ISCW

Implementing Secure Converged Wide Area Networks

Volume 1

Version 1.0

Student Guide

Editorial, Production, and Graphic Services: 07.21.06

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

Table of Contents

Volume 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 self-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 self-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 self-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 self-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 self-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 self-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 self-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 self-study.

Course Introduction

Overview

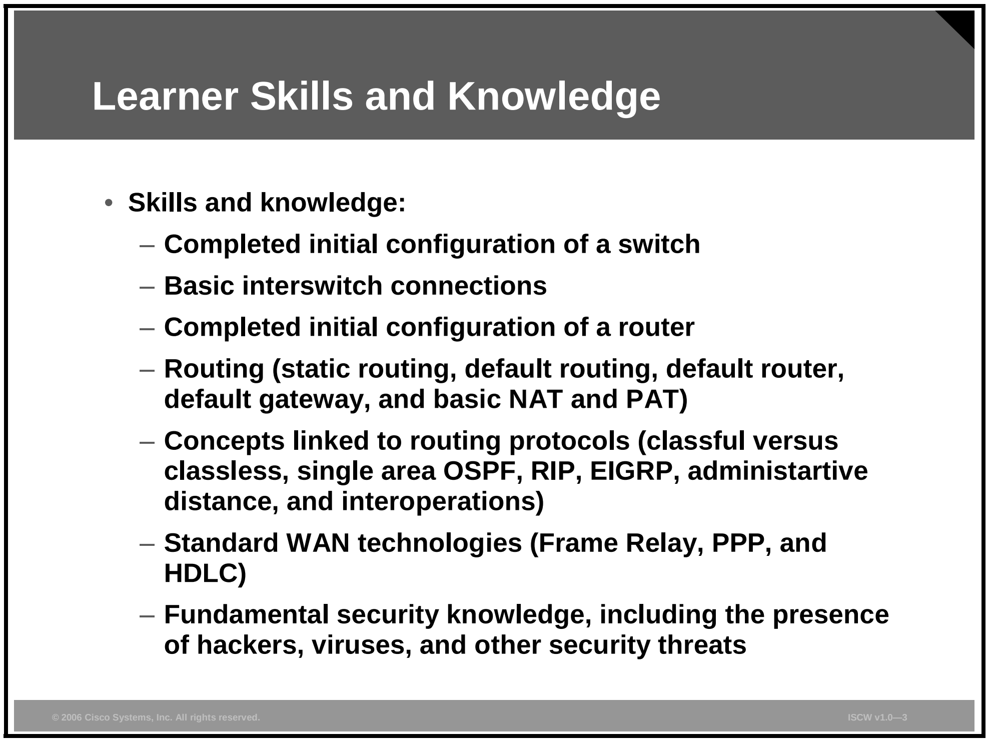
Implementing Secure Converged Wide Area Networks (ISCW) is an advanced course that introduces techniques and features enabling or enhancing WAN and remote access solutions. The course focuses on using one or more of the available WAN connection technologies for remote access between enterprise sites.

This course includes cable modems and DSL with Network Address Translation (NAT), Multiprotocol Label Switching (MPLS), virtual private networks (VPNs), and network security using VPNs with IPSec encryption and Internet Key Exchange (IKE) keys. After taking this course, learners will be able to secure the network environment using existing Cisco IOS security features, and configure the three primary components of the Cisco IOS Firewall Feature set: firewall, intrusion prevention system (IPS), and authentication, authorization, and accounting (AAA). This task-oriented course teaches the knowledge and skills needed to secure Cisco IOS router networks using features and commands in Cisco IOS software, and using a router configuration application. ISCW is part of the recommended learning path for students seeking the Cisco Certified Network Professional (CCNP).

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.

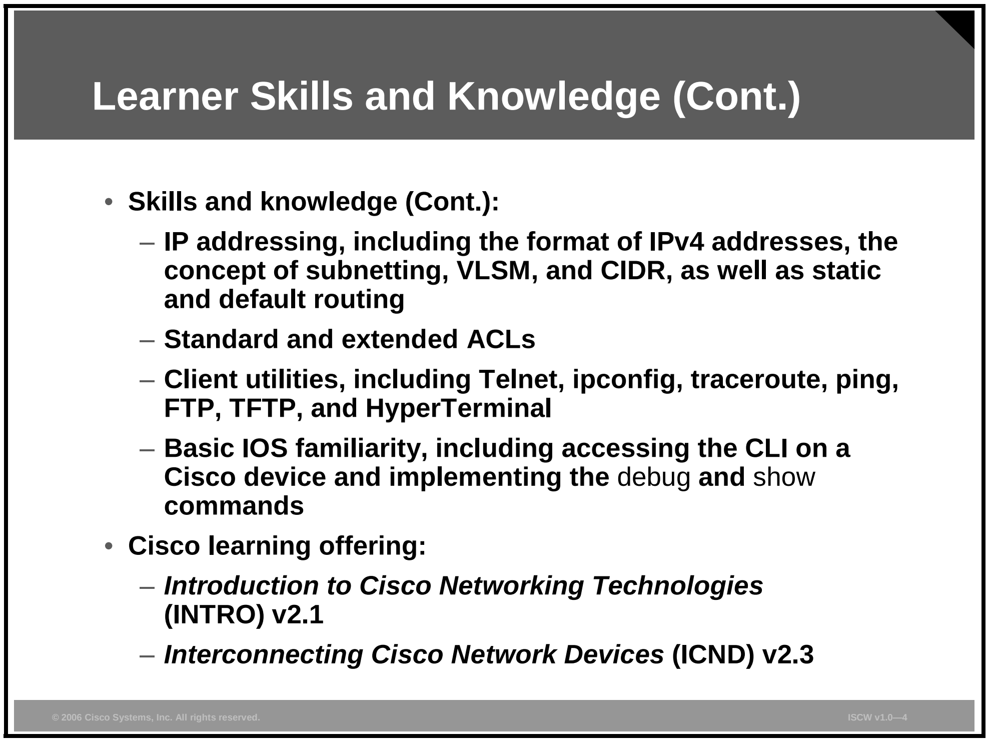
*The PDF files and any printed representation for this material are the property of Cisco Systems, Inc.,
for the sole use by Cisco employees for personal study. The files or printed representations may not be
used in commercial training, and may not be distributed for purposes other than individual self-study.*



Learner Skills and Knowledge

- Skills and knowledge:
  - Completed initial configuration of a switch
  - Basic interswitch connections
  - Completed initial configuration of a router
  - Routing (static routing, default routing, default router, default gateway, and basic NAT and PAT)
  - Concepts linked to routing protocols (classful versus classless, single area OSPF, RIP, EIGRP, administartive distance, and interoperations)
  - Standard WAN technologies (Frame Relay, PPP, and HDLC)
  - Fundamental security knowledge, including the presence of hackers, viruses, and other security threats

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3



Learner Skills and Knowledge (Cont.)

- Skills and knowledge (Cont.):
  - IP addressing, including the format of IPv4 addresses, the concept of subnetting, VLSM, and CIDR, as well as static and default routing
  - Standard and extended ACLs
  - Client utilities, including Telnet, ipconfig, traceroute, ping, FTP, TFTP, and HyperTerminal
  - Basic IOS familiarity, including accessing the CLI on a Cisco device and implementing the debug and show commands
- Cisco learning offering:
  - *Introduction to Cisco Networking Technologies* (INTRO) v2.1
  - *Interconnecting Cisco Network Devices* (ICND) v2.3

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4

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

Course Goal and Objectives

This topic describes the course goal and objectives.

Course Goal

"The goal of the ISCW course is to expand the reach of the enterprise network to teleworkers and remote sites. The theme of implementing a highly available network with connectivity options, such as VPN and wireless, is highlighted."

Implementing Secure Converged Wide Area Networks

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5

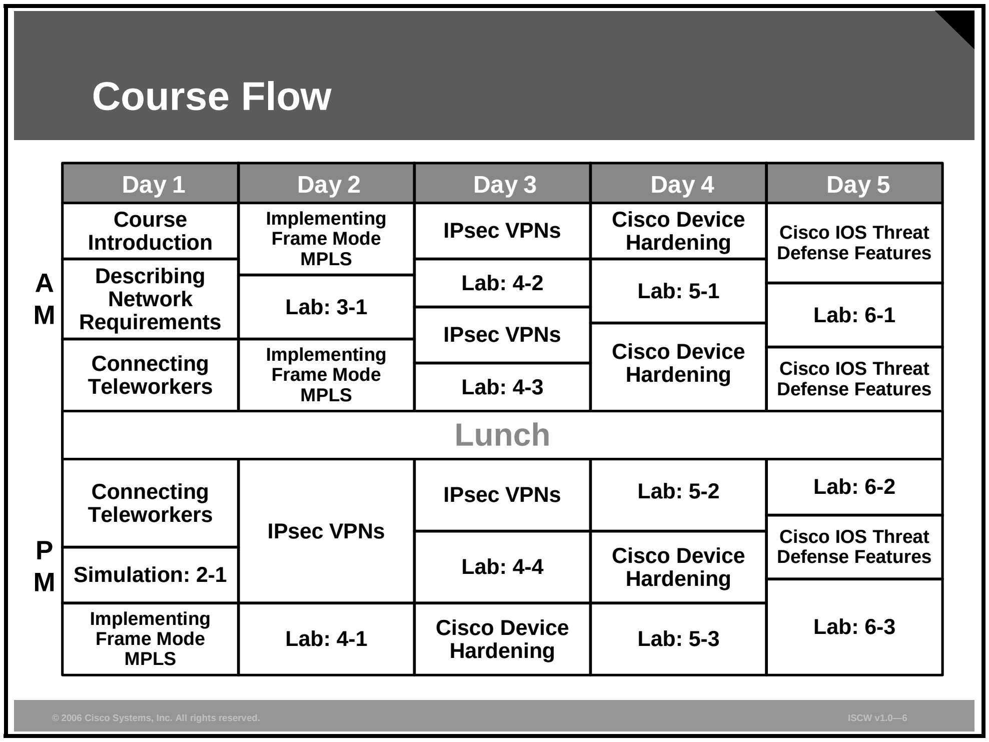
Upon completing this course, you will be able to meet these objectives:

- Describe the remote connectivity requirements for secured access and explain the alignment of these requirements with Cisco network architectures
- Describe and implement teleworker broadband connectivity
- Implement and verify frame-mode MPLS
- Describe and configure a site-to-site IPSec VPN
- Describe and configure Cisco device hardening
- Describe and configure IOS firewall 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 self-study.

Course Flow

This topic presents the suggested flow of the course materials.



Course Flow

	Day 1	Day 2	Day 3	Day 4	Day 5
A M	Course Introduction	Implementing Frame Mode MPLS	IPsec VPNs	Cisco Device Hardening	Cisco IOS Threat Defense Features
	Describing Network Requirements	Lab: 3-1	Lab: 4-2	Lab: 5-1	Lab: 6-1
	Connecting Teleworkers	Implementing Frame Mode MPLS	IPsec VPNs	Cisco Device Hardening	Cisco IOS Threat Defense Features
			Lab: 4-3		
	Lunch				
P M	Connecting Teleworkers	IPsec VPNs	IPsec VPNs	Lab: 5-2	Lab: 6-2
	Simulation: 2-1		Lab: 4-4	Cisco Device Hardening	Cisco IOS Threat Defense Features
	Implementing Frame Mode MPLS	Lab: 4-1	Cisco Device Hardening	Lab: 5-3	Lab: 6-3

© 2006 Cisco Systems, Inc. All rights reserved.

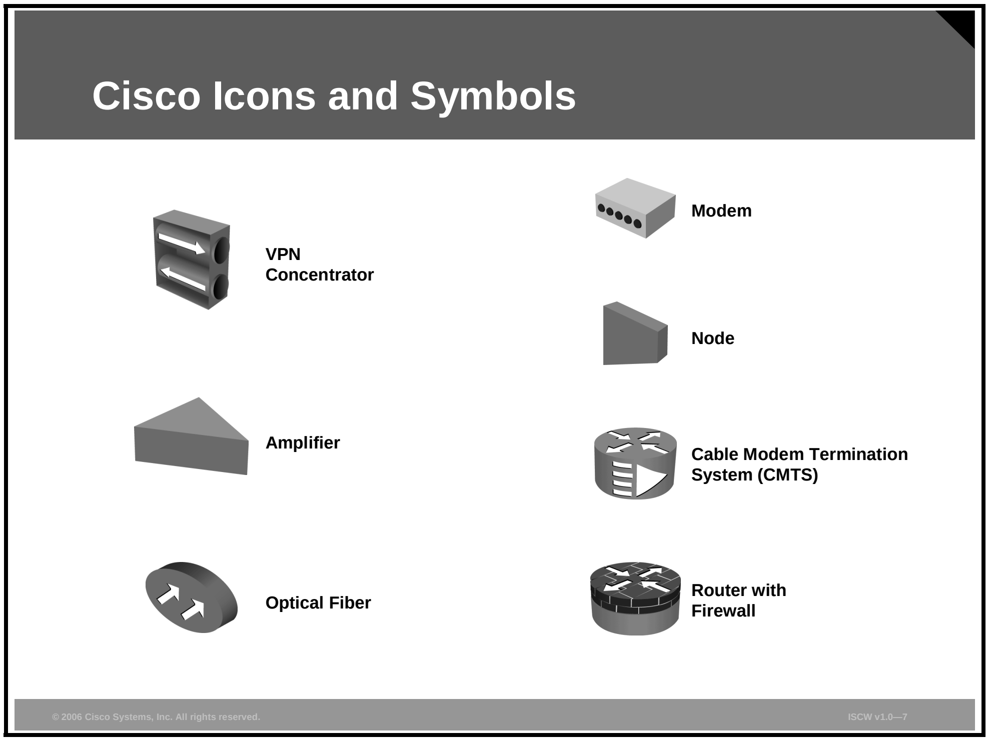
ISCW v1.0—6

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 self-study.

Additional References

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



Cisco Icons and Symbols

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—7

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 self-study.

Your Training Curriculum

This topic presents the training curriculum for this course.

Cisco Career Certifications

Cisco **Certifications**

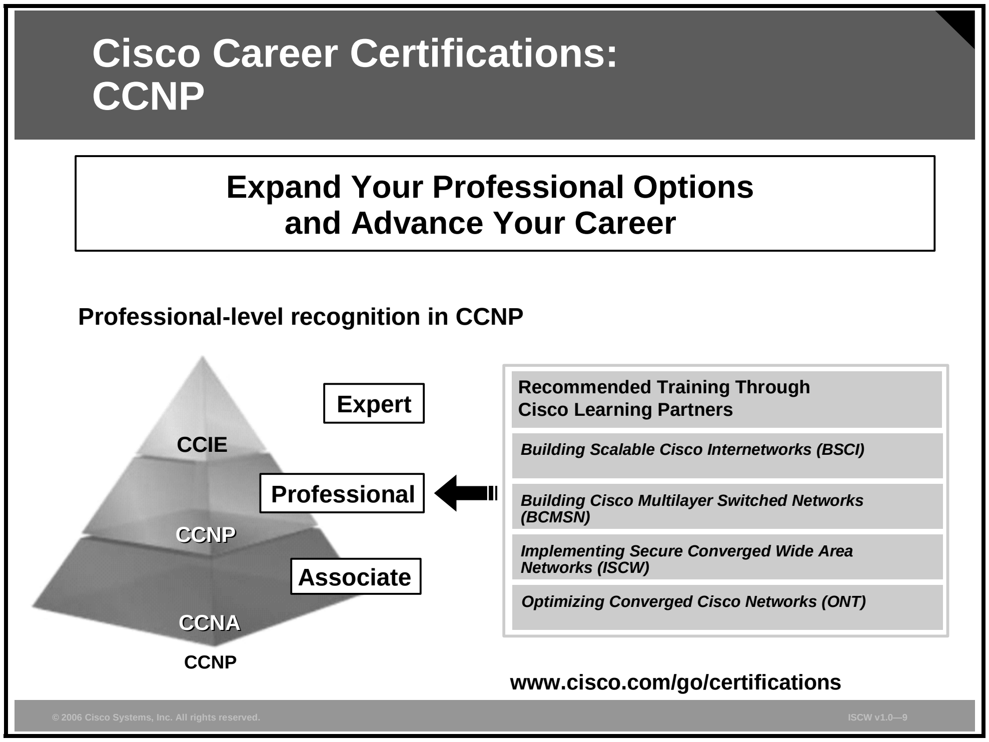
www.cisco.com/go/certifications

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—8

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 self-study.



Cisco Career Certifications: CCNP

Expand Your Professional Options and Advance Your Career

Professional-level recognition in CCNP

CCNP

Recommended Training Through Cisco Learning Partners

- *Building Scalable Cisco Internetworks (BSCI)*
- *Building Cisco Multilayer Switched Networks (BCMSN)*
- *Implementing Secure Converged Wide Area Networks (ISCW)*
- *Optimizing Converged Cisco Networks (ONT)*

www.cisco.com/go/certifications

© 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 self-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 self-study.

Module 1

Network Connectivity Requirements

Overview

This module describes conceptual network models that affect converged networks and the services that run on those networks. The module explains the Cisco vision of the Intelligent Information Network (IIN) and the Cisco Service-Oriented Network Architecture (SONA). The remote connectivity infrastructure and services is discussed within the Cisco enterprise architecture, explaining the diversity of access options for branch offices and teleworkers, with a focus on security.

Module Objectives

Upon completing this module, you will be able to describe the remote connectivity requirements for secured access and explain the alignment of these requirements with Cisco network architectures.

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

Lesson 1

Describing Network Requirements

Overview

Conceptual network models that affect converged networks and the services they offer also affect the integration of remote offices and teleworkers into enterprise networks. This lesson starts with introducing the Cisco Systems vision of the Intelligent Information Network (IIN) and the Cisco Service-Oriented Network Architecture (SONA). This architectural framework shifts the view of the network from a pure traffic transport-oriented view toward a service- and application-oriented view. The Cisco Enterprise Architecture is explained and aligned with the traditional three-layer hierarchical network model. Remote connectivity infrastructure and services options are discussed, and the lesson concludes with an example showing a variety of advanced technology options for secure access.

Objectives

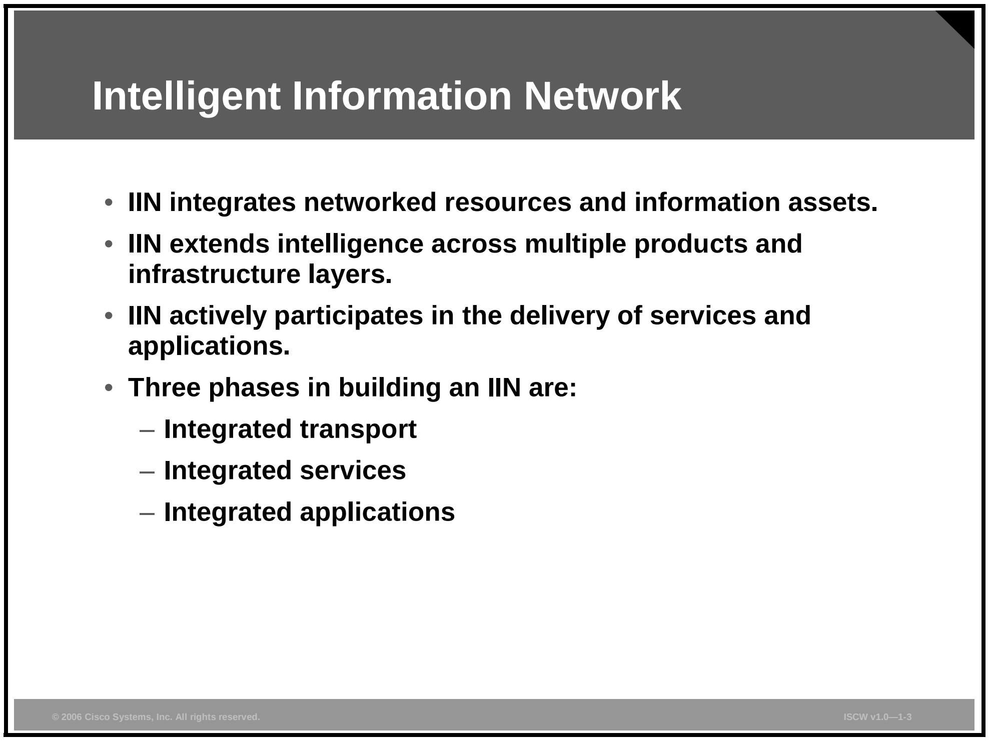
Upon completing this lesson, you will be able to describe the remote connectivity requirements and their alignment with Cisco network architectures. This ability includes being able to meet these objectives:

- Describe the IIN and the SONA framework
- Explain the Cisco conceptual network models, such as Cisco Enterprise Architecture and the Cisco hierarchical network model
- Describe the requirements for establishing secure remote connections in a converged 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 self-study.

IIN and Cisco SONA Framework

This topic describes the IIN, its features, and the Cisco SONA that guides an evolution of enterprise networks towards IIN.



Intelligent Information Network

- IIN integrates networked resources and information assets.
- IIN extends intelligence across multiple products and infrastructure layers.
- IIN actively participates in the delivery of services and applications.
- Three phases in building an IIN are:
  - Integrated transport
  - Integrated services
  - Integrated applications

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—1-3

Intelligent Information Network

The Cisco vision of the future IIN encompasses these features:

- Integration of networked resources and information assets. The modern converged networks with integrated voice, video, and data require that IT departments more closely link the IT infrastructure with the network.
- Intelligence across multiple products and infrastructure layers. The intelligence built into each component of the network is extended network-wide and applies end-to-end.
- Active participation of the network in the delivery of services and applications. With added intelligence within the network devices, the IIN makes it possible for the network to actively manage, monitor, and optimize service and application delivery across the entire IT environment.

The described features show that the IIN offers much more than basic connectivity, bandwidth for users, and access to applications. The IIN offers end-to-end functionality and a centralized, unified control that promotes true business transparency and agility.

The IIN technology vision offers an evolutionary approach that consists of three phases in which functionality can be added to the infrastructure as required:

- **Integrated transport:** Everything—data, voice, and video—consolidates onto an IP network for secure network convergence. By integrating data, voice, and video transport into a single, standards-based, modular network, organizations can simplify network management and generate enterprise-wide efficiencies. Network convergence also lays the foundation for a new class of IP-enabled applications delivered through Cisco IP Communications solutions.

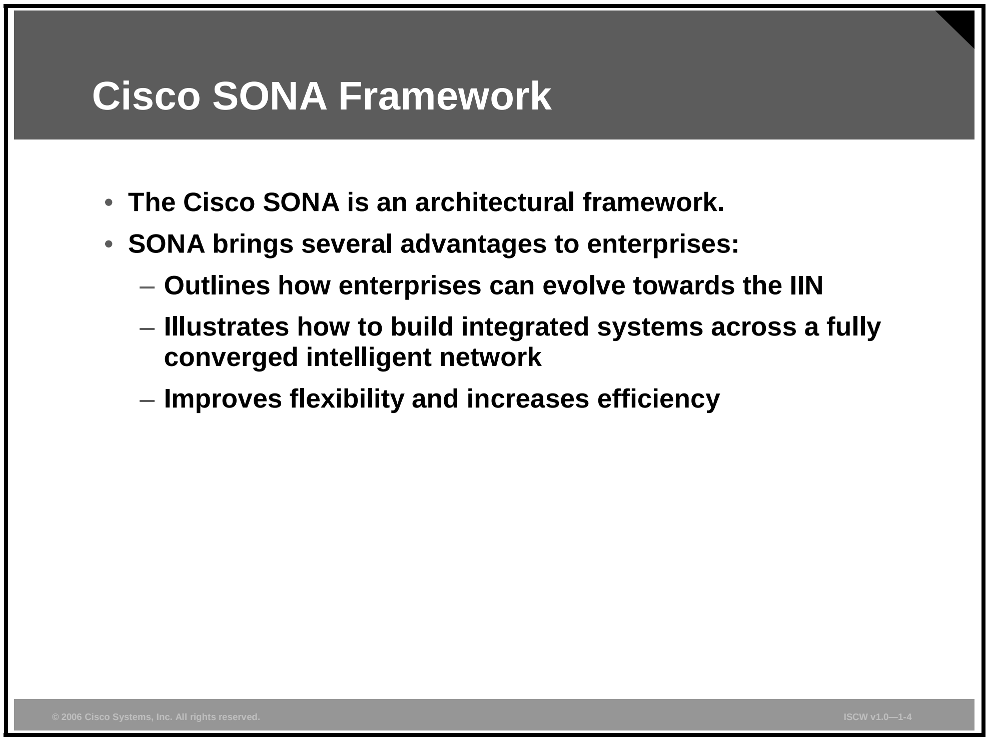
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **Integrated services:** Once the network infrastructure has been converged, IT resources can be pooled, and shared or "virtualized" to flexibly address the changing needs of the organization. Integrated services help to unify common elements, such as storage and data center server capacity. By extending virtualization capabilities to encompass server, storage, and network elements, an organization can transparently use all of its resources more efficiently. Business continuity is also enhanced because shared resources across the IIN provide services in the event of a local systems failure.
- **Integrated applications:** With Application-Oriented Networking (AON) technology, Cisco has entered the third phase of building the IIN. This phase focuses on making the network "application-aware" so that it can optimize application performance and more efficiently deliver networked applications to users. In addition to capabilities such as content caching, load balancing, and application-level security, Cisco AON makes it possible for the network to simplify the application infrastructure by integrating intelligent application message handling, optimization, and security into the existing 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 self-study.

Cisco SONA Framework

With its vision of the IIN, Cisco is helping organizations to address new IT challenges, such as the deployment of service-oriented architectures, web services, and virtualization.



Cisco SONA Framework

- The Cisco SONA is an architectural framework.
- SONA brings several advantages to enterprises:
  - Outlines how enterprises can evolve towards the IIN
  - Illustrates how to build integrated systems across a fully converged intelligent network
  - Improves flexibility and increases efficiency

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—1-4

The Cisco Service-Oriented Network Architecture (SONA) is an architectural framework that guides the evolution of enterprise networks to an IIN. The SONA framework provides these advantages to enterprises:

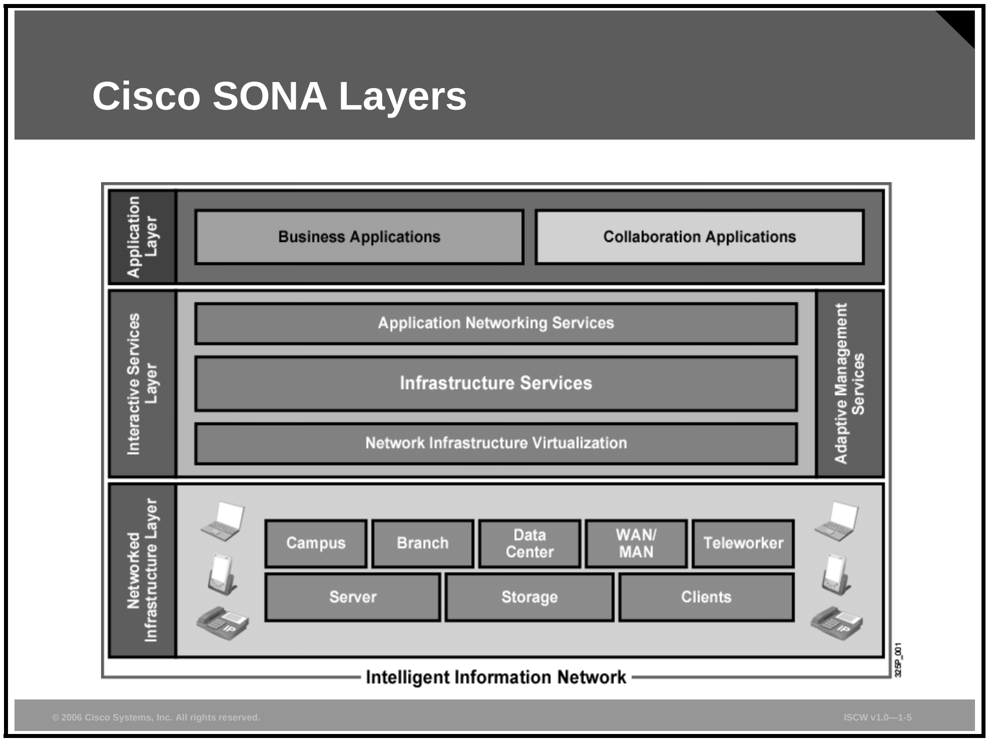
- Outlines the path towards the IIN
- Illustrates how to build integrated systems across a fully converged IIN
- Improves flexibility and increases efficiency, which results in optimized applications, processes, and resources

Cisco SONA uses the extensive product line, services, proven architectures, and experience of Cisco and its partners to help the enterprises achieve their business goals.

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

Cisco SONA Layers

The SONA framework shows how integrated systems can both allow a dynamic, flexible architecture, and provide for operational efficiency through standardization and virtualization.



Cisco SONA Layers

Application Layer
Business Applications
Collaboration Applications
Interactive Services Layer
Application Networking Services
Infrastructure Services
Network Infrastructure Virtualization
Adaptive Management Services
Networked Infrastructure Layer
Campus
Branch
Data Center
WAN/ MAN
Teleworker
Server
Storage
Clients
Intelligent Information Network
32SP_001

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—1-5

The SONA framework brings forth the notion that the network is the common element that connects and enables all components of the IT infrastructure. The SONA outlines these three layers of the IIN:

- **The networked infrastructure layer:** This is where all the IT resources are interconnected across a converged network foundation. The IT resources include servers, storage, and clients. The network infrastructure layer represents how these resources exist in different places in the network, including the campus, branch, data center, WAN, metropolitan-area network (MAN), and teleworker. The objective for customers in this layer is to have anywhere and anytime connectivity.
- **The interactive services layer:** This enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure. This layer comprises these services:
  - — Voice and collaboration services
  - — Mobility services
  - — Security and identity services
  - — Storage services
  - — Computer services
  - — Application networking services
  - — Network infrastructure virtualization
  - — Services management
  - — Adaptive management services

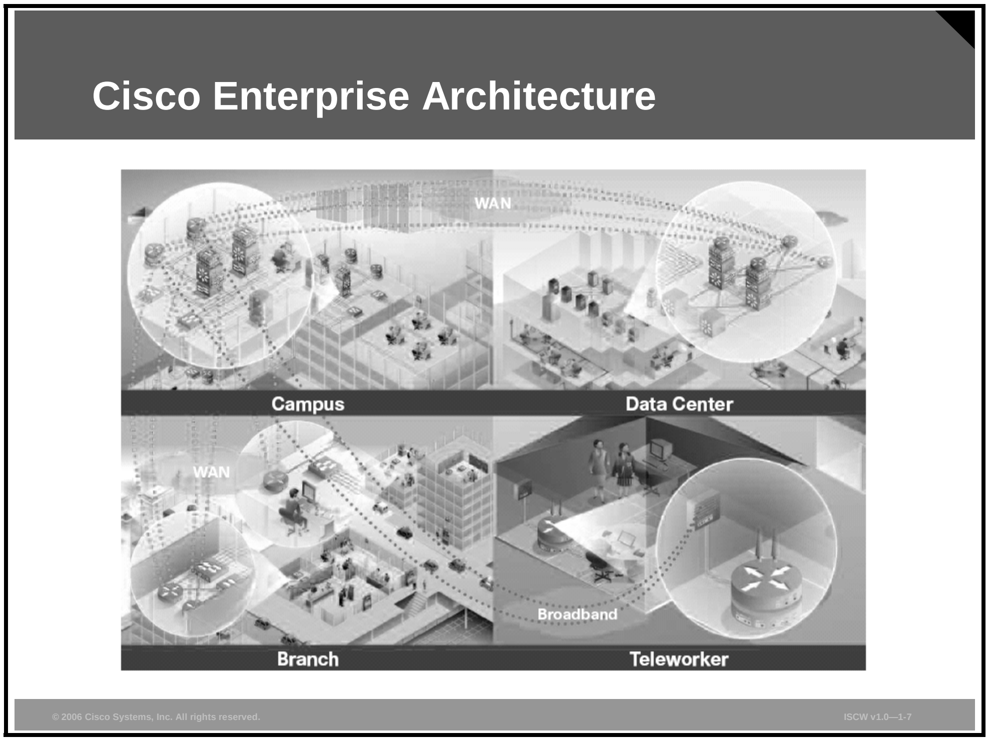
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **The application layer:** This includes business applications and collaboration applications. The objective for customers in this layer is to meet business requirements and achieve efficiencies by leveraging the interactive services layer.

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

Cisco Network Models

This topic describes Cisco network models in the Cisco Enterprise Architecture and their mapping to a traditional three-layer hierarchical network model.



Cisco Enterprise Architecture

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—1-7

Cisco Enterprise Architecture

Cisco provides enterprise-wide systems architecture that helps companies to protect, optimize, and grow their infrastructure to support their business processes. The architecture provides for integration of the entire network—campus, data center, WAN, branches, and teleworkers—offering staff secure access to the tools, processes, and services. The Cisco Enterprise Architecture consists of these elements:

- **Cisco Enterprise *Campus* Architecture:** Combines a core infrastructure of intelligent switching and routing with tightly integrated productivity-enhancing technologies, including Cisco IP Communications, mobility, and advanced security. The architecture provides the enterprise with high availability through a resilient multilayer design, redundant hardware and software features, and automatic procedures for reconfiguring network paths when failures occur. Multicast provides optimized bandwidth consumption, and quality of service (QoS) prevents oversubscription to ensure that real-time traffic, such as voice and video, or critical data is not dropped or delayed. Integrated security protects against and mitigates the impact of worms, viruses, and other attacks on the network—even at the switch port level. Cisco enterprise-wide architecture extends authentication support using standards such as 802.1x and Extensible Authentication Protocol (EAP). It also provides the flexibility to add IPsec and Multiprotocol Label Switching virtual private networks (MPLS VPNs), identity and access management, and VLANs to compartmentalize access. This helps improve performance and security, while also decreasing costs.

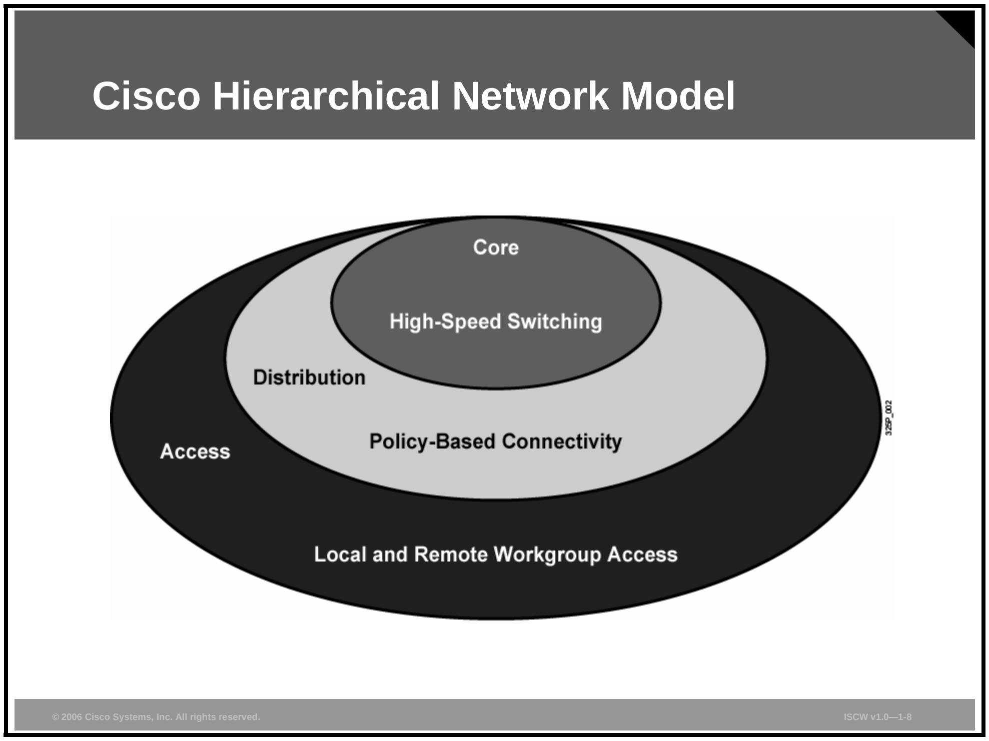
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc.,
for the sole use by Cisco employees for personal study. The files or printed representations may not be
used in commercial training, and may not be distributed for purposes other than individual self-study.

- **The Cisco Enterprise *Data Center* Architecture:** A cohesive, adaptive network architecture that supports the requirements for consolidation, business continuance, and security, while enabling emerging service-oriented architectures, virtualization, and on-demand computing. IT staff can easily provide departmental staff, suppliers, or customers with secure access to applications and resources. This simplifies and streamlines management, significantly reducing overhead. Redundant data centers provide backup using synchronous and asynchronous data, and application replication. The network and devices offer server and application load balancing to maximize performance. This solution allows the enterprise to scale without major changes to the infrastructure.
- **The Cisco Enterprise *Branch* Architecture:** Allows enterprises to extend head-office applications and services, such as security, Cisco IP Communications, and advanced application performance, to thousands of remote locations and users, or to a small group of branches. Cisco integrates security, switching, network analysis, caching, and converged voice and video services into a series of integrated services routers in the branch—so that enterprises can deploy new services when they are ready, without buying new equipment. This solution provides secure access to voice, mission-critical data, and video applications—anywhere, anytime. Advanced network routing, VPNs, redundant WAN links, application content caching, and local IP telephony call processing provide a robust architecture with high levels of resilience for all the branch offices. An optimized network leverages the WAN and LAN to reduce traffic, and save bandwidth and operational expenses. The enterprise can easily support branch offices with the ability to centrally configure, monitor, and manage devices located at remote sites, including tools, such as AutoQoS or the Security Device Manager (SDM) GUI QoS wizard, that proactively resolve congestion and bandwidth issues before they affect network performance.
- **The Cisco Enterprise *Teleworker* Architecture:** Allows enterprises to securely deliver voice and data services to remote small or home offices (small office, home office [SOHO]) over a standard broadband access service, providing a business resiliency solution for the enterprise and a flexible work environment for employees. Centralized management minimizes the IT support costs and robust integrated security mitigates the unique security challenges of this environment. Integrated security- and identity-based networking services enable the enterprise to help extend campus security policies to the teleworker. Staff can securely log into the network over an “always-on” VPN, and gain access to authorized applications and services from a single cost-effective platform. The productivity can further be enhanced by adding an IP phone, providing cost-effective access to a centralized IP Communications system with voice and unified messaging services.
- **Cisco Enterprise *WAN* Architecture:** Offers the convergence of voice, video, and data services over a single IP Communications network. This enables the enterprise to cost-effectively span large geographic areas. QoS, granular service levels, and comprehensive encryption options help ensure the secure delivery of high-quality corporate voice, video, and data resources to all corporate sites—enabling staff to work productively and efficiently wherever they are located. Security is provided with multiservice VPNs (IPsec and MPLS) over Layer 2 or Layer 3 WANs, hub-and-spoke, or full-mesh topologies.

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

Cisco Hierarchical Network Model

Traditionally, the three-layer hierarchical model has been used in network design.



Cisco Hierarchical Network Model

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—1-8

The model provides a modular framework that allows flexibility in network design, and facilitates ease of implementation and troubleshooting. The hierarchical model divides networks or their modular blocks into the access, distribution, and core layers, with these features:

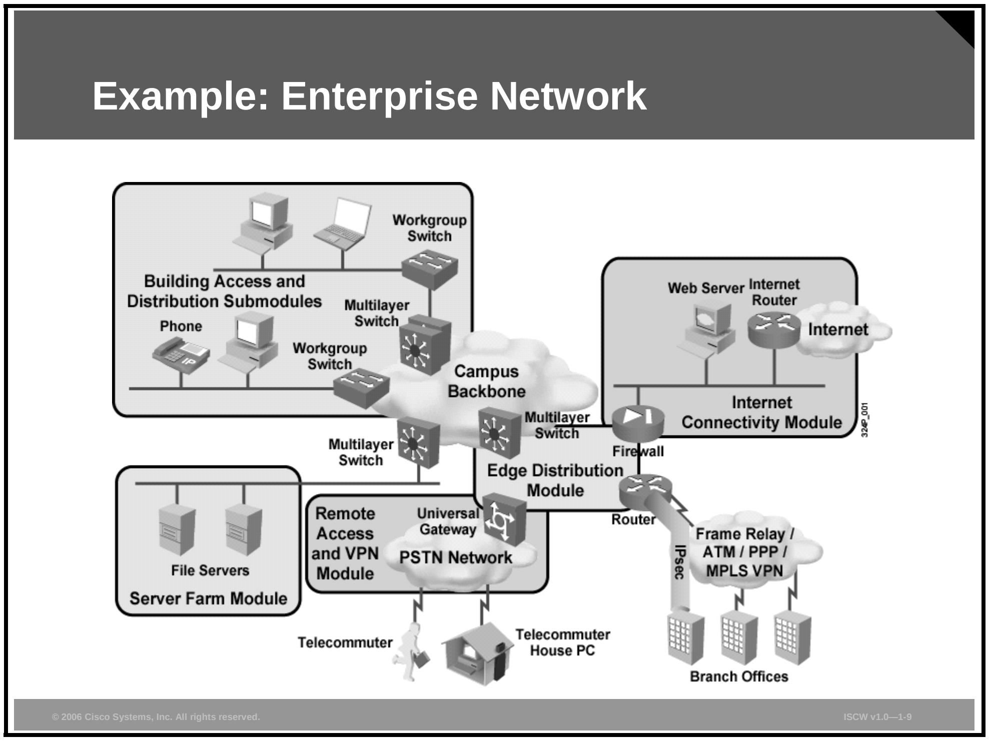
- **Access layer:** Used to grant user access to network devices. In a network campus, the access layer generally incorporates switched LAN devices with ports that provide connectivity to workstations and servers. In the WAN environment, the access layer at remote sites or teleworkers may provide access to the corporate network across WAN technology.
- **Distribution layer:** Aggregates the wiring closets, using switches to segment workgroups and isolate network problems in a campus environment. Similarly, the distribution layer aggregates WAN connection at the edge of the campus and provides policy-based connectivity.
- **Core layer (also referred to as the backbone):** A high-speed backbone, designed to switch packets as fast as possible. Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes very quickly.

Note The hierarchical model can be applied to any network type, such as LANs, WANs, Wireless LANs (WLANs), MANs, and VPNs, and to any modular block of the Cisco networking 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 self-study.

Example: Enterprise Network

The example shows a sample network that was deployed following Cisco Enterprise Architecture and the Cisco hierarchical model design.



Example: Enterprise Network

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—1-9

A branch office or remote site typically has fewer users, and therefore needs a WAN connection with lower requirements in terms of bandwidth and availability.

Remote sites typically connect to the central site and also sometimes connect to some other remote sites. Telecommuters may also require access to remote sites.

Remote site traffic can vary, but is typically sporadic. The network designer must determine whether it is more cost-effective to offer either a permanent or on-demand solution.

The remote site must have a variety of equipment, but does not require the same level of complexity as the central site. Typical WAN technologies used to connect a remote site to the central site include:

- Leased line
- Frame Relay
- ISDN
- Broadband services (cable or DSL)
- MPLS
- VPN

Typical considerations for setting up a remote-site WAN connection are as follows:

- **Multiple access options:** Remote users will connect to the branch site using various media. Branch site WANs must allow for multiple media options and simultaneous access by multiple users. The branch office must also have connectivity to the central or SOHO site.

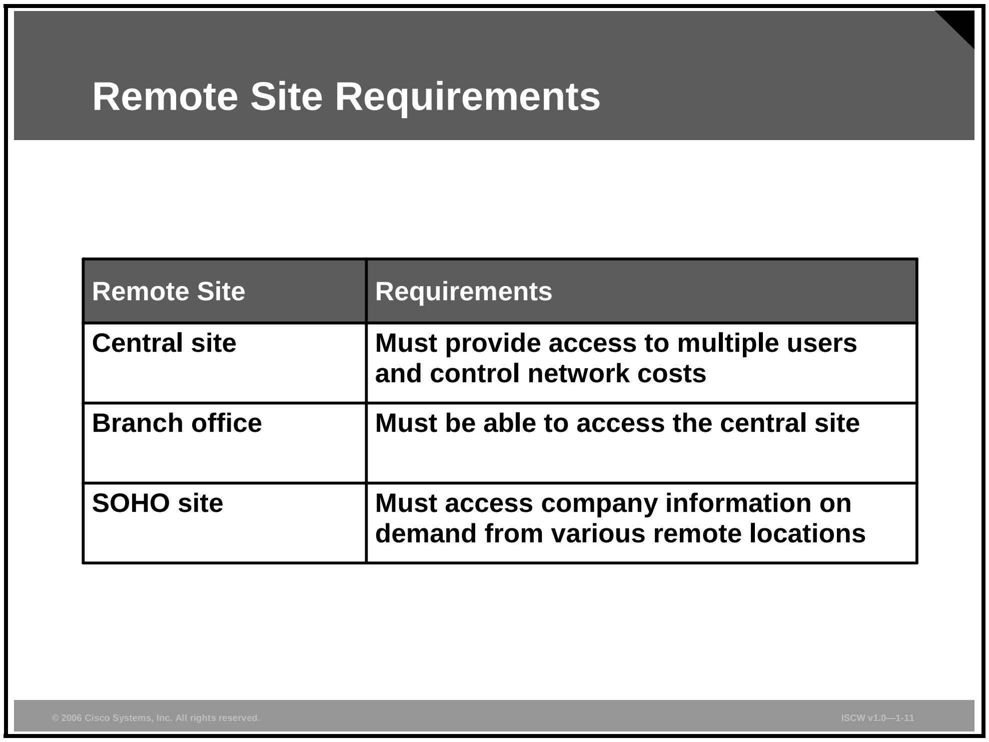
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **Cost:** Depending on the traffic types and connectivity requirements, various connectivity options are typically considered—permanent or on-demand, public and private networks, etc.
- **Access control:** To prevent unauthorized traffic, routers and firewalls use a set of rules that permit or deny certain traffic. Access control is commonly applied to router interfaces, and can be configured to control which data sessions can pass and which will fail.
- **Secure connectivity:** Remote sites and mobile workers can gain secure access to corporate intranets by using VPN solutions, such as IPsec VPN or MPLS VPN.
- **Authentication:** The remote site must be able to authenticate itself to the central site.
- **Redundancy:** In internetworking, duplicate devices, services, or connections can perform the work of original devices, services, or connections in the event of a failure. Branch offices typically require more redundancy than SOHO offices or mobile teleworkers.
- **Infrastructure availability:** Service providers may not offer certain WAN services in some regions. This consideration generally becomes more critical as sites are set up in more remote locations.

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

Remote Connection Requirements in a Converged Network

This topic describes the factors that a network administrator must evaluate for central site, branch office, and SOHO WAN connections.



Remote Site Requirements

Remote Site	Requirements
Central site	**Must provide access to multiple users and control network costs**
Branch office	**Must be able to access the central site**
SOHO site	**Must access company information on demand from various remote locations**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—1-11

A company with multiple sites that vary in size will need a remote network to connect the various locations. Typical locations include these sites:

- **Central site:** The central site is a large site that is often the corporate headquarters or a major office. Regional offices, SOHOs, and mobile workers may need to connect to the central site for data and information. Because users may access the central site via multiple WAN technologies, it is important that the central site accommodate many types of WAN connections from remote locations. The central site is often referred to as headquarters, the enterprise, or corporate.

- **Branch office:** The branch office is an office that generally accommodates employees who have a compelling reason to be located away from the central site, such as a regional sale. Branch office users must be able to connect to the central site to access company information. Branch office is sometimes called remote site, remote office, or sales office. Branch offices can benefit from high-speed Internet access, VPN connectivity to corporate intranets, telecommuting capabilities for work-at-home employees, video conferencing, and economical public switched telephone network (PSTN)-quality voice and fax calls over the managed IP networks.

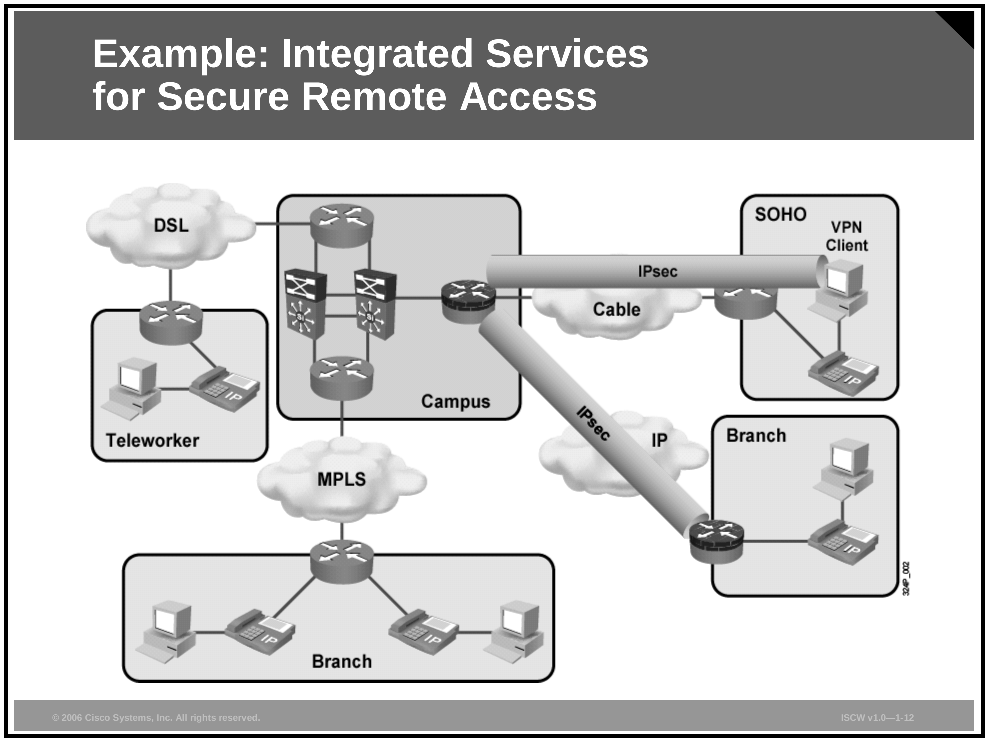
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **SOHO site:** The SOHO site, sometimes referred to as Branch of One, is a small office with one to several employees, or the home office of a telecommuter. Telecommuters may also be mobile users, that is, users who need access while traveling, or who do not work at a fixed company site. Depending on the amount of use and the WAN services available, telecommuters working from home tend to use dialup and broadband services. Mobile users tend to access the company network via an asynchronous dialup connection through the telephone company, or may access the corporate intranet using broadband Internet service and the VPN client software on their laptops. Telecommuters working from home may also use a VPN tunnel gateway router for encrypted data and voice traffic to and from the company intranet. These solutions provide simple and safe access for branch offices or SOHOs to the corporate network site, according to the needs of the users at the sites.

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

Example: Integrated Services for Secure Remote Access

The figure shows a sample converged network with integrated services. DSL and cable have been deployed as two of the advanced physical layer technologies, and MPLS VPNs and IPsec VPNs have been deployed as two of the advanced secured connectivity technologies.



Example: Integrated Services for Secure Remote Access

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—1-12

Internet access is migrating from dialup modems with slow connections to broadband access, using a variety of technologies with much faster transport speeds. The technology takes advantage of existing telephone and cable television distribution infrastructures to provide broadband access to the Internet. While there is no universal definition of broadband, the U.S. Federal Communications Commission (FCC) considers advanced telecom or high speed to be defined as 200 kbps or greater. Generally, a speed of 128 kbps is adequate for most users. Broadband can allow remote office staff and SOHO users to connect to the central site at higher data rates than are available with traditional on-demand technologies.

High-speed broadband access to the Internet through a broadband point of presence (POP) and then to corporate networks using secure VPNs is a reality for many users in the networked world today. This broadband access has the potential to directly improve employee productivity, and to provide a foundation for new voice and video business services over the Internet.

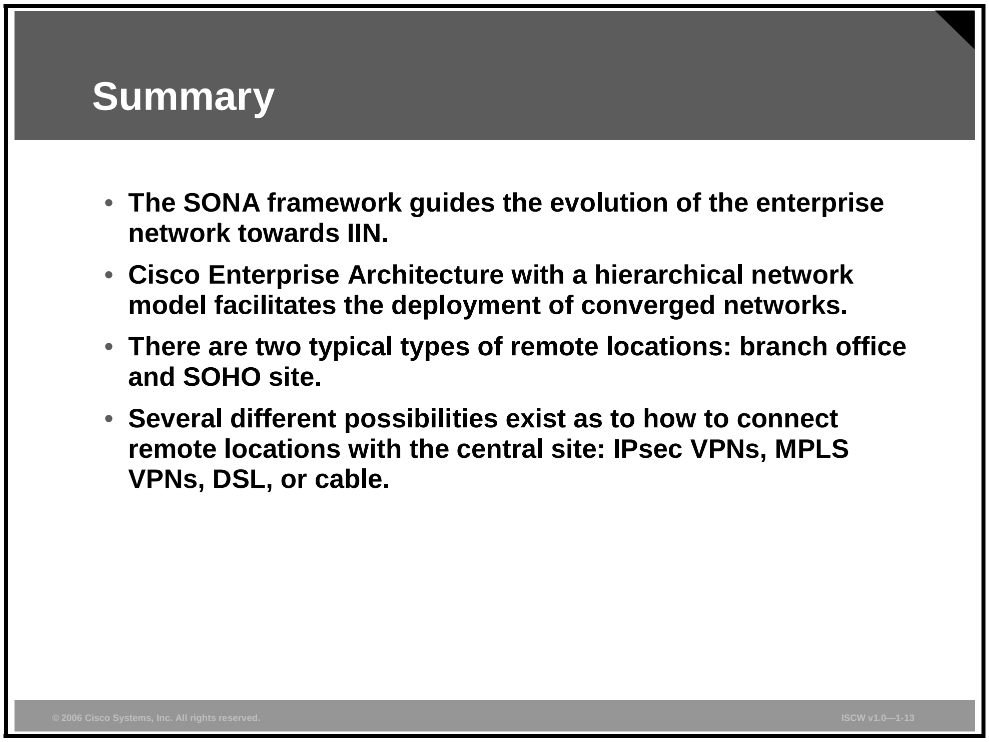
Many corporations and educational institutions have instituted broadband solutions for access by suppliers, customers, and staff. The use of the Internet for secure site-to-site connectivity using VPNs is increasing (IPsec VPN), especially for less critical traffic.

Broadband access options, in addition to the legacy dedicated circuit-switching and packet-switching technologies, include DSL and cable modems.

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

Summary

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



Summary

- The SONA framework guides the evolution of the enterprise network towards IIN.
- Cisco Enterprise Architecture with a hierarchical network model facilitates the deployment of converged networks.
- There are two typical types of remote locations: branch office and SOHO site.
- Several different possibilities exist as to how to connect remote locations with the central site: IPsec VPNs, MPLS VPNs, DSL, or cable.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—1-13

References

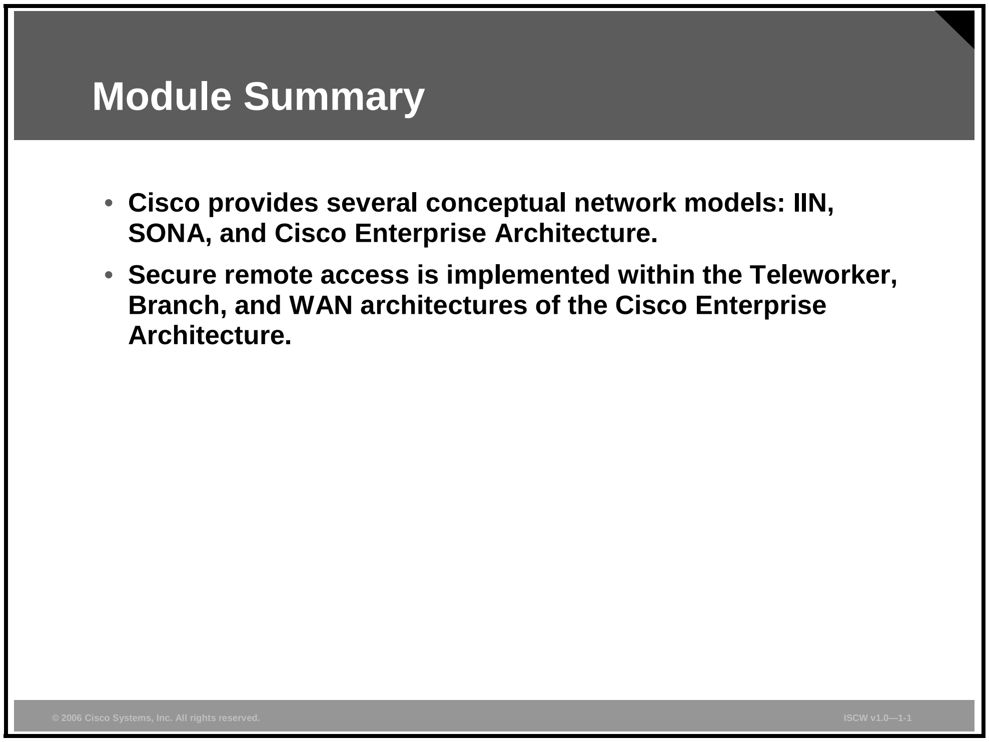
For additional information, refer to these resources:

- IIN collection of documents at http://www.cisco.com/en/US/netsol/ns650/networking_solutions_market_segment_solution.html
- SONA series of documents at http://www.cisco.com/en/US/netsol/ns629/networking_solutions_market_segment_solutions_home.html
- Enterprise Architectures collection of documents at http://www.cisco.com/en/US/netsol/ns517/networking_solutions_market_segment_solutions_home.html

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

Module Summary

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



Module Summary

- **Cisco provides several conceptual network models: IIN, SONA, and Cisco Enterprise Architecture.**
- **Secure remote access is implemented within the Teleworker, Branch, and WAN architectures of the Cisco Enterprise Architecture.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—1-1

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 self-study.

