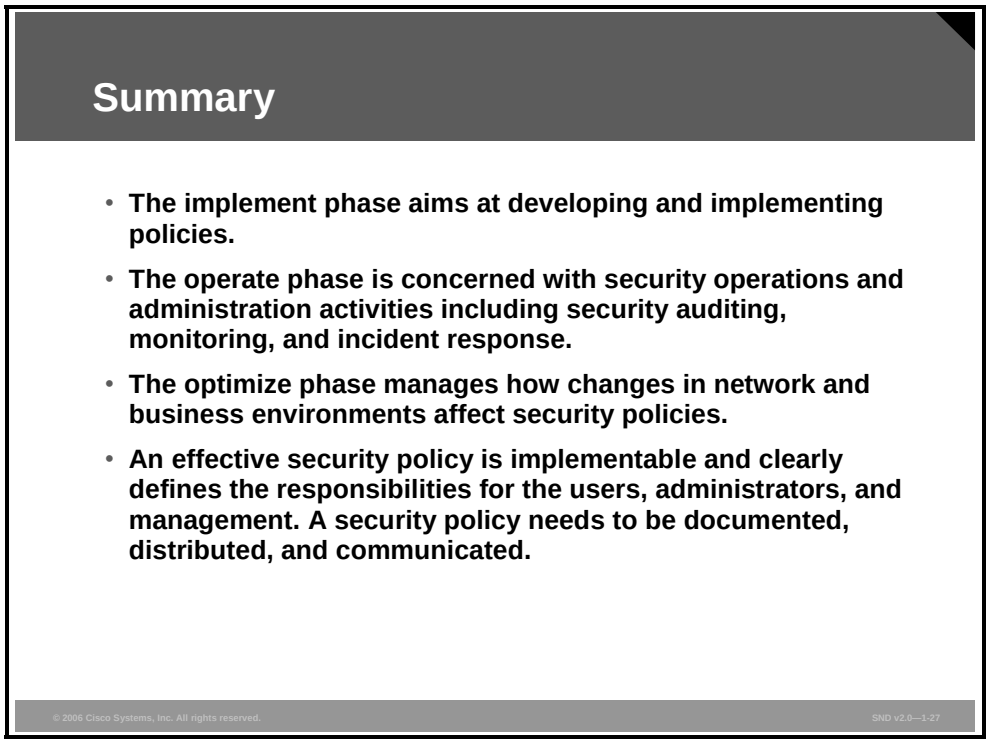


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.





© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 6

# Building Cisco Self-Defending Networks

## Overview

In the past, threats from internal and external sources moved slowly and were easy to defend against. Now Internet worms spread across the world in a matter of minutes. Security systems—and the network itself—must react instantaneously. As the nature of threats to organizations continues to evolve, the defense posture taken by network administrators and managers must also evolve.

The Cisco Self-Defending Network strategy describes the Cisco vision for security systems. The Cisco Self-Defending Network strategy helps customers manage and mitigate more effectively the risks to their networked business systems and applications.

This lesson describes the Cisco Self-Defending Network strategy.

## Objectives

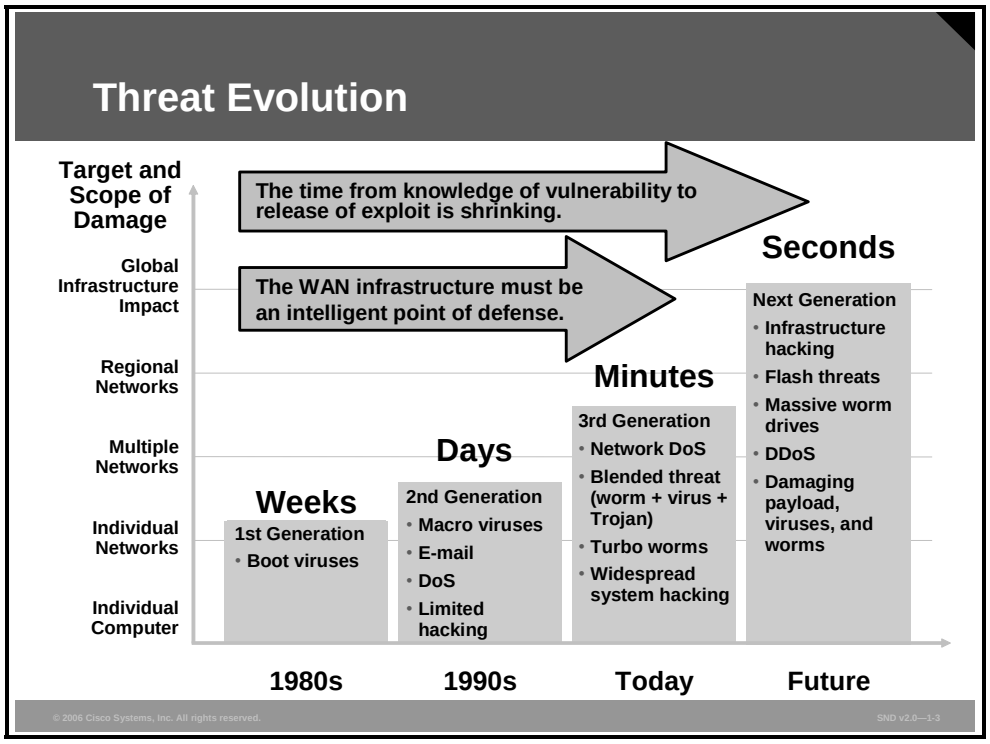
Upon completing this lesson, you will be able to describe how to implement the Cisco Self-Defending Network strategy by enhancing existing network infrastructure with Cisco technologies, products, and solutions. This ability includes being able to meet these objectives:

- Describe how changing threats and challenges demand a new approach to network security
- Describe how to build a Cisco Self-Defending Network in three evolving phases
- Describe the components of the ATD phase of the Cisco Self-Defending Network strategy
- Describe the positioning of the Cisco integrated security portfolio

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Changing Threats and Challenges

This topic describes how changing threats and challenges demand a new approach to network security.




The figure shows how the threats that organizations face have evolved over the past few decades, and how the growth rate of vulnerabilities reported in operating systems and applications is rising. The number and variety of viruses and worms that have appeared over the past three years is daunting, and their rate of propagation is frightening. There have been unacceptable levels of business outages and expensive remediation projects that consume staff, time, and funds not originally budgeted for such tasks.

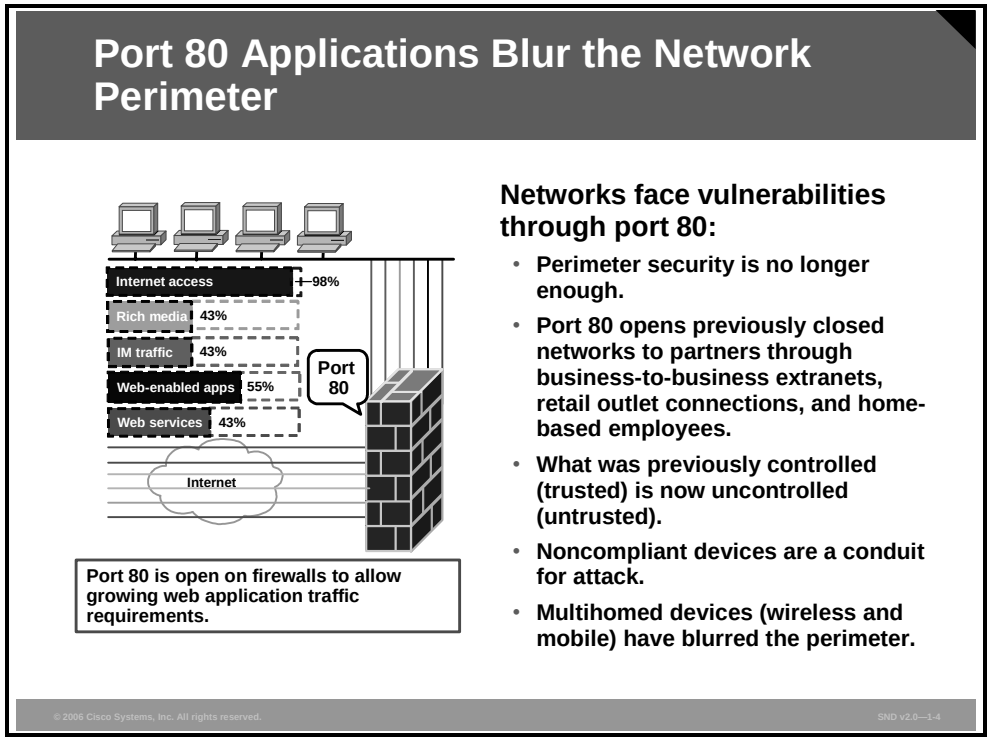
The figure also shows that “blended threats” are evolving. A blended threat uses multiple means of propagation. These threats often have the characteristics of a virus in that they can attach themselves parasitically to files delivered by e-mail. They self-replicate across a network with worm-like ability, and frequently search for and exploit a system or application vulnerability, or multiple vulnerabilities, to gain access to a host and deliver its payload. There is a view that blended threats may be evolving into “flash” threats that may not only exploit new, unknown vulnerabilities, but also have the ability to propagate across the Internet in seconds, seriously affecting the Internet on a global scale.

Also, notice that trends are becoming regional and global in nature. Where attacks once affected single systems or one organization network, more recent attacks are affecting entire regions. For example, attacks have expanded from individual denial of service (DoS) attacks from a single attacker against a single target, to large-scale distributed denial of service (DDoS) attacks emanating from networks of compromised systems known as “botnets.”

Threats are becoming persistent. After an attack starts, attacks may appear in waves as infected systems join the network. Because infections are so complex and have so many end users (employees, vendors, and contractors), multiple types of endpoints (company desktop, home, and server), and multiple types of access (wired, wireless, virtual private network [VPN], and dial-up) infections are difficult to eradicate.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The figure presents an example of the dilemma that network-dependent enterprises face in business environments. You can no longer secure networks by simply securing the network perimeter. Businesses have consolidated their data centers, converged internal networks, and embraced the Internet. Environments that were once self-contained and controlled are now open to partners through business-to-business extranets, retail outlet connections, and home-based employees. By extending the corporate network, the trust boundary has extended across untrusted intermediate networks and into uncontrolled environments.

The growing list of devices that access networks poses more problems. Many devices do not comply with corporate policies. Network users often use compliant devices to access other uncontrolled networks before connecting into the corporate network. As a result, devices on these external networks can become conduits for attacks and related misuse. Here are some of the issues that concern network security experts:

- **Common application interfaces:** The emergence of common application interfaces based on messaging protocols, such as Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP), has increased e-commerce and corporate productivity. However, similar to most new technologies, these new message protocols have introduced an entirely new set of vulnerabilities and attack vectors that corporations need to protect. In the past, firewall policies would filter data carried across many network protocols. Now single transport protocols (such as HTTP on TCP port 80) transport that data. As a result, much of the data that previously resided in packet headers now resides in the packet payload. This change creates significant processing challenges that make it easier for an attacker to evade classic network defenses.



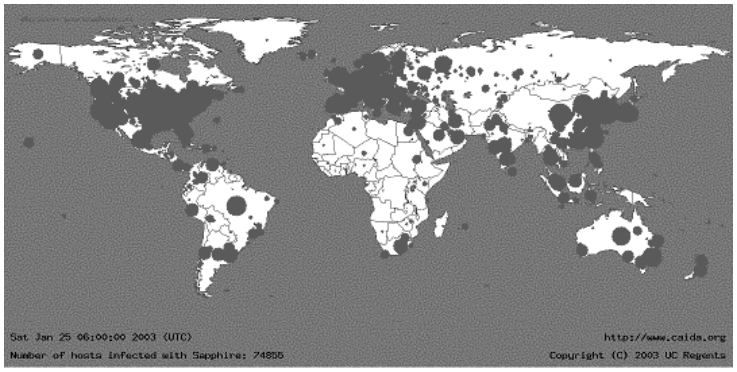
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Security hampering policy:** To meet corporate data confidentiality and integrity requirements, the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) and HTTP Secure (HTTPS) protocols encrypt more and more application-level traffic. This trend makes it much harder for information technology (IT) departments to enforce corporate access policies at the network perimeter, because they cannot inspect the packet payloads of those encrypted flows. Many organizations mistakenly assume that if they comply with regulations, their infrastructure is more secure, which is frequently not the case. Following the law of unintended consequences, the very act of creating compliance may introduce new vulnerabilities. For example, worms and viruses may spread more effectively in a network supporting end-to-end VPNs because the intermediate nodes have no visibility into the traversing traffic. Such traffic may carry worms to sensitive corporate servers in a secure, encrypted packet. In addition to taking longer to diagnose such an attack, these end-to-end VPNs can make it more difficult to remediate the problem.
- **Blurred perimeters:** Tied to the notion of a secure perimeter, the wireless and mobile network within enterprises now supports laptop PCs, personal digital assistants (PDAs), and mobile phones that have more than one network connection. These multihomed hosts are capable of establishing impromptu wireless networks to enable peer-to-peer communication. In addition, devices effectively forward packets at the application level. As a result, network boundaries become much more ambiguous. To manage a secure system and maintain network availability, corporations must be able to extend a control point onto these mobile devices.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## The SQL Slammer Worm: 30 Minutes After "Release"




- **Saturation point was reached within 2 hours of the start of infection.**
- **Infections doubled every 8.5 seconds.**
- **SQL spread 100 times faster than Code Red.**
- **At peak, SQL scanned 55 million hosts per second.**
- **The number of hosts infected was between 250,000 and 300,000.**
- **Internet connectivity was affected worldwide.**

© 2006 Cisco Systems, Inc. All rights reserved.

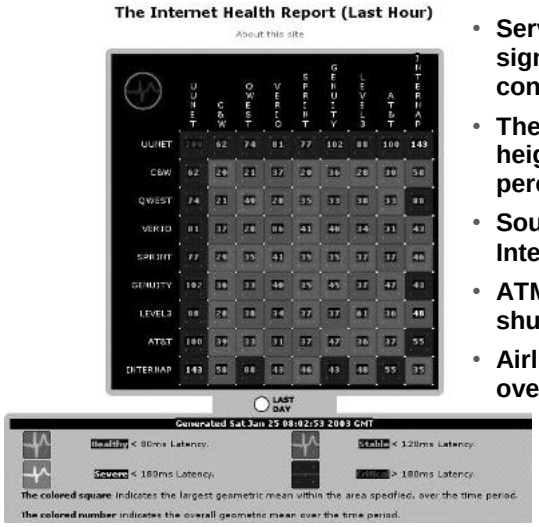

To illustrate the seriousness of network vulnerabilities, consider the effects of the SQL Slammer worm first seen on January 25, 2003. The information in the figure is from the Cooperative Association for Internet Data Analysis (CAIDA) and the University of California at San Diego.

SQL Slammer compromised 90 percent of vulnerable systems within the first 10 minutes, and doubled in size every 8.5 seconds. Within the first 3 minutes, it achieved its maximum scanning rate of over 55 million scans per second.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Network Effects of the SQL Slammer Worm




- **Service providers noted significant bandwidth consumption at peering points.**
- **The average packet loss at the height of the infection was 20 percent.**
- **South Korea lost almost all Internet service.**
- **ATMs around the world were shutdown.**
- **Airline ticketing systems were overwhelmed.**

© 2006 Cisco Systems, Inc. All rights reserved.


The screen shot in the figure was taken by Internet service provider (ISP) UUNET during the height of the infection. The screen shot shows a worm hitting UUNET very hard. It also shows how Internap Network Services had difficulties peering with Qwest Communications International, Genuity, and AT&T.

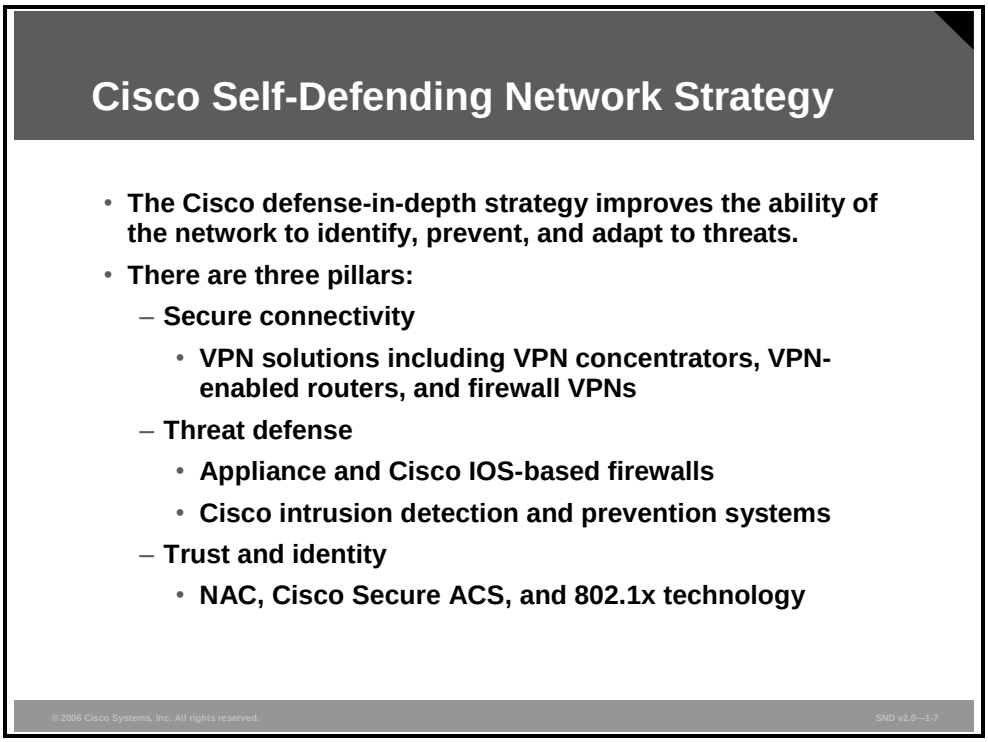
South Korea sustained the most damage with almost total loss of Internet service. (Over 70 percent of South Korean households have Internet service.)

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Building a Cisco Self-Defending Network

This topic describes how to build a Cisco Self-Defending Network in three evolving phases.




Cisco integrated network security solutions incorporate three elements that are critical to effective network security.

- **Cisco Secure Connectivity System:** Increased exposure comes with increased network connectivity. Preserving the confidentiality and integrity of the data and applications that traverse the wired or wireless LAN needs to be an important part of business decisions. The Cisco Secure Connectivity System uses encryption and authentication capabilities to provide secure transport across untrusted networks. To protect data, voice, and video applications over wired and wireless media, Cisco offers IPsec, SSL, Secure Shell (SSH), and Multiprotocol Label Switching (MPLS)-based VPN technologies in addition to the extensive security capabilities that are incorporated into Cisco wireless and IP telephony solutions to ensure the privacy of all IP communications. Cisco Secure Connectivity includes these solutions:
  - Site-to-site VPNs
  - Remote access VPNs
  - Voice security
  - Wireless security
  - Solution management and monitoring

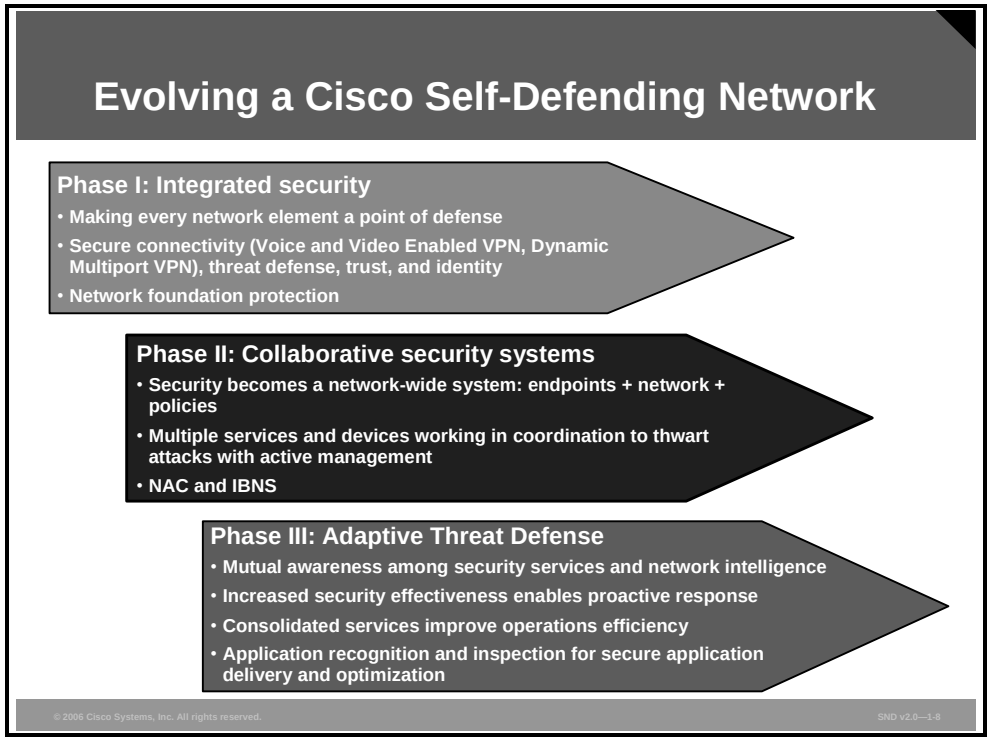


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Cisco Threat Defense System:** Threats are increasingly more destructive and frequent than in the past. Internal and external threats have the ability to significantly affect business profitability. The Cisco Threat Defense System provides a strong defense against known and unknown attacks. Appropriate security technologies and advanced networking intelligence are required to defend effectively against attacks. To be most effective, the defense system technologies must be implemented throughout the network rather than just in point products or technologies, because the source of an attack can start anywhere and instantly spread across all network resources. The Cisco Threat Defense System enhances security in the existing network infrastructure, adds comprehensive security on the endpoints, and adds dedicated security technologies to networking devices and appliances, thereby proactively defending the business, applications, users, and the network. These are the solutions that comprise the Cisco Threat Defense System:
  - Integrated firewall
  - Network intrusion protection
  - Endpoint security
  - Content security
  - Intelligent network and security services (embedded in routers and switches)
  - Management and monitoring
- **Cisco Trust and Identity System:** A trust and identity system is critical for e-business and underpins the creation of any secure network or system. This system provides or denies access to business applications and networked resources based on specific privileges and the rights of a user. The Cisco Trust and Identity System focuses on Network Admission Control (NAC). After validating the identity of a user or device, and after validating compliance with the corporate security policy, NAC enables access to certain resources or portions of the network. The network is responsible for identification, authorization, and enforcement. The Cisco Trust and Identity System includes the Cisco Secure Access Control Server (ACS), authentication protocols such as 802.1x, and authentication, authorization, and accounting (AAA) capabilities in Cisco switches and routers. The Cisco Trust and Identity System has the flexibility to provide a high level of detail in access rights, and to create quarantine zones for noncompliant endpoints and the ability to block unauthorized access entirely.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Most customers do not adopt all of the components of the Cisco Self-Defending Network at one time. This is because it may be difficult to overhaul all of the required subsystems at once without disrupting the integrity of the IT services. Some customers may hesitate to turn over security controls to an automated system until they are confident that the system operates dependably.

The Cisco Self-Defending Network initiative addresses these concerns by providing independently deployable products and then offers solutions that link these products to build effective subsystems. Cisco bases this approach on evolving a Cisco Self-Defending Network on a combination of product development, product acquisitions, systems development, and partner collaboration.

The figure illustrates the evolution of the Cisco Self-Defending Network strategy to date. Note that although point products serve as good incubators for deploying innovative security technologies, these products are not by themselves integrated into the network fabric. Building network security based solely on single-purpose appliances is no longer practical.

Cisco recommends a three-phase approach to developing a Cisco Self-Defending Network:

- **Phase 1—Integrated security:** The first phase of the Cisco Self-Defending Network security strategy focuses on the need for integrated security, a blend of IP and security technologies. This phase aims to distribute security technologies throughout every segment of the network to enable every network element as a point of defense.
- **Phase 2—Collaborative security systems:** The next phase introduces the NAC industry initiative. This initiative is the first industry-wide effort that increases the network ability to identify, prevent, and adapt to security threats. Cisco Identity-Based Networking Services (IBNS) is an integrated solution combining several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. This phase enables the security technologies integrated throughout the network to operate as a coordinated system. Network-wide collaboration among the services and devices throughout the network defeats attacks.

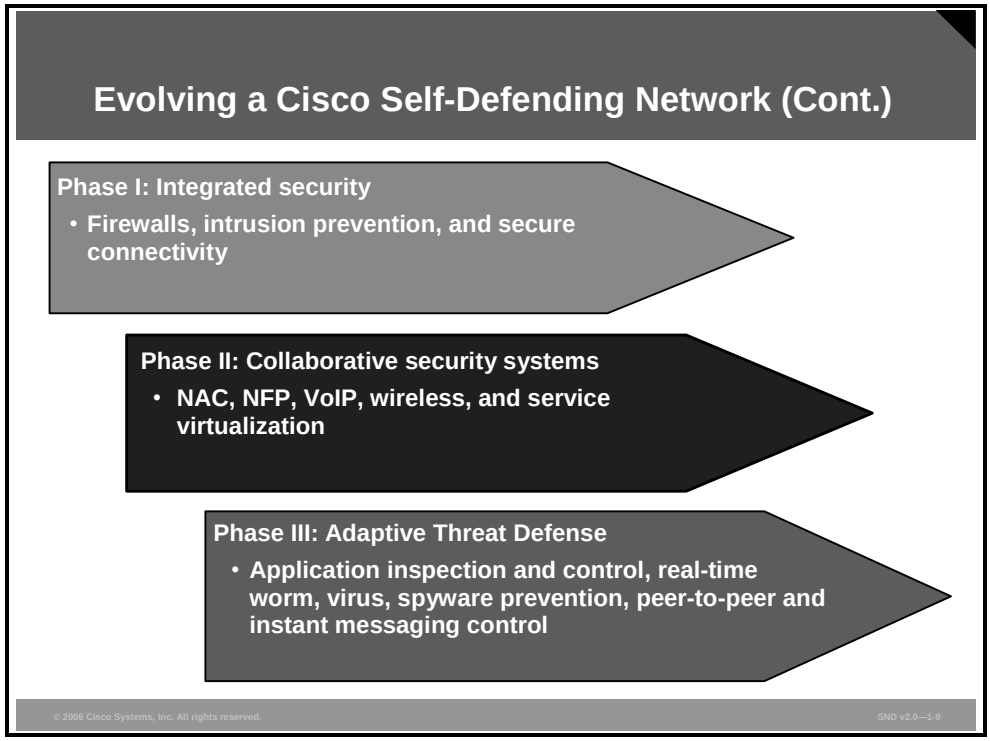


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **Phase 3—Adaptive Threat Defense (ATD):** The third phase deploys innovative and threat defense technologies throughout the integrated security fabric of the network. The goal is to enable more proactive responses to threats with greater operational efficiency by consolidating multiple security services on devices and building mutual awareness among those services. Mutual awareness combines multiple security technologies on a device in a complementary fashion to deliver stronger security services. As a simple example, consider that a firewall provides good Layer 3 and Layer 4 access control and inspection, broad enforcement actions, and strong resiliency. Intrusion prevention systems (IPSs) provide strong application intelligence. Combining and integrating these capabilities provides an application-intelligent device with broad mitigation capabilities and hardened resiliency.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



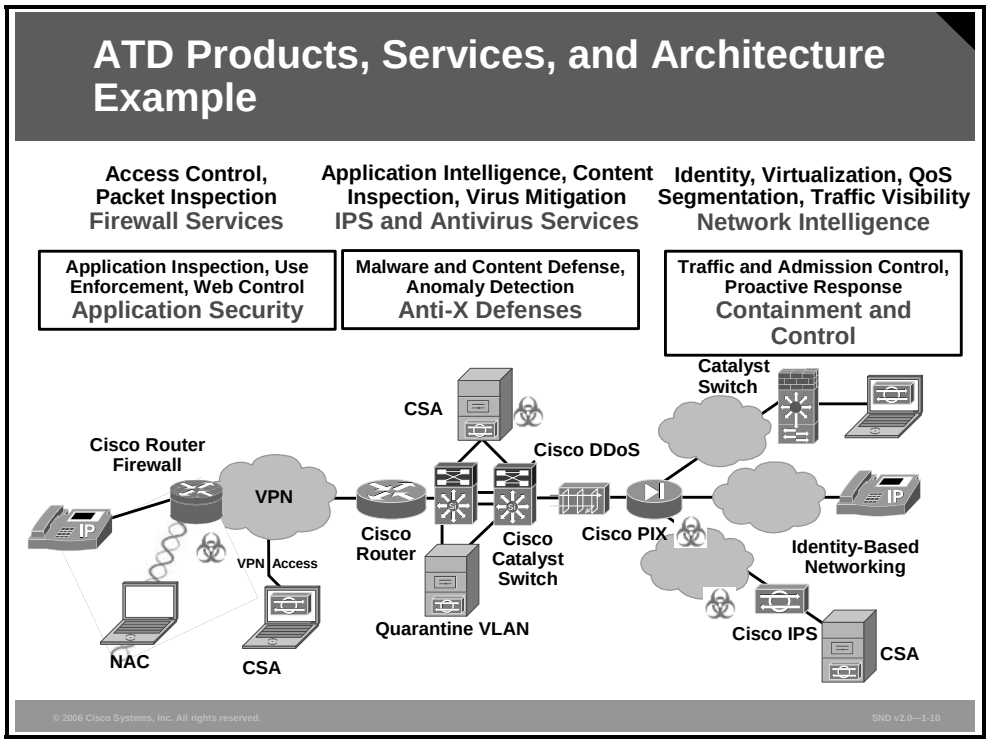

The figure shows the product and technology building blocks of the Cisco Self-Defending Network aligned with each of the development phases. The Cisco Self-Defending Network is built on the pillars of Cisco integrated security, Cisco collaborative security systems, and Cisco ATD, with Cisco Network Foundation Protection (NFP) as an underlying support structure.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Adaptive Threat Defense

ATD is the ultimate goal of the Cisco Self-Defending Network. This topic describes the components of the ATD phase of Cisco Self-Defending Network strategy.




The third phase of the Cisco Self-Defending Network strategy helps minimize further network security risks by dynamically addressing threats at multiple layers to enable tighter control of network traffic, endpoints, users, and applications. ATD also simplifies architectural designs and lowers operational costs. This innovative approach combines security features, multilayer intelligence, application protection, network-wide control, and threat containment within high-performance solutions. ATD is a critical advancement in the Cisco Self-Defending Network security strategy that helps customers to fortify their business systems.

The figure shows the technology components of ATD, the building blocks that converge to provide new services with new applications. These building blocks provide three functions:

- **Firewall services:** These services provide the basis of access control and traffic inspection.
- **IPS and network antivirus services:** These services provide application intelligence with the ability to look at packet payloads.
- **Network intelligence:** Network intelligence includes all network services applicable to security, including network segmentation through VLANs, identity for user knowledge, quality of service (QoS) for controlling the use of bandwidth, routing for topological awareness, and NetFlow for global traffic visibility; “virtualization,” or “virtualized fabric,” is the virtualization of services so that they can be cost-effectively deployed

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Assembling these building blocks provides new services that are integrated throughout the network fabric:

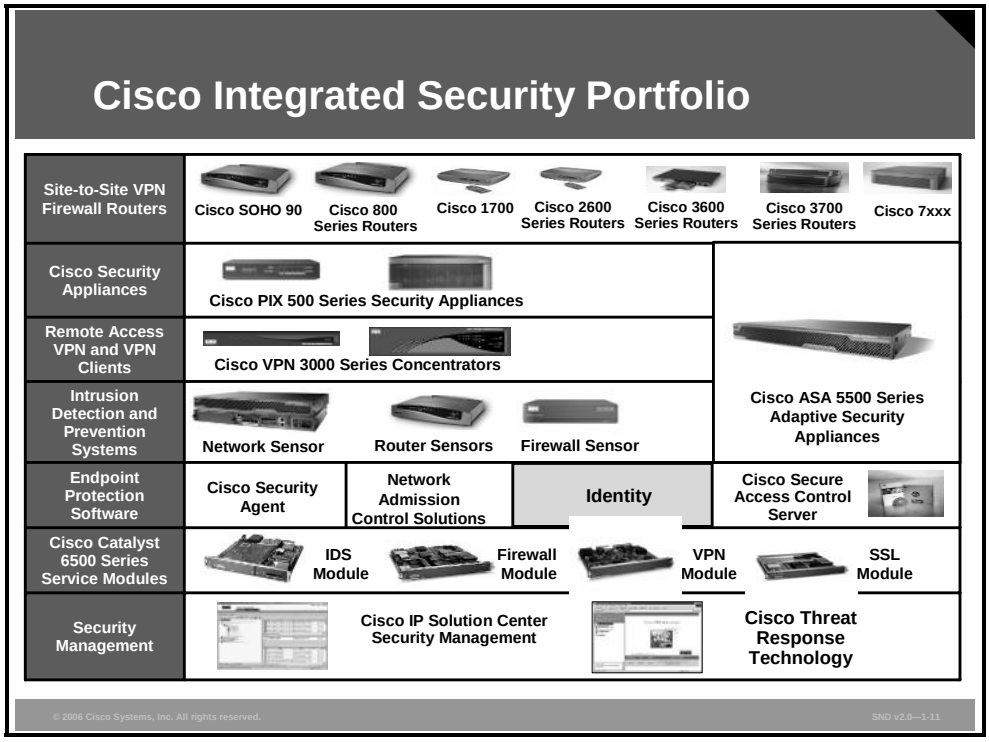
- **Application security:** This service includes granular application inspection in firewalls, intrusion detection systems (IDSs), and IPS appliances, and the ability to enforce appropriate application use policies, such as “don’t allow users to use instant messaging (IM).” This service also includes control of web traffic, including applications that abuse port 80 (such as IM and peer-to-peer) and web services, such as XML applications.
- **Anti-X defenses:** This new class of service includes broad attack mitigation capabilities, (such as malware protection), antivirus, message security (antispam, antiphishing), anti-DDoS, antiworm, and so on. Although these technologies are interesting, anti-X defenses are not just about breadth of mitigation, but about distributing those mitigation points throughout key security enforcement points in the network to stop attacks as far from their intended destination and the core of the network as possible. Stopping an attack before it reaches the network core or host greatly diminishes the damage that the attack can cause and its chances of spreading further.
- **Network containment and control:** Network intelligence and the virtualization of security technologies provide the ability to layer sophisticated auditing, control, and correlation capabilities to control and protect any networked element. This service enables a proactive response to threats by aggregating and correlating security information and by protecting network services such as VoIP and the network infrastructure from activities such as the installation of rogue devices.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Cisco Integrated Security Portfolio

This topic describes the positioning of the Cisco integrated security portfolio.




A truly secure network requires multiple products and technologies that collaborate seamlessly across platforms and integrate tightly with the network infrastructure. The figure illustrates the full range of the Cisco integrated security portfolio. No single product or technology is able to secure a network. There is no other vendor with such a diversity of platforms.

Cisco offers the broadest portfolio of integrated security products in the industry. The portfolio is designed to meet the requirements and diverse deployment models of any network and any environment. Here is a list of some of these products:

- Cisco IOS platforms with integrated IPS, VPN, and stateful firewall to support secure IP connectivity
- Cisco Adaptive Security Algorithm (ASA) with integrated VPN to ensure perimeter security, access control, and IPS
- Cisco PIX security appliances with integrated VPN to ensure perimeter security and access control
- Cisco VPN 3000 Series Concentrators help ensure secure telecommuter connectivity
- Appliance-based network IDS and IPS and integrated network IDS and IPS for Cisco IOS routers, Cisco PIX security appliances, and ASA
- Endpoint protection software (Cisco Security Agent [CSA]) to protect servers and desktops from the damaging effects of known and unknown threats
- Cisco Secure ACS to ensure that users have the proper authority to access corporate resources
- Security modules for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers that provide security throughout the data center

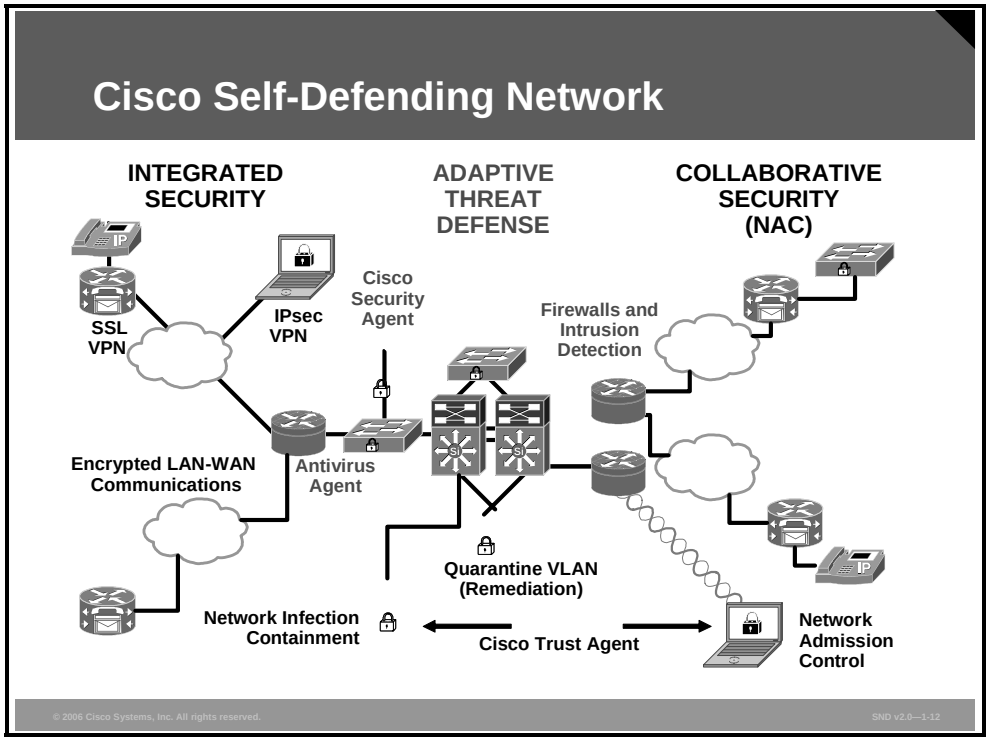
 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Security management products including Cisco Security Manager, Cisco Security Monitoring, Analysis, and Response System (MARS), Cisco Router and Security Device Manager (SDM), and other GUI-based device managers



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Most customers will not adopt all of the components of the Cisco Self-Defending Network at one time, because it may be difficult to overhaul all of the required subsystems at once without disrupting the integrity of the IT services. Some customers may hesitate to turn over security controls to an automated system until they are confident that the system will operate dependably. The Cisco Self-Defending Network initiative deals with these concerns by first providing products that can be usefully deployed independently of one another and then by offering solutions that can link these products together as confidence builds in each product and subsystem. This has proven to be a successful approach based on a combination of product development, product acquisitions, systems development, and partnering.

## Endpoint Protection

One of the realities of viruses and worms is that, along with endpoint infection, they frequently create network congestion as a byproduct of rapid propagation. In effect, CSA becomes a first order dampener to the virus and worm propagation effect. A second and equally compelling reason for deploying CSA is that it establishes a presence on endpoints that can be used to establish a feedback loop between the endpoint and the network resulting in a network that rapidly adapts to emerging threats.

## Admission Control

One of the most high-profile Cisco Self-Defending Network initiatives to date is the Cisco NAC program. NAC allows customers to determine what level of network access to grant to an endpoint based on the security posture of the user, which is based on the security state of the operating system and associated applications. In addition to controlling access, NAC gives IT administrators a way to automatically quarantine and remediate noncompliant endpoints. Making sure that endpoints are in compliance with operating system patches and antivirus software updates is an effective second order dampener to the virus and worm propagation effect. Another way of looking at NAC is as an on-demand vulnerability assessment and patch management tool.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

A distinguishing feature of NAC is that it provides both client and back-end AAA interfaces that allow customers to plug in products from their preferred endpoint security and policy vendors.

## Infection Containment

Strong network admission policies do not eliminate the need to continue monitoring devices once they enter a network. Determined attackers can evade just about any admission check, and the network cannot always rely on, or trust, an infected element to turn itself in. Compliant devices also can become infected through a variety of vectors once they are members of a network (for example, a Universal Serial Bus [USB] key with infected content). To further help protect the network, the Cisco Self-Defending Network is designed to extend the security checks performed at the time of admission for the duration of the network connection. In addition, the Cisco Self-Defending Network can rely on other network elements, including other endpoints, to detect when another endpoint is no longer trustworthy. Cisco regards infection containment as a third-order dampener to the virus and worm propagation effect.

## In-Line IPS and Anomaly Detection

An important area of ongoing security development has been in the area of network IDS (NIDS). One of the first Cisco innovations in this area was to integrate IDS into its router and switching platforms. However, for IDS to fully deliver on its capabilities, it needs to transform into an IPS with in-line filtering capabilities. This provides a mechanism to remove unwanted traffic with fine-grained programmable classification engines.

## Application Security and Anti-X Defense

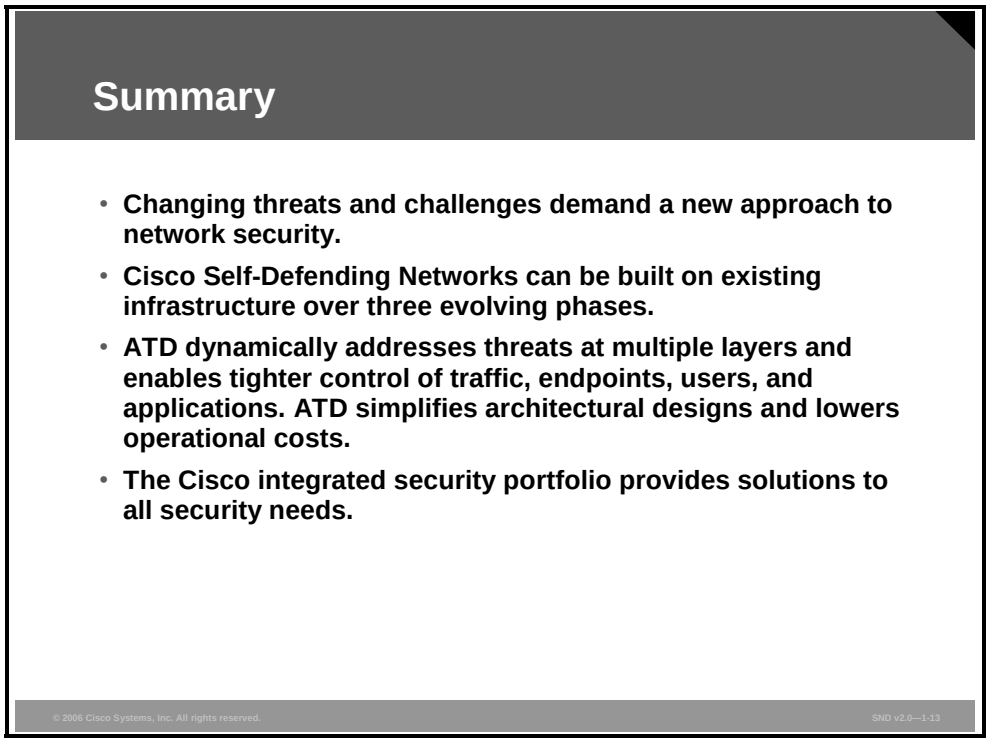
Over the past several years, a number of new application layer network products have emerged to help address new classes of threats that were not adequately addressed by classic firewall and NIDS products, including viruses and worms, e-mail based spam and phishing, spyware, web services abuse, IP telephony abuse, and unauthorized peer-to-peer activity. Cisco has developed the next generation of packet- and content-inspection security services to deal with these types of threats and misuse. This convergence brings granular traffic inspection services to critical network security enforcement points, thereby containing malicious traffic before it can be propagated across the network.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.

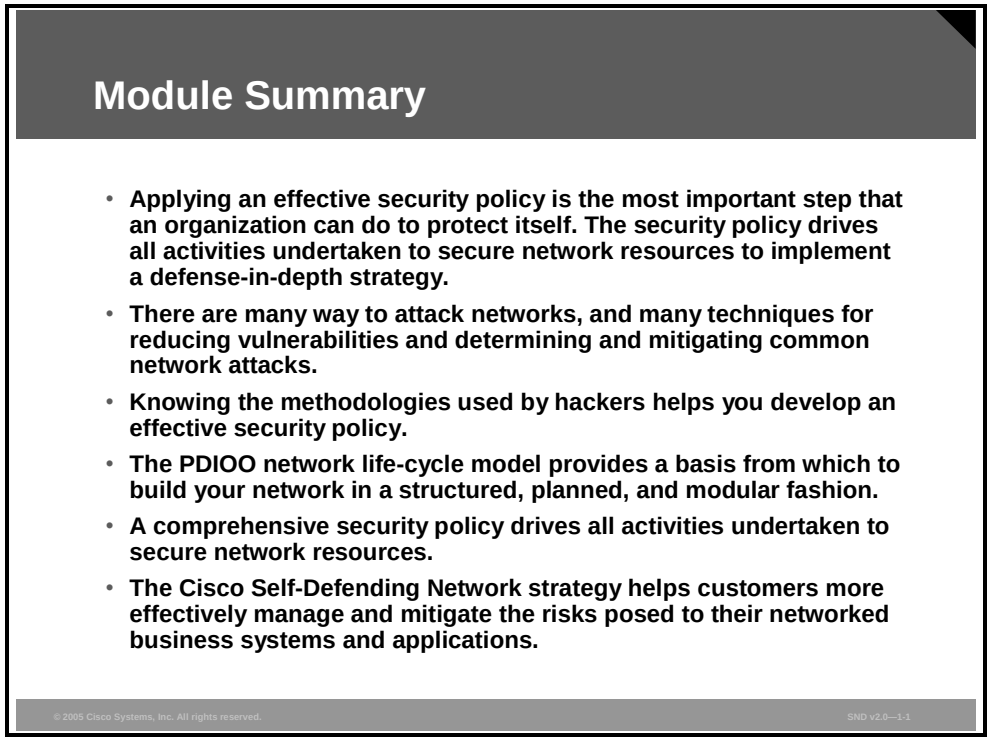



 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module Summary

This topic summarizes the key points that were discussed in this module.




The increasing dependence on networks by government, business, and educational organizations, coupled with the risk brought about by increasing threat levels, supports the need for security decisions to be based on a comprehensive security policy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# References

For additional information, refer to these resources:


- Canavan, S. The SANS Institute. *An Information Security Policy Development Guide for Large Companies.* http://www.sans.org/rr/whitepapers/policyissues/1331.php.
- West-Brown, Moira J., D. Stikvoort, K.P. Kossakowski, et al. Carnegie Mellon Software Engineering Institute. *Handbook for Computer Security Incident Response Teams (CSIRTs).* http://www.cert.org/archive/pdf/csirt-handbook.pdf.
- Cisco Systems, Inc. *Network Security Policy: Best Practices White Paper.* http://www.cisco.com/warp/public/126/secpol.html.
- Computer Security Institute. *2005 CSI/FBI Computer Crime and Security Survey.* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf
- Fyodor. The Art of Port Scanning. http://www.insecure.org/nmap/nmap_doc.html.
- Guel, M. D. The SANS Institute. A Short Primer for Developing Security Policies. http://www.sans.org/resources/policies/Policy_Primer.pdf.
- Information Assurance Technical Framework Forum (IATFF). http://www.iatf.net/.
- Jarmon, D. The SANS Institute. *SANS Security Essentials GSEC Practical Assignment Version 1.3: A Preparation Guide to Information Security Policies.* http://www.sans.org/rr/whitepapers/policyissues/503.php.
- Stoneburner, G., C. Hayden, and A. Feringa. National Institute of Standards and Technology (NIST). *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*. NIST Special Publication 800-27. http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf.
- Oppenheimer, P. Analyzing Business Goals and Constraints of Network Design from Top-Down Network Design, . Indianapolis, Indiana: Pearson Education, Cisco Press; 2004.
- Noens, K . How to Become a Hacker . http://users.pandora.be/mydotcom/library/index.htm.
- SecurityFocus. Password Crackers—Ensuring the Security of Your Password. http://www.securityfocus.com/infocus/1192.
- SecurityFocus. Social Engineering Fundamentals, Part I: Hacker Tactics. http://www.securityfocus.com/infocus/1527.
- SecurityFocus. Social Engineering Fundamentals, Part II: Combat Strategies. http://online.securityfocus.com/infocus/1533.
- Sutton, E. Footprinting: What is it and How Do You Erase Them http://www.infosecwriters.com/text_resources/pdf/Footprinting.pdf.
- VeriSign Inc. *Hacking and Network Defense.* http://www.atapusa.org/downloads/hacking.pdf.
- Weise, J. And C.R. Martin. Sun Microsystems, Inc. *Developing a Security Policy*. http://www.sun.com/blueprints/1201/secpolicy.pdf.


 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are in the Module Self-Check Answer Key.

Q1) What is the main threat to a closed network? (Source: Understanding the Requirement for a Network Security Policy)

A) a deliberate attack from outside
B) a deliberate or accidental attack from inside
C) misuse by customers
D) misuse by employees

Q2) Which two factors have recently influenced the increase in threats from hackers? (Choose two.) (Source: Understanding the Requirement for a Network Security Policy)

A) Hacker tools require more technical knowledge to use.
B) Hacker tools have become more sophisticated.
C) The number of reported security threats has remained constant year to year.
D) Hacker tools require less technical knowledge to use.

Q3) Based on responses to the *2005 CSI/FBI Computer Crime and Security Survey*, which of these trends are true and which are false? (Source: Understanding the Requirement for a Network Security Policy)

| | | | |
|---|---|---|---|
| A) | Virus attack incidents had fallen behind website attack incidents in terms of causing the greater financial loss | T | F |
| B) | The total dollar amount of financial losses resulting from cybercrime is decreasing. | T | F |
| C) | Because of improved safeguards, fewer firms see the need to conduct security audits than in the past. | T | F |
| D) | Fewer firms are reporting computer intrusions to law enforcement than in the past. | T | F |
| E) | Most respondents feel that their companies are expending an adequate amount of money on security training. | T | F |

Q4) What three major dynamics are converging to heighten the need for network security? (Source: Understanding the Requirement for a Network Security Policy)

_____

_____

_____

_____

_____

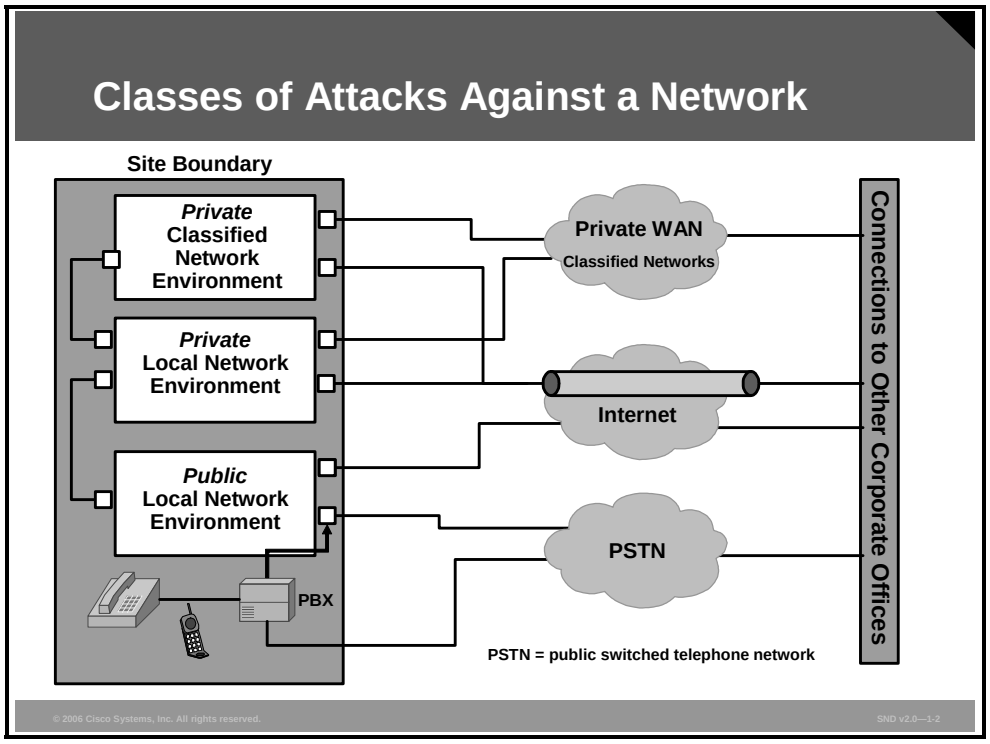


*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q5) What is the underlying basis of ensuring information assurance? (Source: Understanding the Requirement for a Network Security Policy)

A) need to know
B) access control
C) separation
D) robust security measures

Q6) Recall the five classes of attack—passive, active, close-in, insider, and distribution. Consider the generalized topology shown in the figure. List all of the places that are vulnerable to each class of attack. For example, the local private network is susceptible to an insider attack, while the Internet and public switched telephone network are susceptible to active attacks. (Source: Understanding the Requirement for a Network Security Policy)






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q7) Which activity ensures that information and information systems are protected against attacks through the application of security services such as availability, integrity, authentication, confidentiality, and nonrepudiation? (Source: Understanding the Requirement for a Network Security Policy)

A) information assurance
B) risk management
C) security evaluation
D) security planning

Q8) Which set of factors requires balance to achieve information assurance in a defense-in-depth strategy? (Source: Understanding the Requirement for a Network Security Policy)

A) cost, threat, and security
B) people, technology, and operations
C) availability, integrity, and authentication
D) architectures, standards, and criteria

Q9) Which principles are included in a defense-in-depth strategy? (Source: Understanding the Requirement for a Network Security Policy)

A) defend in multiple places
B) build layered defenses
C) use robust components
D) employ robust key management
E) deploy IDS and IPS

Q10) Which two layered defense measures protect against active attacks? (Choose two.) (Source: Understanding the Requirement for a Network Security Policy)

A) encryption and traffic flow security measures
B) access controls and host-based intrusion protection systems on hosts
C) firewalls and intrusion detection and protection systems
D) runtime integrity controls

Q11) Which three factors must companies balance when designing a secure network infrastructure? (Source: Understanding the Requirement for a Network Security Policy)

A) security policy, security architecture, and security technologies
B) identity, perimeter security, and secure connectivity
C) perimeter security, secure connectivity, and security monitoring
D) security policy, security architecture, and security policy management

Q12) List the four common threats to Cisco network physical installations. (Source: Introducing Network Attack Mitigation Techniques)



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q13) Describe each of these four types of security attacks: reconnaissance attacks; access attacks; DoS attacks; and worm, virus, and Trojan horse attacks. (Source: Introducing Network Attack Mitigation Techniques)

_____

_____

_____

Q14) Which type of reconnaissance attack is best mitigated by using strong authentication and cryptography? (Source: Introducing Network Attack Mitigation Techniques)

A) packet sniffers
B) port scans
C) ping sweeps
D) Internet information queries

Q15) Which type of reconnaissance attack is mitigated by turning off ICMP echo and echo-reply? (Source: Introducing Network Attack Mitigation Techniques)

A) packet sniffers
B) port scans
C) ping sweeps
D) Internet information queries

Q16) Which of the following four attacks are classified as access attacks? (Choose four.) (Source: Introducing Network Attack Mitigation Techniques)

A) port redirection
B) trust exploitation
C) password attacks
D) man-in-the-middle attacks
E) DDoS
F) Trojan horse
G) Love Bug

Q17) What are two methods for computing passwords with L0phtCrack? (Choose two.) (Source: Introducing Network Attack Mitigation Techniques)

A) random access generator
B) dictionary cracking
C) brute-force computation
D) password hashing
E) character duplication

Q18) Which type of attack is mitigated by encrypting traffic in an IPsec tunnel? (Source: Introducing Network Attack Mitigation Techniques)

A) packet sniffers
B) password attack
C) man-in-the-middle attacks
D) Internet information queries

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q19) Why are DoS attacks difficult to eliminate? (Source: Introducing Network Attack Mitigation Techniques)

_____

_____

Q20) A virus can spread automatically through a network. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false

Q21) Encryption helps mitigate IP spoofing. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false

Q22) Traffic rate limiting helps mitigate IP spoofing. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false

Q23) As a minimum, antispoofing configurations must meet the requirements of RFC 3704. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false

Q24) What is the name for a malicious code that masquerades as a program? (Source: Introducing Network Attack Mitigation Techniques)

A) a Trojan horse
B) a bomb
C) a virus
D) a worm

Q25) Which malicious code travels from computer to computer making copies of itself? (Source: Introducing Network Attack Mitigation Techniques)

A) a Trojan horse
B) a virus
C) a bomb
D) a worm

Q26) The Love Bug attack is not a virus, but a Trojan horse. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q27) Trojan horse is a specific term referring to a particular attack mechanism. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false

Q28) Worm containment includes tracking down each infected machine inside the network. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false

Q29) A hacker transmitting thousands of ICMP pings from a PC to multiple target servers is an example of a DDoS attack. (Source: Introducing Network Attack Mitigation Techniques)

A) true
B) false

Q30) Why is Telnet not a preferred configuration management protocol? (Source: Introducing Network Attack Mitigation Techniques)

A) Telnet is slow.
B) Telnet does not have a GUI.
C) Telnet is not encrypted.
D) Telnet is too easily spoofed.

Q31) Which three techniques and tools should you use to detect and prevent reconnaissance attacks? (Choose three.) (Source: Introducing Network Attack Mitigation Techniques)

A) access lists
B) cryptography
C) lock-and-key
D) authentication
E) CBAC
F) IDS

Q32) Which type of network attack occurs when an intruder attempts to discover and map systems, services, and vulnerabilities? (Source: Introducing Network Attack Mitigation Techniques)

A) time-of-day attack
B) reconnaissance attacks
C) DoS attacks
D) access attacks

Q33) List the seven steps that hackers typically follow to break into a network. (Source: Thinking Like a Hacker)

Step 1: _____
Step 2: _____
Step 3: _____
Step 4: _____
Step 5: _____
Step 6: _____
Step 7: _____


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q34) List the two common methods that a hacker uses to manipulate users to gain access to the network. (Source: Thinking Like a Hacker)

Q35) Why do hackers use back doors? (Source: Thinking Like a Hacker)

Q36) Why are characters such as | ; < > not acceptable as possible input on a web page? (Source: Thinking Like a Hacker)

Q37) Explain these key factors to consider when designing a secure network: business needs, risk analysis, security policy, industry best practices, and security operations. (Source: Designing a Secure Network Life-Cycle Model)

Q38) Describe what each component of the PDIOO model means in terms of approach to secure network lifecycle management. (Source: Designing a Secure Network Life-Cycle Model)

P _____
D _____
I _____
O _____
O _____

Q39) List the three steps in network design development. (Source: Designing a Secure Network Life-Cycle Model)



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q40) Define each of these terms in the context of security policies. (Source: Developing a Comprehensive Security Policy)

Confidentiality: _____
Integrity: _____
Availability: _____

Q41) Give three reasons for having a security policy. (Source: Developing a Comprehensive Security Policy)

Q42) List three of the components of a comprehensive security policy. (Source: Developing a Comprehensive Security Policy)

Q43) Which section of a security policy specifies how spam is handled? (Source: Developing a Comprehensive Security Policy)

A) acceptable use policy
B) Internet access policy
C) e-mail policy
D) remote access policy
E) campus access policy

Q44) What are the two elements of risk analysis? (Source: Developing a Comprehensive Security Policy)


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q45) Complete the entries in this security matrix. (Source: Developing a Comprehensive Security Policy)

| System | Description | Risk Level | Types of Users |
|---|---|---|---|
| DNS and DHCP servers | | | |
| External e-mail server | | | |
| Internal e-mail server | | | |
| Oracle database | | | |

Q46) What are the four characteristics of a good security policy? (Source: Developing a Comprehensive Security Policy)

Q47) Summarize the characteristics of a blended threat. (Source: Building Cisco Self-Defending Networks)

Q48) Define a flash threat. (Source: Building Cisco Self-Defending Networks)



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q49) Describe the vulnerability stemming from the sources listed in the table: (Source: Building Cisco Self-Defending Networks)

| Source | Vulnerability |
|---|---|
| Common application interfaces | |
| Corporate security policies | |
| Wireless and mobile network within enterprises | |

Q50) Identify the goal of each phase in the evolution of the Cisco Self-Defended Network, and identify the products and technologies associated with each phase. (Source: Building Cisco Self-Defending Networks)

| Phase | Goal | Products and Technologies |
|---|---|---|
| Phase I | | |
| Phase II | | |
| Phase III | | |


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module Self-Check Answer Key

Q1) B

Q2) B, D

Q3) A) false, B) true, C) false, D) true, E) false

Q4) Three converging dynamics:

a. There are new and pending laws in the United States and around the world that require organizations to better protect the privacy of sensitive and personal information.

b. There is a growing level of terrorist and criminal activity being directed at communications networks and computer systems.

c. The increased use of Internet technology and connectivity around the world has made cyber attacks and hacking much easier for a larger number of perpetrators.

Q5) B

Q6) The figure shows how the network is vulnerable to each of these attack vectors:

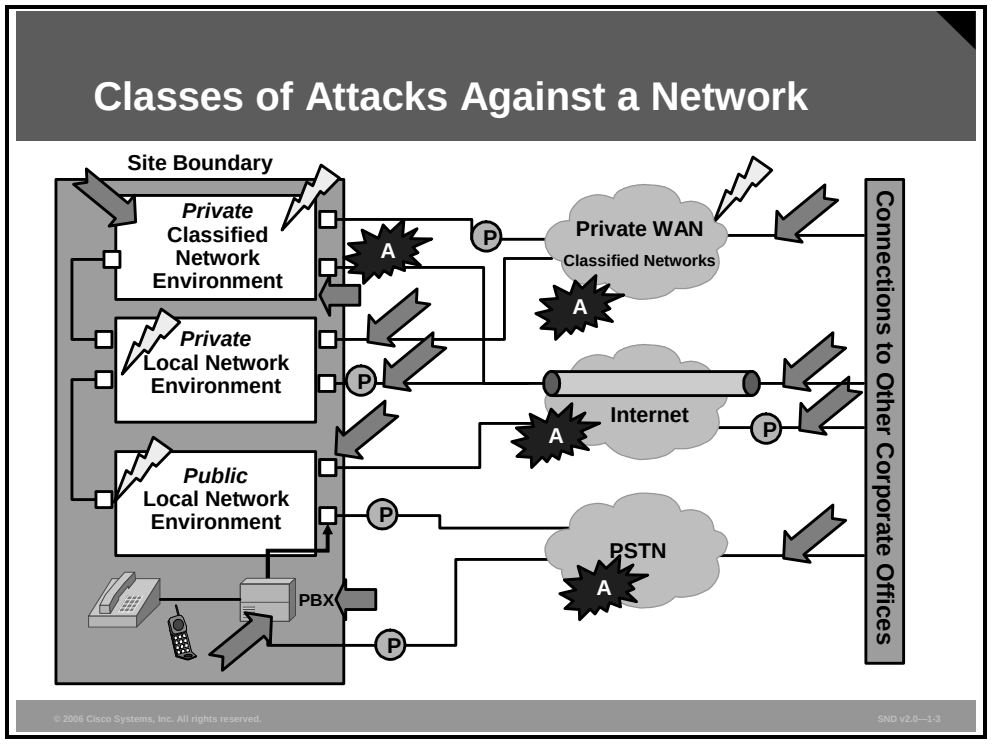
a. The lightning bolt represents an insider attack.

b. The short arrows are close-in attacks.

c. The notched arrows are distribution attacks.

d. The circled letter "P" is a passive attack.

e. The letter "A" in a starburst is an active attack.




Q7) A

Q8) B



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q9) A, B, C, D, E

Q10) B, C

Q11) A

Q12) hardware, environmental, electrical, and maintenance threats

Q13) Four types of network attacks:

- **Reconnaissance attacks:** An intruder attempts to discover and map systems, services, and vulnerabilities.
- **Access attacks:** An intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.
- **DoS attacks:** An intruder attacks your network in a way that damages or corrupts your computer system or denies you and others access to your networks, systems, or services.
- **Worms, viruses, and Trojan horses:** Malicious software is inserted onto a host to damage a system, corrupt a system, replicate itself, or deny services or access to networks, systems, or services.

Q14) A

Q15) C

Q16) A, B, C, D

Q17) B, C

Q18) C

Q19) Although there are software fixes that system administrators can install to limit the damage caused by all known DoS attacks, new DoS attacks are constantly being developed by hackers.

Q20) false

Q21) true

Q22) false

Q23) true

Q24) A

Q25) D

Q26) false

Q27) false

Q28) false

Q29) false

Q30) C

Q31) B, D, F

Q32) B

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q33) Step 1: Perform footprint analysis (reconnaissance).

Step 2: Enumerate information.

Step 3: Manipulate users to gain access.

Step 4: Escalate privileges.

Step 5: Gather additional passwords and secrets.

Step 6: Install back doors.

Step 7: Leverage the compromised system.

Q34) social engineering and password cracking

Q35) Hackers use back doors as a way back into the system if the front door is locked and as a way into the system that is not likely to be detected.

Q36) Using symbols such as these might allow hackers to enter UNIX commands along with usernames and passwords to gain access into the network.

Q37) Here are some of the key factors to consider when designing a secure network:

- **Business needs:** What does your organization want to do with the network?
- **Risk analysis:** What is the risk and cost balance?
- **Security policy:** What are the policies, standards, and guidelines needed to address the business needs and risk?
- **Industry best practices:** What are the reliable, well-understood, and recommended security best practices?
- **Security operations:** Security operations include incident response, monitoring, maintaining, and compliance auditing of the system.

Q38) The PDIOO components are as follows:

- **Plan:** The network designers identify network requirements in this phase. This phase includes analyzing the places where the network designers will install the network and identifying the people and processes that need network services.
- **Design:** In this phase, the network designers accomplish the bulk of the logical and physical design according to the requirements gathered during the plan phase.
- **Implement:** After management approves the design, implementation begins according to the design specifications. Implementation also serves to verify the design.
- **Operate:** Operation is the final test of the effectiveness of the design. The network is monitored during this phase for performance problems and any faults to provide input into the optimize phase of the network life cycle.
- **Optimize:** The optimize phase uses proactive network management techniques to identify and resolve problems before network disruptions arise. The optimize phase may lead to a network redesign if too many problems arise because of design errors or as network performance degrades over time as actual use and capabilities diverge. Redesign may also be required when requirements change significantly.

Q39) Network design development normally follows these three steps: logical design, physical design, and testing.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q40) In the context of a security policy, these terms are defined as follows:

- Confidentiality is a generic term referring to information that requires protection. Security specialists classify information in increasing levels from restricted distribution to secret. Letting such information get into the wrong hands (even within the organization) affects operations. Confidential information is information that should remain private to the company and to certain employees within the company.
- Integrity refers to the accuracy of information and data. Users must keep information accurate and up to date, but more importantly, users should keep information protected to prevent unauthorized people or agencies from tampering with it.
- Availability refers to the accessibility of company information and resources. It is vital that company information and resources be readily available.

Q41) Here are three reasons for a security policy:

- To inform users, staff, and managers of their obligatory requirements for protecting technology and information assets
- To specify the mechanisms through which these requirements can be met
- To provide a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy

Q42) governing policy, technical policies, user policies

Q43) A

Q44) identifying the assets and identifying the threats

Q45) The table shows a completed security analysis matrix.

| System | Description | Risk Level | Types of Users |
|---|---|---|---|
| DNS and DHCP servers | Network applications | Medium | Administrators for configuration;<br>General and privileged users for use |
| External e-mail server | Network application | Low | Administrators for configuration;<br>All others for mail transport between the Internet and the internal mail server |
| Internal e-mail server | Network application | Medium | Administrators for configuration;<br>All other users |
| Oracle database | Network application | Medium or High | Administrators for system internal users for use administration;<br>Privileged users for data updates;<br>General users for data access;<br>All other users for partial data access |

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q46) A good security policy has these four characteristics:

- Can be implemented
- Is enforceable
- Defines roles and responsibilities
- Is documented, distributed, and communicated

Q47) The summary of a blended threat should touch on these points:

- Uses multiple means of propagation
- Has the characteristics of a virus
- Can self-replicate across a network with worm-like ability
- Can search for and exploit a system or application vulnerability or multiple vulnerabilities

Q48) A flash threat exploits new possible unknown vulnerabilities and has the ability to propagate across the Internet in seconds.

Q49) The table identifies the security vulnerability stemming from the listed sources.

| Source | Vulnerability |
|---|---|
| Common application interfaces | Much of the data that used to reside in packet headers now resides in the packet payload. |
| Corporate security policies | In a network supporting end-to-end VPNs, intermediate nodes have no visibility into the traversing traffic. |
| Wireless and mobile network within enterprises | Multihomed hosts establish unplanned wireless networks that enable peer-to-peer communication, allowing packets to be forwarded across devices at the application level. |

Q50) The table identifies the goal of each phase in the evolution of the Cisco Self-Defending Network and identifies the products and technologies associated with each phase.

| Phase | Goal | Products and Technologies |
|---|---|---|
| Phase I | Integrated security | Firewalls, intrusion prevention, and secure connectivity |
| Phase II | Collaborative security systems | NAC, NFP, VoIP, wireless, and service virtualization |
| Phase III | ATD | Application inspection and control; real-time worm, virus, spyware prevention, peer-to-peer communication, and IM control |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module 2

# Securing the Perimeter

## Overview

Traffic from outside a closed network that has a destination inside a closed network will pass through the network perimeter. The routers that are at the network perimeter are an important first step in securing the network. In this lesson, you will learn how to apply your security policy to the perimeter routers; this includes securing administrative access to the router. You will also be introduced to the Cisco Router and Security Device Manager (SDM).

## Module Objectives

Upon completing this module, you will be able to configure routers on the network perimeter with Cisco IOS software security features. This ability includes being able to meet these objectives:

- Explain the importance of developing a security policy for Cisco routers
- Secure Cisco router physical installations and administrative access
- Describe the features and use of the Cisco SDM
- Configure a Cisco router to perform AAA authentication with a local database using Cisco SDM
- Disable unused Cisco router network services and interfaces using Cisco SDM one-step lockdown
- Securely implement management and reporting features of syslog, SSHv2, and SNMPv3
- Explain the best practices for deploying Cisco routers and other perimeter defense products

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

2

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 1

# Applying a Security Policy for Cisco Routers

## Overview

One aspect of network security is ensuring that the network perimeter—the boundary between the inside of a network and the outside—is secure. Traffic will traverse this boundary through a perimeter router. In support of the network security policy, you should also have a router security policy. This policy should address physical security of the router, operating system and configuration security, and, finally, router hardening (which means ensuring that the router itself is protected against attacks).

## Objectives

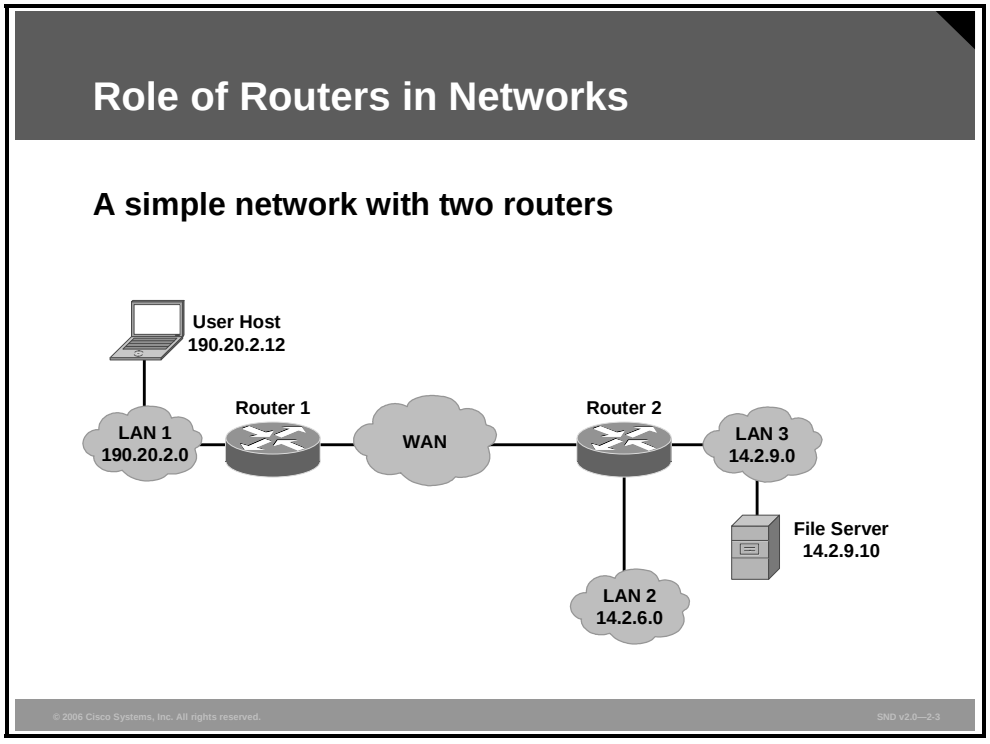
Upon completing this lesson, you will be able to explain the importance of developing a security policy for Cisco routers. This ability includes being able to meet these objectives:

- Describe why the security of routers and their configuration settings is vital to network operation
- Explain the three principles of router security
- Describe how routers enforce a perimeter security policy
- Describe how to provide secure router access for administrators
- Explain why it is important to maintain the most recent versions of Cisco IOS software on network routers
- Explain why logging is an important administrative activity in router management
- Describe the conceptual security layers of a router
- Describe the considerations for developing a security policy for routers
- Describe the recommended approach to applying Cisco IOS security features on network routers

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Role of Routers in Networks

This topic describes why the security of routers and their configuration settings is vital to network operation.




A basic Layer 2 LAN switch connects devices within the same network to form a LAN. A LAN switch makes switching decisions based on Layer 2 MAC addresses. A router routes traffic between different networks based on Layer 3 IP addresses.

When the user host, shown in the figure, sends a message to the file server, it creates a packet with address 14.2.9.10 and passes it to its gateway, router 1. Consulting its internal route table, router 1 forwards the packet to router 2, which consults its own route table before sending the packet over LAN 3 to the file server.

In addition to routing packets, a router may filter traffic. Filtering can protect computers and other network components from illegitimate or hostile traffic.

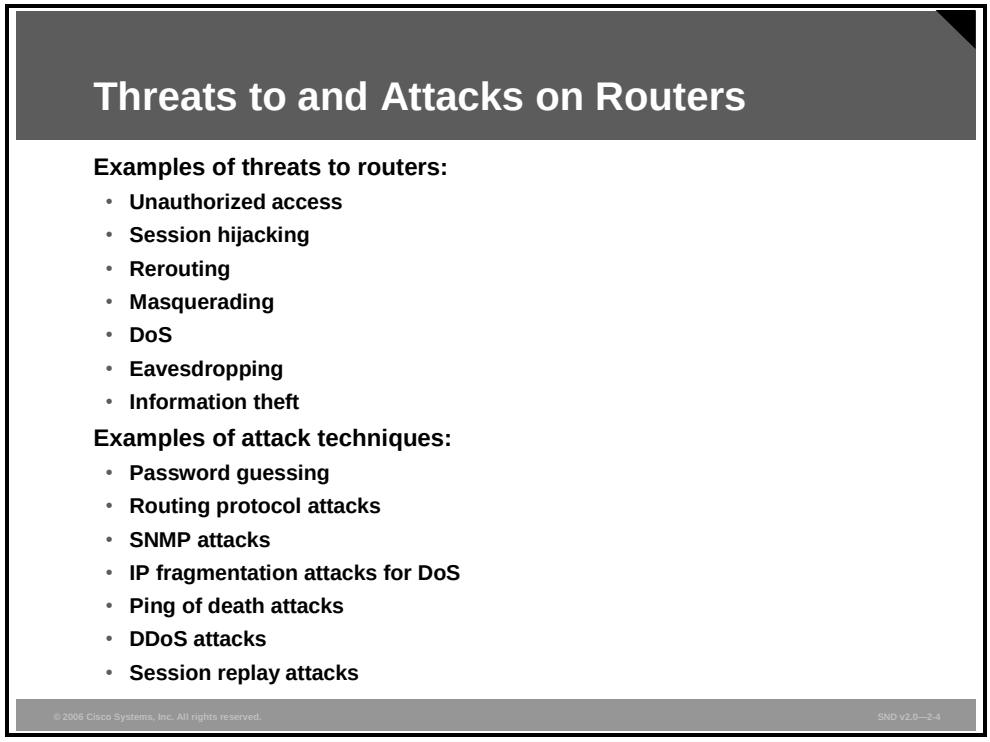
The compromise of a router can lead to various security problems. Here are some examples:

- Compromise of the route tables of a router can result in reduced performance, denial of network communication services, and exposure of sensitive data.
- Compromise of the access control of a router can result in exposure of network configuration details or denial of service (DoS), and can facilitate attacks against other network components.
- A poor router traffic filtering configuration can expose internal network components to scans and attacks and can make it easier for attackers to avoid detection.

In general, well-configured secure routers can greatly improve the overall security posture of a network. A security policy enforced at a router is difficult for negligent or malicious end users to circumvent, thus avoiding a very serious potential source of security problems.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Some general threats to routers include (but are not limited to) unauthorized access, session hijacking, rerouting, masquerading, DoS, eavesdropping, and information theft.

Unauthorized access may occur when one of the following occurs:

- Session hijacking may occur if an attacker can insert falsified IP packets after session establishment via IP spoofing, sequence number prediction and alteration, or other methods.
- Rerouting attacks can include manipulating router updates to cause traffic to flow to unauthorized destinations.
- Masquerade attacks occur when an attacker manipulates IP packets to falsify IP addresses. Masquerades can be used to gain unauthorized access or to inject bogus data into a network.

Here are examples of attack techniques:

- Password guessing can be used as an attempt to access the router management port.
- Routing protocol attacks such as Routing Information Protocol (RIP) attacks where an attacker can forge RIP routing updates to a router to cause the router to forward packets toward the attacker.
- Simple Network Management Protocol (SNMP) attacks are possible because of the numerous vulnerabilities that have been reported in the SNMP implementations of multiple vendors. These vulnerabilities may allow unauthorized privileged access and DoS attacks or cause unstable behavior.
- IP fragmentation attacks can be used to bypass the router traffic filtering. Traditionally, packet filters are only applied to the non-fragments and the initial fragment of an IP packet because they contain both Layer 3 and Layer 4 information that the packet filters can match to a “permit” or “deny” action. Non-initial fragments are traditionally allowed through the packet filters because these fragmented packets do not contain Layer 4 information.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Ping of death attacks involve the creation of an Internet Control Message Protocol (ICMP) echo-request packet that is larger than the maximum packet size of 65,535 bytes. The attacker hopes that the receiving router will crash while attempting to reassemble the packet.
- Distributed denial of service (DDoS) attacks use a number of compromised sites to flood a target site with sufficient traffic or service requests to render it useless to legitimate users.
- Session replay attacks use a sequence of packets or application commands that can be recorded, possibly manipulated, and then replayed to cause an unauthorized action or to gain access.

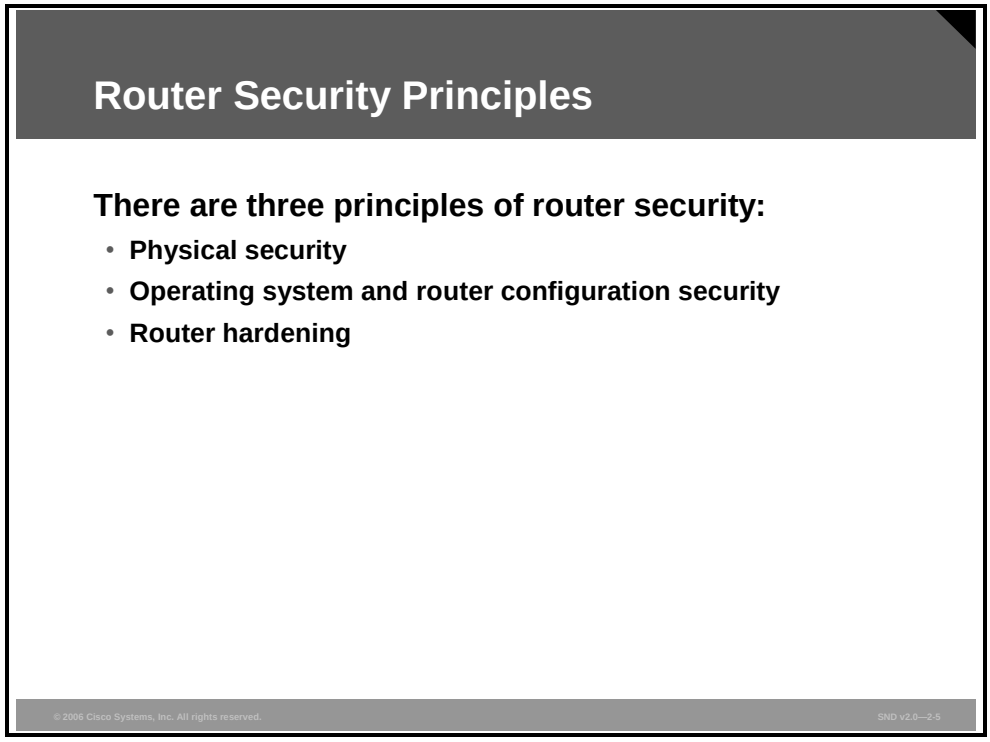
Properly securing a router against these types of attacks will be required to protect the network infrastructure.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Router Security Principles

This topic explains the three principles of router security.




Think about router security in terms of its physical security, the features and performance of the router operating system, the protection of the router configurations, and the elimination of potential abuse of unused ports and services through router hardening. Some specific points to consider about these principles are as follows:

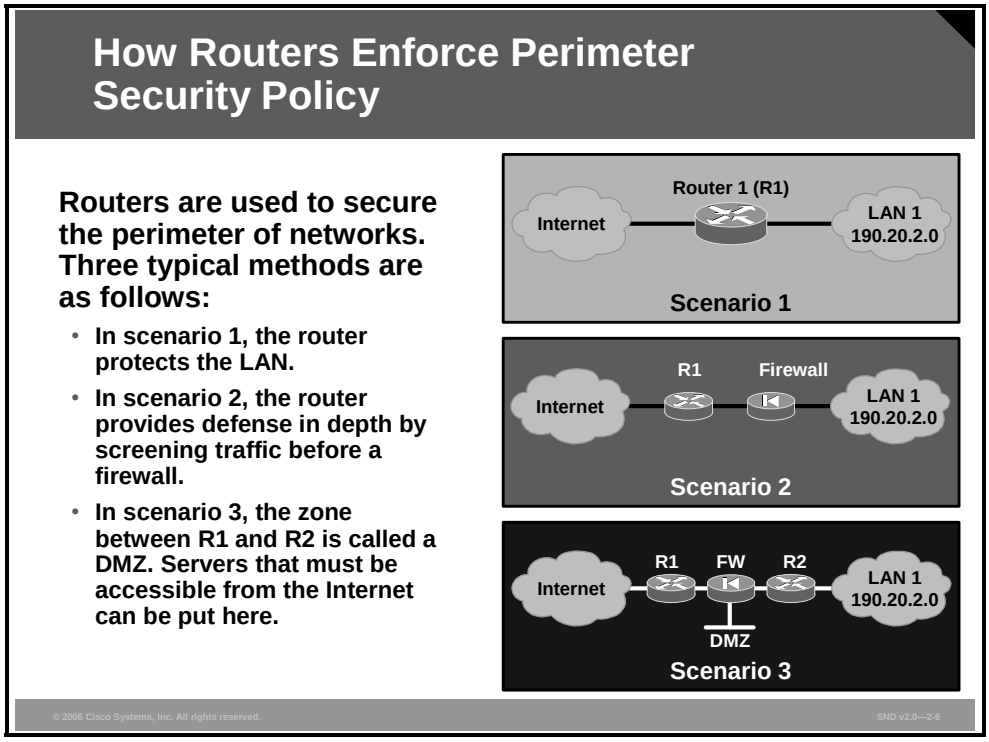
- To provide physical security for a router, take these actions:
  - Place the router in a locked room that is accessible only to authorized personnel, is free of electrostatic or magnetic interference, and has controls for temperature and humidity.
  - Install an uninterruptible power supply and keep spare components available. This reduces the possibility of a DoS attack from power loss to the building.
  - Configure the router with the maximum amount of memory possible. Availability of memory can help protect against some DoS attacks, while supporting the widest range of security services.
  - Store physical devices used to connect to the router in a secure place.
- The security features in an operating system evolve over time; however, the latest version of an operating system may not be the most stable version available. To get the best security performance from your operating system, use the latest stable release that meets the feature requirements of your network. Also, keep a secure copy of the router operating system image and router configuration file as a backup.
- A router is similar to many computers in that it has many services enabled by default. Many of these services are unnecessary and may be used by an attacker for information gathering or for exploitation. You should harden your router configuration by disabling unnecessary services.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# How Routers Enforce a Perimeter Security Policy

This topic describes how routers enforce a perimeter security policy.




A router provides a capability to help secure the perimeter of a protected network. It is a device where security action, based on the security policy of your organization, can be implemented.

To secure a network perimeter, a router can be deployed on its own. Scenario 1 in the figure shows a typical topology with the router being the component that connects the protected network, or internal LAN, to the Internet.

A router can also be used as part of a defense-in-depth approach as shown in scenario 2 in the figure. This approach is preferred to that of using only a router because it is more secure. The router acts as the first line of defense and, in such a deployment, is known as a screening router or perimeter router. It passes all connections intended for the internal LAN to the firewall. The firewall provides additional access control by tracking the state of the connections. The firewall denies the initiation of connections from the outside (untrusted) networks to the inside (trusted) network but allows the internal users to establish connections to the untrusted networks and permit the responses to come back through the firewall. It can also perform user authentication (authentication proxy) where users have to be authenticated before they can gain access to network resources.

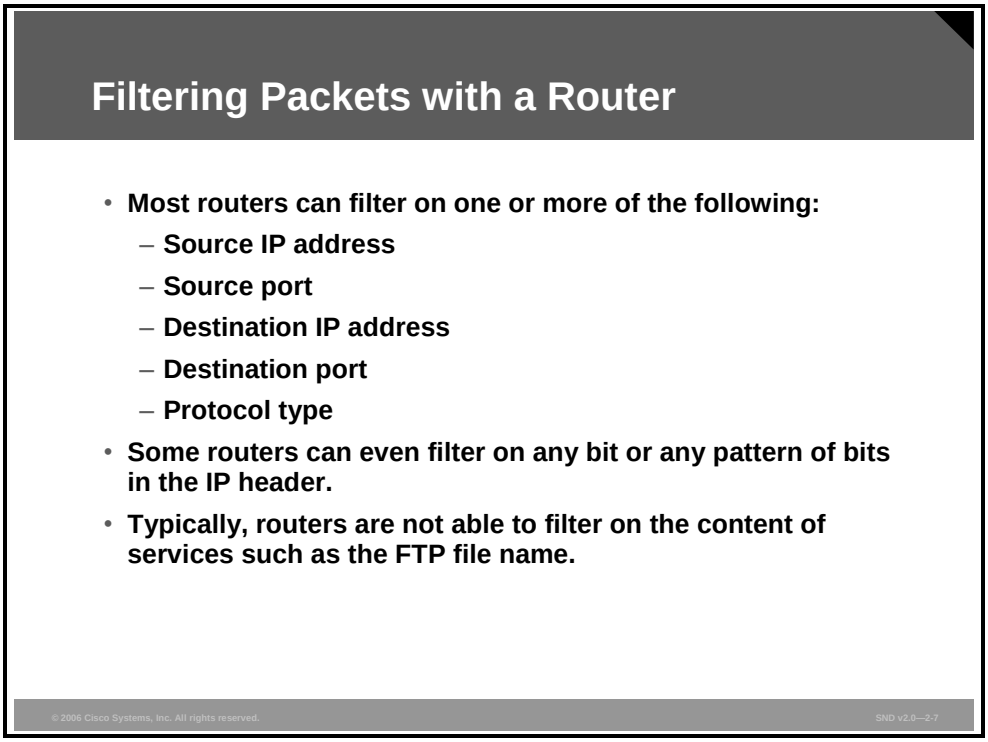
Another approach, shown in scenario 3, is to offer an intermediate area, often called the demilitarized zone (DMZ). The DMZ can be used for servers that must be accessible from the Internet or some other external network. The firewall is set up to permit the required connections (for example, HTTP) from the outside (untrusted) networks to the public servers in the DMZ.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Filtering with a Router

In all three scenarios in the last figure, the router is configured to apply traffic filters. A packet filter for IP services provides control of the data transfer between networks based on IP addresses, protocols, and ports. Some routers have packet filters that apply to network services in both inbound and outbound directions, while others have packet filters that apply only in one direction.




When acting as the gateway between trusted and untrusted networks, packet filters configured on a router can enforce a security policy restricting IP addresses, protocol, and ports according to the security policies of the trusted network.

A filter consists of one or more rules. When the router analyzes a packet against a filter, the packet is compared to each filter rule in the order that the filter was created. If a match is found, the packet is either permitted or denied, and the rest of the filter is ignored. If no match is found, the packet is denied because of the implicit deny rule at the end of the filter. You must carefully create filter rules in the proper order so that all packets are treated according to the intended security policy. One method of ordering involves placing those rules that will handle the bulk of the traffic as close to the beginning of the filter as possible. An example of a packet filter is the access control list (ACL) feature within Cisco IOS software.

Packet filters can also be used to protect against IP address spoofing. In most cases, filtering rules should apply both ingress and egress filtering, including blocking reserved addresses.

## Applying Packet Filters

A packet filter should permit only the required protocols and services. Make a list of the services and protocols that must cross the router and those that the router itself needs for its operation. Create a set of filtering rules that permit the traffic identified on the list and that prohibit all other traffic.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

In cases where only certain hosts or networks need access to particular services, add a filtering rule that permits that service but only for the specific host addresses or address ranges.

A packet filter should deny risky protocols and services. When it is not possible to follow a strict security guideline, you should prohibit services that are commonly not needed, or are known to be popular vehicles for security compromise. The “Example of Vulnerable Services” table lists the services that you could choose to shut down.

Some organizations maintain a list of standard ports and protocols that should be allowed or supported on their networks. For networks that are subject to such lists, it is best to take the first approach, allowing only those ports and protocols on the standard list and rejecting all others.

### Examples of Vulnerable Services

| Port | Transport | Service | Action to Consider |
|---|---|---|---|
| 1 | TCP and UDP | tcpmux | Block completely |
| 7 | TCP and UDP | echo | Block completely |
| 9 | TCP and UDP | discard | Block completely |
| 11 | TCP | systat | Block completely |
| 13 | TCP and UDP | daytime | Block completely |
| 15 | TCP | netstat | Block completely |
| 19 | TCP and UDP | chargen | Block completely |
| 37 | TCP and UDP | time | Block completely |
| 43 | TCP | whois | Block completely |
| 67 | UDP | Bootstrap Protocol (BOOTP) | Block completely |
| 69 | UDP | TFTP | Block completely |
| 79 | TCP | finger | Block from external clients |
| 93 | TCP | SUPDUP | Block completely |
| 111 | TCP and UDP | SunRPC | Block completely |
| 135 | TCP and UDP | loc-srv | Block completely |
| 137 | TCP and UDP | NetBIOS Name Service (NBNS) | Block completely |
| 138 | TCP and UDP | NetBIOS datagram service (NetBIOS-DGM) | Block completely |
| 139 | TCP and UDP | NetBIOS session service (NetBIOS-SSN) | Block completely |
| 161 | TCP and UDP | SNMP | Block from external clients |
| 162 | TCP and UDP | SNMP trap | Block from external clients |
| 177 | UDP | X-Display Manager Client Protocol (XDMCP) | Block completely |
| 445 | TCP | NetBIOS (ds) | Block completely |
| 512 | TCP | UNIX rexec (control) | Block completely |
| 513 | TCP | rlogin | Block from external clients |

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

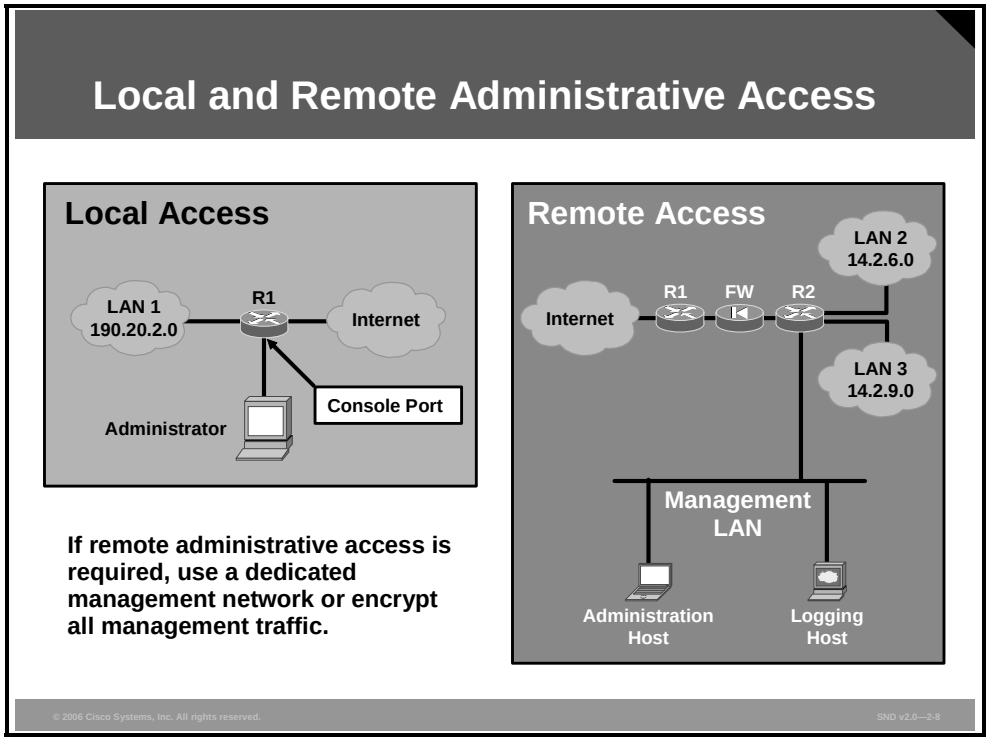
| Port | Transport | Service | Action to Consider |
|---|---|---|---|
| 513 | UDP | whois | Block from external clients |
| 514 | TCP | remote shell protocol (rsh), remote copy protocol (rcp), remote file distribution (rdist) | Block from external clients |
| 514 | UDP | syslog | Block from external clients |
| 515 | TCP | line printer remote (LPR) | Block completely |
| 517 | UDP | talk | Block completely |
| 518 | UDP | ntalk | Block completely |
| 540 | TCP | UNIX-to-UNIX Copy Program (UUCP) | Block completely |
| 1900, 5000 | TCP and UDP | Microsoft UPnP SSDP | Block completely |
| 2049 | UDP | Network File System (NFS) | Block completely |
| 6000–6063 | TCP | Xwindow System | Block completely |
| 6667 | TCP | Internet Relay Chat (IRC) | Block completely |
| 12345 | TCP | NetBus | Block completely |
| 12346 | TCP | NetBus | Block completely |
| 31337 | TCP and UDP | BackOrifice | Block completely |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Local and Remote Administrative Access

This topic describes how to provide secure access for administrators.




Local access usually involves a direct connection to a console port on the router with a dumb terminal or a laptop computer. Remote access typically involves allowing Telnet, Secure Shell (SSH), HTTP, HTTP Secure (HTTPS), or SNMP connections to the router from some computer on the same subnet or on a different subnet.

Ideally, you would only allow local access because some remote access protocols such as Telnet send in clear text to the router. If an attacker can collect network traffic while an administrator is logged in remotely to a router, the attacker can capture passwords or router configuration information. If remote access is required, your options are as follows:

- You can establish a dedicated management network. The management network should include only identified administration hosts and connection to a dedicated interface on an internal router.
- Another method is to encrypt all traffic between the administrator computer and the router. In either case, a packet filter can be configured to only allow the identified administration hosts and protocol to access the router. For example, only permit the administration host IP address to initiate SSH connection to the routers in the network.

In addition to how administrators access the router, there may be a need to have more than one level of administrator or more than one administrative role. Define clearly the capabilities of each level or role in the router security policy. For example, one role might be “network manager,” and administrators authorized to assume this role may be able to view and modify the configuration settings and interface parameters. Another role might be “operators,” and administrators assuming this role might be authorized only to clear connections and counters. In general, it is best to keep the number of fully privileged administrators to a minimum.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

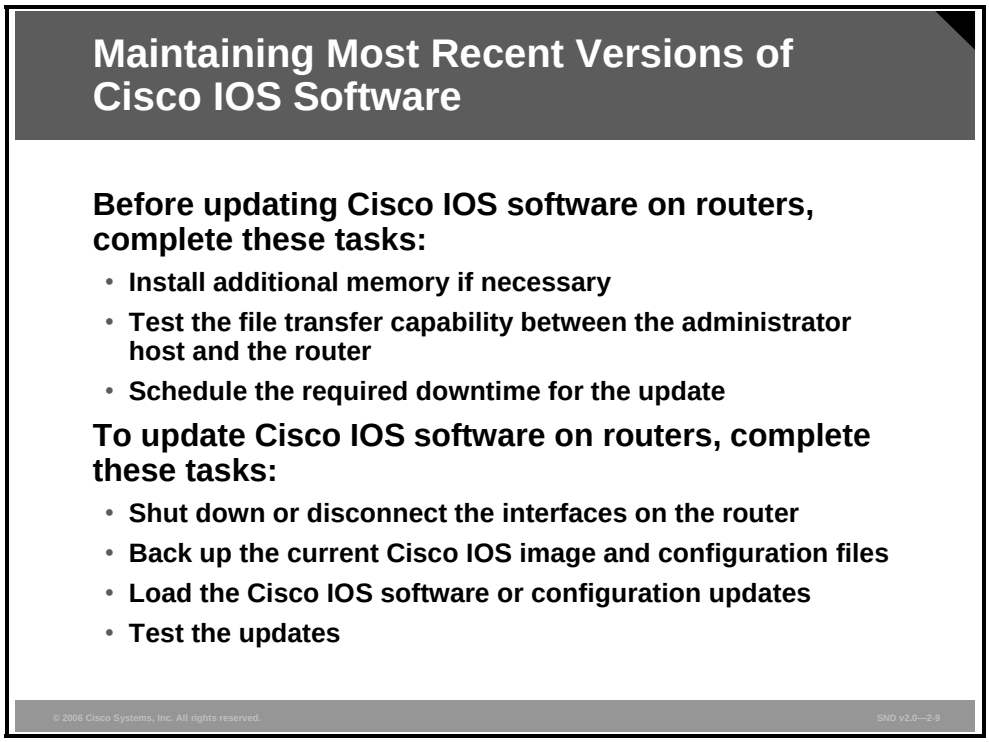
Establishing multiple roles can be accomplished using features such as the Cisco IOS role-based command-line interface (CLI) feature.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Maintaining the Most Recent Versions of Cisco IOS Software

This topic explains why it is important to maintain the most recent versions of Cisco IOS software on network routers.




Periodically, the router will require updates to be loaded for either the operating system or the configuration file. These updates are necessary for one or more of these reasons: to fix known security vulnerabilities, to support new features that allow more advanced security policies, or to improve performance. Before updating, the administrator should complete these tasks:

- Determine the memory required for the update and, if necessary, install additional memory
- Set up and test the file transfer capability between the administrator host and the router
- Schedule the required downtime, normally outside of business hours, for the router to perform the update

After obtaining an update to Cisco IOS software, the administrator should carry out tasks similar to those listed here:

- Shut down the unneeded interfaces on the router not required to perform the update
- Back up the current operating system and the current configuration file to a TFTP server
- Load the update for either the operating system or the configuration file
- Perform tests to confirm that the update works properly (If the tests are successful, re-enable the interfaces on the router; if the tests are not successful, back out the update.)



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

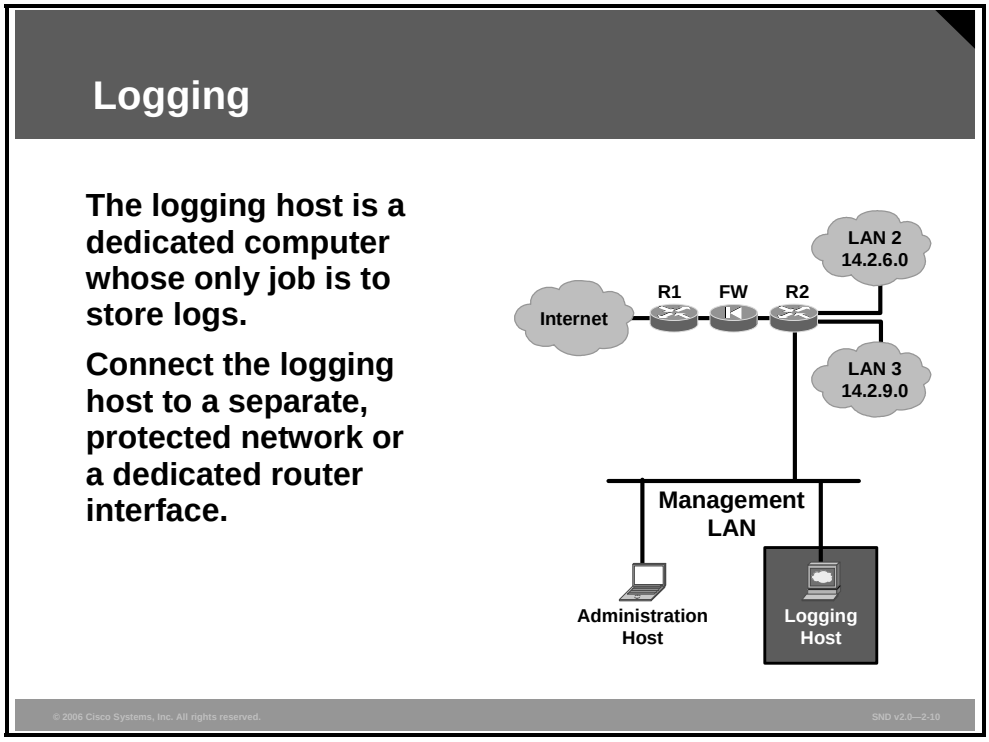
The Cisco IOS resilient configuration feature enables a router to secure and maintain a working copy of the running operating system image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash). A great challenge for network operators is the total downtime experienced after a router has been compromised and its operating software and configuration data erased from its persistent storage. The operator must retrieve an archived copy (if one exists) of the configuration and a working image to restore the router. Recovery must then be performed for each affected router, which adds to the total network downtime.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Logging

This topic explains why logging is an important administrative activity in router management.




Administrators can use logs to verify that a router is working properly or to determine whether the router has been compromised. In some cases, a log can show what types of probes or attacks are being attempted against the router or the protected network.

Configuring logging (syslog) on the router should be done carefully. Send the router logs to a designated log host. The log host should be connected to a trusted or protected network or an isolated and dedicated router interface. Harden the log host by removing all unnecessary services and accounts. Set the level of logging on the router to one that meets the needs of the security policy and expect to modify the log settings as the network evolves. The logging level may need to be modified based on how much of the log information is useful. Two areas that should be logged are matches to filter rules that deny access and changes to the router configuration.

The most important thing to remember about logging is that logs must be reviewed regularly. By checking over the logs periodically, you can gain a feeling for the normal behavior of your network. A sound understanding of normal operation and its reflection in the logs will help you to identify abnormal or attack conditions.

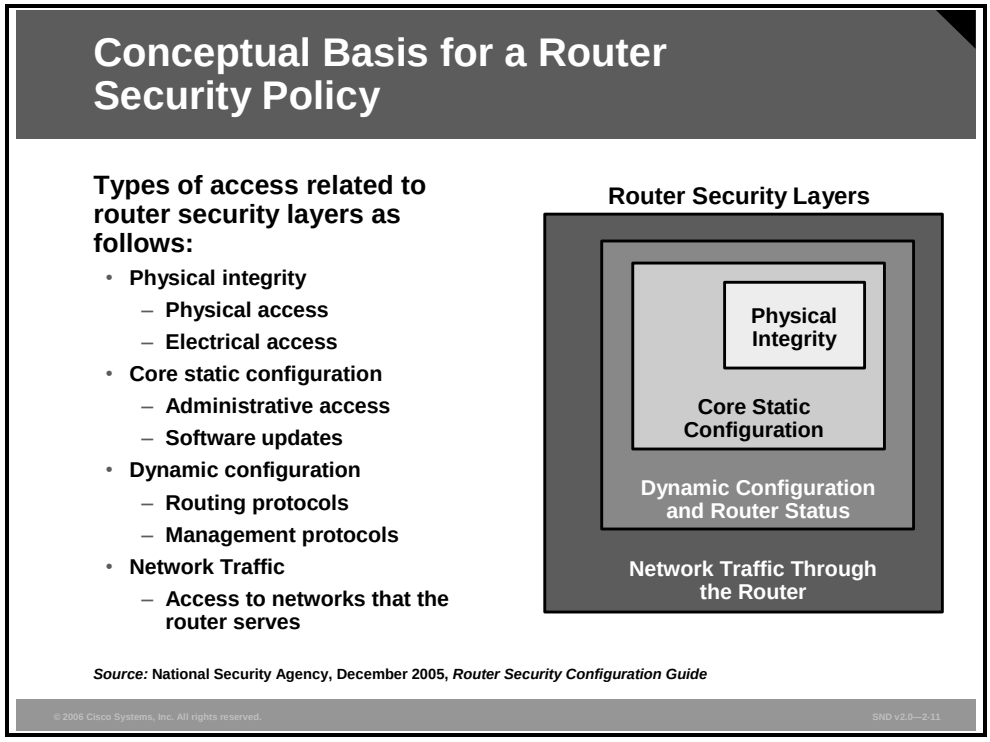
Accurate time stamps are important to logging. All routers are capable of maintaining their own time of day, but this is usually not sufficient. Instead, direct the router to at least two different reliable time servers to ensure the accuracy and availability of time information. Direct the logging host to the reliable time servers. Include a time stamp in each log message. This will allow you to trace network attacks more credibly. Finally, consider also sending the logs to write once, run anywhere (WORA) media or a dedicated printer to deal with worst-case scenarios (for example, compromise of the log host).

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Conceptual Basis for a Router Security Policy

This topic describes the conceptual security layers of a router.




Typically, the network that a router serves will have a security policy, defining roles, permissions, rules of conduct, and responsibilities. The policy for a router must fit into this overall framework. For example, the network security policy might forbid administration of the router from anywhere but the local LAN. The router policy might specify the particular rules to be enforced by the router to prevent remote administration.

A four-zone hierarchy has been developed for managing router security as shown in the figure. The innermost zone is physical integrity. Any router can be compromised by an attacker with full physical access; therefore, physical access must be controlled. The router security policy should define rules for where and how direct connections (usually called console ports or control ports) may be used.

The next zone is the stored software and configuration state of the router itself. If attackers can compromise either of these, they will also gain control of the outer two layers. Some important aspects of the stored configuration are the interface addresses, the usernames and passwords, and the access controls for direct access to the router command interface.

The next zone is the dynamic configuration of the router, which includes the route tables and other dynamic information, such as interface status, Address Resolution Protocol (ARP) tables, and audit logs. If an attacker compromises the router dynamic configuration, the outermost layer will also be compromised.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

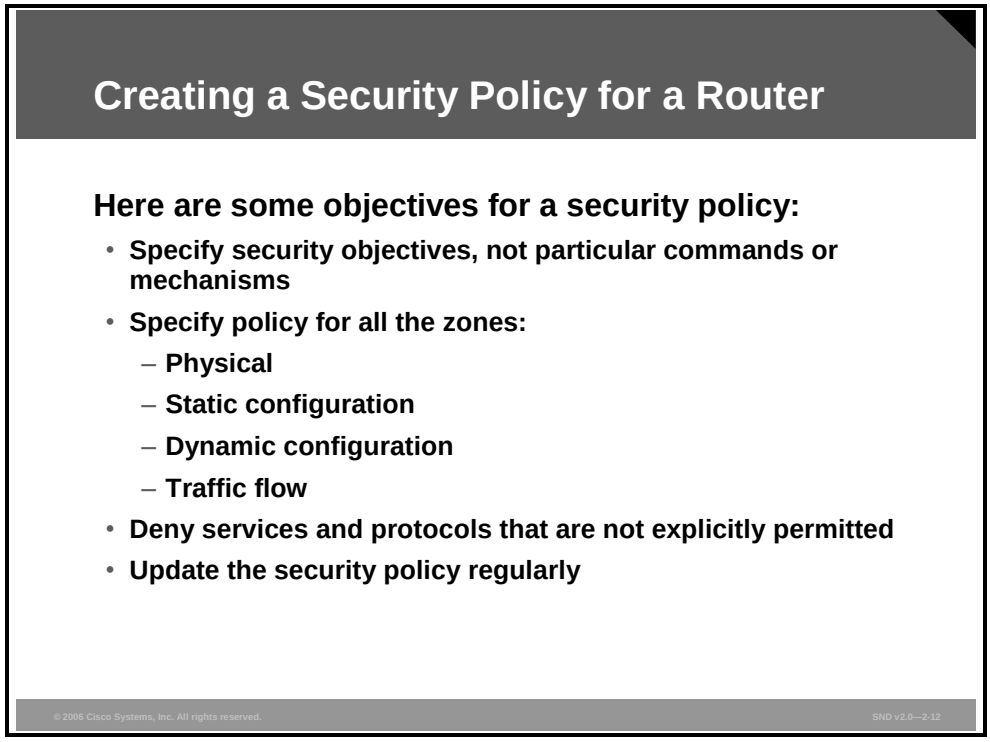
The outer zone of the diagram represents the intranetwork and internetwork traffic that the router manages. The overall network security policy may include rules about this, identifying permitted protocols and services, access mechanisms, and administrative roles. The high-level requirements of the network security policy must be reflected in the configuration of the router and probably in the router security policy.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Creating a Security Policy for a Router

This topic describes the considerations for developing a security policy for routers.