Module 2

Teleworker Connectivity

Overview

Modern companies employ people from all over the world who live too far from the main office to be able to commute to work every day. These employees need to connect to the network at the headquarters to be able to work from their home offices. There are many different ways to connect the teleworkers to the central office and still provide them both speed and security.

Module Objectives

Upon completing this module, you will be able to describe and implement teleworker broadband connectivity. This ability includes being able to meet these objectives:

- Describe the WAN, branch, and SOHO modules that represent remote connections to the enterprise network
- Describe cable technology
- Describe xDSL technologies
- Configure the PPPoE and PPPoA client over DSL
- Verify typical broadband configurations

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

Lesson 1

Describing Topologies for Facilitating Remote Connections

Overview

This lesson describes the benefits of the Enterprise Architecture framework, including building blocks and the remote connection topologies that an enterprise network has to support. The lesson also describes the challenges of connecting teleworkers, considerations to be solved, solution components, and benefits realized.

Objectives

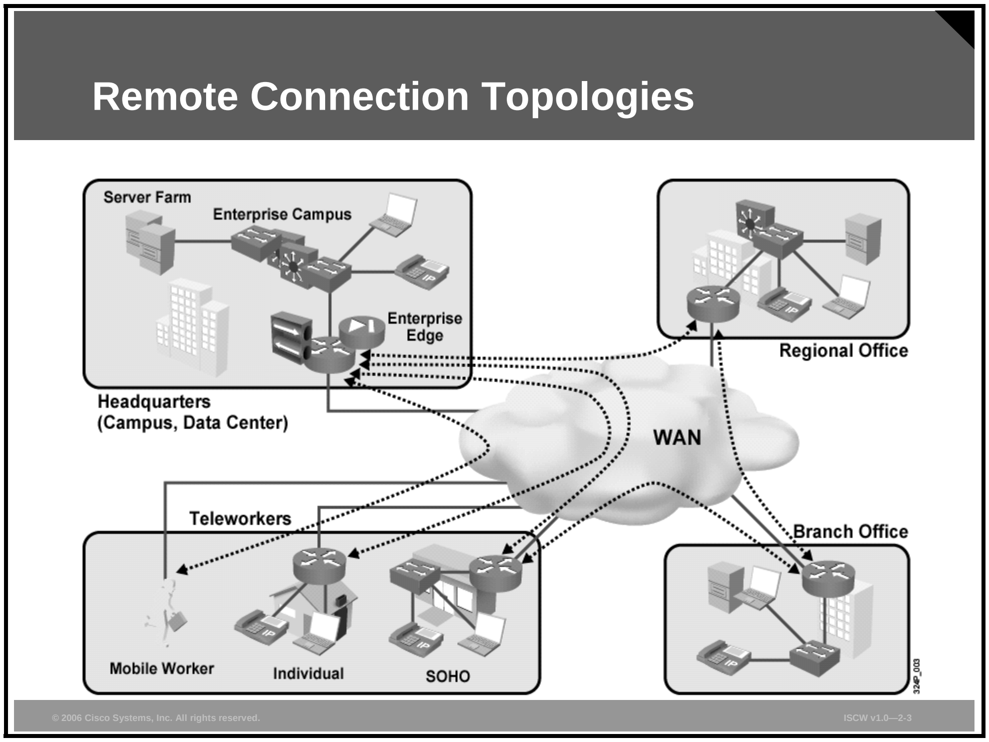
Upon completing this lesson, you will be able to describe the WAN, branch, and small office, home office (SOHO) modules that represent remote connections to the enterprise network. This ability includes being able to meet these objectives:

- Explain the typical remote connections that an enterprise network has to support
- Describe the challenges faced in connecting teleworkers to the enterprise network, and the solutions that exist to address these challenges

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

Remote Connection Topologies

This topic describes the typical remote connections that an enterprise network has to support.



Remote Connection Topologies

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-3

Enterprises require intelligent networks that help them increase application and service effectiveness, and productivity throughout the WAN. At the same time, intelligent networks make it possible to migrate disparate enterprise data, voice, and video networks to a converged, scalable, and dependable IP-based network.

Intelligent networks enable enterprises to reduce costs, because enterprises work globally and span multiple sites, including, for example, central office (CO), remote sites (regional offices and branch offices), and teleworkers (SOHO and mobile workers).

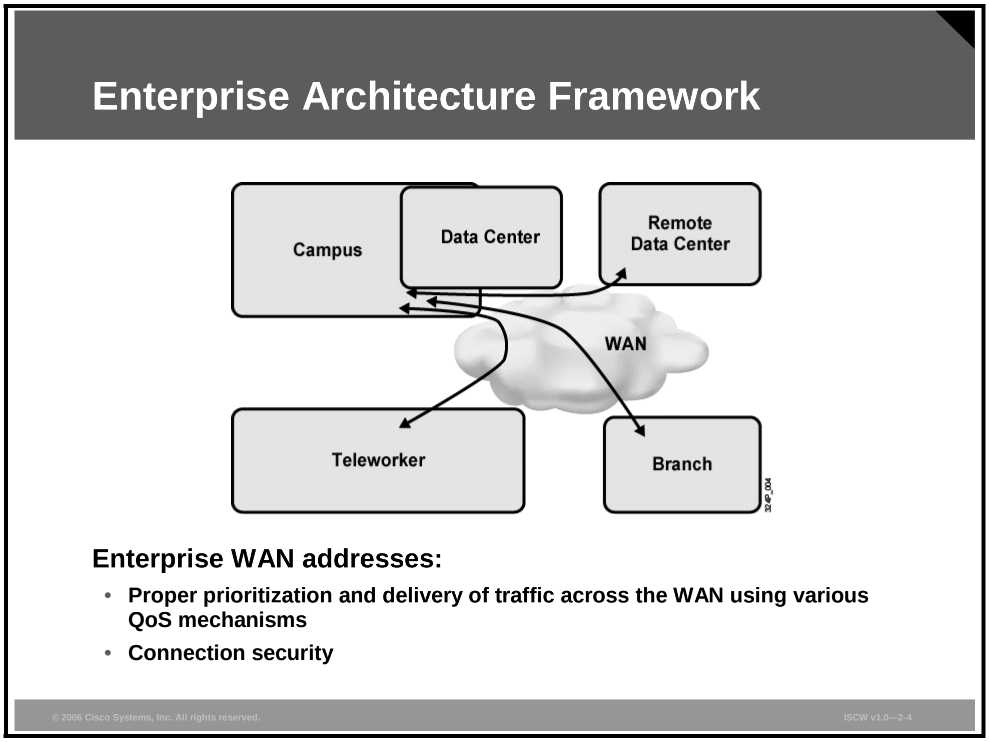
The figure illustrates various remote connection topologies that modern enterprise networks have to support. In some cases, the remote locations connect only to the headquarters (HQ), while in other cases, remote locations must connect to multiple sites (the SOHO in the figure connects both to the branch office as well as to the HQ).

The Cisco Enterprise Architecture framework provides solutions to meet all remote connectivity 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 self-study.

Enterprise Architecture Framework

The Cisco Enterprise Architecture framework addresses the building blocks of the enterprise network: campus, data center, branch, teleworker, and WAN.



Enterprise Architecture Framework

Enterprise WAN addresses:

- **Proper prioritization and delivery of traffic across the WAN using various QoS mechanisms**
- **Connection security**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-4

Each building block addresses different enterprise network requirements:

- **The WAN building block:** Used to connect the campus, data center, branch, and teleworker into an enterprise network.
- **The Enterprise Campus architecture:** Addresses the core infrastructure—intelligent switching and routing integrated with advanced security, mobility, and wireless, and other productivity-enhancing technologies such as VoIP. The integrated security features within the Cisco routers and switches provide defense against various network attacks using standard-based protocols, such as 802.1*x*, Extensible Authentication Protocol (EAP), RADIUS, and IPsec.
- **The data center architecture:** Addresses the adaptive and cohesive infrastructure to adhere to consolidation, business continuance, and security while deploying the service-oriented architectures, virtualization, and on-demand computing. Management is simplified, overhead is reduced, and IT easily provides various users (for example, departmental staff, customers, and suppliers) secure access to resources and applications. Redundant data centers are deployed providing backup, and server and application load-balancing allow maximized performance.
- **The enterprise branch architecture:** Head office applications and services (secure access to voice, mission-critical data, and video applications) are extended to a large number of remote locations and are available anywhere, anytime. The advanced services such as security, switching, network analysis, caching, voice, and video are implemented within integrated services devices, such as the Cisco integrated services routers (ISRs), and can be deployed when needed. The management, configuration, and monitoring of remote devices can be done centrally.

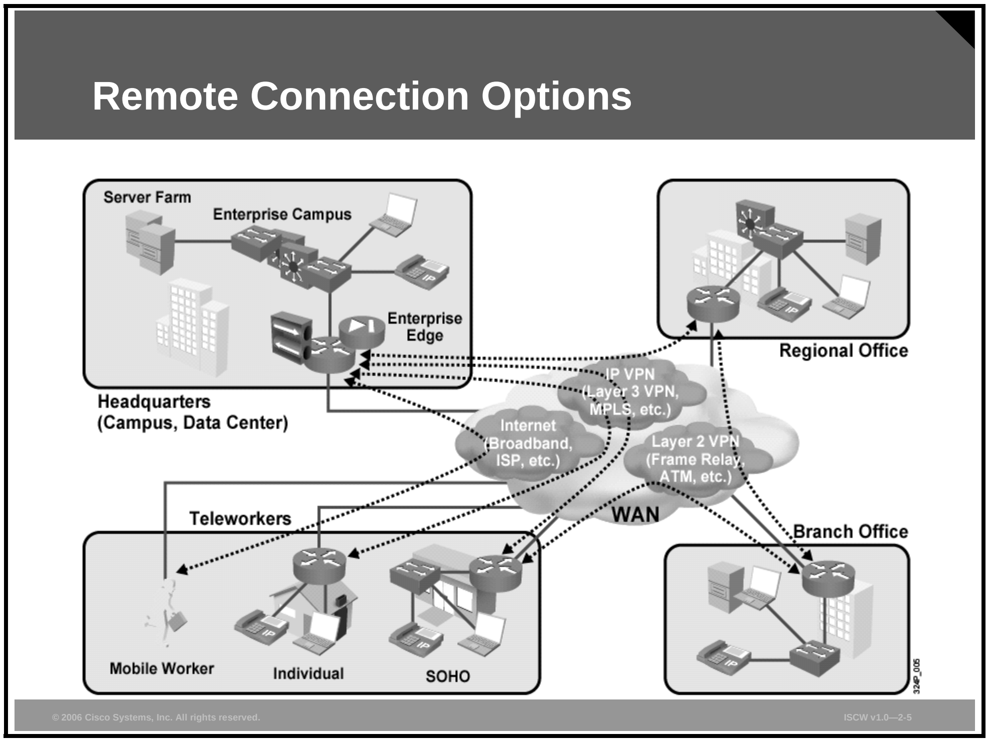
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **The enterprise teleworker architecture:** Provides secure delivery of voice and data services to remote small or home offices over broadband access service, offering employees a flexible work environment. Centralized management minimizes support overhead and costs. Integrated security allows easy extension of HQ security policies to the teleworker. The always-on virtual private network (VPN) allows employees to easily access authorized services and applications, and the addition of IP phones enhances productivity by allowing access to centralized IP Communications with voice and unified messaging.
- **The enterprise WAN architecture:** Offers voice, video, and data traffic convergence over a single IP network and addresses secure and proper delivery of corporate voice, video, and data traffic. This is achieved with the deployment of intelligent quality of service (QoS) mechanisms, granular service levels, and comprehensive encryption options. Security is provided by deploying multiservice VPNs based on Multiprotocol Label Switching (MPLS) or IPsec over Layer 2 and Layer 3 WAN technologies in hub-and-spoke, partial-mesh, or full-mesh topologies.

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

Remote Connection Options

The Cisco Enterprise Architecture framework provides the building blocks to build a secure network that supports advanced technologies, such as VoIP, over the entire enterprise network.



Remote Connection Options

Server Farm
Enterprise Campus
Enterprise Edge
Headquarters (Campus, Data Center)
Regional Office
IP VPN (Layer 3 VPN, MPLS, etc.)
Internet (Broadband, ISP, etc.)
Layer 2 VPN (Frame Relay, ATM, etc.)
WAN
Teleworkers
Branch Office
Mobile Worker
Individual
SOHO
IP
324P_005

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-5

Three of the goals of the Enterprise Architecture framework include the following:

- **Protection:** Helps the enterprise to avoid, mitigate, and rapidly recover from potentially costly business threats or disruptions by ensuring the continuous access to applications, services, and data across an entire enterprise network.
- **Lower the cost of operations:** Helps to reduce the management and operational overhead, and deployment and maintenance expenses.
- **Growth:** Allows for quick, cost-effective addition of new users, branches, applications, and services. This allows the network to scale and for business to grow to quickly accommodate emerging technologies and new products.

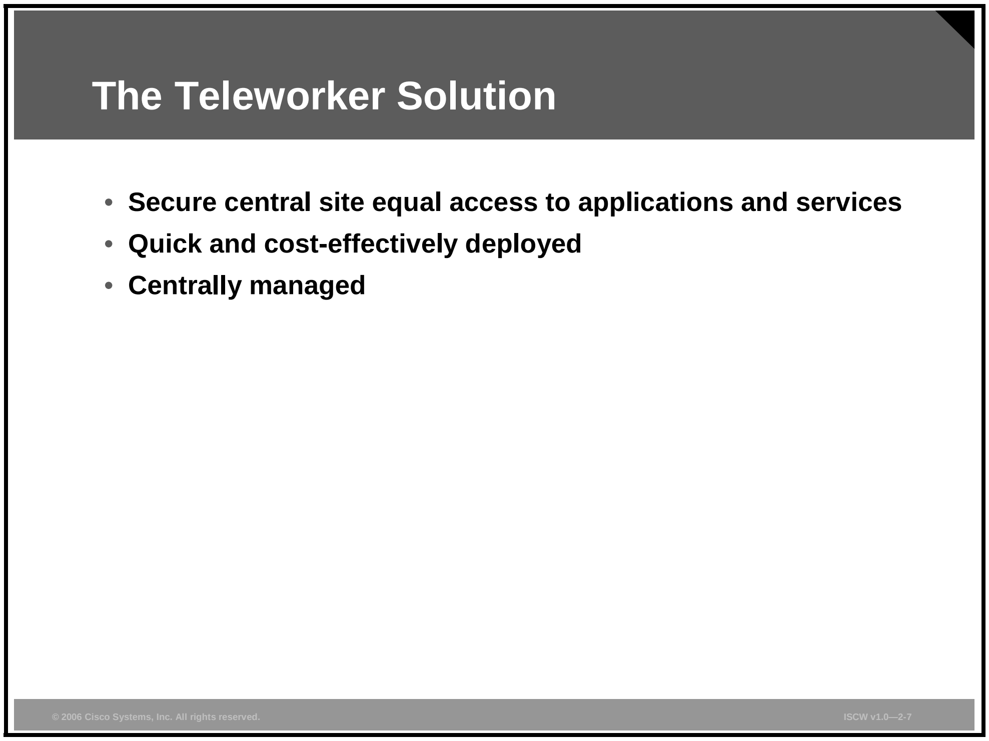
Remote connection options include the following:

- Traditional private WAN Layer 2 technologies, such as Frame Relay, ATM, and leased lines, in which the security of the connection depends on the service provider. You should use strong encryption with IPsec VPNs to strengthen security.
- Service provider MPLS-based IP VPNs offer flexible, scalable, any-to-any connectivity. The security level of the connections without additional IPsec deployment is almost the same as with traditional private WAN Layer 2 technologies.
- Site-to-site and remote access with IPsec VPNs over the public Internet offer connection security at a low cost.

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

The Challenge of Connecting the Teleworker

This topic describes the challenges of connecting the teleworker, and describes the Business-Ready Teleworker solution that addresses these challenges.



The Teleworker Solution

- Secure central site equal access to applications and services
- Quick and cost-effectively deployed
- Centrally managed

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-7

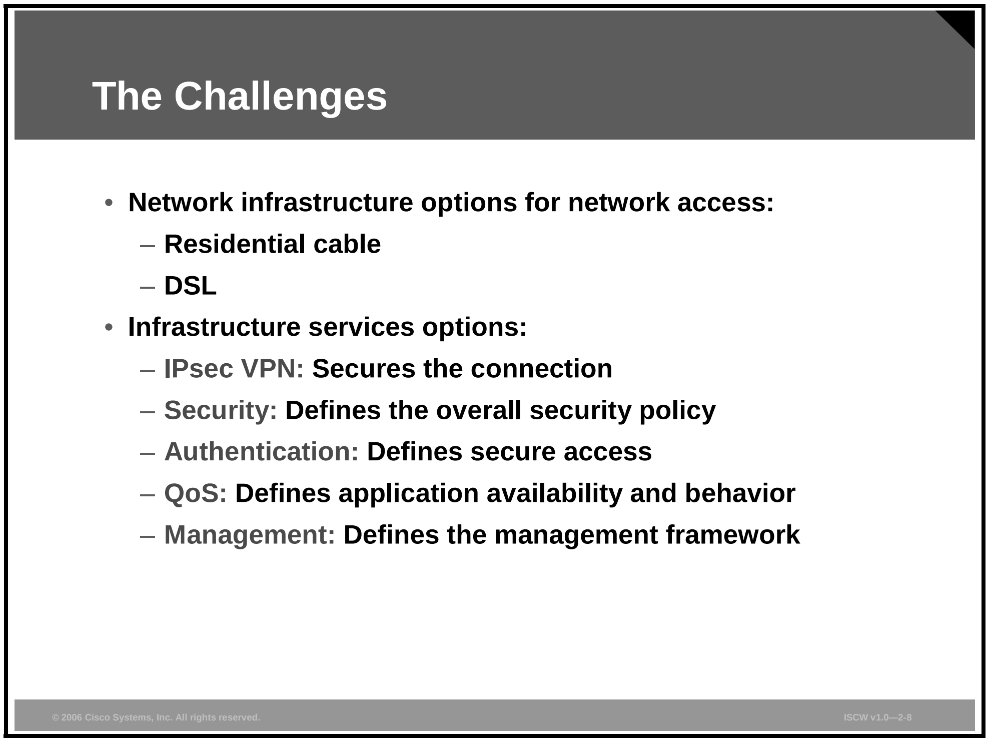
The enterprise teleworker solution provides an always-on, secure, centrally managed connection from the home of a user to the corporate network, to enable businesses to meet these requirements:

- Provide continuity of operations in case of loss of employee access to the workplace by inclement weather, commuter issues, man-made and natural disasters, and so on.
- Increase responsiveness across geographical, functional, business, and decision-making boundaries.
- Provide secure, reliable, manageable employee access to critical network assets and confidential information.
- Cost-effectively extend data, voice, video, and real-time applications over a common network connection.
- Increase employee productivity, satisfaction, and retention.

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

The Challenges

The first consideration that needs to be addressed when connecting the teleworker is the choice of a suitable access network technology.



The Challenges

- **Network infrastructure options for network access:**
  - **Residential cable**
  - **DSL**
- **Infrastructure services options:**
  - **IPsec VPN: Secures the connection**
  - **Security: Defines the overall security policy**
  - **Authentication: Defines secure access**
  - **QoS: Defines application availability and behavior**
  - **Management: Defines the management framework**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-8

The teleworker typically uses diverse applications such as e-mail, web-based applications, mission-critical applications, real-time collaboration, voice, video, and videoconferencing, many of which require a high-bandwidth connection. Therefore, the first factors to consider in a remote connectivity solution are the access network technology and the bandwidth availability.

Two possible options providing high bandwidth include residential cable and DSL. A modem dialup connection, because of its low bandwidth, is not sufficient for the teleworker solution.

A further consideration involves infrastructure services options such as the following:

- **IPsec VPN:** Establishes a secure tunnel over the existing broadband connection between the teleworker remote sites and the central site. Site-to-site VPNs are used to achieve an always-on transparent VPN connection. Remote access VPNs are used to provide an on-demand secured connection.
- **Security:** Safeguards the corporate network and prevents unguarded back doors—the security measures are achieved by deploying firewall, intrusion prevention, and URL filtering services. Depending on the enterprise corporate secure policy, split tunneling may be used to share the broadband connection between secured corporate access and unsecured Internet access at the same time.
- **Authentication:** Defines who gets access to resources—achieved by deploying the identity-based network services with authentication using authentication, authorization, and accounting (AAA) servers, 802.1X port-based access control, Cisco security, and trust agents.

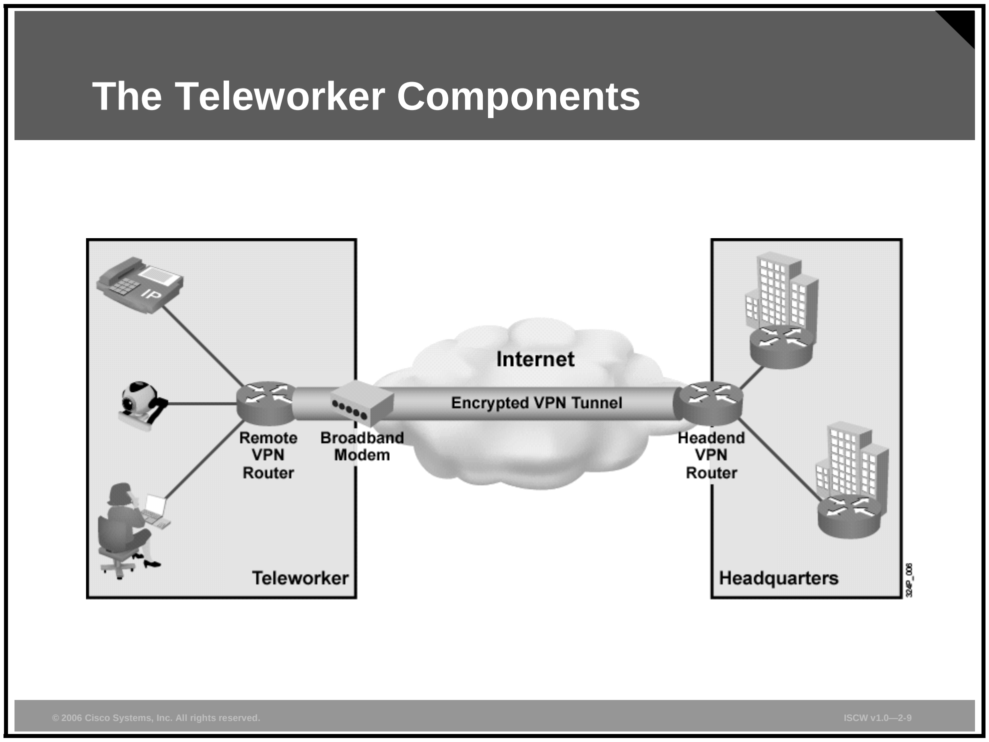
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **QoS:** Addresses the application availability and behavior—the QoS mechanisms have to be used to prioritize the traffic, optimize the use of WAN bandwidth, address the difference in uplink and downlink speed of broadband connection, and achieve adequate performance for applications sensitive to delay and jitter, such as voice and video.
- **Management:** Addresses the complexity of support and the loss of corporate control. IT centrally manages and supports the teleworker connection and equipment, and transparently configures and pushes security and other policies to the remote devices. Tools can be used to implement performance and fault management and to monitor service level agreements (SLAs).

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

The Teleworker Components

The teleworker solution is made up of three major components: home office components located at the teleworkers site, corporate components, and the optional IP telephony components.



The Teleworker Components

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-9

The required home office components are broadband access (cable or DSL), remote VPN router with QoS functionality, and laptop or desktop, while the optional components are IP phone, wireless LAN (WLAN) access point, and Cisco video telephony (VT) camera.

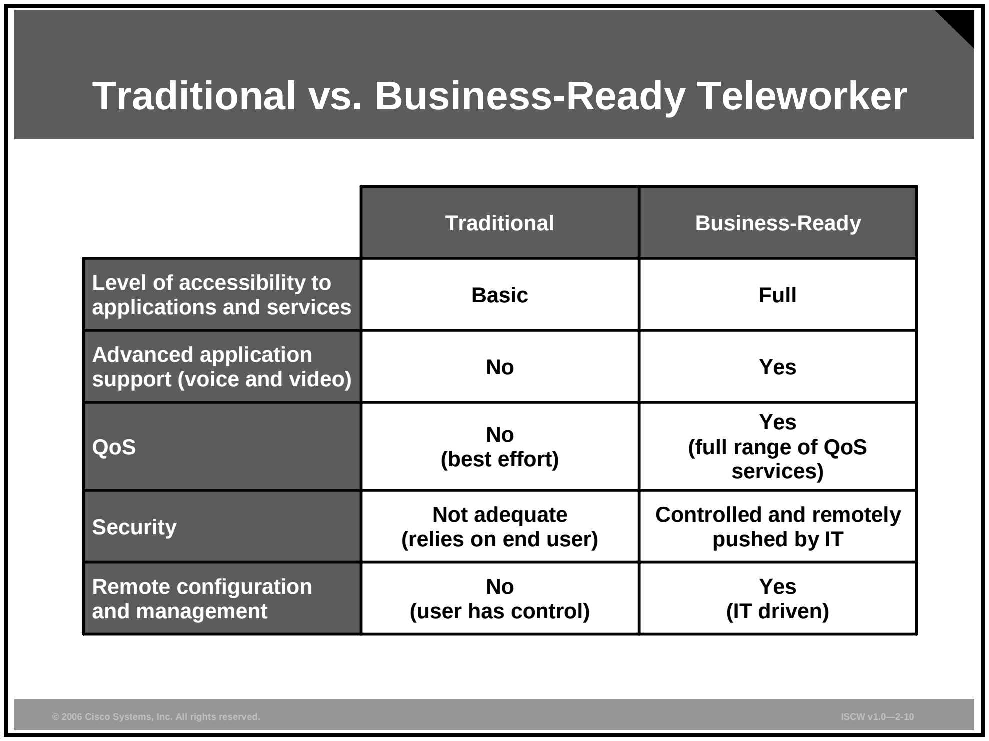
Corporate components are a VPN headend router, VPN concentrator or a multifunction security appliance such as the Cisco Adaptive Security Appliance (ASA), authentication, and central management devices for resilient aggregation and termination of the IPsec VPN tunnels.

The optional IP telephony components are Cisco Unified CallManager for call processing, signaling, and device control; voice gateway for interconnection of traditional phone networks with VoIP environment; IP phones for voice and added value services; voice messaging platform for diverse message consolidation; and Cisco Contact Center for advanced call treatment.

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

Traditional Versus Business-Ready Teleworker

The traditional teleworker solution is based on a software VPN client on the remote user laptop or desktop PC.



Traditional vs. Business-Ready Teleworker

	Traditional	Business-Ready
Level of accessibility to applications and services	Basic	Full
Advanced application support (voice and video)	No	Yes
QoS	No (best effort)	Yes (full range of QoS services)
Security	Not adequate (relies on end user)	Controlled and remotely pushed by IT
Remote configuration and management	No (user has control)	Yes (IT driven)

© 2006 Cisco Systems, Inc. All rights reserved.

The traditional teleworker solution is characterized by these drawbacks:

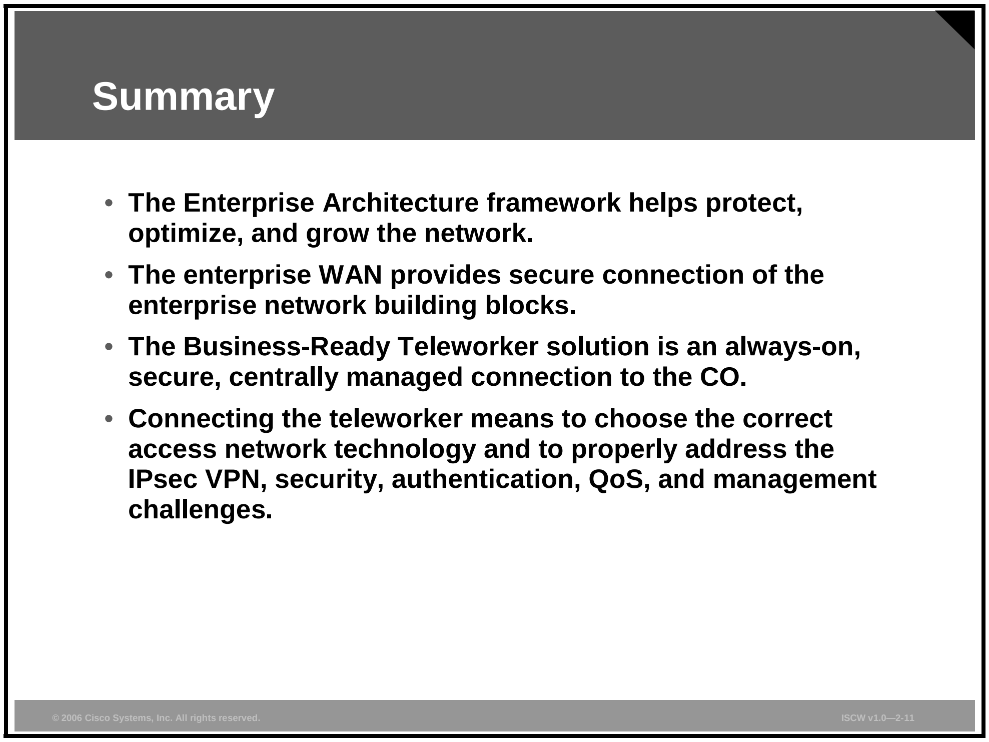
- Lower level of accessibility; for example, the inability to deploy and support advanced applications, such as voice, video, and videoconferencing
- No QoS for efficient delivery and prioritization of traffic
- Inadequate security—security relies on the end user, therefore leaving no control to IT
- Absence of controlled configuration, management, and support by IT

The Business-Ready Teleworker solution overcomes all the weak points of the traditional teleworker solution.

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

Summary

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



Summary

- The Enterprise Architecture framework helps protect, optimize, and grow the network.
- The enterprise WAN provides secure connection of the enterprise network building blocks.
- The Business-Ready Teleworker solution is an always-on, secure, centrally managed connection to the CO.
- Connecting the teleworker means to choose the correct access network technology and to properly address the IPsec VPN, security, authentication, QoS, and management challenges.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-11

References

For additional information, refer to these resources:

- The Cisco Business-Ready Teleworker solution at http://www.cisco.com/en/US/netsol/ns340/ns394/ns430/networking_solutions_package.html
- The Enterprise Architecture framework at http://www.cisco.com/en/US/netsol/ns517/networking_solutions_market_segment_solutions_home.html

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

Lesson 2

Describing Cable Technology

Overview

This lesson describes the cable network technology concepts and architecture. The lesson describes how you can deliver data services over a cable network using the hybrid fiber-coaxial (HFC) architecture. The components of the cable system are described and the cable technology terms are explained.

The lesson also describes how you can use radio frequency (RF) bands in a cable environment. The lesson concludes with the description of the process for provisioning a cable modem in a TCP/IP-based network.

Objectives

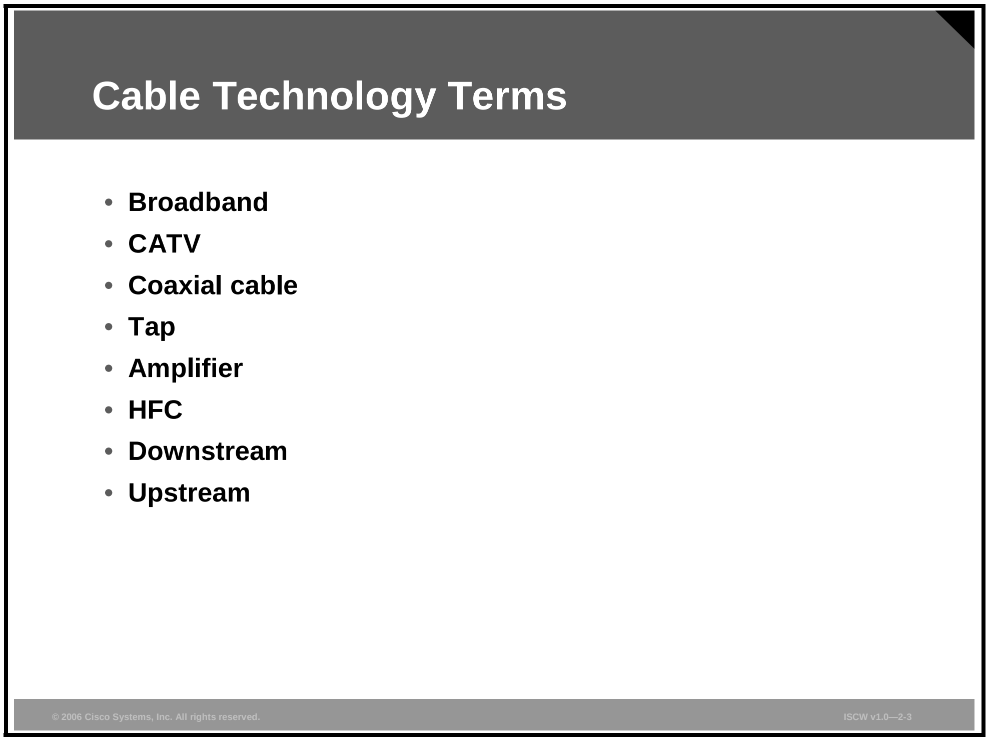
Upon completing this lesson, you will be able to describe cable technology. This ability includes being able to meet these objectives:

- Define basic terminology and standards organizations that are relevant to cable technology
- Describe the components that provide data services in a cable system
- Describe the features of cable technology
- Explain how digital cable systems use the RF bands for signal transmission
- Describe how data services can be delivered over a cable network using an HFC architecture
- Explain the combination of technologies and components that make a cable system work
- Explain the process for provisioning a cable modem in a TCP/IP-based customer 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 self-study.

Cable Technology Terms

This topic describes basic cable technology terms, standards organizations, and RF signaling terms.



Cable Technology Terms

- Broadband
- CATV
- Coaxial cable
- Tap
- Amplifier
- HFC
- Downstream
- Upstream

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-3

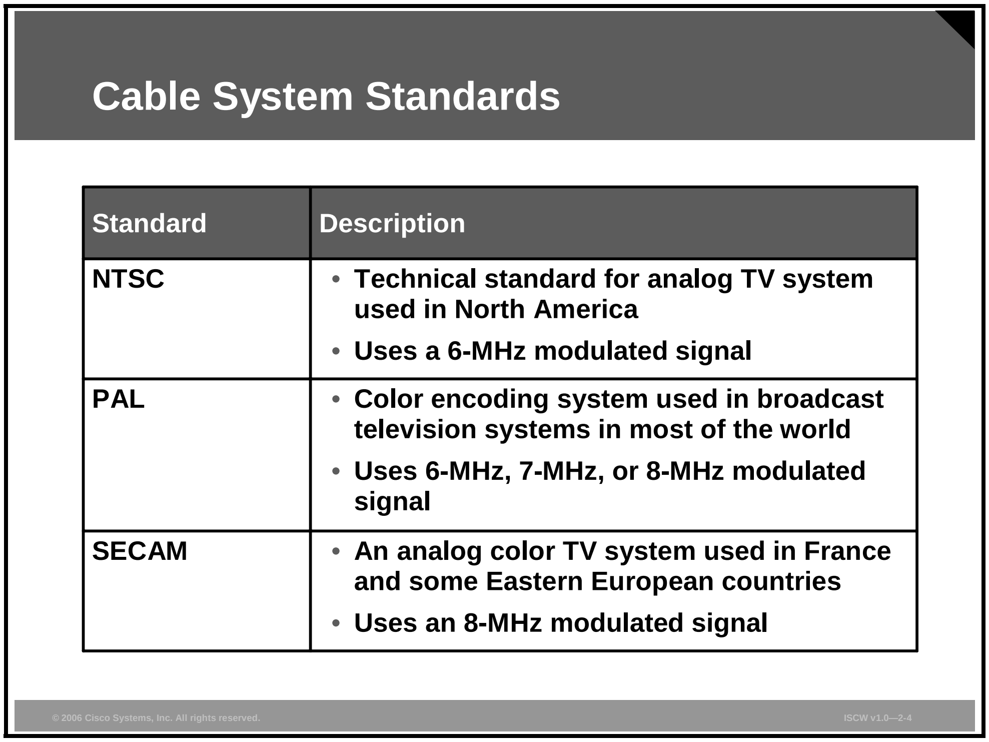
The following key terms are commonly used to describe cable technology:

- **Broadband:** Data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission. In cable systems, the term broadband refers to the frequency-division multiplexing (FDM) of many signals in a wide radio frequency (RF) bandwidth over an HFC network, and the capability to handle vast amounts of information.
- **Community Antenna Television (CATV):** The original meaning of the term CATV changed over the years, so that this term now refers to cable television.
- **Coaxial cable:** The primary medium used to build cable TV systems. Coaxial cable is used to transport RF signals and has certain physical properties that define the attenuation of the signal (cable diameter, dielectric construction, ambient temperature, operating frequency).
- **Tap:** Divides the input signal RF power to support multiple outputs. Typically, the cable operators deploy taps with 2, 4, or 8 ports—called subscriber drop connections.
- **Amplifier:** Device that magnifies an input signal and produces a significantly larger output signal.
- **Hybrid fiber-coaxial (HFC):** A mixed optical-coaxial network in which optical fiber replaces some or all of the traditional trunk portion of the cable network.
- **Downstream:** An RF signal transmission (TV channels, data) from source (headend) to the destination (subscribers). Downstream is also called a forward path.
- **Upstream:** An RF signal transmission opposite to downstream—from subscribers to the headend. Upstream is also called a return or reverse path.

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

Cable System Standards

Commonly used standards in cable systems include National Television Standards Committee (NTSC), Phase Alternating Line (PAL), and Système Electronic Couleur avec Mémoire (SECAM).



Cable System Standards

Standard	Description
NTSC	• Technical standard for analog TV system used in North America • Uses a 6-MHz modulated signal
PAL	• Color encoding system used in broadcast television systems in most of the world • Uses 6-MHz, 7-MHz, or 8-MHz modulated signal
SECAM	• An analog color TV system used in France and some Eastern European countries • Uses an 8-MHz modulated signal

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-4

NTSC is a North American TV technical standard for analog TV systems. The standard was created in 1941 and is named after the National Television System Committee formed in 1940. The standard uses a 6-MHz modulated signal.

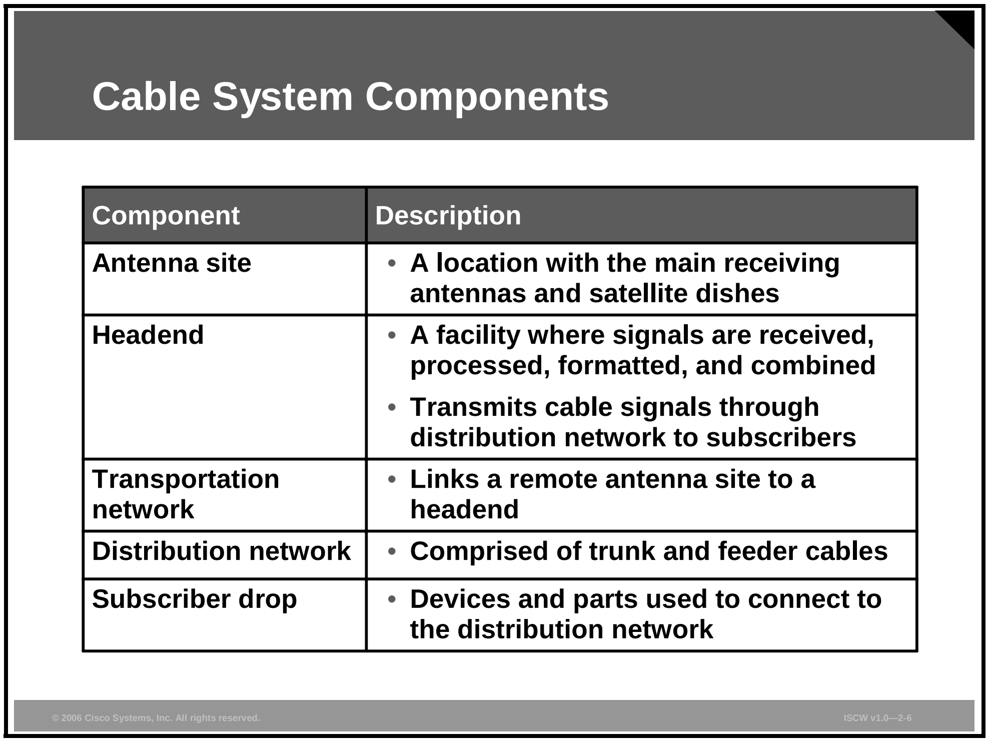
PAL is a color encoding system used in broadcast television systems in most of Europe, Asia, Africa, Australia, Brazil, and Argentina, and uses a 6-MHz, 7-MHz, or 8-MHz modulated signal. The color difference signals an alternate phase at the horizontal line rate.

SECAM is an analog color TV system used in France and certain Eastern European countries that uses an 8-MHz modulated signal.

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

Cable System Components

This topic describes the components of a cable system delivering data services.



Cable System Components

Component	Description
Antenna site	• A location with the main receiving antennas and satellite dishes
Headend	• A facility where signals are received, processed, formatted, and combined • Transmits cable signals through distribution network to subscribers
Transportation network	• Links a remote antenna site to a headend
Distribution network	• Comprised of trunk and feeder cables
Subscriber drop	• Devices and parts used to connect to the distribution network

© 2006 Cisco Systems, Inc. All rights reserved.

The cable system consists of these major components:

- **Antenna site:** An antenna site is a location chosen for optimum reception of over-the-air, satellite, and sometimes point-to-point signals. The main receiving antennas and satellite dishes are located at the antenna site.
- **Headend:** The headend is a master facility where signals are received, processed, formatted, and distributed over to the cable network—the transportation and distribution network. The headend facility is usually unmanned, under security fencing, and is somewhat similar to a telephone company central office.
- **Transportation network:** A transportation network is used to link a remote antenna site to a headend, or a remote headend to the distribution network. The transportation network can be microwave, coaxial supertrunk, or fiber-optic.
- **Distribution network:** In a classic tree-and-branch cable system, the distribution network consists of trunk and feeder cables. The trunk is the backbone that distributes signals throughout the community service area to the feeder, and typically uses 0.750-inch (19-mm) diameter coaxial cable. The feeder branches flow from a trunk and reach all of the subscribers in the service area via coaxial cables. The feeder cable is usually a 0.50-inch (13-mm) diameter coaxial cable.
  In mixed fiber and coaxial cabling (the HFC architecture), optical fiber replaces some or all of the traditional trunks, and carries TV signals and other data services. A web of fiber trunk cables connect the headend (or hub) to the nodes where optical-to-RF signal conversion is performed. Feeder cables originate from the node carrying RF signals to the subscribers. An effective range or service area of a distribution network segment (feeder segment) is from 100 to as many as 2000 subscribers.

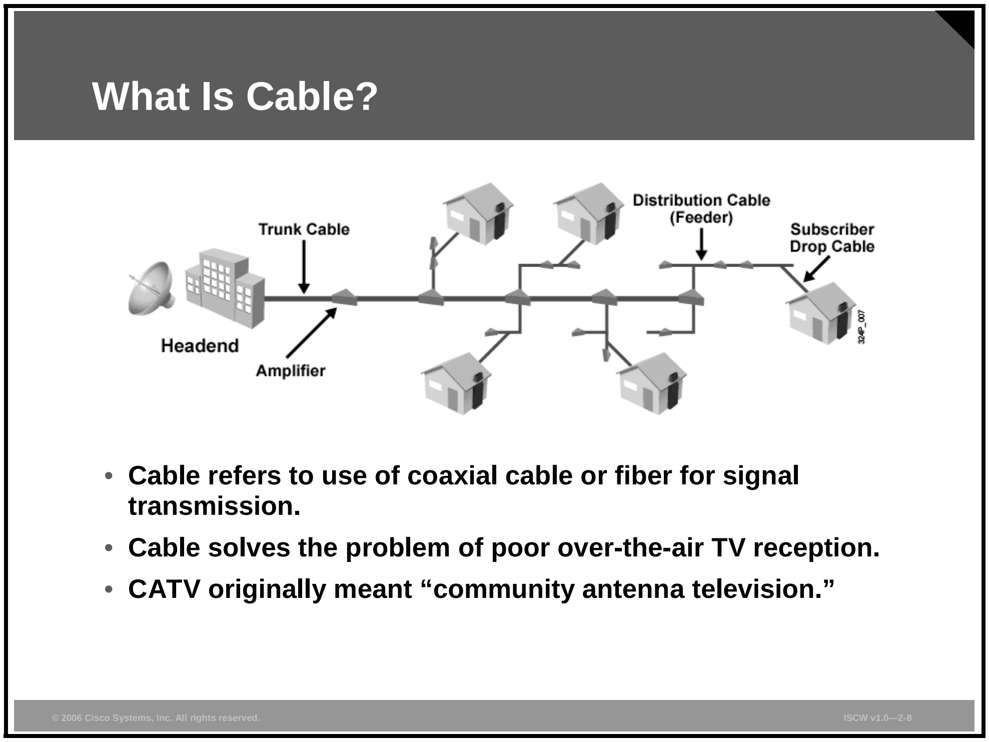
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **Subscriber drop:** A subscriber drop connects the subscriber to the cable services. The subscriber drop is a connection between the feeder part of a distribution network and the subscriber terminal device (for example, TV set, VCR, High Definition TV set-top box, or cable modem). A subscriber drop consists of coaxial cabling (usually 59-series or 6-series coaxial cable), grounding and attachment hardware, passive devices, and a set-top 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 self-study.

Cable Features

This topic describes the features of cable technology.



What Is Cable?

- **Cable refers to use of coaxial cable or fiber for signal transmission.**
- **Cable solves the problem of poor over-the-air TV reception.**
- **CATV originally meant “community antenna television.”**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-8

What is Cable?

A coaxial cable is a type of wire that consists of a center conductor surrounded by insulation, and then a grounded shield of braided wire. The shield is designed to minimize electrical and RF interference.

CATV was developed to solve the problem of poor TV reception with the over-the-air method (via radio waves), in which a television antenna is required.

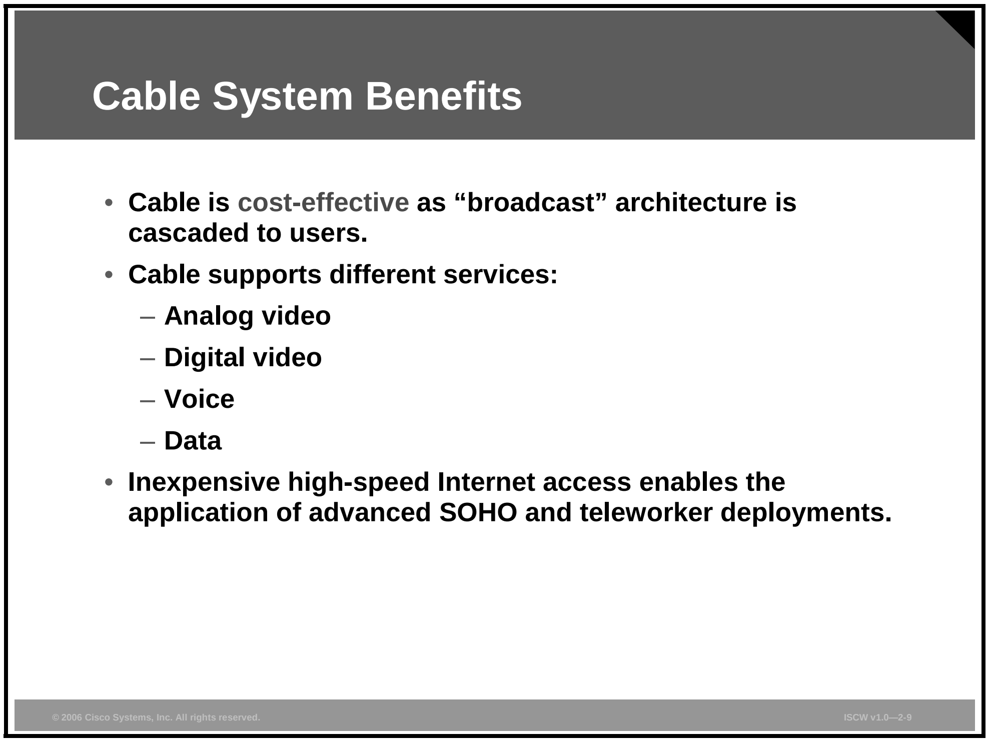
In the beginning, the typical cable TV system consisted of a shared antenna (replaced later with a satellite dish) placed in some high location, to which multiple subscribers connected their TVs via coaxial cable. The first CATV networks were one-way, consisting of various amplifiers in cascade compensating for the signal loss of the coaxial cable in series, with taps to couple video signal from the main trunks to subscriber homes via drop cables.

A CATV system provides television via RF signals transmitted within a sealed coaxial cable line. The system consists of the headend, the trunk, the neighborhood node, the distribution cables, and the subscriber drop cables.

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

Cable System Benefits

The cable system architecture provides a cost-effective solution for densely populated areas by cascading a broadcast architecture to the users.



Cable System Benefits

- **Cable is cost-effective as “broadcast” architecture is cascaded to users.**
- **Cable supports different services:**
  - **Analog video**
  - **Digital video**
  - **Voice**
  - **Data**
- **Inexpensive high-speed Internet access enables the application of advanced SOHO and teleworker deployments.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-9

The development of cable systems enabled the employment of new services—the cable system is capable of supporting telephony and data services, in addition to analog and digital video services. With the advent of high-speed data, telephony, and other similar services, larger cable operators adopted a common practice of keeping various equipment (for example, telephone switches and cable modem termination systems [CMTSs]) in the same facility, integrating all types of services—telephony, data, and analog and digital video services.

A high-speed cable data connection presents a cost-effective solution for accessing the Internet.

Small and medium-size businesses can gain the following benefits from high-speed cable Internet access:

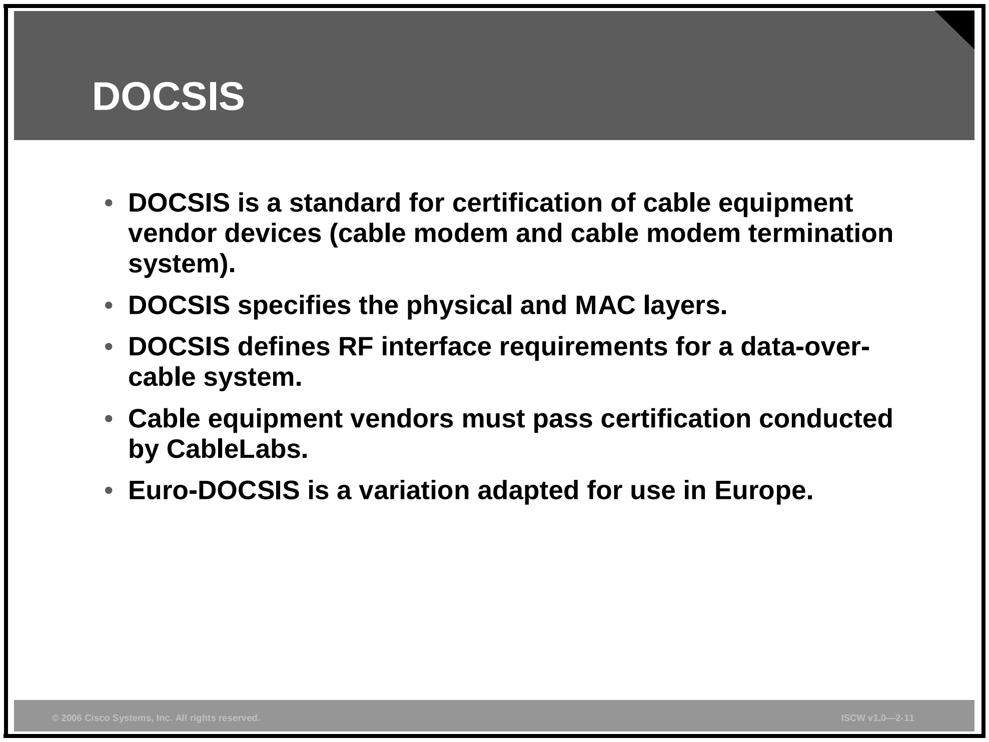
- Virtual private network (VPN) connectivity to corporate intranets
- Small office, home office (SOHO) capabilities for work-at-home employees
- Interactive television
- Public switched telephone network (PSTN)-quality voice and fax calls over the managed IP networks

Many businesses have employees working from their homes. Such employees need secure high-speed remote access to the enterprise network with the same level of accessibility as in the office, and access to the Internet for e-mail communication and use of corporate applications.

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

Digital Signals over RF Channels

This topic describes the current RF used in digital cable systems.



DOCSIS

- **DOCSIS is a standard for certification of cable equipment vendor devices (cable modem and cable modem termination system).**
- **DOCSIS specifies the physical and MAC layers.**
- **DOCSIS defines RF interface requirements for a data-over-cable system.**
- **Cable equipment vendors must pass certification conducted by CableLabs.**
- **Euro-DOCSIS is a variation adapted for use in Europe.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-11

DOCSIS

Data-Over-Cable Service Interface Specifications (DOCSIS) is an international standard developed by CableLabs, a nonprofit research and development consortium for cable-related technologies. CableLabs tests and certifies cable equipment vendor devices (cable modem [CM] and CMTS) and grants DOCSIS-certified or Qualified status.

DOCSIS defines the communications and operation support interface requirements for a data-over-cable system and permits the addition of high-speed data transfer to an existing CATV system. Cable operators employ DOCSIS to provide Internet access over their existing HFC infrastructure.

DOCSIS specifies the Open Systems Interconnection (OSI) Layers 1 and 2 requirements:

- **Physical layer:** For data signals that the cable operator can use, DOCSIS specifies the channel widths (bandwidths of each channel)—200 kHz, 400 kHz, 800 kHz, 1.6 MHz, 3.2 MHz, and 6.4 MHz. DOCSIS also specifies modulation techniques (the way to use the RF signal to convey digital data).
- **MAC layer:** Defines a deterministic access method (time-division multiple access [TDMA] or synchronous code division multiple access [S-CDMA]).

There are these three DOCSIS standards currently used, and a fourth standard under development:

- DOCSIS 1.0 was the first standard issued in March 1997, with revision 1.1 following in April 1999.
- DOCSIS 2.0 was released in January 2002, as a result of an increased demand for symmetric, real-time services such as IP telephony. DOCSIS 2.0 enhanced upstream transmission speeds and quality of service (QoS) capabilities.

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

- DOCSIS 3.0 is under development and expected to feature channel bonding—enabling the use of multiple downstream and upstream channels together at the same time by a single subscriber for increase bandwidth.

More information about DOCSIS can be found at http://www.cablemodem.com/specifications.

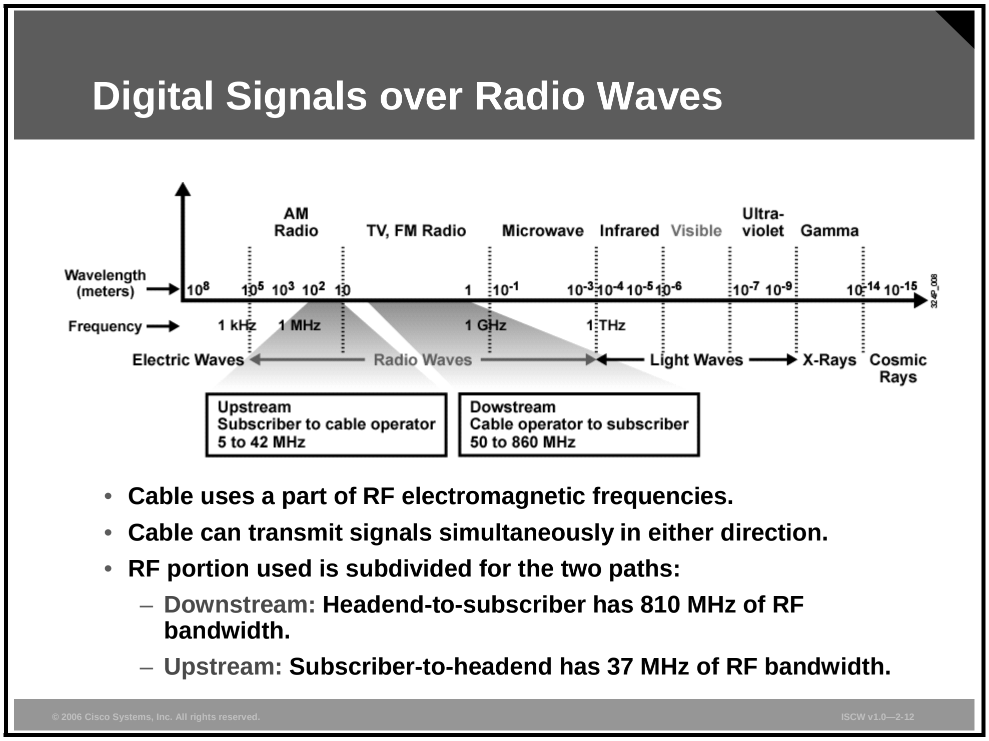
Plans for frequency allocation bands differ between U.S. and European cable systems, therefore Euro-DOCSIS was adapted for use in Europe. The main differences between DOCSIS and Euro-DOCSIS relate to differing channel bandwidths. European cable channels conform to PAL-based standards and are 7 MHz and 8 MHz wide, whereas the North American cable channels conform to the NTSC standard, which specifies 6 MHz-wide cable channels. The wider channels in Euro-DOCSIS architectures permit more bandwidth to be allocated to the downstream data path.

More information about Euro-DOCSIS can be found at http://www.euro-docsis.com.

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

Digital Signals over Radio Waves

The electromagnetic spectrum encompasses a broad range of frequencies. Frequency is the rate at which current (or voltage) cycles occur—the number of “waves” per second. Wavelength is the speed of propagation of the electromagnetic signal divided by its frequency in cycles per second. Radio waves, generally called RF, constitute a portion of the electromagnetic spectrum between approximately 5 MHz and 1 GHz.



Digital Signals over Radio Waves

Upstream
Subscriber to cable operator
5 to 42 MHz

Dowstream
Cable operator to subscriber
50 to 860 MHz

- **Cable uses a part of RF electromagnetic frequencies.**
- **Cable can transmit signals simultaneously in either direction.**
- **RF portion used is subdivided for the two paths:**
  – Downstream: **Headend-to-subscriber has 810 MHz of RF bandwidth.**
  – Upstream: **Subscriber-to-headend has 37 MHz of RF bandwidth.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-12

When you tune a radio or TV set across the RF spectrum to find different radio stations or TV channels, the radio or TV is tuned to different electromagnetic frequencies across that RF spectrum. The same principle applies to the cable system.

The cable TV industry uses the RF portion of the electromagnetic spectrum. Within the cable, different frequencies are used to carry TV channels and data. At the subscriber end, equipment such as TVs, VCRs, and High Definition TV set-top boxes tune to certain frequencies that allow you to view the TV channel or, using a cable modem, to receive high-speed Internet access.

A cable network is capable of transmitting signals on the cable in either direction at the same time. The following frequency scope is used:

- **Downstream:** Transmitting the signals from the cable operator to the subscriber, the outgoing frequencies are in the 50-to-860 MHz range.
- **Upstream:** Transmitting the signals in the reverse path from the subscriber to the cable operator, the incoming frequencies are in the 5-to-42 MHz range.

The downstream frequency range is subdivided into smaller channels as defined by the frequency plan (6 MHz for DOCSIS, 7 MHz and 8 MHz for Euro-DOCSIS). Between the upstream and downstream frequency ranges, a guard band exists. The guard band is required because of the cutoff characteristics of the high-pass and low-pass filtering. The filtering is needed to ensure that the signal does not spill into the adjacent spectrum.

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

In the over-the-air TV broadcast environment, a very-high frequency (VHF) range covering 30-to-300 MHz and an ultra-high frequency (UHF) range covering 300-to-3000 MHz are defined. The cable industry defines the cable TV spectrum for the downstream path as follows:

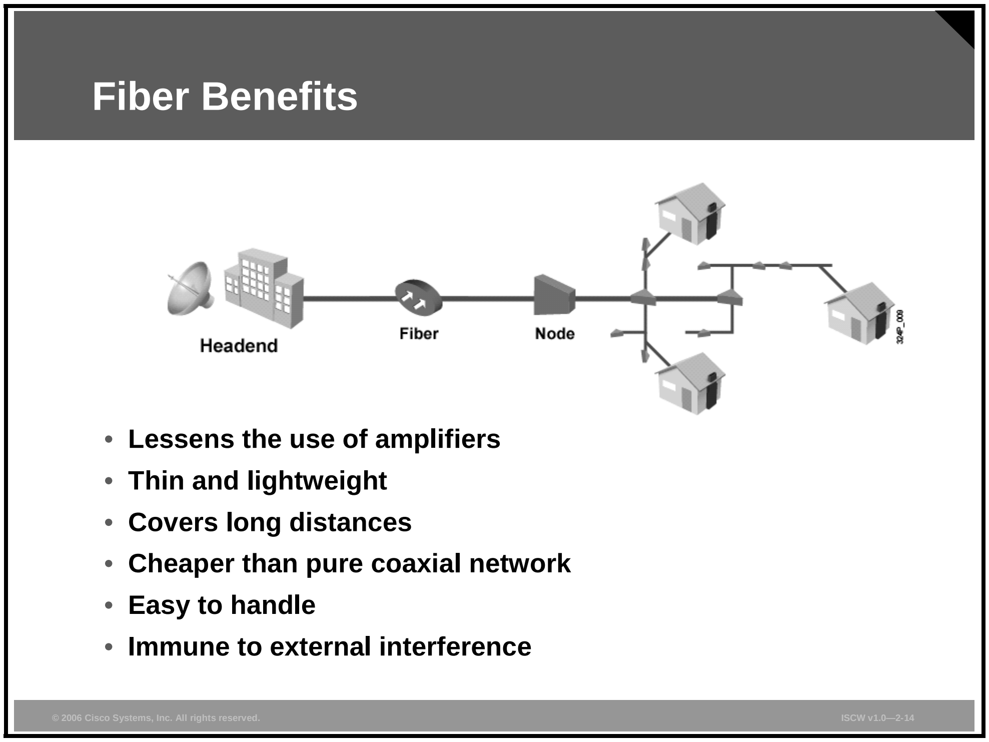
- VHF low band (TV channels 2 through 6)
- VHF midband (TV channels 98, 99, and 14 through 22)
- VHF high band (TV channels 7 through 13)
- VHF superband (TV channels 23 through 36)
- VHF hyperband (TV channels 37 and higher)

There is no frequency plan for the upstream path. The cable operator can monitor the frequency band of the upstream, and place the upstream data signals into clean areas where there is no interference from noise and other signals. The area between 5 and 15 MHz is usually noisy and unusable.

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

Data over Cable

This topic describes how data services can be delivered over an HFC architecture.



Fiber Benefits

- Lessens the use of amplifiers
- Thin and lightweight
- Covers long distances
- Cheaper than pure coaxial network
- Easy to handle
- Immune to external interference

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-14

Fiber Benefits

The signal from the antenna is reduced when traveling along the cable. In order to boost the signal, amplifiers are placed approximately every 2000 feet to ensure that all RF signals are delivered to the user, with enough power to receive all channels within the spectrum (50 to 860 MHz) for analog TV, digital TV, and digital data cable modem services. In a 20-mile plant, approximately 52 amplifiers would be used. However, the amplifiers have limitations—they introduce noise and distortion, and failure of a single amplifier results in disrupted service.

Fiber is used to lessen the number of cable amplifiers throughout the cable plant, and has several benefits over regular coaxial cable:

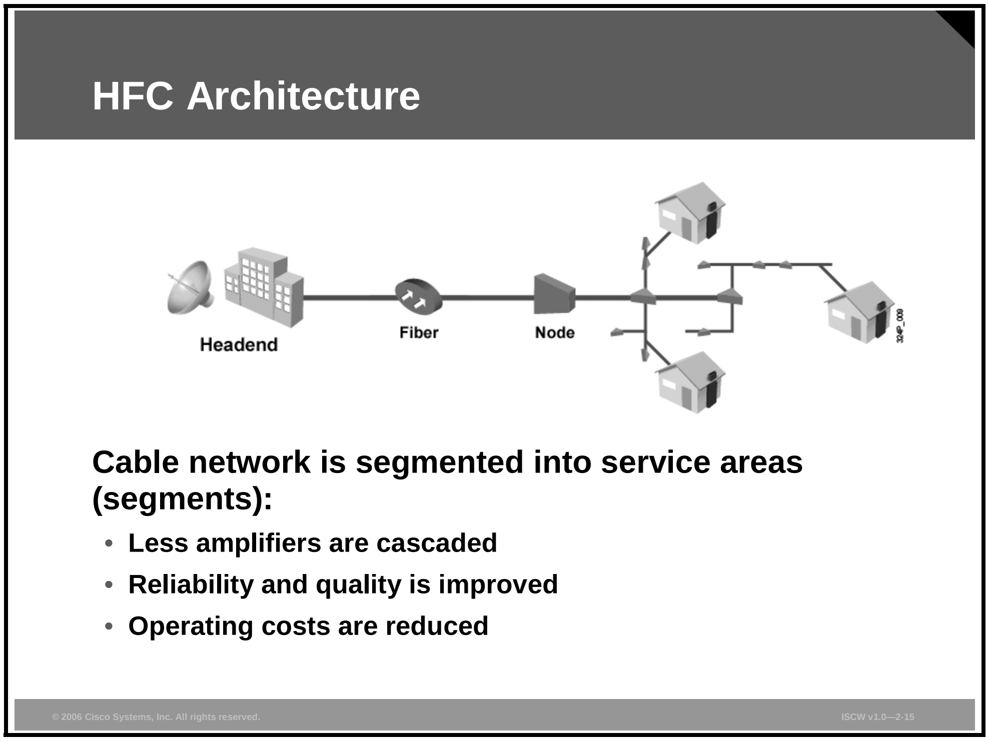
- Thin and lightweight—takes less space
- Covers longer distances
- Induces less or virtually no noise
- Less loss of signal
- Less expensive because fewer amplifiers are required
- Immune to external influences, such as thunder or RF interference
- Easier to handle

Fiber is used in the cable system for trunk cables, which carry downstream traffic from the headend to the neighborhood node, at a signal strength above 50 decibels (dB).

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

HFC Architecture

The HFC architecture is the evolution of an initial cable system and signifies a network that incorporates both optical fiber along with coaxial cable to create a broadband network. By upgrading a cable plant to an HFC architecture, you can deploy a data network over an HFC system to offer high-speed Internet services and you can serve more subscribers. The cable network is segmented into smaller service areas in which fewer amplifiers are cascaded after each optical node—typically five or fewer. The tree-and-branch network architecture for HFC can be a fiber backbone, cable area network, superdistribution, fiber to the feeder, or a ring.



HFC Architecture

Cable network is segmented into service areas (segments):

- **Less amplifiers are cascaded**
- **Reliability and quality is improved**
- **Operating costs are reduced**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-15

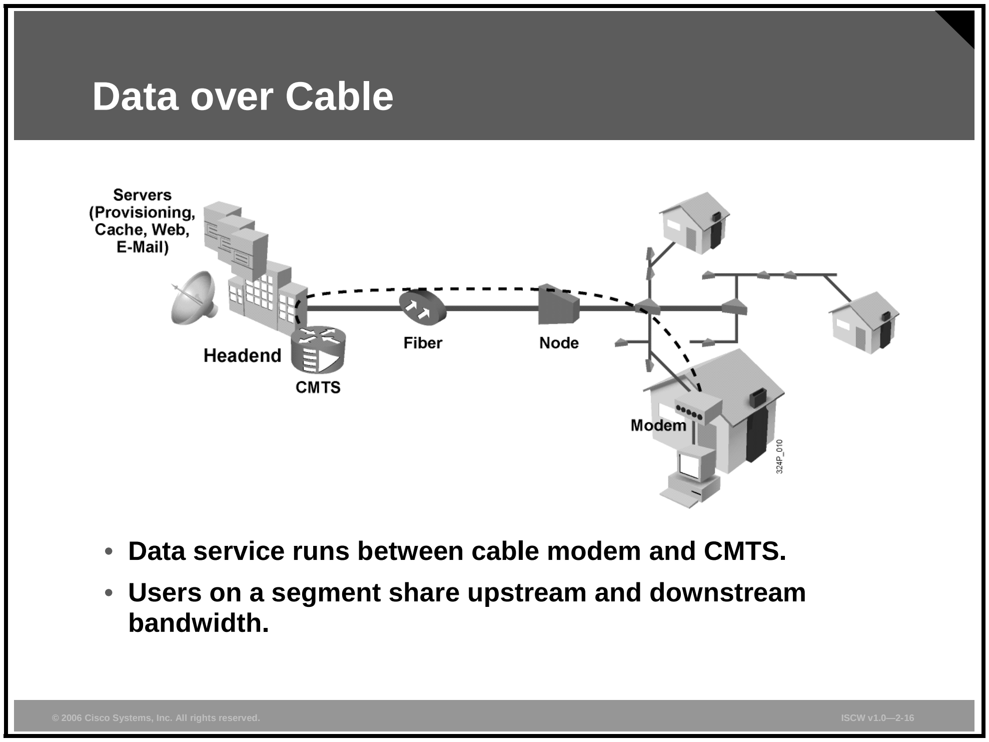
Delivering services over a cable network requires different RF frequencies—the outgoing frequencies are in the 50-to-860 MHz range, the incoming are in the 5-to-42 MHz range. To deliver data services over a cable network TV channels which usually operate at 6 MHz range for the downstream, and 6 MHz or less (for asymmetric cable connections) for upstream traffic from the corresponding frequency range are usually 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 self-study.

Data over Cable

To put upstream and downstream data on a cable system that is to send and receive digital modem signals, two types of equipment are required:

- A CM on the subscriber end
- A CMTS at the headend of the cable operator



Data over Cable

- Data service runs between cable modem and CMTS.
- Users on a segment share upstream and downstream bandwidth.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-16

A headend CMTS communicates with cable modems located in subscriber homes. In addition, a headend incorporates a computer system with databases for providing Internet services to cable subscribers.

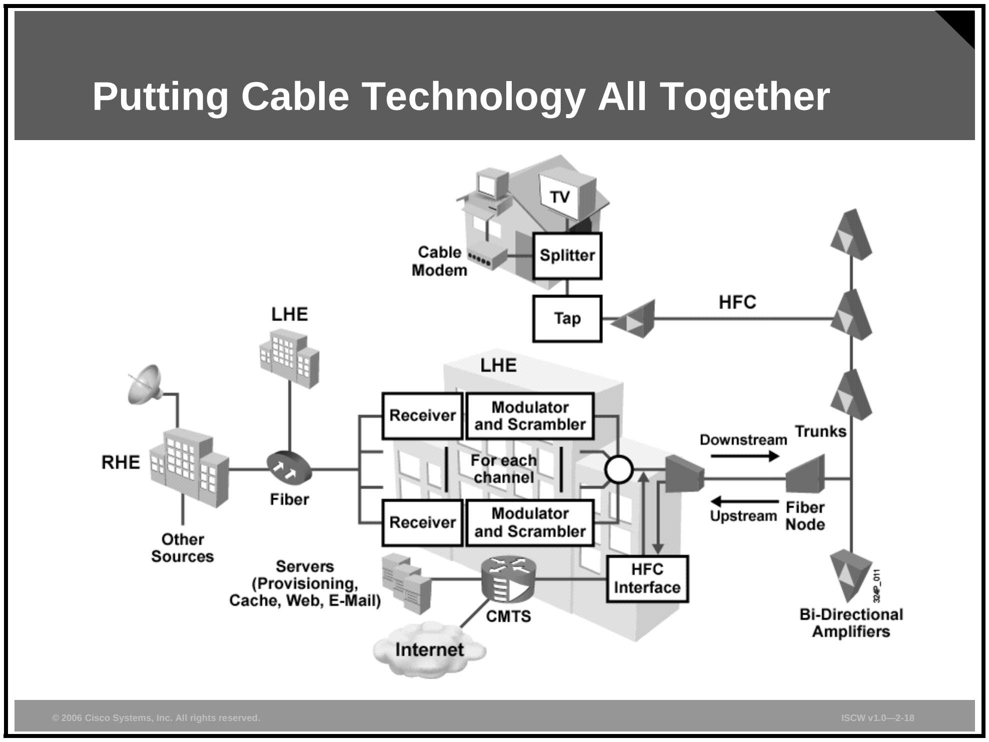
In a modern HFC network, typically 500 to 2000 active data subscribers are connected to a certain cable network segment, all sharing the upstream and downstream bandwidth. The actual bandwidth for Internet service over a CATV line can be up to 27 Mbps on the download path to the subscriber, and about 2.5 Mbps of bandwidth on the upload path. Considering the cable network architecture, cable operator provisioning practices, and traffic load, an individual subscriber can typically reach an access speed of between 256 kbps and 6 Mbps.

When high usage causes congestion, a cable operator has the flexibility to add additional bandwidth for data services. This is achieved by allocating an additional TV channel for high-speed data, thus doubling the downstream bandwidth available to subscribers. Another option for increasing the amount of bandwidth available to subscribers is to reduce the number of subscribers who are served by each network segment. To do that, the cable network is further subdivided by laying the fiber-optic connections closer and deeper into the neighborhoods.

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

Cable Technology: Putting It All Together

This topic describes the use of the various cable components and their technological issues.



Putting Cable Technology All Together

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-18

The figure shows how the different cable technologies work together. Video and data are delivered to subscribers through the cable system.

In the downstream path, the local headend, which distributes TV signals to subscribers via the distribution network, receives the TV signals through satellite dishes, antennas, analog and digital video servers, local programming, and other headends. The CMTS performs modulation of the digital data into an RF signal. At the headend, the signals are combined onto a coaxial cable and then passed to the fiber transmitter. The fiber transmitter performs a signal conversion from RF to light (optical) and sends the signals to a fiber node located in the town or neighborhood. Further down the distribution network, at the fiber node, a conversion from light (optical) back to an RF signal is performed, and the RF signal is passed via the coaxial network comprised of amplifiers, taps, and drops.

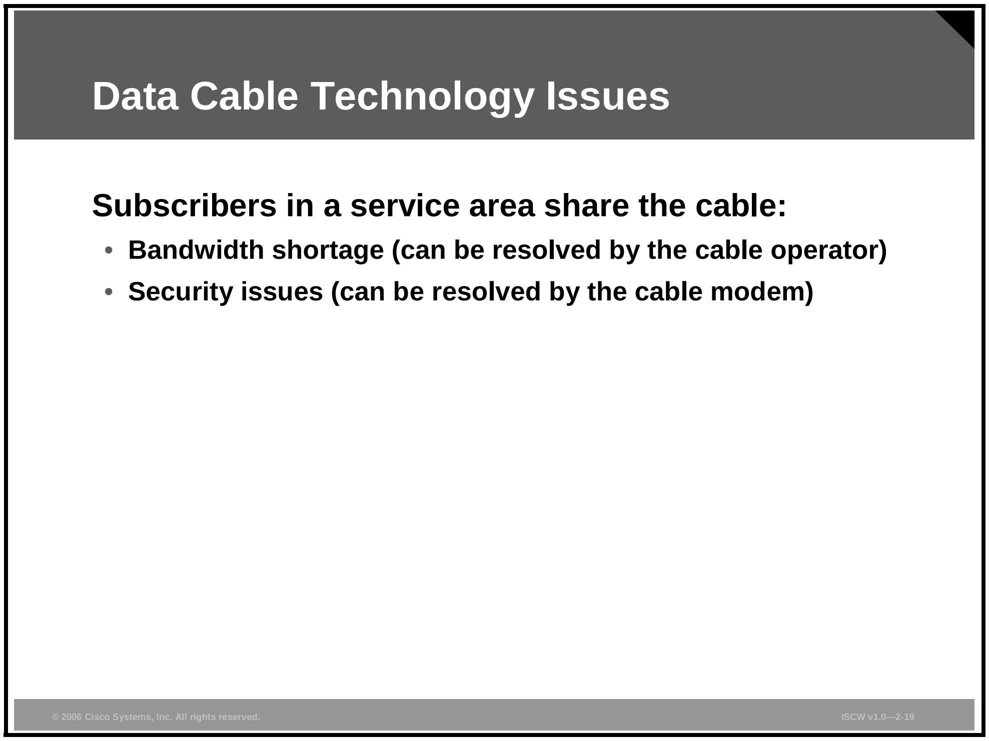
At the subscriber end, an RF splitter divides the combined RF signal into video and data portions. The data portion of the RF signal is received by the cable modem. The cable modem, tuned to the data RF signal channels, demodulates the data RF signal back into digital data, and finally passes it to the computer over an Ethernet connection.

In the upstream direction, the cable modem modulates the digital data from the computer over an Ethernet connection to the data RF signal, and then transmits it at a certain RF and power level. At the headend, the CMTS, tuned to the data RF channels, demodulates the data RF signal back to digital data and routes it to the Internet.

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

Data Cable Technology Issues

The data cable technology issues relate to the fact that subscribers in a certain service area share a coaxial cable line.



Data Cable Technology Issues

Subscribers in a service area share the cable:

- **Bandwidth shortage (can be resolved by the cable operator)**
- **Security issues (can be resolved by the cable modem)**

© 2006 Cisco Systems, Inc. All rights reserved.

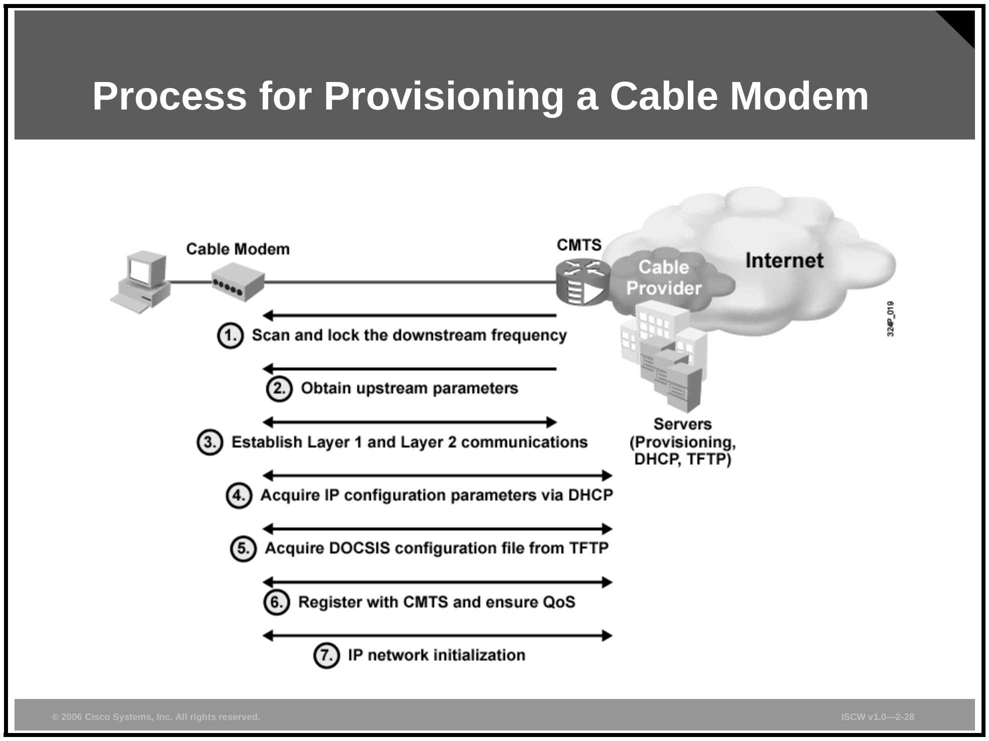
A shared coaxial cable line has these consequences:

- Bandwidth available to a subscriber may vary based on how many subscribers use the service at the same time. The cable operator can resolve this issue by adding RF channels and splitting the service area into multiple smaller areas.
- There is a risk of privacy loss. This can be addressed by encryption and other privacy features specified in the DOCSIS standard used by most cable modems.

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

Provisioning a Cable Modem

This topic describes the steps that provision a cable modem to work in a SOHO of a subscriber using TCP/IP.



Process for Provisioning a Cable Modem

1. Scan and lock the downstream frequency
2. Obtain upstream parameters
3. Establish Layer 1 and Layer 2 communications
4. Acquire IP configuration parameters via DHCP
5. Acquire DOCSIS configuration file from TFTP
6. Register with CMTS and ensure QoS
7. IP network initialization

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-28

The process of provisioning a cable modem to operate with a host system for Internet services consists of several steps. The headend where CMTS is located must have operational provisioning servers, such as DHCP and TFTP servers.

The steps in the initialization and registration are defined by the DOCSIS, and the cable modems are designed and coded to undertake these steps:

Step 1 **Downstream setup:** When the cable modem is powered up, it has to scan and lock the downstream path for the appropriate RF data channel (frequency) for the physical and data link layers to be established.

Step 2 **Upstream setup:** The cable modem listens to the management messages received through the downstream path. The messages include the information on how, where, and when to communicate in the upstream path, and are used to establish the upstream physical and data link layers.

Step 3 **Layer 1 and 2 establishment:** The cable modem communicates with CMTS to establish physical and data link layers.

Step 4 **Obtaining IP address:** After establishing Layer 1 and Layer 2 connectivity with the CMTS, the cable modem requests IP configuration parameter information (IP address, default gateway, and TFTP server) from the DHCP 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 self-study.

Step 5 **Getting the DOCSIS configuration:** Next, the cable modem requests a DOCSIS configuration file from the TFTP server. A DOCSIS configuration file is an ASCII file created by special DOCSIS editors and includes settings, such as downstream channel identification, class of service (CoS) settings, baseline privacy settings, general operational settings, network management information, and vendor-specific settings.

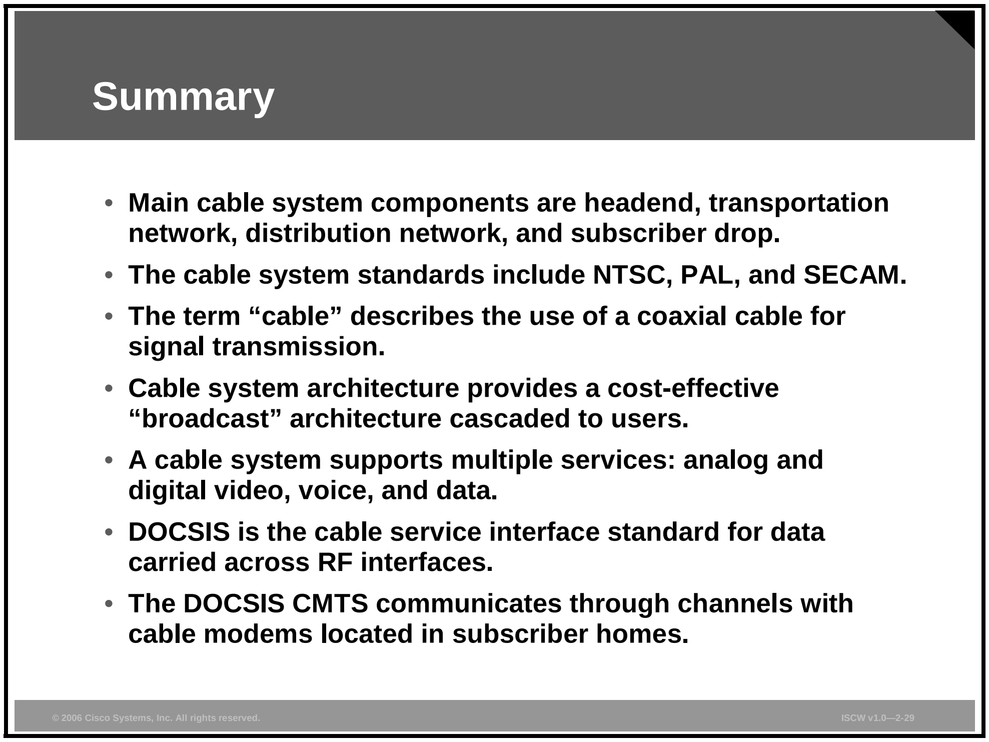
Step 6 **Register QoS with CMTS:** The cable modem registers, negotiates, and ensures QoS settings with the CMTS.

Step 7 **IP network initialization:** When the cable modem initialization and registration is complete, the PC-based network initialization is performed—the PC requests its own IP configuration parameters from the DHCP server. If multiple PC connections behind the cable modem are required, a router can be used. A common scenario is for the router to obtain a public IP address from the DHCP server of the cable provider. The home router also performs Network Address Translation (NAT) and Port Address Translation (PAT) and serves as a DHCP server for the PCs connected behind 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 self-study.

Summary

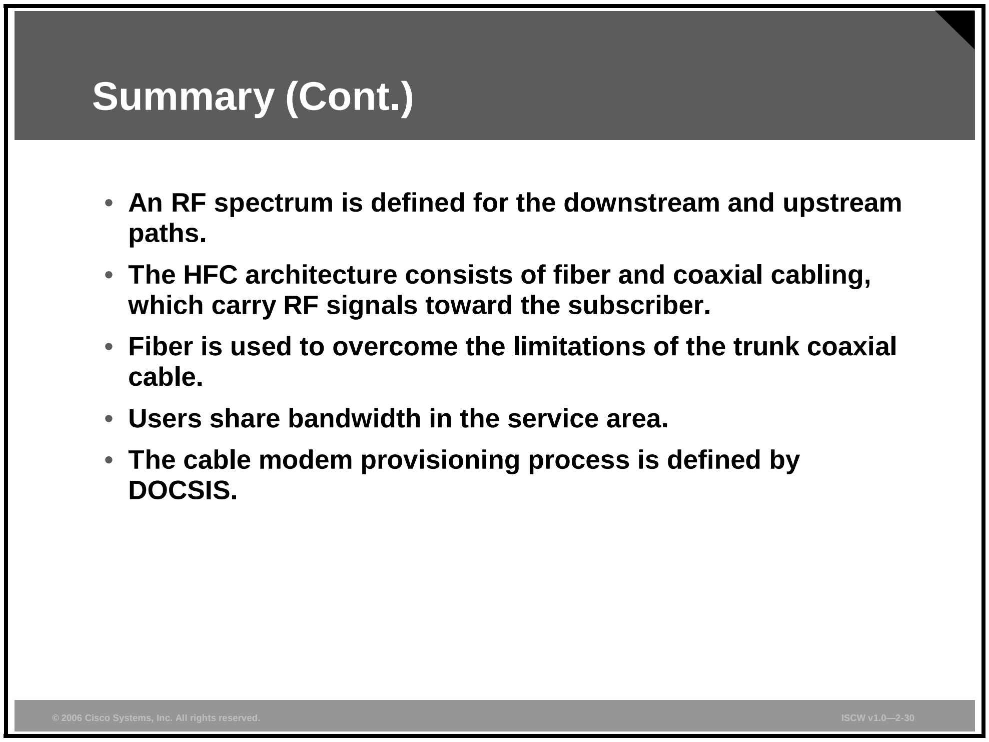
This topic summarizes the key points that were discussed in this lesson.



Summary

- Main cable system components are headend, transportation network, distribution network, and subscriber drop.
- The cable system standards include NTSC, PAL, and SECAM.
- The term “cable” describes the use of a coaxial cable for signal transmission.
- Cable system architecture provides a cost-effective “broadcast” architecture cascaded to users.
- A cable system supports multiple services: analog and digital video, voice, and data.
- DOCSIS is the cable service interface standard for data carried across RF interfaces.
- The DOCSIS CMTS communicates through channels with cable modems located in subscriber homes.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-29



Summary (Cont.)

- An RF spectrum is defined for the downstream and upstream paths.
- The HFC architecture consists of fiber and coaxial cabling, which carry RF signals toward the subscriber.
- Fiber is used to overcome the limitations of the trunk coaxial cable.
- Users share bandwidth in the service area.
- The cable modem provisioning process is defined by DOCSIS.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-30

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

References

For additional information, refer to these resources:

- DOCSIS at www.cablemodem.com/specifications
- Euro-DOCSIS at http://www.euro-docsis.com

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

Lesson 3

Describing DSL Technology

Overview

DSL technology can provide a reliable high-speed alternative for remote access to a central site. This lesson distinguishes among the variations of DSL and explains two encapsulation methods: PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).

Objectives

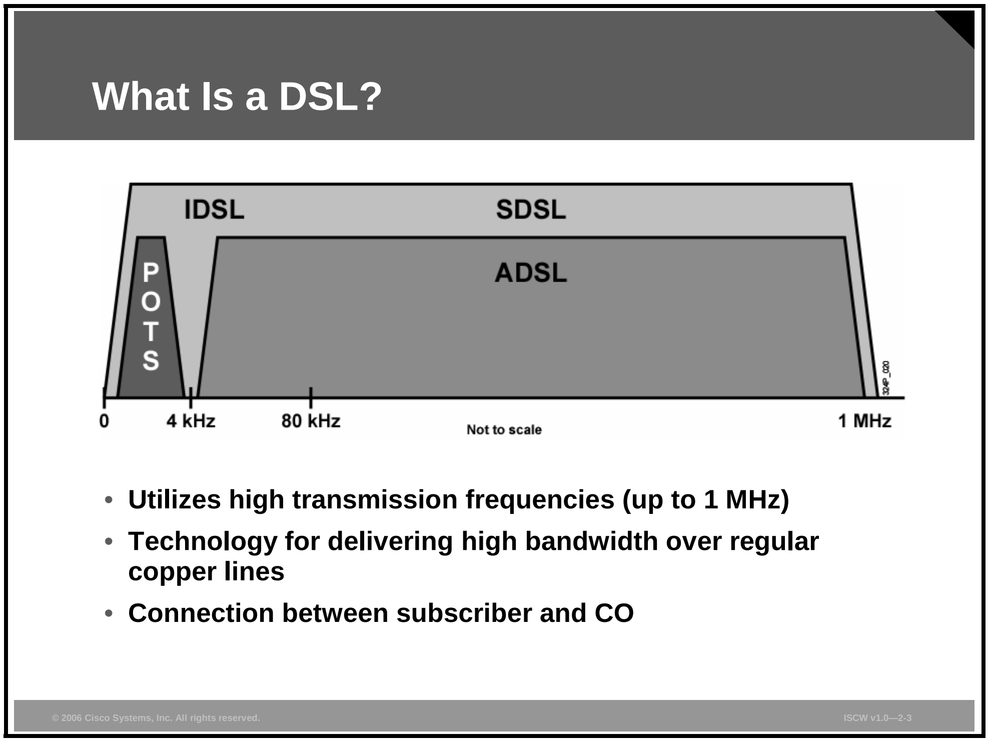
Upon completing this lesson, you will be able to describe xDSL technologies. This ability includes being able to meet these objectives:

- Describe features of DSL
- Describe the variants of DSL
- Explain the distance limitations of DSL
- Explain the basic facts of ADSL technology
- Explain how ADSL coexists with telephony service
- Explain CAP and DMT, the competing modulation standards for ADSL signaling
- Explain how data is transmitted over ADSL infrastructure with PPPoE
- Explain how data is transmitted over ADSL infrastructure with PPPoA

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

DSL Features

This topic describes the features of DSL.



What Is a DSL?

- Utilizes high transmission frequencies (up to 1 MHz)
- Technology for delivering high bandwidth over regular copper lines
- Connection between subscriber and CO

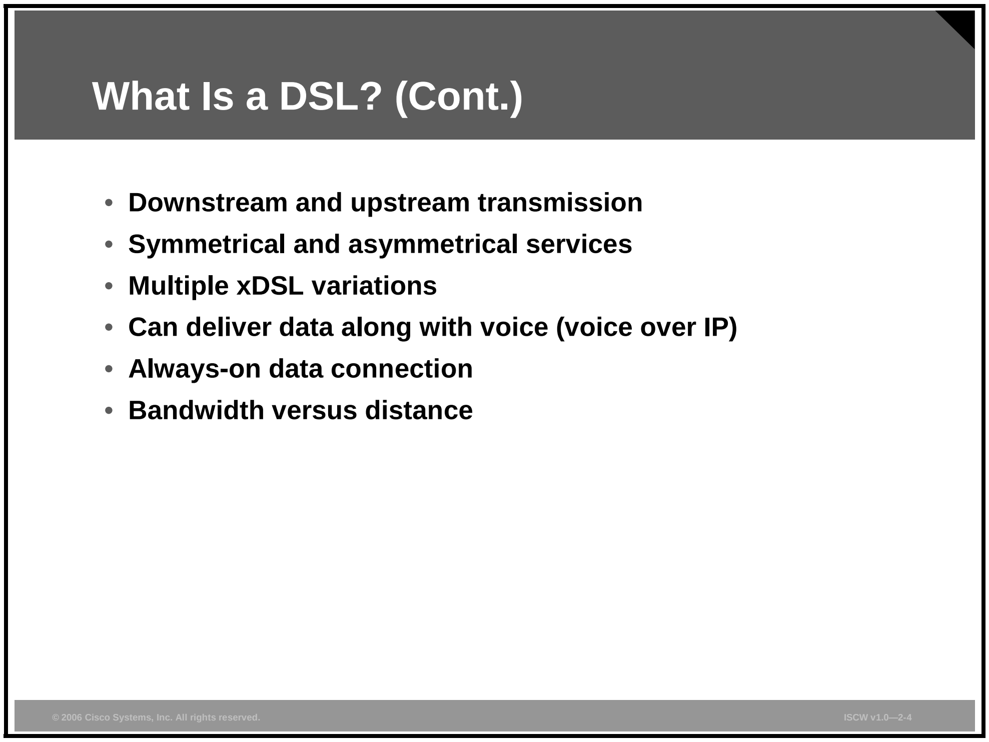
© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-3

Several years ago, research by Bell Labs identified that a typical voice conversation over a local loop only required the use of bandwidth of 300 Hz to 3 kHz. For years the bandwidth above 3 kHz went unused. Advances in technology allowed DSL to use the additional bandwidth from 3 kHz up to 1 MHz to deliver high-speed data services over ordinary copper lines. For example, asymmetric DSL (ADSL) uses a frequency range from approximately 20 kHz to 1 MHz. In order to deliver high-bandwidth data rates to subscribers, a relatively small change to the existing telephone company infrastructure is required.

DSL is not a complete end-to-end solution, but rather a physical layer transmission technology similar to dial, cable, or wireless. DSL connections are deployed in the "last mile" of a local telephone network—the local loop. The connection is set up between a pair of modems on either end of a copper wire extending between the customer premises equipment (CPE) and the DSL access multiplexer (DSLAM). A DSLAM is the device located at the central office (CO) of the provider and concentrates connections from multiple DSL subscribers.

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



What Is a DSL? (Cont.)

- **Downstream and upstream transmission**
- **Symmetrical and asymmetrical services**
- **Multiple xDSL variations**
- **Can deliver data along with voice (voice over IP)**
- **Always-on data connection**
- **Bandwidth versus distance**

© 2006 Cisco Systems, Inc. All rights reserved.

Transmission in DSL can be categorized in terms of direction as follows:

- **Downstream:** Transmission from a CO toward a subscriber.
- **Upstream:** Transmission from a subscriber toward a CO.

The DSL types fall into two major groups, taking into account downstream and upstream speeds:

- **Symmetrical DSL:** Communication in which transmission speeds available for upstream and downstream communication between the source and destination nodes are the same.
- **Asymmetrical DSL:** Communication in which different transmission speeds are used for communication between two ends of a network. Downstream speed is typically higher than upstream.

The term xDSL covers a number of DSL variations, such as ADSL, high-data-rate DSL (HDSL), Rate Adaptive DSL (RADSL), symmetric DSL (SDSL), ISDN DSL (IDSL), and very-high-data-rate DSL (VDSL).

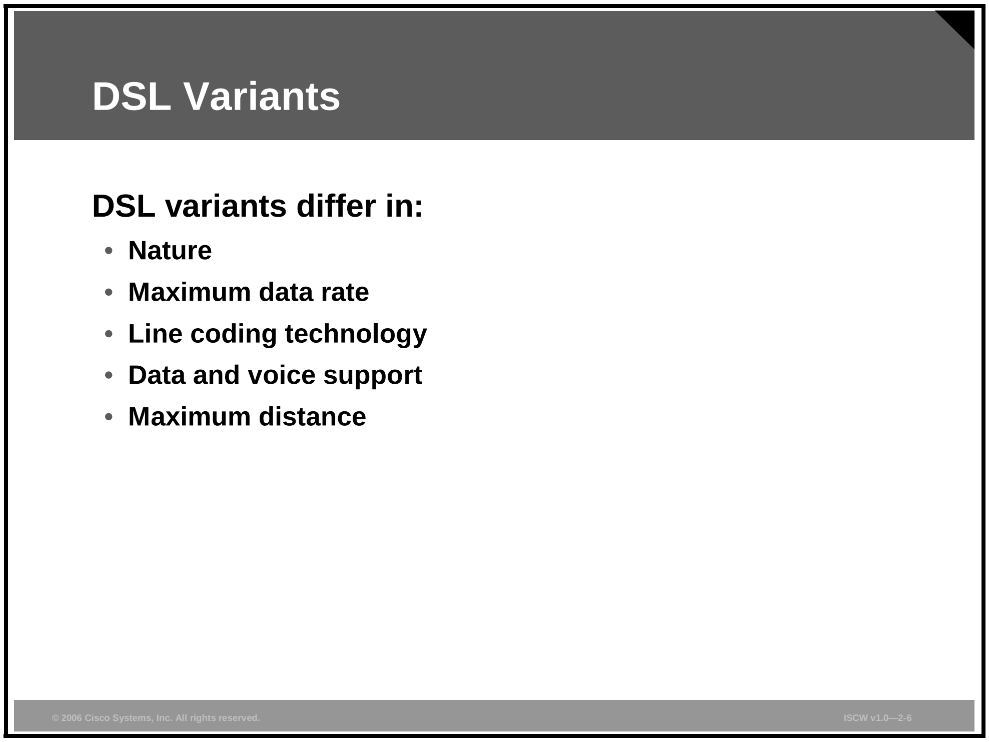
DSL types not using the voice frequencies band allow DSL lines to carry both data and voice signals simultaneously (for example, ADSL and VDSL), while other DSL types occupying the complete frequency range can carry data only (for example, SDSL and IDSL). Data service provided by a DSL connection is always-on.

The data rate that DSL service can provide depends upon the distance between the subscriber and the CO. The smaller the distance, the higher data rate can be achieved. If close enough to a CO offering DSL service, the subscriber might be able to receive data at rates of up to 6.1 Mbps out of a theoretical 8.448 Mbps maximum.

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

DSL Types

This topic describes the various types of DSL.



DSL Variants

DSL variants differ in:

- **Nature**
- **Maximum data rate**
- **Line coding technology**
- **Data and voice support**
- **Maximum distance**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-6

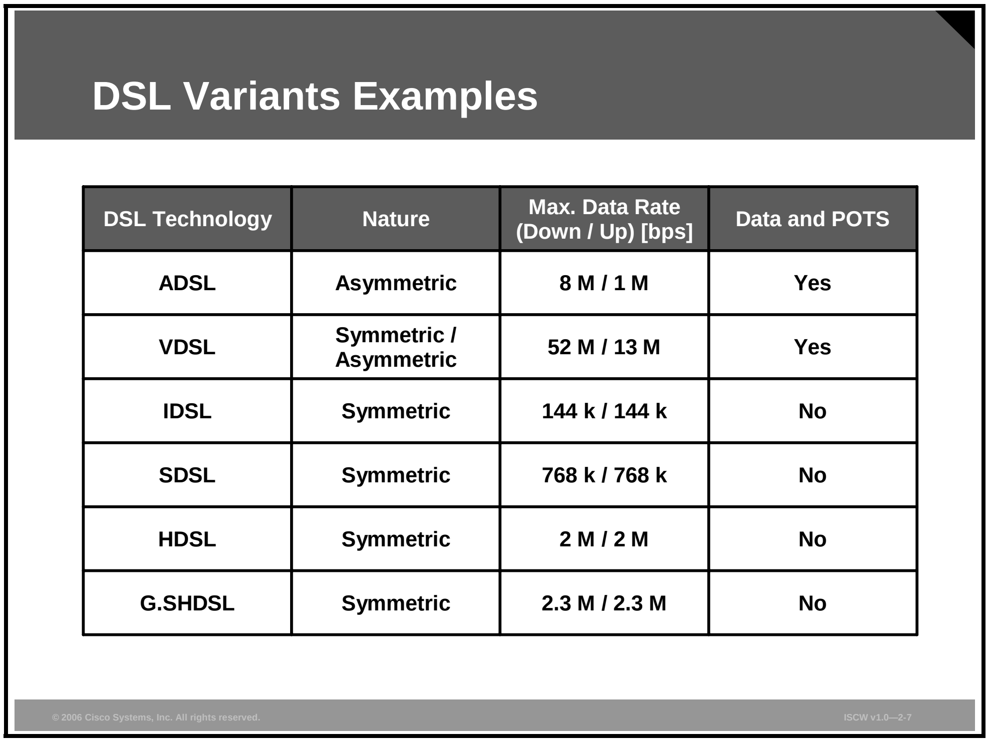
When discussing the DSL variants, the following properties are compared:

- **Nature:** The nature of DSL is the relation between downstream and upstream speeds. Synchronous DSL has the same speeds in both directions, while asynchronous DSL has different downstream and upstream speeds.
- **Maximum data rate:** Defines the maximum speed that can be deployed with a certain type of DSL.
- **Line coding technology:** Describes the technique used to represent digital signals to be transported over a copper twisted pair so that the receiver can interpret them accurately.
- **Data and voice support:** Depending on the usage of the available frequency spectrum, certain DSL types support data and voice simultaneously, while others do not.
- **Maximum distance:** Describes the maximum distance that a certain type of DSL connection can span.

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

DSL Variant Examples

DSL types include ADSL, VDSL, IDSL, SDSL, HDSL, and Symmetrical High-Data-Rate DSL (G.SHDSL). The table lists their characteristics.



DSL Variants Examples

DSL Technology	Nature	Max. Data Rate (Down / Up) [bps]	Data and POTS
ADSL	Asymmetric	8 M / 1 M	Yes
VDSL	Symmetric / Asymmetric	52 M / 13 M	Yes
IDSL	Symmetric	144 k / 144 k	No
SDSL	Symmetric	768 k / 768 k	No
HDSL	Symmetric	2 M / 2 M	No
G.SHDSL	Symmetric	2.3 M / 2.3 M	No

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-7

ADSL is designed to deliver more bandwidth downstream than upstream, and supports data and voice simultaneously over existing copper lines. ADSL is oriented towards residential subscribers, where usually more bandwidth is required in the downstream for applications such as downloading music, movies, playing online games, surfing the Internet, or receiving e-mail with large attachments. The downstream rate ranges from 256 kbps to 8 Mbps, while upstream speed can reach 1 Mbps.

RADSL refers to ADSL service with a data transmission rate that can be adapted to the local loop line conditions.

VDSL can provide symmetrical or asymmetrical services. The downstream bandwidth ranges from 13 Mbps to 52 Mbps. Like ADSL, VDSL also supports data and voice over a single copper line. The Cisco Long Reach Ethernet (LRE) solution is based on Ethernet over VDSL.

IDSL transmits data digitally (rather than via analog) on a twisted-pair copper telephone line across existing ISDN lines. IDSL delivers up to 144 kbps of symmetrical bandwidth derived from two bearer channels (2B at 64 kbps each) plus the signaling channel (D at 16 kbps), thus being essentially a leased-line ISDN BRI in which there is no D channel. IDSL does not support voice; it can only carry data, but has an advantage over ISDN in that it is always on.

SDSL delivers 768 kbps both downstream and upstream over a single copper twisted pair. SDSL technology is proprietary and non-standardized, and can only carry data. The symmetrical nature of SDSL makes it ideal for commercial use in instances in which the end user must send large amounts of data employing applications, such as e-mail messaging to customers with large attachments, uploading of data to corporate servers, or updating web pages.

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

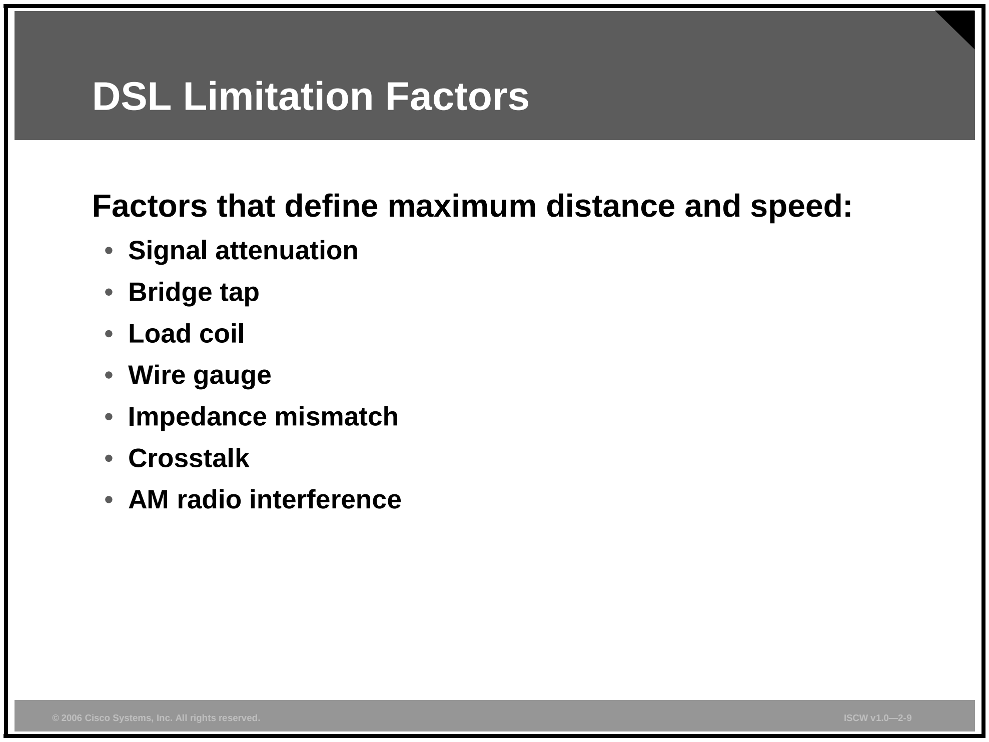
HDSL delivers 1.544 Mbps or 2.048 Mbps of symmetrical bandwidth over two copper twisted pairs. Service providers have been using HDSL as a substitute for T1 and E1. Only data can be carried via HDSL.

G.SHDSL offers symmetrical data rates from 192 kbps to 2.3 Mbps. G.SHDSL is standardized and developed by the International Telecommunication Union (ITU) to address the worldwide SDSL market.

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

DSL Limitations

This topic describes the distance limitations of DSL.



DSL Limitation Factors

Factors that define maximum distance and speed:

- **Signal attenuation**
- **Bridge tap**
- **Load coil**
- **Wire gauge**
- **Impedance mismatch**
- **Crosstalk**
- **AM radio interference**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-9

The DSL types are limited in distance and speed. Speed is inversely proportional to distance—longer distance in the local loop means lower maximum speed that a particular DSL connection supports. The maximum speed that can be achieved by certain DSL connections is also influenced by various impairments in the local loop that attenuate or distort the signal, such as the following:

- **Signal attenuation:** Attenuation means signal loss over distance and is determined by the distance between a subscriber and the CO. The longer the distance, the more attenuation occurs and therefore lower speeds are achieved.
- **Bridge tap:** A bridge tap is an extra telephone wire with an unterminated cable end which is connected to the local loop. Such an unterminated tap can cause noise, reflections, and can radiate power that reduces signal strength and consequently speed. DSL providers should remove bridge taps before installing a DSL connection.
- **Load coil:** Provisioning of loading coils was a standard procedure to improve plain old telephone service (POTS) voice quality on longer local loops. It is also called conditioning the loop. A loading coil is a wrap of wire placed at specific intervals along the local loop to extend the local loop distance. This creates a low-frequency band pass filter and will thus cut off, or block, the DSL frequencies. For the DSL to operate, load coils must be removed from the loop.
- **Wire gauge:** Wire gauge is the thickness of the wire used in the local loop. For higher speeds, thicker wire is used.
- **Impedance mismatch:** The impedance mismatch in the local loop causes echo, which results in noise. The impedance mismatch is caused by changes in wire gauge, wire splices, or corrosion.

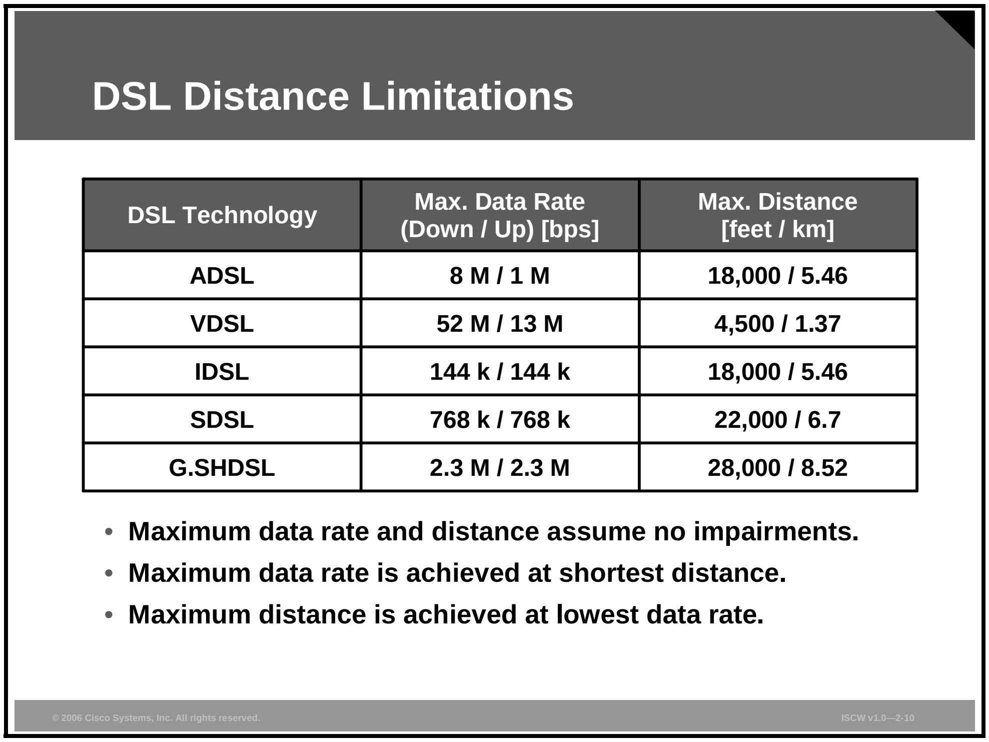
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **Crosstalk:** Crosstalk is the interference between two wires in a bundle, caused by electrical energy.
- **AM radio interference:** AM radio frequencies can interfere with a DSL signal, causing speed reduction. The interference is particularly a problem with in-house wiring, in which untwisted or poorly twisted wiring exists.

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

DSL Distance Limitations

The table summarizes the maximum data rate and operational reach that can be achieved with certain xDSL technology, assuming that there are no defects or impairments in the copper wiring.



DSL Distance Limitations

DSL Technology	Max. Data Rate (Down / Up) [bps]	Max. Distance [feet / km]
ADSL	8 M / 1 M	18,000 / 5.46
VDSL	52 M / 13 M	4,500 / 1.37
IDSL	144 k / 144 k	18,000 / 5.46
SDSL	768 k / 768 k	22,000 / 6.7
G.SHDSL	2.3 M / 2.3 M	28,000 / 8.52

- **Maximum data rate and distance assume no impairments.**
- **Maximum data rate is achieved at shortest distance.**
- **Maximum distance is achieved at lowest data rate.**

© 2006 Cisco Systems, Inc. All rights reserved.

The maximum data rate describes the maximum achievable downstream and upstream bandwidth with the shortest operational distance (distance between the subscriber and the CO). The maximum operational reach is the maximum achievable distance with the lowest operational data rate. The relation between bandwidth and distance is inversely related.

ADSL offers greater distance reachability but the achievable speed is degraded as the distance increases. The maximum distance is limited to approximately 18,000 feet (5.46 km). ADSL2 and ADSL2+ are enhancements to basic ADSL, providing downstream bandwidth of up to 24 Mbps and upstream bandwidth of up to 1.5 Mbps.

VDSL offers the highest operational speed but has the shortest achievable distance. For VDSL to support the maximum speed of 52 Mbps, the subscriber has to be very close to the CO—a range of 1000 feet (300 meters). The maximum operational distance is 4500 feet (1.37 km).

The maximum operating distance of IDSL is limited to 18,000 feet (5.46 km). An IDSL line can be configured for a speed of 64 kbps, 128 kbps, or 144 kbps. The line coding mechanism used is two binary, one quaternary (2B1Q), allowing transparent operation through an ISDN interface.

The use of a single twisted pair limits the operating range of SDSL to about 22,000 feet (6.7 km).

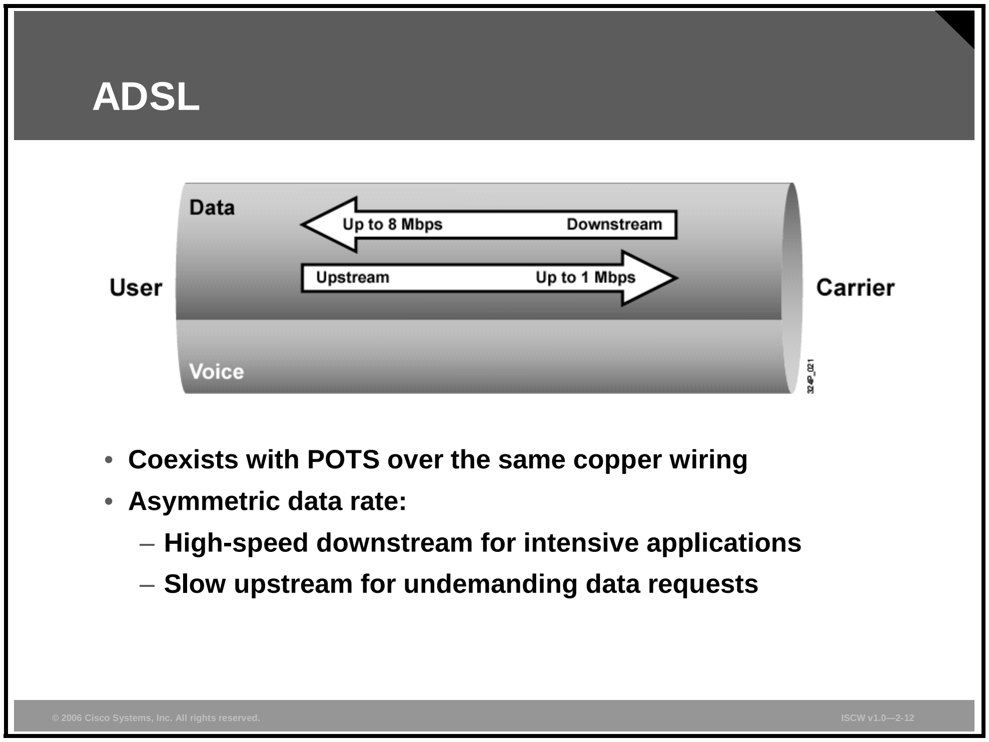
The operating range of HDSL is limited to approximately 12,000 feet (3.7 km).