Here are several important tips to remember when creating the security policy for a router:

- **Specify security objectives, not particular commands or mechanisms:** When the policy specifies the security results to be achieved, rather than a particular command or mechanism, the policy is more portable across router software versions and between different kinds of routers. In some cases, it may not be practical to identify and list all the services and protocols that the router will explicitly permit. A backbone router that must route traffic to many other networks cannot always enforce highly tailored policies on the traffic flowing through it because of performance concerns or differences in the security policies of the different networks served. In these kinds of cases, the policy should clearly state any limitations or restrictions that can be enforced. When drafting a policy, keep most of the directives and objectives high level; avoid specifying the particular mechanisms in the policy.
- **Specify policy for all the zones identified in the figure:** Begin with physical security and work outward to security for the static configuration, the dynamic configuration, and for traffic flow.
- **Services and protocols that are not explicitly permitted should be denied:** When representing the network policy in the router policy, concentrate on services and protocols that have been identified as explicitly needed for network operation. Explicitly permit the needs for operation and deny everything else.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

A security policy must be a “living” document. Make it part of security practice to regularly review network security policy and router security policy. Update the router policy to reflect changes in the network security policy and whenever the security objectives for the router change. It may be necessary to revise the router security policy whenever there is a major change in the network architecture or organizational structure. In particular, examine the router security policy and revise it as needed whenever any of these events occur:

- New connections made between the local network and outside networks
- Major changes to administrative practices, procedures, or staff
- Major changes to the overall network security policy
- Deployment of substantial new capabilities (for example, a new virtual private network [VPN]) or new network components (for example, a new firewall)
- Detection of an attack or serious compromise

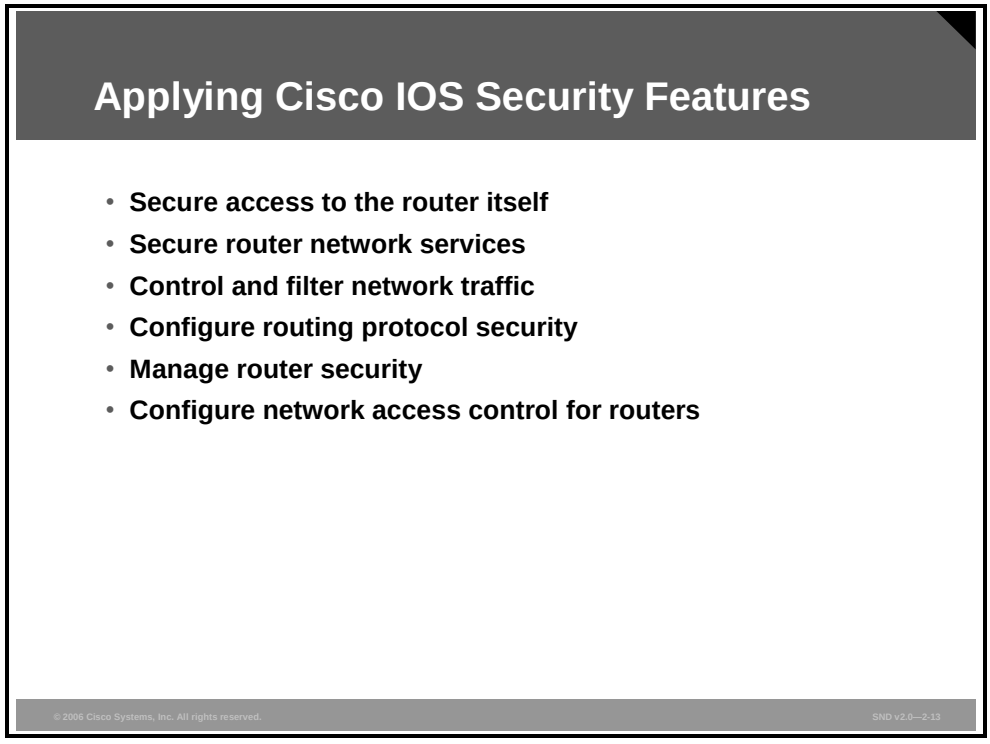
When the router security policy undergoes a revision, notify all individuals authorized to administer the router and all individuals authorized for physical access to it. Maintaining policy awareness is crucial for policy compliance.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Applying Cisco IOS Security Features

This topic describes the recommended approach to applying Cisco IOS security features on network routers.




Before you configure security features on the router, you need a plan for all the Cisco IOS security configuration tasks that you should carry out on your perimeter routers. There are six task groups you should tend to as described in the slide.

- **Secure access to the router itself:** There are several mechanisms used to protect the router itself. These include physical access, user account protection, Cisco IOS image and configuration file protection, remote administration concerns, and configuration issues. When you think about the security of your network, it is important to consider these issues for all your systems, where applicable, and for your routers.
- **Secure router network services:** Cisco routers support a large number of network services at various Open Systems Interconnection (OSI) layers. Some of these services can be restricted or disabled, improving security without degrading the operational use of the router. Some of these services are application layer protocols (such as HTTP, HTTPS, and so on) that allow users and host processes to connect to the router. Other services are automatic processes and settings intended to support legacy or specialized configurations but which are detrimental to security. A general security practice for routers should be to support only traffic and protocols that the network needs.
- **Control and filter network traffic:** Cisco IOS devices use ACLs to separate data traffic into traffic that it will process (permitted packets) and traffic that it will drop and not process (denied packets). Secure configuration of Cisco routers uses ACLs often for restricting access to services on the router itself and for filtering traffic passing through the router.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

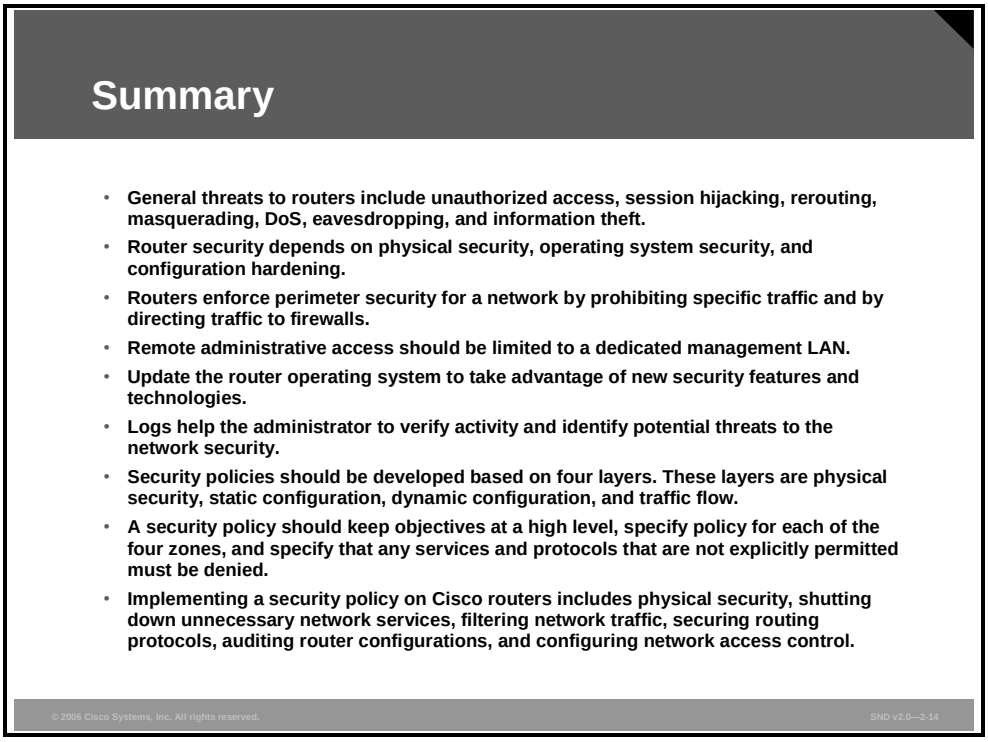
- **Configure routing protocol security:** How can routing protocols be attacked? Attackers who send false routing update packets to an unprotected router can easily corrupt the route table of the router and reroute network traffic in any manner that they desire. The key to preventing such an attack is to protect the route tables from unauthorized and malicious changes by either using static routes or by authenticating the routing updates. Once again, in keeping with a standard security theme, you should also disable all unneeded routing-related services.
- **Manage router security:** Careful management and diligent audit of router operations can reduce network downtime, improve security, and aid in the analysis of suspected security breaches. Cisco routers and Cisco IOS devices are designed to support centralized auditing and management.
- **Configure network access control for routers:** Configure Cisco authentication, authorization, and accounting (AAA) services for controlling access to a router.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Lesson 2

# Securing Administrative Access to Cisco Routers

## Overview

This lesson shows you how to secure Cisco routers using proven methods for physically securing the router and protecting the router administrative access.

## Objectives

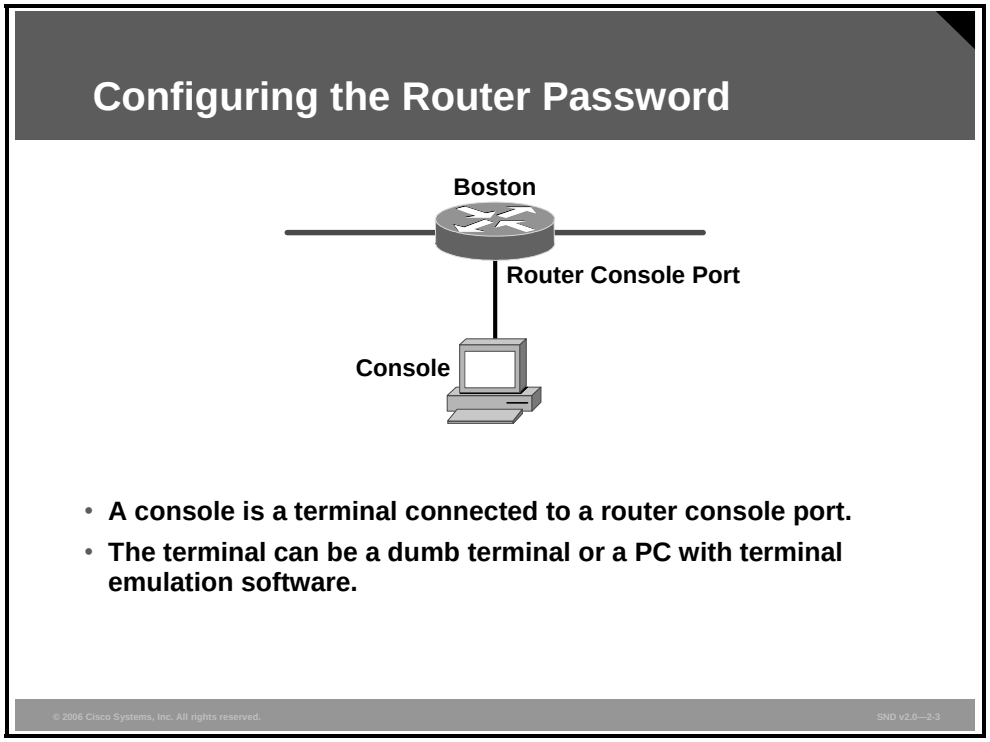
Upon completing this lesson, you will be able to secure Cisco router physical installations and administrative access. This ability includes being able to meet these objectives:

- Explain how to configure passwords to secure administrative access to Cisco routers
- Explain how to secure administrative access to Cisco routers by setting a login failure rate and using Cisco IOS login enhancements
- Explain how to secure administrative access to Cisco routers by setting EXEC timeouts
- Explain how to secure administrative access to Cisco routers using multiple privilege levels
- Explain how to configure the role-based CLI access feature to provide views
- Explain how to use the Cisco IOS resilient configuration feature to secure the Cisco IOS image and configuration file
- Explain how to configure better security for virtual login connections
- Explain how to secure administrative access to Cisco routers by configuring banner messages

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Configuring Router Passwords

This topic describes how to configure secure administrative access to Cisco routers by configuring passwords.




Configuring secure administrative access is an extremely important security task. If an unauthorized person were to gain administrative access to a router, the person could alter routing parameters, disable routing functions, or discover and gain access to other systems in the network.

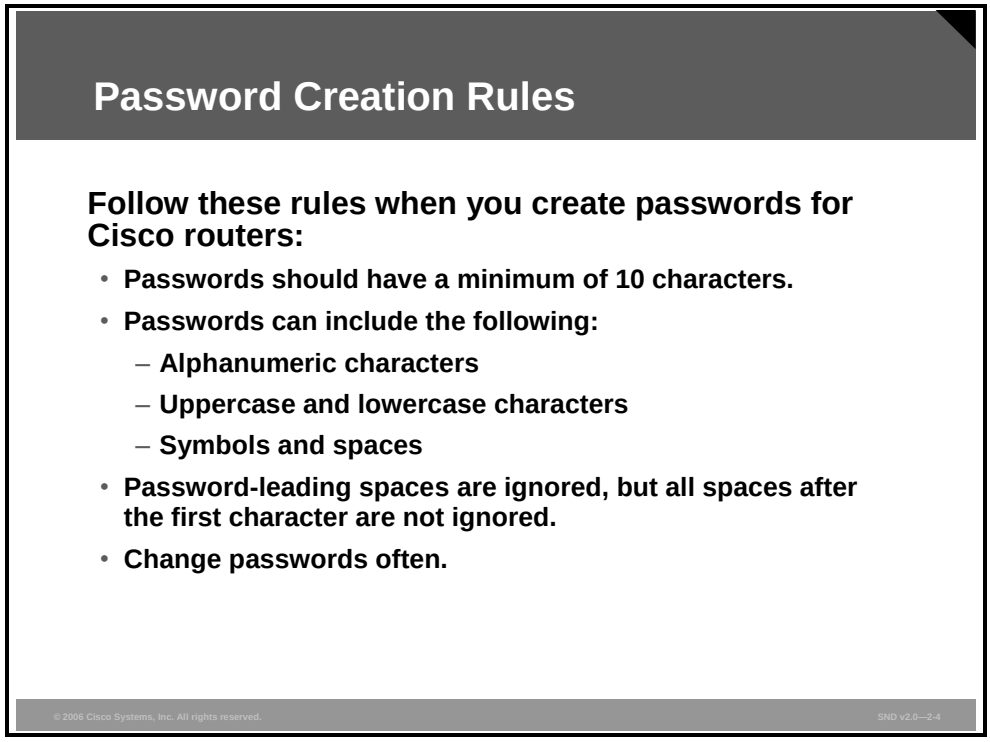
Strong passwords and similar secrets, such as Simple Network Management Protocol (SNMP) community strings, are the primary defense against unauthorized access to your router. The best way to handle most passwords is to maintain them on a TACACS+ or RADIUS authentication server such as the Cisco Secure Access Control Server (ACS). However, routers can have locally configured passwords for privileged access and may also have other password information in their configuration files.

One way to perform initial router configuration tasks is to access the router console port with a console connected to that port. The console you use for this task can be either a dumb terminal or a PC running terminal emulation software. Consoles are only one of the ways that network administrators can obtain administrative access to configure and manage routers. Other ways to gain administrative access include Telnet, Secure Shell (SSH), SNMP, or using HTTP or HTTP Secure (HTTPS) to access the Cisco Router and Security Device Manager (SDM) feature.

The first step in securing Cisco router administrative access is to configure secure system passwords. These passwords are either stored in the router itself (local) or on remote authentication, authorization, and accounting (AAA) servers, such as the Cisco Secure ACS. This topic contains information on configuring local passwords only.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



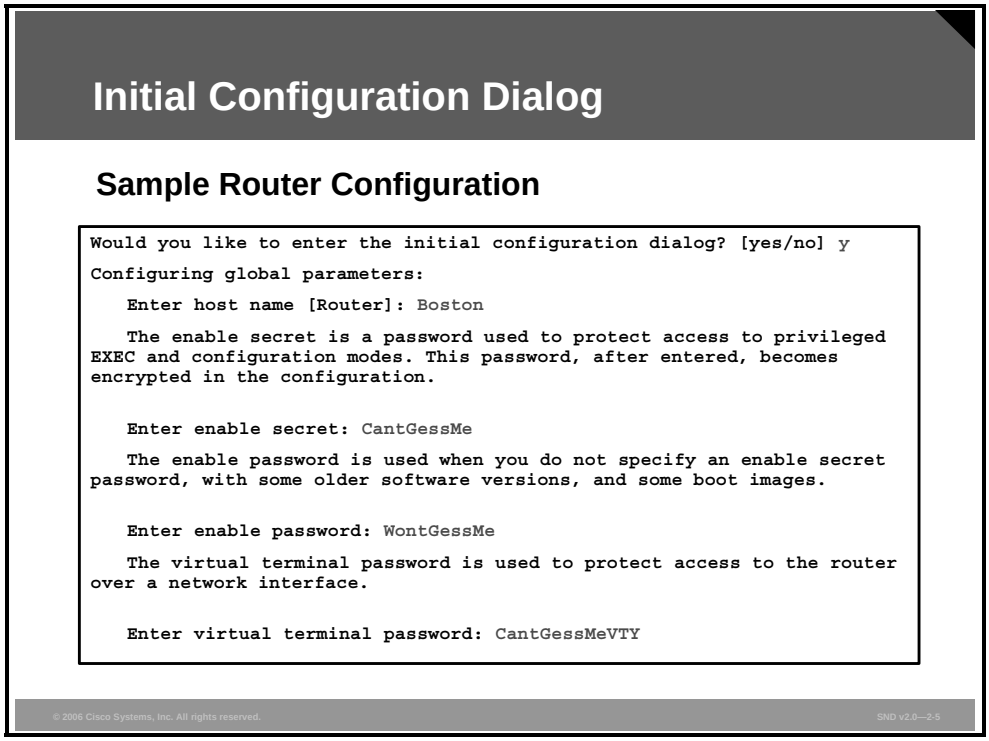

When creating passwords for Cisco routers, always keep these rules in mind:

- It is best to have a minimum of 10 characters for a password. Passwords may include the following:
  - Any alphanumeric character
  - A mix of uppercase and lowercase characters
  - Symbols and spaces
- Passwords should not use dictionary words.
- Password-leading spaces are ignored, but all spaces after the first character are not ignored.
- You should decide when and how often the passwords will be changed.

You may want to add your own rules to this list to make your passwords even safer.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




If you are working on a new router (from the factory) or an existing router that has been reset (possibly using the Cisco password-recovery procedure), you are prompted by the Cisco IOS command-line interface (CLI) when you want to enter the initial configuration dialog. The figure provides a router configuration sample with this initial prompt.

Within the first few questions of the initial configuration dialog, several Cisco router password requirements can be found.

- The router enable secret password
- The router enable password
- The password used to access the router using vty (Telnet)

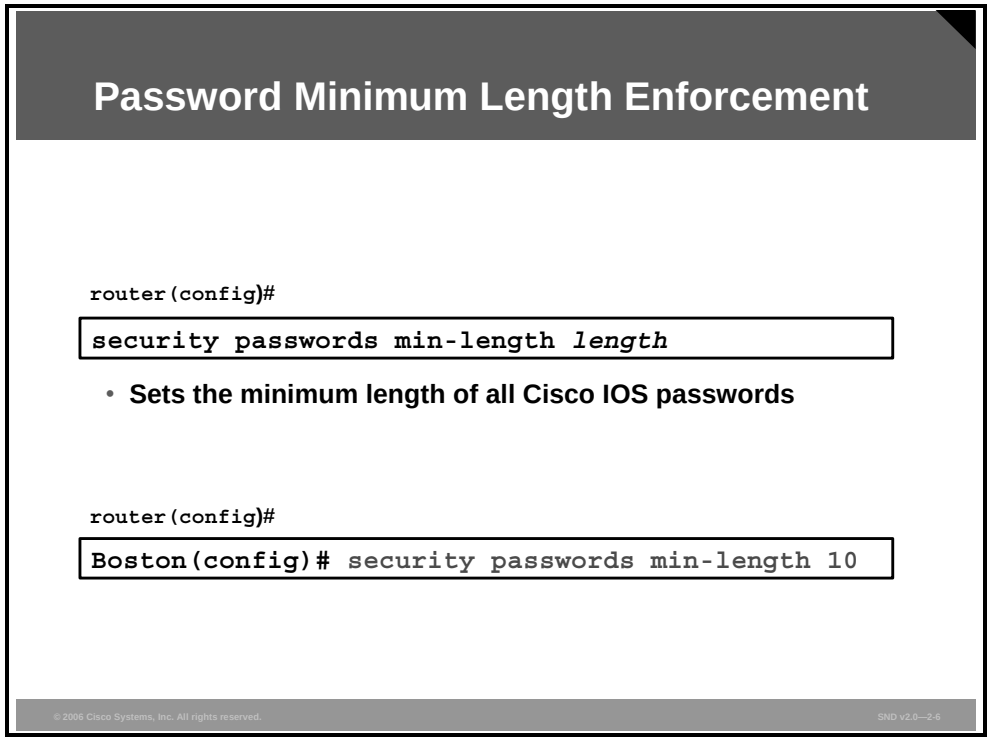
The enable secret password is used to enter enable mode (sometimes referred to as privileged or privileged EXEC mode). You can set the enable secret password by entering a password during the initial configuration dialog (as shown in the figure), or by using the **enable secret** command in global configuration mode. The enable secret password is always encrypted inside the router configuration using a Message Digest 5 (MD5) hashing algorithm.

The **enable password** command is also used to enter enable mode, but it is from older versions of Cisco IOS software. By default, the enable password is not encrypted in the router configuration. Cisco decided to keep the older **enable password** command in later versions of Cisco IOS software even though enable secret password is a safer way to store privileged EXEC passwords. The older command was kept in case the router is downgraded to a version of Cisco IOS software that did not support an enable secret password. The enable password protects the privileged EXEC administrative router access.

The vty password is the line-level password entered when connecting to the router using Telnet. You can set this password during the initial configuration dialog (as shown in the figure) or by using the **password** command in vty configuration mode.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Cisco IOS Release 12.3(1) and later allows administrators to set the minimum character length for all router passwords using the **security passwords** global configuration command. This command provides enhanced security access to the router by allowing you to specify a minimum password length (0 to 16 characters); this eliminates common passwords that are short and prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords created after the command was executed. Existing router passwords remain unaffected.

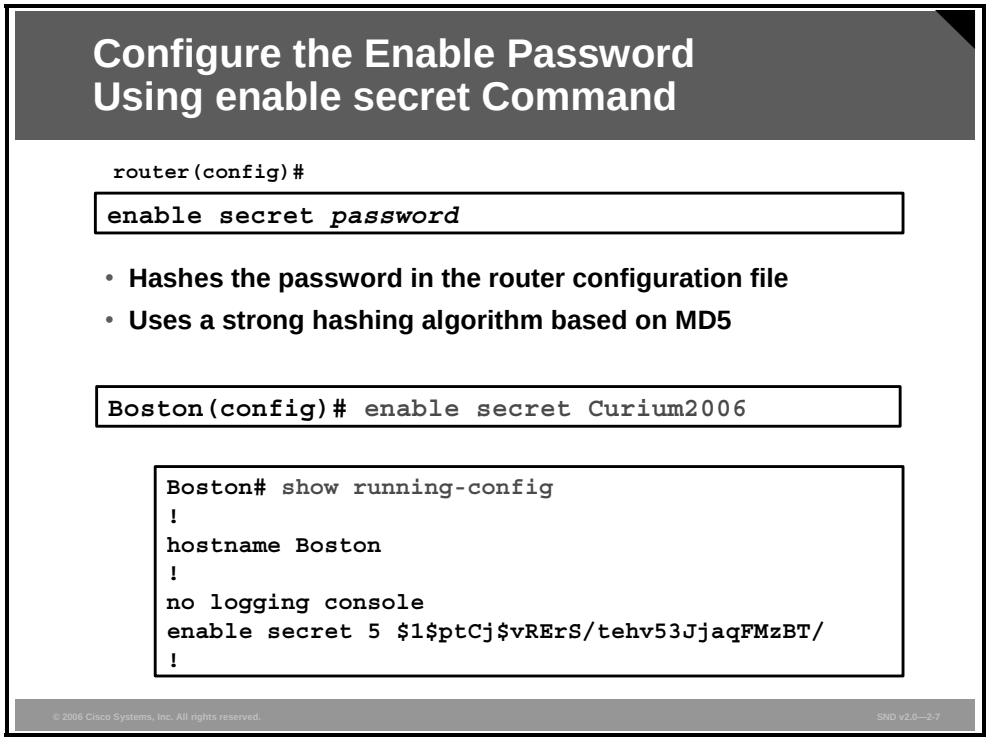
It is highly recommended that you set your minimum password length to at least 10 characters. Never use a length of zero.

After this command is enabled, any attempt to create a new password that is less than the specified length fails and results in an error message similar to this message:

```
Password too short - must be at least 10 characters. Password
configuration failed.
```



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



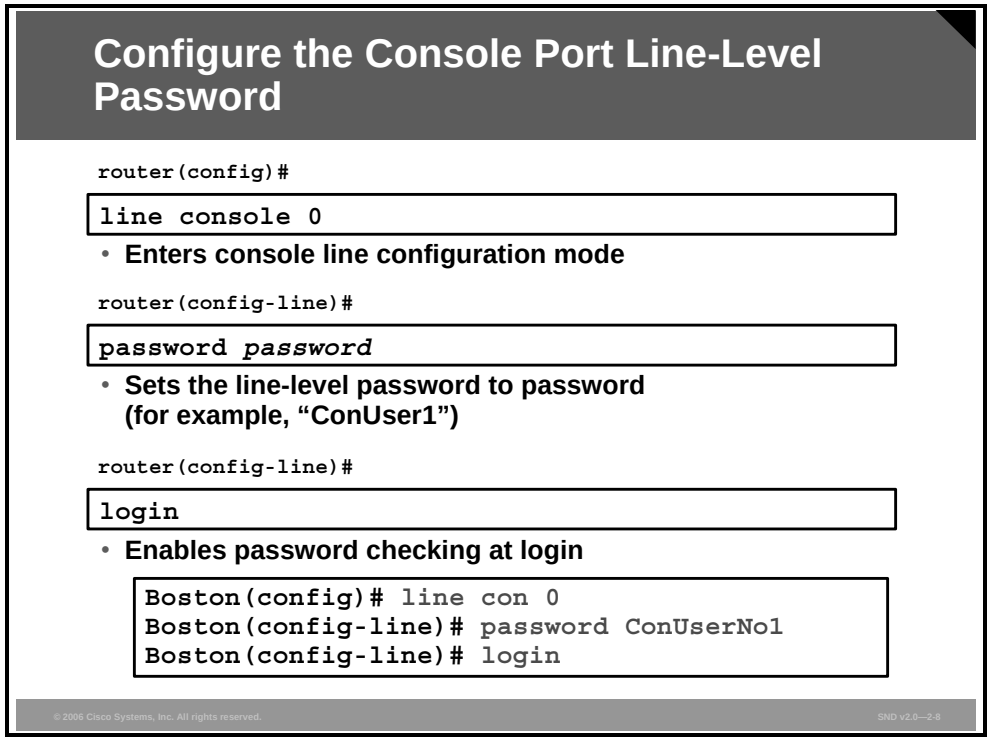

If you did not use the initial configuration dialog to configure your enable secret password, you must use the **enable secret** command in global configuration mode as shown in the figure. The **enable secret** command uses a one-way encryption hash based on MD5 (designated by the number 5 in the sample configuration) and is considered irreversible by most cryptographers. However, even this type of encryption is still vulnerable to brute-force attacks or dictionary attacks.

If you forget the enable secret password, you have no alternative but to replace it using the Cisco router password recovery procedure.

The enable secret password can also be configured using the Cisco SDM GUI configuration tool.



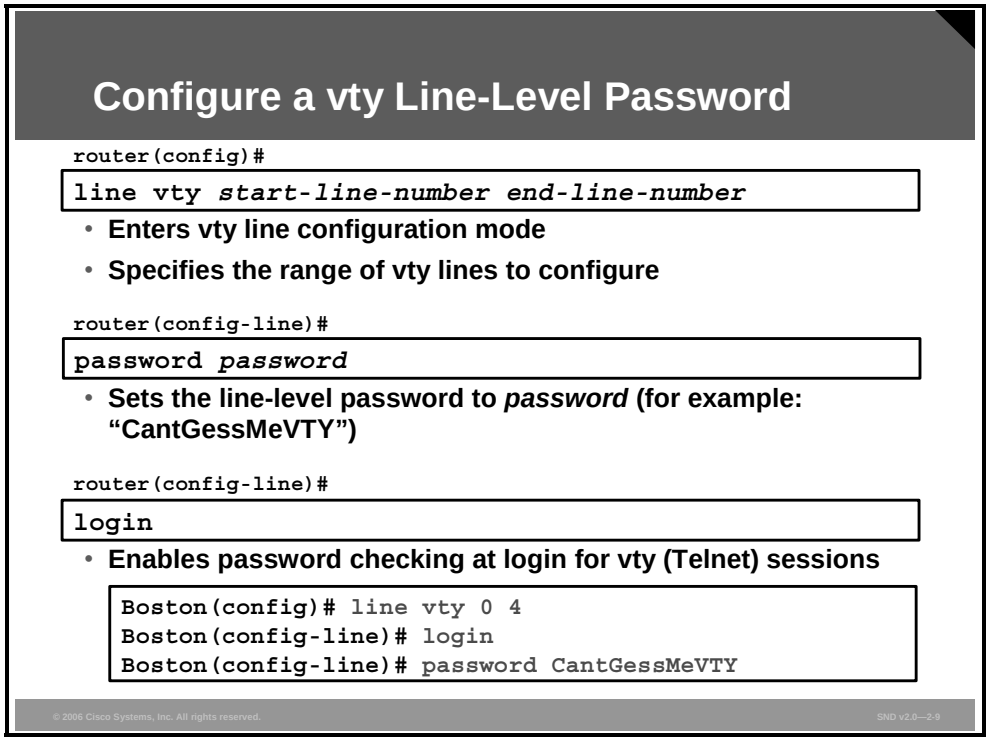
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




By default, the console port does not require a password for console administrative access. However, you should always configure a console port line-level password. The figure illustrates the steps (in global configuration mode) that are required to create a new line-level password for the console.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Cisco routers support multiple Telnet sessions (up to five simultaneous sessions by default, and more can be added), each serviced by a logical vty line. By default, Cisco routers do not have any line-level passwords configured for these vty lines. If you enable password checking, you must also configure a vty password before attempting to access the router using Telnet. If you fail to configure a vty password and password checking is enabled for the vty lines, you will encounter an error message similar to this message:

```
Telnet 10.0.1.2
Trying 10.0.1.2 ….. open

Password required, but none set

[Connection to 10.0.1.2 closed by foreign host]
```

There are two ways to configure a vty password. The first way is to enter the password during the initial configuration dialog. The second way is by using the **password** command in vty configuration mode, as shown in the figure. Always configure passwords for all of the vty ports in this manner.

In the example shown in the figure, vty 0 4 (logical vty 1 to vty 5) are configured simultaneously to look for the password specified. Just like console line-level passwords, vty passwords are, by default, shown as clear text (unencrypted) in the router configuration.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Here are things to consider when securing Telnet connections to a Cisco router:

- If you fail to set an enable password for the router, you will not be able to access privileged EXEC mode using Telnet. Use either the **enable** *password* or **enable secret** *password* command to set the enable password for your routers.
- Telnet access should be limited only to specified systems by building a simple access control list (ACL) that does the following:
  - — Allows Telnet access from specific hosts only (allows certain IP addresses)
  - — Blocks Telnet access from specific untrusted hosts (disallows certain IP addresses)
  - — Ties the ACL to the vty lines using the **access-class** command

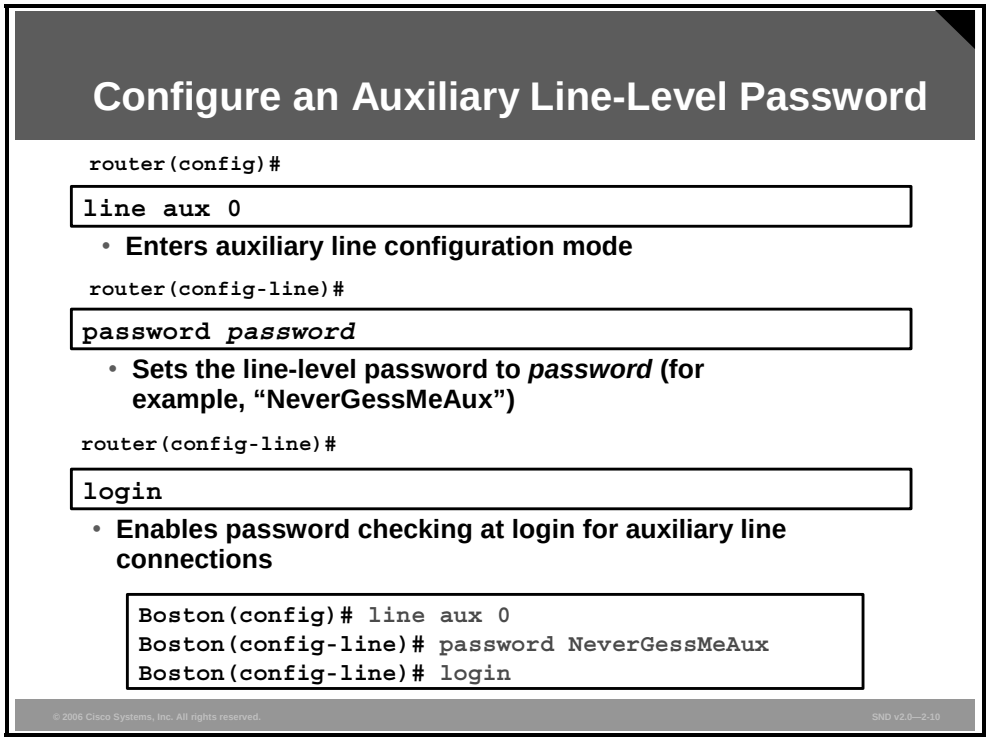
  Here is an example showing ACL 30 restricting Telnet access only from host 10.0.1.1 and denying access from any other hosts (implicit deny) for vty 0 to 4:

```
Boston(config)# access-list 30 permit 10.0.1.1
Boston(config)# line vty 0 4
Boston(config-line)# access-class 30 in
```

- You must configure passwords for each vty on the router. Remember that you can add more vtys to the router, and these lines and the default 0 to 4 lines must be protected.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




By default, Cisco router auxiliary ports do not require a password for remote administrative access. Administrators sometimes use this port to remotely configure and monitor the router using a dial-up modem connection.

Unlike console and vty passwords, the auxiliary password is not configured during the initial configuration dialog and should be configured, as shown in the figure, using the **password** command in auxiliary line configuration mode.

If you wish to turn off the EXEC process for a specified line such as on the auxiliary port, use the **no exec** command within the auxiliary line configuration mode.

Setting the auxiliary line-level password is only one of several steps you must complete when configuring a router auxiliary port for remote dial-in access.

The "Configuring an Auxiliary Line-Level Password" table lists the steps and commands used when configuring an auxiliary port.


© 2006 Cisco Systems, Inc.

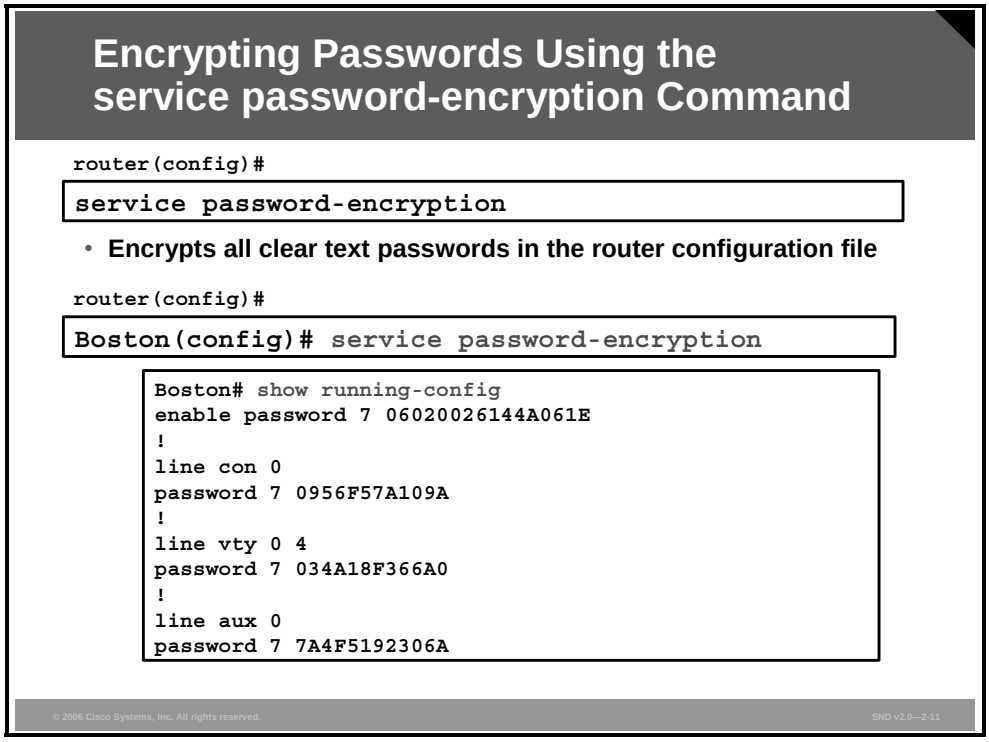
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Configuring an Auxiliary Line-Level Password

| Step | Action | Notes |
|---|---|---|
| **1.** | `Boston(config)# line aux 0`<br>`Boston(config-line)# modem inout` | These commands permit incoming and outgoing modem calls on the specified line. |
| **2.** | `Boston(config-line)# speed 9600` | This command specifies the line speed that should be used to communicate with the modem. |
| **3.** | `Boston(config-line)# transport input all` | This command allows all protocols to use the line. |
| **4.** | `Boston(config-line)# flowcontrol hardware` | This command enables Request To Send (RTS) and Clear To Send (CTS) flow control. |
| **5.** | `Boston(config-line)# login` | These commands authenticate incoming connections using the password configured on the line (the password is configured in Step 6). |
| **6.** | `Boston(config-line)# password NeverGessMeAux` | This command configures the password “NeverGessMeAux” to authenticate incoming calls on the specified line. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Just like console and vty passwords, auxiliary passwords are not encrypted in the router configuration. This is why it is important to use the **service password-encryption** command.

With the exception of the enable secret password, all Cisco router passwords are, by default, stored in clear text form within the router configuration. View these passwords with the **show running-config** command. Sniffers can also see these passwords if your TFTP server configuration files traverse an unsecured intranet or Internet connection. If an intruder gains access to the TFTP server where the router configuration files are stored, the intruder will be able to obtain these passwords.

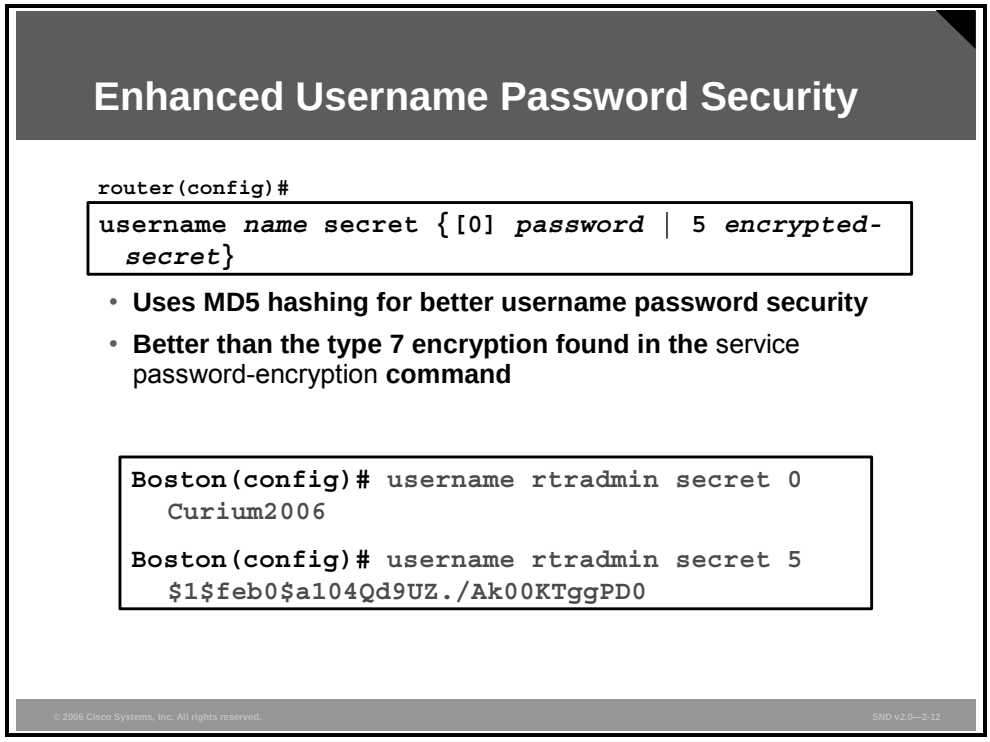
A proprietary Cisco algorithm based on a Vigenere cipher (indicated by the number 7 when viewing the configuration) allows the **service password-encryption** command to encrypt all passwords (except the previously encrypted enable secret password) in the router configuration file. This method is not as safe as MD5, which is used with the **enable secret** command, but prevents casual discovery of the router line-level passwords.

**Note** The encryption algorithm in the **service password-encryption** command is considered relatively weak by most cryptographers, and several Internet sites post mechanisms for cracking this cipher. This posting only proves that relying on the encrypted passwords alone is not sufficient security for your Cisco routers. You need to ensure that the communications link between the console and the routers, or between the TFTP or management server and the routers, is a secured connection. Securing this connection is discussed in the "Configuring Enhanced Support for Virtual Logins" topic.

After all of your passwords have been configured for the router, you should run the **service password-encryption** command in global configuration mode, as shown in the figure.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Cisco routers can maintain a list of usernames and passwords for performing local login authentication.

Starting with Cisco IOS Release 12.0(18)S, system administrators can choose to use an MD5 hashing mechanism to encrypt a user password. MD5 hashing of passwords is a much better encryption scheme than the standard type 7 encryption found in the **service password-encryption** command. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

MD5 hashing of a Cisco IOS user password is accomplished with the **username secret** command in global configuration mode. Administrators can choose to enter a clear text password for MD5 hashing by the router (option 0), or they can enter a previously encrypted MD5 secret (option 5). The syntax for the **username secret** command is as follows:

**username** *name* **secret** {[0] *password* | 5 *encrypted-secret*}

| Command Element | Description |
|---|---|
| *name* | The username |
| **0** | (Optional) Indicates that the clear text password is to be hashed using MD5 |
| *password* | The clear text password to be hashed using MD5 |
| **5** | Indicates that the encrypted-secret password was hashed using MD5 |
| *encrypted-secret* | The MD5 encrypted-secret password that will be stored as the encrypted user password |

**Note** MD5 encryption is a strong encryption method that is not retrievable; therefore, you cannot use MD5 encryption with protocols that require clear text passwords, such as Challenge Handshake Authentication Protocol (CHAP).



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Securing ROMMON with the no service password-recovery Command

```
router(config)#
no service password-recovery
```

- **By default, Cisco routers are factory configured with service password-recovery set.**
- **The no version prevents console from accessing ROMMON.**

```
Boston(config)# no service password-recovery

WARNING:

Executing this command will disable password recovery
   mechanism. Do not execute this command without
   another plan for password recovery.

Are you sure you want to continue? [yes/no]: yes

Boston(config)#
```

© 2006 Cisco Systems, Inc. All rights reserved.


By default, Cisco IOS routers allow a break sequence during startup that forces the router into ROM monitor (ROMMON) mode. Once the router is in ROMMON mode, anyone can choose to enter a new secret password using the well-known Cisco password recovery procedure. This procedure, if performed correctly, leaves the router configuration intact. This scenario presents a potential security breach because anyone who gains physical access to the router console port can enter ROMMON, reset the enable secret password, and discover the router configuration.

This potential security breach can be mitigated using the **no service password-recovery** global configuration command. The **no service password-recovery** command is a hidden Cisco IOS command and has no arguments or keywords.

**Caution** If a router is configured with the **no service password-recovery** command, all access to the ROMMON is disabled. If the router flash memory does not contain a valid Cisco IOS image, you will not be able to use the **rommon xmodem** command to load a new flash image. To repair the router, you must obtain a new Cisco IOS image on a flash SIMM or on a Personal Computer Memory Card International Association (PCMCIA) card (3600 only). Refer to Cisco.com for more information regarding backup flash images.

Once the **no service password-recovery** command is executed, the router boot sequence will look similar to the following:

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
C2600 platform with 65536 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80008000, size: 0xed9ee4
```



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Also, after the **no service password-recovery** command is executed, a **show running configuration** command listing will contain the **no service password-recovery** statement as shown here:

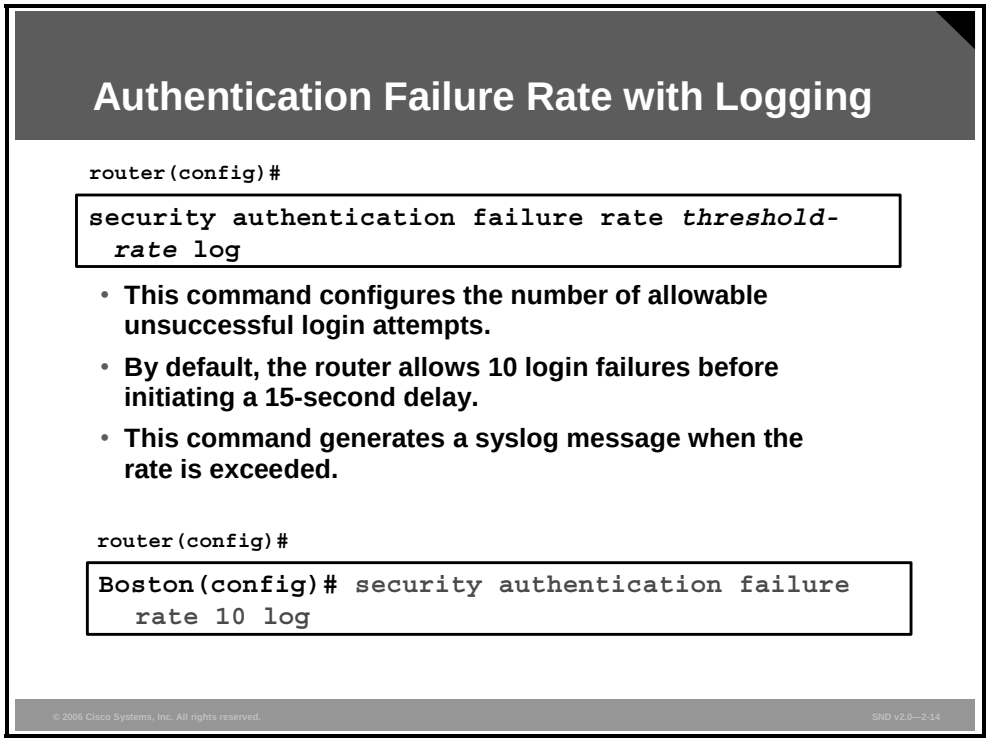
```
!
version 12.0
service tcp-keepalives-in
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service password-recovery
!
hostname Boston
```



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Setting a Login Failure Rate

This topic describes how to secure administrative access to Cisco routers by setting a login failure rate.




Starting with Cisco IOS Release 12.3(1), system administrators can configure the number of allowable unsuccessful login attempts using the **security authentication failure rate** global configuration command, as shown in the slide.

When the number of failed login attempts reaches the configured rate, these two events occur:

- A **TOOMANY_AUTHFAILS** event message is sent by the router to the configured syslog server.
- A 15-second delay timer starts.

Once the 15-second delay has passed, the user may continue to attempt to log in to the router.

The syntax for the **security authentication failure rate** command is as follows:

**security authentication failure rate** *threshold-rate* **log**

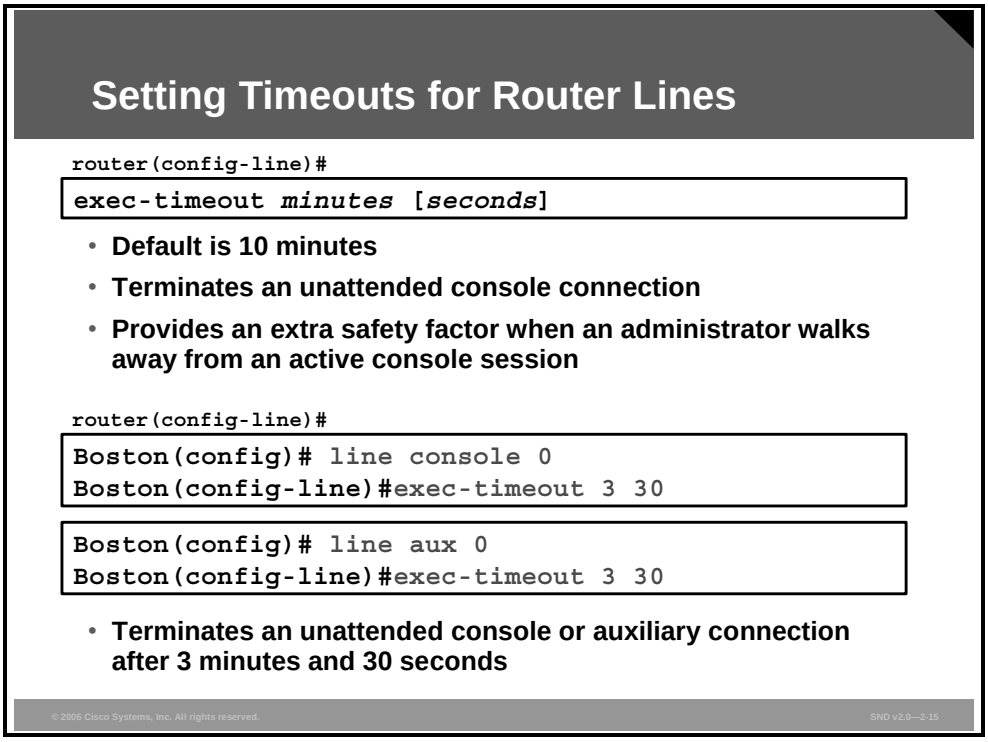
| Command Element | Description |
|---|---|
| *threshold-rate* | This is the number of allowable unsuccessful login attempts. The default is 10 (the range is 2 to 1024). |
| **log** | The **log** keyword is required. This command must result in a generated syslog event. |


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Setting Timeouts

This topic describes how to secure administrative access to Cisco routers by setting timeouts.




By default, an administrative interface stays active (and logged in) for 10 minutes after the last session activity. After that, the interface times out and logs out of the session. It is recommended that you fine-tune these timers to limit the amount of time to within a 2- or 3-minute maximum.

You can adjust these timers using the **exec-timeout** command in line configuration mode for each of the line types used.

The syntax for the **exec-timeout** command is as follows:

**exec-timeout** *minutes* [*seconds*]

| Command Element | Description |
|---|---|
| *minutes* | This integer specifies the number of minutes. |
| *seconds* | (Optional) This integer specifies the additional time interval in seconds. |

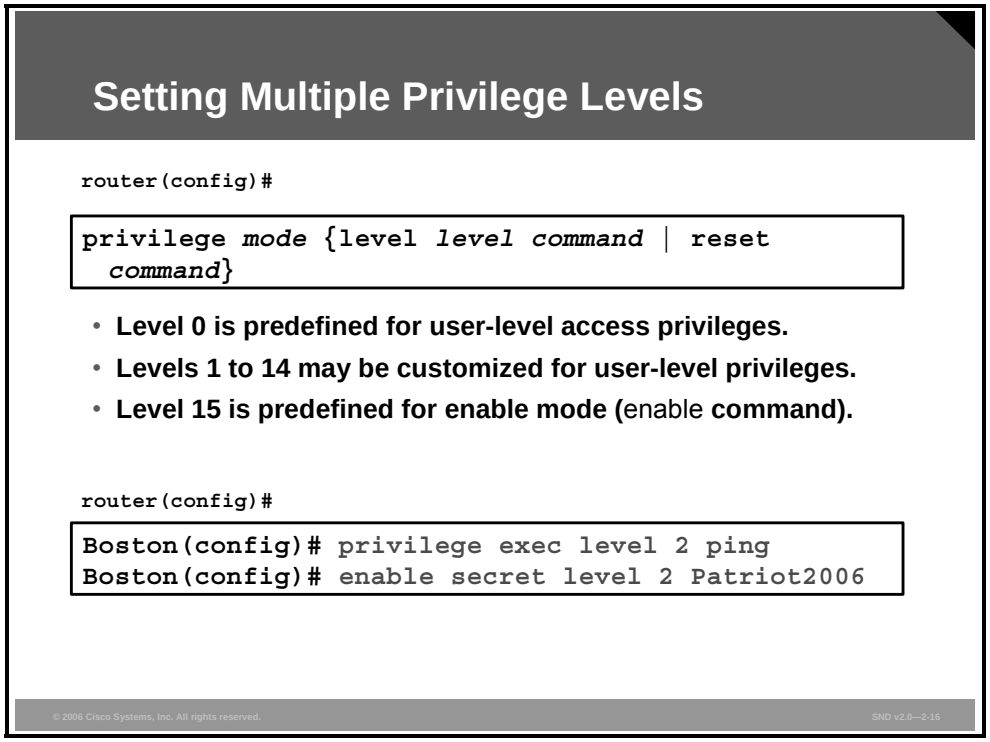
The vty lines **exec timeout** command can also be configured using the Cisco SDM GUI configuration tool.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Setting Multiple Privilege Levels

This topic describes how to secure administrative access to Cisco routers by setting multiple privilege levels.




Cisco routers enable you to configure various privilege levels for your administrators. Different passwords can be configured to control which administrators have access to the various privilege levels. This is especially useful in a help desk environment where certain administrators are allowed to configure and monitor every part of the router (level 15), while other administrators may be restricted to only monitoring (customized levels 2 to 14). The 16 levels (0 to 15) are defined in the figure.

Privileges are assigned to levels 2 to 14 using the **privilege** command from global configuration mode, as shown in the slide.

The example shown in the slide sets the **ping** command to privilege level 2 and establishes "Patriot" as the secret password users must enter to use level 2 commands. Using the **enable 2** command, you will be prompted for the enable secret password for privilege level 2. The **show privilege** command is used to display the current privilege level.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

The syntax for the **privilege** command is as follows:

**privilege** *mode* {**level** *level command* | **reset** *command*}

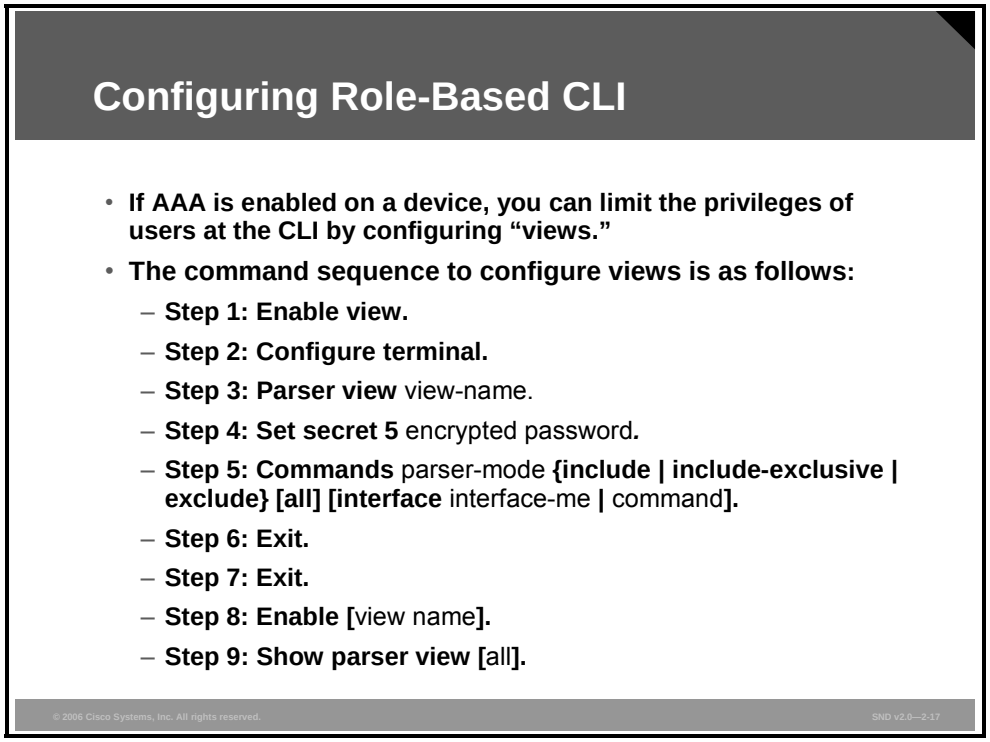
| Command | Description |
|---|---|
| *mode* | This command argument specifies the configuration mode. Use the router(config)**#privilege ?** command to see a complete list of router configuration modes available on your router. |
| **level** | (Optional) This command enables setting a privilege level with a specified command. |
| *level command* | (Optional) This is the privilege level associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15. |
| **reset** | (Optional) This command resets the privilege level of a command. |
| *command* | (Optional) This is the command argument to use when you want to reset the privilege level. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Configuring Role-Based CLI

This topic explains how to configure the role-based CLI access feature to provide views of router configurations.



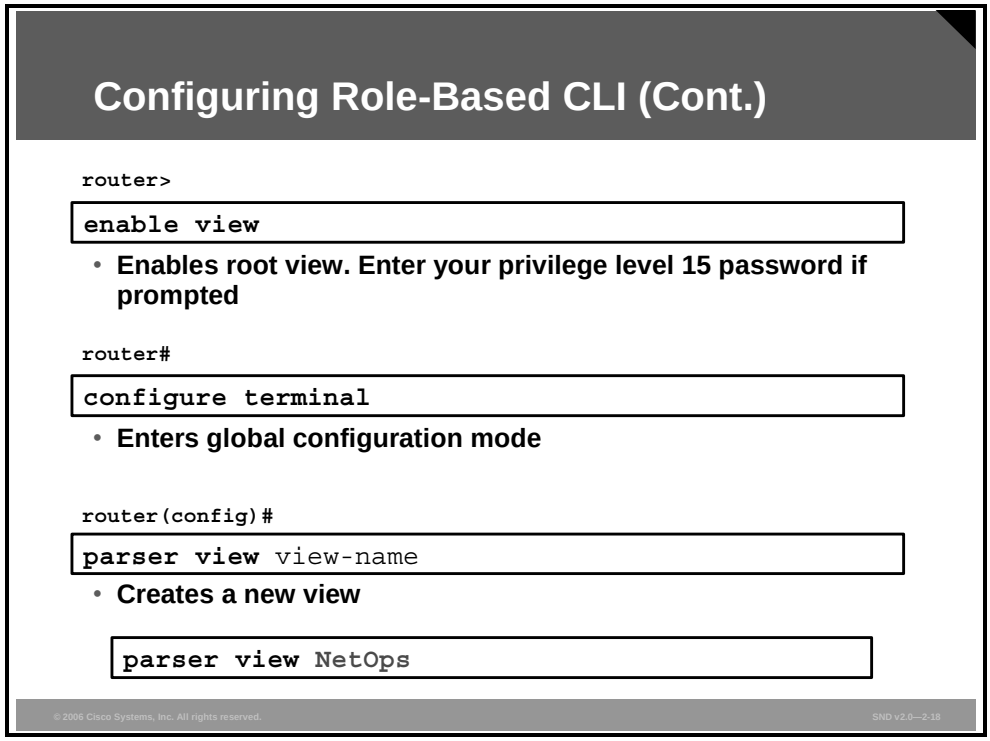

The role-based CLI access feature allows the network administrator to create different "views" of router configurations for different users. Views define what commands are accepted from different users and what configuration information is visible to them. With role-based CLI access, network administrators can exercise better control over Cisco networking devices.

| | |
|---|---|
| **Note** | Before you create a view, you must enable AAA via the **aaa new-model** command. You will learn AAA configuration in the "Configuring AAA Functions on the Cisco IOS Router" lesson. |

To configure a view and then confirm its proper configuration, enter the commands as shown in the figure. The last two steps allow you to preview the views that you have configured.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The key commands that are specific to configuring views for role-based CLI are shown in this and the next figure.

When a system is in "root view," it has all of the access privileges as a user who has level 15 privileges. If the administrator wishes to configure any view to the system, the system must be in root view.

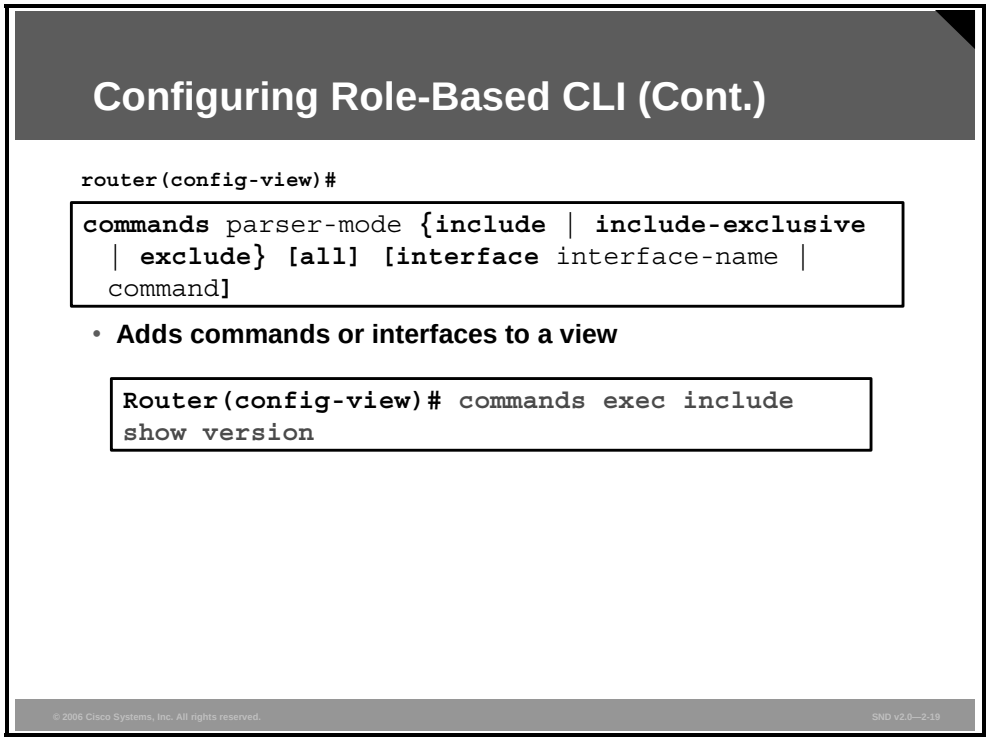
The difference between a user who has level 15 privileges and a root view user is that a root view user can configure a new view and add or remove commands from the view.

### Commands to Create New Views

| Command | Description |
|---|---|
| **enable view** | This command puts you in root view from where you will create views and establish view attributes. |
| **config term** | This command enters you into global configuration mode. |
| **parser view** *view name* | This command creates a view and enters view configuration mode. As shown in the figure, a new view named "first" is created. |
| **secret 0 \| 5** *view-password* | This command configures a password for this view:<br>■ **secret 0** specifies that an *unencrypted p*assword will follow.<br>■ **secret 5** specifies that an *encrypted* secret will follow. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Next, you must assign the commands allowed to the selected view.

The syntax for the **commands** command is as follows:

**commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*]

| Command | Description |
|---|---|
| **commands** | Adds commands or interfaces to a view |
| *parser-mode* | The mode in which the specified command exists |
| **include** | Adds a command or an interface to the view and allows the same command or interface to be added to an additional view |
| **include-exclusive** | Adds a command or an interface to the view and excludes the same command or interface from being added to all other views |
| **exclude** | Excludes a command or an interface from the view (that is, customers cannot access a command or an interface) |
| **all** | A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view |
| **interface** *interface-name* | Interface that is added to the view |
| *command* | Command that is added to the view |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Example—Creating a View Called “NetOps”