The maximum operational distance supported by G.SHDSL is about 28,000 feet (8.5 km), thus offering greater reach over other deployed DSL 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 self-study.

ADSL

This topic describes ADSL technology.



ADSL

- Coexists with POTS over the same copper wiring
- Asymmetric data rate:
  - High-speed downstream for intensive applications
  - Slow upstream for undemanding data requests

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-12

ADSL coexists with POTS over the same twisted-pair telephone line. Three information channels usually exist over the same wiring (depending on the variety of ADSL): a POTS channel for analog voice if that is desired, a varying-speed duplex channel, and a high-speed downstream channel. A user can use the phone line and the ADSL connection simultaneously without adverse effects on either service.

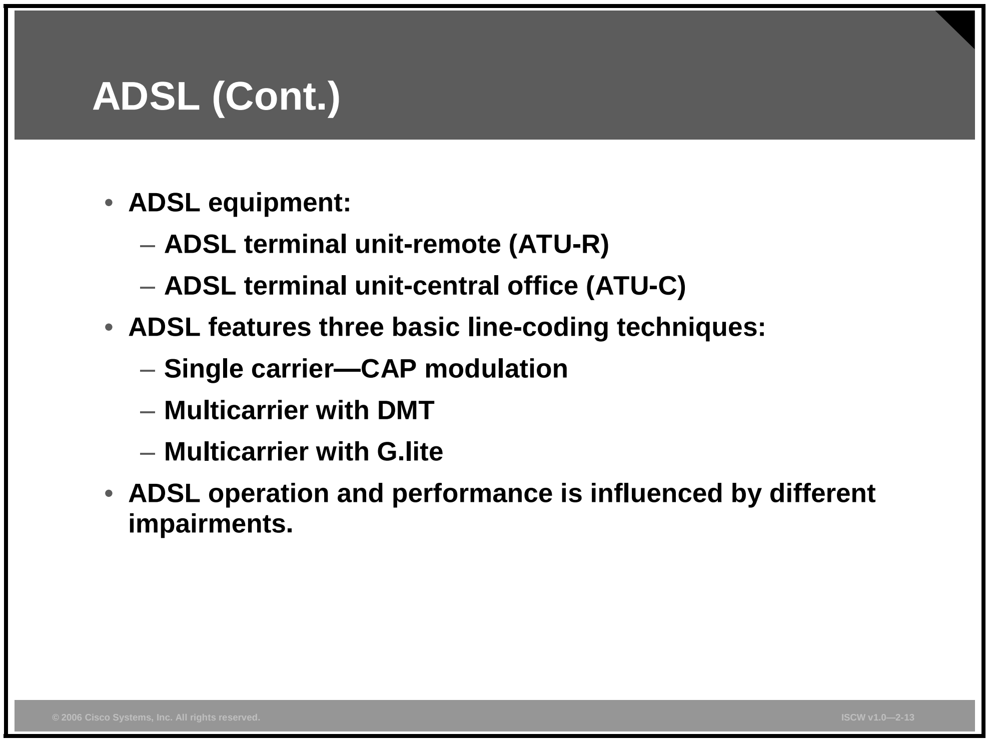
ADSL is characterized by asymmetric data rates, with higher data rates toward the user (downstream) and lower data rates toward the carrier (upstream).

The distance between the end user and the CO provides the guideline for line speeds. Downstream, ADSL supports speeds up to slightly more than 8 Mbps. For upstream, the rate is approximately 1 Mbps. The maximum upstream rate can be provided at distances of up to 18,000 feet (5.486 km) over a one-wire pair without repeaters on an optimized loop. The maximum downstream speed can be achieved at distances up to 12,000 feet (3.658 km) using standard 0.6 mm (24-gauge) wire on an optimal loop.

Standardized in 2004, newer ADSL variants offer improvements over regular ADSL:

- ADSL2 (ITU G.992.3/4) offers higher downstream rates of up to 12 Mbps for spans of less than 8000 feet (2.5 km).
- ADSL2+ (ITU G.992.5) provides up to 24 Mbps for spans of less than 5000 feet (1.5 km).

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



ADSL (Cont.)

- ADSL equipment:
  - ADSL terminal unit-remote (ATU-R)
  - ADSL terminal unit-central office (ATU-C)
- ADSL features three basic line-coding techniques:
  - Single carrier—CAP modulation
  - Multicarrier with DMT
  - Multicarrier with G.lite
- ADSL operation and performance is influenced by different impairments.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-13

ADSL service is deployed between ADSL modems at the subscriber and the CO locations. The CPE ADSL modem is known as the ADSL Transmission Unit-Remote (ATU-R). The CO modem is also called ADSL Transmission Unit-central office (ATU-C). Special devices called DSLAMs are located at the CO—a DSLAM encompasses multiple ATU-Cs.

The basic line-coding techniques associated with ADSL are as follows:

- **Single-carrier:** Carrierless Amplitude and Phase Modulation (CAP)
- **Multicarrier with DMT:** Discrete Multi-Tone (DMT) modulation
- **Multicarrier with G.lite:** G.lite, also known as splitterless ADSL. G.lite offers slower speeds but does not require the signals to be split at the subscriber end. It is the most popular method for the mass market.

The modulation technique used has to correspond with the ADSL CPE and ADSL modems on the DSLAM and is determined by the service provider.

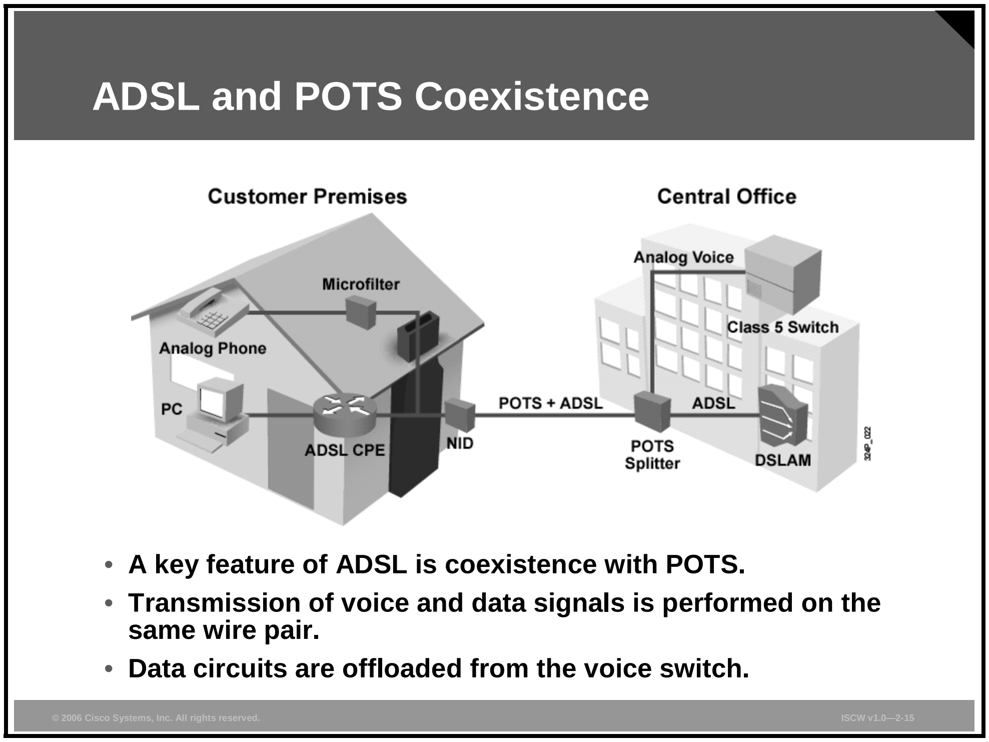
When dealing with problems in ADSL operation, the following should be checked:

- Load coils should be removed from the line for ADSL to operate.
- Throughput is reduced when impedance mismatches are present (for example, different wire gauge used in the line).
- Bridge taps also reduce the achievable throughput.
- Crosstalk from other lines and wiring will degrade the throughput.
- External interference like AM radio interference will result in unpredictable effects on ADSL performance.

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

ADSL and POTS Coexistence

This topic describes how ADSL coexists with traditional telephony service.



ADSL and POTS Coexistence

- **A key feature of ADSL is coexistence with POTS.**
- **Transmission of voice and data signals is performed on the same wire pair.**
- **Data circuits are offloaded from the voice switch.**

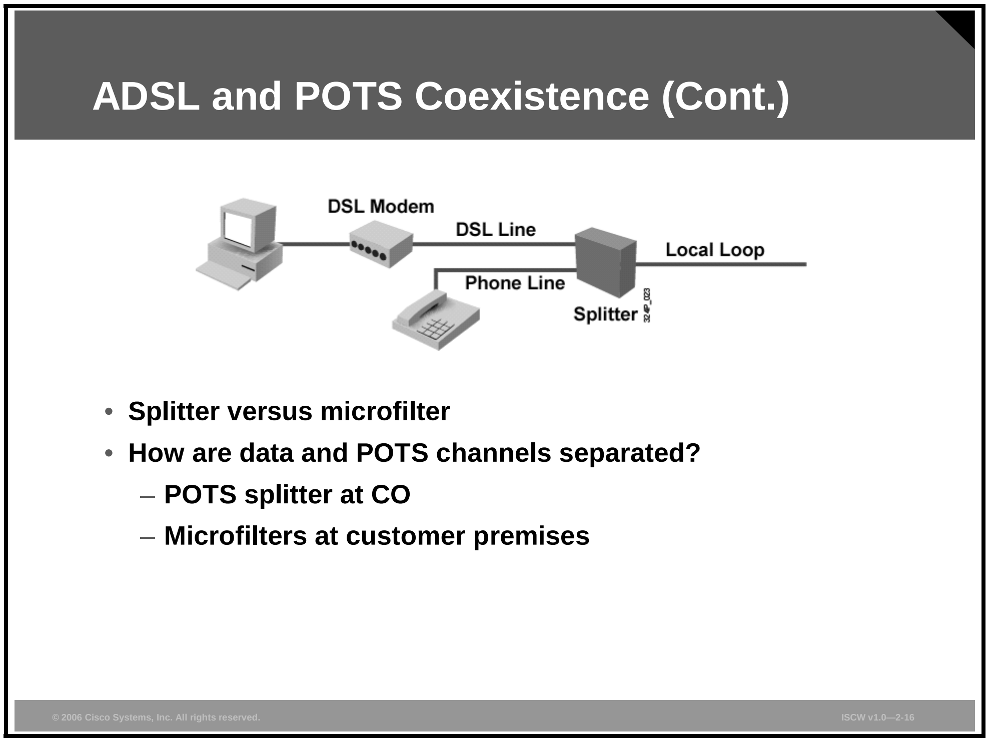
© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-15

The major benefit of ADSL is the ability to provide data services along with voice. When analog voice is integrated with ADSL, the POTS channel is split off from the ADSL modem by filters or splitters, which guarantees uninterrupted regular phone service even if ADSL fails. A user is able to use the phone line and the ADSL connection simultaneously without adverse effects on either service if filters or splitters are in place.

ADSL offloads the data (modem) traffic from the voice switch and keeps analog POTS separate from data. Separating voice and data traffic provides fail-safe emergency-call services for POTS operation. The data channel is established between the CPE modem and the CO DSLAM. The voice channel is established between the telephone and the voice switch at the CO premises.

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



ADSL and POTS Coexistence (Cont.)

- **Splitter versus microfilter**
- **How are data and POTS channels separated?**
  - **POTS splitter at CO**
  - **Microfilters at customer premises**

© 2006 Cisco Systems, Inc. All rights reserved.

POTS splitters are used to separate the DSL traffic from the POTS traffic. The POTS splitter is a passive device. In the event of a power failure, the voice traffic will still be carried to the voice switch in the CO. Splitters may be located at the customer premises but are certainly used in the CO.

A microfilter is a passive low-pass filter with two ends. One end connects to the telephone, and the other end connects to the telephone wall jack.

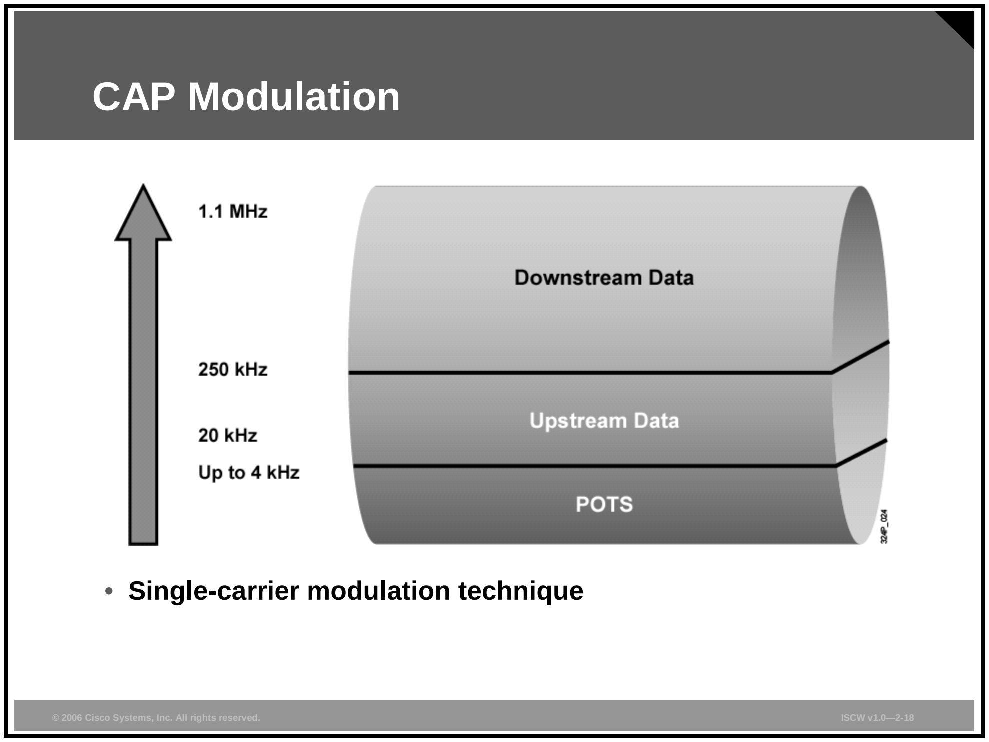
The local loop terminates on the customer premises at the demarcation point in the network interface device (NID). At the demarcation point where the phone line enters the customer premises, a device called a splitter is attached to the phone line. The splitter forks the phone line; one branch provides the original house telephone wiring for the phone, and the other branch connects to the ADSL modem. In addition, the splitter acts as a low-pass filter, allowing only the 0–4 kHz frequencies to pass to or from the phone. Installing the POTS splitter at the NID requires that a technician go out to the customer site to set up the ADSL service, therefore most installations today use microfilters.

At the CO, the POTS splitter separates the voice traffic which goes to the voice switch in the CO and the data traffic which goes to the DSLAM in the CO.

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

ADSL Channels and Encoding

This topic describes the encapsulation types for ADSL.



CAP Modulation

- Single-carrier modulation technique

© 2006 Cisco Systems, Inc. All rights reserved.   ISCW v1.0—2-18

There are two basic types of modulation techniques associated with ADSL: a single-carrier CAP, which is proprietary, and multicarrier standardized DMT.

CAP Modulation

CAP is an easily implemented modulation method used in many of the early installations of ADSL.

CAP modulation creates three separate channels on the wire by dividing the signals into three distinct bands:

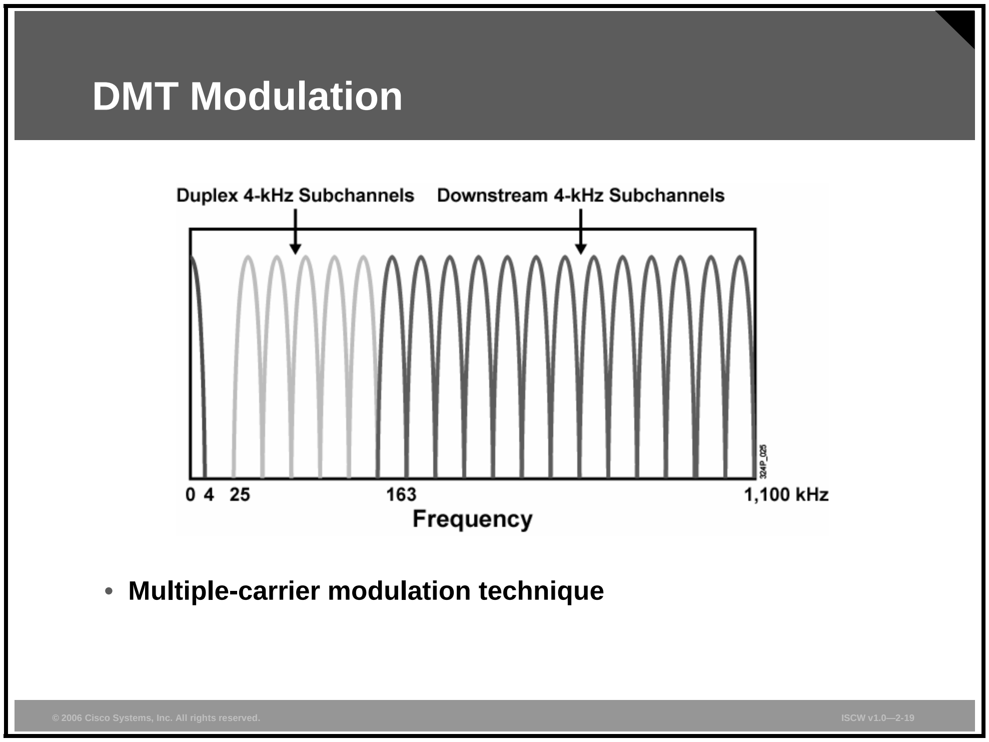
- **Voice channel:** Voice traffic is carried in the 0–4 kHz band.
- **Upstream channel:** The range of 25–160 kHz is allocated for upstream data traffic.
- **Downstream channel:** The range of 240 kHz to 1.5MHz is allocated for downstream data traffic. The actual width of the downstream channel (the upper frequency) varies and depends upon a number of conditions, such as line length or line noise.

The three channels are widely separated to minimize the possibility of interference between the channels on one line or between the signals on different lines. A single-carrier notation means that only one frequency band is used to carry either an upstream or downstream channel.

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

DMT Modulation

DMT modulation is standardized with ANSI and ITU—ITU 992.1 (G.dmt), ITU 992.2 (G.lite), and ANSI T1.413 Issue 2. DMT is the prevailing modulation technique used in modern ADSL deployments.



DMT Modulation

- **Multiple-carrier modulation technique**

© 2006 Cisco Systems, Inc. All rights reserved.

As with CAP, the DMT modulation technique divides the signals on the wire into separate channels. The main difference is that DMT does not use only two wide channels for upstream and downstream data traffic. With DMT, the frequency band is divided into 256 separate 4-kHz-wide channels. Channels 6 to 38 are duplex and used for both upstream and downstream data traffic, and channels 39 and onwards are used only for downstream data traffic. To compensate for noise, the system constantly monitors each channel. When channel quality decreases, the system adjusts the number of bits per channel, or if the quality is too impaired, the signal is shifted to another channel. This system constantly shifts signals among different channels, searching for the best channels for transmission and reception.

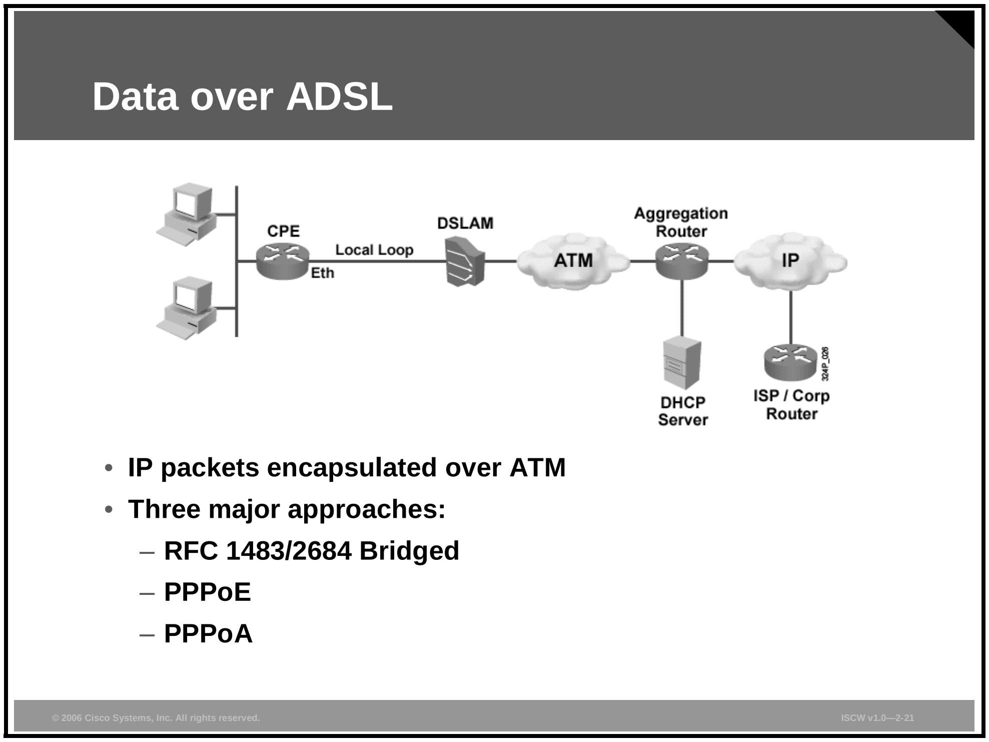
Implementing DMT modulation is more complex than implementing CAP modulation, because it uses a large number of channels. On the other hand, DMT modulation offers more flexibility when traversing lines of differing quality.

G.lite is a less complex version of the DMT standard. G.lite uses only half the subchannels (128) and is thus also known as half-rate DMT. The lower number of channels also determines a lower maximum downstream speed of 1.5 Mbps and a maximum upstream speed of 640 kbps.

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

Data over ADSL: PPPoE

This topic describes PPPoE.



Data over ADSL

- IP packets encapsulated over ATM
- Three major approaches:
  - RFC 1483/2684 Bridged
  - PPPoE
  - PPPoA

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-21

Data over ADSL

DSL is a high-speed Layer 1 transmission technology that works over copper wires.

The DSL Layer 1 connection from the CPE is terminated at the DSLAM. The data link layer protocol that is usually used over DSL is ATM. A DSLAM is basically an ATM switch containing DSL interface cards (ATU-Cs). The DSLAM terminates the ADSL connections, and then switches the traffic over an ATM network to an aggregation router. The aggregation router is the Layer 3 device where IP connection from the subscriber terminates. IP packets over an ATM and DSL connection have to be encapsulated in some way, and these three approaches exist:

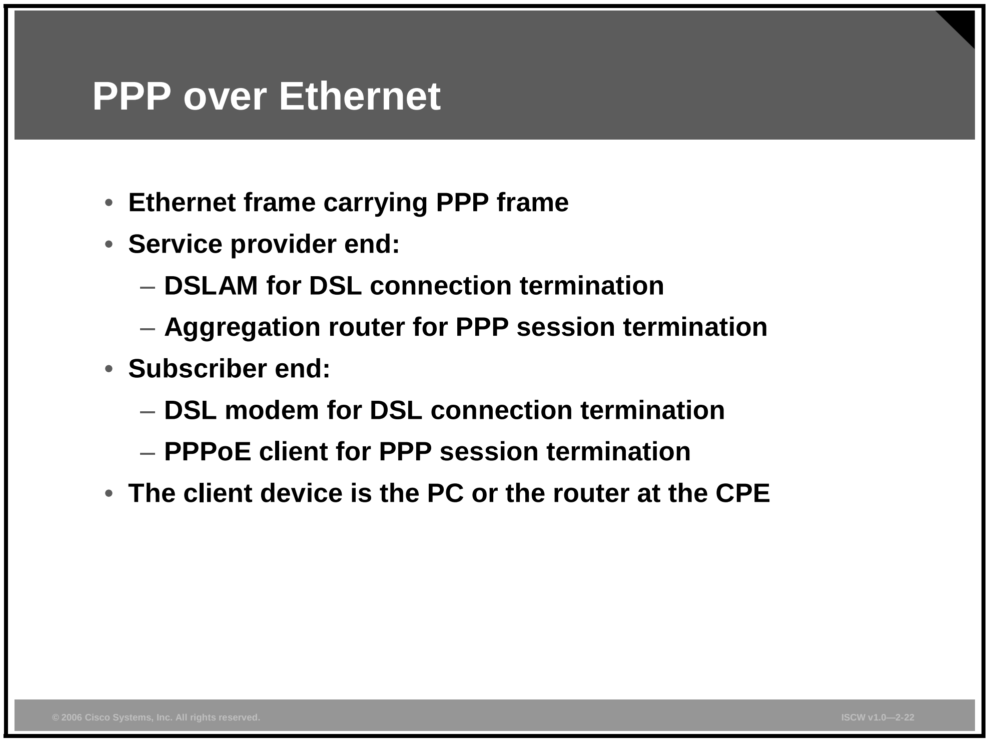
- RFC 1483/2684 Bridged
- PPPoE
- PPPoA

Briefly described using RFC 1483 Bridging, the ADSL CPE bridges the Ethernet frame from the PC of the end user to the aggregation router, where integrated routing and bridging (IRB) is used to provide connectivity to the IP cloud. RFC 1483 Bridging has security and scalability issues, making it unpopular as a deployment architecture. PPPoE and PPPoA are more scalable and secure, but also more complex for implementation.

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

PPP over Ethernet

The CPE bridges the Ethernet frames from the end-user PC to an aggregation router over ATM with an Ethernet frame carrying a PPP frame.



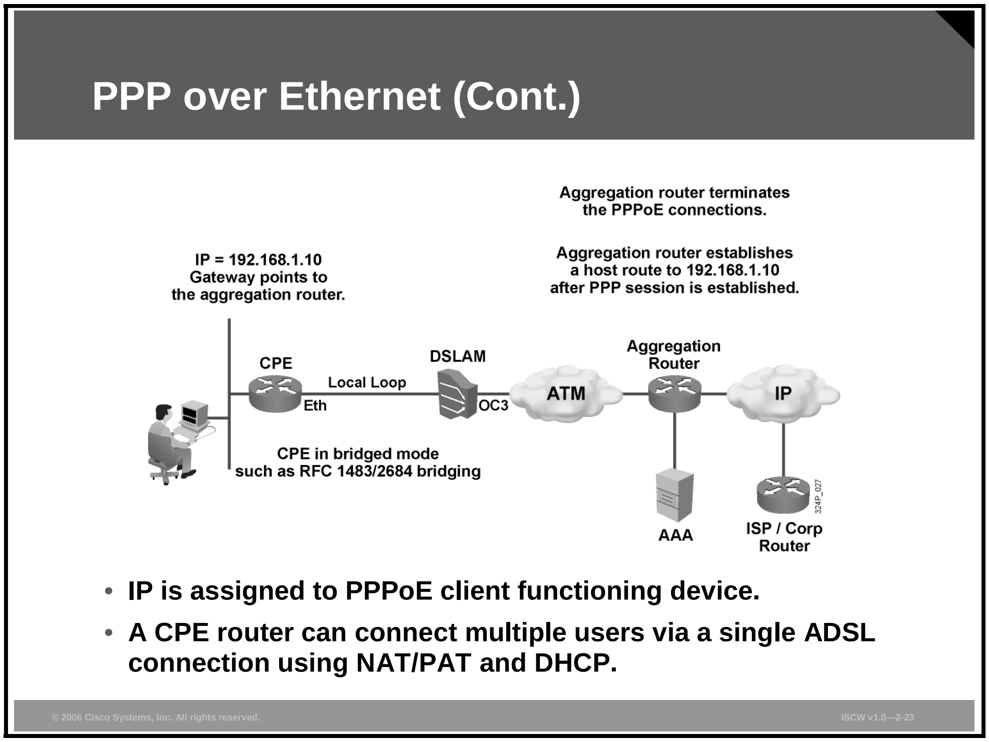
PPP over Ethernet

- **Ethernet frame carrying PPP frame**
- **Service provider end:**
  - **DSLAM for DSL connection termination**
  - **Aggregation router for PPP session termination**
- **Subscriber end:**
  - **DSL modem for DSL connection termination**
  - **PPPoE client for PPP session termination**
- **The client device is the PC or the router at the CPE**

© 2006 Cisco Systems, Inc. All rights reserved.

The PPP session is established between the subscriber device with PPPoE client support—either an end-user PC with PPPoE client software or the CPE router configured as the PPPoE client—and the aggregation 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 self-study.



PPP over Ethernet (Cont.)

Aggregation router terminates the PPPoE connections.

Aggregation router establishes a host route to 192.168.1.10 after PPP session is established.

IP = 192.168.1.10 Gateway points to the aggregation router.

CPE in bridged mode such as RFC 1483/2684 bridging

- **IP is assigned to PPPoE client functioning device.**
- **A CPE router can connect multiple users via a single ADSL connection using NAT/PAT and DHCP.**

© 2006 Cisco Systems, Inc. All rights reserved.

Either the PC or the router can be the PPPoE client. The figure shows a router as a client.

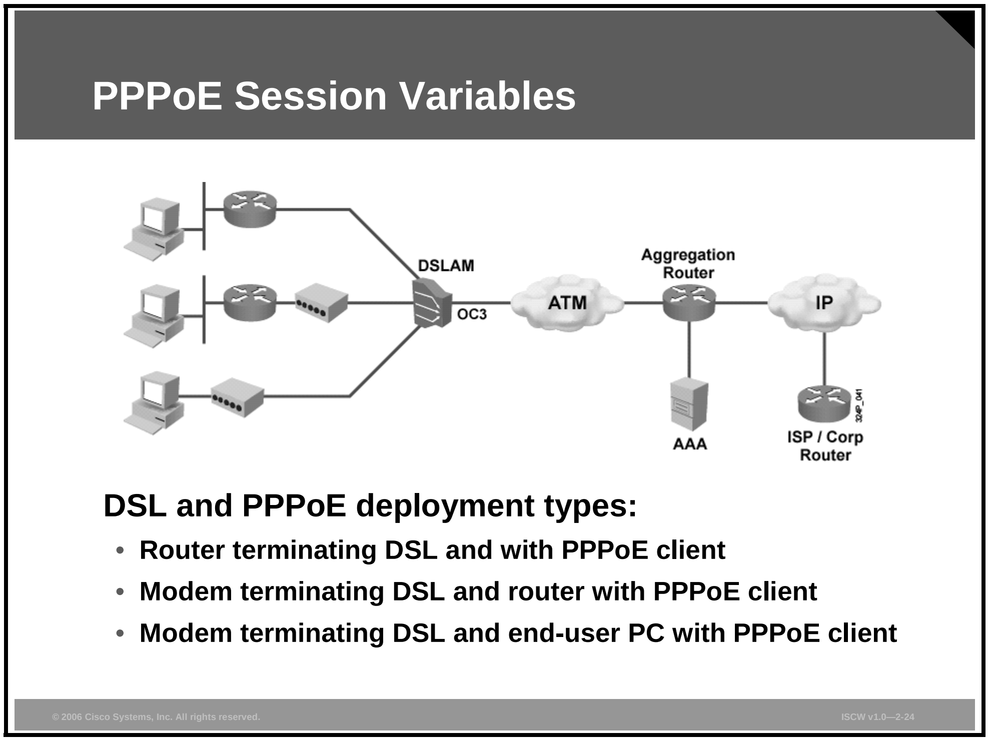
In the PPPoE architecture, the PPPoE client functionality is used to connect to the ADSL service. The PPPoE client first encapsulates the end-user data into a PPP frame, and then the PPP frame is further encapsulated inside an Ethernet frame. The IP address allocation for the PPPoE client is based on the same principle as PPP in dial mode, which is via IP Control Protocol (IPCP) negotiation, with Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication. The aggregation router that authenticates the users can use either a local database on the aggregation router or a RADIUS authentication, authorization, and accounting (AAA) server.

The PPPoE client functionality can be available as a software PPPoE client application on the end-user PC. With this model, PPPoE provides the ability to connect a host over a simple bridging CPE to an aggregation router. A host uses its own PPP stack and the user is presented with a familiar user interface (using the PPPoE client software) similar to establishing a dialup connection. Unlike PPPoA, access control, billing, and type of service can be controlled on a per-user, rather than a per-site, basis.

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

PPPoE Session Variables

Different possibilities exist in establishing a PPPoE session.



PPPoE Session Variables

DSL and PPPoE deployment types:

- **Router terminating DSL and with PPPoE client**
- **Modem terminating DSL and router with PPPoE client**
- **Modem terminating DSL and end-user PC with PPPoE client**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-24

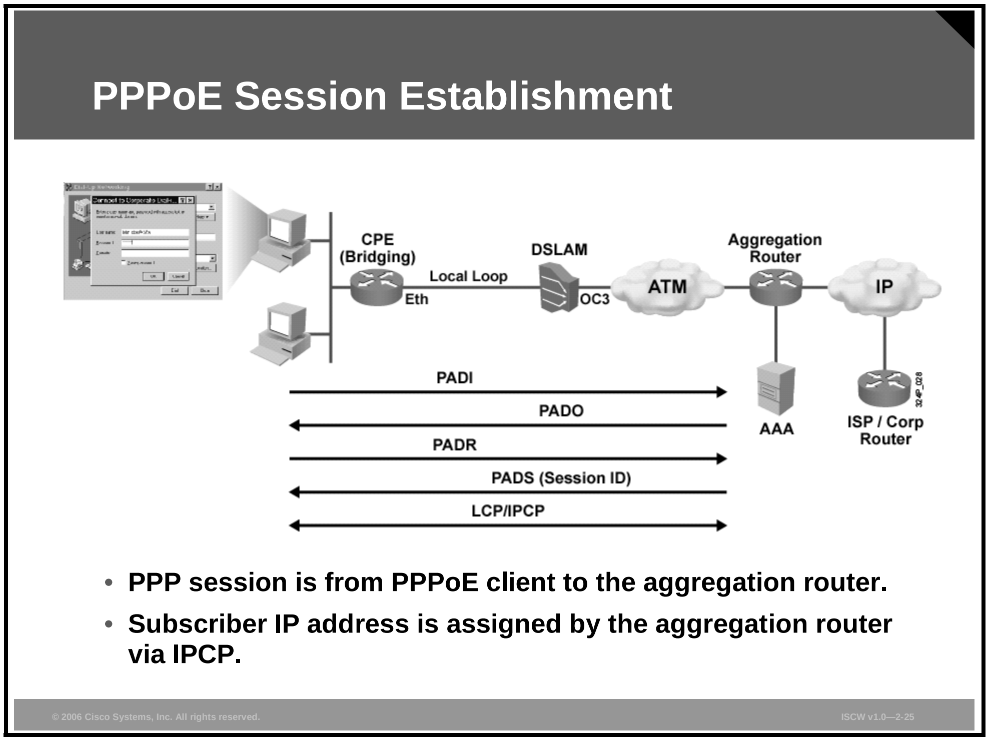
When deploying PPPoE and DSL, these three options are available in regards to the equipment used, DSL termination, and PPPoE client functionality:

- A router with an internal modem and PPPoE client functionality is used to terminate a DSL line and establish a PPPoE session. This option is preferable when support of a PPPoE client software is undesirable. The router can also be a DHCP server, and deploy Network Address Translation (NAT) and Port Address Translation (PAT) to connect multiple users behind the service provider, using a single ADSL connection and a single PPP username and password.
- An external modem is used to terminate a DSL line, and a router with PPPoE client functionality establishes a PPPoE session. A router can also act as a DHCP server and provide NAT and PAT functionality.
- An external modem is used to terminate a DSL line. An end-user PC encompasses the PPPoE client for establishing a PPPoE session.

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

PPPoE Session Establishment

PPP usually only works over a point-to-point connection. For PPP over an Ethernet multiaccess environment, additional enhancements are needed.



PPPoE Session Establishment

- **PPP session is from PPPoE client to the aggregation router.**
- **Subscriber IP address is assigned by the aggregation router via IPCP.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-25

PPPoE has two distinct stages (per RFC 2516): a discovery stage and a PPP session stage.

When a PPPoE client (end-user PC or router) initiates a PPPoE session, it must first perform discovery to identify which PPPoE server can meet the client request. Then, the host must identify the Ethernet MAC address of the peer and establish a PPPoE session ID. Although PPP defines a peer-to-peer relationship, discovery is inherently a client-server relationship. In the discovery process, the PPPoE client discovers an aggregation router (the PPPoE server). There may be more than one PPPoE server that the PPPoE client can communicate with, based on the network topology. The discovery stage allows the PPPoE client to discover all PPPoE servers and then select one.

There are four steps to the discovery stage:

Step 1 The PPPoE client (end-user PC or router) broadcasts a PPPoE Active Discovery Initiation (PADI) packet containing an indication of which service type it is requesting. The destination MAC address is set to broadcast.

Step 2 The PPPoE server (aggregation router) sends a PPPoE Active Discovery Offer (PADO) packet describing which service it can offer. The destination MAC address is the unicast address of the client (end-user PC or router).

Step 3 The PPPoE client sends a unicast PPPoE Active Discovery Request (PADR) packet to the PPPoE server.

Step 4 The PPPoE server sends a unicast PPPoE active discovery session-confirmation (PADS) packet to the client.

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

When discovery has been succssfully completed, both the PPPoE client and the selected PPPoE server have the information that they will use to build their point-to-point connection over the Ethernet. After the PPPoE session begins, PPP goes through the normal link control protocol (LCP) and Network Control Protocol (NCP) process.

A PPPoE active discovery terminate (PADT) packet may be sent anytime after a session has been established to indicate that a PPPoE session has been terminated. Either the PPPoE client or the PPPoE server may send it.

More information on the PPPoE specification can be obtained in RFC 2516.

Per RFC 2516, the maximum receive unit (MRU) option must not be negotiated to a size larger than 1492 bytes, because Ethernet has a maximum payload size of 1500 octets. The PPPoE header is 6 octets and the PPP protocol ID is 2 octets, so the PPP maximum transmission unit (MTU) must not be greater than (1500 – 8 =) 1492 bytes.

An Ethernet and PPPoE frame contains one of these Ethertypes:

- 0x8863 Ethertype = PPPoE control packets
- 0x8864 Ethertype = PPPoE data packets

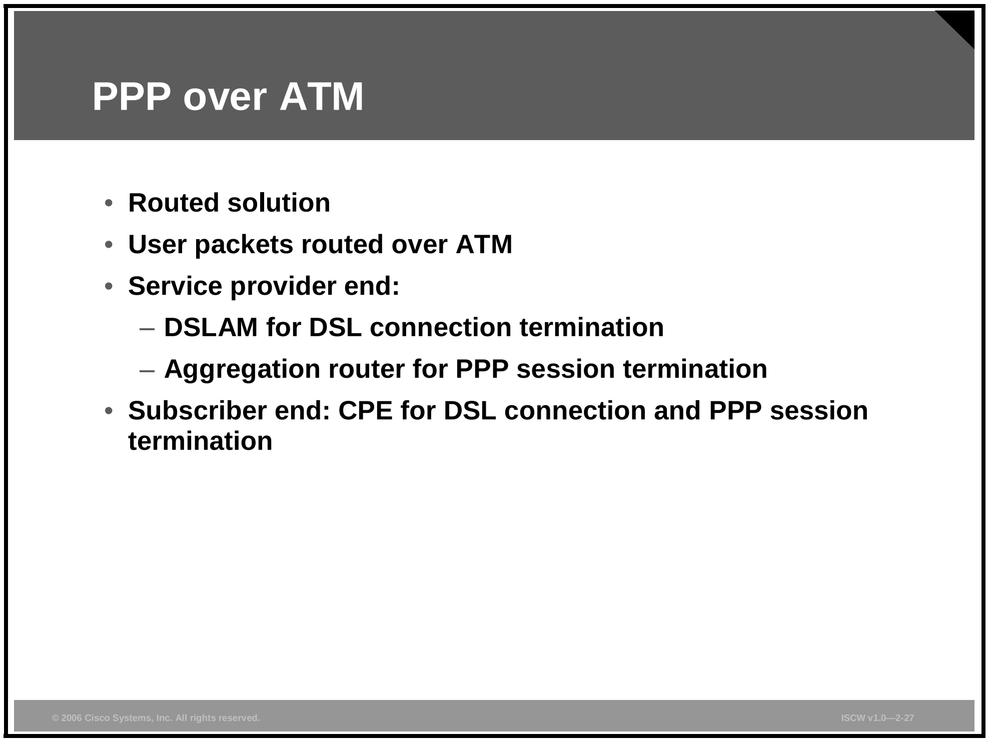
This is what a PPPoE frame looks like:

```
Ethernet Header | PPPoE Header | PPP PID | User 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 self-study.

Data over ADSL: PPPoA

This topic describes PPPoA.



PPP over ATM

- Routed solution
- User packets routed over ATM
- Service provider end:
  - DSLAM for DSL connection termination
  - Aggregation router for PPP session termination
- Subscriber end: CPE for DSL connection and PPP session termination

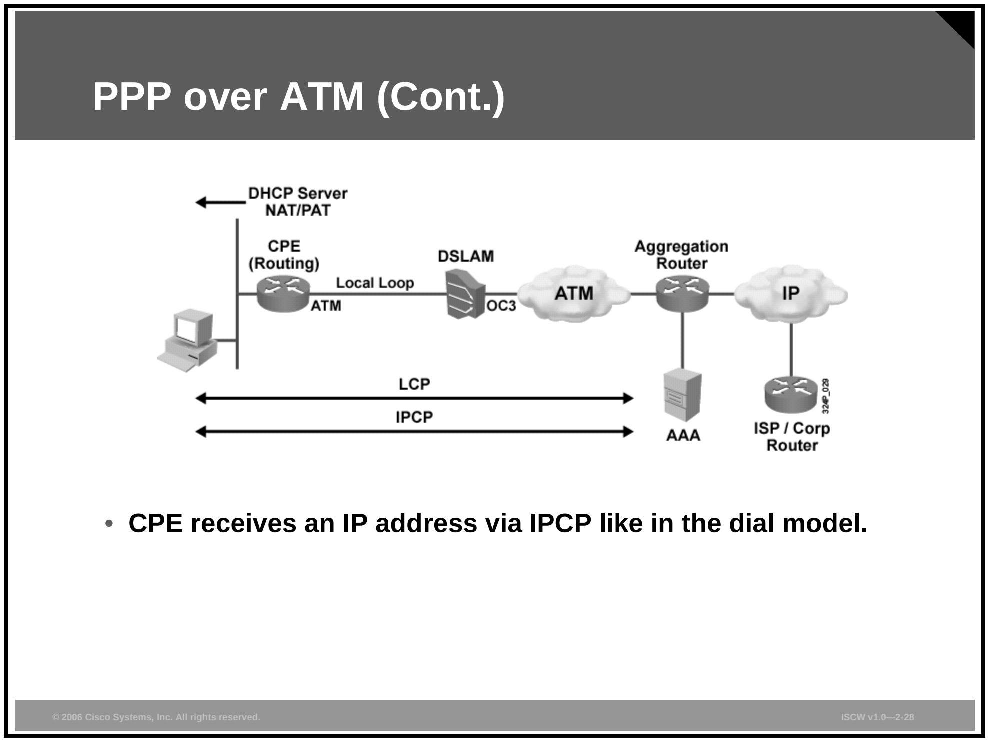
© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-27

PPPoA is a routed solution, unlike RFC 1483 Bridged and PPPoE, in which the CPE is set up as a bridge, bridging the Ethernet frames from the end-user PC to the aggregator router.

With PPPoA, the CPE routes the packets from the end-user PC over ATM to an aggregation router. The PPP session is established between the CPE and the aggregation router. Unlike PPPoE, PPPoA does not require host-based (PPPoE client) software.

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



PPP over ATM (Cont.)

- **CPE receives an IP address via IPCP like in the dial model.**

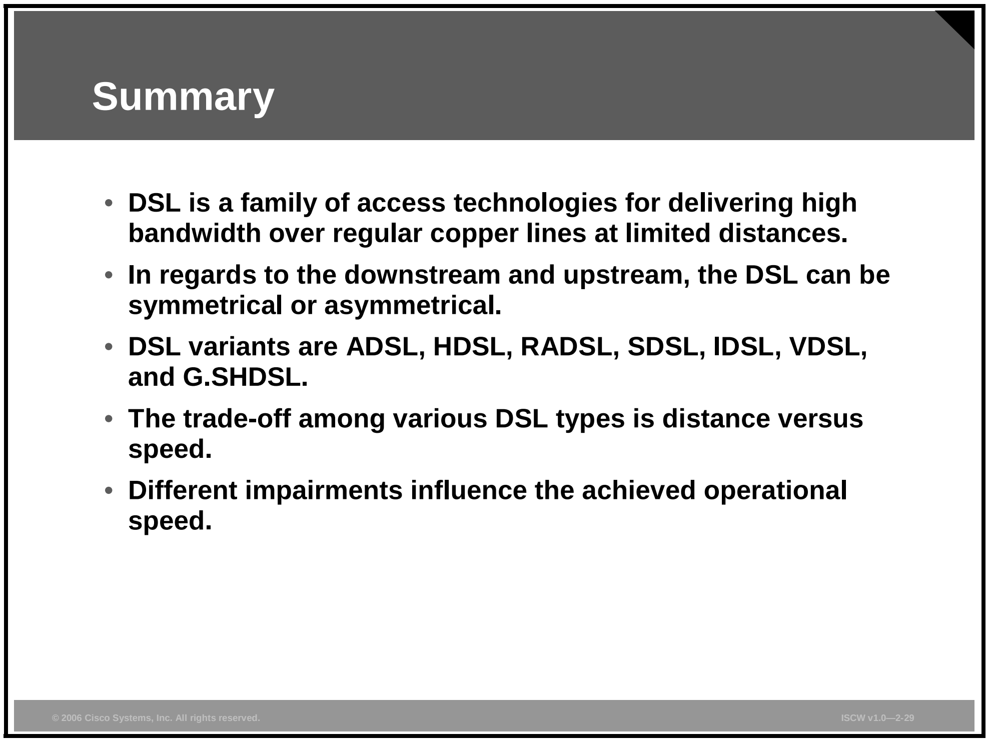
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-28

With PPPoA, a PPP session is established between the CPE and the aggregation router. The CPE device must have a PPP username and password configured for authentication to the aggregation router that terminates the PPP session from the CPE. The aggregation router that authenticates the users can either use a local database on the aggregation router or a RADIUS AAA server. The PPPoA session authentication can be based on PAP or CHAP. After the PPP username and password have been authenticated, IPCP negotiation takes place and the IP address is assigned to the CPE. After the IP address has been assigned, a host route is established both on the CPE and the aggregation router. The aggregation router must assign only one IP address to the CPE, and the CPE can be configured as a DHCP server and use NAT and PAT to support multiple hosts connected via Ethernet behind the CPE.

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

Summary

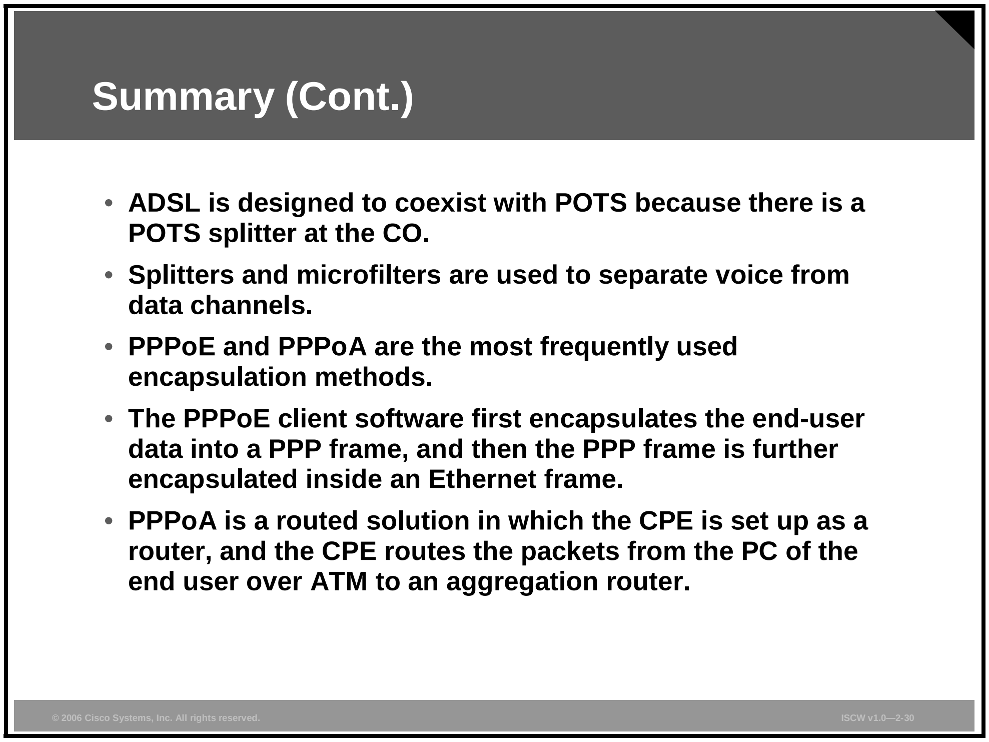
This topic summarizes the key points that were discussed in this lesson.



Summary

- DSL is a family of access technologies for delivering high bandwidth over regular copper lines at limited distances.
- In regards to the downstream and upstream, the DSL can be symmetrical or asymmetrical.
- DSL variants are ADSL, HDSL, RADSL, SDSL, IDSL, VDSL, and G.SHDSL.
- The trade-off among various DSL types is distance versus speed.
- Different impairments influence the achieved operational speed.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-29



Summary (Cont.)

- ADSL is designed to coexist with POTS because there is a POTS splitter at the CO.
- Splitters and microfilters are used to separate voice from data channels.
- PPPoE and PPPoA are the most frequently used encapsulation methods.
- The PPPoE client software first encapsulates the end-user data into a PPP frame, and then the PPP frame is further encapsulated inside an Ethernet frame.
- PPPoA is a routed solution in which the CPE is set up as a router, and the CPE routes the packets from the PC of the end user over ATM to an aggregation router.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-30

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

Lesson 4

Configuring the CPE as the PPPoE or PPPoA Client

Overview

DSL is an ideal solution for high-bandwidth remote access to a central site. DSL is a high-speed Layer 1 transmission technology that works over copper wires. ATM is used as the data link layer protocol over DSL. PPP over Ethernet (PPPoE) provides the ability to connect a network of hosts over a simple bridging DSL customer premises equipment (CPE) access device to an aggregation router. Typically, the end-user PC uses the PPPoE client software on the PC to connect to the DSL service. However, instead of using the PPPoE client software on the end-user PC, the CPE (DSL router) can be configured as the PPPoE client. This configuration will allow multiple PCs behind the CPE (DSL router) to connect to the DSL service using a single DSL connection and PPP username and password. In this case, the CPE (DSL router) would be configured for routing.

This lesson discusses how to configure the CPE (DSL router) as the PPPoE client.

Objectives

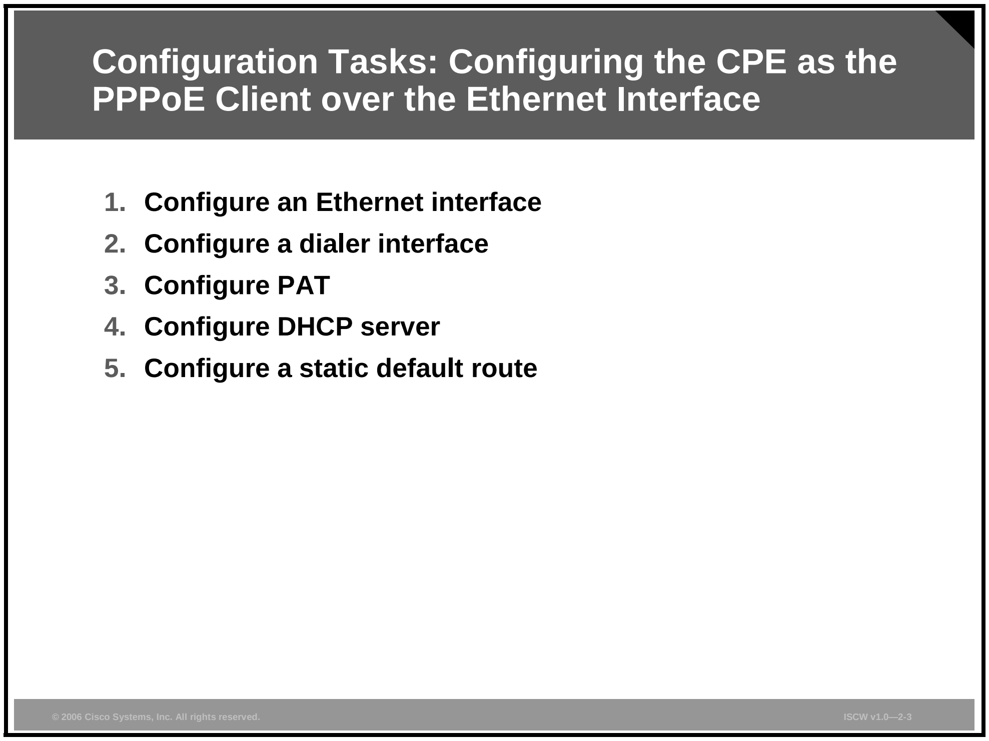
Upon completing this lesson, you will be able to configure the PPPoE client over DSL. This ability includes being able to meet these objectives:

- Configure a Cisco router as a PPPoE client
- Configure an ATM interface for PPPoE client operations
- Configure the PPPoE DSL dialer interface
- Configure PAT
- Describe how to configure a DHCP server to allocate an IP address to the users behind the client DSL router
- Configure a static route
- Review the output of various **debug** and **show** commands to verify the PPPoE operations
- Describe the step-by-step procedure to configure a PPPoA on the CPE router
- Configure the DSL ATM interface

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

Configuration of a Cisco Router as the PPPoE Client

This topic describes the configuration tasks that are required to configure a Cisco Systems router as a PPPoE client. Configuring DSL requires global and interface configuration commands.



Configuration Tasks: Configuring the CPE as the PPPoE Client over the Ethernet Interface

1. **Configure an Ethernet interface**
2. **Configure a dialer interface**
3. **Configure PAT**
4. **Configure DHCP server**
5. **Configure a static default route**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-3

Use the PPP over Ethernet (PPPoE) DSL configuration steps listed here in addition to dial-on-demand routing (DDR)-derived commands:

Step 1 Configure the Ethernet interface of the Cisco router with a PPPoE client configuration.

Step 2 Create and configure the dialer interface of the Cisco router for PPPoE with a negotiated IP address and a maximum transmission unit (MTU) size of 1492.

Step 3 Configure Port Address Translation (PAT) on the Cisco router to allow the sharing of the dynamic public IP address of the dialer interface.

Step 4 Configure the Cisco router to allow it to be the DHCP server for the end-user PCs behind it.

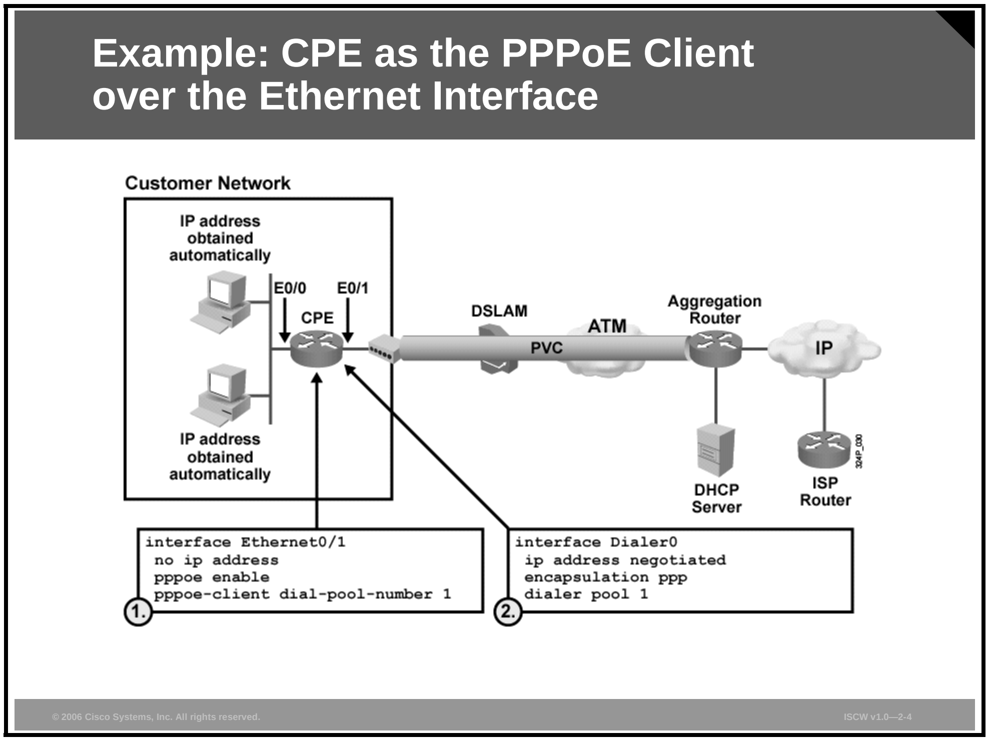
Step 5 Configure a static default route on the Cisco router.

Note Prior to Cisco IOS software Release 12.2(13)T, you had to first configure a PPPoE virtual private dialup network (VPDN) group before the steps described above. This was only done for PPPoE, not for PPP over ATM (PPPoA).

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

Example: CPE as the PPPoE Client over the Ethernet Interface

The figure shows a sample configuration for a CPE router acting as the PPPoE client.



Example: CPE as the PPPoE Client over the Ethernet Interface

1.