```
Router#enable view
Password: Curium2006
Router#configure terminal
router(config)#parser view NetOps
router(config-view)#secret 0 hardtocrackpw
router(config-view)#commands exec include ping
router(config-view)#commands exec include all show
router(config-view)#commands exec include telnet
router(config-view)#commands exec include traceroute
router(config-view)#commands exec include write
router(config-view)#commands exec include configure
router(config-view)#commands configure include access-list
router(config-view)#commands configure include all interface
router(config-view)#commands configure include all ip
```

© 2006 Cisco Systems, Inc. All rights reserved.


The example shown in the figure creates the NetOps view, configures a password for this view, and then assigns the commands allowed for this view.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Example—Verifying Commands Available to the NetOps View

```
router#enable view NetOps
Password: hardtocrackpw
router#
Jan  3 13:45:03.887: %PARSER-6-VIEW_SWITCH: successfully set to view 'NetOps'.
router#?
Exec commands:
  configure   Enter configuration mode
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  ping        Send echo messages
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
  write       Write running configuration to memory, network, or terminal
router#configure terminal
router(config)#?
Configure commands:
  access-list  Add an access list entry
  do           To run exec commands in config mode
  exit         Exit from configure mode
  interface    Select an interface to configure
  ip           Global IP configuration subcommands
```

© 2006 Cisco Systems, Inc. All rights reserved.

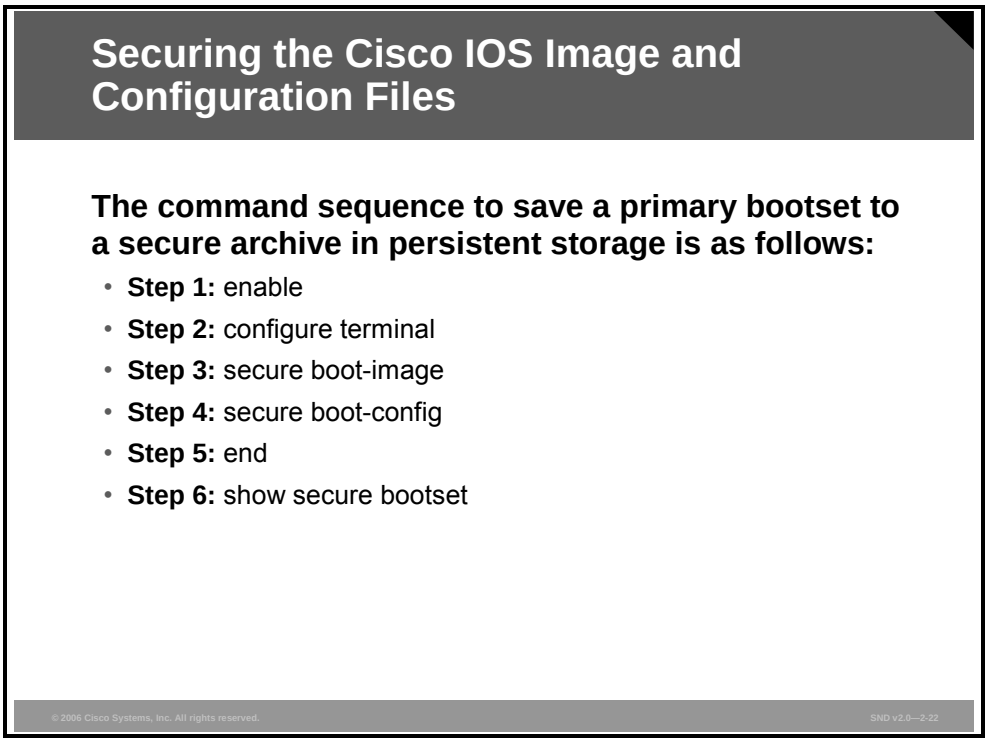

To verify a view, use the **enable view** command. Enter the view that you want to verify, then use the question mark (**?)** command to verify that the commands available in the view are correct. The figure shows an example that accesses the NetOps view and verifies its capability.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Securing the Cisco IOS Image and Configuration Files

This topic explains how to use the Cisco IOS resilient configuration feature to secure the Cisco IOS image and configuration files.



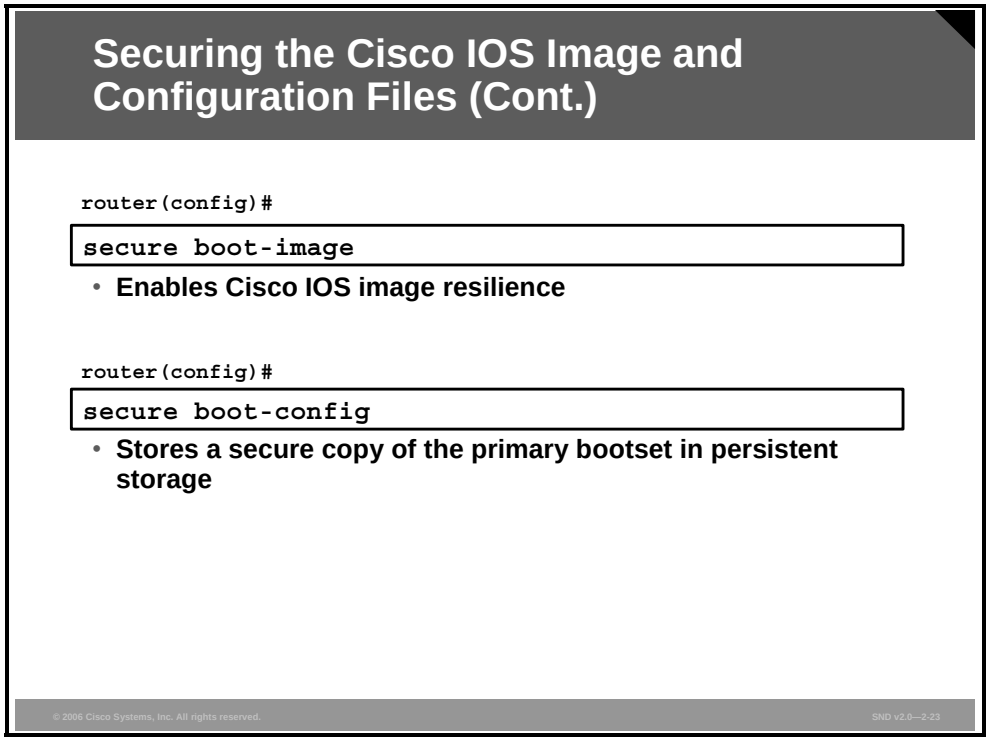

The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash storage).

A great challenge for network operators is the total downtime experienced after a router has been compromised and its operating software and configuration data erased from its persistent storage. The operator must retrieve an archived copy (if one is available) of the configuration and a working image to restore the router. Recovery must then be performed for each affected router, adding to the total network downtime.

The Cisco IOS Resilient Configuration feature is intended to speed up the recovery process. This feature maintains a secure working copy of the router image and the startup configuration at all times. These secure files cannot be removed by the user. This set of image and router running configuration is referred to as the bootset.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Secured files will not appear on the output of a **dir** command issued from an executive shell because the Cisco IOS file system prevents secure files in a directory from being listed. ROMMON mode does not have any such restriction and can be used to list and boot secured files. The running image and running configuration archives will not be visible in the Cisco IOS **dir** command output. Instead, use the **show secure bootset** command to verify archive existence.

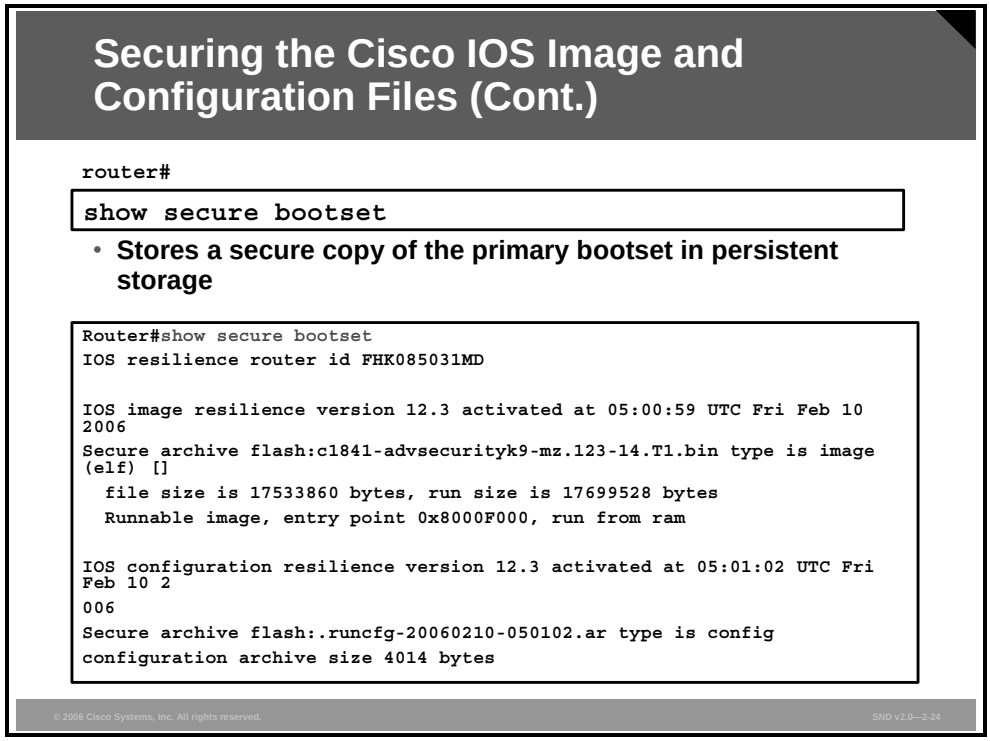
The "Commands to Secure the Cisco IOS Image and Running Configuration" table describes the key commands required to secure the Cisco IOS image and running configuration.

### Commands to Secure the Cisco IOS Image and Running Configuration

| Command | Description |
|---|---|
| **secure boot-image** | This command enables Cisco IOS image resilience. When turned on for the first time, the running image (as displayed in the **show version** command output) is secured, and a syslog entry is generated. This command will function properly only when the system is configured to run an image from a disk with an advanced technology attachment (ATA) interface. Images booted from a TFTP server cannot be secured. Because this command has the effect of "hiding" the running image, the image file will not be included in any directory listing of the disk.<br><br>If the router is configured to bootup with Cisco IOS resilience and an image with a different version of Cisco IOS is detected, a message similar to this is displayed at bootup:<br><br>**ios resilience :Archived image and configuration version 12.2 differs from running version 12.3**<br><br>Run **secure boot-config** and **image** commands to upgrade archives to the running version. |
| **secure boot-config** | This command takes a snapshot of the router running configuration and securely archives it in persistent storage. |

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



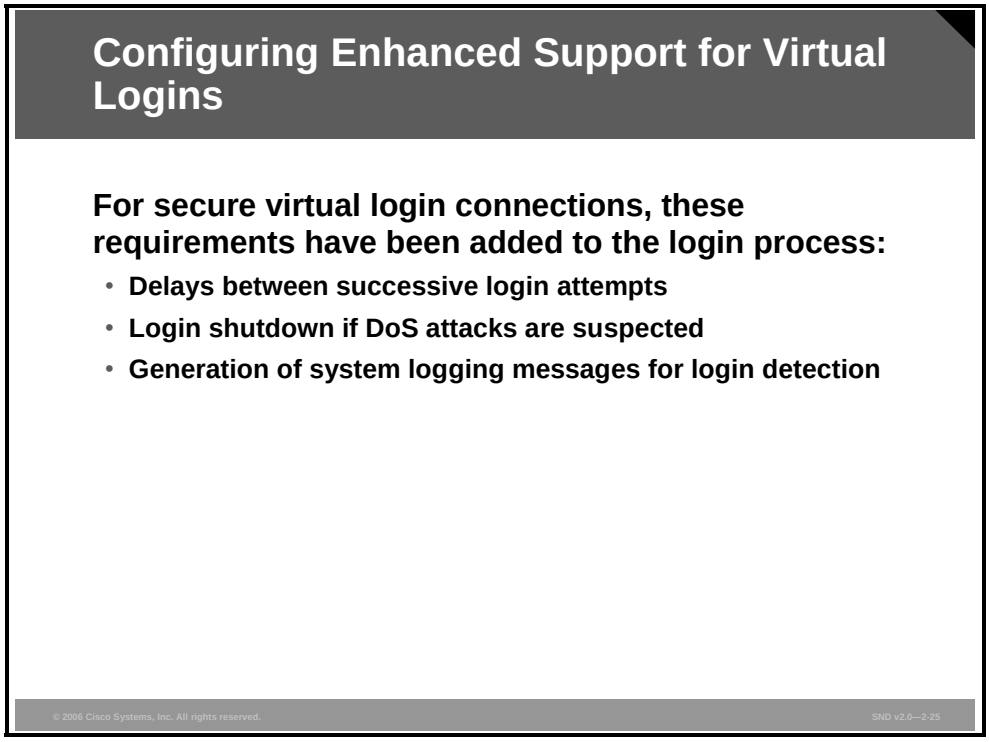

The figure shows an example of the **show secure bootset** command output. This step is important to verify that the Cisco IOS image and configuration files have been properly backed up and secured.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Configuring Enhanced Support for Virtual Logins

This topic explains how to configure better security for virtual login connections.




The Cisco IOS Login Enhancements feature allows users to better secure their Cisco IOS devices when creating a virtual connection, such as Telnet, SSH, or HTTP. Thus, users can help slow down dictionary attacks and help protect their router from a possible denial of service (DoS) attack.

To better configure security when opening a virtual login connection, these requirements have been added to the login process:

- Delays between successive login attempts
- Login shutdown if DoS attacks are suspected
- Generation of system logging messages for login detection

A Cisco IOS device can accept virtual connections as fast as connections can be processed. Introducing a delay between login attempts helps to protect your router from a possible dictionary attack. Delays can be enabled in one of these ways:

- Via the **login delay** command; this is the new global configuration mode command that allows you to specify the number of seconds.
- Via the **login block-for** command. You must enter this command before issuing the **login delay** command. However, if you enter only the **login block-for** command, a login delay of 1 second is automatically enforced.
- Via the **auto secure** command; if you enable **auto secure**, a login delay of 1 second is automatically enforced.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

If the configured number of connection attempts fails within a specified time period, the Cisco IOS device will not accept any additional connections for a period of time called the “quiet period.” Hosts that are permitted by a predefined ACL are excluded from the quiet period.

The number of failed connection attempts that trigger the quiet period can be specified via the new global configuration mode **login block-for** command. The predefined ACL that is excluded from the quiet period can be specified via the new global configuration mode **login quiet-mode access-class** command.

This functionality is disabled by default, and it is not enabled if **auto secure** is enabled.

After the router switches to and from quiet mode, logging messages are generated. Also, if configured, logging messages are generated upon every successful or failed login request.

Logging messages can be generated for successful login requests via the new global configuration command **login on-success**. The **login on-failure** command generates logs for failed login requests.

Logging messages for failed login attempts are automatically enabled when the **auto secure** command is issued, but are not automatically enabled for successful login attempts via the **auto secure** command.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Configuring Enhanced Support for Virtual Logins (Cont.)

**The command sequence to secure virtual login connections is as follows:**

- **Step 1:** enable
- **Step 2:** configure terminal
- **Step 3:** login block-for *seconds* attempts *tries* within *seconds*
- **Step 4:** login quiet-mode access-class {*acl-name* | *acl-number*}
- **Step 5:** login delay *seconds*
- **Step 6:** login on-failure log [every *login*]
- **Step 7:** login on-success log [every *login*]

© 2006 Cisco Systems, Inc. All rights reserved.

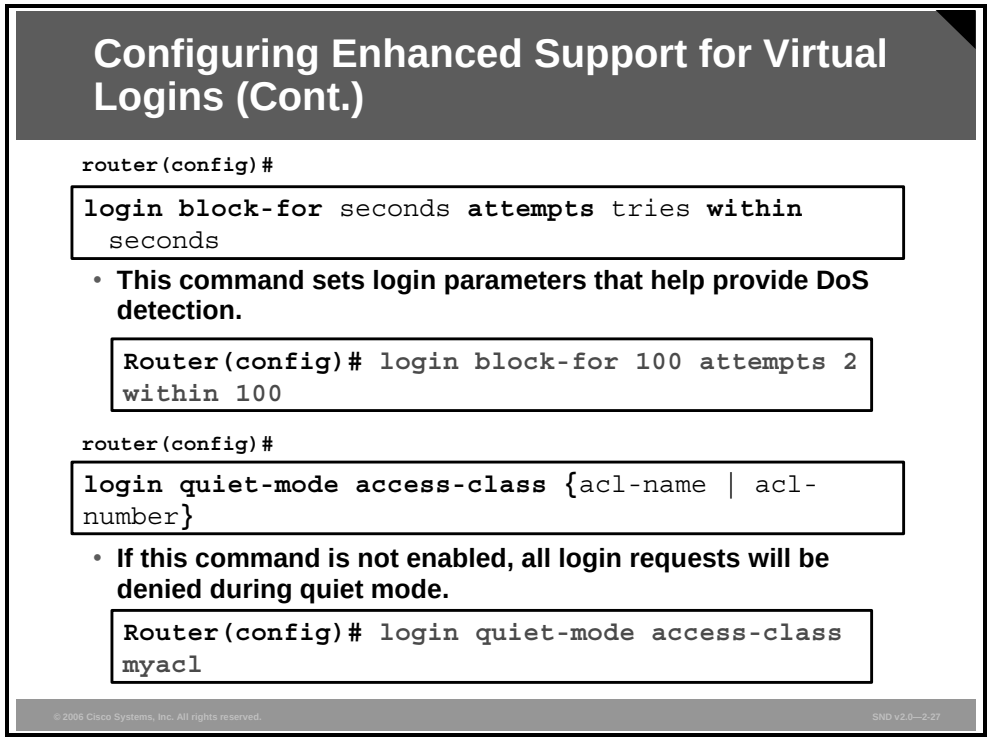

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, these defaults are enforced:

- There is a default login delay of 1 second.
- All login attempts made via Telnet, SSH, and HTTP are denied during the quiet period; that is, no ACLs are exempt from the login period until the **login quiet-mode access-class** command is issued.

Use the command sequence shown in the figure to configure your Cisco IOS device for login parameters that help detect suspected DoS attacks and slow down dictionary attacks.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



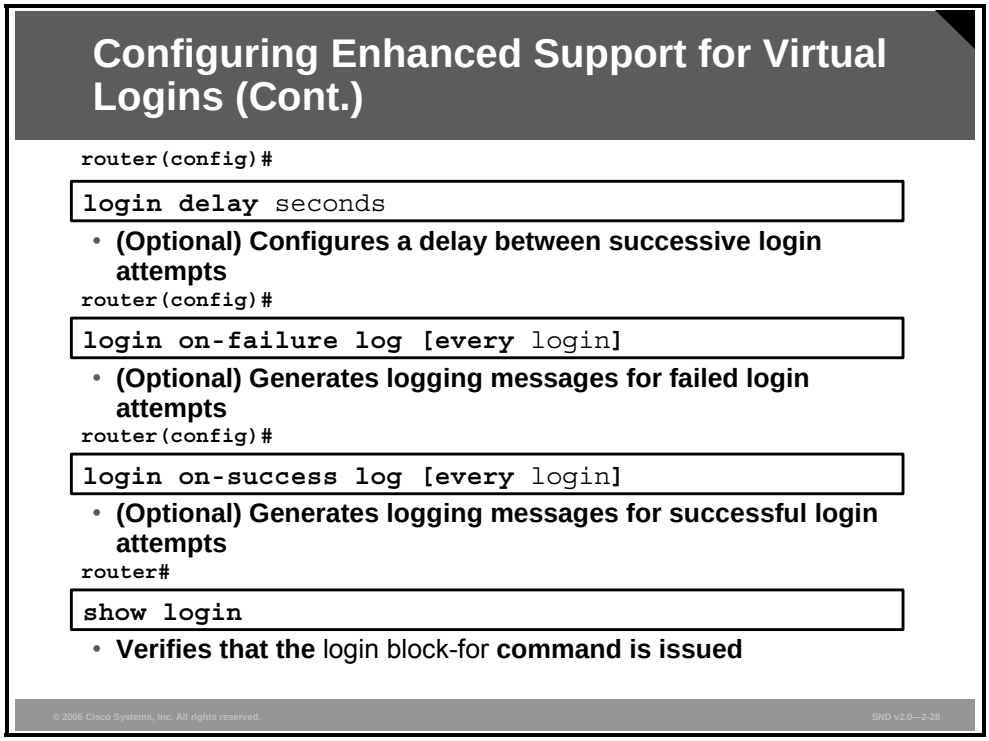

The “Enabling Support for Virtual Logins” table describes the commands required to set the parameters for the quiet period.

### Enabling Support for Virtual Logins

| Command | Description |
|---|---|
| **login block-for** *seconds* **attempts** *tries* **within** *seconds* | This command must be issued before any other login command can be used.<br>This command configures your Cisco IOS device for login parameters that help provide DoS detection. |
| **login quiet-mode access-class** {*acl-name* \| *acl-number*} | (Optional) This command specifies an ACL that is to be applied to the router when it switches to quiet mode.<br>The example in the figure shows a configuration that invokes an ACL named “myacl”. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




To enable a login delay and to log successful and failed attempts to login, use the commands shown in the figure.

This sample output from the **show login** command verifies that the **login block-for** command is issued. In this example, the command is configured to block login hosts for 100 seconds if more than 15 (16 or more) login requests fail within 100 seconds. Five login requests have already failed.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins
will be disabled for 100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95
seconds.
Present login failure count 5.
```

This sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if more than 2 (3 or more) login requests fail within 100 seconds.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
```



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

```
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins
will be disabled for 100 seconds.

Router presently in Quiet-Mode, will remain in Quiet-Mode for 93
seconds.
Denying logins from all sources.
```

This sample output from the **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures

Information about login failure's with the device

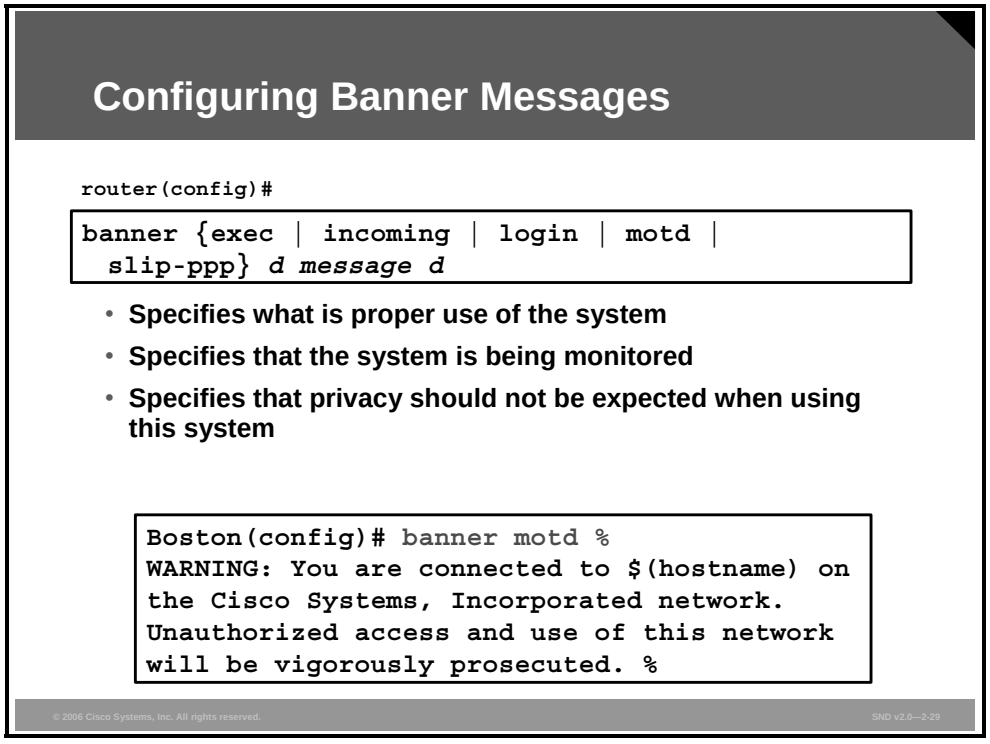
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Configuring Banner Messages

This topic describes how to secure administrative access to Cisco routers by configuring banner messages.




Banner messages should be used to warn would-be intruders that they are not welcome on your network. Banners are very important, especially from a legal perspective. Intruders have been known to win court cases because they did not encounter appropriate warning messages when accessing router networks.

Choosing what to place in your banner messages is important and should be reviewed by legal counsel before placing them on your routers. Never use the word “welcome” or any other familiar greeting that may be misconstrued as an invitation to use the network.

Banners are disabled by default and must be explicitly enabled by the administrator. As shown in the figure, use the **banner** command from global configuration mode to specify appropriate messages.

Banner message can also be configured using Cisco SDM.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

The syntax for the **banner** command is as follows:

**banner** {**exec** | **incoming** | **login** | **motd** | **slip-ppp**} *d message d*

| Command Element | Description |
|---|---|
| **banner exec** | This command specifies and enables a message to be displayed when an EXEC process is created on the router (an EXEC banner). |
| **banner incoming** | This command specifies and enables a banner to be displayed when there is an incoming connection to a terminal line from a host on the network. |
| **banner login** | This command specifies and enables a customized banner to be displayed before the username and password login prompts. |
| **banner motd** | This command specifies and enables a message-of-the-day (MOTD) banner. |
| **banner slip-ppp** | This command specifies and enables a banner to be displayed when a Serial Line Interface Protocol (SLIP) or PPP connection is made. |
| *d* | This represents the delimiting character of your choice—for example, a pound sign (#). You cannot use the delimiting character in the banner message. |
| *message* | This represents message text. You can include tokens in the form $(*token*) in the message text. Tokens are replaced with the corresponding configuration variable. |

This list contains valid tokens for use within the *message* section of the **banner** command.

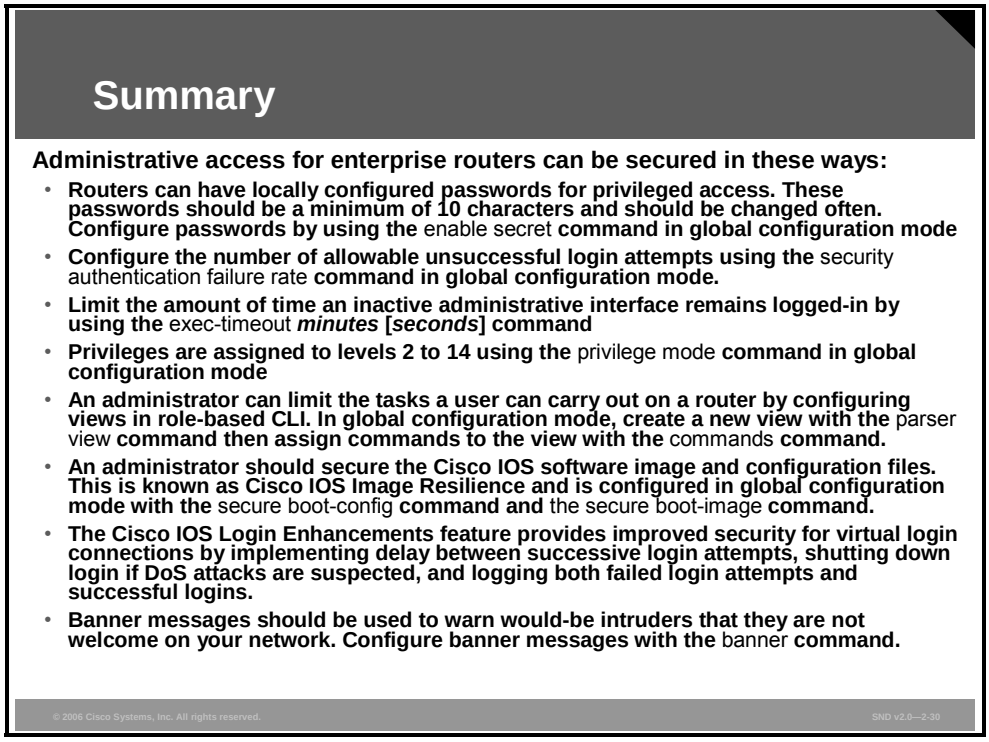
- **$(hostname):** Displays the hostname for the router
- **$(domain):** Displays the domain name for the router
- **$(line):** Displays the vty or TTY (asynchronous) line number
- **$(line-desc):** Displays the description attached to the line



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 3

# Introducing Cisco SDM

## Overview

Cisco Router and Security Device Manager (SDM) is an intuitive, web-based tool for easy and reliable deployment and management of services on Cisco IOS routers. Cisco SDM simplifies router and security configuration through smart wizards, which help users quickly and easily deploy, configure, and monitor Cisco routers without requiring knowledge of the Cisco IOS software command-line interface (CLI).

This lesson will introduce you to the look and feel of the Cisco SDM, and to the features that are configurable from it.

## Objectives

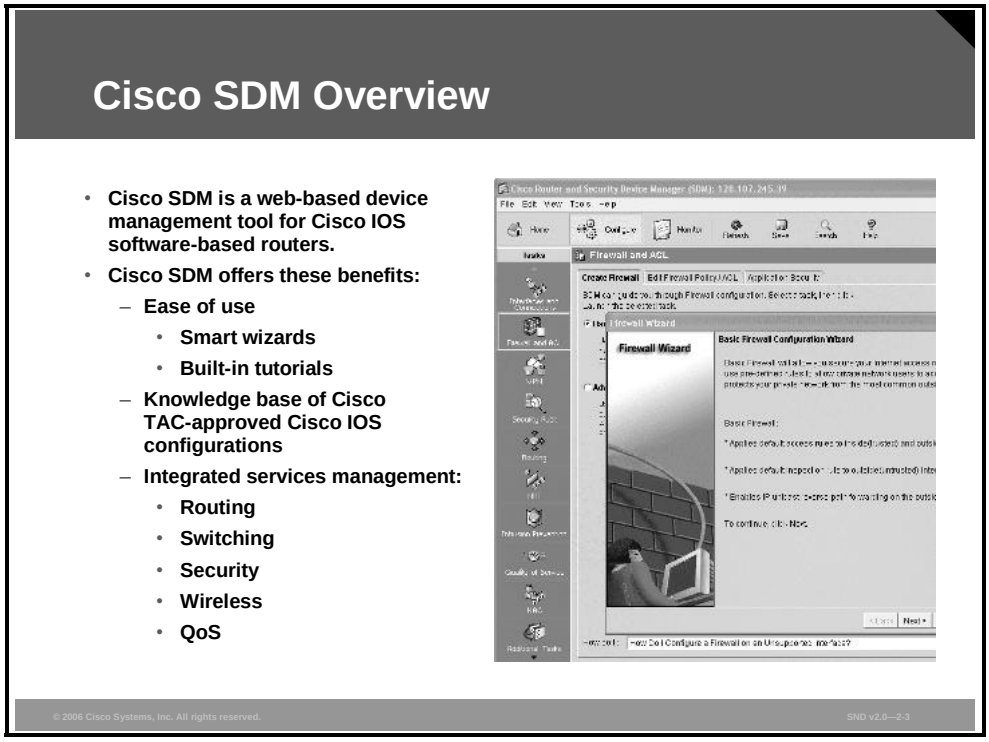
Upon completing this lesson, you will be able to describe the features and use of Cisco SDM. This ability includes being able to meet these objectives:

- Describe the key features, concepts, and purpose of Cisco SDM
- Describe how to set up a router to run Cisco SDM and Cisco SDM Express
- Describe how to launch Cisco SDM Express to configure a new router
- Describe how to launch the Cisco SDM application
- Describe how to navigate the Cisco SDM GUI
- Describe the common wizards in Cisco SDM

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Cisco SDM Overview

This topic describes the key features, concepts, and purpose of Cisco SDM.




Cisco SDM is an intuitive, web-based device manager for easy and reliable deployment and management of services on Cisco IOS routers. Cisco SDM offers users these benefits:

- Smart wizards in Cisco SDM have built-in intelligence about Cisco Technical Assistance Center (TAC)-recommended Cisco IOS configurations for different use scenarios.
- Cisco SDM can recommend an optimum security configuration for a router based on detection of such areas as LAN and WAN connections, access control lists (ACLs), Network Address Translation (NAT), IPsec policies, and firewall rules.
- Cisco SDM includes features such as WAN and virtual private network (VPN) troubleshooting, router security audit, and One-Step Lockdown that leverage the integration of routing, WAN access, and security technology.
- For novices, Cisco SDM helps users with limited CLI knowledge and security expertise to configure basic network security implementations. For experts, Cisco SDM has power tools that improve productivity. As a device manager, Cisco SDM manages one device at a time.

**Note** The Cisco SDM CD-ROM or the Cisco SDM image from the Cisco IOS Software Center (http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm) supports Cisco SDM installation on a PC hard disk or router flash memory. When installed on a PC, Cisco SDM requires no files on the router flash memory and can manage an installed base of Cisco routers that may not have enough flash memory space to load Cisco SDM files.

- Cisco SDM supports Cisco IOS Release 12.2(11)T6 or later.
- Cisco SDM has no impact on router DRAM or CPU.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Cisco SDM works in conjunction with other management tools and the CLI over Telnet.
- Refer to the *Cisco Router and Security Device Manager Version 2.2 User's Guide* for details on supported platforms and Cisco IOS software requirements.

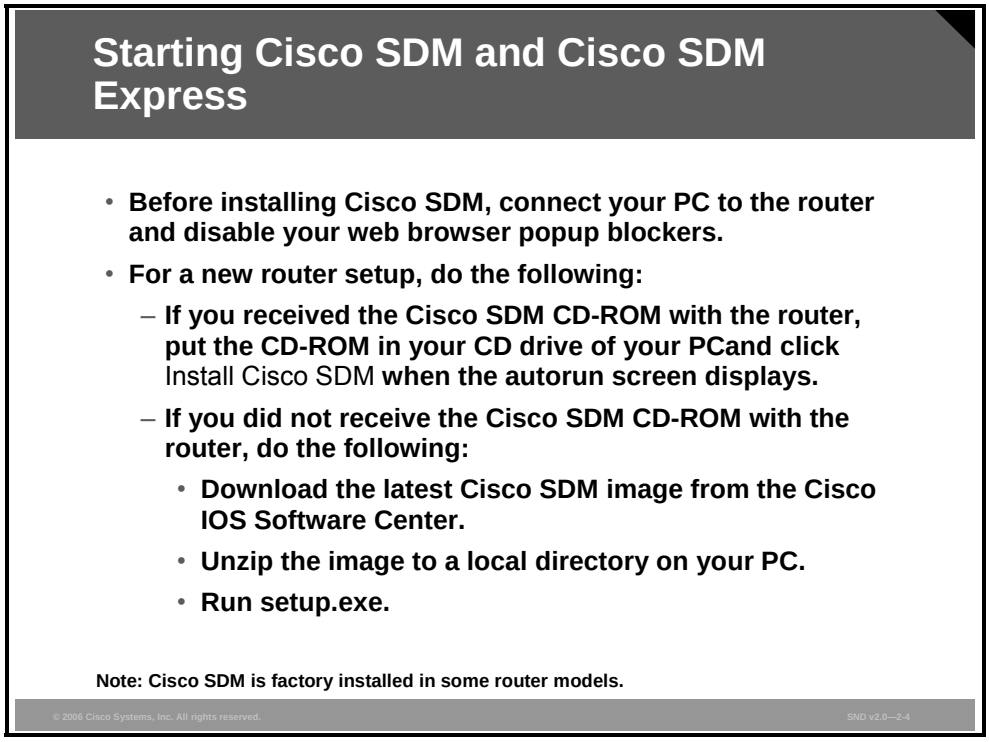
| | |
|---|---|
| **Note** | You should review your security policy to ensure that there is no policy that prohibits enabling a web server daemon on routers. SDM requires HTTP to be enabled. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Starting Cisco SDM and Cisco SDM Express

This topic describes how to set up a router to run Cisco SDM and Cisco SDM Express.




Cisco SDM is a web-based tool that is supported on Microsoft Windows-based PC platforms. You should refer to the *Cisco Router and Security Device Manager Quick Start Guide* for details on the operating systems and web browsers that are supported by Cisco SDM.

Cisco SDM is factory installed in some router models. If it is not installed on your router, it will either be available on a CD-ROM that is included with new routers or it can be downloaded from Cisco.com. When installing Cisco SDM, the install options include options to install Cisco SDM Express, Cisco SDM, or both.

| | |
|---|---|
| **Note** | Cisco SDM ships preinstalled on all new Cisco 850 Series and Cisco 870 Series Access Routers, and on Cisco 1800 Series, Cisco 2800 Series, and Cisco 3800 Series Integrated Services Routers. |

## Additional Preparation for Existing Routers

If the router is an existing one and is not configured with the Cisco SDM default configuration, you need to configure these services on the router for Cisco SDM to access the router properly:

- Privilege 15 user: **username** *name* **privilege 15 secret** *password*
- HTTP server enabled: ip http server
  - ip http authentication local
  - ip http secure-server (for enabling HTTP Secure [HTTPS] access to Cisco SDM)
  - ip http timeout-policy idle 600 life 86400 request 1000

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Define the protocol to use to connect to the Telnet and Secure Shell (SSH) vty lines
  - line con 0
  - login local
  - line vty 0 4
    - privilege level 15
    - login local
    - transport input telnet ssh
  - line vty 5 15
    - privilege level 15
    - login local
    - transport input telnet ssh



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Files Required to Run Cisco SDM from a Router

```
router#show flash
-#- --length-- -----date/time------ path
1     19312988 Dec 13 2005 01:23:50 +00:00 c2800nm-
advsecurityk9-mz.124-5.bin
2          3317 Feb 8 2006 00:00:30 +00:00 startup.config
3          1646 Feb 8 2006 18:31:50 +00:00 sdmconfig-2811.cfg
4       4049920 Feb 8 2006 18:32:32 +00:00 sdm.tar
5        812544 Feb 8 2006 18:32:56 +00:00 es.tar
6       1007616 Feb 8 2006 18:33:14 +00:00 common.tar
7          1038 Feb 8 2006 18:33:24 +00:00 home.shtml
8        113152 Feb 8 2006 18:33:42 +00:00 home.tar
9        511939 Feb 8 2006 18:33:56 +00:00 128MB.sdf
10       234040 Feb 8 2006 18:34:32 +00:00 attack-drop.sdf
```

© 2006 Cisco Systems, Inc. All rights reserved.


When you want to run Cisco SDM from your router, for Cisco SDM Version 2.2a and later, these files must be loaded on the router flash memory:

- sdmconfig-modelxxx.cfg is the manufacture default config file for the router
- sdm.tar
- es.tar (This file is for Cisco SDM Express and is optional once Cisco SDM is installed.)
- common.tar
- home.shtml
- home.tar

A file for wireless interfaces, wlanui.tar, is required if there are wireless interfaces to manage.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Launching Cisco SDM Express

This topic describes how to launch Cisco SDM Express to configure a new router.

## Launching Cisco SDM Express

- **To launch Cisco SDM Express:**
  - **For a new router, in a web browser go to https://10.10.10.1**
  - **For existing routers go to https://<router IP address>**
- **The first time that you access the router by web browser, you will get the Cisco SDM Express wizard.**




© 2006 Cisco Systems, Inc. All rights reserved.


On a new router, you can access Cisco SDM Express from your PC web browser by going to IP address http://10.10.10.1. The factory default router configuration file that comes with Cisco SDM configures the router Ethernet IP address to 10.10.10.1.

If the proper files are loaded on the router flash memory, when you access the router for the first time, the Cisco SDM Express wizard appears. Simply enter the required information, noting that some fields provide a default value.

When you launch Cisco SDM from the router, Cisco SDM checks router configuration. If certain features are not configured, Cisco SDM Express will be launched. For example, when Cisco SDM sees the manufacture default on the router (sdmconfig-xxx.cfg), Cisco SDM Express will be launched.

After you have completed the initial router configuration with Cisco SDM Express, you will not be presented with the Cisco SDM Express wizard again. If changes are needed, you can edit configurations using the full Cisco SDM tool.

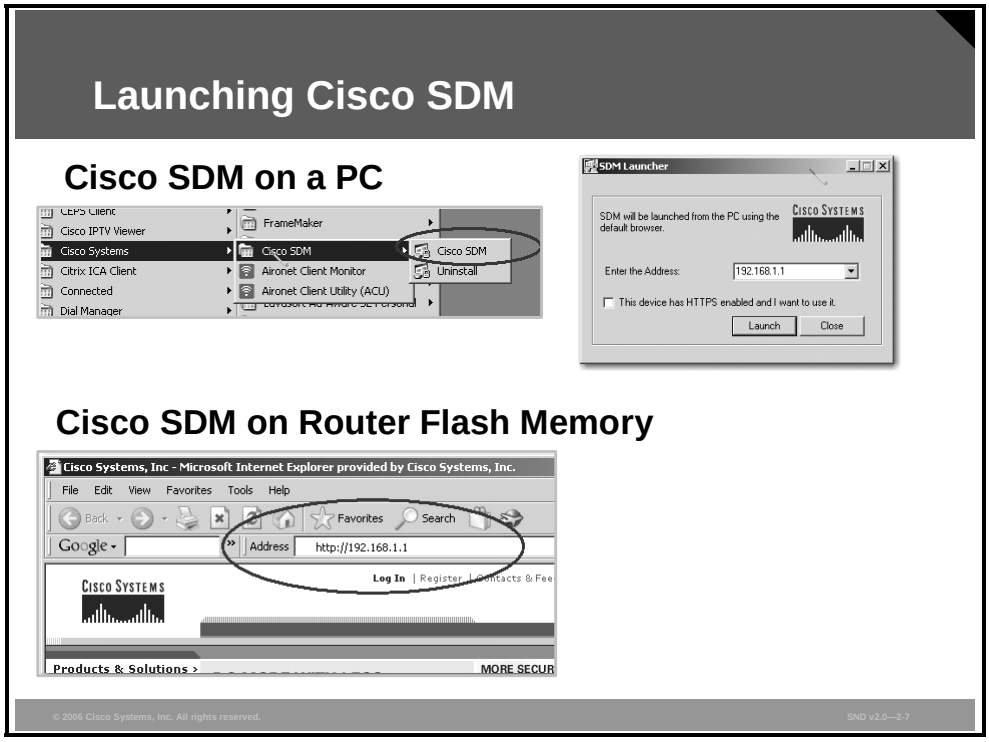
Details about Cisco SDM Express can be found in the *Cisco SDM Express 2.2 User's Guide.*



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Launching Cisco SDM

This topic describes how to launch the Cisco SDM application.




If you installed Cisco SDM on an administrator PC, go to the Microsoft Windows program menu (choose **Start** > **Programs (All Programs)** > **Cisco Systems** > **Cisco SDM**). Then provide the IP address of the LAN interface on the router—as configured previously with the Cisco SDM Express Wizard—in the Cisco SDM Launcher window. If Cisco SDM is on the router flash memory, open a web browser and enter the new IP address of the LAN interface there. Follow the prompts, including inputting your administrator credentials (username and password), to reach the Cisco SDM home page.

If you installed Cisco SDM on the router flash memory, open an HTTP or HTTPS connection from a web browser to the router to access Cisco SDM. Follow the prompts, including inputting your administrator credentials (username and password), to reach the Cisco SDM home page.

### Browser Requirements

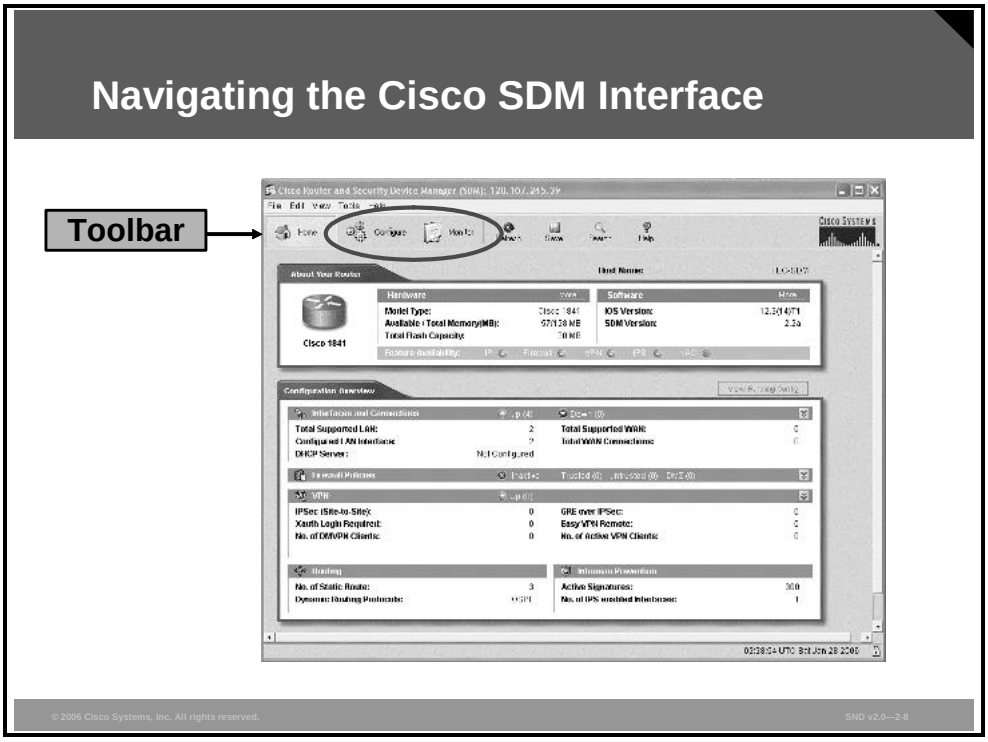
| Software Type | Specifications |
|---|---|
| Browser | ■ Microsoft Internet Explorer 5.5 or later<br>■ Netscape Navigator 7.1 or 7.2<br>■ Mozilla Firefox 1.0.5 |
| Java software | ■ Java Virtual Machine (JVM) built-in browsers required<br>■ Java plug-in Java 2 Standard Edition (J2SE) (Java Runtime Environment [JRE] version 1.4.2_05 or later) |

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Navigating the Cisco SDM Interface

This topic describes how to navigate the Cisco SDM GUI.




The home page, shown in the figure, appears each time you successfully log in to Cisco SDM.

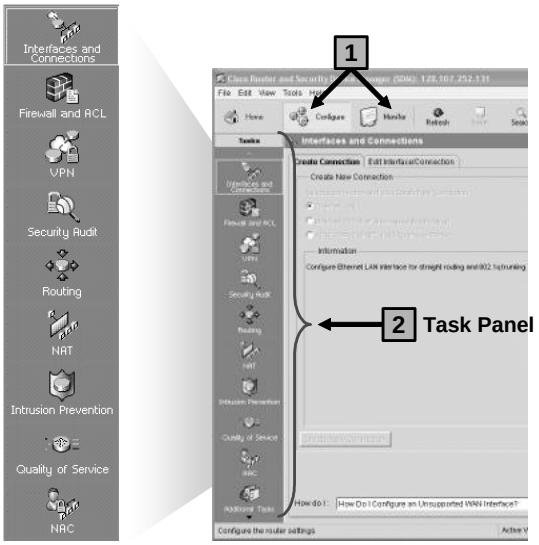
Navigating the Cisco SDM user interface on the home page is done through the toolbar. Two of the modes on the toolbar, Configure mode, and Monitor mode, are also used to navigate the interface. To select a mode, click the corresponding button in the toolbar. For each mode, a task panel is available showing the wizard options available for that mode.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Navigating the Cisco SDM Interface (Cont.)

1. **Choose** Configure **or** Monitor**.**
2. **From the task panel that appears, launch wizards.**




© 2006 Cisco Systems, Inc. All rights reserved.


Configure mode provides wizards for the novice. More experienced users are able to perform tasks in any order and outside of the wizards.

Monitor mode is where the user can view the current status of the router.

The Refresh button is used to resynchronize the router running configuration with Cisco SDM, because Cisco SDM does not synchronize with the router configuration automatically.

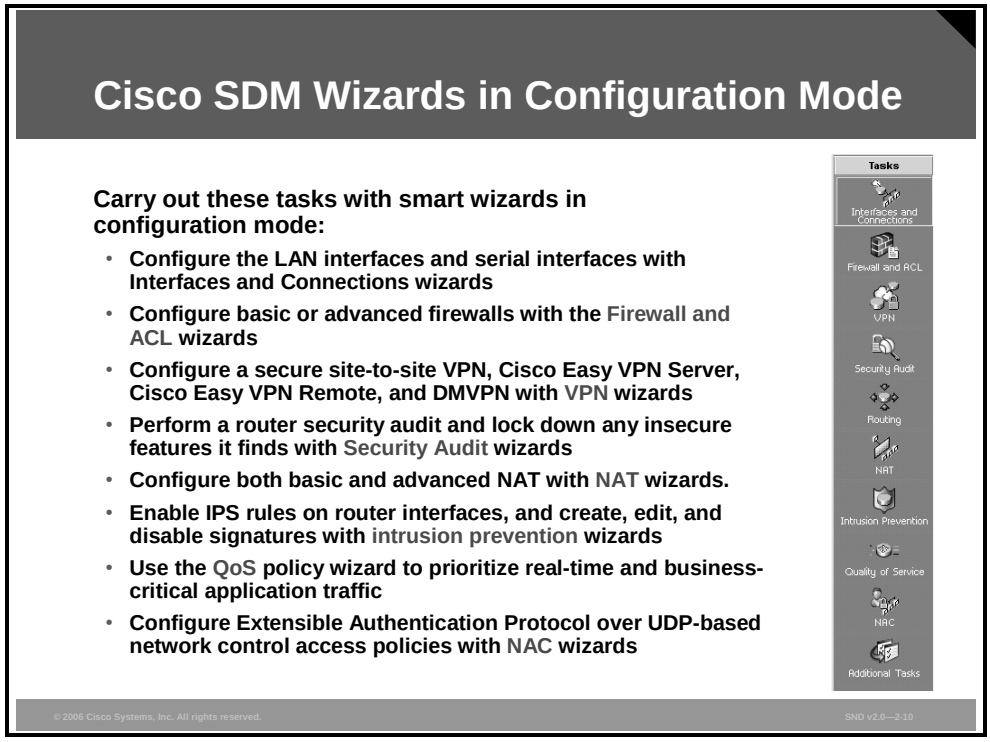
The Save button is used to save the running configuration to the startup configuration.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Cisco SDM Wizards

This topic describes the common wizards in Cisco SDM.




When accessing a wizard, a dialog box appears if there is a new configuration that has not yet been reflected in Cisco SDM. The dialog box states that you must perform Refresh or Deliver before entering wizard mode. Click either the **Refresh** or **Deliver** button to perform the required function.

When the requested page, such as the Configuration mode page, appears, the wizards are displayed on the left. In general, the functions of the available wizards in configuration mode are as follows:

- The Interfaces and Connection window displays the router interfaces and connections. The window also enables you to add, edit, and delete connections and to enable or disable connections such as those listed here:
  - The LAN wizard is used to configure the LAN interfaces and DHCP.
  - The WAN wizard is used to configure PPP, Frame Relay, and High-Level Data Link Control (HDLC) WAN interfaces.
- Firewalls provide these two wizards: a basic firewall wizard with inside and outside interfaces, and an advanced firewall wizard with inside and outside and demilitarized zone (DMZ) interfaces.
- For VPN, there are four wizards: site-to-site VPN, Cisco Easy VPN Remote, Cisco Easy VPN Server, and Dynamic Multipoint VPN (DMVPN).
- The Security Audit task contains two wizards: the router security audit and a One-Step Lockdown wizard.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- The Routing window displays the configured static routes and Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP)-configured routes. From this window, you can configuring the RIP, OSPF, or EIGRP routing protocol parameters; review the routes; add new static routes; edit existing static routes; and delete static routes.
- The NAT Rules window lets you view NAT rules, view address pools, and set translation timeouts. From this window, you can also designate interfaces as inside or outside interfaces.
- From Cisco IOS Release 12.3(8)T, the Intrusion Prevention window allows the user to enable or disable Cisco IOS Intrusion Prevention System(IPS) features on any interface in the router. If a Cisco Intrusion Detection System (IDS) Access Router Network Module (Cisco IDS Network Module) is installed in the router, this window displays basic status information for the module. If the Cisco IDS Network Module has been configured, you will also be able to start the Cisco IDS Device Manager (IDM) software on the Cisco IDS Network Module and select the router interfaces that you want the Cisco IDS Network Module to monitor from this window.

---

**Note** If Cisco SDM detects that the Cisco IDS Network Module has not been configured, it prompts you to open a session to the network module so that you can configure it. You can use Telnet or SSH for this session.

---

- The Quality of Service (QoS) page allows you to configure QoS rules and policies for your router.

When you finish using a wizard, all changes are automatically delivered using generated CLI commands. A user can choose whether to copy the running configuration to the startup configuration file.

For additional details on the tasks listed on this page, and on Network Admission Control (NAC) tasks, refer to the *Cisco Router and Security Device Manager Version 2.2 User's Guide.*

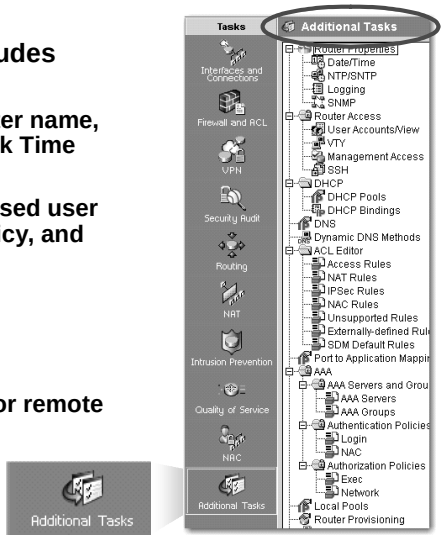
 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Configuration Mode—Advanced Configuration

**The additional Tasks option includes these advanced configurations:**

- **Router Properties, including router name, domain name, password, Network Time Protocol, date, and time**
- **Router Access, including role-based user access, management access policy, and SSH**
- **DHCP**
- **DNS and Dynamic DNS Methods**
- **Port-to-Application Mapping**
- **AAA, including local (on router) or remote server-based authentication and authorization**
- **Router Provisioning**




© 2006 Cisco Systems, Inc. All rights reserved.


At the bottom of the Cisco SDM configuration task bar there is an Additional Tasks option. Click **Additional Tasks** to enter this mode. You can perform tasks in any order you want, and you can always see existing configurations.

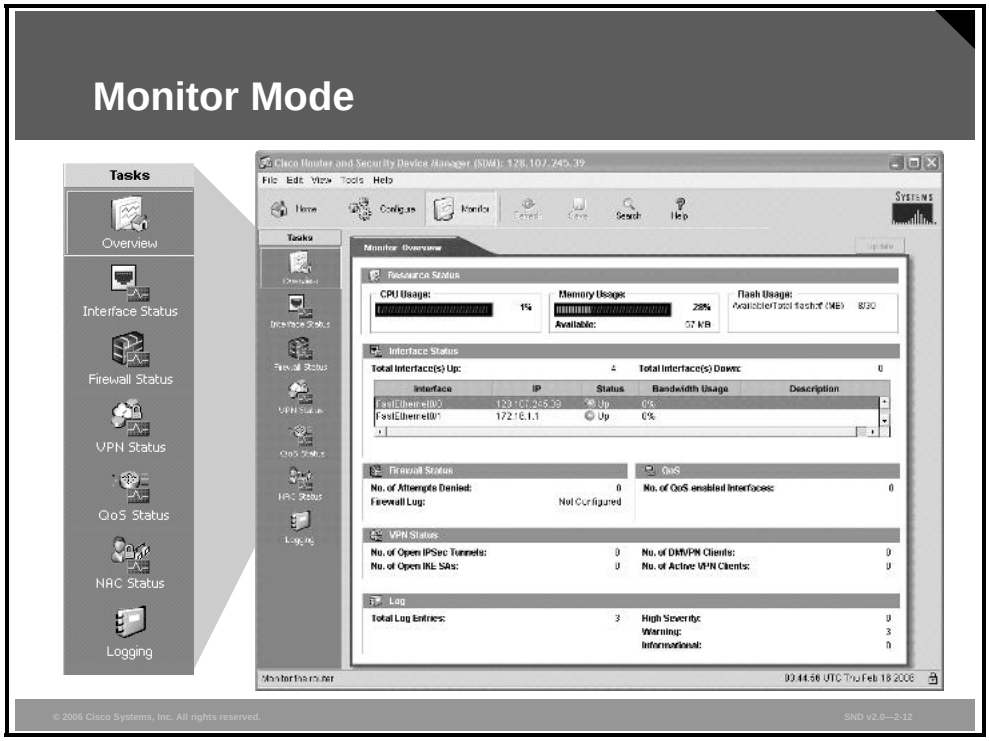
The Router Properties window lets you define the overall attributes of the router, such as the router name, domain name, password, Simple Network Management Protocol (SNMP) status, Domain Name System (DNS) server address, user accounts, router log attributes, vty settings, SSH settings, and other router access security settings.

Use the Router Access window to create and manage security policies to access and manage the router. You can create, edit, and delete role-based user access accounts and set up management access policies to limit the Telnet, SNMP, or Cisco SDM access to the router from specific hosts or networks.

For additional details on the features and functions available in this mode, refer to the *Cisco Router and Security Device Manager Version 2.2 User's Guide.*



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Monitor mode lets you view information about your router including the router interfaces, firewall, and any active VPN connection. You can also view any messages in the router event log.

The monitor function includes the following:

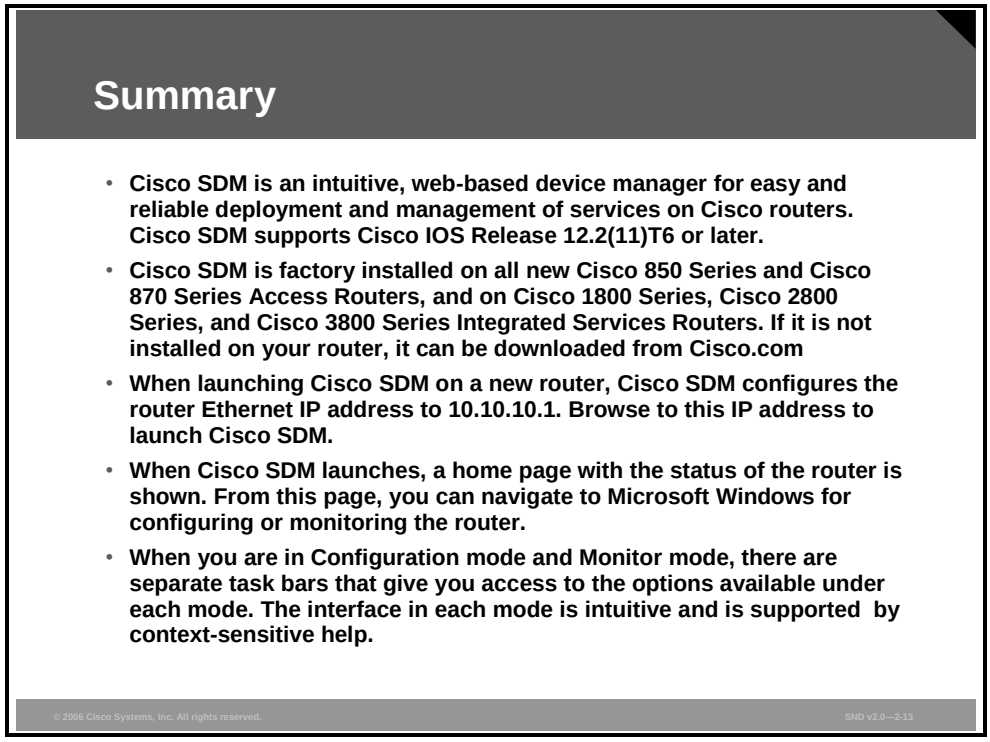
- An Overview section provides the router status, including a list of the error log entries.
- Interface Status is used to select the interface and conditions to monitor; for example, packets and errors and in or out.
- Firewall Status displays a log with the number of entry attempts that were denied by the firewall.
- VPN Status displays statistics about active VPN connections.
- QoS Status displays QoS policy information on the interfaces.
- NAC Status displays information such as the number of active NAC sessions on the routers.
- Logging contains the event log categorized by severity level, such as a UNIX syslog service.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Lesson 4

# Configuring AAA Functions on the Cisco IOS Router

## Overview

This lesson presents an introduction to implementing authentication, authorization and accounting (AAA).

## Objectives

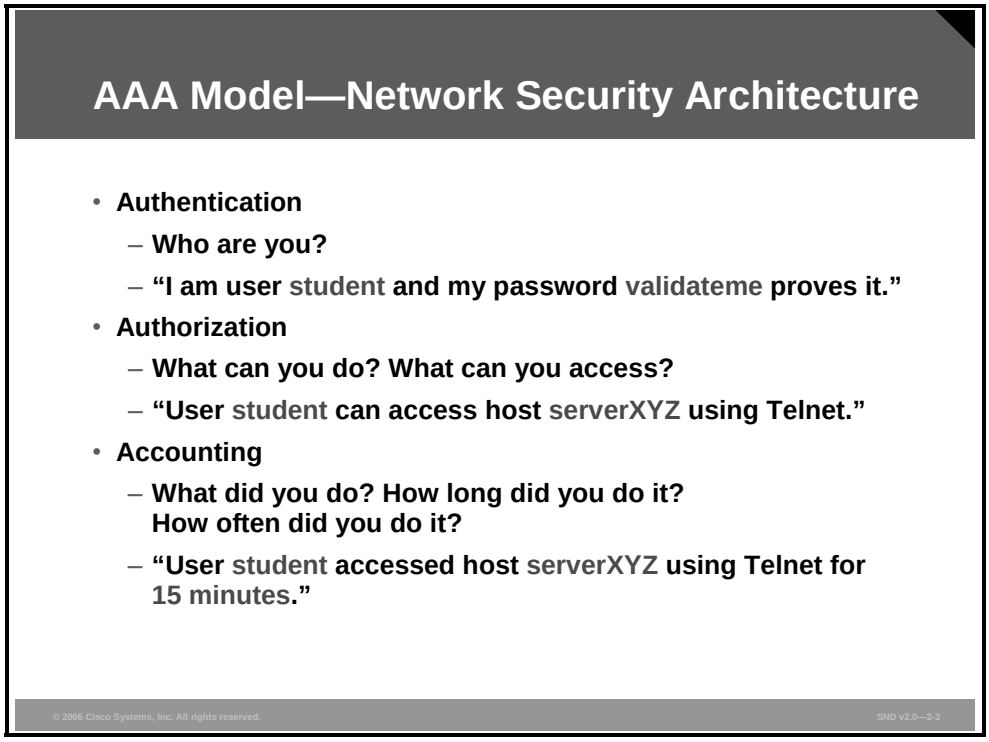
Upon completing this lesson, you will be able to configure a Cisco router to perform AAA authentication with a local database using Cisco Router and Security Device Manager (SDM). This ability includes being able to meet these objectives:

- Describe the functions and importance of AAA
- Describe three ways that Cisco implements AAA services for Cisco routers
- Describe the methods of authentication used to provide remote access to a LAN
- Describe the features of TACACS+ and RADIUS AAA protocols
- Describe the various authentication methods in use in terms of the degree of security that they provide and their ease of use
- Describe how PPP enables authentication between remote clients and servers using PAP, CHAP, or MS-CHAP
- Describe the three general steps that are required to configure a Cisco router to perform AAA using a local database for authentication
- Describe how to configure AAA on Cisco peripheral routers using **aaa** commands
- Explain how to troubleshoot AAA on a Cisco peripheral router using the **debug aaa** command
- Describe how to configure AAA using the Cisco SDM GUI

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Identification and Authentication

This topic describes the functions and importance of AAA.




AAA services provide a higher degree of scalability than the line-level and privileged EXEC authentication that you have learned so far.

Unauthorized access in campus, dial-up, and Internet environments creates the potential for network intruders to gain access to sensitive network equipment and services. The Cisco AAA architecture enables systematic and scalable access security.

Network and administrative access security in the Cisco environment, whether it involves campus, dial-up, or Internet (IPsec virtual private network [VPN]) access, is based on a modular architecture that has three functional components: authentication, authorization, and accounting:

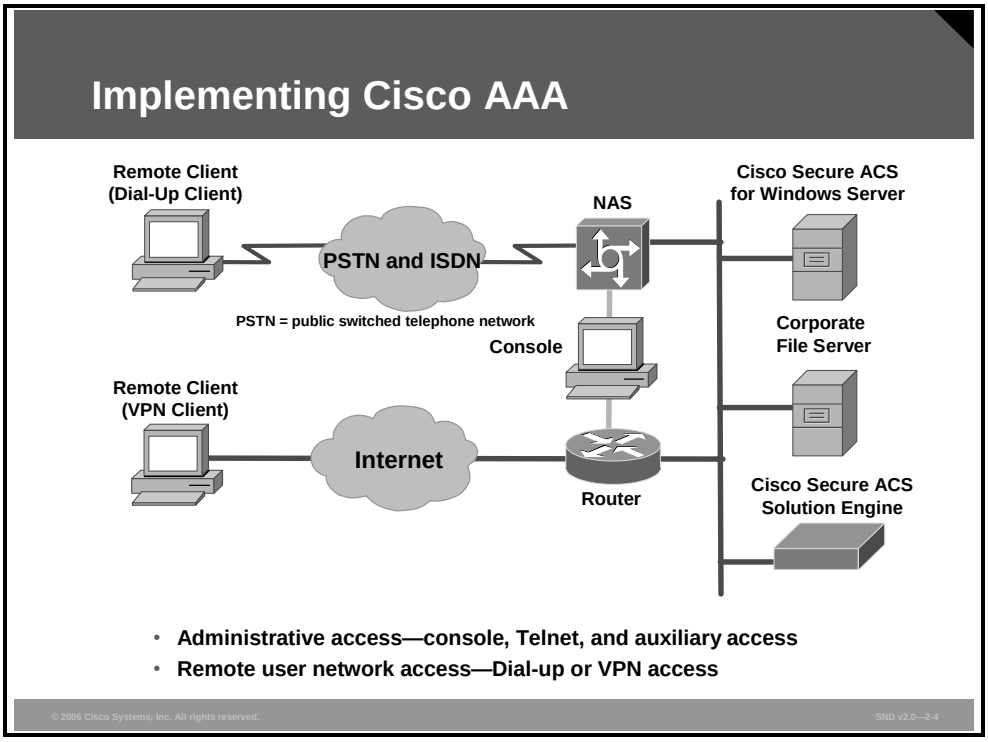
- **Authentication:** Authentication requires users and administrators to prove that they really are who they say they are. Authentication is established using a username and password, challenge and response, token cards, and other methods as in this example: "I am user *student* and my password *validateme* proves it."
- **Authorization:** After authenticating the user and administrator, authorization services decide which resources the user and administrator are allowed to access and which operations the user and administrator are allowed to perform as in this example: "User *student* can access host *serverXYZ* using Telnet."
- **Accounting and auditing:** Accounting records what the user and administrator actually did, what they accessed, and how long they accessed it for accounting and auditing purposes. Accounting keeps track of how network resources are used as in this example: "User *student* accessed host *serverXYZ* using Telnet for 15 minutes."


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Introduction to AAA for Cisco Routers

This topic describes the three ways that Cisco implements AAA services for Cisco routers.




Two examples of AAA implementation include authenticating remote users accessing the corporate LAN through dial-up or Internet (IPsec VPN) connections as shown in the figure and authenticating administrator access to the router console port, auxiliary port, and vty ports.

Cisco networking products support AAA access control using a local usernames-passwords database or remote security server databases. A local security database is configured in the router for a small group of network users using the **username** *xyz* **password** *strongpassword* command. A remote security database is a separate server running an AAA security protocol, providing AAA services for multiple network devices and large numbers of network users.

Cisco provides three ways of implementing AAA services for Cisco routers:

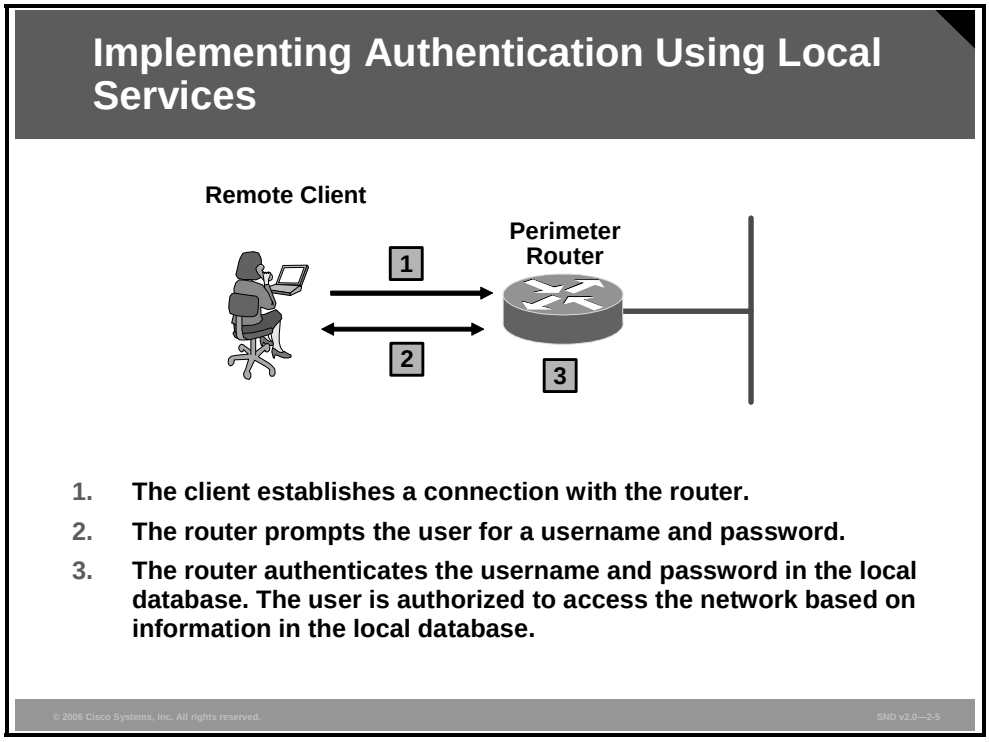
- **Self-contained AAA:** AAA services may be self-contained in the router or network access server (NAS) itself. This form of authentication is also known as local authentication.
- **Cisco Secure Access Control Server (ACS) for Windows Server:** AAA services on the router or NAS contact an external Cisco Secure ACS for Microsoft Windows systems for user and administrator authentication.
- **Cisco Secure ACS Solution Engine:** AAA services on the router or NAS contact an external Cisco Secure ACS Solution Engine for user and administrator authentication.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Authenticating Remote Access

This topic describes the methods of authentication used to provide remote access to a LAN.




If you have one or two NASs or routers providing access to your network for a limited number of users, you may store username and password security information locally on the Cisco NASs or routers. This is referred to as local authentication on a local security database. Local authentication characteristics are as follows:

- Used for small networks
- Stores username and password in the Cisco router
- User authenticates against the local security database in the Cisco router
- Does not require an external database

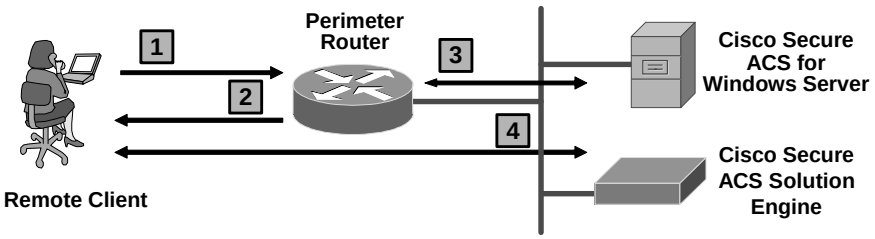
The system administrator must populate the local security database by specifying username and password profiles for each user that might log in.

The figure shows how local authentication typically works.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Implementing Authentication Using External Servers




1. The client establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router passes the username and password to the Cisco Secure ACS (server or engine).
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the router (administrative access) or the network based on information found in the Cisco Secure ACS database.

© 2006 Cisco Systems, Inc. All rights reserved.


The problem with local implementations of AAA is that it does not scale well. Most corporate environments have multiple Cisco routers and NASs with multiple router administrators and hundreds or thousands of users needing access to the corporate LAN. Maintaining local databases for each Cisco router and NAS for this size of network is not feasible.

One or more Cisco Secure ACS systems (servers or engines) can manage the entire user and administrative access needs for an entire corporate network using one or more databases.

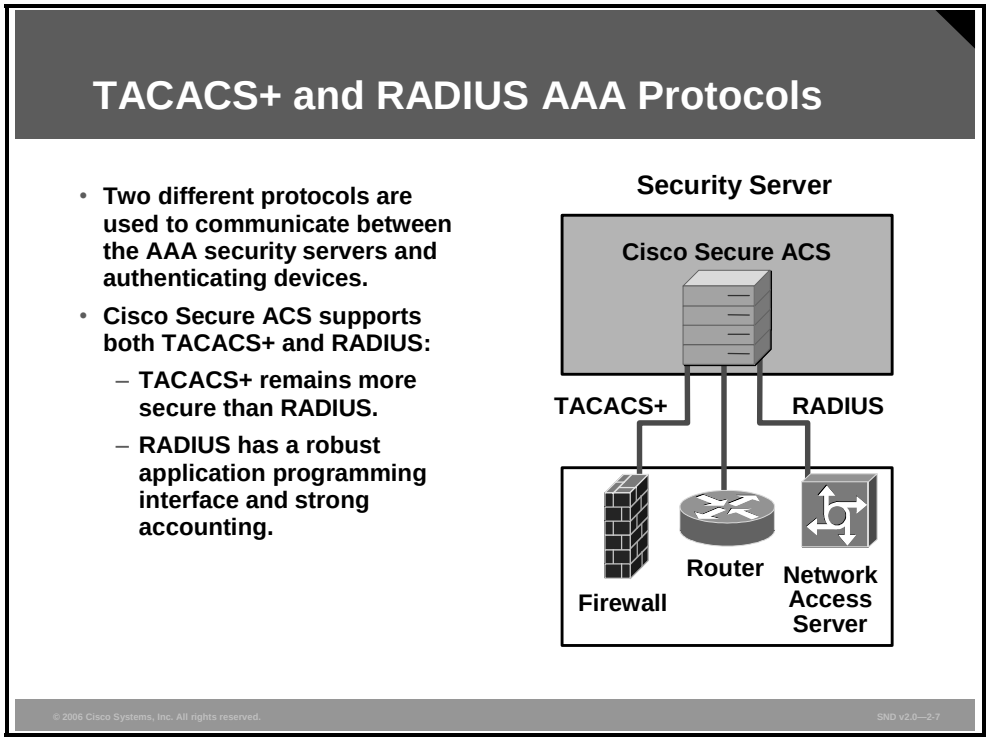
External AAA systems, such as the Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine, communicate with Cisco routers and NASs using the TACACS+ or RADIUS protocols to implement AAA functions.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# TACACS+ and RADIUS AAA Protocols

This topic describes the features of TACACS+ and RADIUS AAA protocols.




TACACS+ and RADIUS are the two predominant AAA protocols used by Cisco security appliances, routers, and switches for implementing AAA. Cisco developed the Cisco Secure ACS Family of AAA servers to support both TACACS+ and RADIUS.

The Cisco Secure ACS Family is a comprehensive and flexible platform for securing access to the network. Cisco Secure ACS secures network access for the following:

- Dial-up access via Cisco network access servers and routers
- Router and switch console, auxiliary, and vty port administrative and network access
- Cisco Adaptive Security Appliance (ASA) products
- Cisco VPN 3000 Series Concentrators (RADIUS only)

Cisco Secure ACS works closely with the NAS, router, Cisco VPN 3000 Concentrator, and Cisco ASA products to implement a comprehensive security policy via the AAA architecture. Cisco Secure ACS also works with industry-leading token cards and servers.

The Cisco Secure ACS for Windows Server is easily managed via standard browsers, which enables simple moves, adds, and changes to usernames, passwords, and network devices. Cisco Secure ACS is implemented on Microsoft Windows 2000 Server platforms.

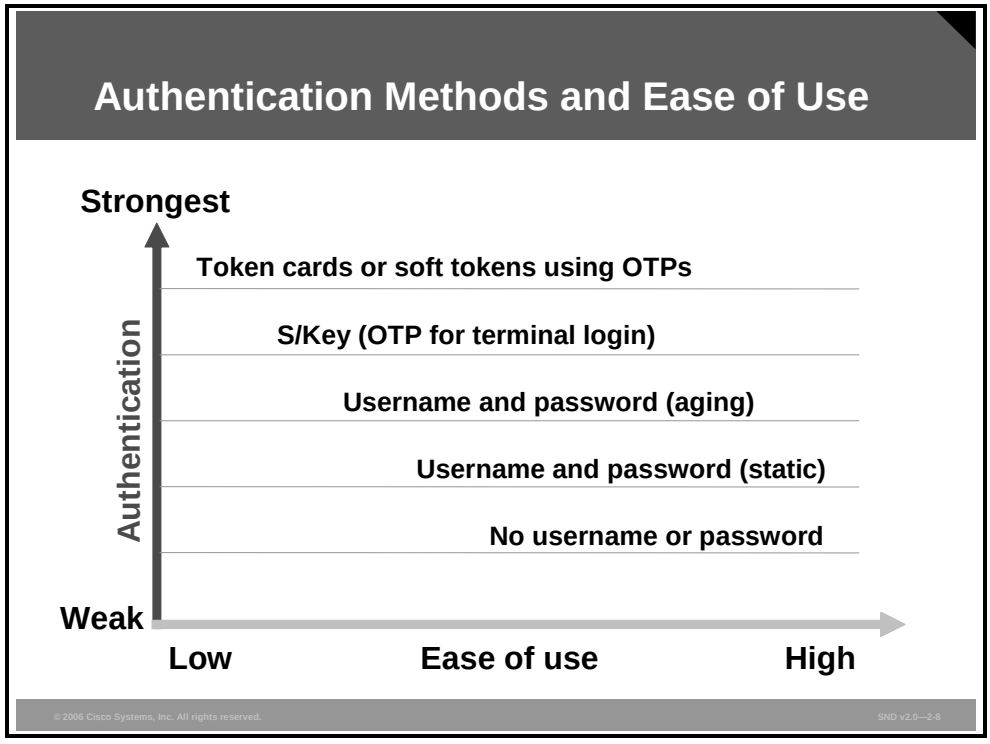
The Cisco Secure ACS Solution Engine performs many of the same functions as the Cisco Secure ACS for Windows Server products but in a single rack-unit, mounted, dedicated hardware platform.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Authentication Methods

This topic describes the various authentication methods in use in terms of the degree of security that they provide and their ease of use.




The most common method of user authentication is the use of usernames and passwords. These methods range from weak to strong in authentication security. Simple authentication methods use a database of usernames and passwords, while methods that are more complex use one-time passwords (OTPs). Consider each of the methods listed in the figure from the bottom of the list up, as follows:

- **No username or password:** Some system administrators and users decide not to use the username and password capabilities of their access devices. This is the least secure option. A network intruder only has to discover the access method to gain access to the networked system.
- **Username and password (static):** The username and password stay the same until changed by the system administrator or user. This method is susceptible to playback attacks, eavesdropping, theft, and password-cracking programs.
- **Username and password (aging):** The username and password expire after a set time (usually 30 to 60 days) and must be reset, usually by the user, before network access is granted. This method is susceptible to playback attacks, eavesdropping, theft, and password cracking, but to a lesser degree than static username and password pairs.



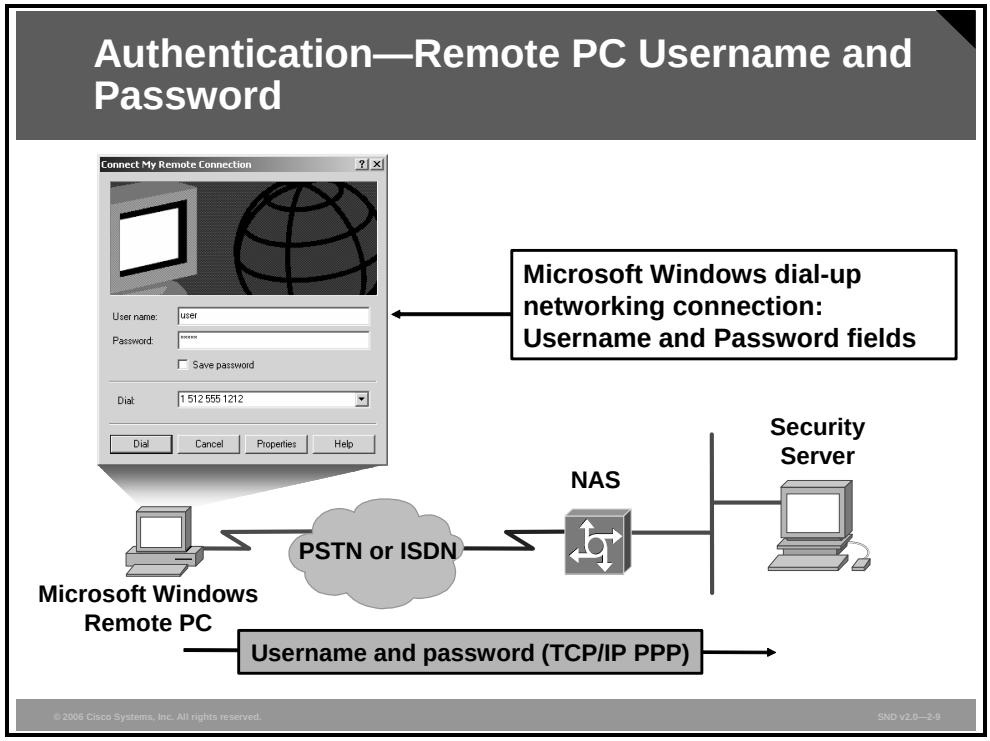
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **OTPs:** Using OTPs is a stronger method than the previous two methods. This method provides the most secure username and password authentication. Most OTP systems are based on a secret passphrase, which is used to generate a list of passwords. OTPs are only good for one login and are therefore not useful to anyone who manages to eavesdrop and capture the OTP. S/Key is an OTP method developed and trademarked by Telcordia (Bellcore) and is typically used for terminal logins. In S/Key, the secret passphrase is used to generate the first password, and each successive password is generated from the previous one by encrypting it. A list of passwords is generated by the S/Key server software and is distributed to users.
- **Token cards and soft tokens:** This method is based on something that you have (token card) and something that you know (token card PIN). Token cards are typically small electronic devices with the relative complexity and approximate size of a credit card calculator. There are many token card vendors, and each has its own token card server. The PIN is placed (manually or automatically generated) into the card, which generates a secure password. A token server receives and validates the password. The password interplay usually consists of a remote client computer, an NAS, and a security server running token security software.

The authentication method should be chosen and implemented based on the guidelines established in the network security policy.

 © 2006 Cisco Systems, Inc.

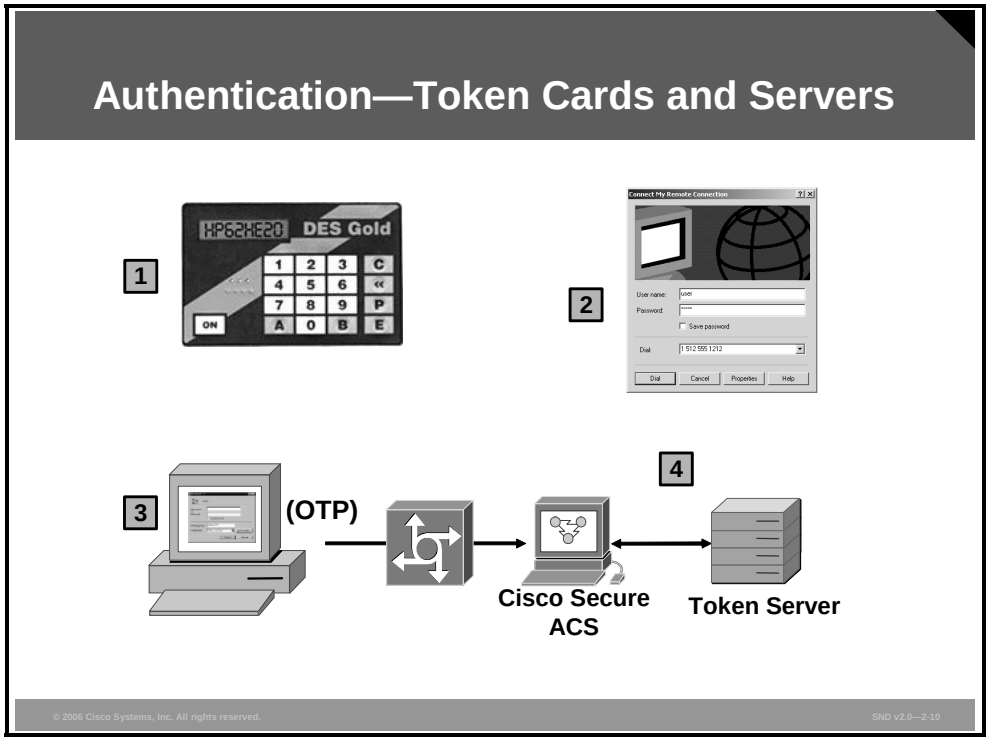
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




An example of dial-up authentication using username and password authentication is shown in the figure. On the client end, a Microsoft Windows dial-up networking connection prompts users for their username and password. This information is sent for authentication over communication lines using TCP/IP and PPP to a remote NAS or a security server. As a matter of policy, do not allow users to check the Save Password check box.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Another OTP authentication method that adds a new layer of security is accomplished with a token card (or “smartcard”) and a token server. Each token card is programmed to a specific user, and each user has a unique PIN that can generate a password keyed strictly to the corresponding card. OTP authentication takes place between the specified token server with a token card database and the user.

Token cards and servers generally work as shown in the figure and as described in these steps:

**Step 1** The user generates an OTP with the token card that uses a security algorithm.

**Step 2** The user enters the OTP into the authentication screen generated by the remote client (in this example the ”Connect My Remote Connection” dialog box).

**Step 3** The remote client sends the OTP to the token server via the network and an authenticating device, either directly or through the AAA server.

**Step 4** The token server uses the same algorithm to verify that the password is correct and authenticates the remote user.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Two token card and server methods are used:

- **Time-based:** In this system, the token card contains a cryptographic key and generates a password (or token) using a PIN entered by the user. The password is entered into the remote client, which sends it to the token server. The password is loosely synchronized in time to the token server. The server compares the token received to a token generated internally. If they match, the user is authenticated and allowed access.
- **Challenge response:** In this system, the token card stores a cryptographic key. The token server generates a random string of digits and sends it to the remote client that is trying to access the network. The remote user enters the random string, and the token card computes a cryptographic function using the stored key and random string. The result is sent back to the token server, which has also computed the function. If the results match, the user is authenticated.

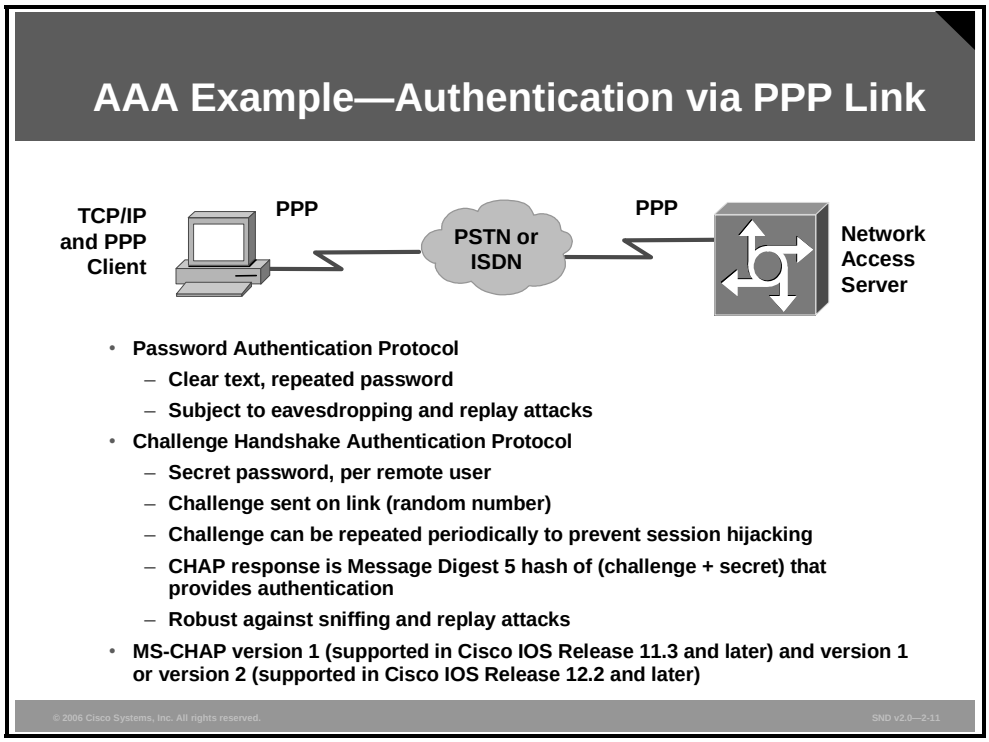
Token cards are now implemented in software for installation on the remote client. SofToken, which generates single-use passwords without the associated cost of a hardware token, is one example of a software token card.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Point-to-Point Authentication Protocols

This topic describes how PPP enables authentication between remote clients and servers using Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).




An important component to consider in remote access security is support for authentication accomplished with PAP, CHAP, and MS-CHAP. PPP is a standard encapsulation protocol for the transport of different network layer protocols (including, but not limited to IP) across serial point-to-point links. PPP enables authentication between remote clients and servers using PAP, CHAP, or MS-CHAP.

PAP provides a simple method for the remote client to establish its identity using a two-way handshake. The handshake is done only after initial PPP link establishment. After the link establishment phase is complete, a username and password pair is repeatedly sent in clear text by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

CHAP is used to periodically verify the identity of the peer using a three-way handshake. The handshake is done upon initial link establishment and may be repeated anytime after the link has been established. Upon link establishment these tasks are executed:

- After the link establishment phase is complete, the authenticator sends a “challenge” message to the peer.
- The peer responds with a value calculated using a one-way hash function based on the received challenge and a secret known only to the authenticator and that remote client. The secret is not sent over the link. Although the authentication is only one-way, by negotiating CHAP in both directions, the same secret set may easily be used for mutual authentication.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection should be terminated.
- At random intervals, the authenticator sends a new challenge to the peer and repeats the three-way handshake steps.

CHAP provides protection against playback attack by the peer using an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges.

MS-CHAP is the Microsoft version of CHAP. MS-CHAP is an extension of the CHAP described in RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP).* MS-CHAP enables PPP authentication between a PC using Microsoft Windows and an NAS. PPP authentication using MS-CHAP can be used with or without AAA security services.

MS-CHAP differs from standard CHAP as follows:

- MS-CHAP is enabled while the remote client and the NAS negotiate PPP parameters after link establishment.
- The MS-CHAP response packet is in a format designed for compatibility with Microsoft Windows networking products.
- MS-CHAP enables the network security server (authenticator) to control retry and password-changing mechanisms. MS-CHAP allows the remote client to change the MS-CHAP password.
- MS-CHAP defines a set of reason-for-failure codes returned to the remote client by the NAS.

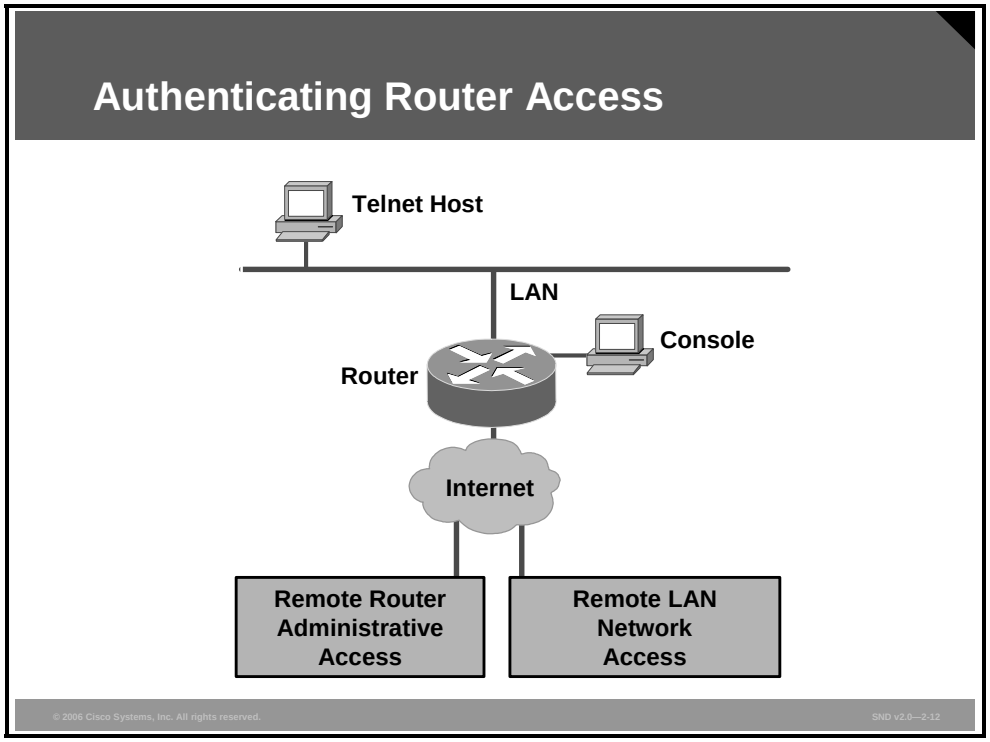
The **ppp authentication ms-chap** command used in Cisco IOS Release 11.3 and later allows Cisco routers to define MS-CHAP authentication.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Authenticating Router Access

This topic describes the three general steps that are required to configure a Cisco router to perform AAA using a local database for authentication.




It is important that you secure the interfaces of all your routers, particularly your network access servers and perimeter routers connecting to the Internet.

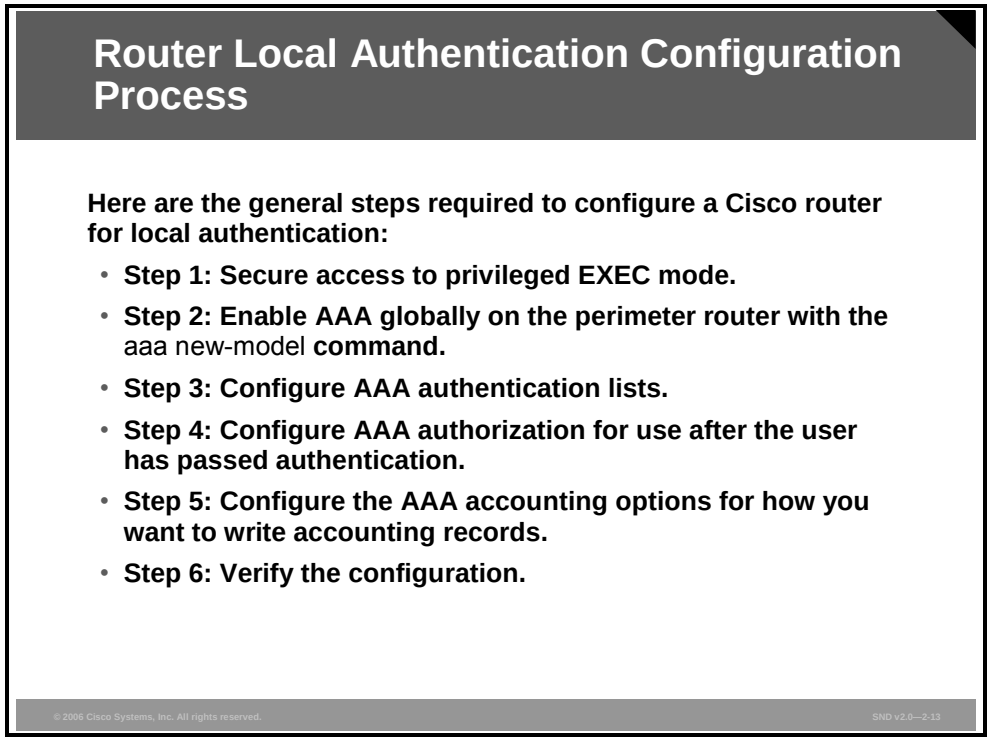
You must configure the router to secure administrative access and remote LAN network access using **aaa** commands. The router access modes, port types, and AAA command elements are compared in the "Router Access" table.

### Router Access

| Access Type | Modes | Network Access Server Ports | Common AAA Command Element |
|---|---|---|---|
| Remote administrative access | Character (line or EXEC mode) | TTY, vty, auxiliary, and console | **login**, **exec**, and **enable** commands |
| Remote network access | Packet (interface mode) | async, group-async BRI and PRI | **ppp** and **network** commands |


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



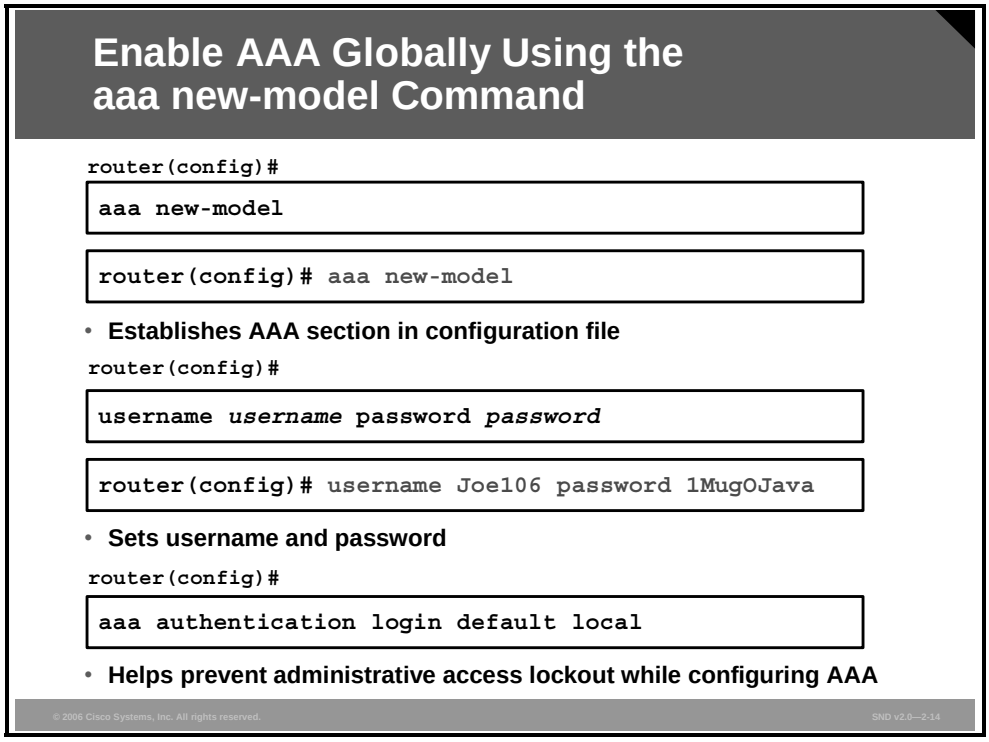

The figure shows the general steps required to configure the router for AAA using local authentication.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Configuring AAA for Cisco Routers

This topic describes how to configure AAA on a Cisco router using **aaa** commands.




The first step in configuring an NAS or router to use the AAA process is to enable AAA using the **aaa new-model** command.

If an administrative Telnet or console session is lost while enabling AAA on a Cisco router and no local AAA user authentication account and method exists, the administrator will be locked out of the router. Therefore, it is important that you configure a local username-password database account and local authentication as shown in the figure.

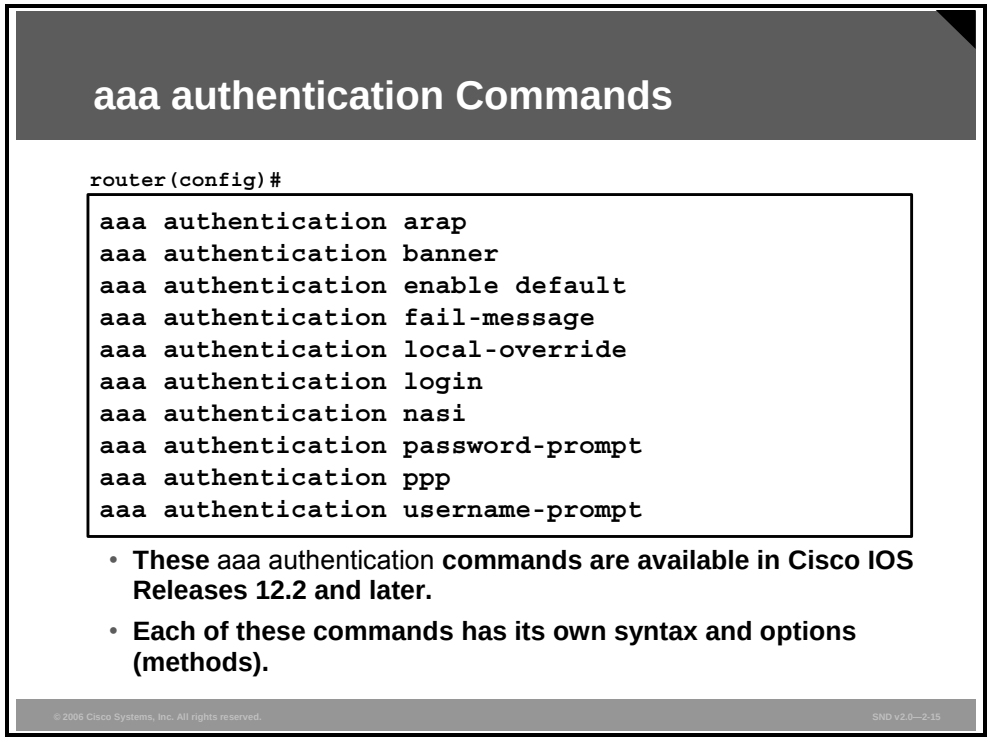
At a minimum, the commands listed here should be entered in this order:

1. Router(config)# **aaa new-model**
2. Router(config)# **username** *username* **password** *password*
3. Router(config)# **aaa authentication login default local**

Specifying the local authentication method enables you to re-establish your Telnet or console session and use the locally defined authentication list to access the router. If you fail to do this and you become locked out of the router, physical access to the router is required (console session), and you will have to perform a password recovery sequence. At worst, the entire configuration saved in NVRAM can be lost.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The figure contains a complete listing of **aaa authentication** commands for Cisco IOS Release 12.2 and later. The "AAA Authentication Commands" table describes each of these commands



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

### AAA Authentication Commands

| Command | Description |
|---|---|
| **aaa authentication arap** | To enable an AAA authentication method for AppleTalk Remote Access Protocol (ARAP) users using RADIUS or TACACS+, use the **aaa authentication arap** global configuration command. Use the **no** form of this command to disable this authentication. |
| **aaa authentication banner** | This command creates a personalized login banner. |
| **aaa authentication enable default** | To enable AAA authentication to determine if a user can access the privileged command level, use the **aaa authentication enable default** global configuration command. Use the **no** form of this command to disable this authorization method. |
| **aaa authentication fail-message** | This command creates a message to be displayed when a user fails login. |
| **aaa authentication local-override** | To configure the Cisco IOS software to check the local user database for authentication before attempting another form of authentication, use the **aaa authentication local-override** global configuration command. Use the **no** form of this command to disable the override. |
| **aaa authentication login** | To set AAA authentication at login, use the **aaa authentication login** global configuration command. Use the **no** form of this command to disable AAA authentication. |
| **aaa authentication nasi** | To specify AAA authentication for NetWare Access Server Interface (NASI) clients connecting through the access server, use the **aaa authentication nasi** global configuration command. Use the **no** form of this command to disable authentication for NASI clients. |
| **aaa authentication password-prompt** | To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** global configuration command. Use the **no** form of this command to return to the default password prompt text. |
| **aaa authentication ppp** | To specify one or more AAA authentication methods for use on serial interfaces running PPP, use the **aaa authentication ppp** global configuration command. Use the **no** form of this command to disable authentication. |
| **aaa authentication username-prompt** | To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** global configuration command. Use the **no** form of this command to return to the default username prompt text. |

It is important that you learn these three commands and how to implement them in an AAA environment:

- The **aaa authentication login** command
- The **aaa authentication ppp** command
- The **aaa authentication enable default** command

After enabling AAA globally on the access server, you need to define the authentication method lists and apply them to lines and interfaces. These authentication method lists are security profiles that indicate the service, PPP, dot1x, or login and authentication method. Up to four authentication methods (local, group TACACS+, group RADIUS, line, or enable authentication) may be applied to a line or interface. A good security practice is to have either local or enable authentication as the final method used to recover from a severed link to the chosen method server.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Complete these steps to define an authentication method list using the **aaa authentication** command:

**Step 1** Use the **aaa authentication** command in global configuration mode to configure an AAA authentication method list, as follows:

1. Specify the service (PPP, dot1x, and so on) or login authentication.
2. Identify a method list name or use the default method list name. The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

   A list name is any alphanumeric string that you choose. Multiple method lists can be configured on the router, but each one has to have a unique method list name.

   A method list is a sequential list describing the authentication methods to be queried to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method has an error. Errors mean that the security server has not responded to an authentication query.

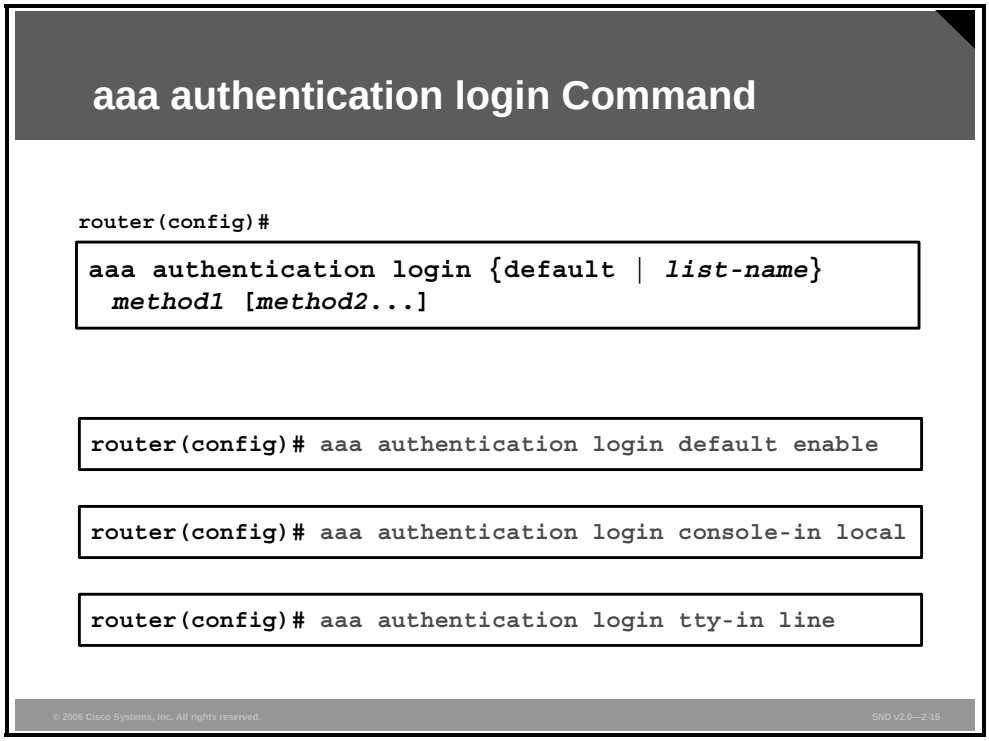
**Step 2** Specify the authentication method (local, group TACACS+, group RADIUS, line, or enable authentication, and so on), and specify how the router should handle requests when one of the methods is not operating (for example, if the AAA server is down). You can specify up to four methods for AAA to try before stopping the authentication process.

**Step 3** After defining these authentication method lists, apply them to each of the following:

- **Lines:** TTY, vty, console, auxiliary, and async lines, or the console port for login and asynchronous lines (in most cases) for ARAP
- **Interfaces:** Interfaces sync, async, and virtual configured for PPP, Serial Line Interface Protocol (SLIP), NASI, or ARAP



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




To set AAA authentication for login to the router administration port, use the **aaa authentication login** command in global configuration mode, as shown in this figure. The entries are defined here:

- The **aaa authentication login default enable** command specifies a default login authentication method list using the enable password.
- The **aaa authentication login console-in local** command specifies a login authentication method list named “console-in” using the local username-password database on the router.
- The **aaa authentication login tty-in line** command specifies a login authentication method list named “tty-in” using the line password configured on the router.

Here is the syntax for the **aaa authentication login** command:



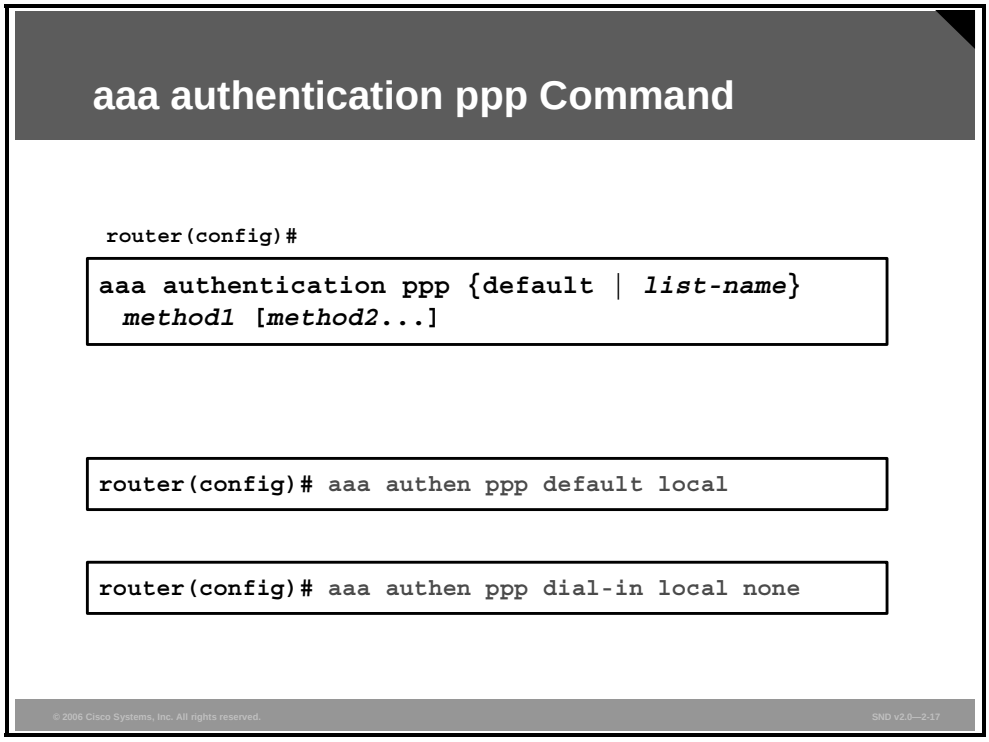
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

**aaa authentication login** {**default** | *list-name*} *method1* [*method2*. . .]

| Command Element | Description |
|---|---|
| **default** | Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in |
| *list-name* | Character string used to name the list of authentication methods activated when a user logs in |
| *method* | Specifies at least one of these keywords:<br>■ **enable:** Uses the enable password for authentication<br>■ **krb5:** Uses Kerberos 5 for authentication<br>■ **krb5-telnet:** Uses the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router<br>■ **line:** Uses the line password for authentication<br>■ **local:** Uses the local username database for authentication<br>■ **local-case:** Uses case-sensitive local username authentication<br>■ **none:** Uses no authentication<br>■ **group radius:** Uses the list of all RADIUS servers for authentication<br>■ **group tacacs+:** Uses the list of all TACACS+ servers for authentication<br>■ **group** *group-name*: Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** commands |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

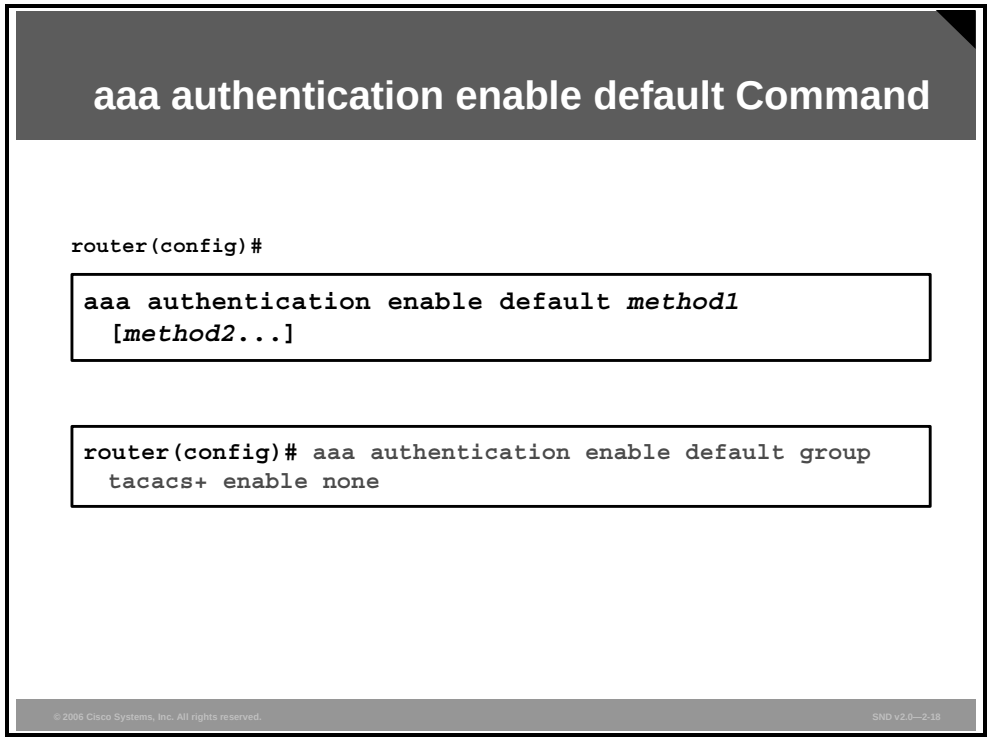



To specify one or more AAA authentication methods for use on serial interfaces running PPP, use the **aaa authentication ppp** command in global configuration mode, as shown in the figure. The entries are defined here:

- The **aaa authentication ppp default local** command specifies a default PPP authentication method list using the local username-password database on the router.
- The **aaa authentication ppp dial-in local none** command specifies a PPP authentication method list named “dial-in” first, using the local username-password database on the router. No authentication is used if the local username is not defined.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Use the **aaa authentication enable default** command in global configuration mode, as shown in this figure, to enable AAA authentication to determine if a user can access the privileged command level.

The syntax for the **aaa authentication enable default** command is as follows:

**aaa authentication enable default** *method1* [*method2. . .]*

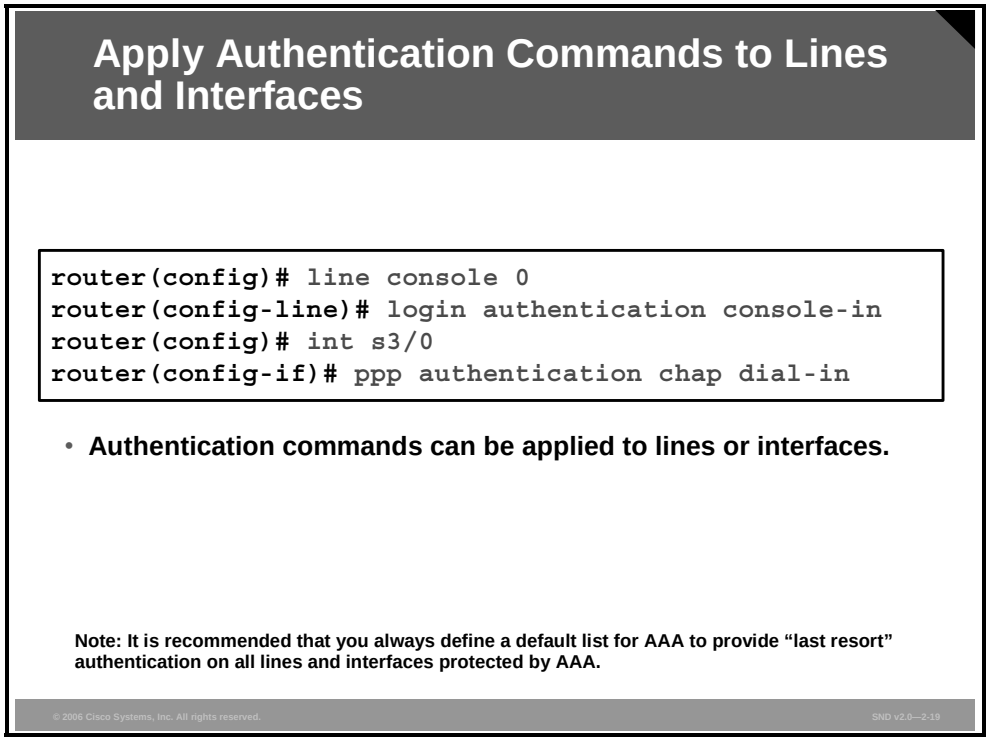
The example in the figure creates an authentication list that first tries to contact a TACACS+ server. If the TACACS+ server does not respond, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured), the user is allowed access to privileged mode with no authentication.

### AAA Authentication Enable Default Methods

| Keyword | Description |
|---|---|
| **enable** | Uses the enable password for authentication |
| **line** | Uses the line password for authentication |
| **none** | Uses no authentication |
| **group radius** | Uses the list of all RADIUS hosts for authentication<br>Note: The RADIUS method does not work on a per-username basis. |
| **group tacacs+** | Uses the list of all TACACS+ hosts for authentication |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** commands |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



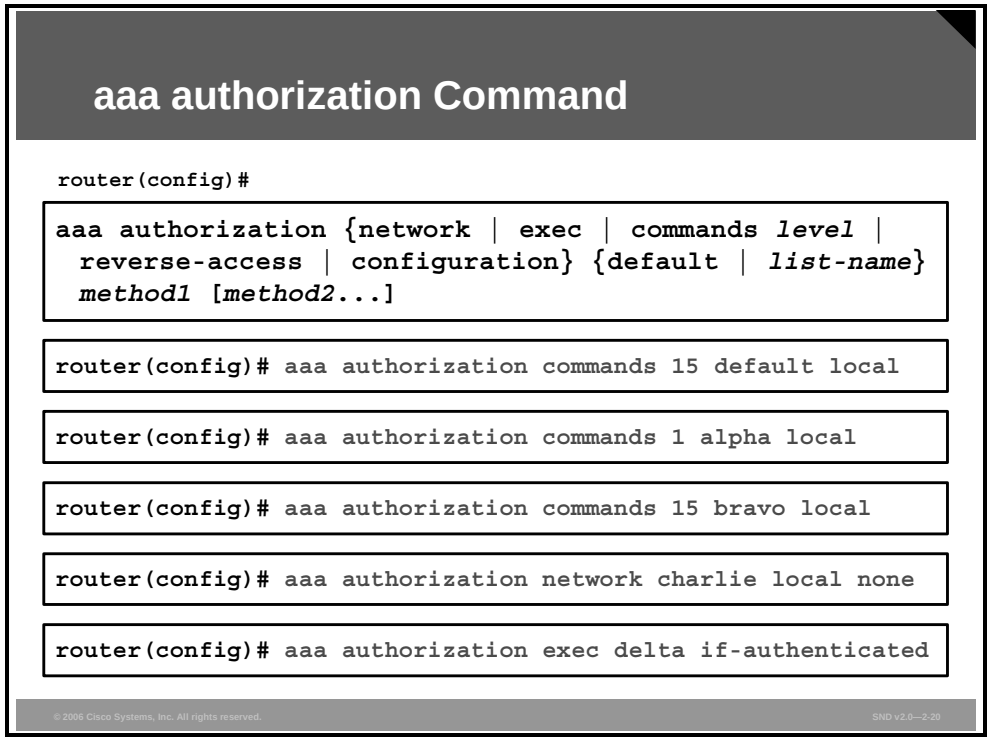

As shown in the figure, authentication commands can be applied to router lines and interfaces.

Here is a brief explanation of the examples shown in the figure:

- **line console 0:** Enters line console configuration mode
- **login authentication console-in:** Uses the authentication method list named "console-in" for login authentication on console port 0
- **int s3/0:** Specifies port 0 of serial interface slot number 3
- **ppp authentication chap dial-in:** Uses the authentication method list named "dial-in" for PPP CHAP authentication on interface s3/0



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Use the **aaa authorization** command in global configuration mode, as shown in the figure, to set parameters that restrict administrative EXEC access to the routers or user access to the network.

The syntax for the **aaa authorization** command is as follows:

**aaa authorization** {**network | exec | commands** *level* | **reverse-access | configuration**} {**default** | *list-name*} *method1* [*method2. . .*]

Refer to the "AAA Authorization Command Syntax" table for a full description of the command syntax.

### AAA Authorization Command Syntax

| Command Element | Description |
|---|---|
| **network** | This command element runs authorization for all network-related service requests, including SLIP, PPP Network Control Protocol (NCP), and ARAP. |
| **exec** | This command element runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as **autocommand** command information. |
| **commands** | This command element runs authorization for all commands at the specified privilege level. |
| *level* | This is the specific command level that should be authorized. Valid entries are 0 to 15. |
| **reverse-access** | This command element runs authorization for reverse access connections, such as reverse Telnet. |
| **configuration** | This command element downloads the configuration from the AAA server. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

| Command Element | Description |
|---|---|
| **default** | This command element uses the listed authentication methods, *list-name* and *method*, as the default list of methods for authorization. |
| *list-name* | This is the character string that is used to name the list of authorization methods. |
| *method* | This specifies at least one of these keywords:<br>■ **group** *group-name***:** Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** commands<br>■ **if-authenticated:** Allows the user to access the requested function if the user is authenticated<br>■ **krb5-instance:** Uses the instance defined by the **kerberos instance map** command<br>■ **local:** Uses the local database for authorization<br>■ **none:** No authorization performed |

There is a provision for naming the authorization list after specifying the service just as there is for naming an authentication list. Also, the list of methods is not limited to a single method but may have up to four failing over methods listed, similar to what the **aaa authentication** command provides.

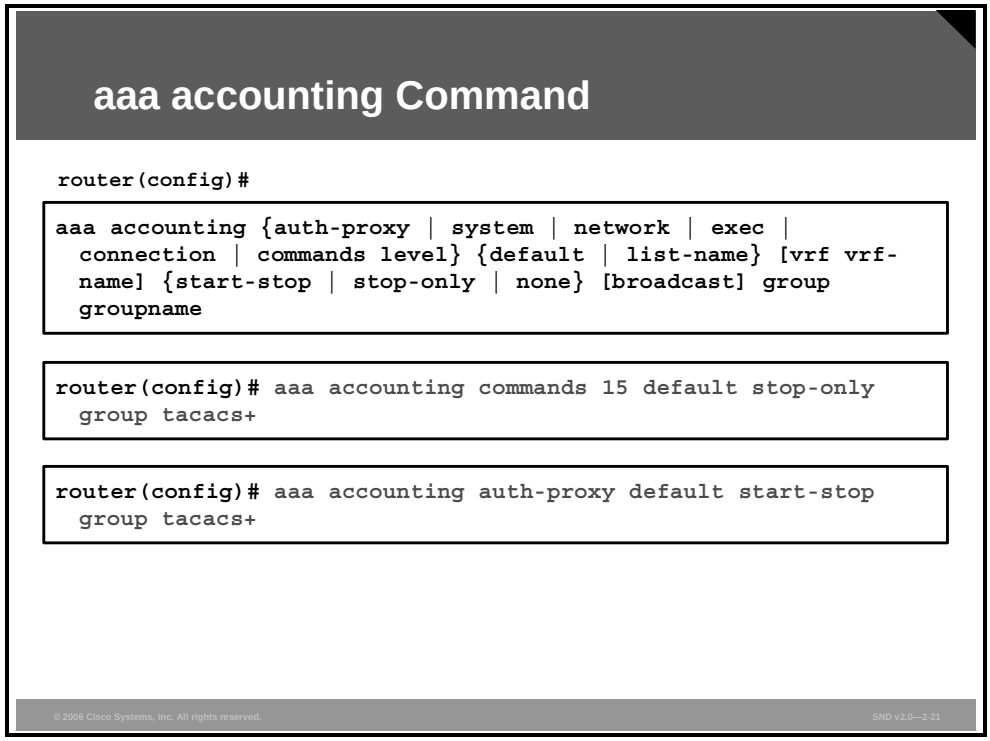
Named authorization lists allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

A brief explanation of the examples is as follows:

- **aaa authorization commands 1 alpha local:** This command uses the local username database to authorize the use of all level 1 commands for the alpha method list.
- **aaa authorization commands 15 bravo local: This command** uses the local database to authorize the use of all level 15 commands for the bravo method list.
- **aaa authorization network charlie local none: This command** uses the local database to authorize the use of all network services, such as SLIP, PPP, and ARAP, for the charlie method list. If the local username is not defined, this command performs no authorization and the user can use all network services.
- **aaa authorization exec delta if-authenticated: This command** lets the user run the EXEC process if the user is already authenticated.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




To enable AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command. Refer to the "AAA Accounting Command Syntax" table for a description of the command syntax.

The first example in the figure defines a default command accounting method list where accounting services are provided by a TACACS+ security server set for privilege level 15 commands with a stop-only restriction.

The second example defines a default authentication proxy accounting method list where accounting services are provided by a TACACS+ security server for authentication proxy events with a start-stop restriction.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## AAA Accounting Command Syntax

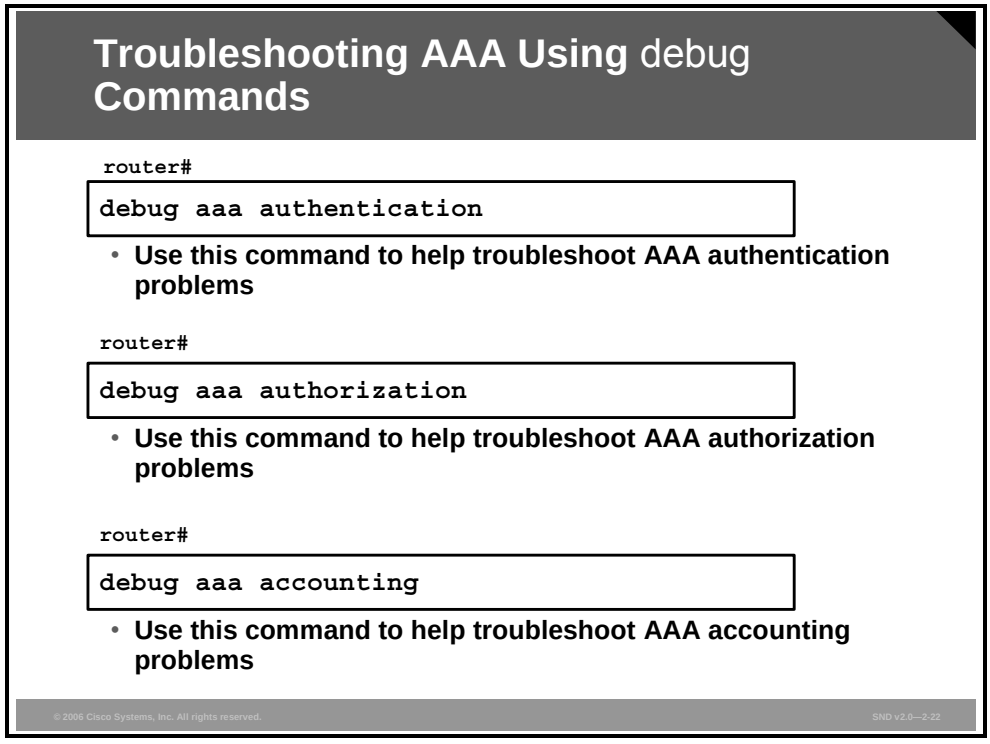
| Command Element | Description |
|---|---|
| **auth-proxy** | This command element provides information about all authenticated proxy user events. |
| **system** | This command element performs accounting for all system-level events not associated with users, such as reloads. |
| **network** | This command element runs accounting for all network-related service requests, including SLIP, PPP, PPP NCP, and ARAP. |
| **exec** | This command element runs accounting for EXEC shell sessions. This keyword might return user profile information, such as what is generated by the **autocommand** command. |
| **connection** | This command element provides information about all outbound connections made from the NAS, such as Telnet, local-area transport (LAT), IBM TN3270 terminal emulator, packet assembler and disassembler, and rlogin. |
| **commands level** | This command element runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 to 15. |
| **default** | This command element makes the listed accounting methods, named by *list-name,* to be the default list of methods for accounting services. |
| **list-name** | This is the character string that is used to name the list of at least one of the accounting methods. |
| **vrf** *vrf-name* | (Optional) This command element specifies a VPN routing and forwarding (VRF) configuration.<br>Note: VRF is used only with system accounting. |
| **start-stop** | This command element sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice was received by the accounting server. |
| **stop-only** | This command element sends a stop accounting notice at the end of the requested user process. |
| **none** | This command element disables accounting services on this line or interface. |
| **broadcast** | (Optional) This command element enables sending accounting records to multiple AAA servers. It simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. |
| **group** *group-name* | This command element defines the character string used to name the group of accounting methods. |


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Troubleshooting AAA for Cisco Routers

This topic explains how to troubleshoot AAA on a Cisco peripheral router using **debug aaa** commands.




Use these **debug** commands on your routers to trace AAA packets and monitor authentication, authorization, or accounting activities:

- The **debug aaa authentication** command displays debugging messages on authentication functions.
- The **debug aaa authorization** command displays debugging messages on authorization functions.
- The **debug aaa accounting** command displays debugging messages on accounting functions.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Troubleshooting AAA Using the debug aaa authentication Command