```
interface Ethernet0/1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
```

2.

```
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
```

© 2006 Cisco Systems, Inc. All rights reserved.

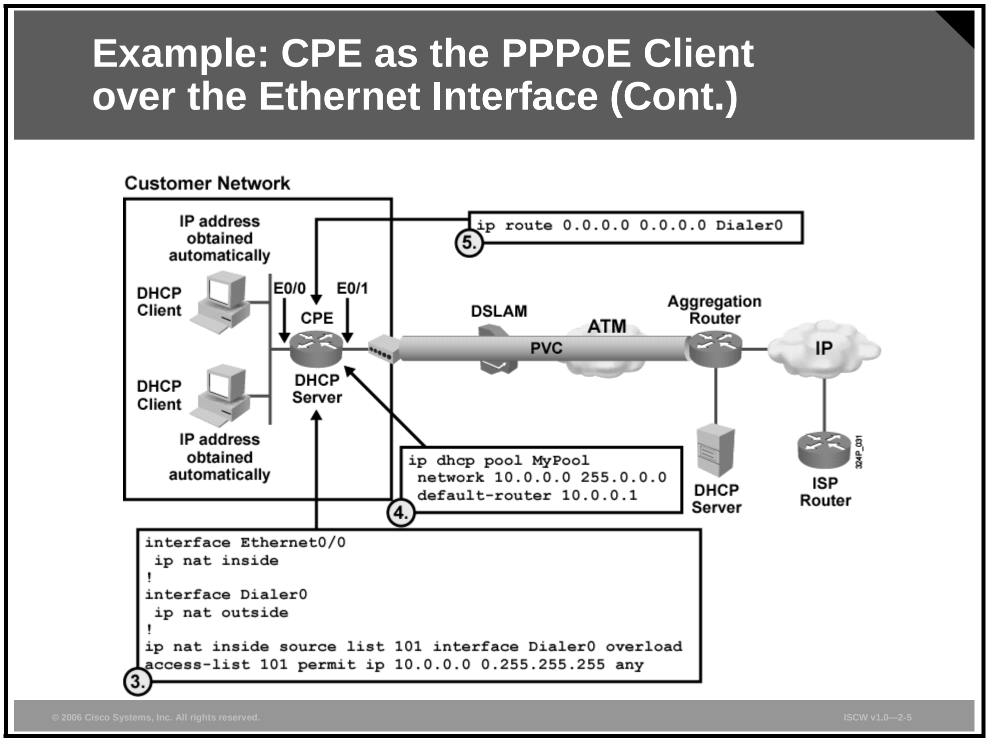
ISCW v1.0—2-4

The first two steps are as follows:

Step 1 Configure Ethernet interface.

Step 2 Configure dialer interface.

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



Example: CPE as the PPPoE Client over the Ethernet Interface (Cont.)

```
ip route 0.0.0.0 0.0.0.0 Dialer0
```

```
ip dhcp pool MyPool
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
```

```
interface Ethernet0/0
 ip nat inside
!
interface Dialer0
 ip nat outside
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
```

© 2006 Cisco Systems, Inc. All rights reserved.

The figure shows the remaining configuration steps for a CPE router acting as the PPPoE client:

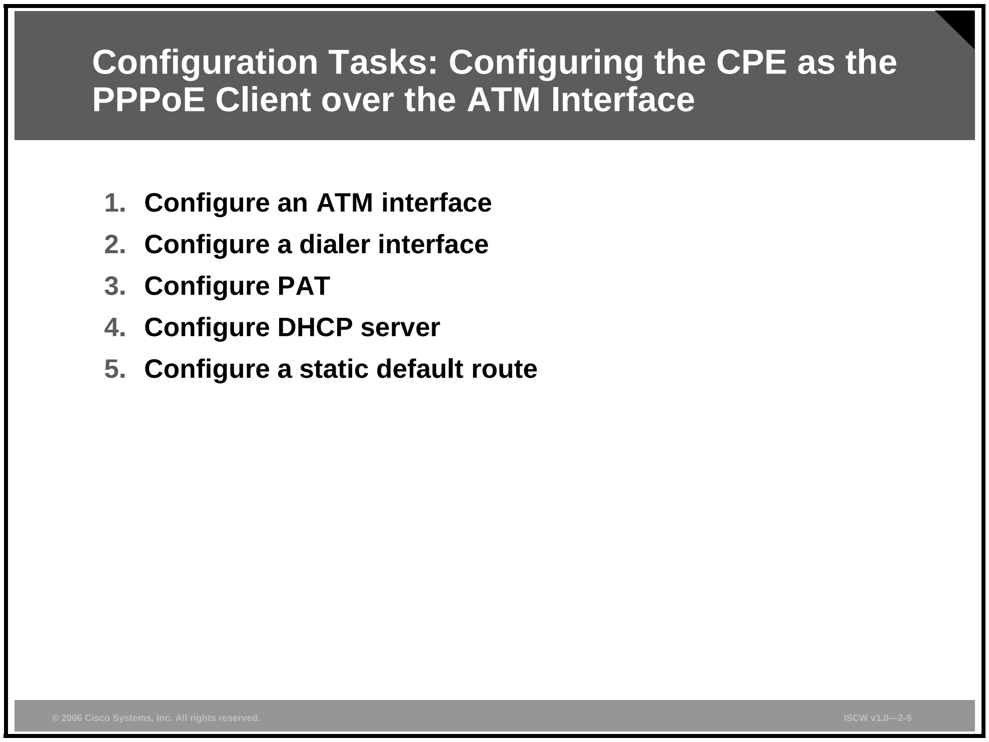
Step 3 Configure PAT.

Step 4 Enable a DHCP server on the router for clients in the customer network.

Step 5 Configure an IP default route.

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

Configuring the CPE as the PPPoE Client over the ATM Interface



Configuration Tasks: Configuring the CPE as the PPPoE Client over the ATM Interface

1. **Configure an ATM interface**
2. **Configure a dialer interface**
3. **Configure PAT**
4. **Configure DHCP server**
5. **Configure a static default route**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-6

Configuring the CPE as the PPPoE client over an ATM interface is very similar to configuring it over the Ethernet interface. The only difference is that you configure the ATM interface in the first step rather than an Ethernet interface.

Use the PPPoE DSL configuration steps listed here in addition to DDR-derived commands:

Step 1 Configure the ATM interface (asymmetric DSL [ADSL] interface) of the Cisco router with an ATM permanent virtual circuit (PVC) and encapsulation.

Step 2 Create and configure the dialer interface of the Cisco router for PPPoE with a negotiated IP address and an MTU size of 1492.

Step 3 Configure PAT on the Cisco router to allow the sharing of the dynamic public IP address of the dialer interface.

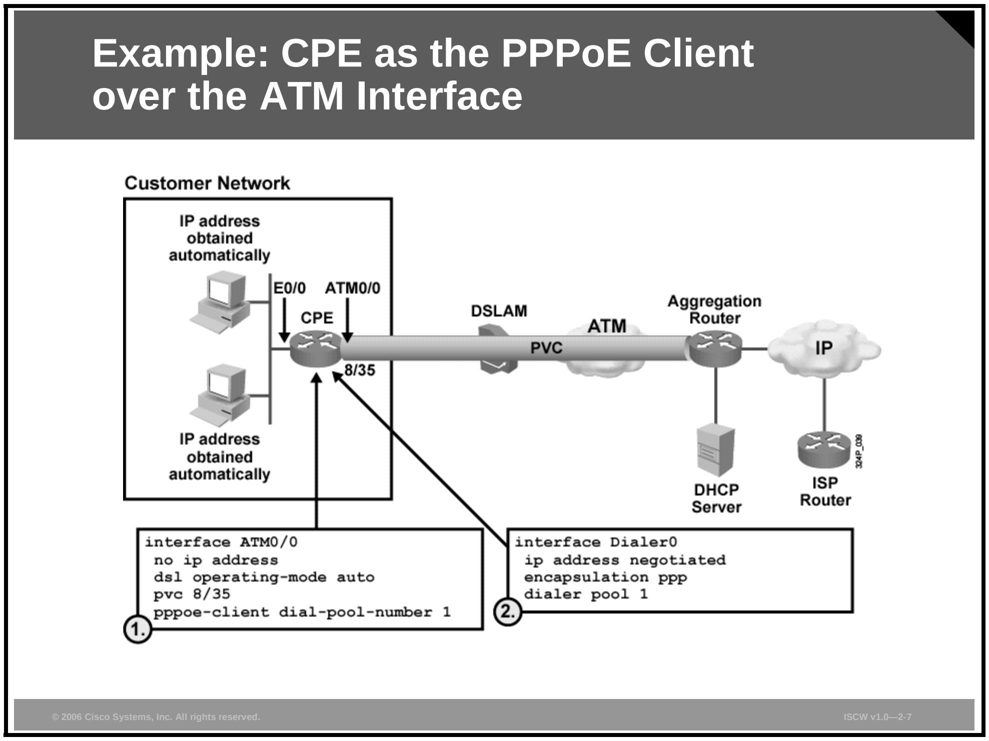
Step 4 Configure the Cisco router to allow it to be the DHCP server for the end-user PCs behind it.

Step 5 Configure a static default route on the Cisco 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 self-study.

Example: CPE as the PPPoE Client over the ATM Interface

The figure shows a sample configuration for a CPE router acting as the PPPoE client over an ATM interface.



Example: CPE as the PPPoE Client over the ATM Interface

Customer Network
IP address obtained automatically
E0/0
ATM0/0
CPE
8/35
IP address obtained automatically
DSLAM
PVC
ATM
Aggregation Router
IP
DHCP Server
ISP Router
324P_039
1.
2.
© 2006 Cisco Systems, Inc. All rights reserved.
ISCW v1.0—2-7

```
interface ATM0/0
 no ip address
 dsl operating-mode auto
 pvc 8/35
 pppoe-client dial-pool-number 1
```

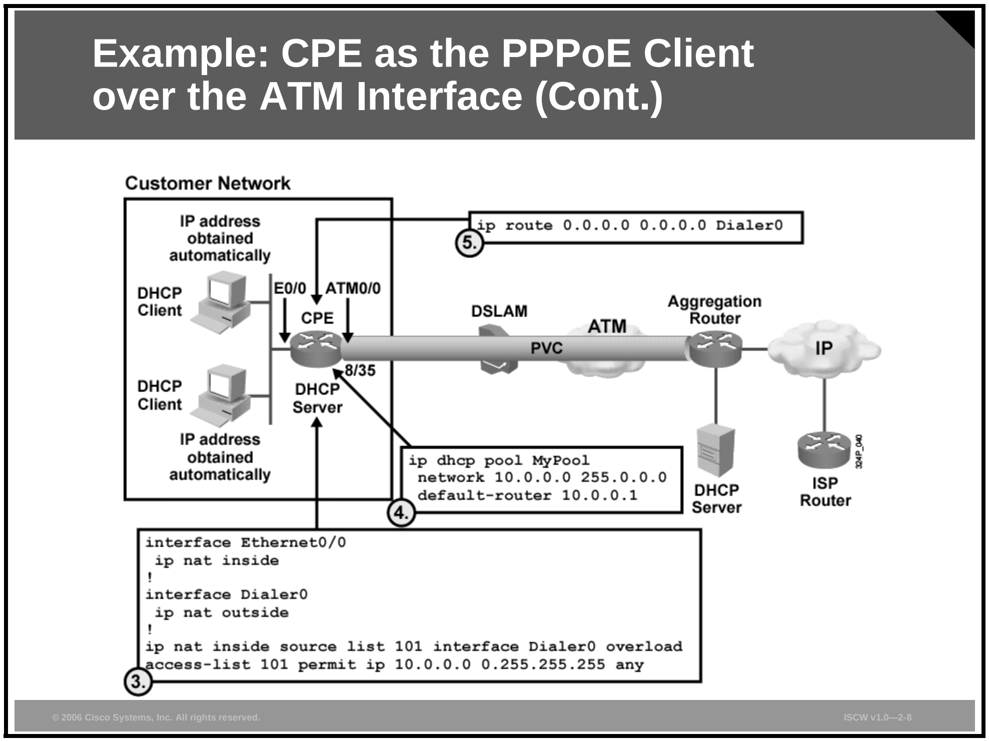
```
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
```

The first two steps are as follows:

Step 1 Configure ATM interface.

Step 2 Configure the dialer interface.

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



Example: CPE as the PPPoE Client over the ATM Interface (Cont.)

```
ip route 0.0.0.0 0.0.0.0 Dialer0
```

```
ip dhcp pool MyPool
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
```

```
interface Ethernet0/0
 ip nat inside
!
interface Dialer0
 ip nat outside
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-8

The figure shows the remaining configuration steps for a CPE router acting as the PPPoE client:

Step 3 Configure PAT.

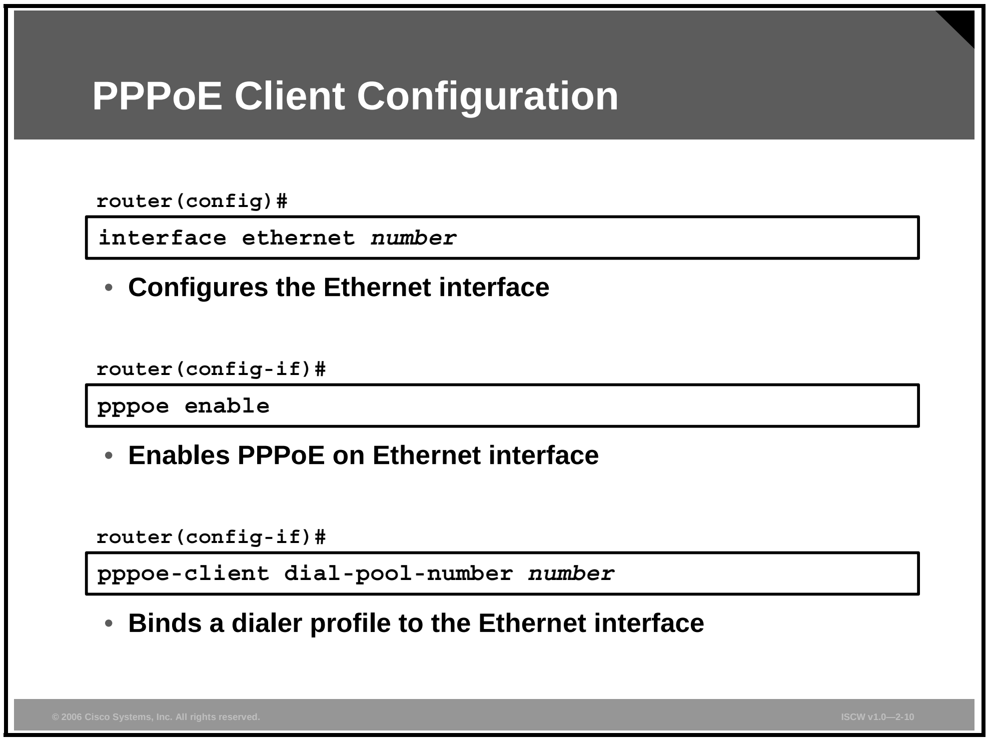
Step 4 Enable a DHCP server on the router for clients in the customer network.

Step 5 Configure an IP default route.

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

Configuration of a PPPoE Client

This topic describes how to configure a PPPoE client. After the PPPoE virtual private dialup network (VPDN) group has been defined, the ATM interface must be configured.



PPPoE Client Configuration

```
router(config)#
interface ethernet number
```

- **Configures the Ethernet interface**

```
router(config-if)#
pppoe enable
```

- **Enables PPPoE on Ethernet interface**

```
router(config-if)#
pppoe-client dial-pool-number number
```

- **Binds a dialer profile to the Ethernet interface**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-10

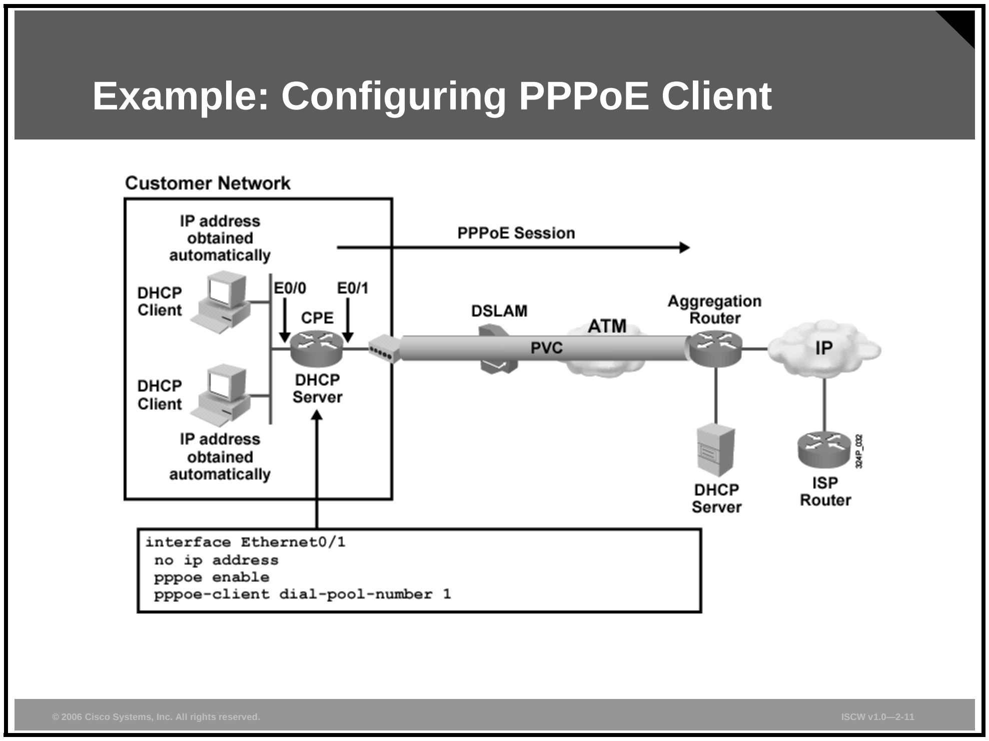
Configure the Ethernet interface (ADSL interface) of the Cisco router with an ATM PVC and encapsulation, as follows:

- To configure a PPPoE client on an Ethernet interface, use the **interface ethernet** command in global configuration mode to enter interface configuration mode.
- Next, enable the PPPoE on Ethernet interface.
- Finally, specify which dialer interface to use. Use the **pppoe-client dial-pool-number** command to bind the Ethernet interface to a dialer interface to set the encapsulation to PPPoE client.

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

Example: Configuring PPPoE Client

To configure a PPPoE client on a router, use the configuration example shown in the figure.



Example: Configuring PPPoE Client

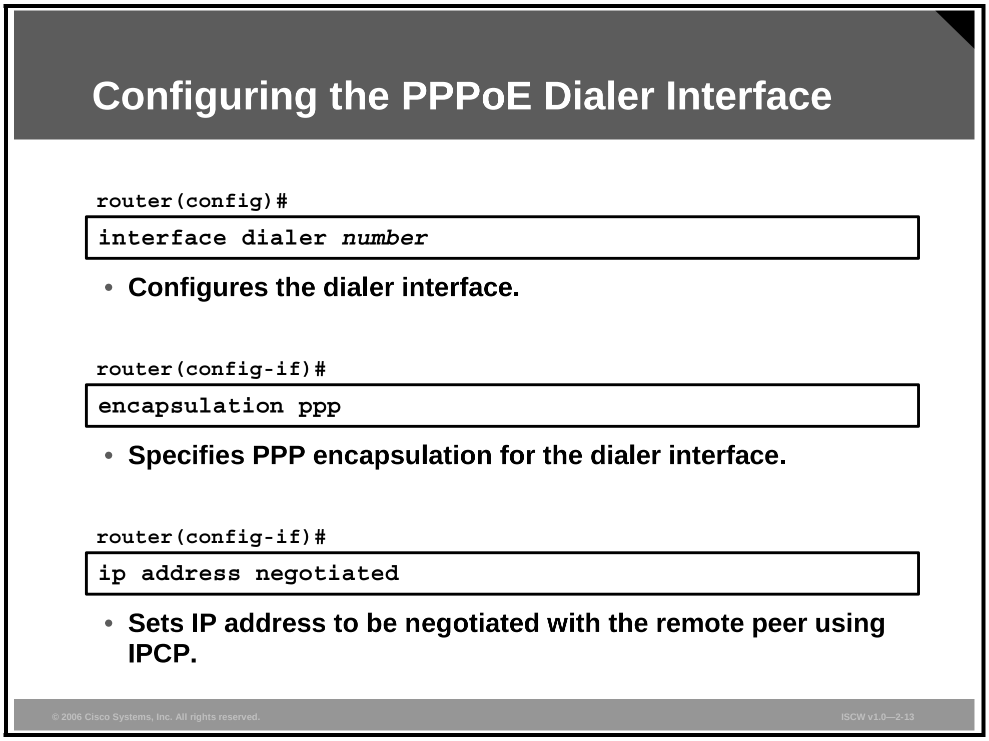
```
interface Ethernet0/1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
```

© 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 self-study.

Configuration of the PPPoE DSL Dialer Interface

This topic describes the commands that are required to configure a DSL dialer interface. After the ATM interface has been configured, the dialer interface must be configured.



Configuring the PPPoE Dialer Interface

```
router(config)#
interface dialer number
```

- **Configures the dialer interface.**

```
router(config-if)#
encapsulation ppp
```

- **Specifies PPP encapsulation for the dialer interface.**

```
router(config-if)#
ip address negotiated
```

- **Sets IP address to be negotiated with the remote peer using IPCP.**

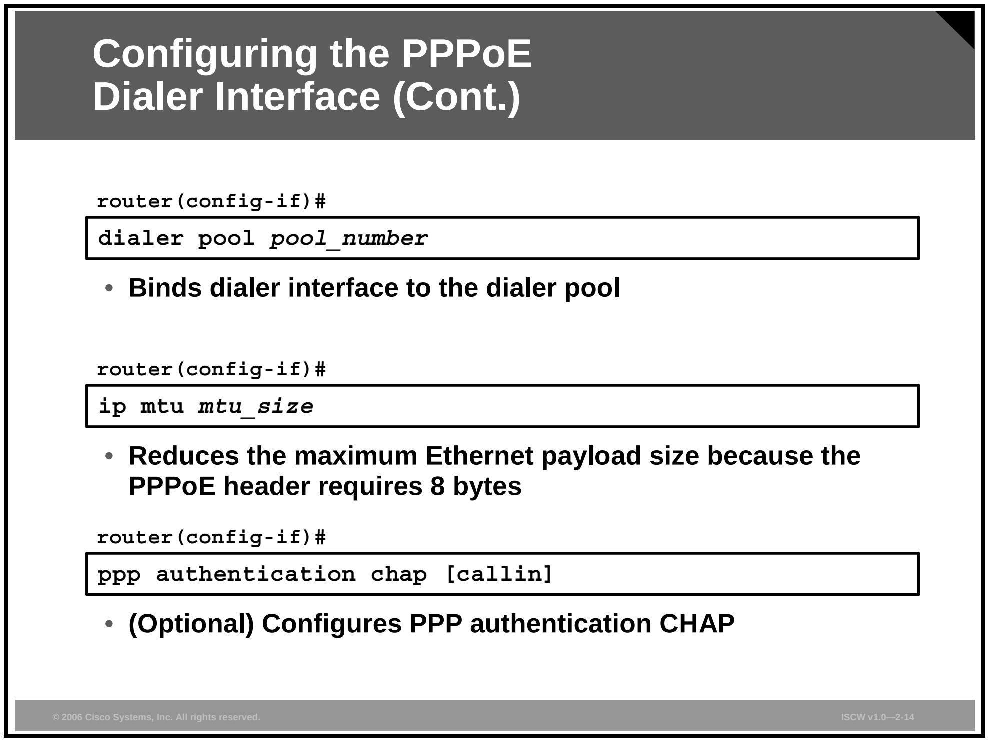
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-13

Use the commands in the table for PPPoE DSL dialer configuration.

Dialer Commands for DSL

Command	Description
`ip address negotiated`	Enables a dynamic address from the service provider using IP Control Protocol (IPCP). With IPCP, DSL routers automatically negotiate a globally unique (registered or public) IP address for the dialer interface from the service provider aggregation router.
`encapsulation ppp`	Specifies PPP encapsulation for the dialer interface.
`no cdp enable`	Stops Cisco Discovery Protocol (CDP) advertisements from going out the dialer interface.

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



Configuring the PPPoE Dialer Interface (Cont.)

```
router(config-if)#
dialer pool pool_number
```

- **Binds dialer interface to the dialer pool**

```
router(config-if)#
ip mtu mtu_size
```

- **Reduces the maximum Ethernet payload size because the PPPoE header requires 8 bytes**

```
router(config-if)#
ppp authentication chap [callin]
```

- **(Optional) Configures PPP authentication CHAP**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-14

Use the additional commands in the table for PPPoE DSL dialer configuration.

Additional Dialer Commands for DSL

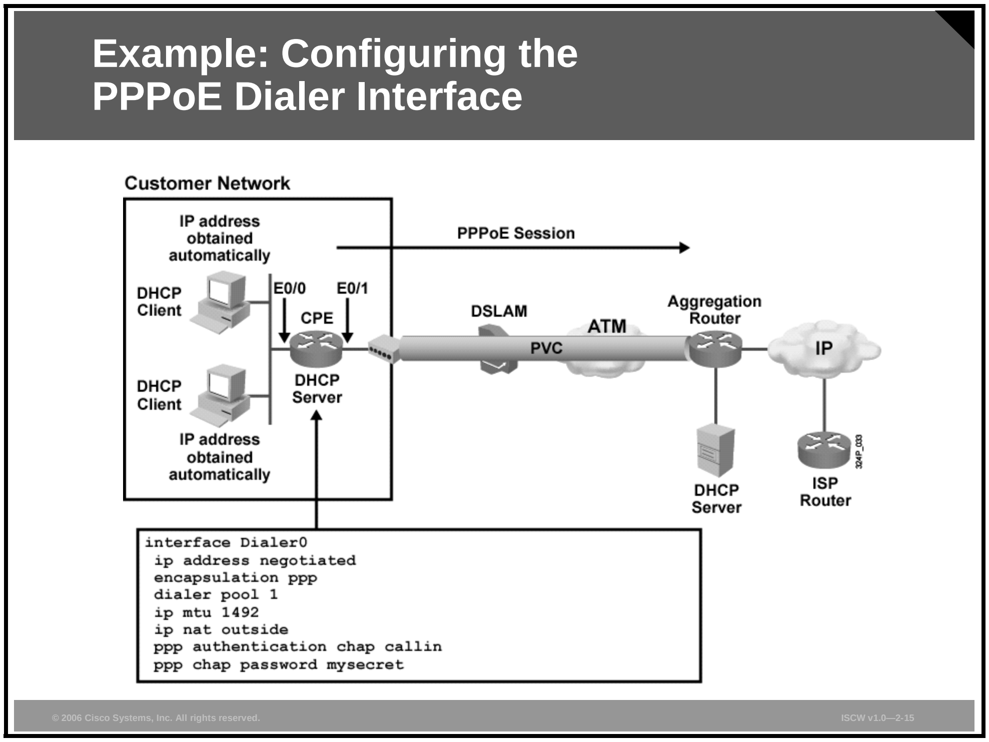
Command	Description
`dialer pool` *`pool_number`*	Specifies to which pool the dialer interface is assigned.
`ip mtu` *`mtu_size`*	Sets the maximum Ethernet payload size. Reduces the MTU size from 1500 to 1492, because the PPPoE header plus PPP protocol ID require eight bytes.
`ppp authentication chap [callin]`	(Optional) Configures the Challenge Handshake Authentication Protocol (CHAP). With the keyword **callin**, the access server will only authenticate the remote device if the remote device initiated the call.

Note Unlike an ISDN DDR configuration, DSL is always *on*. Therefore, a dialer list is not required to identify interesting 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 self-study.

Example: Configuring the PPPoE Dialer Interface

Use this configuration example to configure a PPPoE dialer interface on the router.



Example: Configuring the PPPoE Dialer Interface

```
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ip mtu 1492
 ip nat outside
 ppp authentication chap callin
 ppp chap password mysecret
```

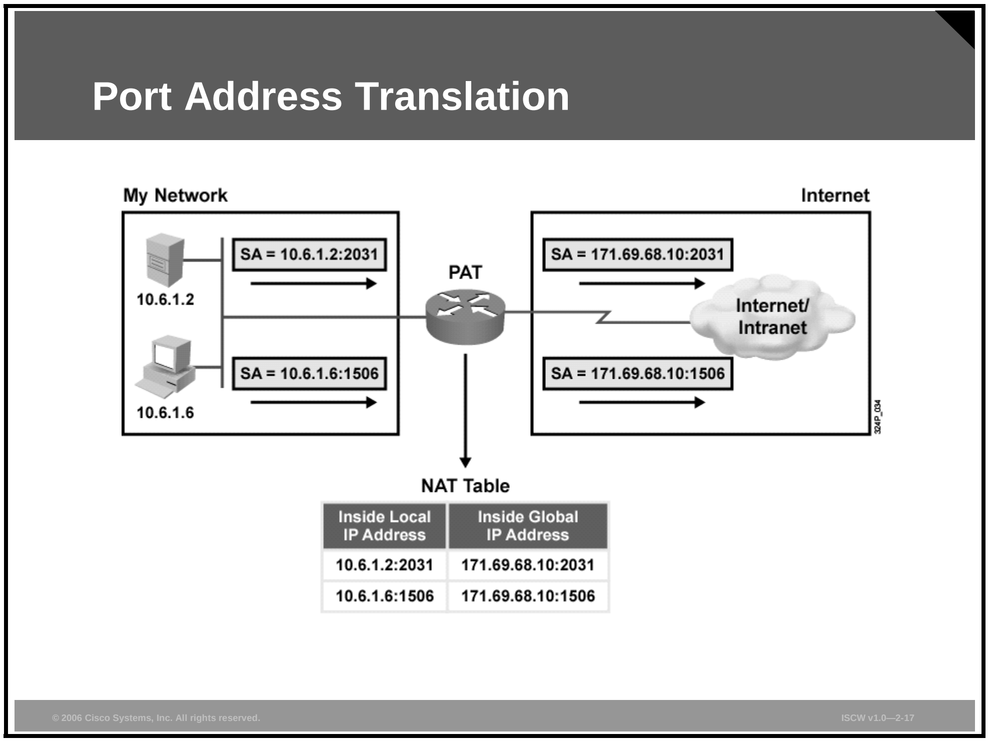
© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-15

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

Configuration of PAT

This topic describes how to configure addressing translations using PAT.



Port Address Translation

NAT Table

Inside Local IP Address	Inside Global IP Address
10.6.1.2:2031	171.69.68.10:2031
10.6.1.6:1506	171.69.68.10:1506

© 2006 Cisco Systems, Inc. All rights reserved.

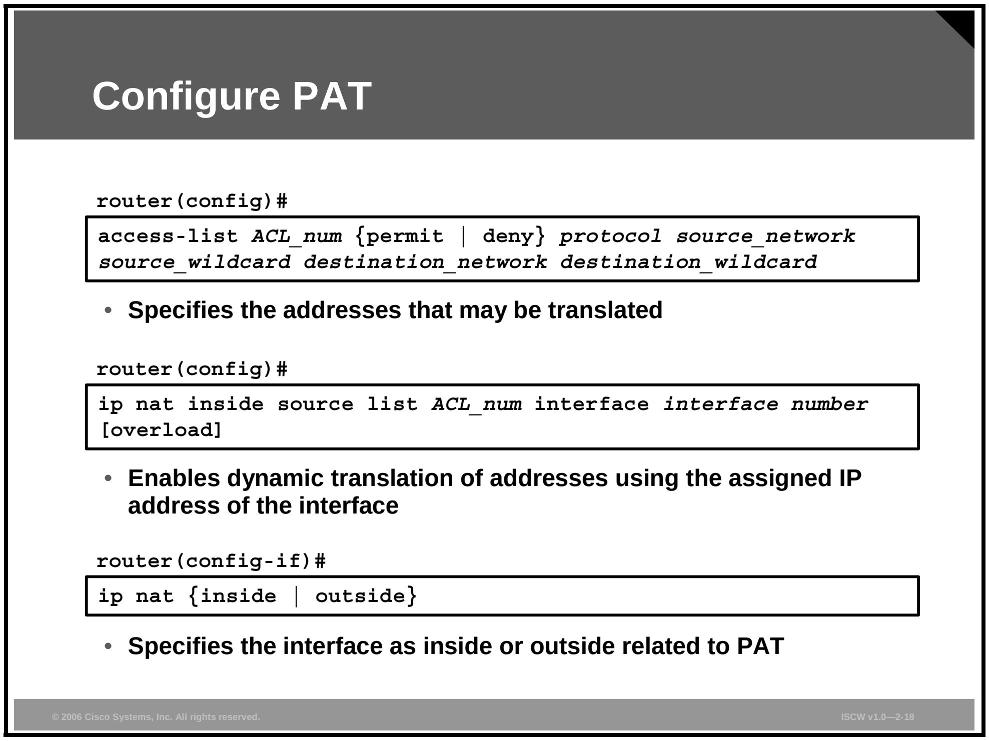
One of the main features of Network Address Translation (NAT) is static PAT, which is also referred to as overload in Cisco IOS configuration. You can translate several internal addresses using NAT into just one or a few external addresses by using PAT.

PAT uses unique source port numbers on the inside global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number of internal addresses that NAT can translate into one external address is, theoretically, as many as 65,536. PAT attempts to preserve the original source port. If the source port is already allocated, PAT attempts to find the first available port number. It starts from the beginning of the appropriate port group, 0–511, 512–1023, or 1024–65,535. If PAT does not find a port that is available from the appropriate port group and if more than one external IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. PAT continues trying to allocate the original source port until it runs out of available ports and external IP addresses.

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

Configure PAT

NAT overload, commonly referred to as PAT, and PPP and IPCP are popular techniques used to scale limited addresses.



Configure PAT

```
router(config)#
```

```
access-list ACL_num {permit | deny} protocol source_network
source_wildcard destination_network destination_wildcard
```

- **Specifies the addresses that may be translated**

```
router(config)#
```

```
ip nat inside source list ACL_num interface interface number
[overload]
```

- **Enables dynamic translation of addresses using the assigned IP address of the interface**

```
router(config-if)#
```

```
ip nat {inside | outside}
```

- **Specifies the interface as inside or outside related to PAT**

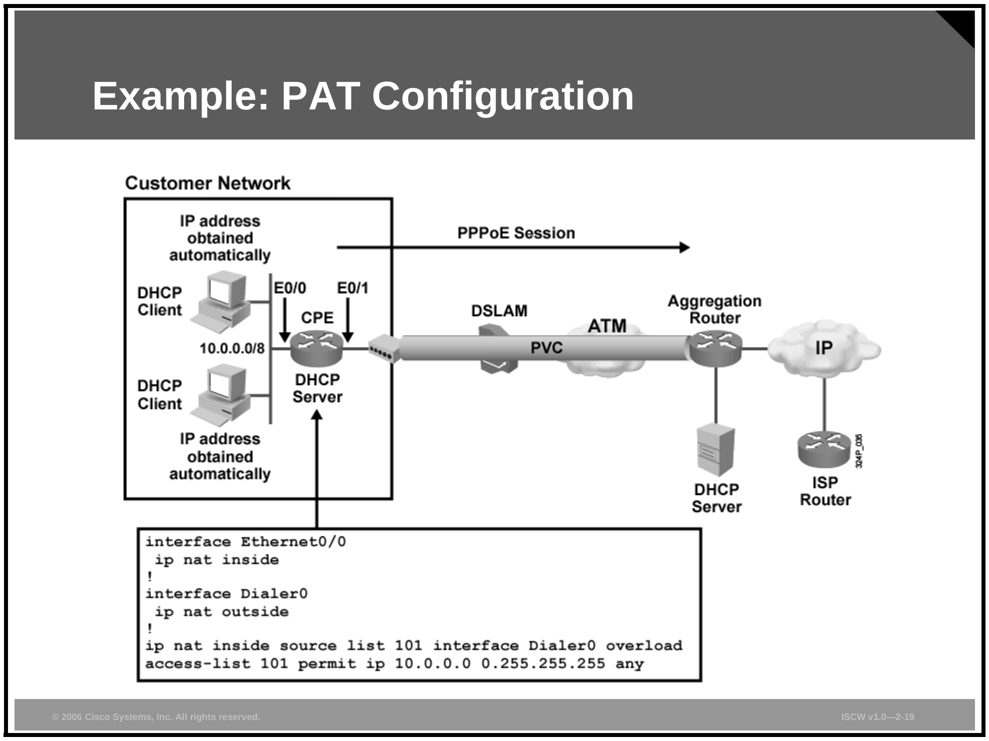
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-18

Using NAT overload means that you can share the one registered IP address of the public interface for all the devices behind the PAT router to access the Internet.

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

Example: PAT Configuration

The figure illustrates a sample PAT configuration on the Cisco router.



Example: PAT Configuration

```
interface Ethernet0/0
 ip nat inside
!
interface Dialer0
 ip nat outside
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-19

The access list will match any source address in the 10.0.0.0/8 network.

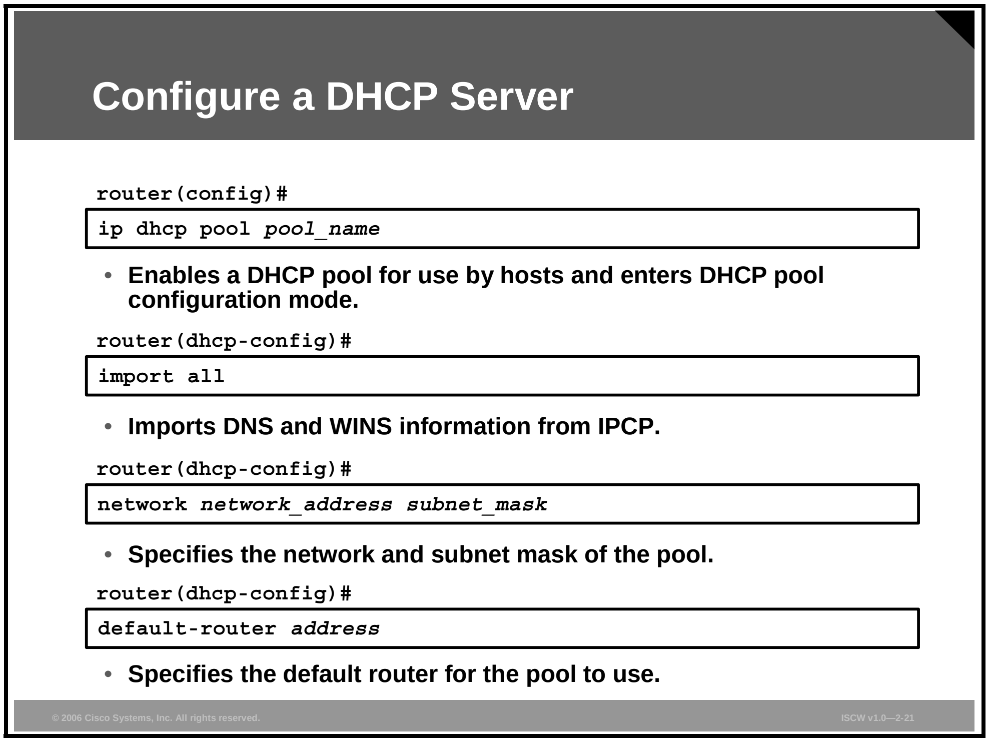
In this example, the Dialer0 interface is the outside interface, and the Ethernet0/0 interface is the inside interface.

The 10.x.x.x source addresses will be translated using PAT to the Dialer0 IP address. The Dialer0 interface receives its IP address from the service provider aggregation router using IPCP.

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

Configuration of DHCP to Scale DSL

This topic describes how to scale DSL by configuring a DHCP server on the client DSL router.



Configure a DHCP Server

```
router(config)#
ip dhcp pool pool_name
```

- **Enables a DHCP pool for use by hosts and enters DHCP pool configuration mode.**

```
router(dhcp-config)#
import all
```

- **Imports DNS and WINS information from IPCP.**

```
router(dhcp-config)#
network network_address subnet_mask
```

- **Specifies the network and subnet mask of the pool.**

```
router(dhcp-config)#
default-router address
```

- **Specifies the default router for the pool to use.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-21

The Cisco IOS DHCP Server feature is a full implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client.

The Cisco IOS DHCP Server was enhanced to allow configuration information to be updated automatically. Network administrators can configure one or more centralized DHCP servers to update specific DHCP options within the DHCP pools. The remote servers can request or “import” these option parameters from the centralized servers.

To configure a DHCP address pool on a Cisco IOS DHCP Server and enter DHCP pool configuration mode, use the **ip dhcp pool** global configuration command.

To import DHCP option parameters into the Cisco IOS DHCP Server database, use the **import all** DHCP pool configuration command.

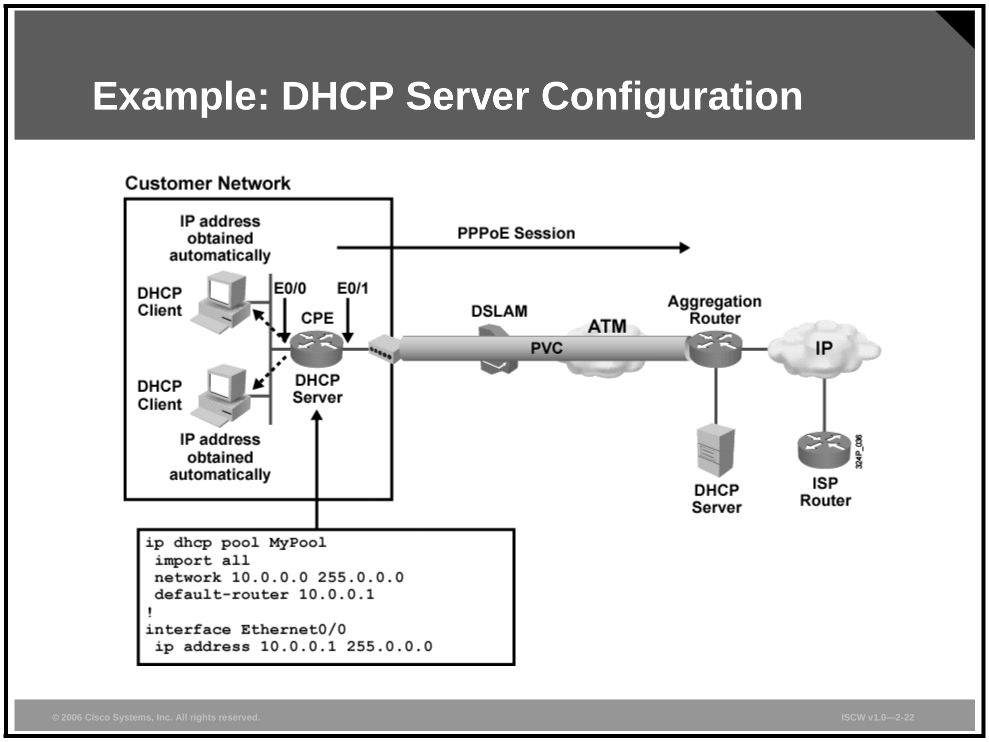
To configure the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP Server, use the **network** DHCP pool configuration command.

To specify the default router list for a DHCP client, use the **default-router** DHCP pool configuration command. Note that the DHCP server excludes this address from the pool of assignable addresses.

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

Example: Configuring a DHCP Server

This example describes how to configure the Cisco router as the DHCP server for the end-user PCs behind the router Ethernet interface.



Example: DHCP Server Configuration

```
ip dhcp pool MyPool
 import all
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
!
interface Ethernet0/0
 ip address 10.0.0.1 255.0.0.0
```

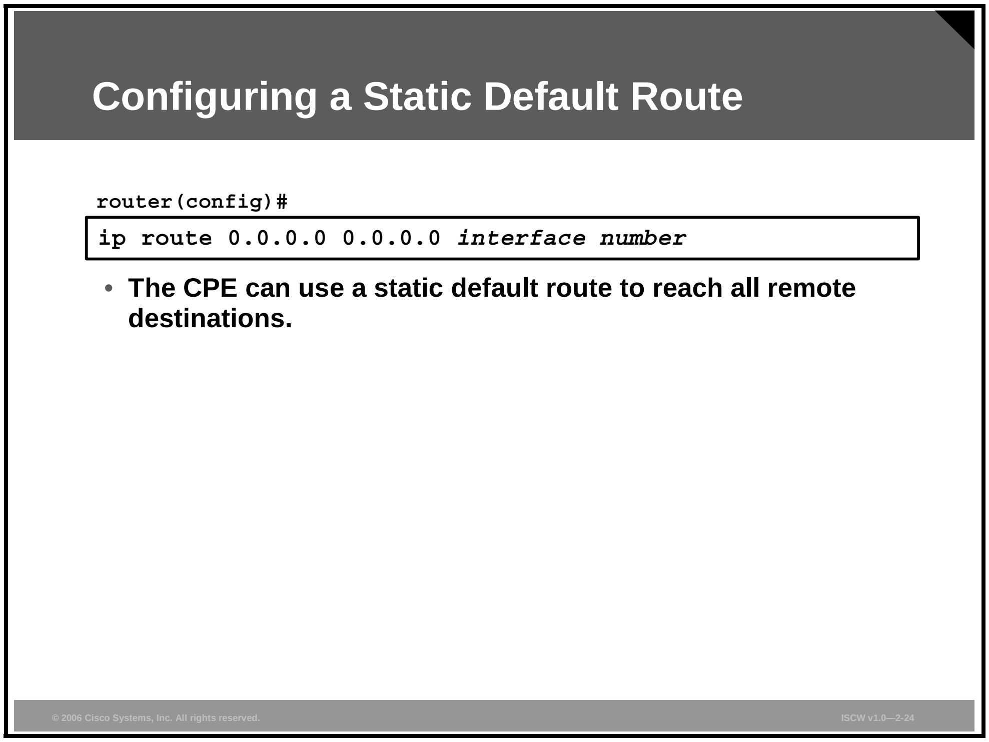
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-22

In this example, a DHCP address pool with the name *MyPool* is configured. The CPE router will act like a DHCP server to the hosts, connected to the Ethernet 0/0 interface. Hosts will get IP addresses from range 10.0.0.2 to 10.255.255.254 with the subnet mask 255.0.0.0. The IP address 10.0.0.1 is excluded from this range, because it is already used on the router interface. Hosts will get a default route pointing to the router interface IP address 10.0.0.1, and other parameters that the router gets from the aggregation router, such as Domain Name System (DNS) and Windows Internet Naming Service (WINS) setup.

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

Configuration of a Static Default Route

This topic describes how to configure a static default route pointing to the dialer interface.



Configuring a Static Default Route

```
router(config)#
ip route 0.0.0.0 0.0.0.0 interface number
```

- **The CPE can use a static default route to reach all remote destinations.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-24

You can configure a static default route on a Cisco router to allow the router to reach all unknown destinations toward the dialer interface. In most DSL installations, the CPE will not be running a dynamic routing protocol to the aggregation router of the service provider. Therefore, a static default route is required on a Cisco router.

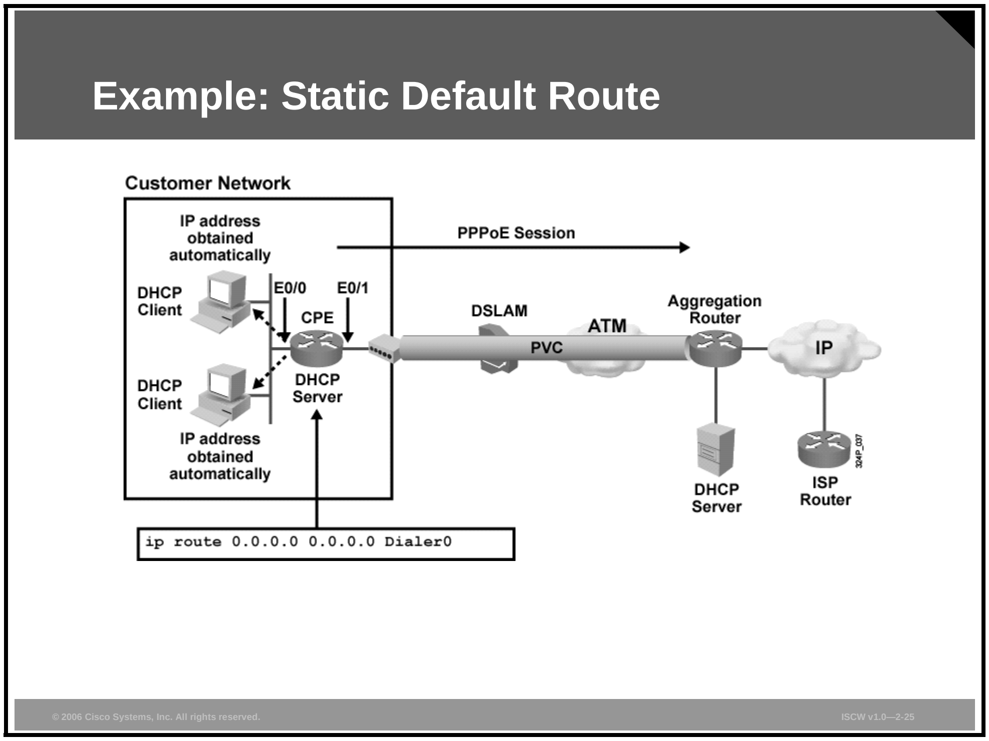
When a PPPoE session has been established between a Cisco router and the aggregation router of the service provider, the dialer interface IP address is assigned from the service provider aggregation router via IPCP. The service provider aggregation router will automatically build a /32 host route to reach the Cisco router dialer interface.

To configure a static default route on a Cisco router, enter global configuration mode and use the **ip route 0.0.0.0 0.0.0.0** command. The interface in this example is Dialer0 connected to the external 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 self-study.

Example: Configuring a Static Default Route

This example describes how to configure a static default route on a Cisco router.



Example: Static Default Route

```
ip route 0.0.0.0 0.0.0.0 Dialer0
```

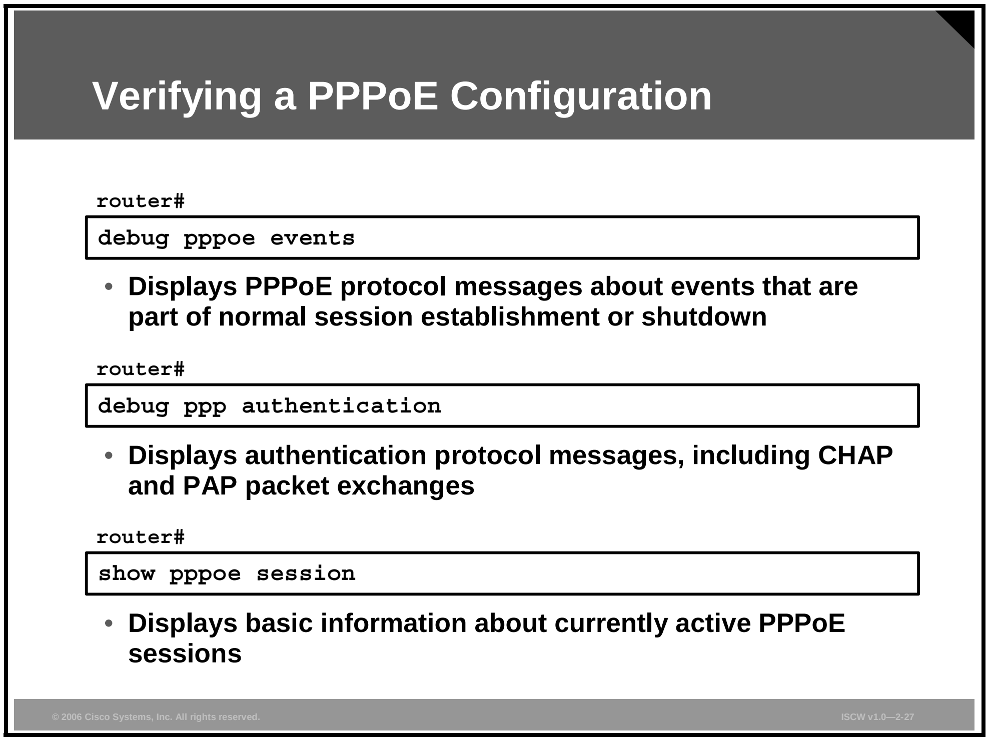
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-25

In this example, a static default route points to a Dialer0 interface, which is used for a PPPoE connection.

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

Verifying a PPPoE Configuration

This topic describes verification of a PPPoE configuration and provides an example of a complete PPPoE configuration.



Verifying a PPPoE Configuration

```
router#
debug pppoe events
```

- **Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown**

```
router#
debug ppp authentication
```

- **Displays authentication protocol messages, including CHAP and PAP packet exchanges**

```
router#
show pppoe session
```

- **Displays basic information about currently active PPPoE sessions**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-27

To verify proper PPPoE session establishment and PPP authentication, use the **debug** commands in the table.

Cisco IOS debug Commands

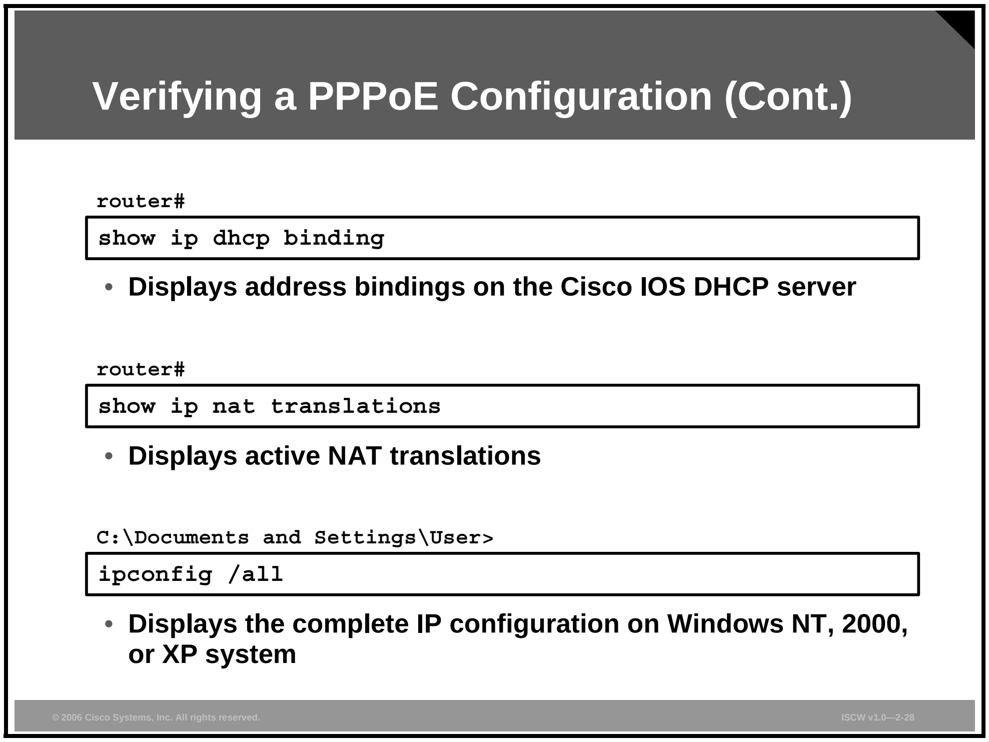
Command	Description
`debug pppoe events`	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown
`debug ppp authentication`	Displays authentication protocol messages, including CHAP and Password Authentication Protocol (PAP) packet exchanges

Note Prior to Cisco IOS software Release 12.2(13)T, the command used to display the PPPoE protocol session establishment or shutdown messages was **debug vpdn pppoe-events**.

Cisco IOS show Command

Command	Description
`show pppoe session`	Displays basic information about currently active PPPoE sessions.

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



Verifying a PPPoE Configuration (Cont.)