```
router# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN
  priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1'
  list=''
action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default"
  list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```

© 2006 Cisco Systems, Inc. All rights reserved.


To display information on AAA authentication, use the **debug aaa authentication** command in privileged EXEC command mode, as shown in the figure. Use the **no debug aaa authentication** form of the command to disable this debug mode.

This figure contains debug output for a successful AAA authentication using a local database.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Troubleshooting AAA Using the debug aaa accounting Command

```
router# debug aaa accounting
16:49:21: AAA/ACCT: EXEC acct start, line 10
16:49:32: AAA/ACCT: Connect start, line 10, glare
16:49:47: AAA/ACCT: Connection acct stop:
task_id=70 service=exec port=10 protocol=telnet
  address=172.31.3.78 cmd=glare bytes_in=308
  bytes_out=76 paks_in=45 paks_out=54 elapsed_time=14
```

© 2006 Cisco Systems, Inc. All rights reserved.

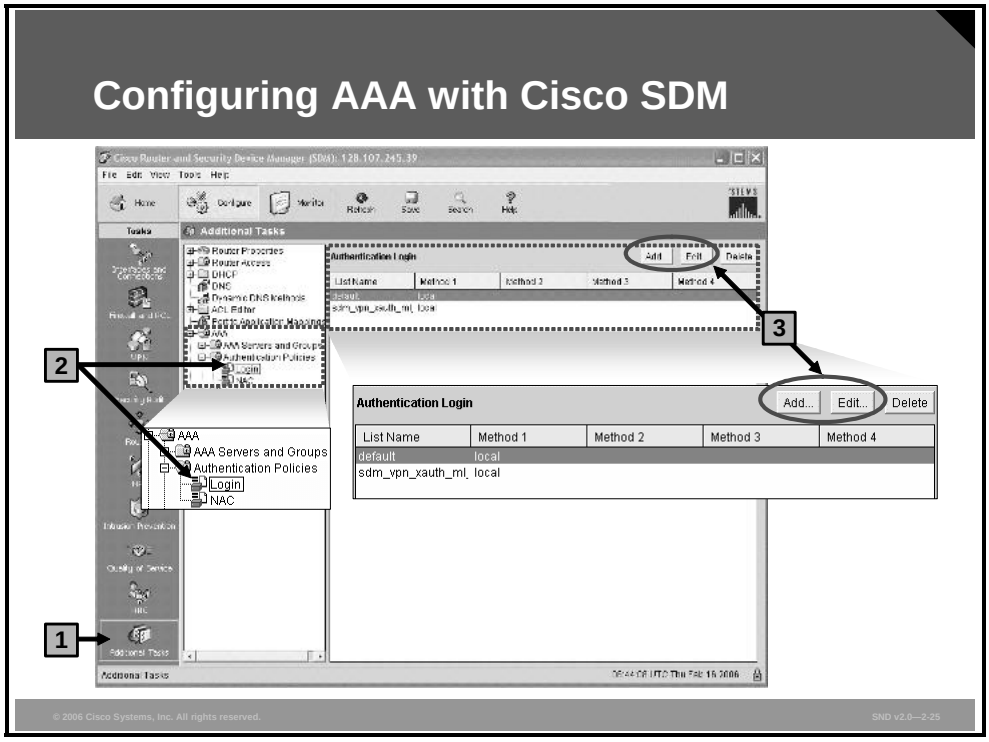

To display information on AAA accounting, use the **debug aaa accounting** command in privileged EXEC command mode, as shown in the figure. Use the **no debug aaa accounting** form of the command to disable this debug mode.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Configuring AAA with Cisco SDM

This topic describes how to configure AAA using the Cisco SDM GUI.




AAA can also be configured and edited using Cisco SDM. After the **aaa new-model** command has been configured on the router using the CLI, choose **Additional Tasks > AAA**.

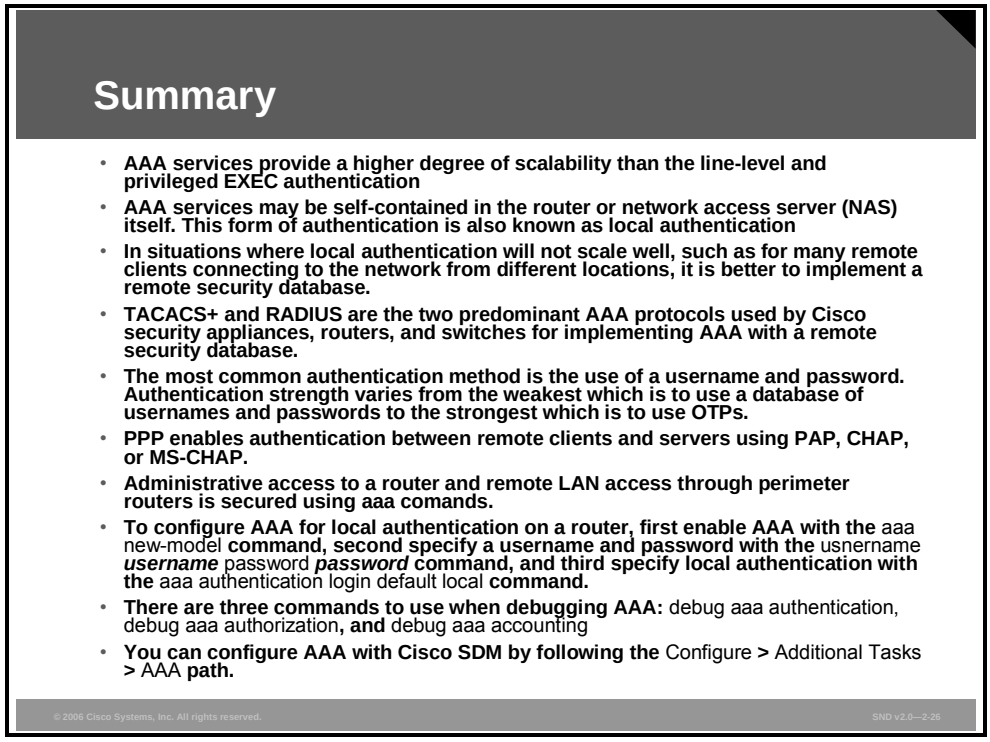
The figure shows the AAA Authentication Login configuration screen. It shows the two login authentication method lists configured on the router. One is the default method list, and the other is the sdm_vpn_xauth_ml_1 method list. Both method lists use the local database to perform login authentication. This screen can be used to configure new login authentication method lists, or to edit or delete existing login authentication method lists on the router.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Lesson 5

# Disabling Unused Cisco Router Network Services and Interfaces

## Overview

Cisco routers are initially deployed with services that are enabled by default.

This lesson concerns Cisco configuration settings that network administrators should consider changing on their routers, especially on their perimeter routers, to improve security. The lesson presents basic configuration settings that are almost universally applicable in IP networks and a few unexpected situations that you should be aware of.

The list of configuration settings discussed is not exhaustive, and it cannot be substituted for understanding on the part of the network administrator; it is meant to be a reminder of some of the things that are sometimes forgotten. Many of the services that can be enabled in Cisco routers require careful security configuration. However, this lesson describes services that are enabled by default, or that are almost always enabled by users, and that may need to be disabled.

Consideration of these services is particularly important because some of the default settings in Cisco IOS software are there for historical reasons; they made sense when they were chosen but would probably be different if new defaults were chosen today. Other defaults make sense for most systems but may create security exposures if they are used in devices that form part of a network perimeter defense. Still other defaults are actually required by standards but are not always desirable from a security point of view.

This lesson describes ways to secure networks by shutting off unnecessary network services and interfaces.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Objectives

Upon completing this lesson, you will be able to disable unused Cisco router network services and interfaces. This ability includes being able to meet these objectives:

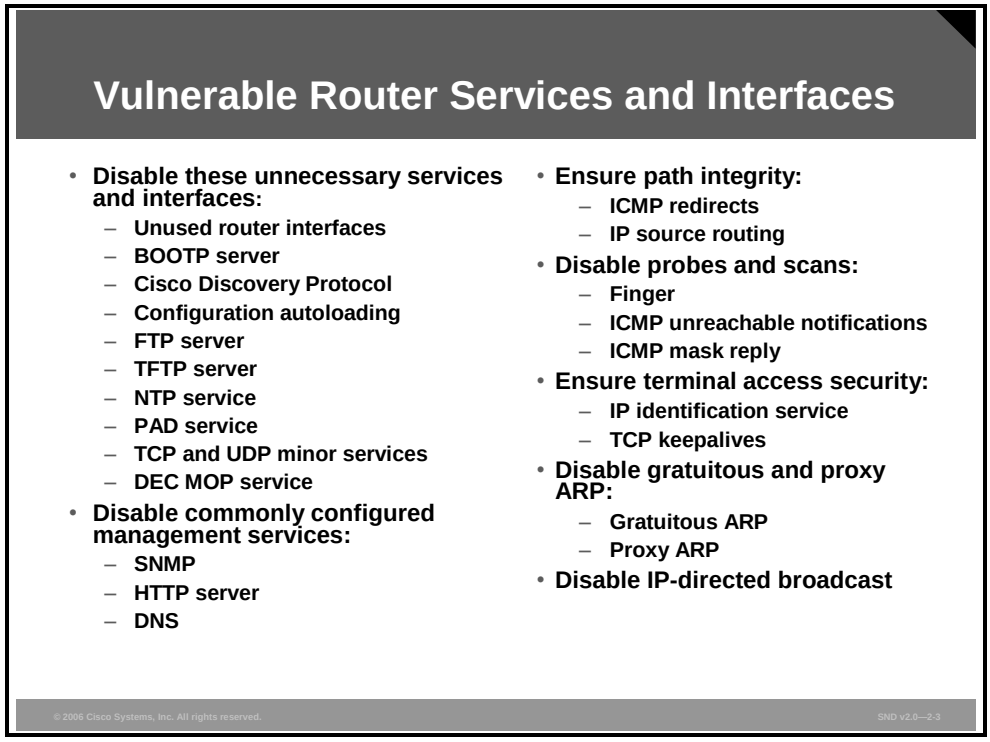
- Describe the router services and interfaces that are vulnerable to network attacks
- Explain the vulnerabilities posed by commonly configured router management services
- Describe how to secure a router with the Cisco SDM One-Step Lockdown feature or the CLI **auto secure** command
- Explain the limitations of using the Cisco SDM One-Step Lockdown feature


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Vulnerable Router Services and Interfaces

This topic describes the router services and interfaces that are vulnerable to network attacks.




Cisco routers support many network services that may not be required in certain enterprise networks. The services listed in the figure have been chosen for their vulnerability to malicious exploitation. These are the router services most likely to be used in network attacks. For ease of learning, the services are grouped as follows:

- **Disable unnecessary services and interfaces**:
  - **Router interfaces:** You should limit unauthorized access to the router and the network by disabling unused open router interfaces.
  - **Bootstrap Protocol (BOOTP) server:** This service is enabled by default. This service allows a router to act as a BOOTP server for other routers. This service is rarely required and should be disabled.
  - **Cisco Discovery Protocol (CDP):** This service is enabled by default. CDP is used primarily to obtain protocol addresses of neighboring Cisco devices and to discover the platforms of those devices. CDP is media- and protocol-independent and runs on most equipment manufactured by Cisco, including routers, access servers, switches, and IP phones. If not required, this service should be disabled globally or on a per-interface basis.
  - **Configuration autoloading:** This service is disabled by default. Autoloading of configuration files from a network server should remain disabled when not in use by the router.
  - **FTP server:** This service is disabled by default. The FTP server enables you to use your router as an FTP server for FTP client requests. Because it allows access to certain files in the router flash memory, this service should be disabled when it is not required.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **TFTP server:** This service is disabled by default. The TFTP server enables you to use your router as a TFTP server for TFTP clients. This service should be disabled when it is not in use, because it allows access to certain files in the router flash memory.
- **Network Time Protocol (NTP) service:** This service is disabled by default. When enabled, the router acts as a time server for other network devices. If configured insecurely, NTP can be used to corrupt the router clock and potentially the clock of other devices that learn time from the router. Correct time is essential for setting proper time stamps for IPsec encryption services, log data, and diagnostic and security alerts. If this service is used, restrict which devices have access to NTP. Disable this service when it is not required.
- **Packet assembler/disassembler (PAD) service:** This service is enabled by default. The PAD service allows access to X.25 PAD commands when forwarding X.25 packets. This service should be explicitly disabled when not in use.
- **TCP and UDP minor services:** Theses services are enabled in Cisco IOS software releases before Cisco IOS Release 11.3 and disabled in Cisco IOS Release 11.3 and later. The minor services are provided by small servers (daemons) running in the router. They are potentially useful for diagnostics but are rarely used. Disable this service explicitly.
- **Maintenance Operation Protocol (MOP) service:** This service is enabled on most Ethernet interfaces. MOP is a Digital Equipment Corporation (DEC) maintenance protocol that should be explicitly disabled when it is not in use.

- **Disable and restrict commonly configured management services:**
  - **Simple Network Management Protocol (SNMP):** This service is enabled by default. The SNMP service allows the router to respond to remote SNMP queries and configuration requests. If required, restrict which SNMP systems have access to the router SNMP agent and use SNMP version 3 (SNMPv3) whenever possible, because this version offers secure communication not available in earlier versions of SNMP. Disable this service when it is not required.
  - **HTTP or HTTP Secure (HTTPS) configuration and monitoring:** The default setting for this service is Cisco device dependent. This service allows the router to be monitored or have its configuration modified from a web browser via an application such as the Cisco Router and Security Device Manager (SDM). You should disable this service if it is not required. If this service is required, restrict access to the router HTTP or HTTPS service using access control lists (ACLs).
  - **Domain Name System (DNS):** This client service is enabled by default. By default, Cisco routers broadcast name requests to 255.255.255.255. Restrict this service by disabling it when it is not required. If the DNS lookup service is required, make sure that you set the DNS server address explicitly.
- **Ensure path integrity:**
  - **Internet Control Message Protocol (ICMP) redirects:** This service is enabled by default. ICMP redirects cause the router to send ICMP redirect messages whenever the router is forced to resend a packet through the same interface on which it was received. This information can be used by attackers to redirect packets to an untrusted device. This service should be disabled when not required.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- **IP source routing:** This service is enabled by default. The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that a datagram will take toward its ultimate destination and, generally, the route that any reply will take. These options can be exploited by an attacker to bypass the intended routing path and security of the network. Also, some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending datagrams with source routing options. Disable this service when it is not required.

- **Disable probes and scans:**
  - **Finger service:** This service is enabled by default. The finger protocol (port 79) allows users throughout the network to obtain a list of the users currently using a particular device. The information displayed includes the processes running on the system, the line number, connection name, idle time, and terminal location. This information is provided through the Cisco IOS software **show users** EXEC command. Unauthorized persons can use this information for reconnaissance attacks. Disable this service when it is not required.
  - **ICMP unreachable notifications:** This service is enabled by default. This service notifies senders of invalid destination IP networks or specific IP addresses. This information can be used to map networks and should be explicitly disabled on interfaces to untrusted networks.
  - **ICMP mask reply:** This service is disabled by default. When enabled, this service tells the router to respond to ICMP mask requests by sending ICMP mask reply messages containing the interface IP address mask. This information can be used to map the network, and this service should be explicitly disabled on interfaces to untrusted networks.

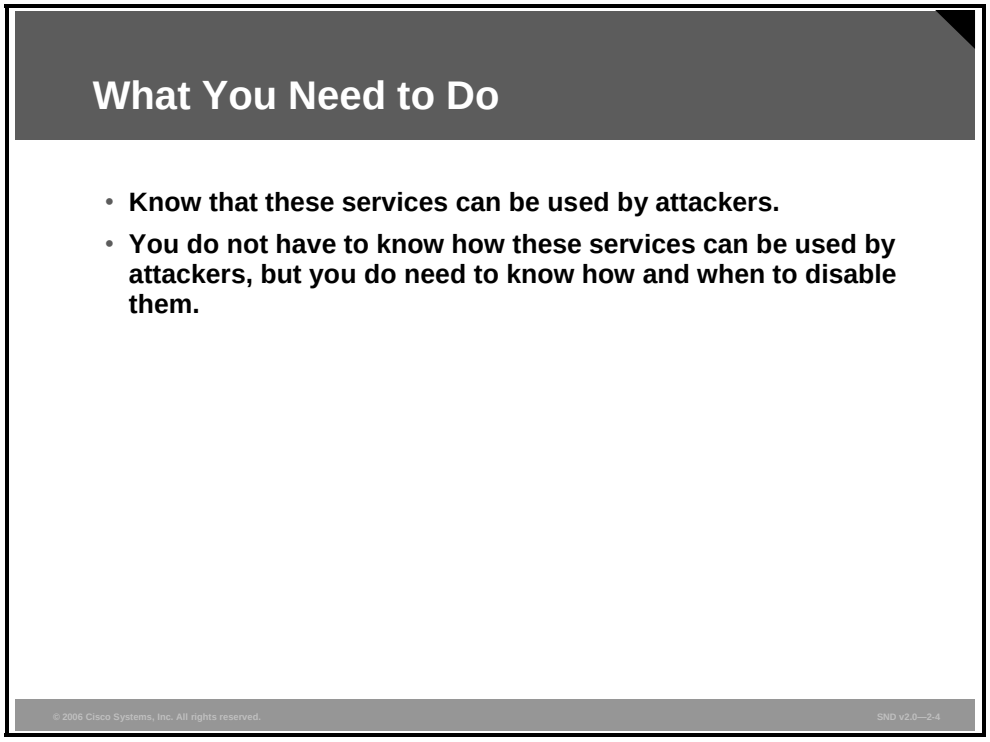
- **Ensure terminal access security:**
  - **IP identification service:** This service is enabled by default. The identification protocol (specified in RFC 1413, *Identification Protocol*) reports the identity of a TCP connection initiator to the receiving host. This data can be used by an attacker to gather information about your network, and this service should be explicitly disabled.
  - **TCP keepalives:** This service is disabled by default. TCP keepalives help “clean up” TCP connections where a remote host has rebooted or otherwise stopped processing TCP traffic. Keepalives should be enabled globally to manage TCP connections and prevent certain denial of service (DoS) attacks.

- **Disable gratuitous and proxy Address Resolution Protocol (ARP):**
  - **Gratuitous ARP:** This service is enabled by default. Gratuitous ARP is the main mechanism used in ARP poisoning attacks. You should disable gratuitous ARPs on each router interface unless this service is needed.
  - **Proxy ARP:** This service is enabled by default. This feature configures the router to act as a proxy for Layer 2 address resolution. This service should be disabled unless the router is being used as a LAN bridge.

- **Disable IP-directed broadcast:** This service is enabled in Cisco IOS software releases before Cisco IOS Release 12.0 and disabled in Cisco IOS Release 12.0 and later. IP-directed broadcasts are used in the common and popular smurf DoS attacks and other related attacks. This service should be disabled when not required.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



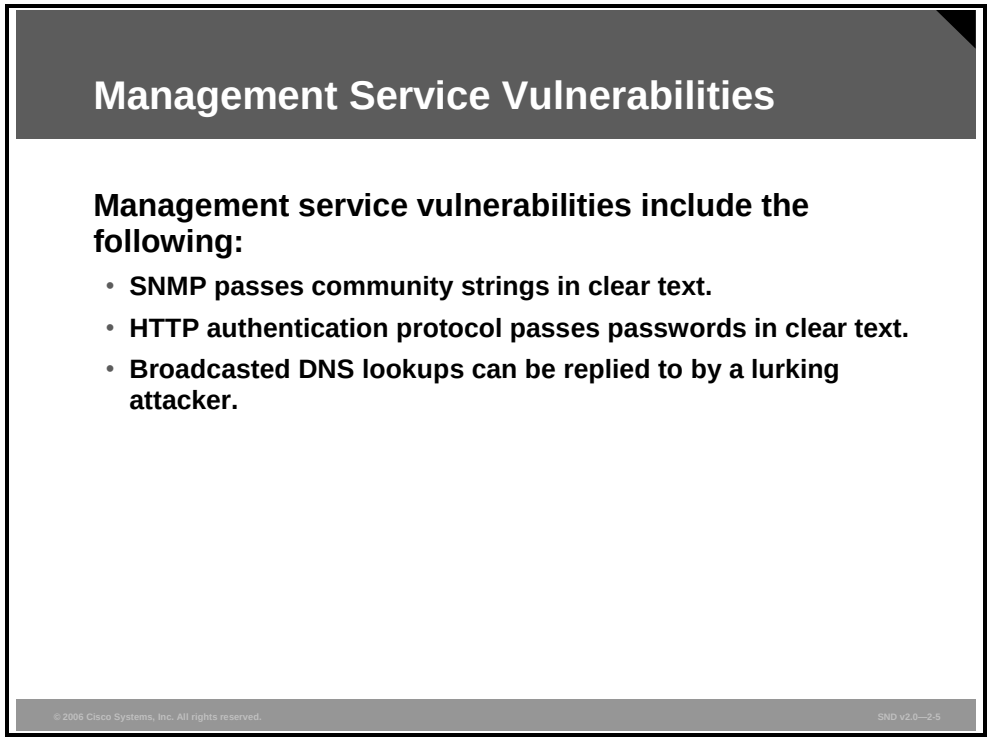

Leaving unused network services enabled increases the possibility of malicious exploitation of those services. Turning off or restricting access to unused services greatly improves network security. While it is not required that you explain why many of these services pose the vulnerabilities they do, you do need to know how and when they need to be disabled.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Management Service Vulnerabilities

This topic explains the vulnerabilities posed by commonly configured management services.




SNMP is a network protocol that provides a facility for managing the network devices through a network management system (NMS). SNMP is very widely used for router monitoring and frequently used for router configuration changes. Version 1 of the SNMP protocol (SNMPv1), however, which is the most commonly used, is often a security risk for these reasons:

- SNMPv1 uses authentication strings called community strings, which are stored and sent across the network in plain text. Most SNMP implementations send these strings repeatedly as part of periodic polling.
- SNMPv1 is easily spoofed.

Because SNMP can be used to retrieve a copy of the network routing table, and other sensitive network information, Cisco recommends disabling SNMP if your network does not require it or that you use SNMPv3, which has much stronger security mechanisms.

Most Cisco IOS software releases support remote configuration and monitoring using HTTP. The authentication protocol used for HTTP sends a clear text password across the network. With HTTP Secure (HTTPS), the session data is encrypted. Cisco SDM uses either HTTP or HTTPS.

Access to the HTTP and HTTPS service should be limited by configuring an access class that only allows access to directly connected nodes.

By default, the Cisco router DNS lookup service sends name queries to the 255.255.255.255 broadcast address. Using this broadcast address should be avoided because it may allow an attacker to emulate one of your DNS servers and respond to router queries with erroneous data.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

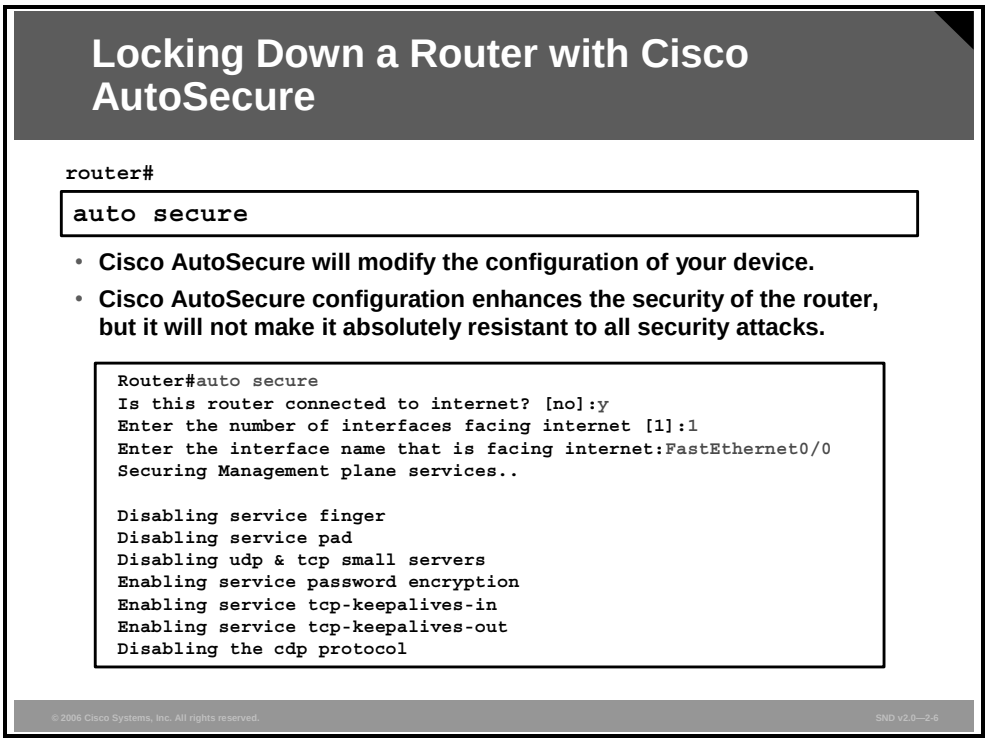
This service is enabled by default. If your routers need to use this service, make sure that you explicitly set the IP address of your DNS servers in the router configuration.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Locking Down Your Router with Cisco AutoSecure

This topic explains how to secure a router with the Cisco SDM One-Step Lockdown feature or the command-line interface (CLI) **auto secure** command.




Cisco AutoSecure is a Cisco IOS feature that lets you more easily configure security features on your router, so that your network is better protected. Cisco AutoSecure can be configured from the privileged EXEC mode using the **auto secure** command in one of these two modes:

- Interactive mode prompts the user with options to enable and disable services and other security features. Cisco AutoSecure defaults to this mode.
- Noninteractive mode automatically executes the Cisco AutoSecure command with the recommended Cisco default settings. This mode is enabled with the **no-interact** command option.

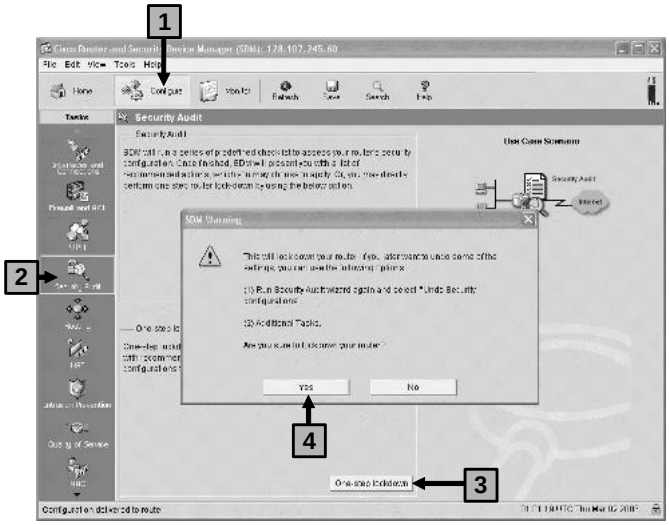
The figure shows an abstracted example of the first three steps of an interactive Cisco AutoSecure configuration.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Locking Down a Router with Cisco SDM

1. **Choose** Configure**.**
2. **Choose** Security Audit**.**
3. **Click** One-step Lockdown**.**
4. **In the Cisco SDM Warning dialog box, click Yes.**
5. **Deliver commands to the router.**



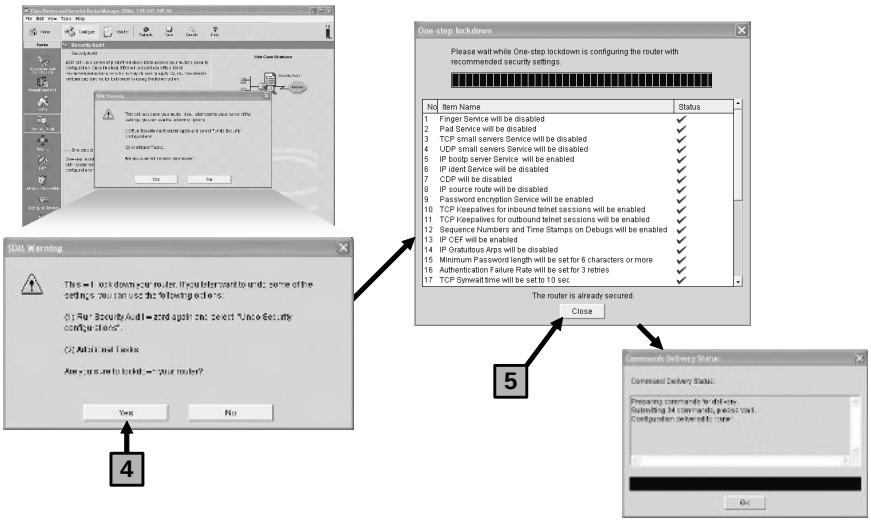

© 2006 Cisco Systems, Inc. All rights reserved.


Cisco SDM implements almost all of the configurations that Cisco AutoSecure offers with the One-Step Lockdown feature. This feature is found in the Configure mode on the Security Audit page.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Locking Down a Router with Cisco SDM (Cont.)




© 2006 Cisco Systems, Inc. All rights reserved.


One-Step Lockdown tests your router configuration for any potential security problems and automatically makes any necessary configuration changes to correct any problems found. The conditions checked for and, if needed, corrected are as follows:

- Disable finger service
- Disable PAD service
- Disable TCP small servers service
- Disable UDP small servers service
- Disable IP BOOTP server service
- Disable IP identification service
- Disable CDP
- Disable IP source route
- Enable password encryption service
- Enable TCP keepalives for inbound Telnet sessions
- Enable TCP Keepalives for outbound Telnet sessions
- Enable sequence numbers and time stamps on debugs
- Enable IP CEF
- Disable IP gratuitous ARPs
- Set minimum password length to less than 6 characters
- Set authentication failure rate to less than 3 retries
- Set TCP synwait time
- Set banner
- Enable logging



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

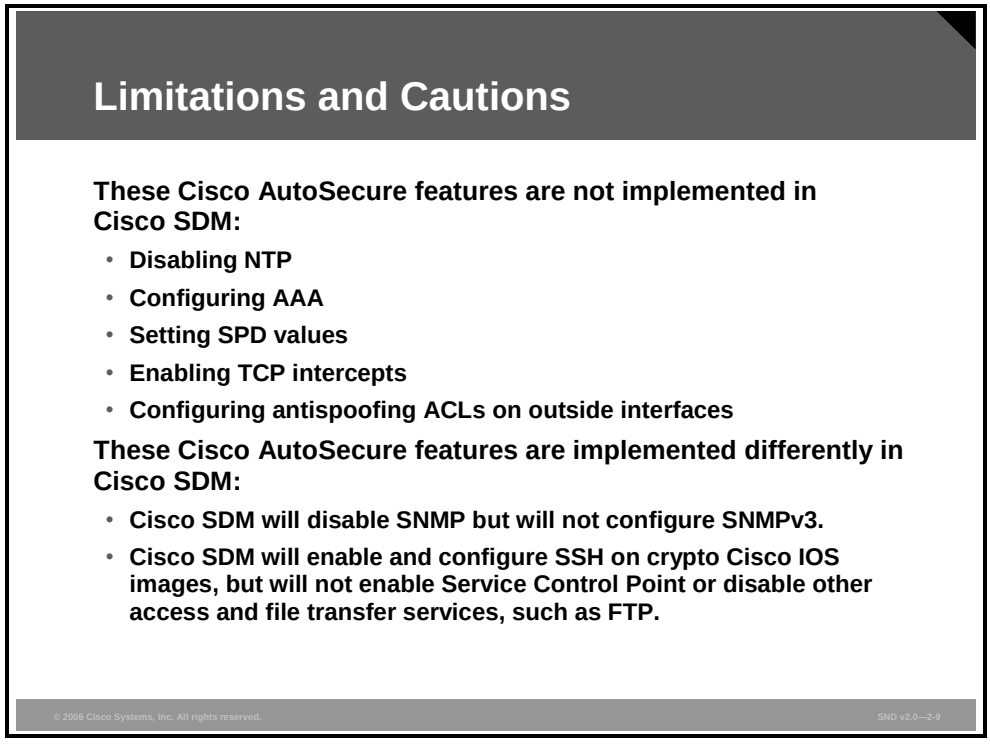
- Set enable secret password
- Disable SNMP
- Set scheduler interval
- Set scheduler allocate
- Set users
- Enable Telnet settings
- Enable NetFlow switching
- Disable IP redirects
- Disable IP proxy ARP
- Disable IP directed broadcast
- Disable MOP service
- Disable IP unreachables
- Disable IP mask reply
- Disable IP unreachables on null interface
- Enable Unicast Reverse Path Forwarding (RPF) on outside interfaces
- Enable firewall on all of the outside interfaces
- Set access class on HTTP server service
- Set access class on vty lines
- Enable SSH for access to the router
- Enable Authentication, Authorization, and Accounting (AAA)

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Limitations and Cautions

This topic explains the limitations of using the Cisco SDM One-Step Lockdown feature or the CLI **auto secure** command.