```
router#
show ip dhcp binding
```

- **Displays address bindings on the Cisco IOS DHCP server**

```
router#
show ip nat translations
```

- **Displays active NAT translations**

```
C:\Documents and Settings\User>
ipconfig /all
```

- **Displays the complete IP configuration on Windows NT, 2000, or XP system**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-28

To verify proper PPPoE configuration, DHCP setup, and NAT configuration, use the commands in the tables.

Additional Cisco IOS show Commands

Command	Description
`show ip dhcp binding`	Displays address bindings on the Cisco IOS DHCP server
`show ip nat translations`	Displays active NAT translations

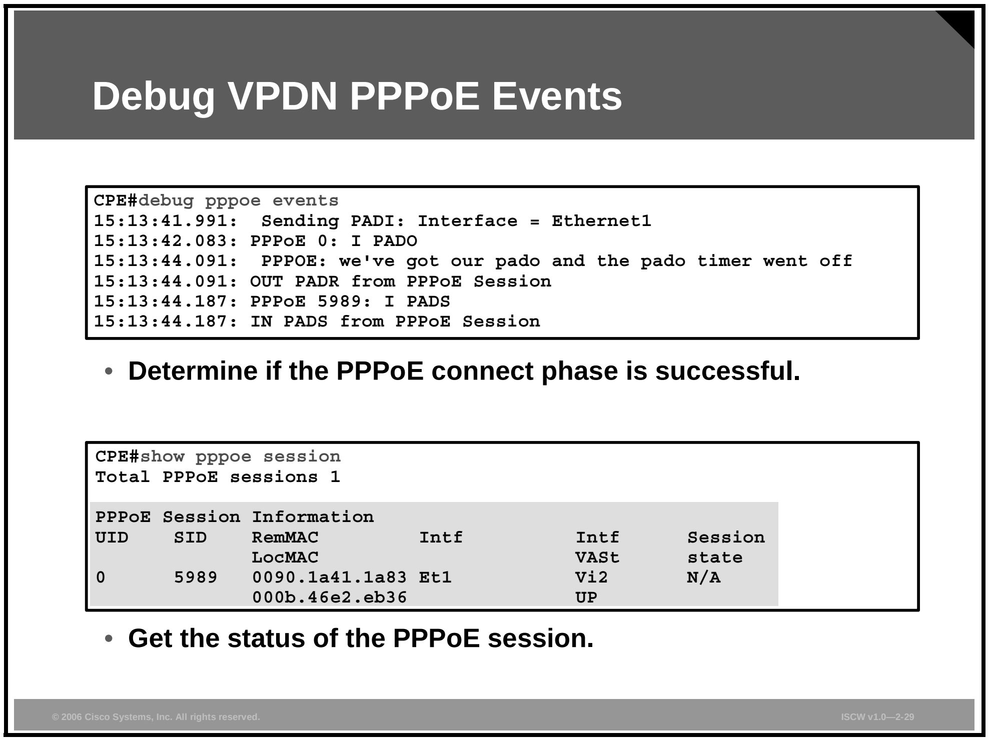
Windows NT, 2000, and XP Command

Command	Description
`ipconfig /all`	Displays the complete IP configuration on Windows NT, 2000, and XP systems including IP address, network mask, default gateway, DNS, etc.

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

Debug PPPoE Events

Use the VPDN PPPoE **debug** commands to determine if the PPPoE connect phase is successful.



Debug VPDN PPPoE Events

```
CPE#debug pppoe events
15:13:41.991:  Sending PADI: Interface = Ethernet1
15:13:42.083: PPPoE 0: I PADO
15:13:44.091:  PPPOE: we've got our pado and the pado timer went off
15:13:44.091: OUT PADR from PPPoE Session
15:13:44.187: PPPoE 5989: I PADS
15:13:44.187: IN PADS from PPPoE Session
```

- **Determine if the PPPoE connect phase is successful.**

```
CPE#show pppoe session
Total PPPoE sessions 1

PPPoE Session Information
UID    SID    RemMAC         Intf          Intf      Session
              LocMAC                       VASt      state
0      5989   0090.1a41.1a83 Et1           Vi2       N/A
              000b.46e2.eb36               UP
```

- **Get the status of the PPPoE session.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-29

The significant fields shown in the output are:

- **15:13:41.991: Sending PADI: Interface = Ethernet1:** A broadcast Ethernet frame that requests a PPPoE server.
- **15:13:44.091: PPPOE: we've got our pado and the pado timer went off:** This is a unicast reply from a PPPoE server (similar to a DHCP offer).
- **15:13:44.091: OUT PADR from PPPoE Session:** This is a unicast reply that accepts the offer.
- **15:13:44.187: IN PADS from PPPoE Session:** This is a confirmation and the establishment completes.

After the PPPoE session is established, use the **show pppoe session** command in order to get the status.

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

Debug PPP Authentication

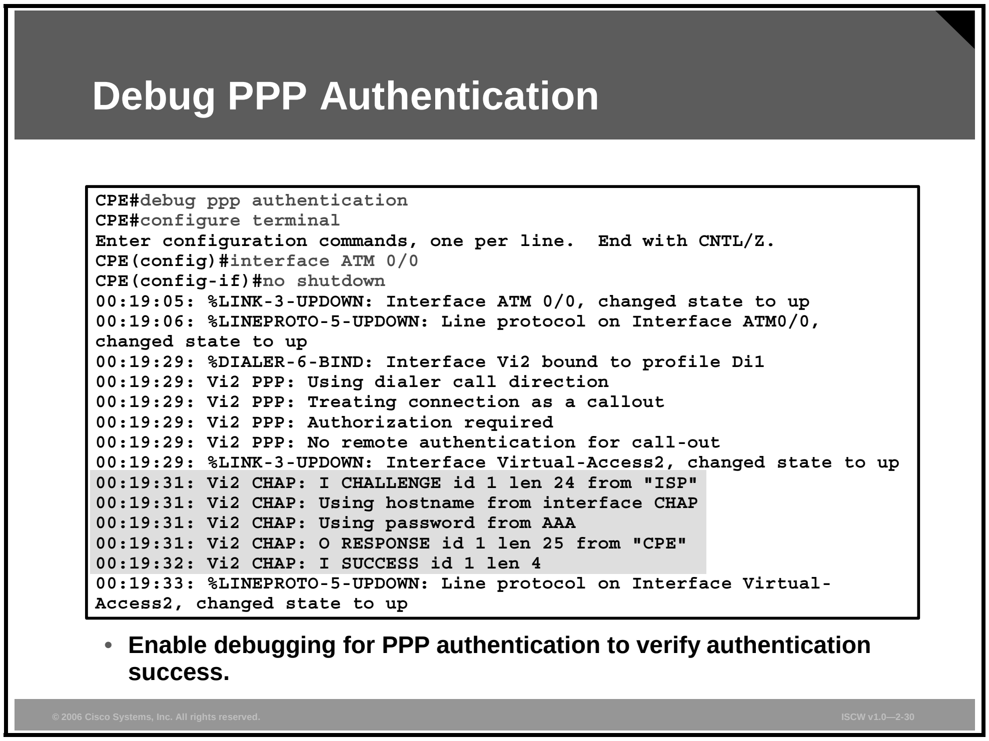
To verify PPP authentication success, follow these steps:

Step 1 Enable PPP authentication debugging with the **debug ppp authentication** command.

Step 2 Enable an external ATM interface on the router.

Step 3 Observe debugging messages on the router. CHAP authentication should be successful, as it is shown in the printout.

Step 4 Disable debugging with the **no debug ppp authentication** command.



Debug PPP Authentication

```
CPE#debug ppp authentication
CPE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CPE(config)#interface ATM 0/0
CPE(config-if)#no shutdown
00:19:05: %LINK-3-UPDOWN: Interface ATM 0/0, changed state to up
00:19:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0,
changed state to up
00:19:29: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
00:19:29: Vi2 PPP: Using dialer call direction
00:19:29: Vi2 PPP: Treating connection as a callout
00:19:29: Vi2 PPP: Authorization required
00:19:29: Vi2 PPP: No remote authentication for call-out
00:19:29: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
00:19:31: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
00:19:31: Vi2 CHAP: Using hostname from interface CHAP
00:19:31: Vi2 CHAP: Using password from AAA
00:19:31: Vi2 CHAP: O RESPONSE id 1 len 25 from "CPE"
00:19:32: Vi2 CHAP: I SUCCESS id 1 len 4
00:19:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access2, changed state to up
```

- **Enable debugging for PPP authentication to verify authentication success.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-30

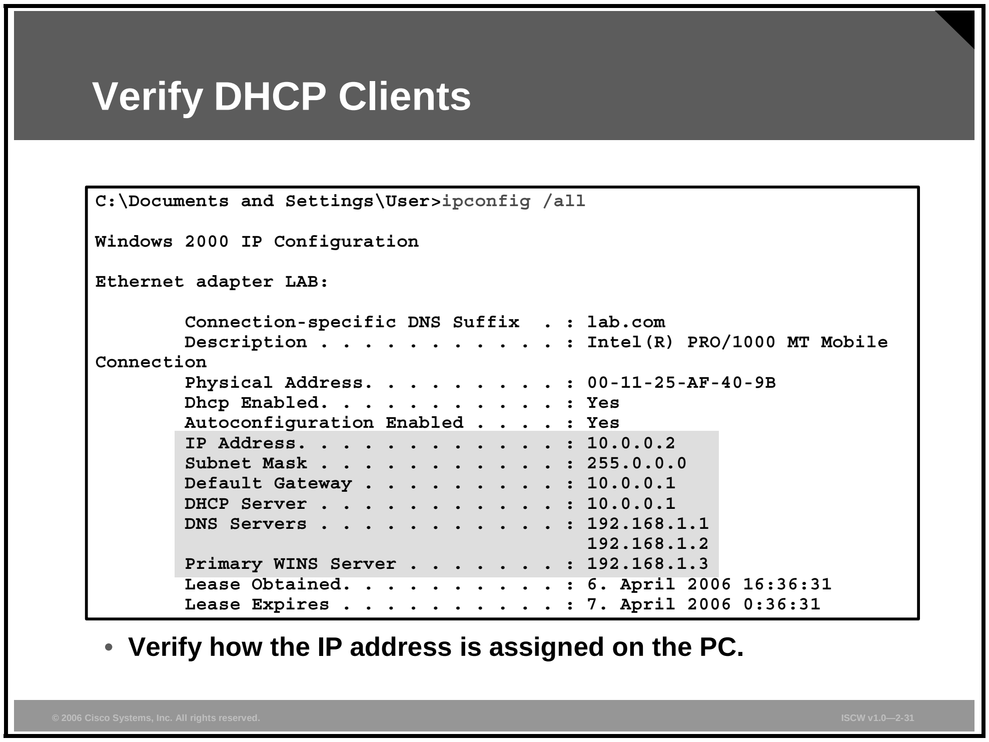
If CHAP authentication is successful, verify the connectivity from your router toward an IP address on the Internet.

The DSL connection is established to the ISP router and will stay up permanently. The CHAP authentication verifies the identity of the remote node using a three-way handshake at the establishment of the session and periodically during the session.

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

Verify DHCP Clients

Verify how the IP address is assigned on the PC.



Verify DHCP Clients

```
C:\Documents and Settings\User>ipconfig /all

Windows 2000 IP Configuration

Ethernet adapter LAB:

        Connection-specific DNS Suffix  . : lab.com
        Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Mobile
Connection
        Physical Address. . . . . . . . . : 00-11-25-AF-40-9B
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.0.0.2
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . : 10.0.0.1
        DHCP Server . . . . . . . . . . . : 10.0.0.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1
                                            192.168.1.2
        Primary WINS Server . . . . . . . : 192.168.1.3
        Lease Obtained. . . . . . . . . . : 6. April 2006 16:36:31
        Lease Expires . . . . . . . . . . : 7. April 2006 0:36:31
```

- **Verify how the IP address is assigned on the PC.**

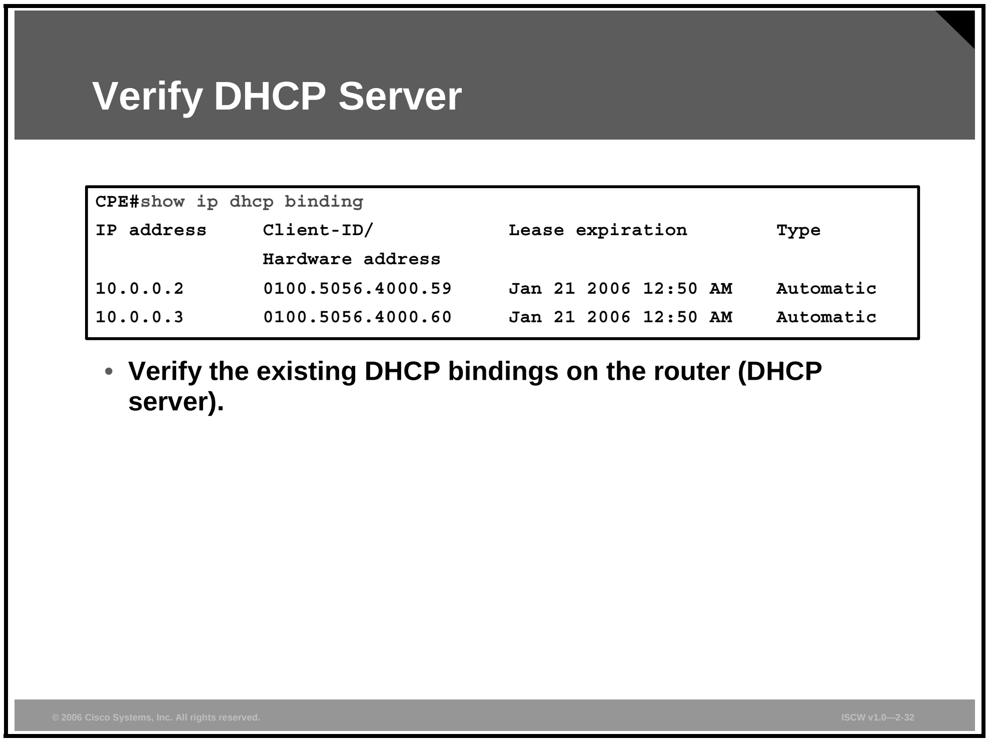
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-31

Open the command prompt on the PC and check the IP setup. The output of the **ipconfig** command on the PC confirms that the PC has obtained the IP address (10.0.0.2), subnet mask (255.0.0.0), default gateway address (10.0.0.1), DNS servers (192.168.1.1 and 192.168.1.2), and WINS server (192.168.1.3) from the DHCP 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 self-study.

Verify DHCP Server

To verify the existing automatic and manual DHCP bindings on the router, use the **show ip dhcp binding** command.



Verify DHCP Server

```
CPE#show ip dhcp binding
IP address     Client-ID/            Lease expiration        Type
               Hardware address
10.0.0.2       0100.5056.4000.59     Jan 21 2006 12:50 AM    Automatic
10.0.0.3       0100.5056.4000.60     Jan 21 2006 12:50 AM    Automatic
```

- **Verify the existing DHCP bindings on the router (DHCP server).**

© 2006 Cisco Systems, Inc. All rights reserved.

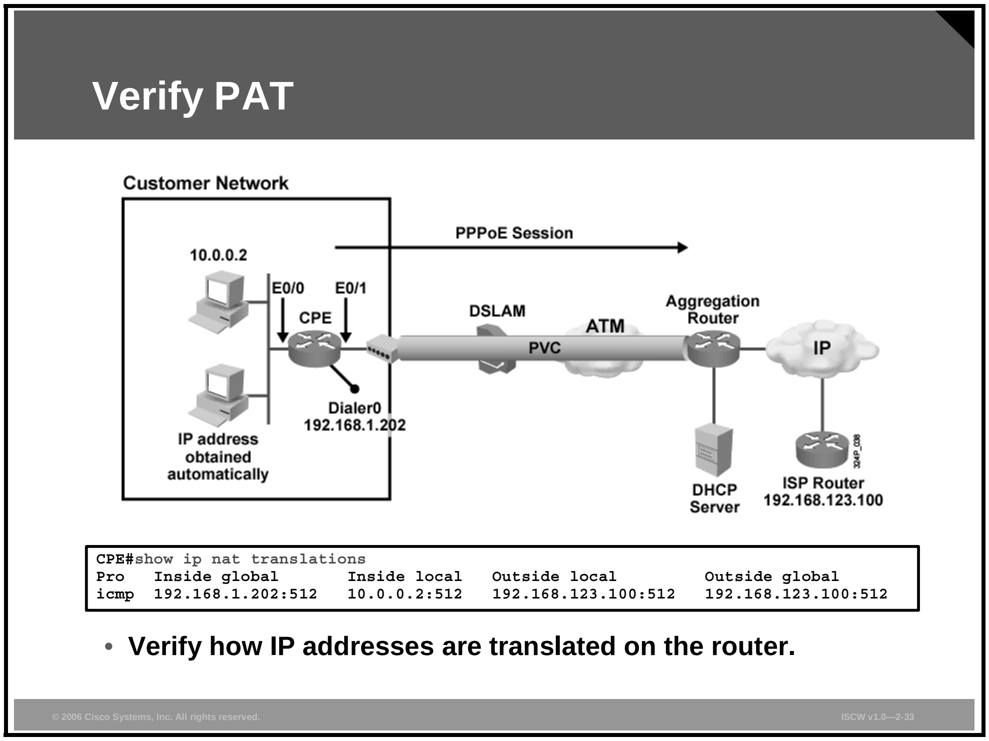
The output shows the mapping between the IP address, assigned to the DHCP client, and the hardware address (client ID), which belongs to the host. Lease expiration shows how long this mapping is valid. After expiration, the DHCP server will send a new binding, which can be the same or a different IP address. Type defines whether the binding was automatically or manually set.

The client ID is composed from media type, which is Ethernet, with code **01** and MAC address of the 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 self-study.

Verify PAT

Check the IP NAT (PAT) translation table on the router. There is an entry in the table, which is added by the PAT.



Verify PAT

```
CPE#show ip nat translations
Pro   Inside global       Inside local   Outside local        Outside global
icmp  192.168.1.202:512   10.0.0.2:512   192.168.123.100:512  192.168.123.100:512
```

- **Verify how IP addresses are translated on the router.**

© 2006 Cisco Systems, Inc. All rights reserved.

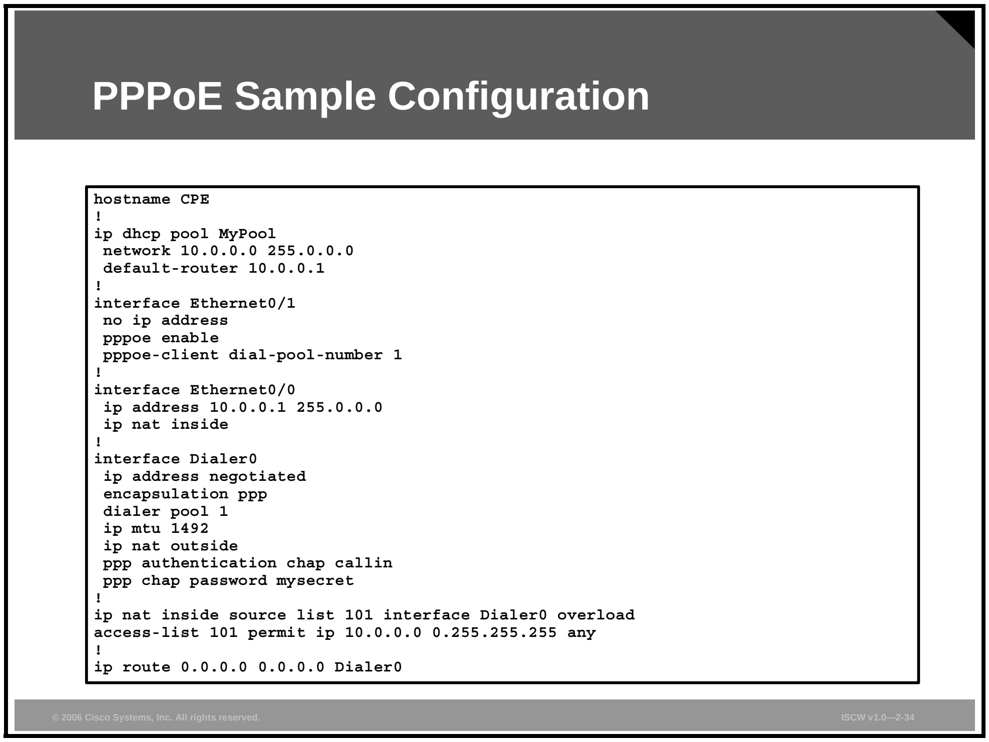
ISCW v1.0—2-33

The PAT translation table shows the translations between IP addresses and ports. In this example, the router translate packets for Internet Control Message Protocol (ICMP) from source IP address 10.0.0.2 and port number 512 (inside local) into IP address 192.168.1.202 and the same port 512 (inside global). Outside local and global IP addresses are the same, which means that the router changes only the *source* IP addresses and ports for the packets going from the customer network to the Internet, and changes *destination* IP addresses and ports for the packets going in the opposite direction (from the Internet to the customer 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 self-study.

PPPoE Sample Configuration

The example presents the complete PPPoE client configuration with PAT, DHCP services, and the static default routing.



PPPoE Sample Configuration

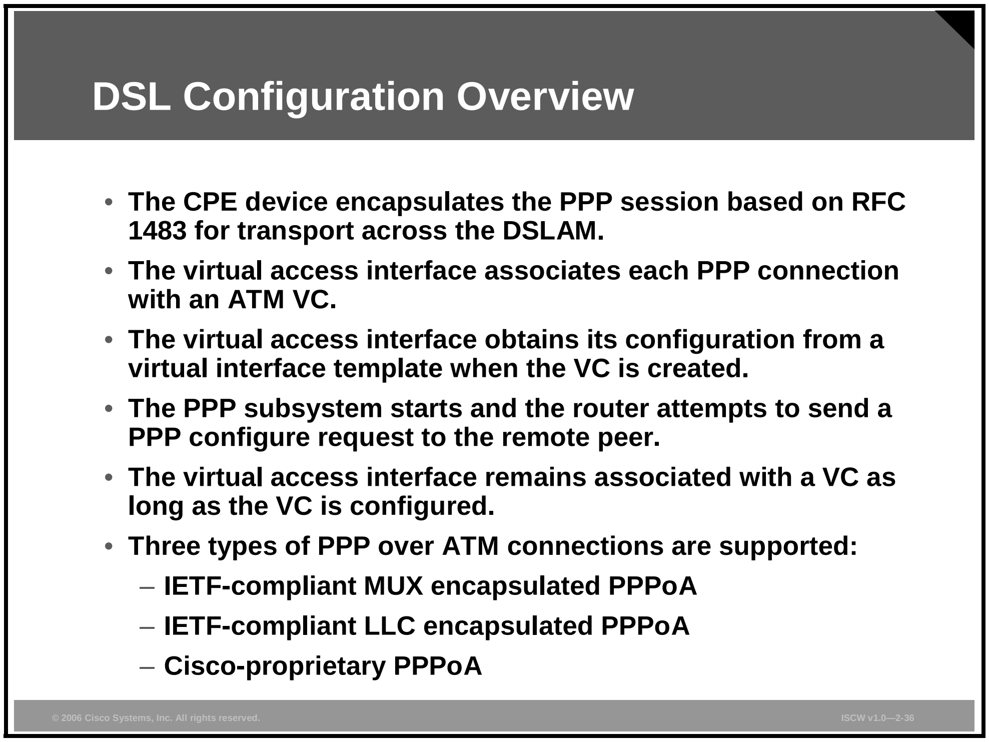
```
hostname CPE
!
ip dhcp pool MyPool
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
!
interface Ethernet0/1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Ethernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
!
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ip mtu 1492
 ip nat outside
 ppp authentication chap callin
 ppp chap password mysecret
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
!
ip route 0.0.0.0 0.0.0.0 Dialer0
```

© 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 self-study.

Configuration of a PPPoA DSL Connection

This topic describes the configuration of a PPPoA connection.



DSL Configuration Overview

- The CPE device encapsulates the PPP session based on RFC 1483 for transport across the DSLAM.
- The virtual access interface associates each PPP connection with an ATM VC.
- The virtual access interface obtains its configuration from a virtual interface template when the VC is created.
- The PPP subsystem starts and the router attempts to send a PPP configure request to the remote peer.
- The virtual access interface remains associated with a VC as long as the VC is configured.
- Three types of PPP over ATM connections are supported:
  - IETF-compliant MUX encapsulated PPPoA
  - IETF-compliant LLC encapsulated PPPoA
  - Cisco-proprietary PPPoA

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-36

With PPPoA, a CPE device encapsulates a PPP session for transport across a DSL access multiplexer (DSLAM). PPPoA is commonly used in small office, home office (SOHO) and branch office environments, although it is not limited to them. It has greater flexibility for the home than the average PPPoE deployment because the customer LAN behind the CPE is under the complete control of the customer and the CPE acts as a router, rather than a bridge for PPPoE (where the CPE bridges the PPPoE frame from the end-user PC running the PPPoE client software).

When you configure PPPoA, a logical interface, known as a virtual access interface, associates each PPP connection with an ATM virtual circuit (VC). You can create this logical interface by configuring an ATM PVC or switched virtual circuit (SVC). This configuration encapsulates each PPP connection in a separate PVC or SVC, allowing each PPP connection to terminate at the router ATM interface as if received from a typical PPP serial interface.

The virtual access interface for each VC obtains its configuration from a virtual interface template (virtual template) when the VC is created. Before you create the ATM VC, it is recommended that you create and configure a virtual template.

Once you have configured the router for PPPoA, the PPP subsystem starts and the router attempts to send a PPP configure request to the remote peer. If the peer does not respond, the router periodically goes into a “listen” state and waits for a configuration request from the peer. After a timeout, the router again attempts to reach the remote router by sending configuration requests.

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

The virtual access interface remains associated with a VC as long as the VC is configured. If you remove the configuration of the VC, the virtual access interface is marked as deleted. If you shut down the associated ATM interface, you will also cause the virtual access interface to be marked as down, and you will bring the PPP connection down. If you set a keepalive timer for the virtual template on the interface, the virtual access interface uses the PPP echo mechanism to verify the existence of the remote peer.

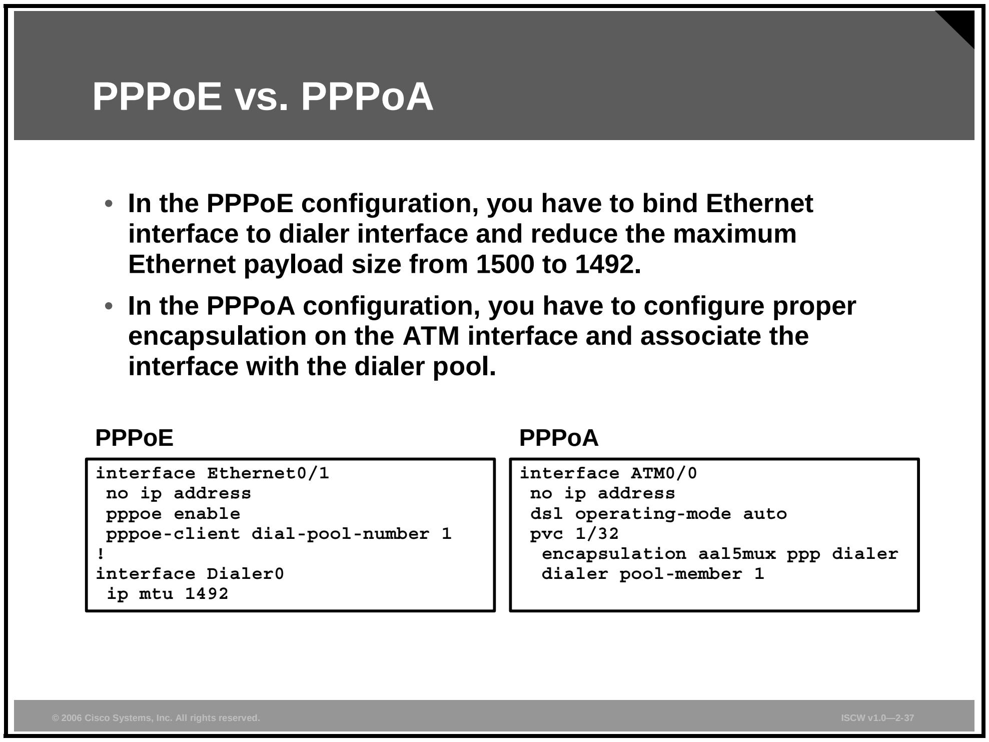
These three types of PPPoA connections are supported:

- Internet Engineering Task Force (IETF)-compliant multiplex (MUX) encapsulated PPPoA
- IETF-compliant logical link control (LLC) encapsulated PPPoA
- Cisco-proprietary PPPoA

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

PPPoE vs. PPPoA

The PPPoE and PPPoA configurations are similar.



PPPoE vs. PPPoA

- **In the PPPoE configuration, you have to bind Ethernet interface to dialer interface and reduce the maximum Ethernet payload size from 1500 to 1492.**
- **In the PPPoA configuration, you have to configure proper encapsulation on the ATM interface and associate the interface with the dialer pool.**

PPPoE

```
interface Ethernet0/1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Dialer0
 ip mtu 1492
```

PPPoA

```
interface ATM0/0
 no ip address
 dsl operating-mode auto
 pvc 1/32
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-37

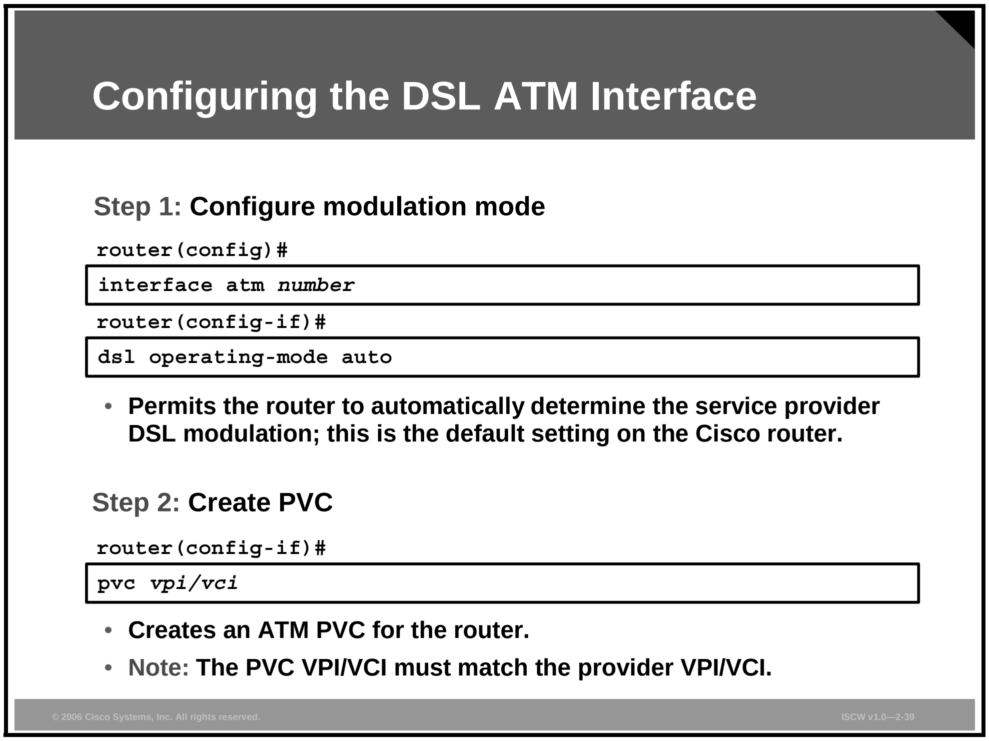
The only difference between PPPoE and PPPoA configurations is shown in the configuration outputs:

- VPDN group is enabled for PPPoE, and the ATM PVC is configured for PPPoE client encapsulation, but in the PPPoA configuration you have to configure proper ATM adaptation layer 5 (AAL5) encapsulation on the ATM PVC.
- In the PPPoE client configuration, you also have to reduce the dialer interface MTU size from 1500 to 1492.

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

Configuration of the DSL ATM Interface

This topic lists commands and explains the procedure, in four steps, to configure a DSL ATM interface.



Configuring the DSL ATM Interface

Step 1: Configure modulation mode

```
router(config)#
interface atm number
router(config-if)#
dsl operating-mode auto
```

- **Permits the router to automatically determine the service provider DSL modulation; this is the default setting on the Cisco router.**

Step 2: Create PVC

```
router(config-if)#
pvc vpi/vci
```

- **Creates an ATM PVC for the router.**
- **Note: The PVC VPI/VCI must match the provider VPI/VCI.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-39

Use the **dsl operating-mode auto** interface configuration command to specify that the router automatically detect the DSL modulation that the service provider is using and set the DSL modulation to match.

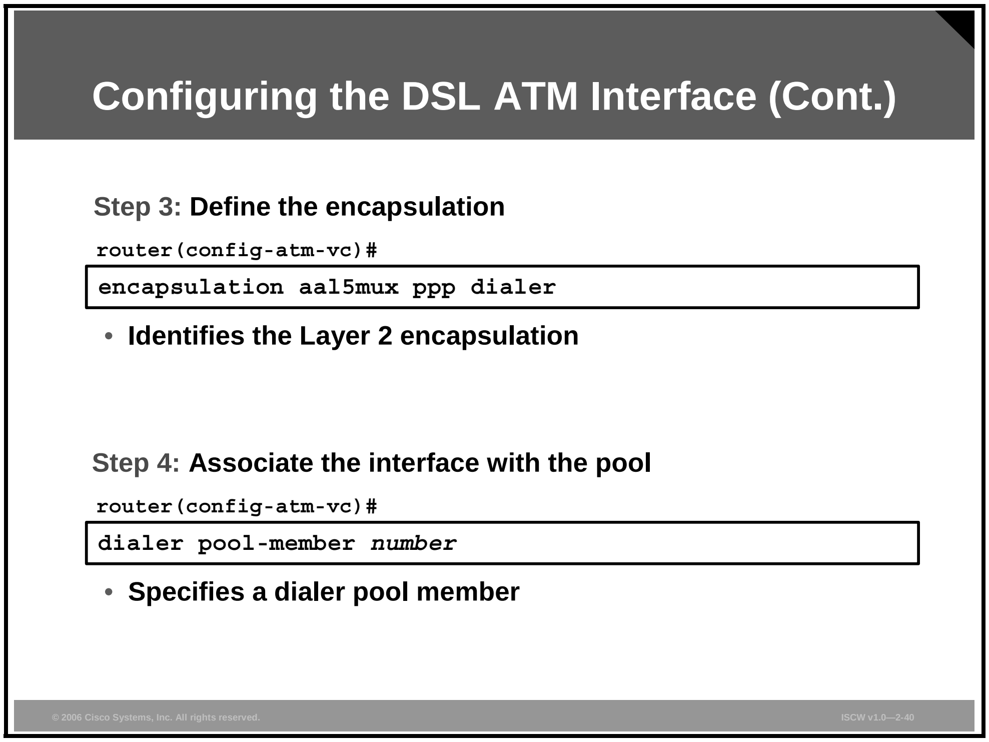
An incompatible DSL modulation configuration can result in failure to establish a DSL connection to the DSLAM of the service provider.

Use the **pvc** interface configuration command to set the virtual path identifier/virtual channel identifier (VPI/VCI) that is used by the DSL service provider, as shown in the table. Settings for the VPI/VCI value on the Cisco router must match the configuration on the DSLAM of the service provider switch configuration. ATM uses the VPI/VCI to identify an ATM VC.

pvc Parameters

Parameter	Description
vpi	VPI from the service provider
vci	VCI from the service provider

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



Configuring the DSL ATM Interface (Cont.)

Step 3: **Define the encapsulation**

```
router(config-atm-vc)#
encapsulation aal5mux ppp dialer
```

- **Identifies the Layer 2 encapsulation**

Step 4: **Associate the interface with the pool**

```
router(config-atm-vc)#
dialer pool-member number
```

- **Specifies a dialer pool member**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-40

The encapsulation method must correspond with that configured on the aggregation router. The table shows the encapsulation commands.

Encapsulation Commands

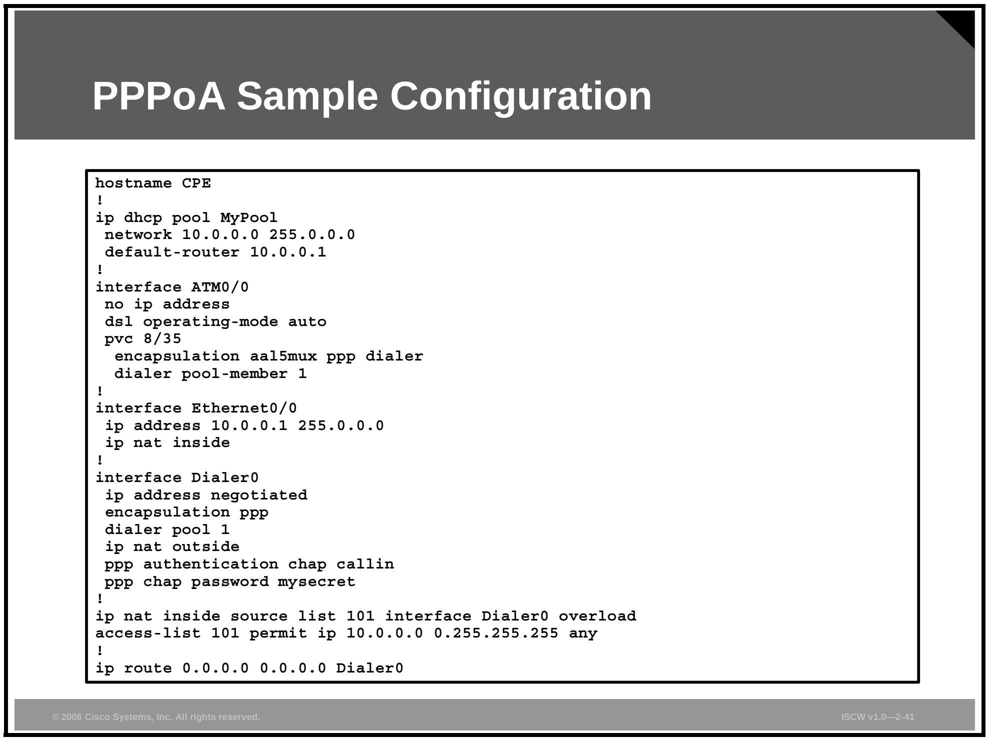
Command	Description
`encapsulation aal5mux ppp dialer`	Sets the encapsulation for PPPoA, which uses AAL5 in the MUX mode
`dialer pool-member` ***`number`***	Links the ATM interface to a dialer interface

Use the **dialer pool-member** command to specify which dialer interfaces may use the ATM physical interface on the Cisco 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 self-study.

PPPoA Sample Configuration

This section shows an example of a complete PPPoA configuration.



PPPoA Sample Configuration

```
hostname CPE
!
ip dhcp pool MyPool
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
!
interface ATM0/0
 no ip address
 dsl operating-mode auto
 pvc 8/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
!
interface Ethernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
!
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ip nat outside
 ppp authentication chap callin
 ppp chap password mysecret
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
!
ip route 0.0.0.0 0.0.0.0 Dialer0
```

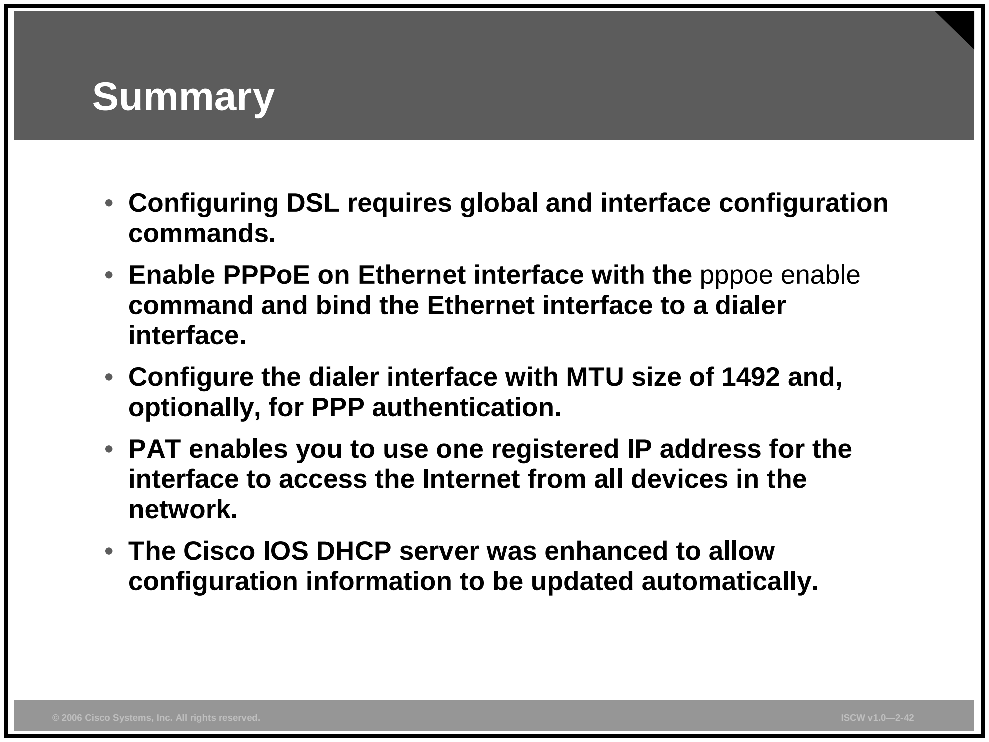
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-41

The example presents the complete PPPoA configuration with PAT, DHCP services, and static default routing.

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

Summary

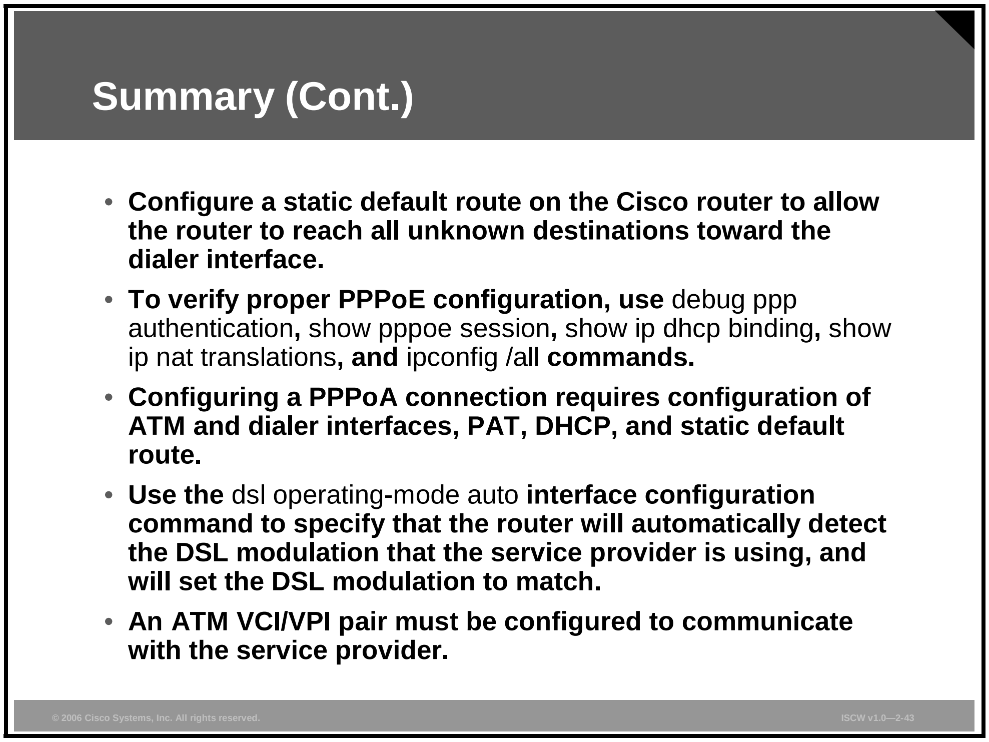
This topic summarizes the key points that were discussed in this lesson.



Summary

- **Configuring DSL requires global and interface configuration commands.**
- **Enable PPPoE on Ethernet interface with the** pppoe enable **command and bind the Ethernet interface to a dialer interface.**
- **Configure the dialer interface with MTU size of 1492 and, optionally, for PPP authentication.**
- **PAT enables you to use one registered IP address for the interface to access the Internet from all devices in the network.**
- **The Cisco IOS DHCP server was enhanced to allow configuration information to be updated automatically.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-42



Summary (Cont.)

- **Configure a static default route on the Cisco router to allow the router to reach all unknown destinations toward the dialer interface.**
- **To verify proper PPPoE configuration, use** debug ppp authentication**,** show pppoe session**,** show ip dhcp binding**,** show ip nat translations**, and** ipconfig /all **commands.**
- **Configuring a PPPoA connection requires configuration of ATM and dialer interfaces, PAT, DHCP, and static default route.**
- **Use the** dsl operating-mode auto **interface configuration command to specify that the router will automatically detect the DSL modulation that the service provider is using, and will set the DSL modulation to match.**
- **An ATM VCI/VPI pair must be configured to communicate with the service provider.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-43

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

Lesson 5

Verifying Broadband ADSL Configurations

Overview

This lesson describes troubleshooting methods for Layer 1 and Layer 2. The lesson describes some reasons why an asymmetric DSL (ADSL) connection might fail to be established, and describes how to repair the connection if it fails.

Objectives

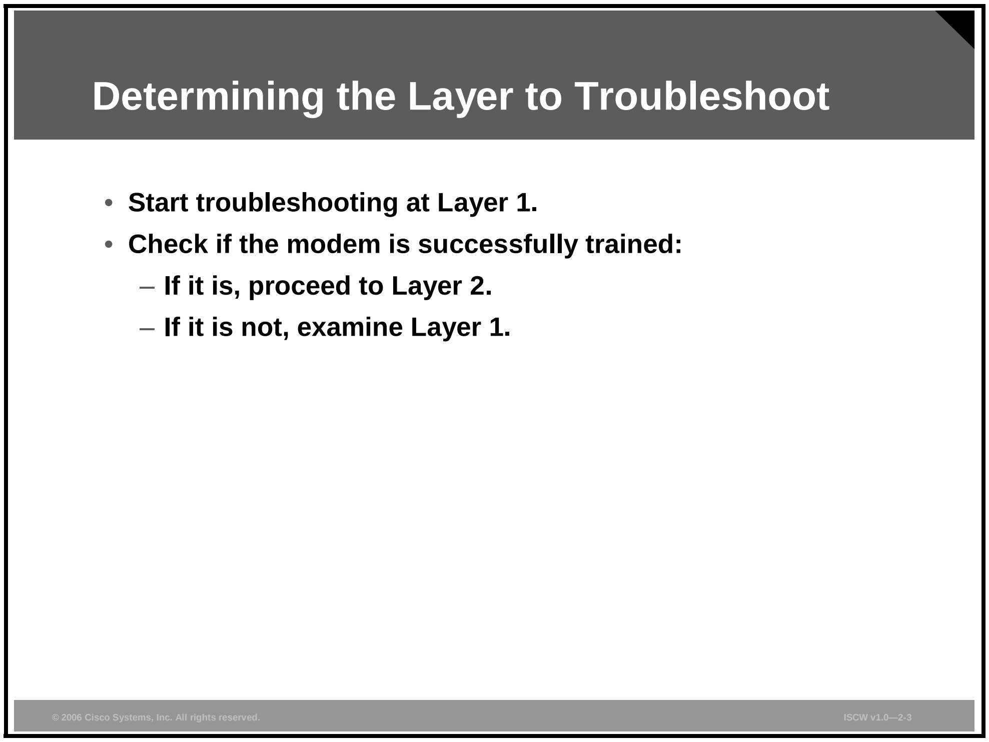
Upon completing this lesson, you will be able to verify typical broadband configurations. This ability includes being able to meet these objectives:

- Explain the bottom-up approach to troubleshooting a DSL connection problem
- Explain the procedure to isolate problems to Layer 1
- Explain the procedure to confirm an Administratively Down state
- Explain the procedure to confirm the correct DSL operating mode on the CPE router ATM interface
- Explain the procedure to isolate problems to Layer 2
- Explain how to determine if data is being received from the ISP
- Explain how to determine if PPP is negotiating successfully

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

Layer Troubleshooting

This topic describes the first ADSL troubleshooting step—determining which layer of the ADSL service is failing. There are many reasons why a DSL connection might not function properly.



Determining the Layer to Troubleshoot

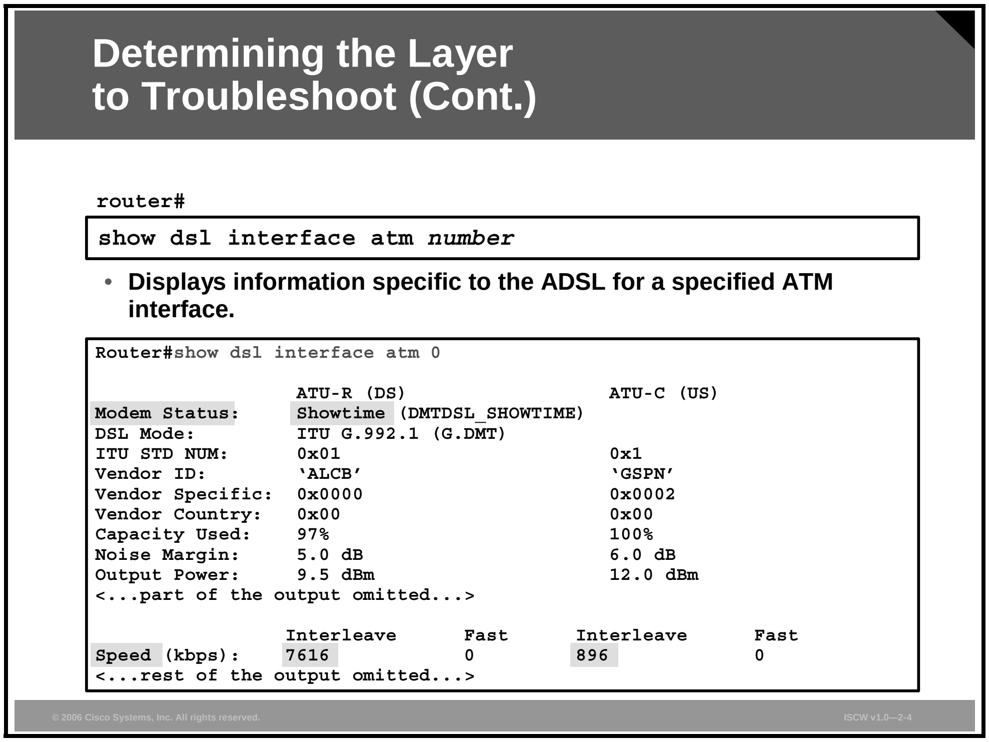
- Start troubleshooting at Layer 1.
- Check if the modem is successfully trained:
  - If it is, proceed to Layer 2.
  - If it is not, examine Layer 1.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-3

A problem with a nonfunctional ADSL service can reside at Layer 1, Layer 2, or Layer 3. Troubleshooting of the problem should start by determining which ADSL service layer is failing. To do that, use a bottom-up approach—that is, start troubleshooting at Layer 1.

The first thing to check is whether the customer premises equipment (CPE) DSL modem has been successfully trained to the DSL access multiplexer (DSLAM) in the central office (CO). If it has, then the problem does not persist at Layer 1 and the troubleshooting can proceed to Layer 2. Otherwise, Layer 1 should be examined in more detail.

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



Determining the Layer to Troubleshoot (Cont.)

```
router#
show dsl interface atm number
```

- **Displays information specific to the ADSL for a specified ATM interface.**

```
Router#show dsl interface atm 0

                    ATU-R (DS)                    ATU-C (US)
Modem Status:       Showtime (DMTDSL_SHOWTIME)
DSL Mode:           ITU G.992.1 (G.DMT)
ITU STD NUM:        0x01                          0x1
Vendor ID:          'ALCB'                        'GSPN'
Vendor Specific:    0x0000                        0x0002
Vendor Country:     0x00                          0x00
Capacity Used:      97%                           100%
Noise Margin:       5.0 dB                        6.0 dB
Output Power:       9.5 dBm                       12.0 dBm
<...part of the output omitted...>

                   Interleave      Fast      Interleave      Fast
Speed (kbps):      7616            0         896             0
<...rest of the output omitted...>
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-4

Start troubleshooting Layer 1 by verifying whether a Cisco Systems CPE router is trained and successfully initialized to the DSLAM using the **show dsl interface atm** command.

When a router is successfully trained to the DSLAM, the modem status field will have the value **Showtime**. Along with that value, the command will also display the upstream and downstream speed in kbps (in the row **Speed**, the **Interleave** or **Fast** columns will have a nonzero value). If the router is trained, then proceed to Layer 2 examination and troubleshooting.

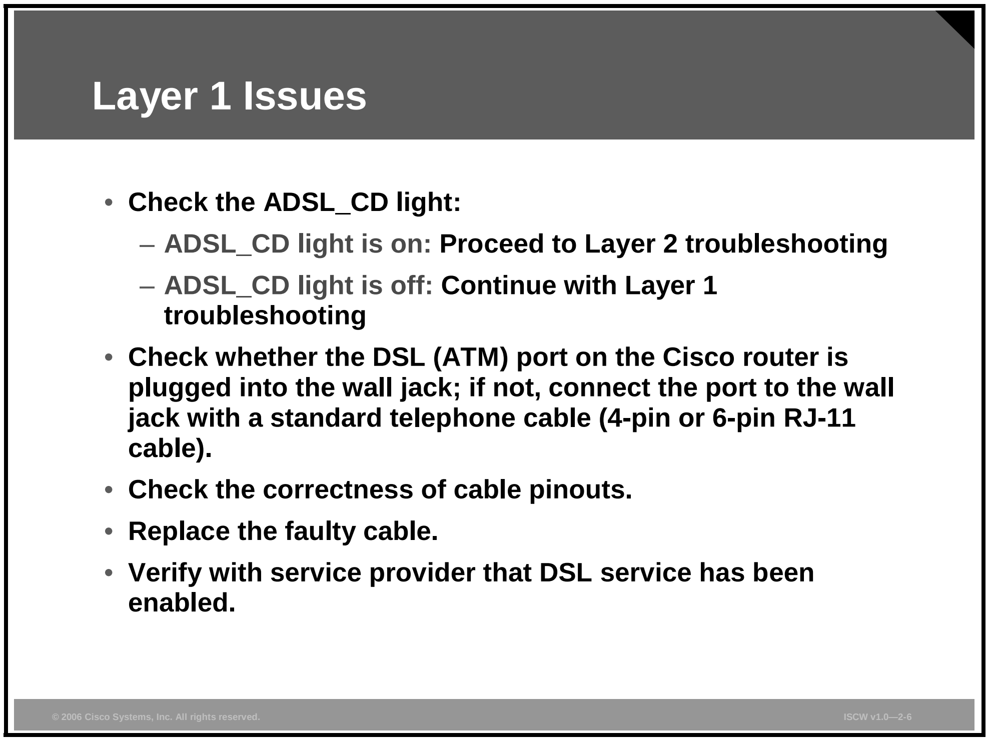
When training is not successful, as shown in this output, the problem persists at Layer 1 and should be isolated there.

```
Router#show dsl interface atm 0
Line not activated: displaying cached data from last
activation
Log file of training sequence:
<...rest of the output omitted...>
```

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

Layer 1 Issues

This topic describes the steps that are used to determine whether Layer 1 is the cause of the problem.



Layer 1 Issues

- **Check the ADSL_CD light:**
  - ADSL_CD light is on: **Proceed to Layer 2 troubleshooting**
  - ADSL_CD light is off: **Continue with Layer 1 troubleshooting**
- **Check whether the DSL (ATM) port on the Cisco router is plugged into the wall jack; if not, connect the port to the wall jack with a standard telephone cable (4-pin or 6-pin RJ-11 cable).**
- **Check the correctness of cable pinouts.**
- **Replace the faulty cable.**
- **Verify with service provider that DSL service has been enabled.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-6

You can monitor the status of the ATM interface on the router by checking the status of the Carrier Detect (CD) light on the router front panel:

- If the CD light is *on*, proceed to Layer 2 troubleshooting.
- If the CD light is *off*, continue with Layer 1 troubleshooting.

Next, use the **show interface atm** privilege level command from the enable mode of the router to check the status of the ATM interface on the router.

If the ATM interface status is down and the line protocol is down, the router is not seeing a carrier on the ADSL line. Such a status usually indicates two possible issues:

- The active pins on the DSL wall jack may be incorrect—the registered jack-11 (RJ-11) connector provides an xDSL connection to an external media via a standard RJ-11 6-pin modular jack.
- The service provider may not be providing DSL service on this wall jack.

The Cisco router uses a standard RJ-11 cable to provide the ADSL connection to the wall jack. The center pair of pins on the RJ-11 cable is used to carry the ADSL signal (pins 3 and 4 on a 6-pin cable, or pins 2 and 3 on a 4-pin cable).

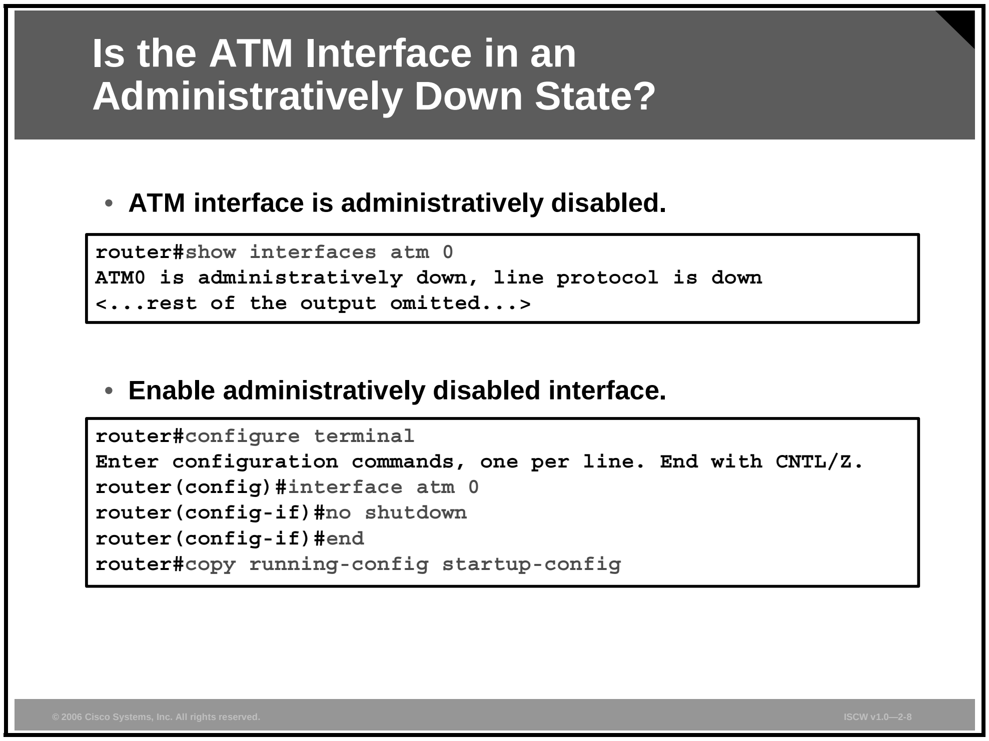
If the correct pins on the wall jack are being used, and the ATM interface is still down and the line protocol is down, replace the RJ-11 cable between the DSL port and the wall jack.

If the interface is still down and the line protocol is down after you have replaced the RJ-11 cable, contact the service provider to verify that ADSL service has been enabled on the wall jack that is being 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 self-study.

Administratively Down State for an ATM Interface

This topic describes troubleshooting situations in which the interface is down because of an administrative action. This is the simplest problem to resolve.



Is the ATM Interface in an Administratively Down State?

- ATM interface is administratively disabled.

```
router#show interfaces atm 0
ATM0 is administratively down, line protocol is down
<...rest of the output omitted...>
```

- Enable administratively disabled interface.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#interface atm 0
router(config-if)#no shutdown
router(config-if)#end
router#copy running-config startup-config
```

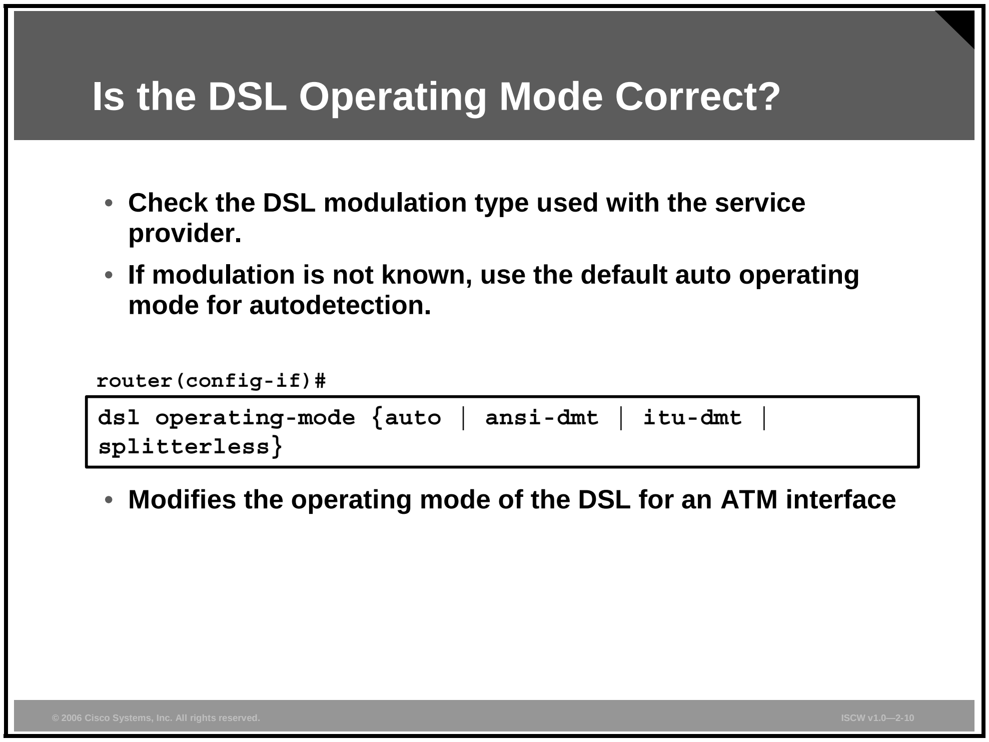
© 2006 Cisco Systems, Inc. All rights reserved.

The **show interface atm** command also shows whether the interface is administratively disabled. If such a case exists, enable the interface by using the **no shutdown** command under the interface 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 self-study.

Correct DSL Operating Mode?

This topic describes the procedure to correct the DSL operating mode.



Is the DSL Operating Mode Correct?

- **Check the DSL modulation type used with the service provider.**
- **If modulation is not known, use the default auto operating mode for autodetection.**

```
router(config-if)#
dsl operating-mode {auto | ansi-dmt | itu-dmt |
splitterless}
```

- **Modifies the operating mode of the DSL for an ATM interface**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-10

At this point of the troubleshooting process, everything that was checked up to now in the Layer 1 troubleshooting procedure is verified and is operating properly. The next step is to ensure that the correct DSL operating mode is being used. Check with the service provider whether the DSLAM supports the particular DSL chipset (for example, Alcatel) and the configured modulation method of the deployed Cisco CPE DSL router. If the DSL modulation being used by the service provider is unknown, Cisco recommends use of the default *auto* operating mode to autodetect the modulation type.

dsl operating-mode {**auto** | **ansi-dmt** | **itu-dmt** | **splitterless**}

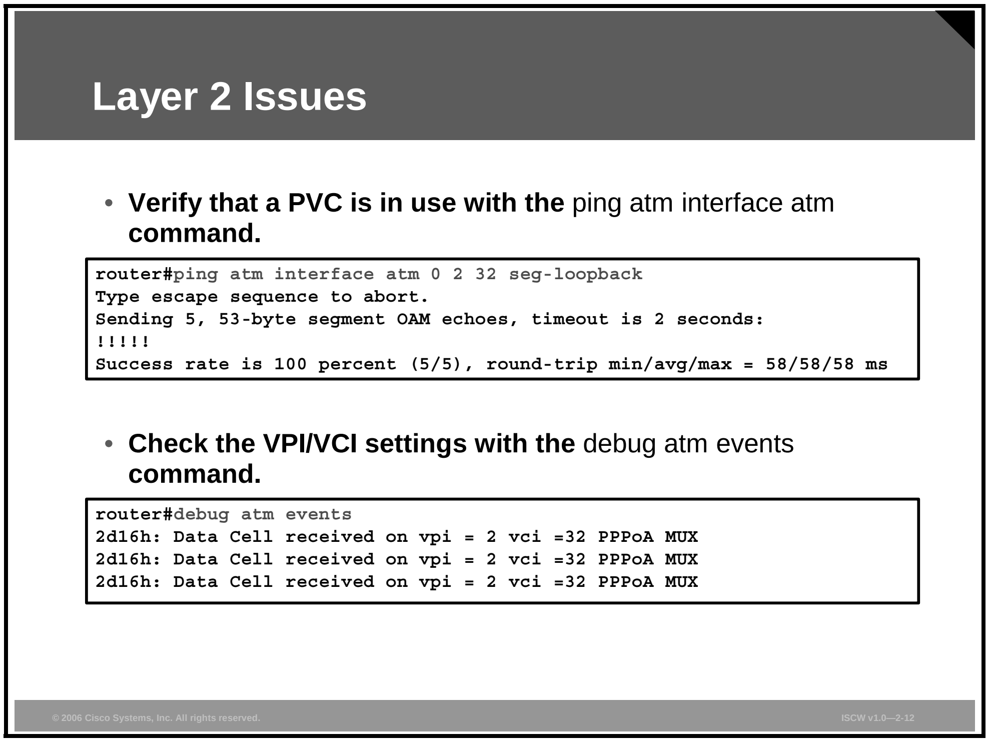
dsl operating-mode Parameters

Parameter	Description
`auto`	Configures the ADSL line after autonegotiating with the DSLAM located at the CO. This is the default operating mode.
`ansi-dmt`	Configures the ADSL line to use the ANSI T1.413 Issue 2 mode.
`itu-dmt`	Configures the ADSL line to use the G.992.1 mode.
`splitterless`	Configures the ADSL line to use the G.992.2 (G.lite) 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 self-study.

Layer 2 Issues

This topic describes the steps that are used to determine whether there is a Layer 2 problem.



Layer 2 Issues

- **Verify that a PVC is in use with the** ping atm interface atm **command.**

```
router#ping atm interface atm 0 2 32 seg-loopback
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 58/58/58 ms
```

- **Check the VPI/VCI settings with the** debug atm events **command.**

```
router#debug atm events
2d16h: Data Cell received on vpi = 2 vci =32 PPPoA MUX
2d16h: Data Cell received on vpi = 2 vci =32 PPPoA MUX
2d16h: Data Cell received on vpi = 2 vci =32 PPPoA MUX
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-12

After establishing that Layer 1 is not an issue, the troubleshooting can continue at Layer 2.

First, check whether a permanent virtual circuit (PVC) is configured at the DSLAM by using the **ping atm interface atm** command. This command sends Operation, Administration, and Maintenance (OAM) F5 loopback packets to the DSLAM. A successful ping designates that a PVC is configured at the DSLAM.

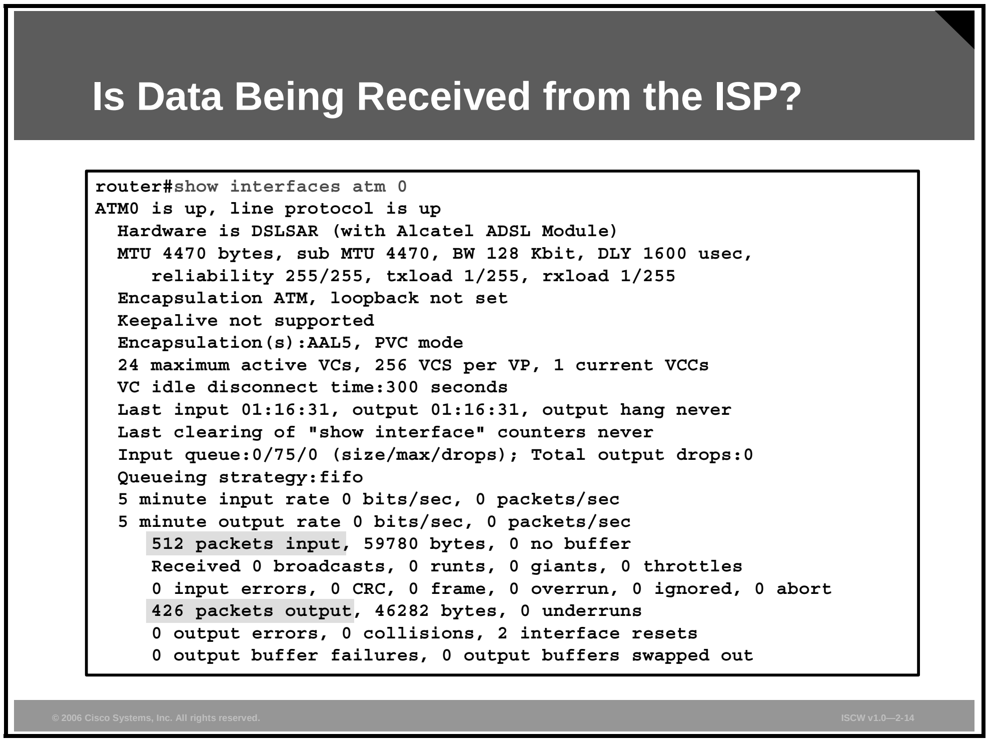
Next, check whether the correct virtual path identifier/virtual channel identifier (VPI/VCI) values are configured on the router, by using the **debug atm events** command. The output shows the VPI/VCI values that the DSLAM expects. During the debug process, use another working Internet connection and begin to ping the static IP address assigned by your Internet service provider (ISP). It is important that the ATM interface status is up, the line protocol is up, and that the IP address provided by the ISP is being pinged. If there is no output for 60 seconds, debugging the VPI/VCI values is probably incorrect and you should contact ISP support. Finally, verify the VPI/VCI values and make the necessary changes to the configuration.

At the end, turn off debugging by using the **undebug all** 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 self-study.

Data Received from the ISP

This topic describes how to determine if data is being received from the ISP.



Is Data Being Received from the ISP?

```
router#show interfaces atm 0
ATM0 is up, line protocol is up
  Hardware is DSLSAR (with Alcatel ADSL Module)
  MTU 4470 bytes, sub MTU 4470, BW 128 Kbit, DLY 1600 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5, PVC mode
  24 maximum active VCs, 256 VCS per VP, 1 current VCCs
  VC idle disconnect time:300 seconds
  Last input 01:16:31, output 01:16:31, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:fifo
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     512 packets input, 59780 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     426 packets output, 46282 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-14

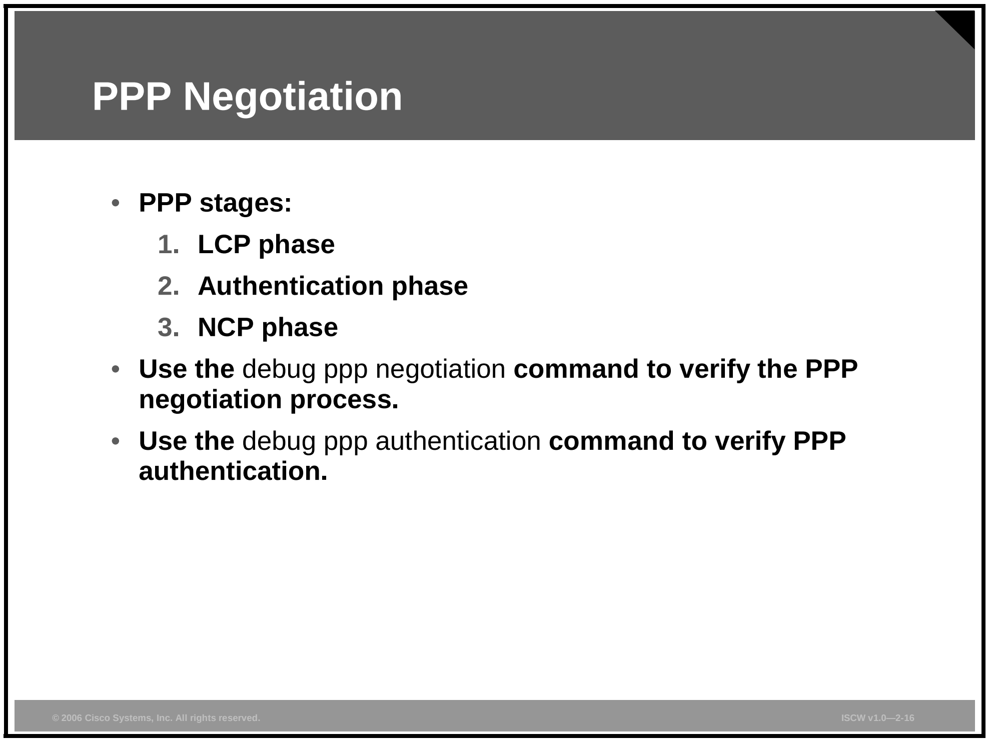
If the correct VPI/VCI values are being used and the PVC is active, then the next step is to verify that data is being sent and received on the ATM interface.

The **show interfaces atm** command shows the interface status and counters for incoming and outgoing packets. If the incoming and outgoing packet counters are incrementing, the router is receiving and sending packets from the ISP, therefore data is received from the ISP and is also sent toward the ISP.

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

Proper PPP Negotiation

This topic describes the procedure for determining if PPP is negotiating successfully.



PPP Negotiation

- **PPP stages:**
  1. **LCP phase**
  2. **Authentication phase**
  3. **NCP phase**
- **Use the** debug ppp negotiation **command to verify the PPP negotiation process.**
- **Use the** debug ppp authentication **command to verify PPP authentication.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-16

With Layer 1 set up properly, correct VPI/VCI being used, PVC being active, and data being received and sent, the next step is to ensure that a PPP session is established properly between the Cisco CPE router and the aggregation router of the service provider. You can observe the PPP negotiation process by issuing the **debug ppp negotiation** and **debug ppp authentication** commands.

PPP session setup goes through three stages:

1. **Link control protocol (LCP):** A mandatory phase in which parameters to establish, configure, and test the data-link connection are negotiated.

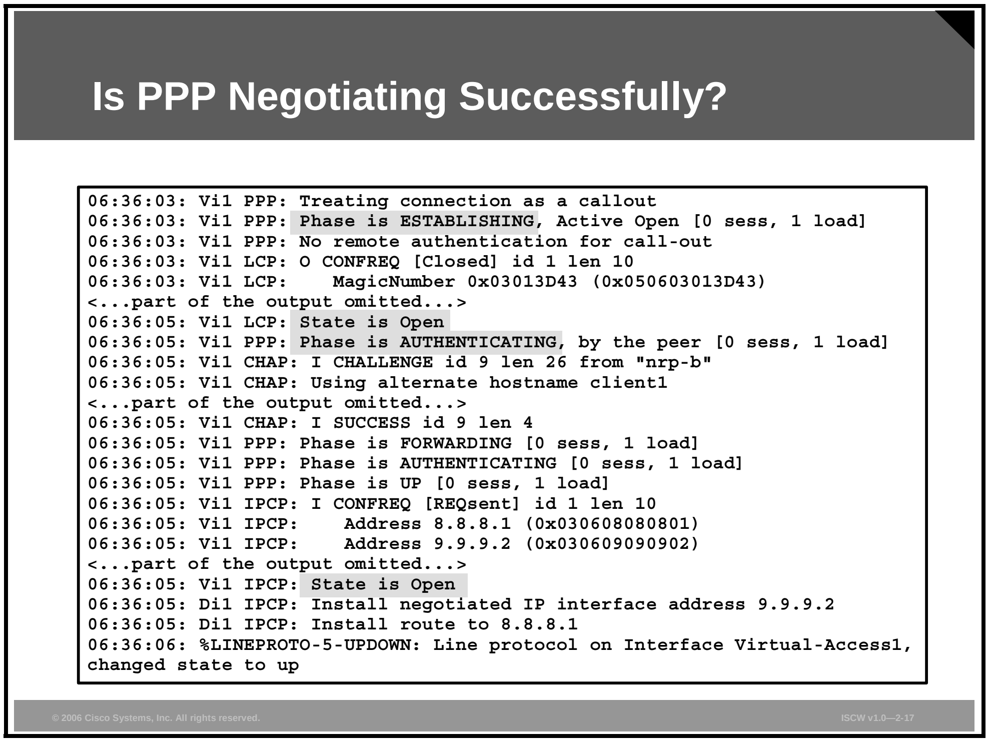
2. **Authentication:** In this optional phase, the authentication is performed with the authentication protocol (Challenge Handshake Authentication Protocol [CHAP] or Password Authentication Protocol [PAP]) agreed upon in LCP negotiation.

3. **Network Control Protocol (NCP):** This mandatory phase is used to establish and configure different network-layer protocols. The most common Layer 3 protocol negotiated is IP. The routers exchange IP Control Protocol (IPCP) messages to negotiate options specific to the IP protocol.

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

Is PPP Negotiating Successfully?

The debug output in the figure shows the successful PPP session establishment.