Not all the features of Cisco AutoSecure are implemented in Cisco SDM. As of Cisco SDM Version 2.2a, these Cisco AutoSecure features are not part of the Cisco SDM One-Step Lockdown:

- **Disabling NTP:** Based on input, Cisco AutoSecure will disable NTP if it is not necessary. Otherwise, NTP will be configured with Message Digest 5 (MD5) authentication. Cisco SDM does not support disabling NTP.
- **Configuring AAA:** If the AAA service is not configured, Cisco AutoSecure configures local AAA and prompts for configuration of a local username and password database on the router. Cisco SDM does not support AAA configuration.
- **Setting Selective Packet Discard (SPD) values:** Cisco SDM does not set SPD values.
- **Enabling TCP intercepts:** Cisco SDM does not enable TCP intercepts.
- **Configuring antispoofing ACLs on outside interfaces:** Cisco AutoSecure creates three named access lists used to prevent antispoofing source addresses. Cisco SDM does not configure these ACLs.

These Cisco AutoSecure features are implemented differently in Cisco SDM:

- **Disable SNMP:** Cisco SDM will disable SNMP; however, unlike Cisco AutoSecure, Cisco SDM does not provide an option for configuring SNMPv3.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

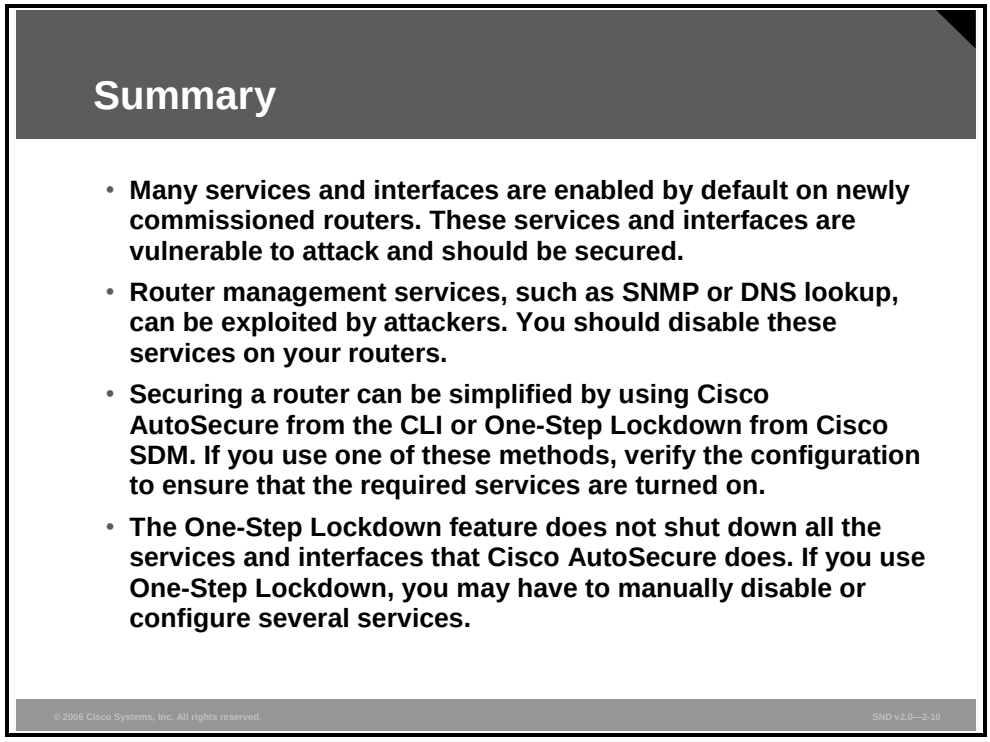
- **Enable Secure Shell (SSH) for access to the router:** Cisco SDM will enable and configure SSH on crypto Cisco IOS images; however, unlike Cisco AutoSecure, Cisco SDM will not enable Service Control Point or disable other access and file transfer services, such as FTP.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Lesson 6

# Implementing Secure Management and Reporting

## Overview

This lesson describes how to securely implement the management and reporting features of syslog, Secure Shell (SSH), and Simple Network Management Protocol version 3 (SNMPv3).

## Objectives

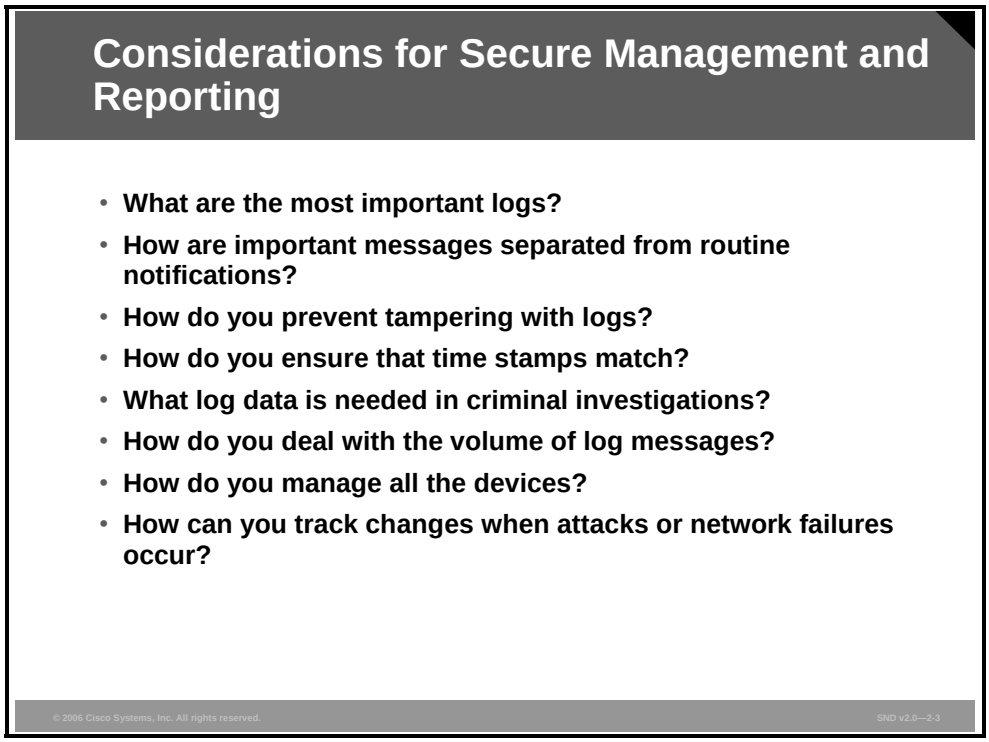
Upon completing this lesson, you will be able to securely implement the management and reporting features of syslog, SSH, and SNMPv3. This ability includes being able to meet these objectives:

- Describe the factors that you must consider when planning the secure management and reporting configuration of network devices
- Describe the factors that affect the architecture of secure management and reporting in terms of in-band and out-of-band information paths
- Describe how the syslog function plays a key role in network security
- Describe how to use Cisco SDM to monitor log messages
- Describe the security features of SNMPv3
- Describe the steps used to configure an SSH server for secure management and reporting
- Describe how to enable management features using Cisco SDM

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Secure Management and Reporting Planning Considerations

This topic describes the factors that you must consider when planning the secure management and reporting configuration of network devices.




Configuring logging for your Cisco routers is a straightforward operation when your network contains only a few Cisco routers. However, logging and reading information from hundreds of devices can prove to be a challenging proposition and can raise the questions listed in the figure.

Securing administrative access and device configurations is also a straightforward operation for smaller Cisco router networks. However, managing administrative access and device configurations for many more devices can raise questions such as those shown in the figure.

Each of these issues is specific to your needs. To identify the priorities of reporting and monitoring, input from management and from the network and security teams is required. The implemented security policy should also play a large role in answering these questions.

From a reporting standpoint, most networking devices can send syslog data that can be invaluable when you are troubleshooting network problems or security threats. You can send this data to your syslog analysis host from any device whose logs you wish to view. This data can be viewed in real time or on demand and in scheduled reports. Depending on the device involved, you can choose various logging levels to ensure that the correct amount of data is sent to the logging device. You must also flag device log data within the analysis software to permit granular viewing and reporting. For example, during an attack, the log data provided by Layer 2 switches might not be as interesting as the data provided by the intrusion detection system (IDS).


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

To ensure that log messages are synchronized with one another, clocks on hosts and network devices must be synchronized. For devices that support it, Network Time Protocol (NTP) provides a way to ensure that accurate time is kept on all devices. When you are dealing with an attack, seconds matter, because it is important to identify the order in which a specified attack occurred.

For example, the Cisco Security Monitoring, Analysis, and Response System (MARS) is a Cisco security appliance that can receive and analyze syslog messages from various networking devices and hosts from Cisco and other vendors. Cisco Security MARS extends the portfolio of security management products for the Cisco Self-Defending Network initiative. Cisco Security MARS is the first purpose-built appliance for real-time Security Threat Management (STM). This product monitors the multiple types of logging and reporting traffic available from the diverse security and network products that make up enterprise networks. Cisco Security MARS combines network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities. The result is a system that helps customers to readily and accurately identify, manage, and eliminate network attacks and to maintain network security compliance.

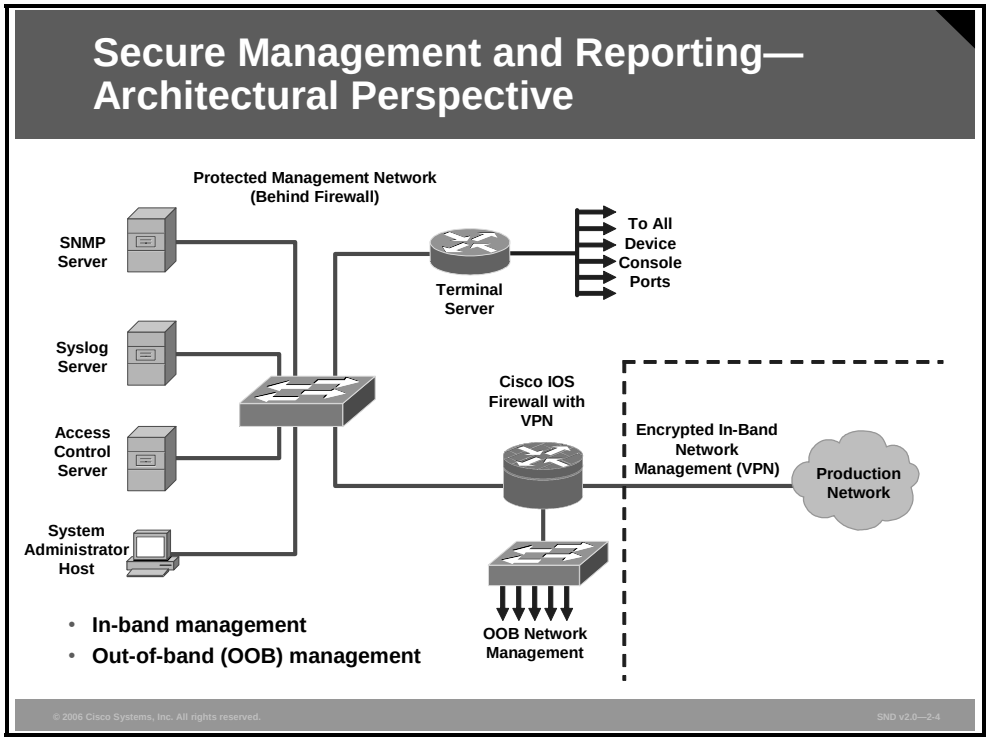
Configuration change management is another issue related to secure management. When a network is under attack, it is important to know the state of critical network devices and when the last known modifications occurred. Creating a plan for change management should be a part of your comprehensive security policy; however, at a minimum, you should record changes using authentication systems on the devices and archive configurations via FTP or TFTP.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Secure Management and Reporting Architecture

This topic describes the factors that affect the architecture of secure management and reporting.




The figure shows a management module with two network segments separated by a Cisco IOS router that acts as a firewall and a virtual private network (VPN) termination device. The segment outside the firewall connects to all the devices that require management. The segment inside the firewall contains the management hosts themselves and the Cisco IOS routers that act as terminal servers.

Information flow between management hosts and the managed devices can take two paths:

- **Out-of-band (OOB):** Information flows within a network on which no production traffic resides.
- **In-band:** Information flows across the enterprise production network or the Internet (or both).

The connection to the production network is only provided for selective Internet access, limited in-band management traffic, and IPsec-protected management traffic from predetermined hosts. In-band management occurs only when a management application itself does not function OOB, or when the Cisco device being managed does not physically have enough interfaces to support the normal management connection. It is this latter case that employs IPsec tunnels. The Cisco IOS firewall is configured to allow syslog information into the management segment, and, in addition, Telnet, SSH, and SNMP, if these services are first initiated by the inside network.

 © 2006 Cisco Systems, Inc.

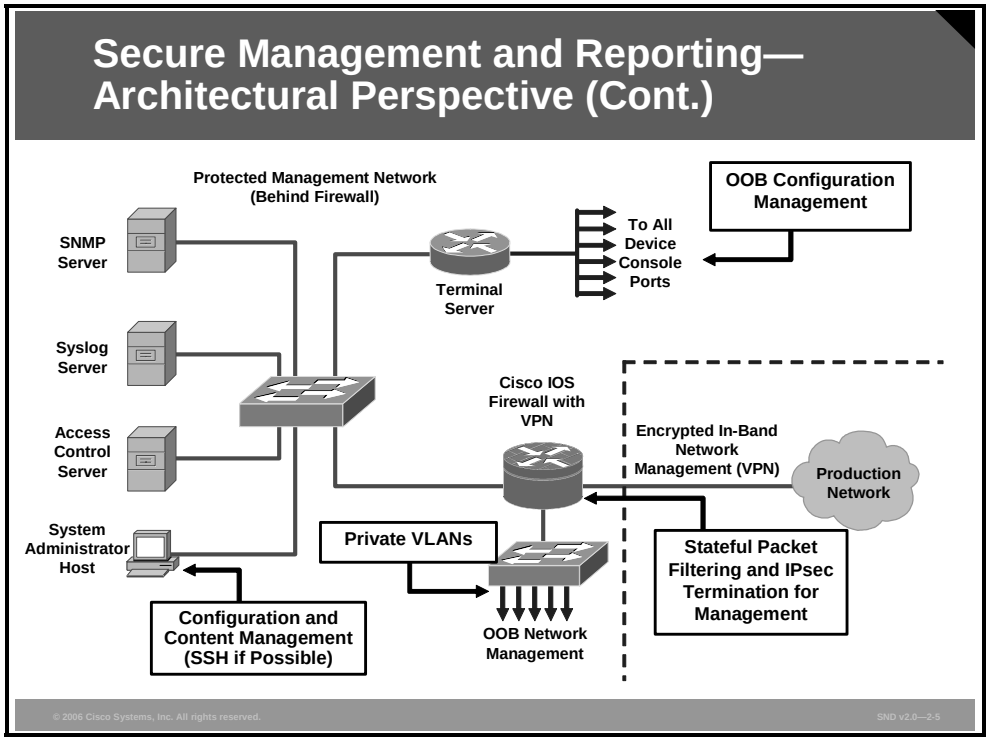
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Because the management network has administrative access to nearly every area of the network, it can be a very attractive target to hackers. The management module has been built with several technologies designed to mitigate such risks. The first primary threat is a hacker attempting to gain access to the management network itself. This threat can be mitigated only through the effective deployment of security features in the remaining modules in the enterprise. All the remaining threats assume that the primary line of defense has been breached. To mitigate the threat of a compromised device, strong access control is implemented at the firewall, and at every other possible device, to prevent exploitation of the management channel. A compromised management device cannot even communicate with other hosts on the same management subnet because private VLANs (PVLANs) on the management segment switches force all traffic from the management devices directly to the Cisco IOS firewall, where filtering takes place.

SNMP management has its own set of security needs. Use SNMPv3 where possible, because SMNPv3 supports authentication and encryption. Keeping SNMP traffic on the management segment allows the traffic to traverse an isolated segment when it pulls management information from devices. To reduce security risks, SNMP management only pulls information from devices rather than being allowed to push changes to the devices. To ensure management information is pulled, each device is configured with a read-only SNMP community string. You may configure an SNMP read-write community string when using an OOB network; however, be aware of the increased security risk of a clear text string allowing modification of device configurations if an older SNMP version is used.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



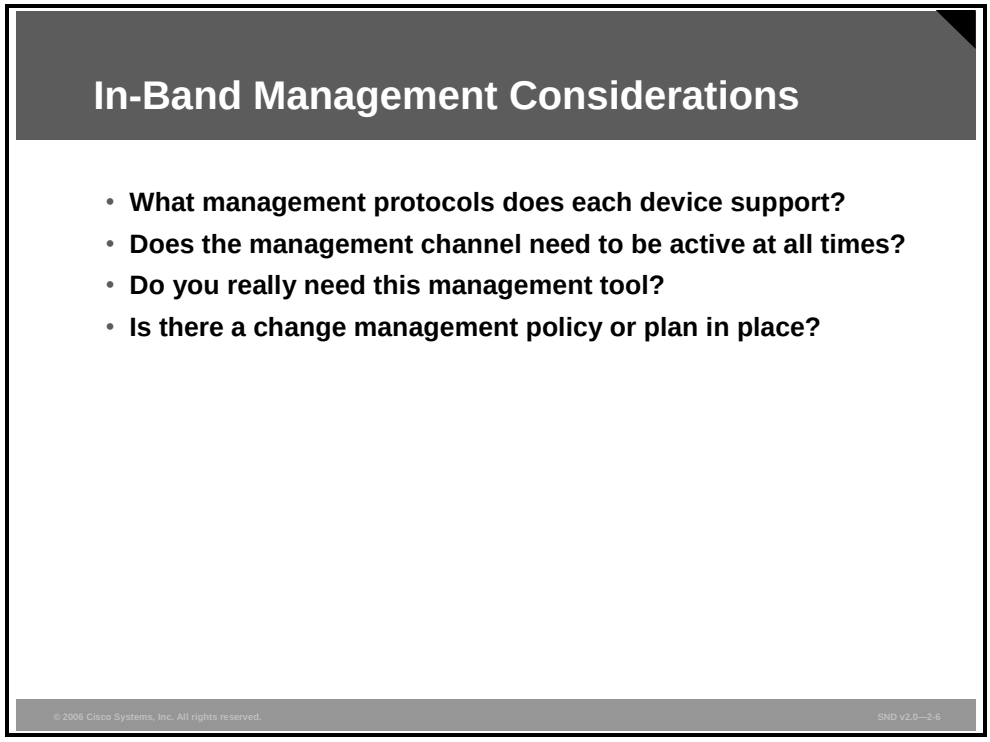

Network administrators need to securely manage all devices and hosts in the network. Management includes logging and reporting information flow, including content, configurations, and new software, from the devices to the management hosts.

From an architectural perspective, providing OOB management of network systems is the best first step in any management and reporting strategy. Devices should have a direct local connection to such a network where possible, and where impossible (because of geographic or system-related issues), the device should connect via a private encrypted tunnel over the production network. Such a tunnel should be preconfigured to permit only the traffic required for management and reporting. The tunnel should also be locked down so that only appropriate hosts can initiate and terminate tunnels.

OOB management is not always desirable. Often the decision depends on the type of management application that you are running and the protocols that are required. For example, consider a management tool with the goal of determining the reachability of all the devices on the production network. If a critical link failed between two core switches, you would want this management console to alert an administrator. If this management application is configured to use an OOB network, it may never determine that the link has failed, because the OOB network makes all devices appear to be attached to a single OOB management network. With management applications such as these, it is preferable to run the management application in-band. In-band management needs to be configured in a secure manner.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

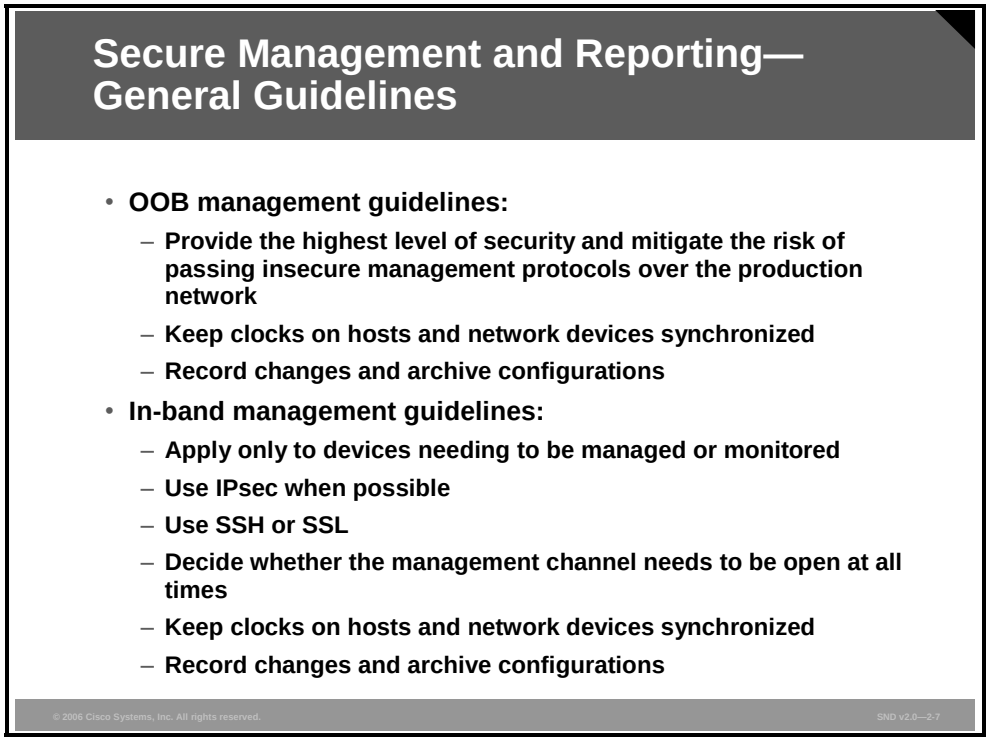



When in-band management of a device is required, you should consider these questions:

- **What management protocols does the device support?** Devices with IPsec should be managed by simply creating a tunnel from the management network to the device. This setup allows many insecure management protocols to flow over a single encrypted tunnel. When IPsec is not possible because it is not supported on a device, other, less secure options must be chosen. For configuration of the device, SSH or Secure Sockets Layer (SSL) can often be used instead of Telnet to encrypt any configuration modifications made to a device. These protocols can sometimes also be used to push and pull data to a device instead of insecure protocols such as TFTP and FTP. Often, however, TFTP is required on Cisco equipment to back up configurations or to update software versions. This fact leads to the second question.
- **Does this management channel need to be active at all times?** If not, temporary holes can be placed in a firewall while the management functions are performed and then later removed. This process does not scale with large numbers of devices, however, and should be used sparingly, if at all, in enterprise deployments. If the channel needs to be active at all times, such as with SNMP, the third question should be considered.
- **Do you really need this management tool?** Often, SNMP managers are used on the inside of a network to ease troubleshooting and configuration. However, SNMP should be treated with the utmost care because the underlying protocol has its own set of security vulnerabilities. If SNMP is required, consider providing read-only access to devices via SNMP, and treat the SNMP community string with the same care that you might use for a root password on a critical UNIX host. Know that by introducing SNMP into your production network, you are introducing a potential vulnerability into your environment. Finally, if you do need the tool, use SNMPv3 authentication and encryption features.
- **Is there a change management policy or plan in place?** If you are going to adopt new management methodologies, does everyone who needs access have access? Are old tools disabled? These issues should be dealt with in your change management policy.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The figure outlines guidelines for OOB and in-band management of the architecture.

As a general rule, OOB management is appropriate for large enterprise networks. In smaller networks, in-band management is recommended as a means of achieving a more cost-effective security deployment. In such architectures, management traffic flows in-band in all cases and is made as secure as possible using tunneling protocols and secure variants to insecure management protocols; for example, SSH is used whenever possible instead of Telnet.

To ensure that log messages are synchronized with one another, clocks on hosts and network devices must be synchronized. For devices that support it, NTP provides a way to ensure that accurate time is kept on all devices.

NTP is used to synchronize the clocks of various devices across a network. Synchronization of the clocks within a network is critical for digital certificates and for correct interpretation of events within syslog data. A secure method of providing clocking for the network is for network administrators to implement their own master clocks. The private network should then be synchronized to Coordinated Universal Time (UTC) via satellite or radio. However, clock sources are available that synchronize via the Internet for network administrators who do not wish to implement their own master clocks because of cost or other reasons.

An attacker could attempt a denial of service (DoS) attack on a network by sending bogus NTP data across the Internet in an attempt to change the clocks on network devices in such a manner that digital certificates are considered invalid. Further, an attacker could attempt to confuse a network administrator during an attack by disrupting the clocks on network devices. This scenario would make it difficult for the network administrator to determine the order of syslog events on multiple devices.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

NTP version 3 (NTPv3) and above supports a cryptographic authentication mechanism between peers. The use of the authentication mechanism, and the use of access control lists (ACLs) that specify which network devices are allowed to synchronize with other network devices, is recommended to help mitigate such an attack.

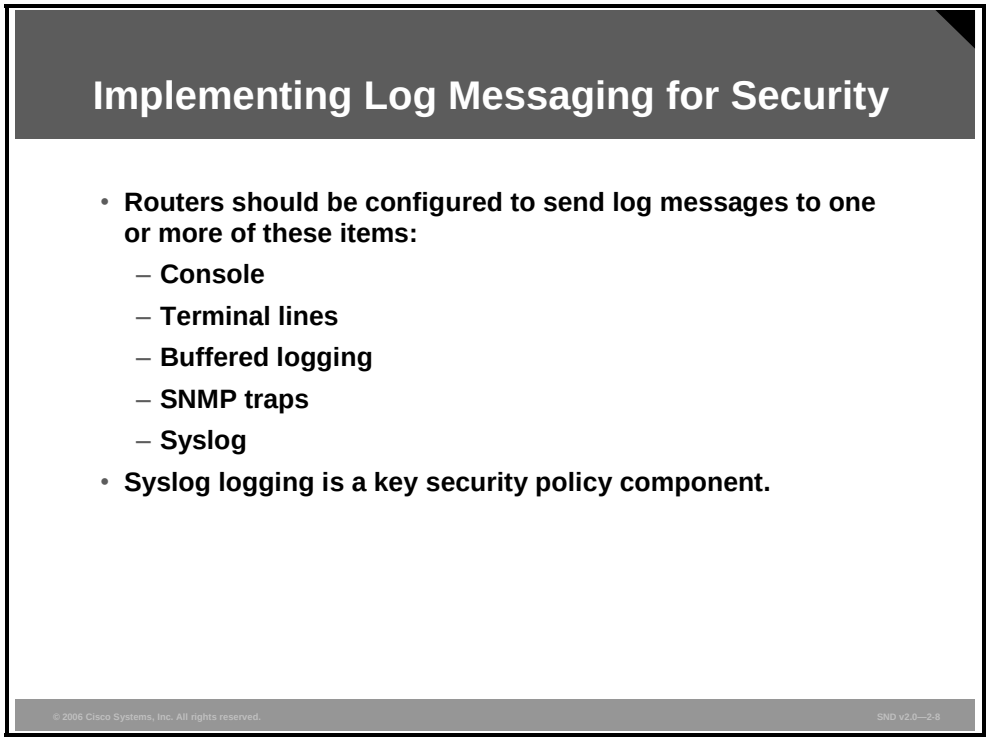
The network administrator should weigh the cost benefits of pulling the clock time from the Internet against the possible risk of doing so and allowing unsecured packets through the firewall. Many NTP servers on the Internet do not require any authentication of peers. Therefore, the network administrator must trust that the clock itself is reliable, valid, and secure. NTP uses UDP port 123.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Using Syslog Logging for Network Security

This topic describes how the syslog function plays a key role in network security.



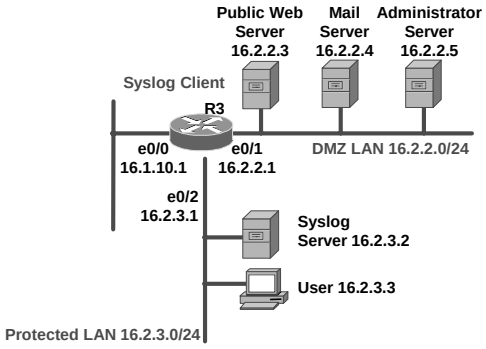

Implementing a router logging facility is an important part of any network security policy. Cisco routers can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Cisco routers can direct log messages to several different facilities. You should configure the router to send log messages to one or more of these items:

- **Console:** Console logging is used when modifying or testing the router while it is connected to the console. Messages sent to the console are not stored by the router and, therefore, are not very valuable as security events.
- **Terminal lines:** Enabled EXEC sessions can be configured to receive log messages on any terminal lines. Similar to console logging, this type of logging is not stored by the router and, therefore, is only valuable to the user on that line.
- **Buffered logging:** You may direct a router to store log messages in router memory. Buffered logging is a little more useful as a security tool but has the drawback of having events cleared whenever the router is rebooted.
- **SNMP traps:** Certain router events may be processed by the router SNMP agent and forwarded as SNMP traps to an external SNMP server. This is a viable security logging facility but requires the configuration and maintenance of an SNMP system.
- **Syslog:** Cisco routers can be configured to forward log messages to an external syslog service. This service may reside on any number of servers, including Microsoft Windows and UNIX-based systems or the Cisco Security MARS appliance. Syslog is the most popular message logging facility, because this facility provides long-term log storage capabilities and a central location for all router messages.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Syslog Systems




- **A syslog server is a host that accepts and processes log messages from one or more syslog clients.**
- **A syslog client is a host that generates log messages and forwards them to a syslog server.**

© 2006 Cisco Systems, Inc. All rights reserved.

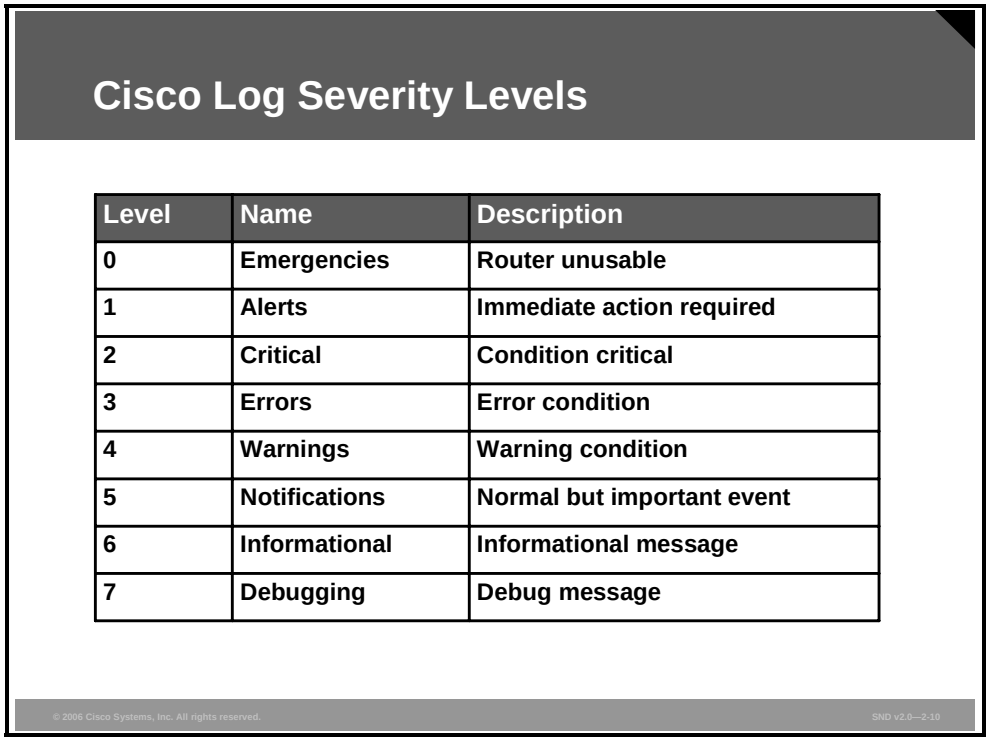

Syslog is the standard for logging system events. As shown in the figure, syslog implementations contain two types of systems:

- **Syslog servers:** These systems are also known as log hosts. These systems accept and process log messages from syslog clients.
- **Syslog clients:** Syslog clients are routers or other types of Cisco equipment that generate and forward log messages to syslog servers.

| | |
|---|---|
| **Note** | Performing forensics on router logs can become very difficult if your router clocks are not running the proper time. It is recommended that you use an NTP facility to ensure that all of your routers are operating at the correct time. |



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Cisco router log messages fall into one of eight levels as shown in the figure. The lower the level number, the higher the severity level, as the log messages in this table denote.

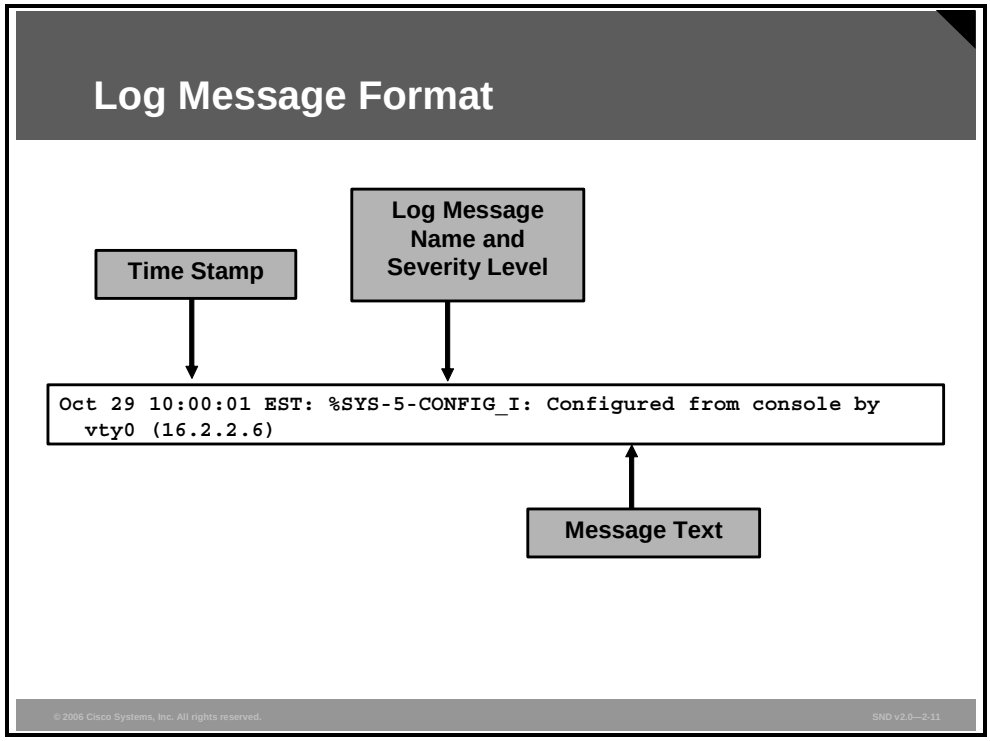
### Cisco Router Log Severity Messages

| Syslog Level | Definition | Example |
|---|---|---|
| 0: LOG_EMERG | A panic condition normally broadcast to all users | Cisco IOS software could not load |
| 1: LOG_ALERT | A condition that should be corrected immediately, such as a corrupted system database | Temperature too high |
| 2: LOG_CRIT | Critical conditions; for example, hard device errors | Unable to allocate memory |
| 3 : LOG_ERR | Errors | Invalid memory size |
| 4: LOG_WARNING | Warning messages | Crypto operation failed |
| 5: LOG_NOTICE | Conditions that are not error conditions, but should possibly be handled specially | Interface changed state, up or down |
| 6: LOG_INFO | Informational messages | Packet denied by ACL |
| 7: LOG_DEBUG | Messages that contain information normally of use only when debugging a program | Packet type invalid |

**Note** When entering logging levels in commands in Cisco IOS Release11.3 and earlier, you must specify the level name. Cisco IOS Release 12.0 and later supports using either the level number or the level name or both.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




Cisco router log messages contain these three main parts:

- Time stamp
- Log message name and severity level
- Message text

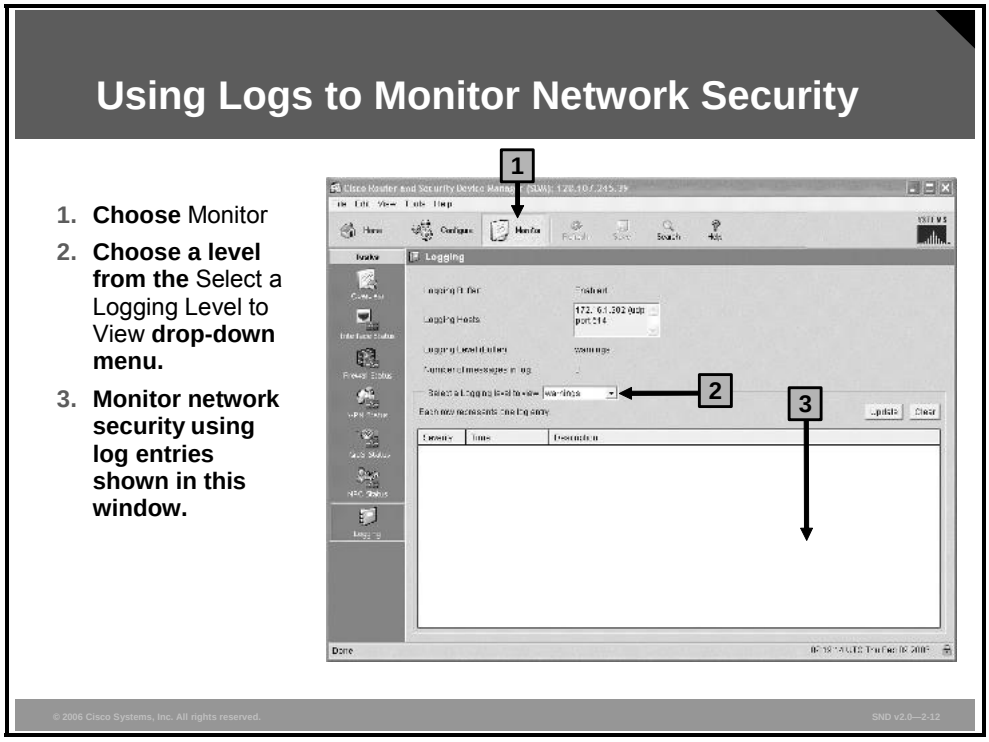
The figure shows a syslog entry example for a level 5 syslog message, indicating that someone has configured the router using the vty 0 port.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Using Logs to Monitor Network Security

This topic describes how to use logs to monitor network security.




Cisco Router and Security Device Manager (SDM) can be used to monitor logging. The figure shows the logging screen in the Monitor > Logging window of the Cisco SDM utility.

From this screen you can perform these functions:

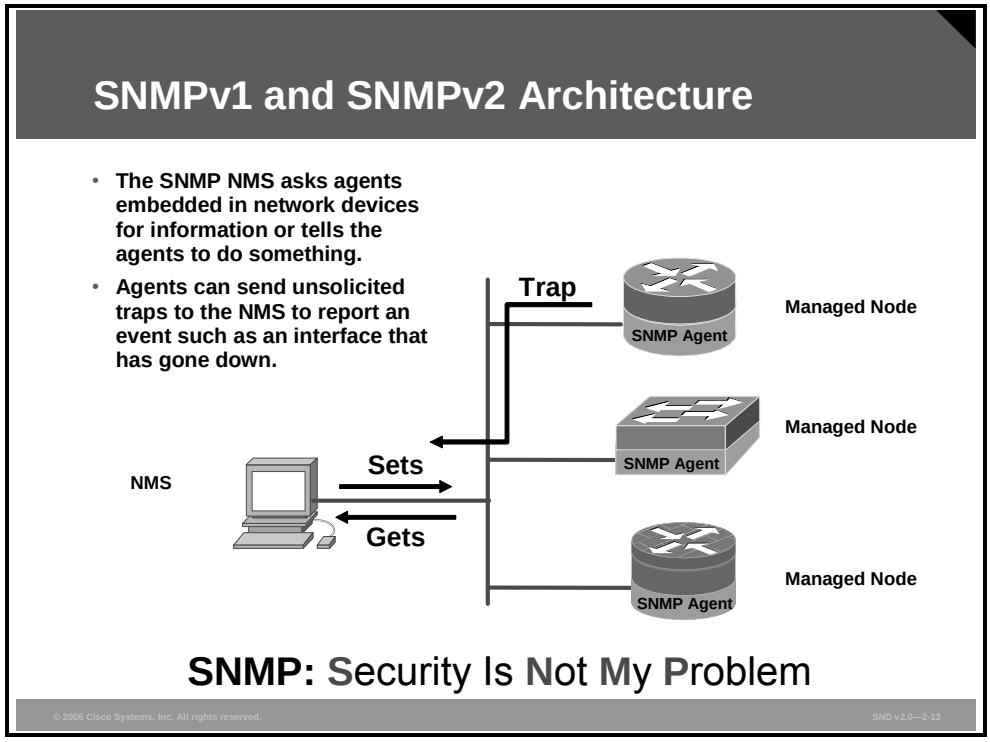
- Show the logging hosts where the router logs messages to
- Choose the minimum severity level that a router log message must have for it to be forwarded to the syslog server
- Monitor the router syslog messages, update the screen to show the most current log entries, and erases all syslog messages from the router log buffer

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Using SNMPv3

This topic describes the security features of SNMPv3.




SNMP was developed to manage nodes (servers, workstations, routers, switches, hubs, and security appliances) on an IP network. All versions of SNMP are application layer protocols that facilitate the exchange of management information between network devices. SNMP is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

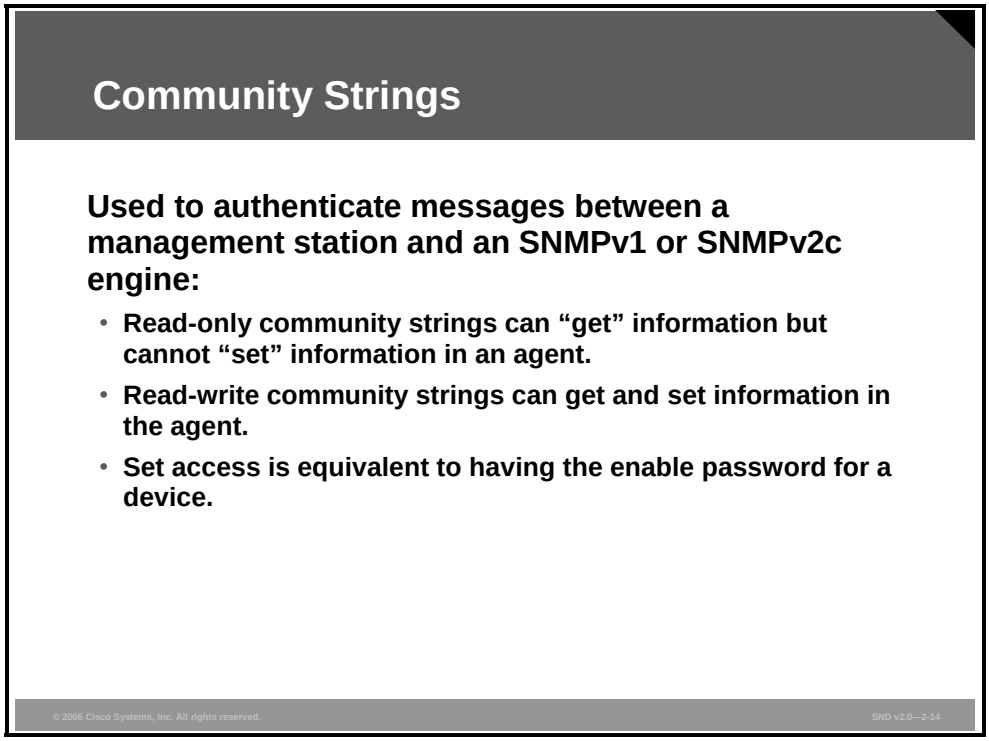
SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2) are based on three concepts: managers, agents, and MIB. In any configuration, at least one manager node runs SNMP management software. Network devices that need to be managed, such as switches, routers, servers, and workstations, are equipped with an SMNP agent software module. The agent is responsible for providing access to a local MIB of objects that reflects the resources and activity at its node.

The SNMP manager can retrieve, or “get,” information from the agent, and change, or “set,” information in the agent. Sets can change variables (settings, configuration) in the agent device or initiate actions in devices. A reply to a set indicates the new setting in the device. For example, a set can cause a router to reboot, send, or receive a configuration file. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

The action of gets and sets are the vulnerabilities that open SNMP to attack.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




SNMPv1 and SNMPv2 use a community string to access router SNMP agents. SNMP community strings act like passwords. An SNMP community string is a text string used to authenticate messages between a management station and an SNMP engine.

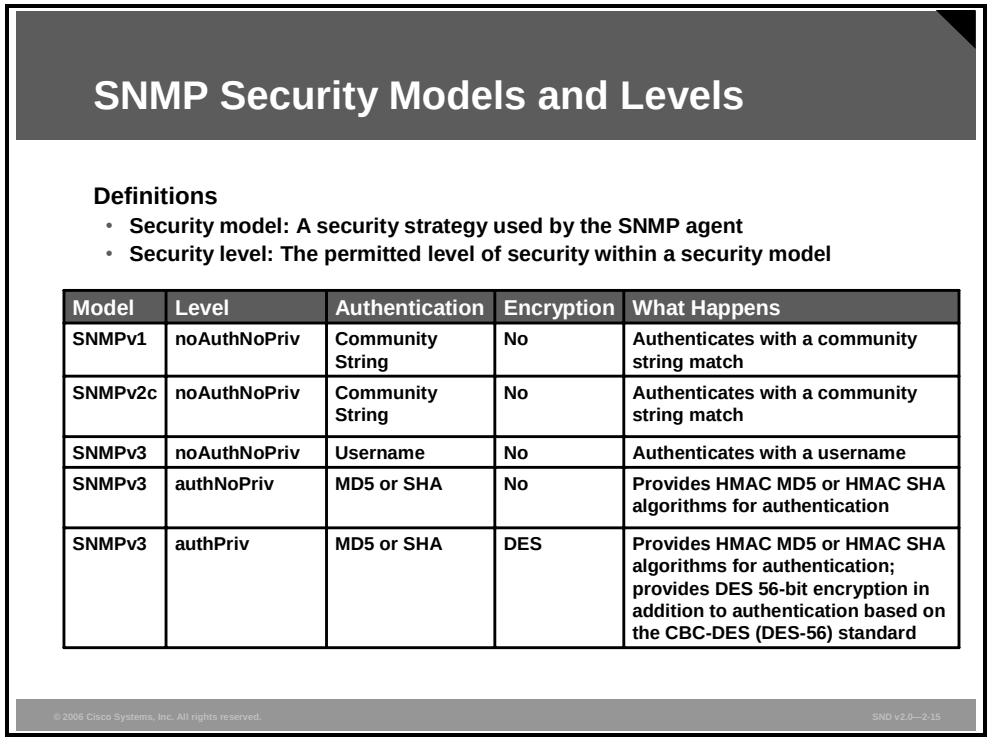
- If the manager sends one of the correct read-only community strings, it can get information but not set information in an agent.
- If the manager uses one of the correct read-write community strings, it can get or set information in the agent.

In effect, having set access is equivalent to having the enable password.

SNMP agents accept commands and requests only from SNMP systems using the correct community string. By default, most SNMP systems use “public” as a community string. If you configure your router SNMP agent to use this commonly known community string, anyone with an SNMP system is able to read the router MIB. Because router MIB variables can point to things such as routing tables and other security-critical parts of the router configuration, it is extremely important that you create your own custom SNMP community strings.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet.

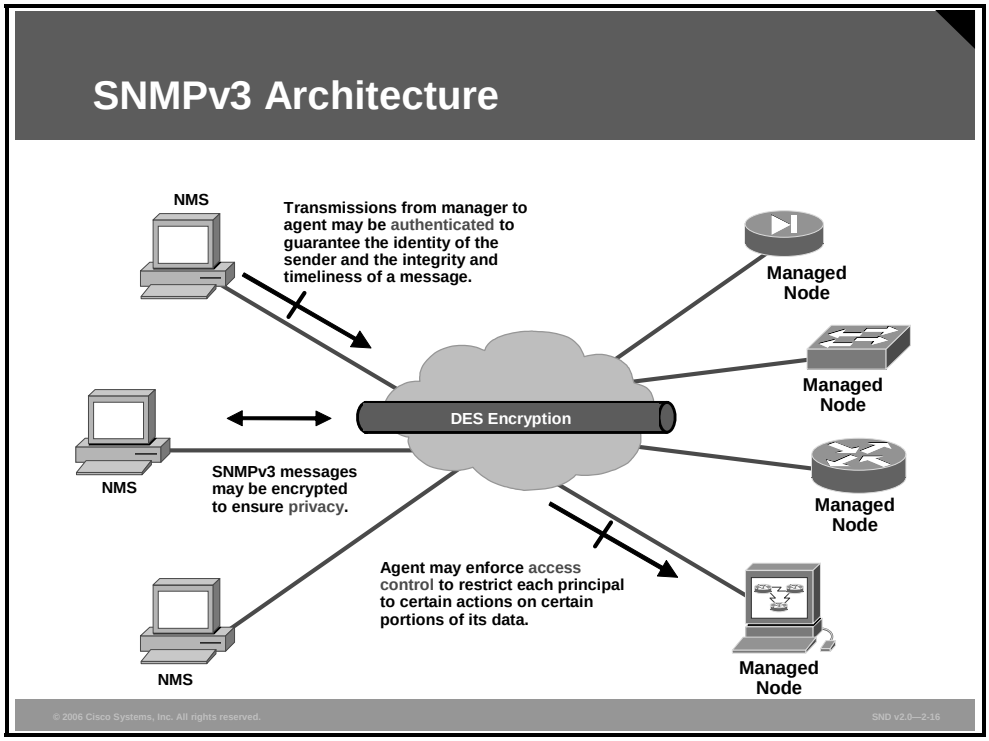
- A security model is an authentication strategy that is set up for a user and the group in which the user resides. Currently, Cisco IOS software supports three security models: SNMPv1, SNMPv2c, and SNMPv3.
- A security level is the permitted level of security within a security model. The security level is a type of security algorithm performed on each SNMP packet. The three levels are noAuth, auth, and Priv, as described here:
  - The noAuth level authenticates a packet by a string match of the username or community string.
  - The auth level authenticates a packet by using either the Hashed Message Authentication Code (HMAC) with Message Digest 5 (MD5) or Secure Hash Algorithms (SHA). This method is described in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication.*
  - The Priv level authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the cipher block chaining (CBC)- Data Encryption Standard (DES) (DES-56) algorithm.

SNMPv3 adds security and remote configuration capabilities to the previous versions. SNMPv3 provides three security model and security level options.

The “SNMP Security Models and Levels” table in the figure identifies what the combinations of security models and levels mean.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*



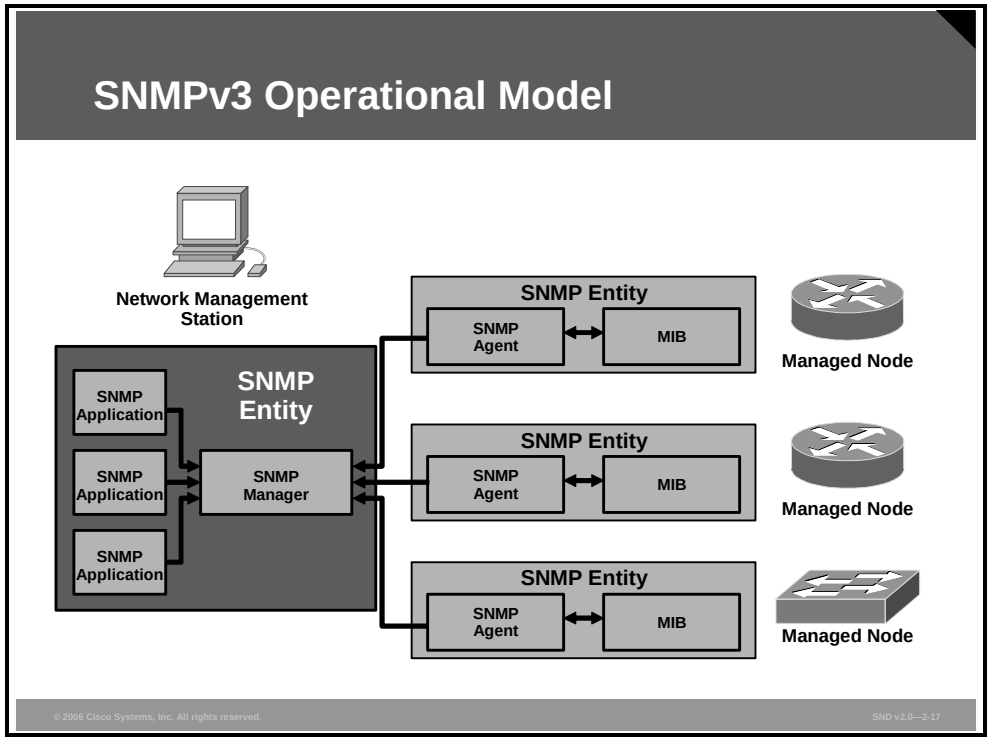

In its natural evolution, the current version of SNMPv3 addresses the vulnerabilities of earlier versions by including three important services: authentication, privacy, and access control.

SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are as follows:

- **Message integrity:** Ensuring that a packet has not been tampered with in transit
- **Authentication:** Determining that the message is from a valid source
- **Encryption:** Scrambling the contents of a packet to prevent it from being seen by an unauthorized source


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




In SNMPv3, the concepts of separate SNMP agents and SNMP managers do not apply. These concepts have been combined into single SNMP entities. Each managed node and the network management station (NMS) is a single entity.

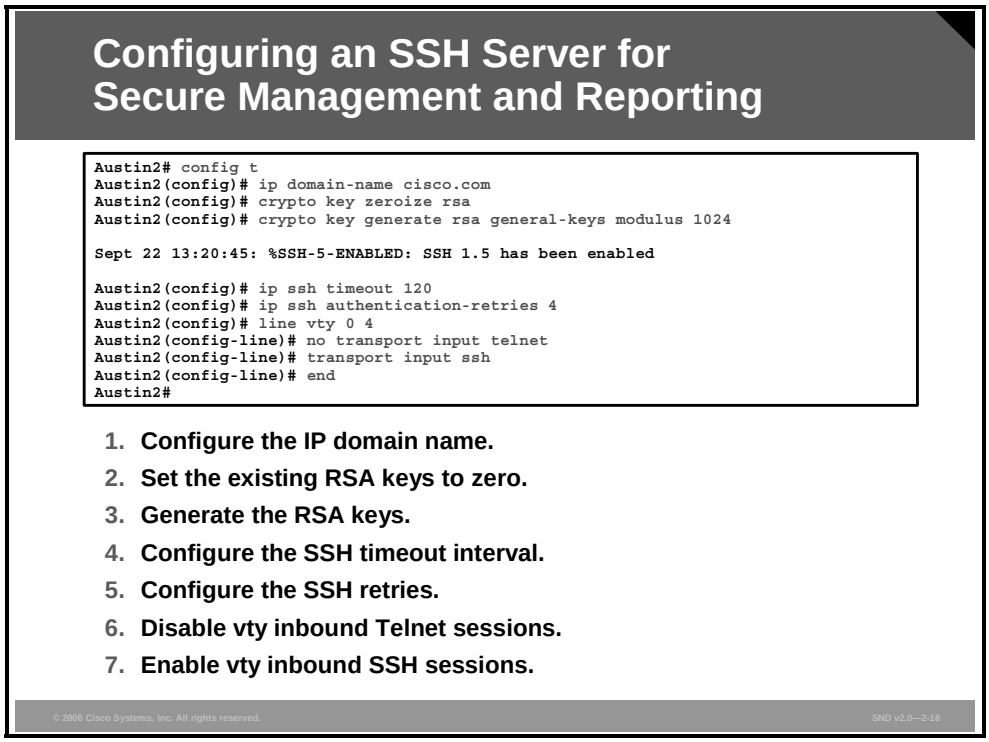
- **Managed node SNMP entities:** The managed node SNMP entity includes an SNMP agent and an SNMP MIB. The agent implements the SNMP protocol and allows a managed node to provide information to the NMS and accept instructions from it. The MIB defines the information that can be collected and used to control the managed node. Information exchanged using SNMP takes the form of objects from the MIB.
- **NMS SNMP entities:** The SNMP entity on an NMS includes an SNMP manager and SNMP applications. The manager implements the SNMP protocol and collects information from managed nodes and sends instructions to them. The SNMP applications are software applications used by the network administrator to manage the network.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Configuring an SSH Server for Secure Management and Reporting

This topic describes the steps used to configure an SSH server for secure management and reporting.




Whenever possible, you should use SSH instead of Telnet to manage your Cisco routers. SSH version 1 (SSHv1) is supported in Cisco IOS Release 12.1(1)T and later, while SSH version 2 (SSHv2) is supported in Cisco IOS Release 12.3(4)T and later. Cisco routers configured for SSH act as SSH servers. You must provide an SSH client, such as PuTTY, OpenSSH, or Tera Term, for the administrator workstation that you wish to use to configure and manage routers using SSH.

**Note** Cisco routers with Cisco IOS Releases 12.1(3)T and later can act as both SSH clients and SSH servers. This means that you could initiate an SSH client-to-server session from your router to a central SSH server system. SSH employs strong encryption to protect the SSH client-to-server session. Unlike Telnet, where anyone with a sniffer can see exactly what you are sending to and receiving from your routers, SSH encrypts the entire session.

Complete these tasks before configuring your routers for SSH server operations:

- Ensure that the target routers are running a Cisco IOS Release 12.1(1)T image or later with the IPsec feature set. Only Cisco IOS software images containing the IPsec feature set support an SSH server.
- Ensure that the target routers are configured for local authentication, or for authentication, authorization, and accounting (AAA) for username or password authentication, or both.
- Ensure that each of the target routers has a unique hostname.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- Ensure that each of the target routers is using the correct domain name of your network.

Complete these steps to configure your Cisco router to support an SSH server:

**Step 1** Configure the IP domain name of your network using the **ip domain-name** command in global configuration mode:

```
Austin2(config)#ip domain-name cisco.com
```

**Step 2** Generate keys to be used with SSH by generating the Rivest, Shamir, and Adleman (RSA) keys using the **crypto key generate rsa** command in global configuration mode:

```
Austin2(config)#crypto key generate rsa general-keys modulus
1024
```

**Note** The minimum recommended key length is modulus 1024.

Rivest, Shamir, and Adelman are the inventors of this best-known public key algorithm.

**Step 3** Optionally, to display the generated keys, use the **show crypto key mypubkey rsa** command in privileged EXEC mode.

**Step 4** Configure the time that the router waits for the SSH client to respond using the **ip ssh timeout** command in global configuration mode:

```
Austin2(config)#ip ssh timeout 120
```

**Step 5** Configure the SSH retries using the **ip ssh authentication-retries** command in global configuration mode:

```
Austin2(config)#ip ssh authentication-retries 4
```

**Caution** Be sure to disable Telnet transport input on all of the router vty lines; otherwise, the router will continue to allow insecure Telnet sessions.

**Step 6** Disable vty inbound Telnet sessions.

```
Austin2(config)#line vty 0 4
Austin2(config-line)#no transport input telnet
```

**Step 7** Enable vty inbound SSH sessions.

```
Austin2(config-line)#transport input ssh
```

The SSH protocol is automatically enabled once you generate the SSH (RSA) keys, as shown in the figure. Once the keys are created, you may access the router SSH server using your SSH client software.

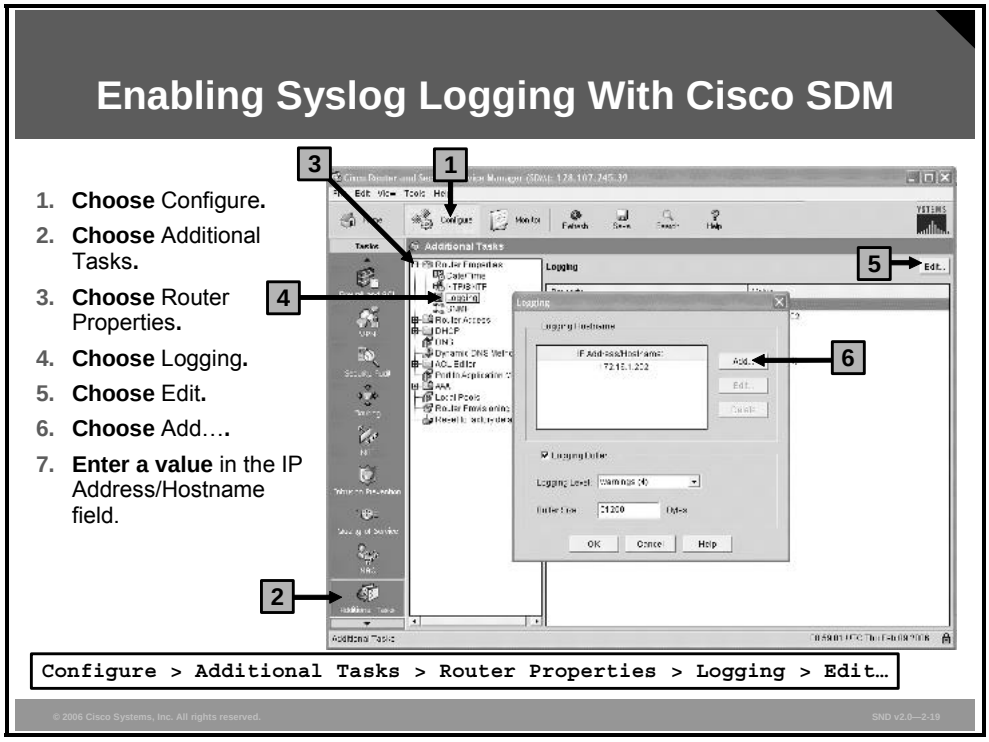
The procedure for connecting to a Cisco router SSH server varies depending on the SSH client application that you are using. Generally, the SSH client passes your username to the router SSH server. The router SSH server prompts you for the correct password. Once the password has been verified, you can configure and manage the router as if you were a standard vty user.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Enabling Management Features

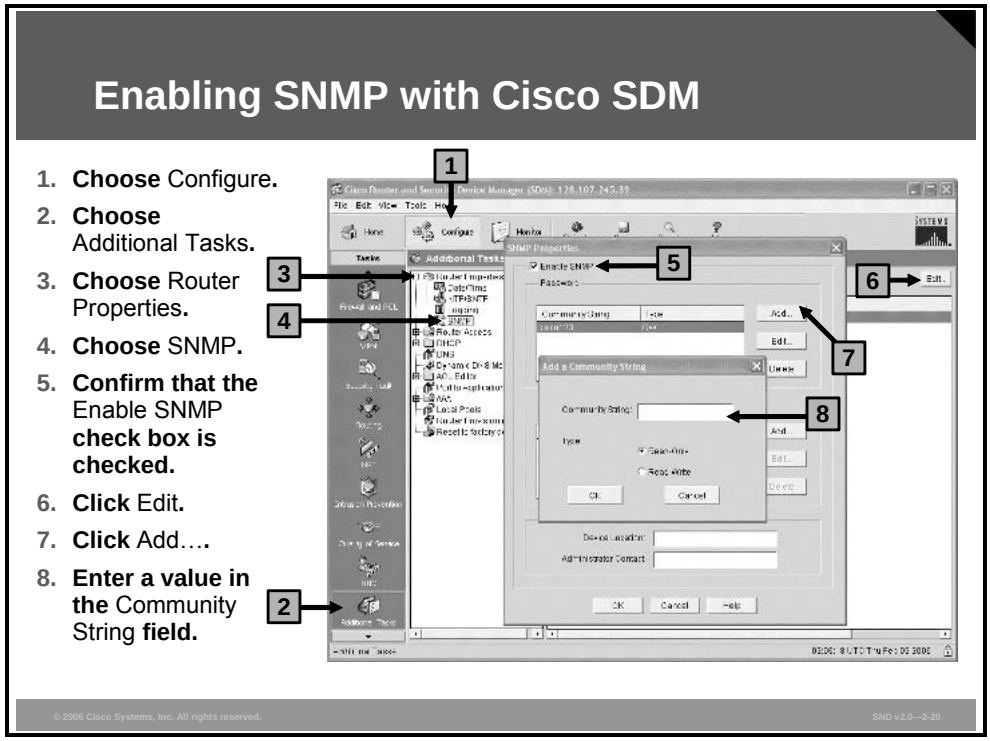
This topic describes how to enable management features with Cisco SDM.




The procedure to enable syslog logging on your router using Cisco SDM is shown in the figure. Enter an IP address of a logging host.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The procedure to enable SNMP, set SNMP community strings, and enter SNMP trap manager information with Cisco SDM is shown in the figure.

| **Note** | SNMPv3 cannot be configured using Cisco SDM Version 2.2a or earlier version. |
|---|---|

Check the **Enable SNMP** check box to enable SNMP support. Uncheck this box to disable SNMP support. SNMP is enabled by default.

SNMP community strings are embedded passwords to MIBs. MIBs store data about router operation and are meant to be available to authenticated remote users. The two types of community strings are public community strings, which provide read-only access to all objects in the MIB except community strings, and private community strings, which provide read- -write access to all objects in the MIB except community strings.

The community string table lists all of the configured community strings and their types. Click the **Add** button to display the Add a Community String dialog box, shown in the figure, and create new community strings. Click the **Edit** or **Delete** buttons to edit or delete the community string that you chose in the table.

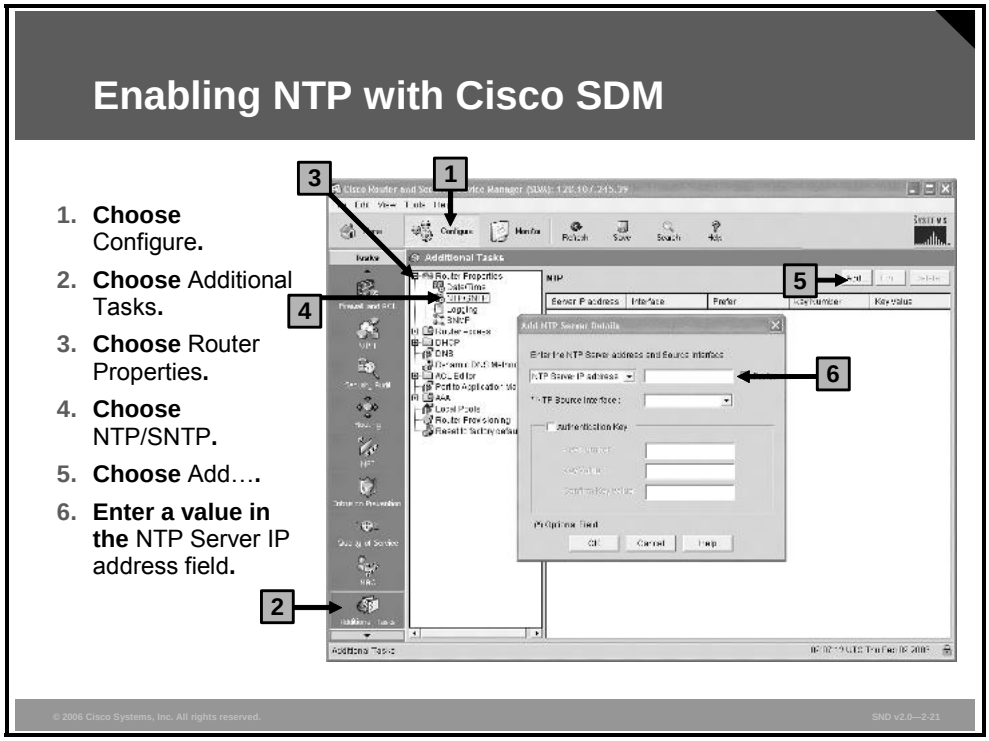
Enter the IP addresses and community strings of the trap receivers. These are normally the IP addresses of the SNMP management stations monitoring your domain. Check with your site administrator to determine the address if you are unsure of it. Click the **Add**, **Edit**, or **Delete** buttons to administer trap receiver information.

SNMP Server Location is a text field that you can use to enter the SNMP server location. It is not a configuration parameter that will affect the operation of the router.

SNMP Server Contact is a text field that you can use to enter contact information for a person managing the SNMP server. It will not affect the operation of the router.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The procedure to configure NTP using Cisco SDM is shown in the figure.

NTP allows routers on your network to synchronize their time settings with an NTP server. A group of NTP clients that obtains time and date information from a single source will have more consistent time settings. This window allows you to view the NTP server information that has been configured, add new information (click **Add…**), and edit (click **Edit…**) or delete (click **Delete…**) existing information.

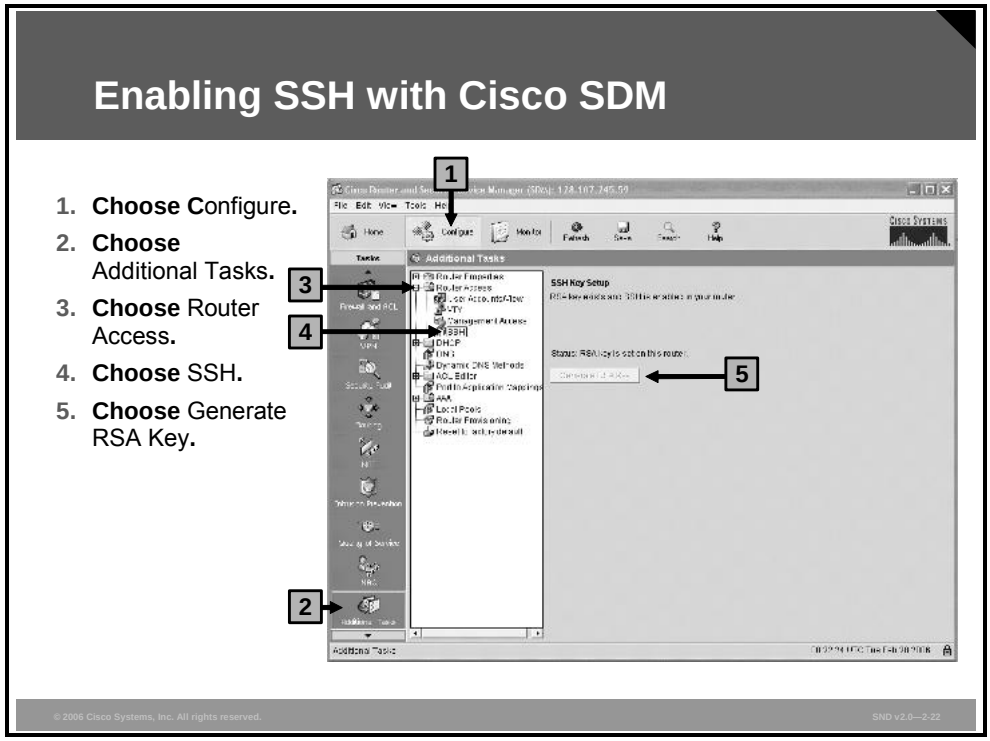
| | |
|---|---|
| **Note** | If your router does not support NTP commands, this branch will not appear in the Router Properties tree. |

When you click **Add…** or **Edit…**, you will be presented with the dialog box shown in the figure. Here are some details about the dialog box options:

- The Server IP Address is the IP address of an NTP server. If your organization does not have an NTP server, you may want to use a publicly available server, such as the server described at http://www.eecis.udel.edu/~mills/ntp/clock2a.html.
- The NTP Source Interface is the interface that the router will use to communicate with the NTP server.
- Check the **Prefer** check box if this NTP server has been designated as a preferred NTP server. Preferred NTP servers will be contacted before nonpreferred servers are contacted. There can be more than one preferred NTP server.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*




The procedure to enable SSH servers on your router using Cisco SDM is shown in the figure.

Cisco SDM can be used to configure an SSH server on a router. The SSH server is a feature that enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality similar to that of an inbound Telnet connection, but it also provides strong encryption to be used with Cisco IOS software authentication. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients. This feature is disabled if the router is not using an IPsec DES or Triple-Data Encryption Standard (3DES) Cisco IOS software image, and if the SSH branch of the Additional Tasks tree does not appear.

The SSH key settings have these two status options:

- **Crypto key is not set on this device:** This notice appears if there is no cryptographic key configured for the device. If there is no key configured, you can enter a modulus size and generate a key.
- **RSA key is set on this router:** This option appears if a cryptographic key has been generated, in which case SSH is enabled on this router.

If no cryptographic key has been generated, there will be two buttons that appear on the SSH configuration dialog box. The two buttons are as follows:

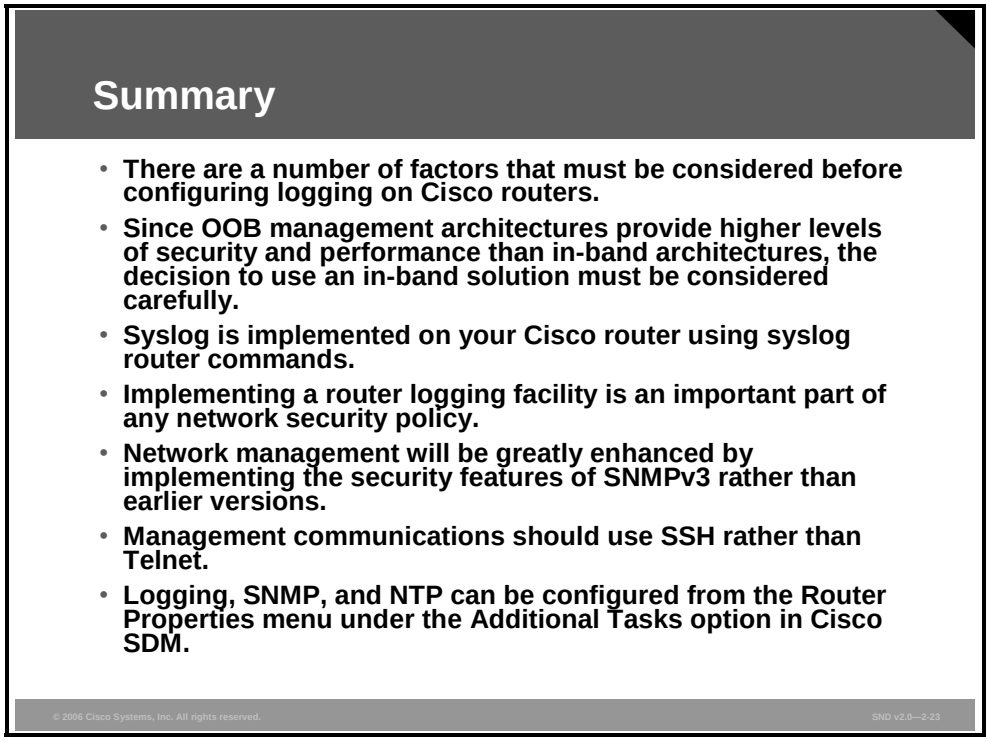
- **Key Modulus Size:** Click this button and enter the modulus size that you want to give the key. If you want a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.
- **Generate RSA Key:** Click this button to generate a cryptographic key for the router using the modulus size that you entered. If the cryptographic key has already been generated, this button is disabled.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.






*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Lesson 7

# Defending the Network Perimeter with Cisco Products

## Overview

This lesson introduces network perimeter security with Cisco IOS software on Cisco integrated services router platforms and some specialized security applications, including Network Admissions Control (NAC) and Cisco Secure Access Control Server (ACS). The lesson concludes with a section on best practices for securing the network perimeter.

## Objectives

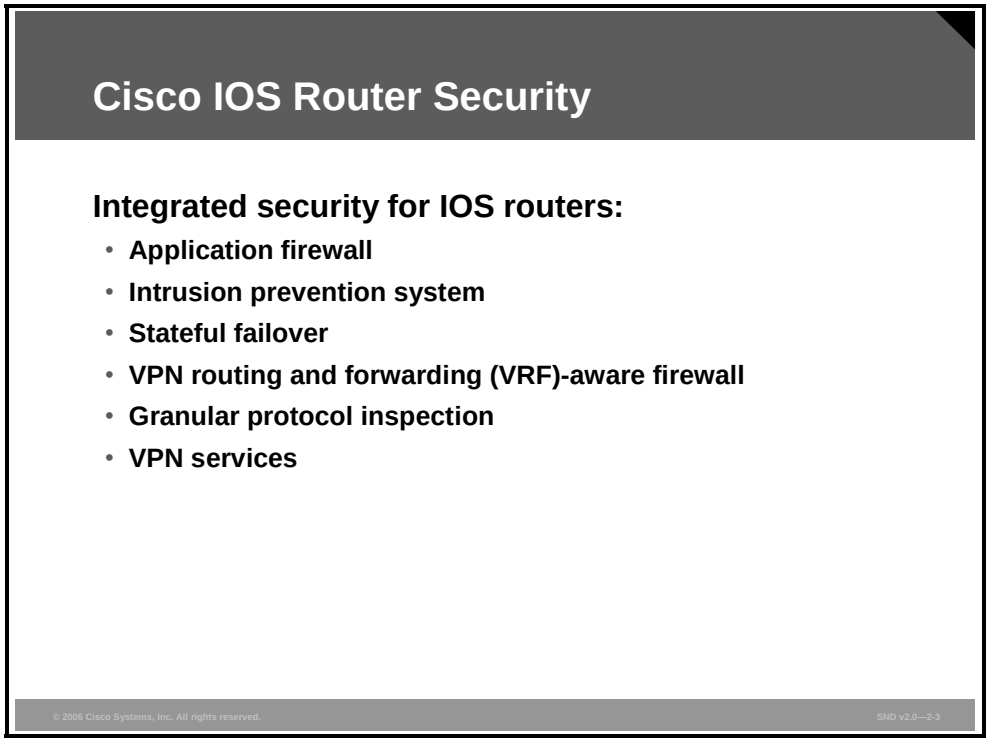
Upon completing this lesson, you will be able to explain the best practices for deploying Cisco routers and other perimeter defense products. This ability includes being able to meet these objectives:

- Describe how to secure the network perimeter with Cisco IOS software security features
- Describe the security features of the Cisco Integrated Services Router Family
- Describe the use of Cisco Secure ACS to provide network security though identification and authentication

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Cisco IOS Security Features

This topic describes how to secure the network perimeter with Cisco IOS software security features.




Cisco IOS software-based devices incorporate various security services to create an integrated and scalable network.

The Cisco IOS Firewall is a security-specific option for Cisco IOS software. The Cisco IOS Firewall provides integrated network security with robust stateful firewall functionality and intrusion prevention for network perimeters. It adds greater depth and flexibility to existing Cisco IOS security functionality (such as authentication, encryption, and failover), by delivering these state-of-the-art security features: stateful, multiservice application-based filtering for traffic types such as HTTP (Java blocking), Simple Network Management Protocol (SNMP), FTP, TFTP, H.323, session initiation protocol (SIP), Skinny Client Control Protocol (SCCP), Rapid Spanning Tree Protocol (RTSP), RealAudio, and many more; dynamic per-user authentication, authorization, and accounting (AAA); URL filtering, and others.

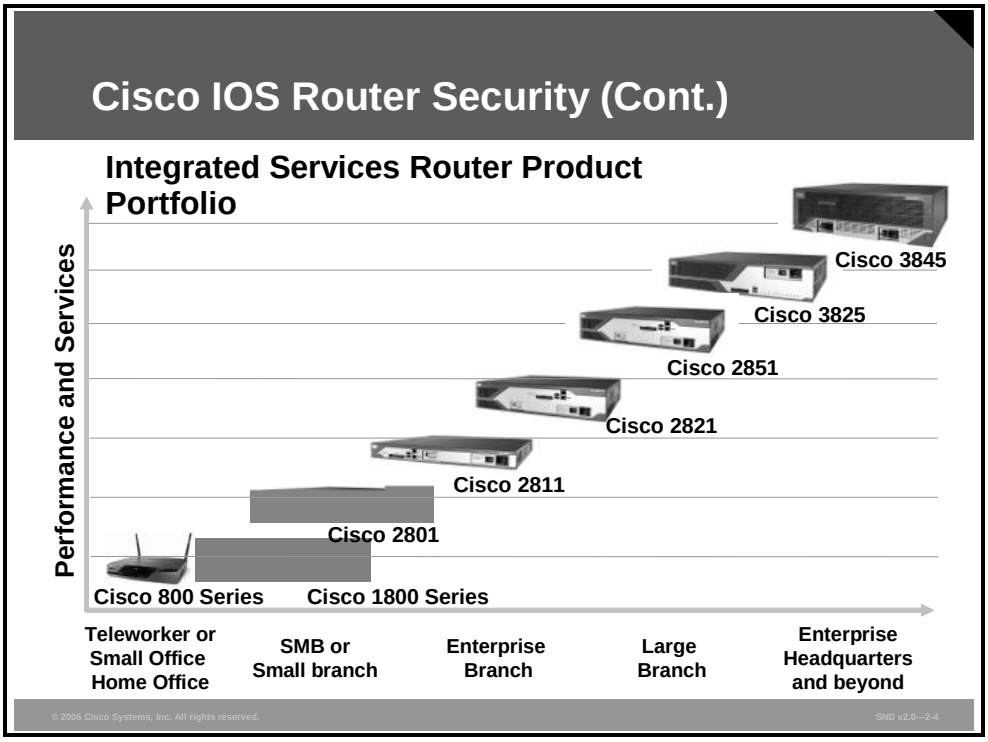
The Cisco IOS Firewall offers sophisticated security and policy enforcement services for connections within an organization (intranet) and between partner networks (extranets) and for securing Internet connectivity for remote and branch offices. The Cisco IOS Firewall also allows firewall functions to be implemented at the individual context level for virtual fragmentation reassembly deployment.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Introducing the Cisco Integrated Services Router Family

This topic describes the security features of the Cisco Integrated Services Router Family.




## Cisco 800 Series Routers

The Cisco 850 Series Access Routers supports broadband cable and Asymmetric Digital Subscriber Line (ADSL) over analog telephone lines. Designed for very small offices, the routers provide secure WAN connectivity with optional integrated wireless LAN (WLAN) connectivity in a single device. Easy setup allows the Cisco 850 Series Access Routers to be deployed at small remote offices and at small businesses, and remote management features enable information technology (IT) managers and service providers to support remote sites.

The Cisco 870 Series Access Routers extends the high-performance, secure concurrent services, including firewall, virtual private networks (VPNs), and WLANs, at broadband speeds to small offices. Easy deployment and centralized management features enable the Cisco 870 Series Access Routers to be deployed in small offices or teleworker sites as part of an enterprise network, to be used by small and medium-sized businesses for secure WAN and WLAN connectivity, or to be used by service providers to offer business-class broadband and WLAN services.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Cisco 1800 Series Integrated Services Routers

The Cisco 1800 Series Integrated Services Routers is the next evolution of the Cisco 1700 Series Modular Access Routers. The new Cisco 1800 Series fixed-configuration routers are designed for secure broadband, Metro Ethernet, and wireless connectivity. This series of routers also helps businesses reduce costs by enabling deployment of a single device to provide multiple services (integrated router with redundant link, LAN switch, firewall, VPN, intrusion prevention systems [IPSs], wireless technology, and quality of service [QoS]), typically performed by separate devices.

## Cisco 2800 Series Integrated Services Routers

The Cisco 2800 Series Integrated Services Router architecture has been designed to meet the expanding requirements of small-to-medium sized branch offices and small-to-medium enterprise businesses for delivery of secure, concurrent data, voice, and video services at wire-speed performance. The Cisco 2800 Series Integrated Services Routers are the next evolution of the Cisco 2600 Series Multiservice Access Routers and include four platforms: the Cisco 2801, Cisco 2811, Cisco 2821, and Cisco 2851 Integrated Services Routers.

## Cisco 3800 Series Integrated Services Routers

The Cisco 3800 Series Integrated Services Router architecture has been designed to deliver the performance, availability, and reliability required for scaling mission-critical security, IP telephony, business video, network analysis, and web applications in the most demanding enterprise environments. Built for performance, the Cisco 3800 Series Integrated Services Routers deliver multiple secure, concurrent data, voice, and video services at wire-speed performance. The Cisco 3800 Series Integrated Services Router architecture builds on the powerful Cisco 3700 Series Multiservice Access Routers and includes these two platforms: the Cisco 3825 Integrated Services Router and the Cisco 3845 Integrated Services Router.

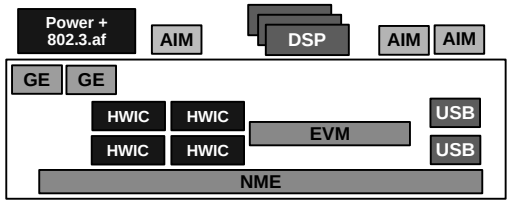
 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Cisco IOS Router Security (Cont.)

**Cisco Integrated Services router features:**

- **Built-in VPN acceleration**
  - **3DES/AES encryption**
- **Secure voice**
  - **PVDM modules**
  - **Support SRTP**
- **High-performance AIM**
  - **3DES, AES, and compression**
  - **Ten times faster than previous platforms**
- **USB port**
  - **Removable secure credentials**




GE = Gigabit Ethernet
EVM = extension voice module
NME = network module enhanced

© 2006 Cisco Systems, Inc. All rights reserved.


Cisco integrated services routers deliver additional options to enhance security in the network. Some of the security related features of the Cisco integrated services routers are as follows:

- **Built-in VPN acceleration:** The built-in, hardware-based encryption acceleration offloads the VPN processes to provide increased VPN throughput with minimal impact on the router CPU.
- **Secure voice:** The digital signal processor (DSP) slots of the integrated services routers are using packet voice DSP modules (PVDMs) that provide conferencing, transcoding and secure voice features. With Secure Real-Time Transport Protocol (SRTP), the whole voice payload is encrypted while the header is still in clear text to support features such as QoS.
- **High-performance advanced integration module** (**AIM):** The VPN encryption AIM is a solution for aggregation-type applications, such as Dynamic Multipoint VPN (DMVPN), where large numbers of remote VPN tunnels are required. Additionally, the VPN encryption AIMs help ensure that your investments are compatible with future versions by allowing more room to grow if the VPN performance requirements in your network increase.
- **Universal Serial Bus (USB) port:** As of Cisco IOS Release 12.3(14)T, the USB eToken and USB flash support are available. The USB eToken feature provides secure configuration distribution and allows users to store VPN credentials for deployment. The USB flash feature allows users to store images and configurations using USB flash memory.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Cisco IOS Router Security (Cont.)

### Packet Voice DSP Modules




- **Digital signal processor slots for voice**
- **PVDM module support SRTP to allow secure communications with IP phones using AES encryption**
- **Enables secure calls from Cisco IP phones to Cisco CallManager**

© 2006 Cisco Systems, Inc. All rights reserved.


The High Density Voice Network Module (NM-HDV) contains five 72-pin single inline memory module (SIMM) sockets or banks for packet PVDMs numbered 0 through 4. Each socket can be filled with a single 72-pin PVDM. The PVDMs must be installed starting from slot 0.

| | |
|---|---|
| **Note** | PVDM and PVDM2 modules are not interchangeable. Use PVDM modules with the NM-HDV network module only, and use PVDM2 modules with the NM-HDV2 network module only. |

The PVDM2 modules are used with onboard voice interface cards on the Cisco 2801, 2811, 2821, and 2851 Integrated Services Routers. They are also used with the Cisco High-Density Analog and Digital Extension Module for Voice and Fax supported on the Cisco 2821, 2851, 3825, and 3845 Integrated Services Router platforms.

The voice gateway modules on the Cisco multiservice and integrated services routers interoperate with Cisco IP Phone 7940, 7960, and 7970 that support media encryption. The Cisco IP Phone 7970 supports media encryption with the Cisco CallManager 4.0 release, while the Cisco IP Phone 7960 and Cisco IP Phone 7940 support media encryption with the Cisco CallManager 4.1 release.

Media authentication and encryption in Cisco Survivable Remote Site Telephony mode is supported beginning with the Cisco IOS Release 12.3(14)T and Cisco CallManager 4.1.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Cisco IOS Router Security (Cont.)

**Cisco integrated services router acceleration hardware:**

- **Onboard VPN acceleration hardware**
  - **Encryption and compression**
- **Cisco 1800 Series Integrated Services Routers supports one AIM module**
  - **AIM-VPN/BPII-PLUS**
- **Cisco 2800 Series Integrated Services Routers and Cisco 3825 Integrated Services Router supports two AIM modules**
  - **AIM-VPN/EPII-PLUS**
- **Cisco 3845 Integrated Services Router supports two AIM modules**
  - **AIM-VPN/HPII-PLUS**

© 2006 Cisco Systems, Inc. All rights reserved.


The Cisco integrated services router series provides a built-in VPN encryption acceleration for IPsec Data Encryption Standard (DES), Triple-Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) 128, 192, and 256 bit key sizes. In addition, you can use an AIM for VPN encryption. There are three types of these modules:

- AIM-VPN/BPII-PLUS: Basic performance AIM
- AIM-VPN/EPII-PLUS: Enhanced performance AIM
- AIM-VPN/HPII-PLUS: High performance AIM

These modules increase the router encryption and compression performance. The modules all support these encryption standards:

- Encryption: IPsec DES, 3DES
- Authentication: Rivest, Shamir, and Adleman (RSA) and Diffie Hellman (DH)
- Data integrity: Secure Hash Algorithm 1 (SHA-1) and Message Digest 5 (MD5)
- Optimized for all three AES key sizes: AES-128, AES-192, and AES-256.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Cisco IOS Router Security (Cont.)

**Cisco integrated services router network modules:**

- **Cisco HWIC-AP 802.11 Netowork Module**
- **Cisco IPS Network Module**
- **Cisco Content Engine Network Module for content security**
- **Cisco Network Analysis Module**
- **Many others including:**
  - **WIC-2T**
  - **WIC-1B**
  - **VWIC-1MFT**



© 2006 Cisco Systems, Inc. All rights reserved.


The Cisco High-Speed WAN Interface Card (HWIC)-Access Point (AP) 802.11 Network Module is an integrated secure 802.11 access point for modular integrated services routers. It provides these features:

- Single-band 802.11b/g or dual-band 802.11a/b/g radios
- Extensive WLAN security capabilities including the following:
  - Support for wireless fidelity protected access enterprise mode and personal mode
  - Wired equivalent privacy WEP), Temporal Key Integrity Protocol (TKIP), key management
  - 802.1x
  - Cisco Lightweight Extensible Authentication Protocol (LEAP) and Extensible Authentication Protocol (EAP)
  - AAA, RADIUS, and NAC

The Cisco IPS Network Module for Cisco Routers includes innovative technologies that give users the confidence to take preventative actions on a broader range of threats. These technologies, including correlation and validation tools, greatly reduce the risk of dropping legitimate traffic.

The Cisco 2800 and 3800 Series Content Engine Network Modules offer the only router-integrated application and content networking system in the industry. Available configurations include a 40-GB hard disk or an 80-GB internal hard disk.

The Cisco Network Analysis Module (NAM) for integrated services routers has these features:

- The module is quick to deploy and easy to use with an embedded web-based NAM Traffic Analyzer GUI.
- The module analyzes traffic flows for applications, hosts, conversations, and IP-based services such as QoS and VoIP.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

- The module collects NetFlow Data Export (NDE) to provide broad application-level visibility.
- The module tracks response times using the Administrative Reporting Tool (ART) MIB to isolate application performance problems related to the network or to the server.

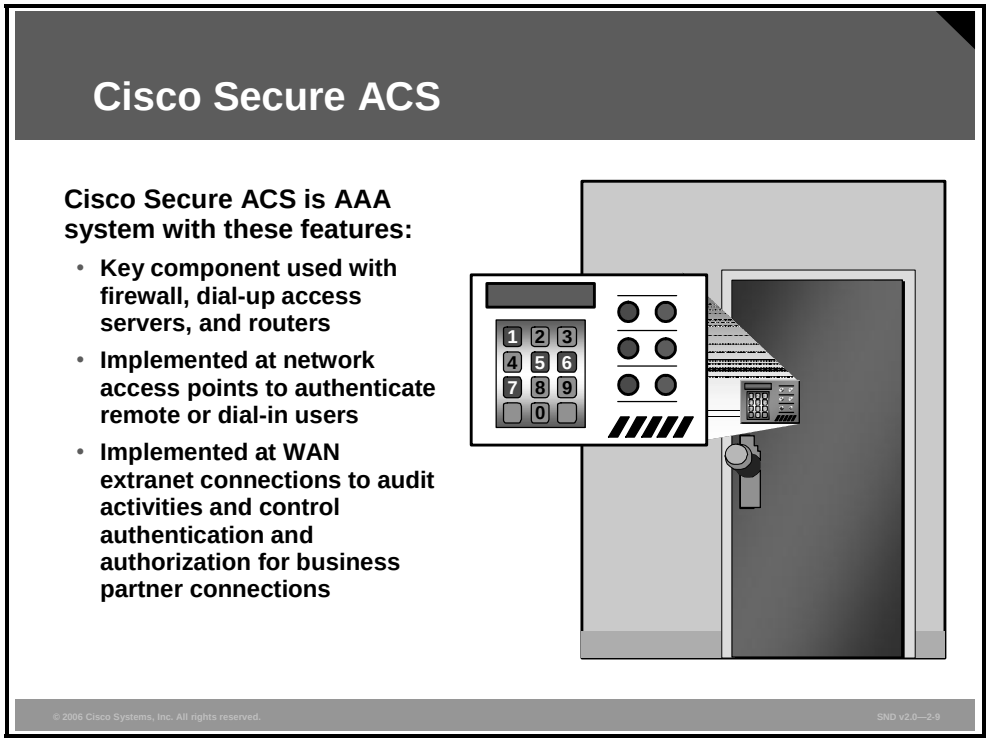
**Note** For a complete list of supported modules refer to http://www.cisco.com/warp/public/765/tools/quickreference/routerperformance.pdf.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Identity Solutions

This topic describes the use of Cisco Secure ACS to provide network security through identification and authentication.




You can leverage the Cisco Secure ACS framework to control administrator access and configuration for all network devices in your network that are enabled by RADIUS and TACACS+. Here are some of the advanced features of the Cisco Secure ACS:

- Automatic service monitoring
- Database synchronization and importing of tools for large-scale deployments
- Lightweight Directory Access Protocol (LDAP) user authentication support
- User and administrative access reporting
- Restrictions such as time of day and day of week
- User and device group profiles


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

## Cisco Secure ACS—Product Summary

**Here is a Cisco Secure ACS product summary:**

- **Easy-to-use web GUI**
- **Full RADIUS and TACACS+ user and administrator access control**
- **High performance (500+ authorizations per second)**
- **Supports LDAP, Novell Directory Services, and Open Database Connectivity datastores**
- **Scalable data replication and redundancy services**
- **Full accounting and user reporting features**
- **Supports third-party one-time passwords**



© 2006 Cisco Systems, Inc. All rights reserved.

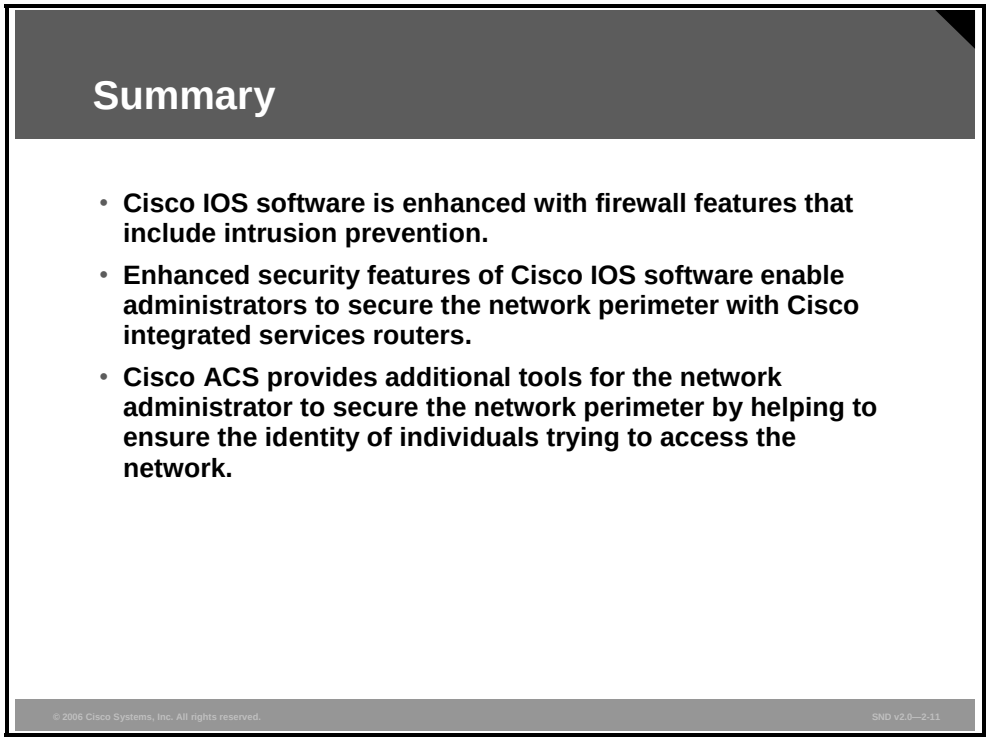

This figure summarizes the features of Cisco Secure ACS.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Summary

This topic summarizes the key points that were discussed in this lesson.




# References

For additional information, refer to these resources:

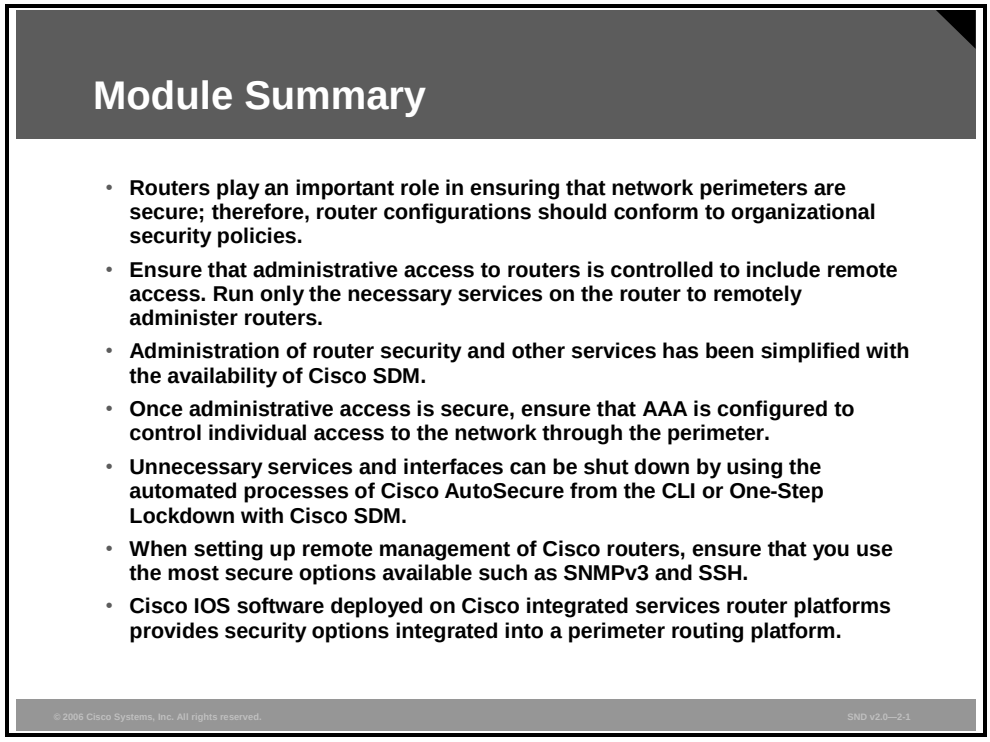
- Cisco Systems, Inc. Security and VPN. http://www.cisco.com/en/US/products/hw/vpndevc/index.html.
- Cisco Systems, Inc. Cisco Self-Defending Network. http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_package.html.


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module Summary

This topic summarizes the key points that were discussed in this module.




The security of a network environment includes the security of Layer 2 devices in the LAN, including wired and wireless devices. You must ensure that these LAN devices are accounted for in the security policy for your organization, and then you must configure the built-in features in these devices to secure your LAN.



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# References

For additional information, refer to these resources:

- Antoine, V., R. Bongiorni, A. Borza, et al. National Security Agency. *Router Security Configuration Guide*. http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf.
- Cisco Systems, Inc. *Role-Based CLI Access*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtclivws.htm.
- Cisco Systems, Inc. *Cisco SDM Express 2.2 User's Guide*. http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a0080530bc5.html#wp1039240.
- Cisco Systems, Inc. *Cisco Router and Security Device Manager Version 2.2 User's Guide*. http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_book09186a00804bfd82.html.
- Cisco Systems, Inc. How to Use Cisco IOS Resilient Configuration. http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008022a7ce.html#wp1027188.
- Cisco Systems, Inc. Cisco IOS Login Enhancements.http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb3.html.
- Cisco Systems, Inc. Security and VPN. http://www.cisco.com/en/US/products/hw/vpndevc/index.html.
- Cisco Systems, Inc. Cisco Self-Defending Network. http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_package.html.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) Considering how routers function, describe the security concerns that arise for unsecured routers. (Source: Applying a Security Policy for Cisco Routers)

_____

_____

Q2) Which command is used to enter privileged or privileged EXEC mode? (Source: Securing Administrative Access to Cisco Routers)

Q3) List the passwords that are, by default, shown as clear text (unencrypted) in the router configuration. (Source: Securing Administrative Access to Cisco Routers)

Q4) By default, Cisco router auxiliary ports do not require a password for remote administrative access. (Source: Securing Administrative Access to Cisco Routers)

A) true
B) false

Q5) What is the default number of failed attempts and delay time before login can begin again? (Source: Securing Administrative Access to Cisco Routers)

Q6) What happens when the number of failed login attempts reaches the configured rate? (Source: Securing Administrative Access to Cisco Routers)

Q7) How long does an administrative interface stay active (and logged in) by default? (Source: Securing Administrative Access to Cisco Routers)

Q8) In the **banner motd** command, the **motd** keyword stands for _____. (Source: Securing Administrative Access to Cisco Routers)

Q9) Describe what you are able to do in the “Configure” and the “Monitor” modes of the Cisco Router and Security Device Manager. (Source: Introducing Cisco SDM)



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q10) Name the strongest authentication method. (Source: Configuring AAA Functions on the Cisco IOS Router)

---

Q11) List the three pieces of the S/Key system. (Source: Configuring AAA Functions on the Cisco IOS Router)

---

Q12) Put the three steps required to configure the router for AAA in the correct order. Put the letter "A" in the blank next to your choice for the first step, the letter "B" for the second step and so on. (Source: Configuring AAA Functions on the Cisco IOS Router)

_____ 1. Configure AAA on the router. _____

_____ 2. Secure access to privileged EXEC and configuration mode on vty, asynchronous, auxiliary, and TTY ports. _____

_____ 3. Enable AAA globally on the router. _____

Q13) How can you guard against the risk of being locked out of a router should the administrative session fail while you are in the process of enabling AAA? (Source: Configuring AAA Functions on the Cisco IOS Router)

---

Q14) What authentication method uses "something you have and something you know"? (Source: Configuring AAA Functions on the Cisco IOS Router)

A) token card
B) OTP
C) username and password (aging)
D) username and password (static)


© 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q15) Match the commands to the description by placing the letter of the command in the space provided beside the description (Source: Configuring AAA Functions on the Cisco IOS Router)

A) **aaa new-model**
B) **aaa authentication**
C) **aaa authentication login**
D) **aaa authentication ppp**
E) **aaa authentication enable default**
F) **aaa authorization**

_____ 1. In global configuration mode, this command enables the authentication process.

_____ 2. In global configuration mode, this command enables AAA authentication to determine if a user can assess the privileged command level.

_____ 3. This command forces the router to override every other authentication method previously configured for the router lines.

_____ 4. In global configuration mode, this command specifies one or more AAA authentication methods for use on serial interfaces.

_____ 5. In global configurations mode, this command sets AAA authentication at login.

_____ 6. In global configuration mode, this command sets parameters that restrict administrative access to the routers or user access to the network.

Q16) List the three **debug** commands used for troubleshooting AAA. (Source: Configuring AAA Functions on the Cisco IOS Router)

---

Q17) Which command is used to disable CDP? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) **shutdown cdp**
B) **no cdp**
C) **no cdp server**
D) **no cdp run**

Q18) Which two commands disable autoloading? (Choose two.) (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) **no boot network**
B) **no service autoloading**
C) **no service config**
D) **no autoload config**

Q19) Which command disables FTP with Cisco IOS software releases prior to Cisco IOS Release 12.3? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) **no ftp-server write-enable**
B) **no ftp-server enable**



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q20) Which service should be disabled to prevent a Cisco router from accessing a copy of a Cisco IOS image on another Cisco router running the same protocol? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) CDP
B) BOOTP server
C) configuration autoloading
D) MOP

Q21) Which service can attackers use during reconnaissance attacks to learn of neighboring Cisco devices? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) finger
B) configuration autoloading
C) CDP
D) IP source routing

Q22) Match the threats to the correct mitigation technique. (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) An attacker is corrupting the network time base.
B) An attack on the X.25 interface can cause disruptions to both route processing and device stability.
C) An attacker sends a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable by the attacker and falsifying the source port to be the DNS service port (port 53).
D) This protocol is a potential attack vector on the router.

_____ 1. disable MOP service

_____ 2. disable PAD service

_____ 3. disable the NTP service globally

_____ 4. disable small servers

Q23) Which service requires five steps to completely disable access to the router? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) SNMP
B) HTTP
C) DNS lookup
D) TFTP
E) FTP

Q24) Which service should not be disabled if a router management tool, such as the Cisco Router and Security Device Manager , is used to manage the router? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) SNMP
B) HTTP
C) DNS lookup
D) TFTP
E) FTP

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q25) Which command is used to define an SNMP password? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) **snmp-server enable**
B) **snmp-server host**
C) **snmp-server community**
D) **snmp-server password**
E) **snmp-server manager**

Q26) Which router command enables the sending of all types of SNMP traps? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

A) **snmp-server community**
B) **snmp-server enable informs**
C) **snmp-server enable traps snmp**
D) **snmp-server enable traps**

Q27) What Cisco IOS software feature should be disabled to stop attackers from mapping your network? (Source: Disabling Unused Cisco Router Network Services and Interfaces)

Q28) What are some of the considerations when planning how to implement logging on a network? (Source: Implementing Secure Management and Reporting)

Q29) Besides being able to securely manage devices on a network, what other security concern should a network administrator have with respect to attacks or network failure? (Source: Implementing Secure Management and Reporting)



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q30) Label the descriptions as either out-of-band or in-band. (Source: Implementing Secure Management and Reporting)

A) Information flows across the enterprise production network or the Internet (or both). _____
B) Information flows within a network on which no production traffic resides. _____
C) This type of management is recommended for devices in large enterprise networks. _____
D) This type of management is recommended for devices in smaller networks. _____

Q31) Label the guidelines as applicable to in-band management, as applicable to out-of-band management, or as applicable to both. (Source: Implementing Secure Management and Reporting)

A) In-band management uses IPsec when possible. _____
B) Out-of-band provides the highest level of security and mitigates the risk of passing insecure management protocols over the production network management. _____
C) Both keep clocks on hosts and network devices synchronized. _____
D) In-band management uses SSH or SSL instead of Telnet. _____
E) Both record changes and archive configurations. _____

Q32) What two types of systems are parts of a syslog implementation? (Source: Implementing Secure Management and Reporting)

---

Q33) Indicate the severity number (0 to 7) after the corresponding name and description of log events. (Source: Implementing Secure Management and Reporting)

A) emergencies (router unusable) _____
B) informational (informational message) _____
C) errors (error condition) _____
D) warnings (warning condition) _____
E) alerts (immediate action required) _____
F) notifications (informational message) _____
G) debugging (debug message) _____
H) critical (condition critical) _____

Q34) Describe some of the security features available with the Cisco Integrated Services Router (Source: Defending the Network Perimeter with Cisco Products)

---

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

# Module Self-Check Answer Key

Q1) Compromise of the route tables of a router can result in denial of network services and exposure of sensitive data. Compromise of router access control can result in exposure of network configuration details, which can facilitate attacks against other network components. Finally, a poor router filtering configuration can expose internal network components to scans and attacks, and make it easier for attackers to avoid detection.

Q2) the **enable secret** command

Q3) All Cisco router passwords are, by default, stored in clear text form except the enable secret password.

Q4) A

Q5) 10 login failures and a 15-second delay

Q6) A TOOMANY_AUTHFAILS event message is sent by the router to the configured syslog server and a set time delay timer begins.

Q7) 10 minutes

Q8) **motd s**pecifies and enables a message-of-the-day (MOTD) banner.

Q9) Configure mode provides wizards for the novice. More experienced users are able to perform tasks in any order and outside of the wizards. Your are able to configure interfaces, configure Cisco IOS firewall and ACLs, configure VPNs, carry out a security audit, configure basic and advanced NAT, configure intrusion prevention, configure QoS, and configure Network Control Access policies. Monitor mode is where the user can view the current status of the router for all the configurations done earlier.

Q10) Token cards or soft tokens using OTPs

Q11) the client, the host, and a password calculator

Q12) A-3, B-1, C-2

Q13) provide for a local login method

Q14) A

Q15) A-3, B-1, C-5, D-4, E-2, F-6

Q16) **debug aaa authorization**, **debug aaa authentication**, and **debug aaa accounting**

Q17) D

Q18) A, C

Q19) B

Q20) B

Q21) C

Q22) A-3, B-2 , C-4, D-1

Q23) A

Q24) B

Q25) C

Q26) D

Q27) disable ICMP unreachable messages



*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*

Q28) These questions should be considered when planning to implement logging on a network:

- Which logs are most important?
- How do you separate important messages from mere notifications?
- How do you ensure that logs are not tampered with in transit?
- How do you ensure that your time stamps match each other when multiple devices report the same alarm?
- What information is needed if log data is required for a criminal investigation?
- How do you deal with the volume of messages that can be generated by a large network?

Q29) Besides figuring out how to securely manage many devices in many locations, a network administrator must be able to track changes on devices to troubleshoot when attacks or network failures occur.

Q30) A) in-band

B) out-of-band

C) out-of-band

D) in-band

Q31) A) in-band management

B) out-of-band management

C) both in-band management and out-of-band management

D) in-band management

E) both in-band and out-of-band management

Q32) syslog servers and syslog clients

Q33) A) 0 B) 6 C) 3 D) 4 E) 1 F) 5 G) 7 H) 2

Q34) Some of the security related features of the Cisco integrated services routers are built-in VPN acceleration, secure voice, high-performance AIM, and USB port.

 © 2006 Cisco Systems, Inc.

*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.*