Is PPP Negotiating Successfully?

```
06:36:03: Vi1 PPP: Treating connection as a callout
06:36:03: Vi1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 1 load]
06:36:03: Vi1 PPP: No remote authentication for call-out
06:36:03: Vi1 LCP: O CONFREQ [Closed] id 1 len 10
06:36:03: Vi1 LCP:    MagicNumber 0x03013D43 (0x050603013D43)
<...part of the output omitted...>
06:36:05: Vi1 LCP: State is Open
06:36:05: Vi1 PPP: Phase is AUTHENTICATING, by the peer [0 sess, 1 load]
06:36:05: Vi1 CHAP: I CHALLENGE id 9 len 26 from "nrp-b"
06:36:05: Vi1 CHAP: Using alternate hostname client1
<...part of the output omitted...>
06:36:05: Vi1 CHAP: I SUCCESS id 9 len 4
06:36:05: Vi1 PPP: Phase is FORWARDING [0 sess, 1 load]
06:36:05: Vi1 PPP: Phase is AUTHENTICATING [0 sess, 1 load]
06:36:05: Vi1 PPP: Phase is UP [0 sess, 1 load]
06:36:05: Vi1 IPCP: I CONFREQ [REQsent] id 1 len 10
06:36:05: Vi1 IPCP:    Address 8.8.8.1 (0x030608080801)
06:36:05: Vi1 IPCP:    Address 9.9.9.2 (0x030609090902)
<...part of the output omitted...>
06:36:05: Vi1 IPCP: State is Open
06:36:05: Di1 IPCP: Install negotiated IP interface address 9.9.9.2
06:36:05: Di1 IPCP: Install route to 8.8.8.1
06:36:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-17

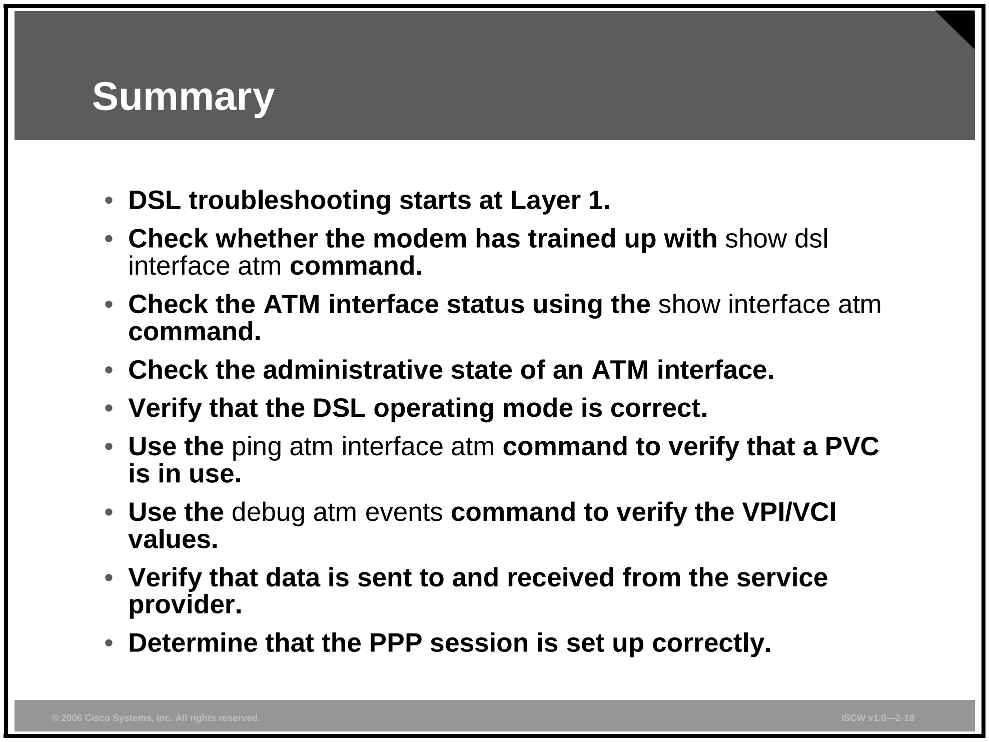
In case the PPP session does not come up successfully, there are four main points of failure in a PPP negotiation:

- There is no response from the remote device (aggregation router of the service provider).
- LCP is not opened.
- PAP or CHAP authentication failure occurs.
- IPCP failures.

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

Summary

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



Summary

- **DSL troubleshooting starts at Layer 1.**
- **Check whether the modem has trained up with** show dsl interface atm **command.**
- **Check the ATM interface status using the** show interface atm **command.**
- **Check the administrative state of an ATM interface.**
- **Verify that the DSL operating mode is correct.**
- **Use the** ping atm interface atm **command to verify that a PVC is in use.**
- **Use the** debug atm events **command to verify the VPI/VCI values.**
- **Verify that data is sent to and received from the service provider.**
- **Determine that the PPP session is set up correctly.**

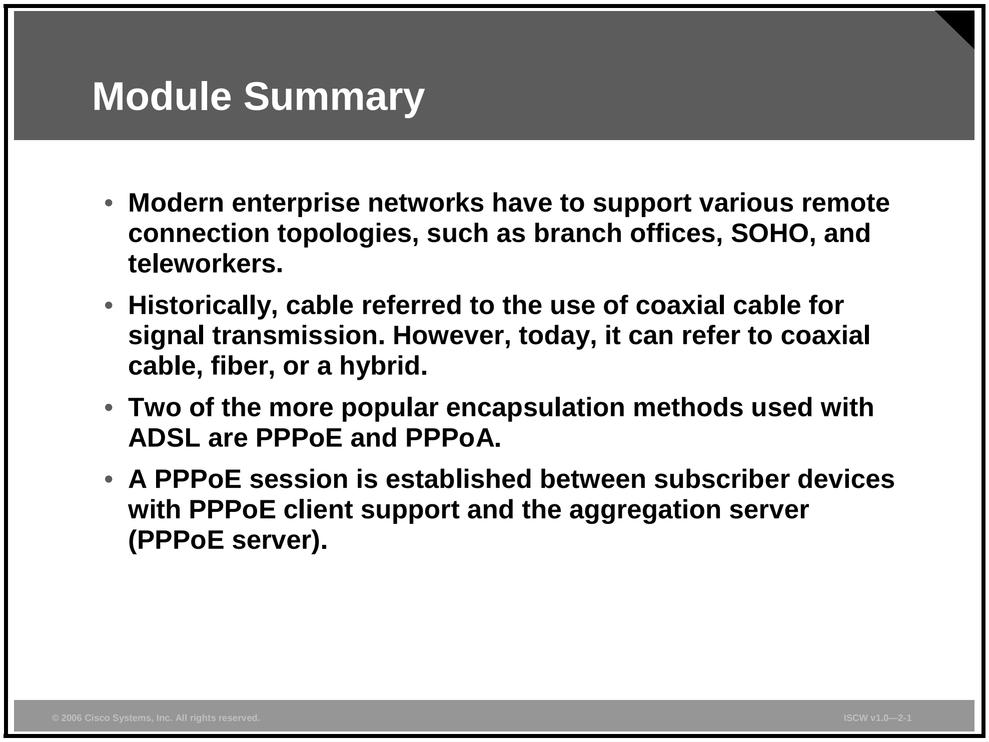
© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—2-18

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

Module Summary

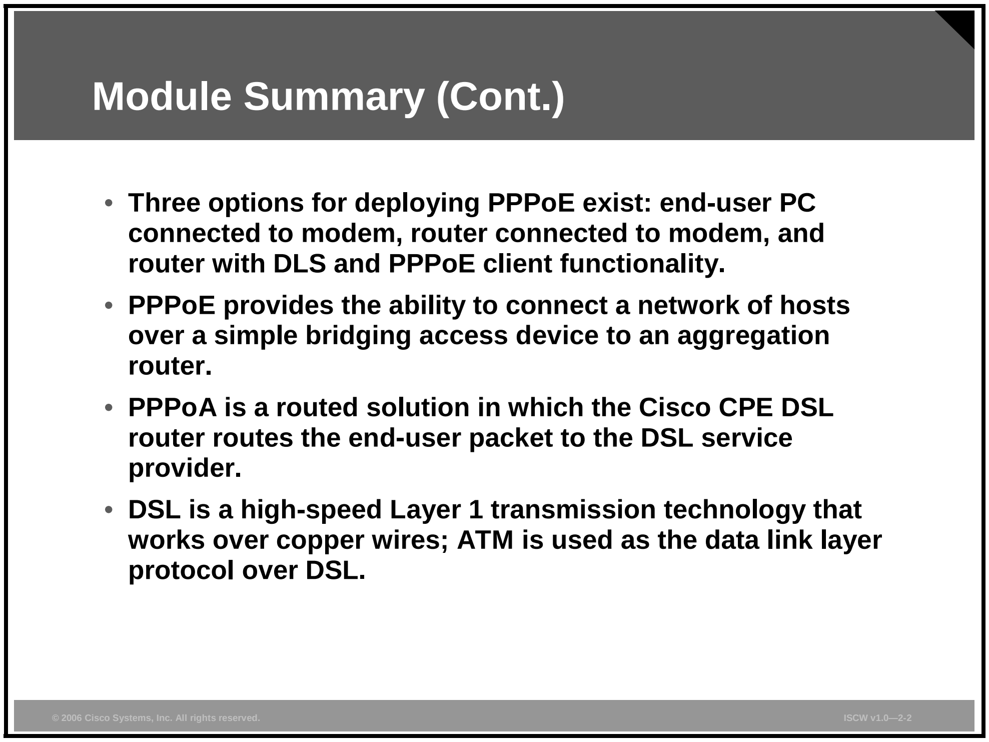
This topic summarizes the key points that were discussed in this module.



Module Summary

- Modern enterprise networks have to support various remote connection topologies, such as branch offices, SOHO, and teleworkers.
- Historically, cable referred to the use of coaxial cable for signal transmission. However, today, it can refer to coaxial cable, fiber, or a hybrid.
- Two of the more popular encapsulation methods used with ADSL are PPPoE and PPPoA.
- A PPPoE session is established between subscriber devices with PPPoE client support and the aggregation server (PPPoE server).

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-1



Module Summary (Cont.)

- Three options for deploying PPPoE exist: end-user PC connected to modem, router connected to modem, and router with DLS and PPPoE client functionality.
- PPPoE provides the ability to connect a network of hosts over a simple bridging access device to an aggregation router.
- PPPoA is a routed solution in which the Cisco CPE DSL router routes the end-user packet to the DSL service provider.
- DSL is a high-speed Layer 1 transmission technology that works over copper wires; ATM is used as the data link layer protocol over DSL.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—2-2

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

This module concentrated on teleworkers and the different ways to connect teleworkers to the enterprise network. The most typical technologies, cable and variants of the DSL, were described in detail. The module also covered instructions on how to verify the configurations of broadband connections.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-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) Which Enterprise Architecture Framework building block provides secure data and voice delivery to remote small and home offices? (Source: Topologies for Facilitating Remote Connections)

A) the Data Center
B) the Enterprise Branch
C) the Enterprise Campus
D) the Enterprise Teleworker
E) the Enterprise WAN

Q2) Which two of the following are the infrastructure services challenges that the teleworker solution addresses? (Choose two.) (Source: Topologies for Facilitating Remote Connections)

A) inexpensive remote connection
B) high availability
C) security policy
D) redundant routing topology
E) management framework
F) three-layered network architecture

Q3) What is the reason that fiber is used in cable networks? (Source: Describing Cable Technology)

A) to provide redundant paths
B) to reduce the number of amplifiers in the network
C) to amplify the cable signal
D) to provide broadcast architecture cascaded to the users

Q4) Which xDSL variant offers only asymmetrical service, and allows voice and data coexistence? (Source: Describing DSL Technology)

A) SDSL
B) IDSL
C) ADSL
D) HDSL

Q5) When deploying ADSL, which two line-coding techniques are available? (Choose two.) (Source: Describing DSL Technology)

A) PPPoE
B) CAP
C) PPPoA
D) DMT
E) ATU-R
F) ATU-C

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

Q6) When configuring a PPPoE client on the Cisco router, on which interface is the MTU size set to 1492? (Source: Configuring the CPE as the PPPoE or PPPoA Client)

A) the Ethernet interface
B) the ATM interface
C) the serial interface
D) the dialer interface

Q7) When configuring DSL on a Cisco router, where does the information for the correct VPI/VCI come from? (Source: Configuring the CPE as the PPPoE or PPPoA Client)

A) the DSL SP
B) the DSL modem manufacturer
C) the local electronics retail store
D) can be any number that is locally assigned by the customer

Q8) When determining whether the Cisco DSL router has trained up successfully, which command is used? (Source: Verifying Broadband ADSL Configurations)

A) `debug ip packet`
B) `debug dsl operation`
C) `show dsl train`
D) `show dsl interface atm 0`

Q9) What is the problem if data is sent and received from the provider but there is no IP connectivity? (Source: Verifying Broadband Configurations)

A) The ATM interface on the router is administratively disabled.
B) The VPI/VCI pair is incorrect.
C) The PPP session is not properly set up.
D) The cable with the wrong pin out 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 self-study.

Module Self-Check Answer Key

Q1)	D
Q2)	C, E
Q3)	B
Q4)	C
Q5)	B, D
Q6)	D
Q7)	A
Q8)	D
Q9)	C

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

Module 3

Frame Mode MPLS Implementation

Overview

Modern service providers face many challenges in terms of customer demand, including an ongoing need for value-added services. Conventional IP packet forwarding has several limitations, and more and more service providers realize that something else is needed. Not only must service providers be concerned with protecting their existing infrastructure, but they must also find ways to generate new services that are not currently supported using existing technologies.

Multiprotocol Label Switching (MPLS) is a high-performance method for forwarding packets through a network. MPLS enables routers at the edge of a network to apply simple labels to packets. This practice allows the MPLS-enabled routers to switch packets according to labels, with minimal routing lookup overhead.

This module describes the features of MPLS compared with hop-by-hop IP routing. MPLS concepts and terminology, along with MPLS label format and label switch router (LSR) architecture, and the assignment and distribution of labels are explained. The module reviews switching implementations, focusing on Cisco Express Forwarding (CEF). The module also describes the implementation of frame mode MPLS on Cisco IOS platforms.

This module also introduces virtual private networks (VPNs) and two major VPN design options: the overlay VPN and the peer-to-peer VPN. In addition, the module explains VPN terminology and topologies, and describes MPLS VPN architecture and operations.

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

Module Objectives

Upon completing this module, you will be able to implement and verify frame mode MPLS. This ability includes being able to meet these objectives:

- Describe the MPLS conceptual model with data and control planes, and describe the function of the MPLS label
- Describe how labels are allocated and distributed in a frame mode MPLS network, and describe how IP packets cross an MPLS network
- Describe the steps that are required to successfully implement MPLS
- Explain the evolution of MPLS VPNs, and describe MPLS VPN routing and packet flow

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

Lesson 1

Introducing MPLS Networks

Overview

This lesson describes the basic concepts and architecture of Multiprotocol Label Switching (MPLS). The lesson describes some of the MPLS components and labels. The four fields that make up an MPLS label are explained, as well as how label stacking is used and how labels are forwarded in frame mode and cell mode environments.

To fully understand MPLS, you must understand the format of an MPLS label and the function of each field in that label. You also need to know how path information is passed from node to node in the network.

Objectives

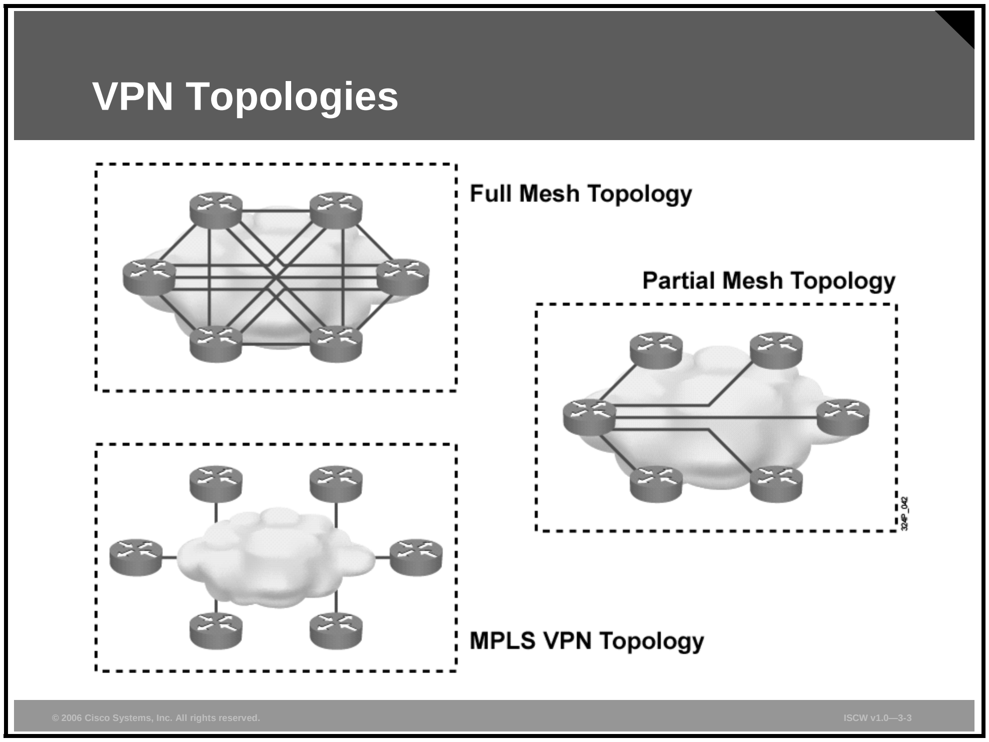
Upon completing this lesson, you will be able to describe the MPLS conceptual model with data and control planes, and describe the function of the MPLS label. This ability includes being able to meet these objectives:

- Identify the elements of the MPLS conceptual model
- Describe the router switching mechanisms
- Describe the MPLS data and control planes
- Identify the structure of an MPLS label and its format
- Explain the function of different types of LSRs in MPLS networks
- Explain the interactions between the control plane and the data plane in an LSR that enable the basic functions of label switching and forwarding of labeled packets to occur

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

The MPLS Conceptual Model

This topic describes MPLS.



VPN Topologies

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-3

You can connect sites using different topologies. For optimal routing between sites, a full mesh topology is required. The full mesh topology provides a dedicated virtual circuit between any two customer edge (CE) routers in the network, but the full mesh solution is very expensive.

For a less expensive solution, you may use partial mesh topology or hub-and-spoke topology, but routing is not optimal with these solutions. The partial mesh topology reduces the number of virtual circuits, usually to the minimum number that provides optimum transport between major sites.

The hub-and-spoke topology is the ultimate reduction within the partial mesh topology. Many sites (spokes) are connected directly to the central site (or sites), or hub (or hubs), with no direct connectivity between the spokes. To prevent single points of failure, the hub-and-spoke topology is sometimes extended to a *redundant* hub-and-spoke topology.

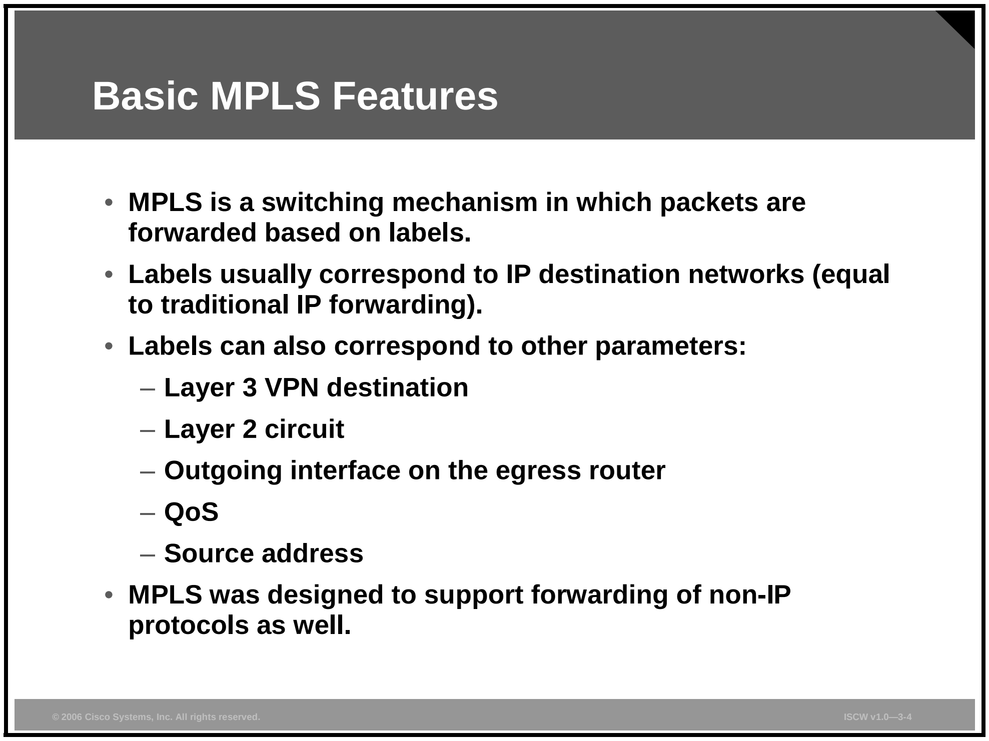
MPLS virtual private network (MPLS VPN) topology provides optimal routing between sites, and you need only one connection to the MPLS VPN service provider.

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

Basic MPLS Features

In a traditional IP network, routing lookups are performed on every router. Each router in the network makes an independent decision when forwarding packets.

MPLS helps reduce the number of routing lookups and can change the forwarding criteria. This capability eliminates the need to run a particular routing protocol on all the devices.



Basic MPLS Features

- **MPLS is a switching mechanism in which packets are forwarded based on labels.**
- **Labels usually correspond to IP destination networks (equal to traditional IP forwarding).**
- **Labels can also correspond to other parameters:**
  - **Layer 3 VPN destination**
  - **Layer 2 circuit**
  - **Outgoing interface on the egress router**
  - **QoS**
  - **Source address**
- **MPLS was designed to support forwarding of non-IP protocols as well.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-4

MPLS is a switching mechanism that assigns labels (numbers) to packets, then uses those labels to forward packets. The labels are assigned at the edge of the MPLS network, and forwarding inside the MPLS network is done solely based on labels.

Labels usually correspond to a path to Layer 3 destination addresses, similar to IP destination-based routing. Labels can also correspond to Layer 3 VPN destinations (MPLS VPN) or non-IP parameters, such as a Layer 2 circuit or outgoing interface on the egress router. This includes Cisco Systems solutions for transporting Layer 2 packets over an MPLS backbone, such as Any Transport over MPLS (AToM), quality of service (QoS), or source address.

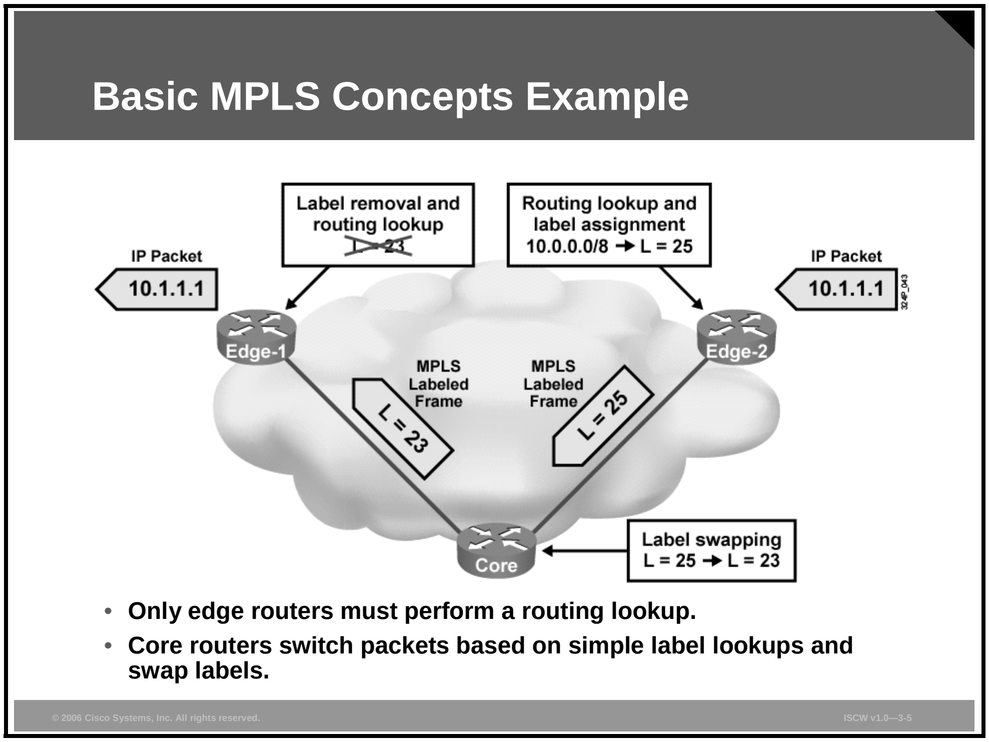
MPLS is designed to support forwarding of protocols other than TCP/IP. Label switching within the network is performed in the same manner regardless of the Layer 3 protocol.

In MPLS labeling in larger networks, only the edge routers perform a routing lookup. All the core routers forward packets based on the labels, which leads to faster forwarding of packets through the service provider 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 self-study.

Example: MPLS Concepts

The figure illustrates a situation in which the intermediary router, or core router, does not have to perform a time-consuming routing lookup. Instead, the core router simply swaps a label with another label (25 is replaced by 23) and forwards the packet to the Edge-1 router based on the label received from the Edge-1 (23).



Basic MPLS Concepts Example

Label removal and routing lookup
~~L = 23~~

Routing lookup and label assignment
10.0.0.0/8 → L = 25

Label swapping
L = 25 → L = 23

- Only edge routers must perform a routing lookup.
- Core routers switch packets based on simple label lookups and swap labels.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-5

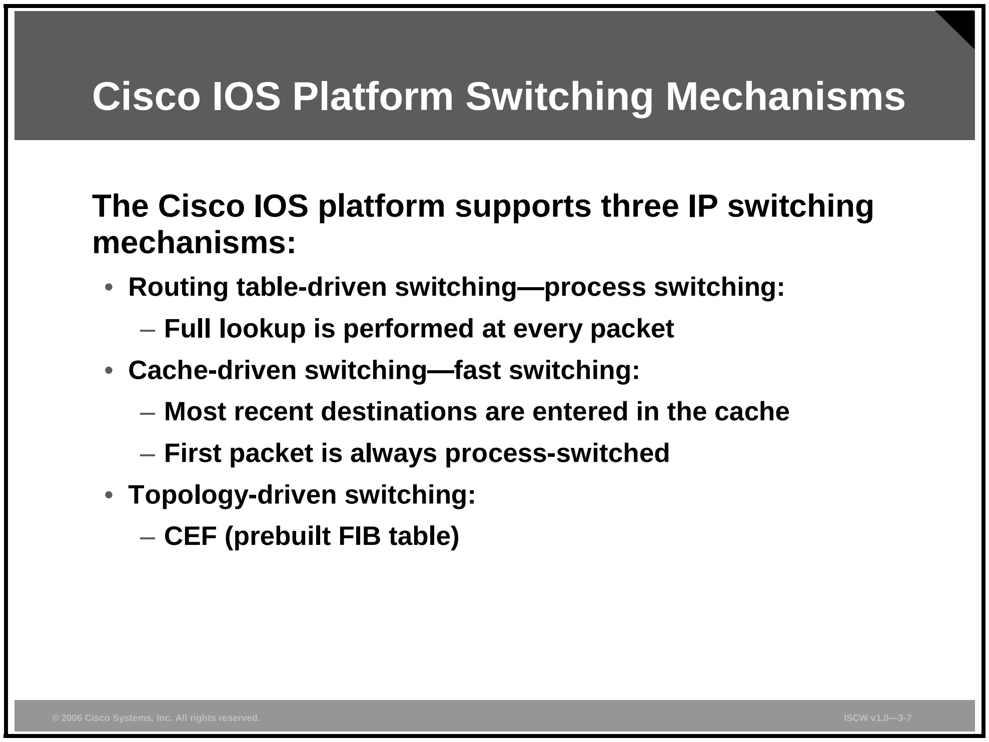
In this example, assume that the Edge-2 router is informed that, in order to reach the 10.1.1.1 network, it should assign a label of 25 to the packet and forward the packet to the core router. The core router is informed that when it receives a packet with a label of 25, it should swap that label with a label of 23 and forward the packet to the Edge-1 router. The actual method used to inform the routers of these label allocations is discussed later.

In larger networks, the result of MPLS labeling is that only the routers at the edge of an MPLS network perform a routing lookup. All the core MPLS routers forward packets based on labels.

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

Router Switching Mechanisms

This topic describes the router switching mechanisms.



Cisco IOS Platform Switching Mechanisms

The Cisco IOS platform supports three IP switching mechanisms:

- **Routing table-driven switching—process switching:**
  - **Full lookup is performed at every packet**
- **Cache-driven switching—fast switching:**
  - **Most recent destinations are entered in the cache**
  - **First packet is always process-switched**
- **Topology-driven switching:**
  - **CEF (prebuilt FIB table)**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-7

Because Cisco Express Forwarding (CEF) provides the foundation for MPLS switching, it is important to understand the purpose of CEF and how it functions, and how the network uses CEF information when forwarding packets.

What Are Cisco IOS Platform Switching Mechanisms?

The first and oldest switching mechanism available in Cisco routers is process switching. Because process switching must find a destination in the routing table (possibly a recursive lookup) and construct a new Layer 2 frame header for every packet, it is very slow and is normally not used.

To overcome the slow performance of process switching, Cisco IOS platforms support several switching mechanisms that use a cache to store the most recently used destinations. The cache uses a faster searching mechanism and it stores the entire Layer 2 frame header to improve the encapsulation performance. The first packet whose destination is not found in the fast-switching cache is process-switched, and an entry is created in the cache. The subsequent packets are switched in the interrupt code using the cache to improve performance.

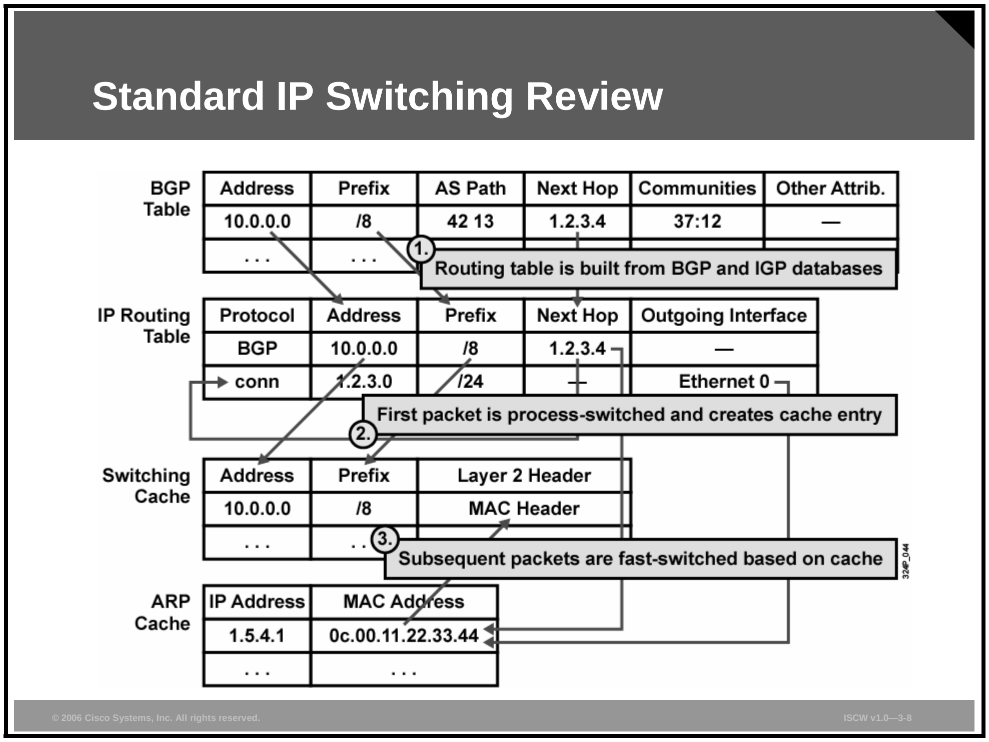
The latest and preferred Cisco IOS platform switching mechanism is CEF, which incorporates the best of the previous switching mechanisms. CEF supports per-packet load balancing (previously supported only by process switching), per-source or per-destination load balancing, fast destination lookup, and many other features not supported by other switching mechanisms.

The CEF cache, or Forwarding Information Base (FIB) table, is essentially a replacement for the standard routing table.

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

Using Standard IP Switching

There is a specific sequence of events that occurs when process switching and fast switching are used for destinations learned through Border Gateway Protocol (BGP). The figure illustrates this sequence of events.



Standard IP Switching Review

BGP Table

Address	Prefix	AS Path	Next Hop	Communities	Other Attrib.
10.0.0.0	/8	42 13	1.2.3.4	37:12	—
. . .	. . .				

1. Routing table is built from BGP and IGP databases

IP Routing Table

Protocol	Address	Prefix	Next Hop	Outgoing Interface
BGP	10.0.0.0	/8	1.2.3.4	—
conn	1.2.3.0	/24	—	Ethernet 0

2. First packet is process-switched and creates cache entry

Switching Cache

Address	Prefix	Layer 2 Header
10.0.0.0	/8	MAC Header
. . .	. .	

3. Subsequent packets are fast-switched based on cache

ARP Cache

IP Address	MAC Address
1.5.4.1	0c.00.11.22.33.44
. . .	. . .

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-8

The following steps occur with process switching and fast switching:

Step 1 When a BGP update is received and processed in the BGP table, an entry is created in the routing table if it is selected as the best route.

Step 2 When the first packet arrives for this destination, the router tries to find the destination in the fast-switching cache. Because the destination is not in the fast-switching cache, process switching has to switch the packet. A recursive lookup is performed to find the outgoing interface. If the Layer 2 address is not found in the cache, an Address Resolution Protocol (ARP) request is triggered. In this example, if the destination is in network 10.0.0.0/8, the next hop to reach network 10.0.0.0/8, according to BGP, is 1.2.3.4, and to reach network 1.2.3.0/24, the outgoing interface is Ethernet 0. Finally, an entry is created in the fast-switching cache.

Step 3 All subsequent packets for the same destination are fast-switched, as follows:

— The switching occurs in the interrupt code (the packet is processed immediately).

— Fast destination lookup is performed (no recursive lookup).

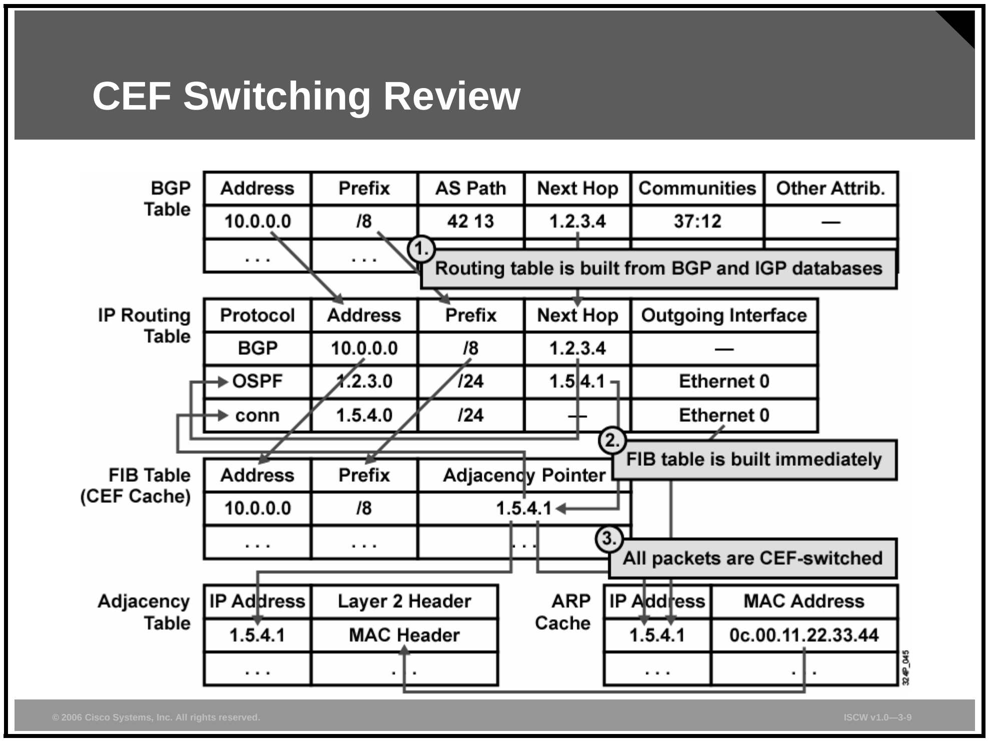
— The encapsulation uses a pregenerated Layer 2 header that contains the destination and Layer 2 source (MAC) address. (No ARP request or ARP cache lookup is necessary.)

Whenever a router receives a packet that should be fast-switched but the destination is not in the switching cache, the packet is process-switched. A full routing table lookup is performed, and an entry in the fast-switching cache is created to ensure that the subsequent packets for the same destination prefix will be fast-switched.

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

What Is CEF Switching Architecture?

CEF uses a different architecture from process switching or any other cache-based switching mechanism.



CEF Switching Review

BGP Table

Address	Prefix	AS Path	Next Hop	Communities	Other Attrib.
10.0.0.0	/8	42 13	1.2.3.4	37:12	—
. . .	. . .				

1. Routing table is built from BGP and IGP databases

IP Routing Table

Protocol	Address	Prefix	Next Hop	Outgoing Interface
BGP	10.0.0.0	/8	1.2.3.4	—
OSPF	1.2.3.0	/24	1.5.4.1	Ethernet 0
conn	1.5.4.0	/24	—	Ethernet 0

2. FIB table is built immediately

FIB Table (CEF Cache)

Address	Prefix	Adjacency Pointer
10.0.0.0	/8	1.5.4.1
. . .	. . .	. . .

3. All packets are CEF-switched

Adjacency Table

IP Address	Layer 2 Header
1.5.4.1	MAC Header
. . .	. . .

ARP Cache

IP Address	MAC Address
1.5.4.1	0c.00.11.22.33.44
. . .	. . .

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-9

CEF uses a complete IP switching table, the FIB table, which holds the same information as the IP routing table. The generation of entries in the FIB table is not packet-triggered but change-triggered. When something changes in the IP routing table, the change is also reflected in the FIB table.

Because the FIB contains the complete IP switching table, the router can make definitive decisions based on the information in it. Whenever a router receives a packet that should be CEF-switched, but the destination is not in the FIB, the packet is dropped.

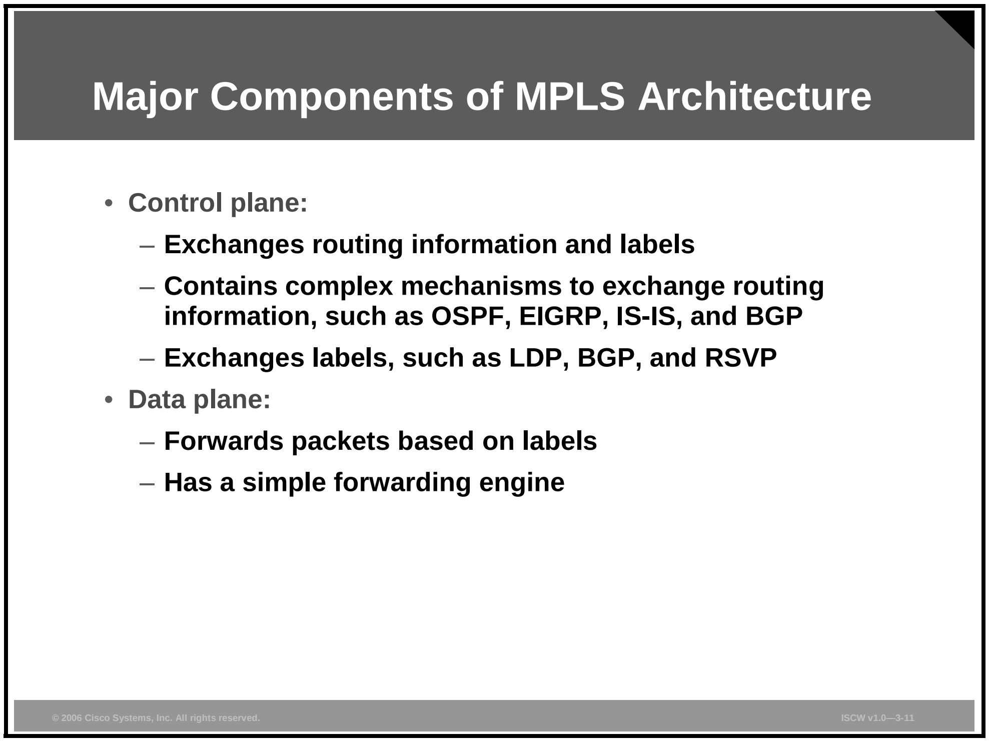
The FIB table is also different from other fast-switching caches in that it does not contain information about the outgoing interface and the corresponding Layer 2 header. That information is stored in a separate table, the adjacency table. This table is more or less a copy of the ARP cache, but instead of holding only the destination MAC address, it holds the Layer 2 header.

Note If the router carries full Internet routing (more than 100,000 networks), enabling the CEF may consume excessive memory. Enabling the distributed CEF will also affect memory utilization on Versatile Interface Processor (VIP) modules or line cards, because the entire FIB table will be copied to all VIP modules or line cards.

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

MPLS Architecture

This topic describes the main components of the MPLS architecture.



Major Components of MPLS Architecture

- Control plane:
  - Exchanges routing information and labels
  - Contains complex mechanisms to exchange routing information, such as OSPF, EIGRP, IS-IS, and BGP
  - Exchanges labels, such as LDP, BGP, and RSVP
- Data plane:
  - Forwards packets based on labels
  - Has a simple forwarding engine

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-11

To support multiple protocols, MPLS divides the classic router architecture into two major components:

- **Control plane:** Control plane takes care of the routing information exchange and the label exchange between adjacent devices.
- **Data plane:** Data plane takes care of forwarding based on either destination addresses or labels; this is also known as the forwarding plane.

A large number of different routing protocols, such as Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), Routing Information Protocol (RIP), and BGP, can be used in the control plane.

The control plane also requires protocols, such as the label exchange protocols: MPLS Label Distribution Protocol (LDP) or BGP (used by MPLS VPN).

Resource Reservation Protocol (RSVP) is used by MPLS Traffic Engineering to reserve resources (bandwidth) in the network.

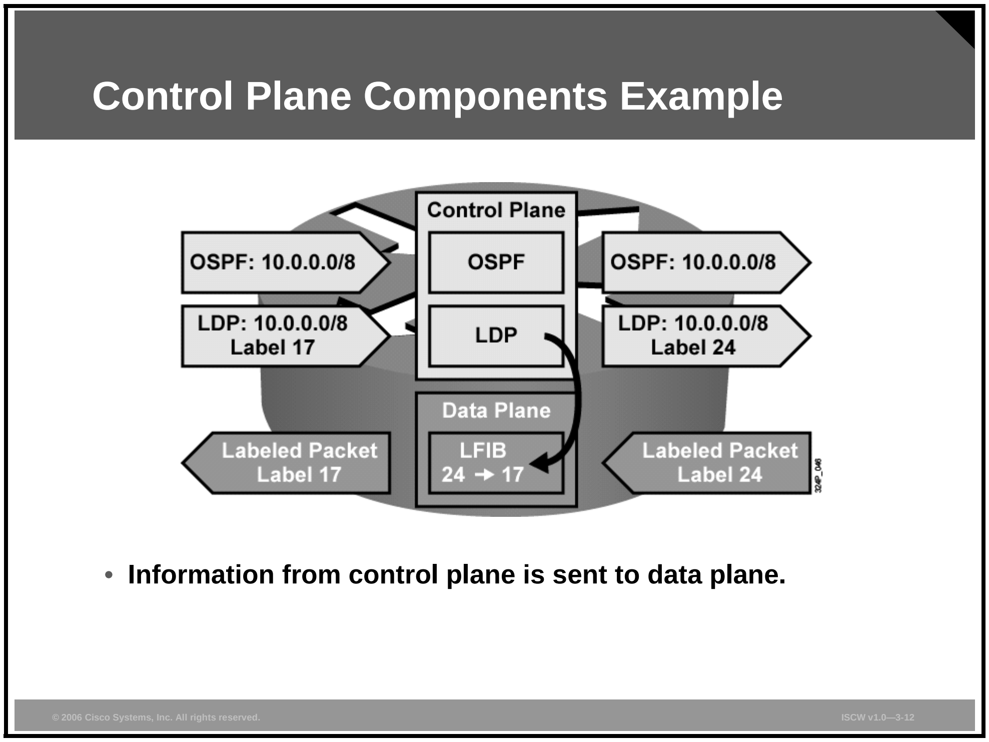
The data plane, however, is a simple label-based forwarding engine that is independent of the type of routing protocol or label exchange protocol. The Label Forwarding Information Base (LFIB) table is used to store the label information that the forwarding engine uses to forward packets. The LFIB table is populated by the label exchange protocol used (LDP, BGP, or RSVP).

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

Example: Control Plane Components

MPLS can implement destination-based forwarding that uses labels to make forwarding decisions.

In this example, a Layer 3 routing protocol is needed to propagate Layer 3 routing information. A label exchange mechanism is simply an add-on to propagate labels that are used for Layer 3 destinations.



Control Plane Components Example

- **Information from control plane is sent to data plane.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-12

The figure illustrates the two components of the control plane:

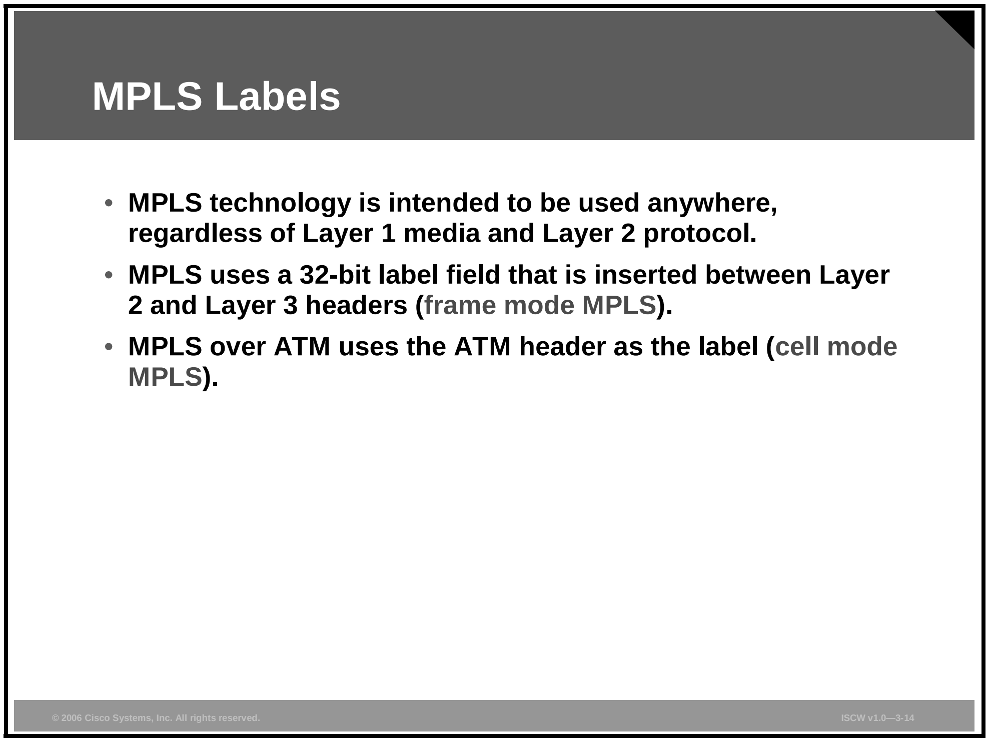
- OSPF, which receives and forwards a routing update for IP network 10.0.0.0/8.
- LDP, which receives label 17 to be used for packets with destination address 10.x.x.x. A local label 24 is generated and sent to upstream neighbors when the packets are destined for 10.x.x.x. LDP inserts an entry into the LFIB table of the data plane, where an incoming label 24 is mapped to an outgoing label 17.

The data plane then forwards all packets with label 24 through the appropriate interfaces after swapping label 24 for label 17.

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

MPLS Labels

This topic describes the structure of an MPLS label and its format.



MPLS Labels

- **MPLS technology is intended to be used anywhere, regardless of Layer 1 media and Layer 2 protocol.**
- **MPLS uses a 32-bit label field that is inserted between Layer 2 and Layer 3 headers (frame mode MPLS).**
- **MPLS over ATM uses the ATM header as the label (cell mode MPLS).**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-14

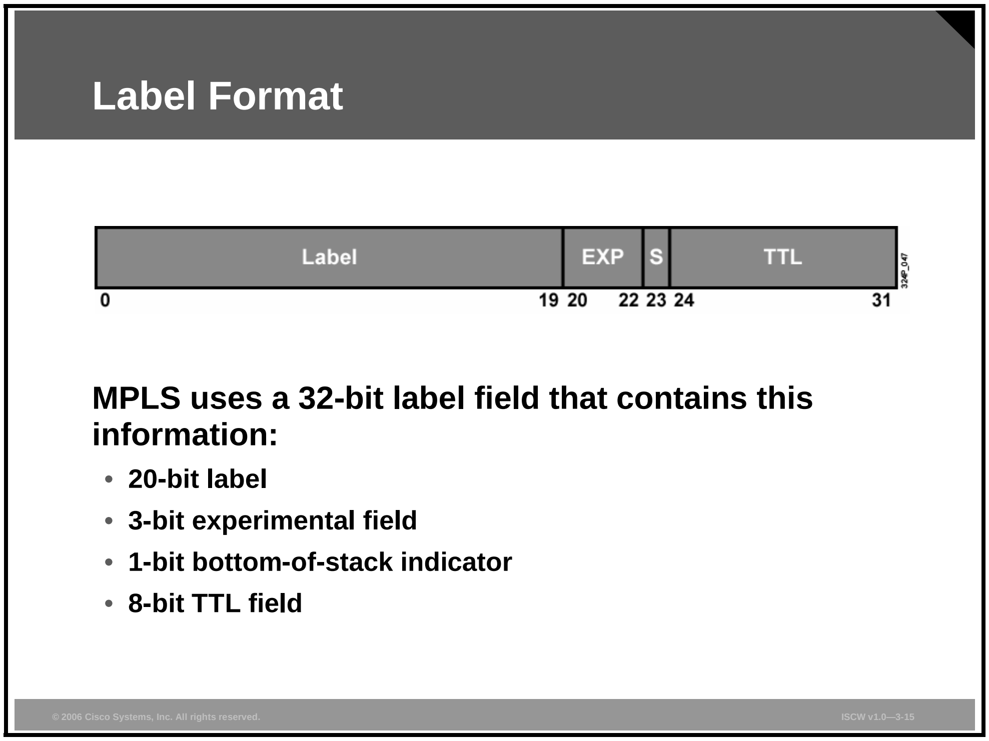
MPLS is designed for use on any media and Layer 2 encapsulation. Most Layer 2 encapsulations are frame-based, and MPLS simply inserts (commonly called “imposes”) a 32-bit label between the Layer 2 and Layer 3 headers (frame mode MPLS).

ATM is a special case where fixed-length cells are used and a label cannot be inserted on every cell. MPLS uses the virtual path identifier/virtual channel identifier (VPI/VCI) fields in the ATM header as a label (cell mode MPLS).

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

Label Format

The 32-bit MPLS label contains four fields.



Label Format

MPLS uses a 32-bit label field that contains this information:

- **20-bit label**
- **3-bit experimental field**
- **1-bit bottom-of-stack indicator**
- **8-bit TTL field**

© 2006 Cisco Systems, Inc. All rights reserved.   ISCW v1.0—3-15

The table describes the fields contained in the 32-bit MPLS label.

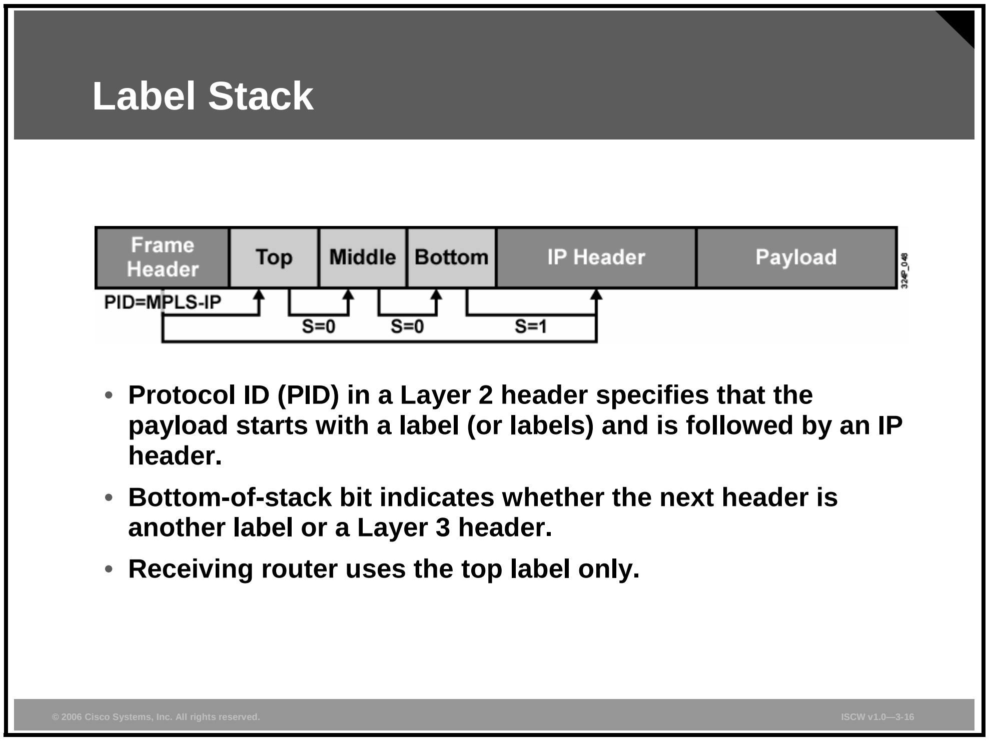
32-Bit Label Fields

Field	Description
20-bit label	The actual label. Values 0 to 15 are reserved.
3-bit experimental (EXP) field	Undefined in the RFC. Used by Cisco to define a class of service (CoS) (IP precedence).
Bottom-of-stack bit	MPLS allows multiple labels to be inserted. The bottom-of-stack bit determines if this label is the last label in the packet. If this bit is set (1), it indicates that this is the last label.
8-bit Time to Live (TTL) field	Has the same purpose as the TTL field in the IP header.

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

Label Stack

A label does not contain any information about the Layer 3 protocol that is being carried in a packet. A new protocol ID (PID) is used for every MPLS-enabled Layer 3 protocol.



Label Stack

- **Protocol ID (PID) in a Layer 2 header specifies that the payload starts with a label (or labels) and is followed by an IP header.**
- **Bottom-of-stack bit indicates whether the next header is another label or a Layer 3 header.**
- **Receiving router uses the top label only.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-16

Usually, only one label is assigned to a packet. Here are some scenarios in which more than one label is used:

- **MPLS VPNs:** Multiprotocol BGP (MP-BGP) is used to propagate a second label that identifies the VPN in addition to the one that is propagated by LDP to identify the path.
- **MPLS TE:** MPLS traffic engineering (TE) uses RSVP to establish Label Switched Path (LSP) tunnels. RSVP propagates labels that are used to identify the tunnel LSP in addition to the one that is propagated by LDP to identify the underlying LSP.
- **MPLS VPNs combined with MPLS TE:** Three or more labels are used to identify the VPN, tunnel LSP, and the underlying LSP.

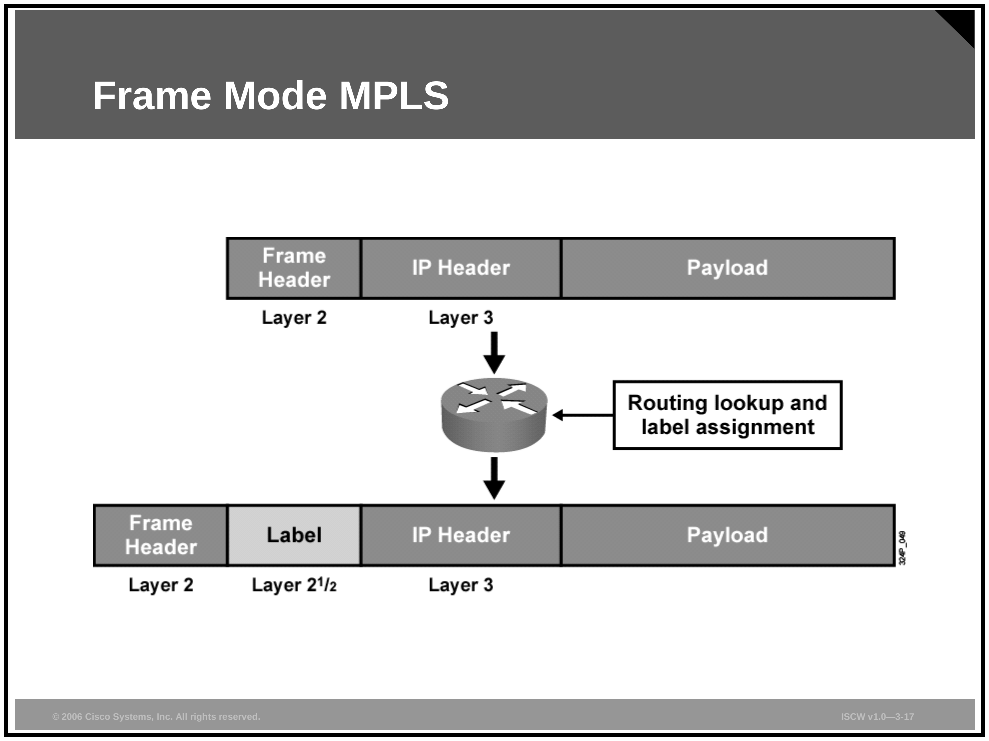
These Ethertype values are used to identify Layer 3 protocols with most Layer 2 encapsulations:

- **Unlabeled IP unicast:** PID = 0x0800 identifies that the frame payload is a classic unicast IP packet.
- **Labeled IP unicast:** PID = 0x8847 identifies that the frame payload is a unicast IP packet with at least one label preceding the IP header. The bottom-of-stack bit indicates when the IP header actually starts.
- **Labeled IP multicast:** PID = 0x8848 identifies that the frame payload is a multicast IP packet with at least one label preceding the IP header. The bottom-of-stack bit indicates when the IP header actually starts.

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

Example: Frame Mode MPLS

The figure shows an edge router that receives a normal IP packet.



Frame Mode MPLS

Frame Header	IP Header	Payload
Layer 2	Layer 3	

Routing lookup and label assignment

Frame Header	Label	IP Header	Payload
Layer 2	Layer $2\frac{1}{2}$	Layer 3	

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-17

The ingress edge router performs these tasks after it receives an IP packet:

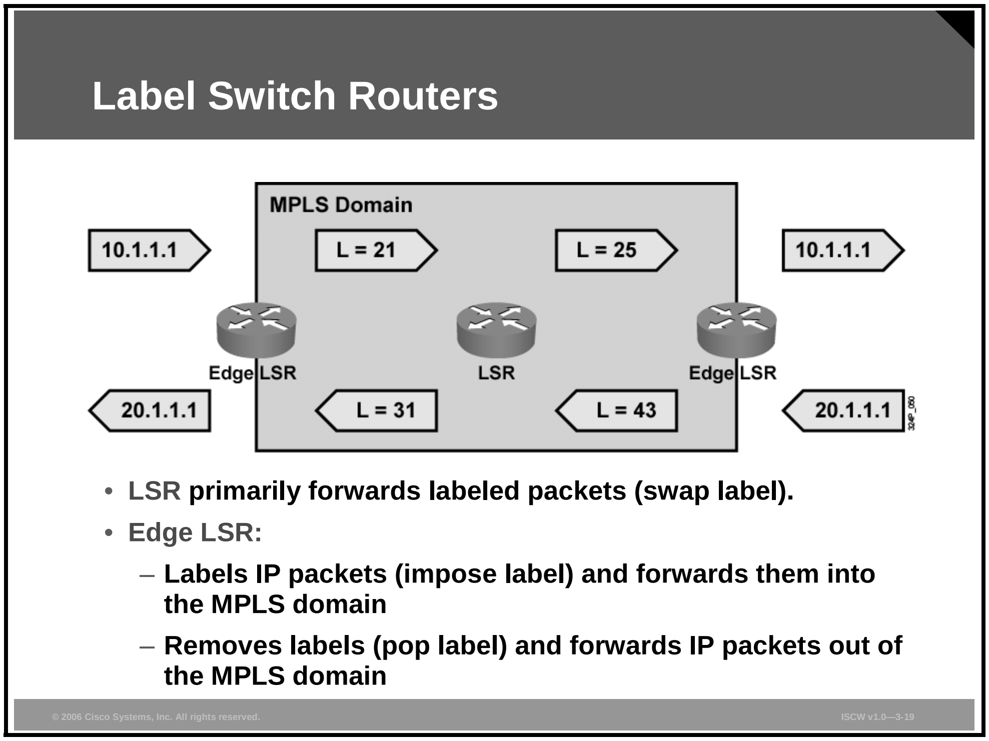
- It performs a routing lookup to determine the outgoing interface.
- If the outgoing interface is enabled for MPLS and if a next-hop label for the destination exists, it assigns and inserts a label between the Layer 2 frame header and the Layer 3 packet header. The router then changes the Layer 2 Ethertype value to indicate that this is a labeled packet.
- The router sends the labeled packet.

Note Other routers in the core simply forward packets based on the label.

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

Label Switch Routers

This topic describes Label Switch Routers (LSRs) and edge LSRs, and the function they serve in MPLS networks.



Label Switch Routers

- **LSR primarily forwards labeled packets (swap label).**
- **Edge LSR:**
  - **Labels IP packets (impose label) and forwards them into the MPLS domain**
  - **Removes labels (pop label) and forwards IP packets out of the MPLS domain**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-19

Some of the terminology used in describing MPLS is as follows:

- **LSR:** A device that forwards packets primarily based on labels.
- **Edge LSR:** A device that primarily labels packets or removes labels.

Note LSR and Edge LSR are only used in this context in the RFC. Cisco refers to LSR as the general class of router running MPLS. What the RFC refers to as LSR, Cisco calls a P router; what the RFC refers to as Edge LSR, Cisco calls a provider edge router (PE router).

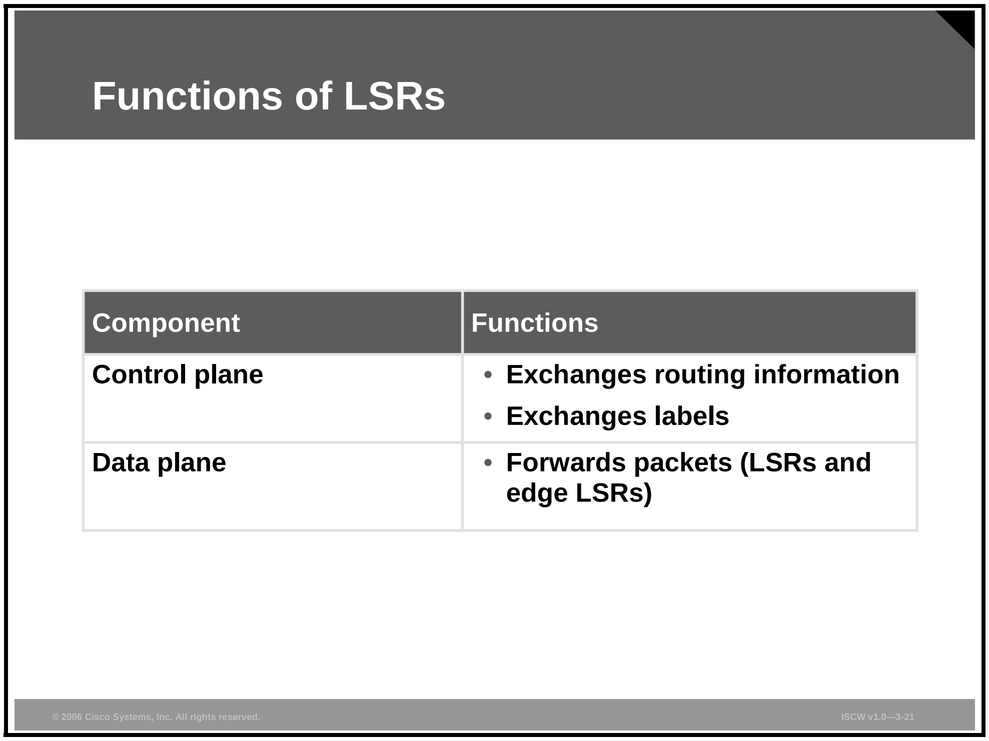
LSRs and edge LSRs are usually capable of doing both label switching and IP routing. Their names are based on their positions in an MPLS domain. Routers that have all interfaces enabled for MPLS are called LSRs because they mostly forward labeled packets. Routers that have some interfaces that are not enabled for MPLS are usually at the edge of an MPLS domain—autonomous systems (ASs). These routers also forward packets based on IP destination addresses and label them if the outgoing interface is enabled for MPLS.

For example, an edge LSR receives a packet for destination 10.1.1.1, imposes label 21, and forwards the frame to the LSR in the MPLS backbone. LSR swaps label 21 with label 25 and forwards the frame. The edge LSR removes label 25 and forwards the packet based on IP destination address 10.1.1.1.

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 self-study.

LSR Component Architecture

This topic explains the process that occurs between the components of an LSR to enable labeling and forwarding of labeled packets.



Functions of LSRs

Component	Functions
Control plane	• **Exchanges routing information** • **Exchanges labels**
Data plane	• **Forwards packets (LSRs and edge LSRs)**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-21

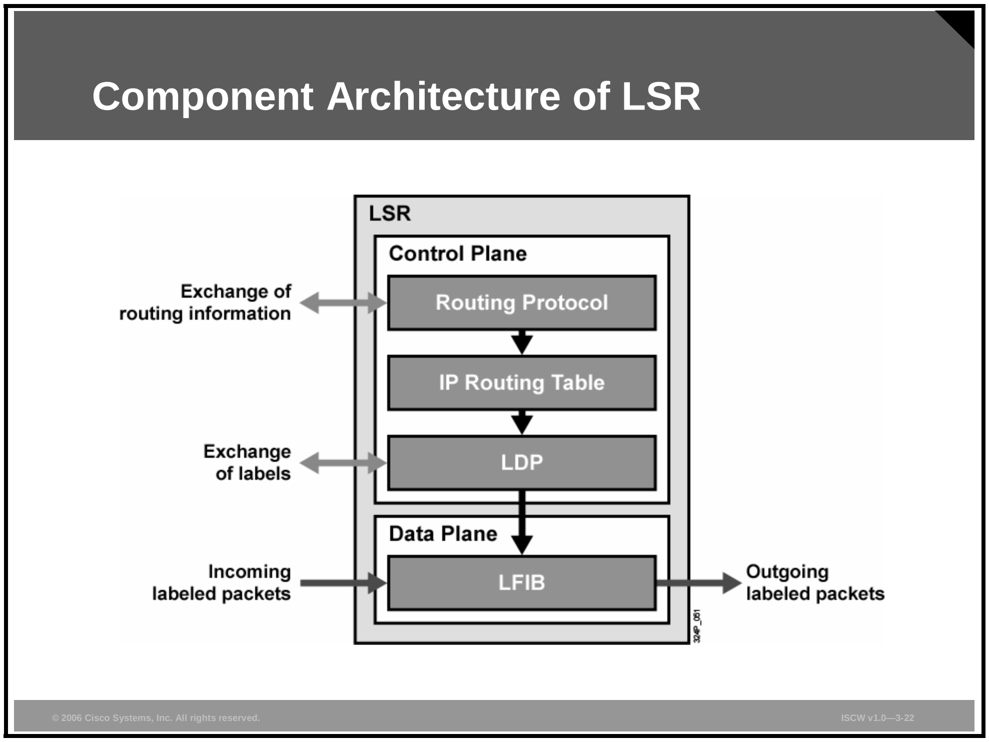
LSRs of all types must perform these functions:

- Exchange routing information (control plane)
- Exchange labels (control plane)
- Forward packets (data plane): Frame mode MPLS forwards packets based on the 32-bit label

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

Component Architecture of LSR

The primary function of an LSR is to forward labeled packets. Therefore, every LSR needs a Layer 3 routing protocol (for example, OSPF, EIGRP, or IS-IS) and a label distribution protocol (for example, LDP).



Component Architecture of LSR

© 2006 Cisco Systems, Inc. All rights reserved.

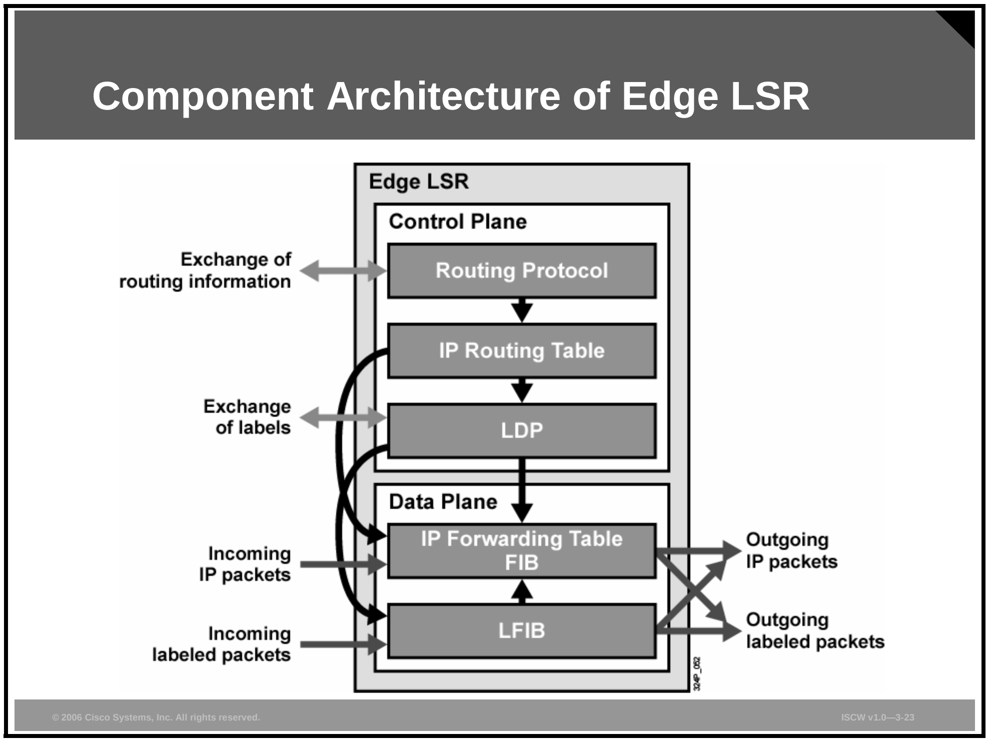
ISCW v1.0—3-22

LDP populates the LFIB table in the data plane that is used to forward labeled packets.

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

Component Architecture of Edge LSR

Edge LSRs also forward IP packets based on their IP destination addresses and, optionally, label them if a label exists.



Component Architecture of Edge LSR

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-23

These combinations are possible:

- A received IP packet is forwarded based on the IP destination address and sent as an IP packet.
- A received IP packet is forwarded based on the IP destination address and sent as a labeled packet.
- A received labeled packet is forwarded based on the label; the label is changed (swapped) and the labeled packet is sent.
- A received labeled packet is forwarded based on the label; the label is removed and the IP packet is sent.

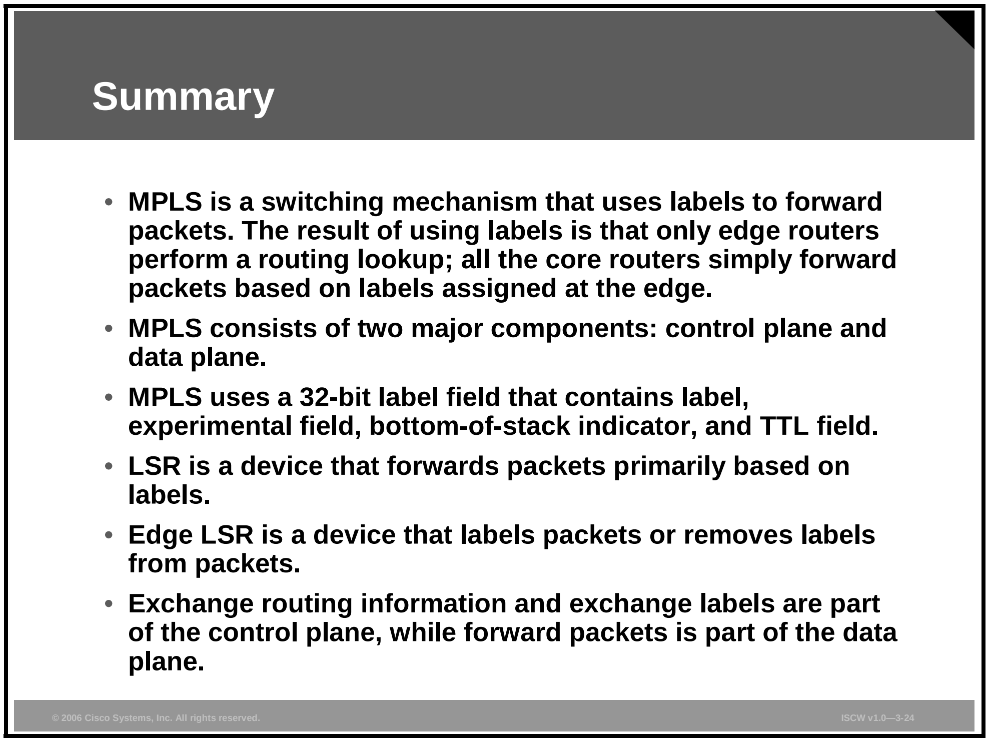
These scenarios are possible if the network is not configured properly:

- A received labeled packet is dropped if the label is not found in the LFIB table, even if the IP destination exists in the IP forwarding table—also called the FIB.
- A received IP packet is dropped if the destination is not found in the IP forwarding table (FIB table), even if there is an MPLS label-switched path toward the destination.

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

Summary

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



Summary

- MPLS is a switching mechanism that uses labels to forward packets. The result of using labels is that only edge routers perform a routing lookup; all the core routers simply forward packets based on labels assigned at the edge.
- MPLS consists of two major components: control plane and data plane.
- MPLS uses a 32-bit label field that contains label, experimental field, bottom-of-stack indicator, and TTL field.
- LSR is a device that forwards packets primarily based on labels.
- Edge LSR is a device that labels packets or removes labels from packets.
- Exchange routing information and exchange labels are part of the control plane, while forward packets is part of the data plane.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-24

References

For additional information, refer to these resources:

- RFC 3031: *Multiprotocol Label Switching Architecture* at http://www.ietf.org/rfc/rfc3031.txt
- RFC 3032: *MPLS Label Stack Encoding* at http://www.ietf.org/rfc/rfc3032.txt

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

Lesson 2

Assigning MPLS Labels to Packets

Overview

This lesson describes how label allocation and label distribution function in a frame mode Multiprotocol Label Switching (MPLS) network. The lesson also describes how MPLS uses the Penultimate Hop Popping (PHP) function to eliminate routing lookups, and how the MPLS data structures are built. The lesson also explains how information gets distributed and placed into appropriate tables for both labeled and unlabeled packet usage.

Objectives

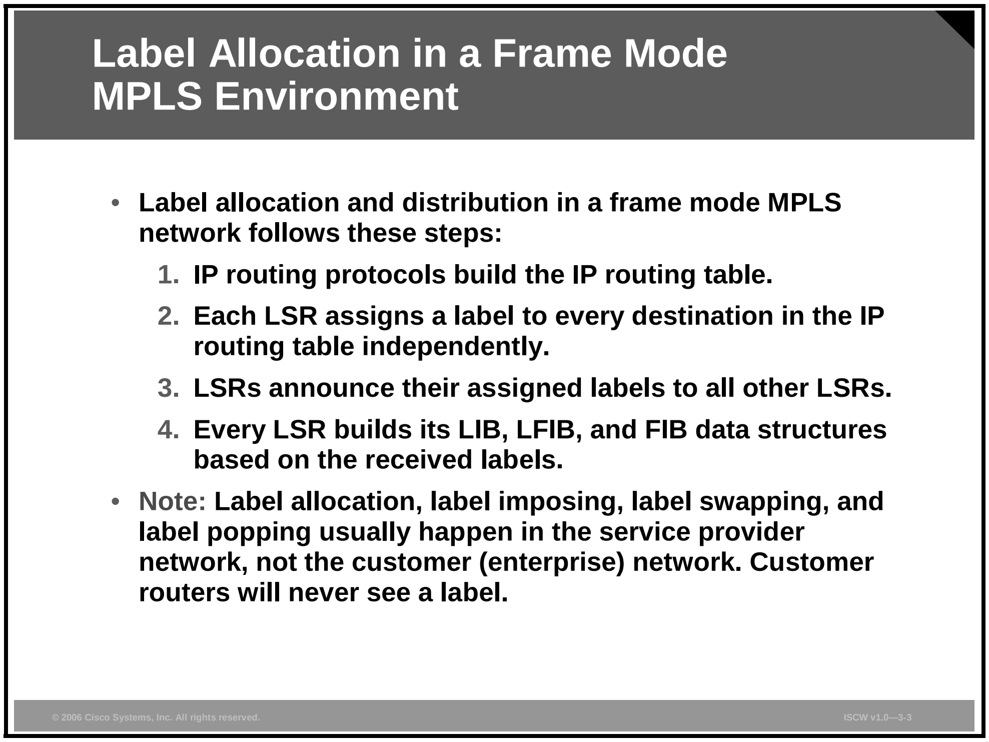
Upon completing this lesson, you will be able to describe how labels are allocated and distributed in a frame mode MPLS network, and describe how IP packets cross an MPLS network. This ability includes being able to meet these objectives:

- Identify how label allocation is performed in a frame mode MPLS network
- Identify how labels are distributed in a frame mode MPLS network
- Explain how the LFIB table is populated
- Identify packet propagation across an MPLS network
- Describe how PHP improves MPLS performance by eliminating routing lookups on egress LSRs

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

Label Allocation in a Frame Mode MPLS Environment

This topic describes how labels are allocated and distributed in a frame mode MPLS network.



Label Allocation in a Frame Mode MPLS Environment

- **Label allocation and distribution in a frame mode MPLS network follows these steps:**
  1. **IP routing protocols build the IP routing table.**
  2. **Each LSR assigns a label to every destination in the IP routing table independently.**
  3. **LSRs announce their assigned labels to all other LSRs.**
  4. **Every LSR builds its LIB, LFIB, and FIB data structures based on the received labels.**
- **Note: Label allocation, label imposing, label swapping, and label popping usually happen in the service provider network, not the customer (enterprise) network. Customer routers will never see a label.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-3

Label allocation and distribution in a Unicast IP routing network and MPLS functionality, including label allocation and distribution, can be divided into these steps:

Step 1 The routers exchange information using standard or vendor-specific Interior Gateway Protocol (IGP), such as Open Shortest Path First [OSPF], Intermediate System-to-Intermediate System [IS-IS], and Enhanced Interior Gateway Routing Protocol [EIGRP]).

Step 2 Local labels are generated. One locally unique label is assigned to each IP destination found in the main routing table and stored in the Label Information Base (LIB) table.

Step 3 Local labels are propagated to adjacent routers, where these labels might be used as next-hop labels (stored in the Forwarding Information Base [FIB] and Label Forwarding Information Base [LFIB] tables to enable label switching).

Step 4 Every label switch router (LSR) builds its LIB, LFIB, and FIB data structures based on received labels.

These data structures contain label information:

- The LIB, in the control plane, is the database used by Label Distribution Protocol (LDP) where an IP prefix is assigned a locally significant label that is mapped to a next-hop label that has been learned from a downstream neighbor.
- The LFIB, in the data plane, is the database used to forward labeled packets. Local labels, previously advertised to upstream neighbors, are mapped to next-hop labels, previously received from downstream neighbors.

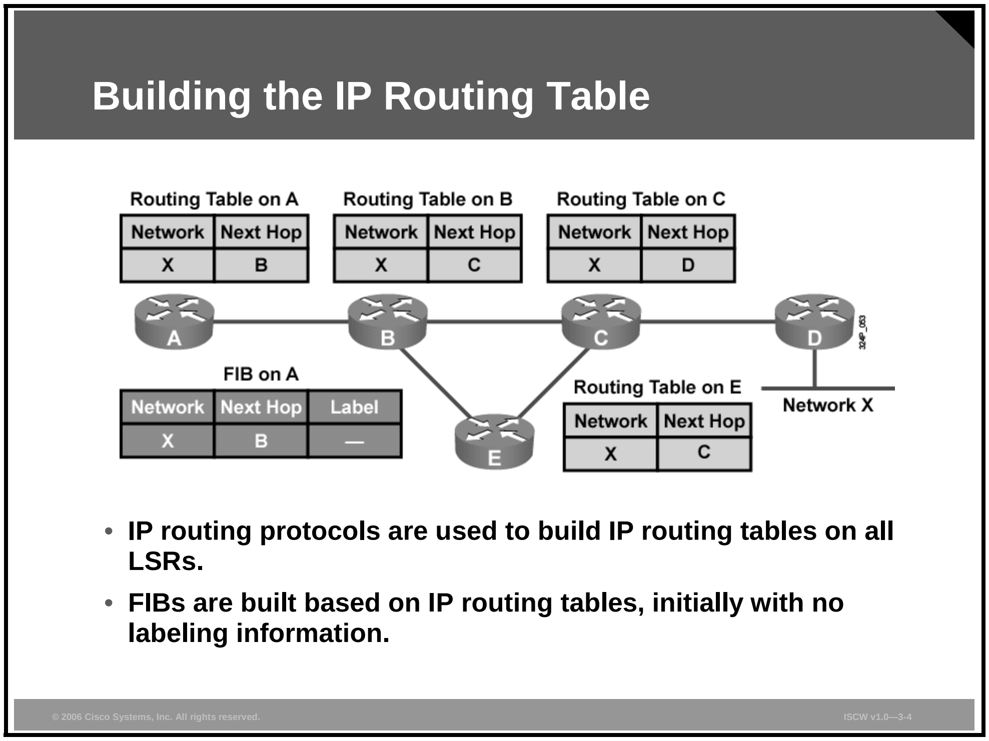
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- The FIB, in the data plane, is the database used to forward unlabeled IP packets. A forwarded packet is labeled if a next-hop label is available for a specific destination IP network. Otherwise, a forwarded packet is not labeled.

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

Example: Label Allocation

The figure illustrates how all routers learn about network X via an IGP, such as OSPF, IS-IS, or EIGRP.



Building the IP Routing Table

Routing Table on A

Network	Next Hop
X	B

Routing Table on B

Network	Next Hop
X	C

Routing Table on C

Network	Next Hop
X	D

FIB on A

Network	Next Hop	Label
X	B	—

Routing Table on E

Network	Next Hop
X	C

- **IP routing protocols are used to build IP routing tables on all LSRs.**
- **FIBs are built based on IP routing tables, initially with no labeling information.**

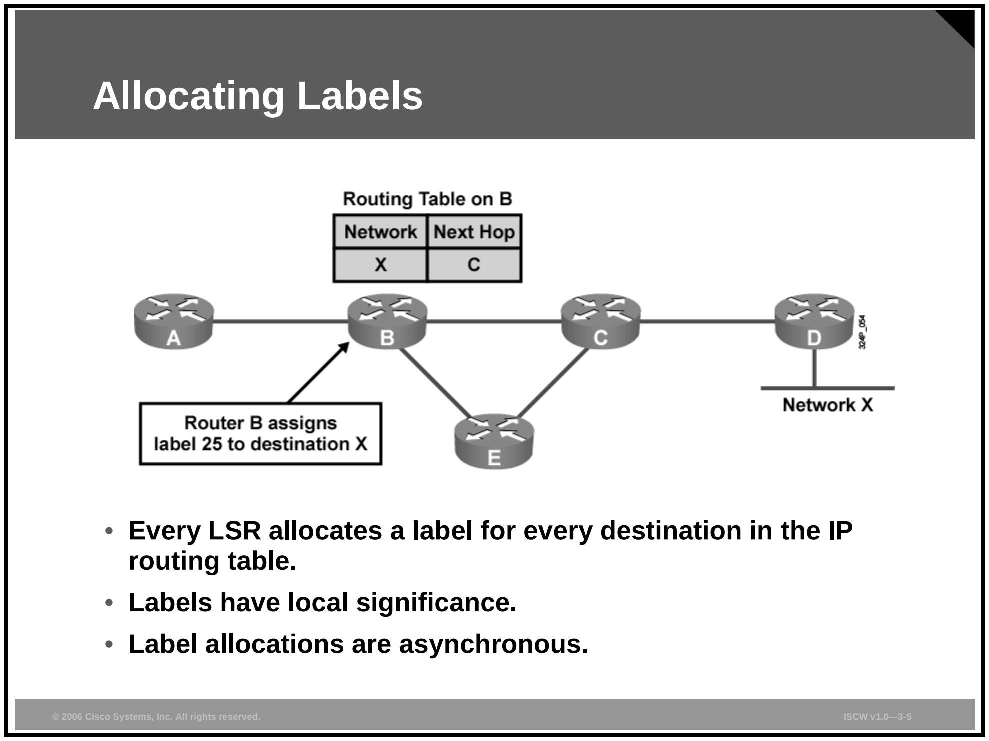
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-4

As a starting point for this example, the IGP has converged and the FIB table on router A contains the entry for network X that is mapped to the IP next-hop address B. However, at this time, a next-hop label is not available, which means that all packets are forwarded in a traditional way (as unlabeled packets).

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

Allocating Labels

Routers generate labels regardless of other routers (asynchronous allocation of labels).



Allocating Labels

Routing Table on B

Network	Next Hop
X	C

Router B assigns label 25 to destination X

- **Every LSR allocates a label for every destination in the IP routing table.**
- **Labels have local significance.**
- **Label allocations are asynchronous.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-5

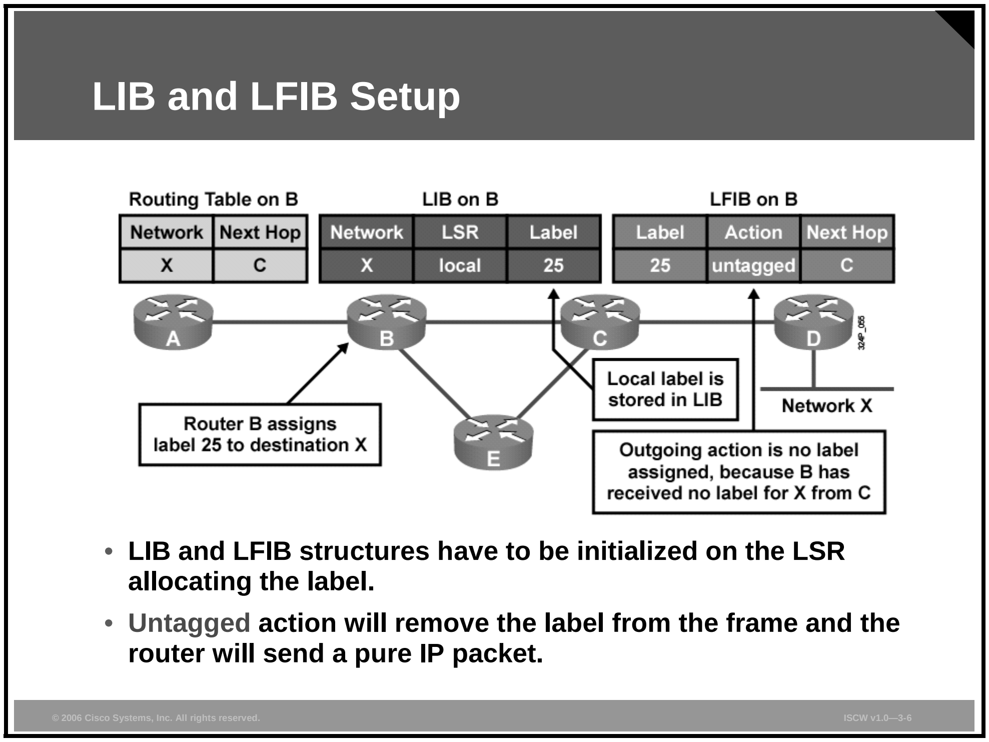
Although any of the routers could be first to generate a label, for this example it is assumed that router B is the first router to generate the label. Router B generates a locally significant and locally unique label (for this example, 25), and assigns it to IP network X.

Note	Labels 0 to 15 are 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 self-study.

LIB and LFIB Setup

When a label is assigned to an IP prefix, it is stored in two tables: LIB and LFIB.



LIB and LFIB Setup

Routing Table on B

Network	Next Hop
X	C

LIB on B

Network	LSR	Label
X	local	25

LFIB on B

Label	Action	Next Hop
25	untagged	C

A
B
C
D
E
Network X
Router B assigns label 25 to destination X
Local label is stored in LIB
Outgoing action is no label assigned, because B has received no label for X from C

- **LIB and LFIB structures have to be initialized on the LSR allocating the label.**
- **Untagged action will remove the label from the frame and the router will send a pure IP packet.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-6

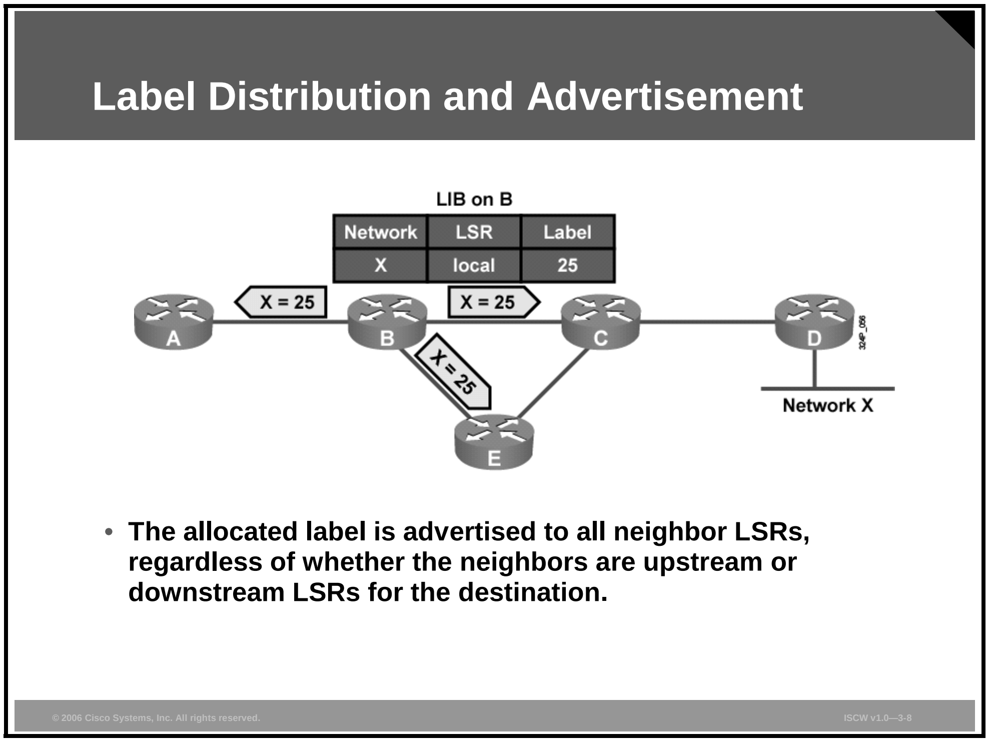
The LIB table is used to maintain the mapping between the IP prefix (network X), the assigned label (25), and the assigning router (local).

The LFIB table is modified to contain the local label mapped to the forwarding action. In this case, the action is untagged because no label for network X has been received from a neighbor. The untagged action is used until the next-hop label is received from the downstream neighbor (router C in this case).

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

Label Distribution and Advertisement

This topic describes how MPLS labels are distributed and advertised within an MPLS network.



Label Distribution and Advertisement

LIB on B

Network	LSR	Label
X	local	25

- **The allocated label is advertised to all neighbor LSRs, regardless of whether the neighbors are upstream or downstream LSRs for the destination.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-8

MPLS adds a new piece of information that must be exchanged between adjacent routers. There are two possible approaches to propagating this additional label information between adjacent routers:

- Extend the functionality of existing routing protocols
- Create a new protocol dedicated to exchanging labels

Extending the functionality of existing router protocols requires much more time and effort because of the large number of different routing protocols. This first approach also causes interoperability problems between routers that support the new functionality and those that do not. Therefore, the Internet Engineering Task Force (IETF) selected the second approach. The LDP in the control plane exchanges labels and stores them in the LIB.

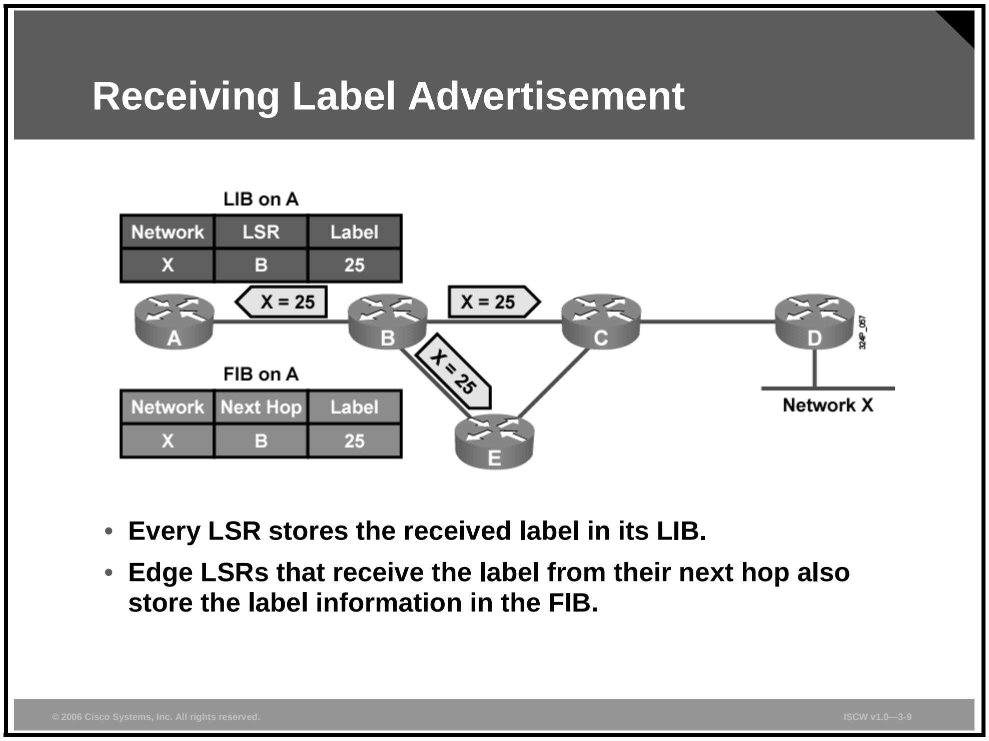
The figure illustrates the next step after a local label has been assigned. Router B propagates this label, 25, to all adjacent neighbors where this label can be used as a next-hop label. The allocated label is advertised to all neighbor LSRs, regardless of whether the neighbors are upstream or downstream LSRs for the destination.

Note	Because router B cannot predict which routers might use it as the downstream neighbor, router B sends its local mappings to all LDP neighbors.

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

Receiving Label Advertisement

Upon receiving an LDP update from router B, routers A, C, and E can fill in the missing information in their LIB, LFIB, and FIB tables.



Receiving Label Advertisement

LIB on A

Network	LSR	Label
X	B	25

FIB on A

Network	Next Hop	Label
X	B	25

- **Every LSR stores the received label in its LIB.**
- **Edge LSRs that receive the label from their next hop also store the label information in the FIB.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-9

Label 25, received from LSR B, is stored in the LIB table as the label for network X.

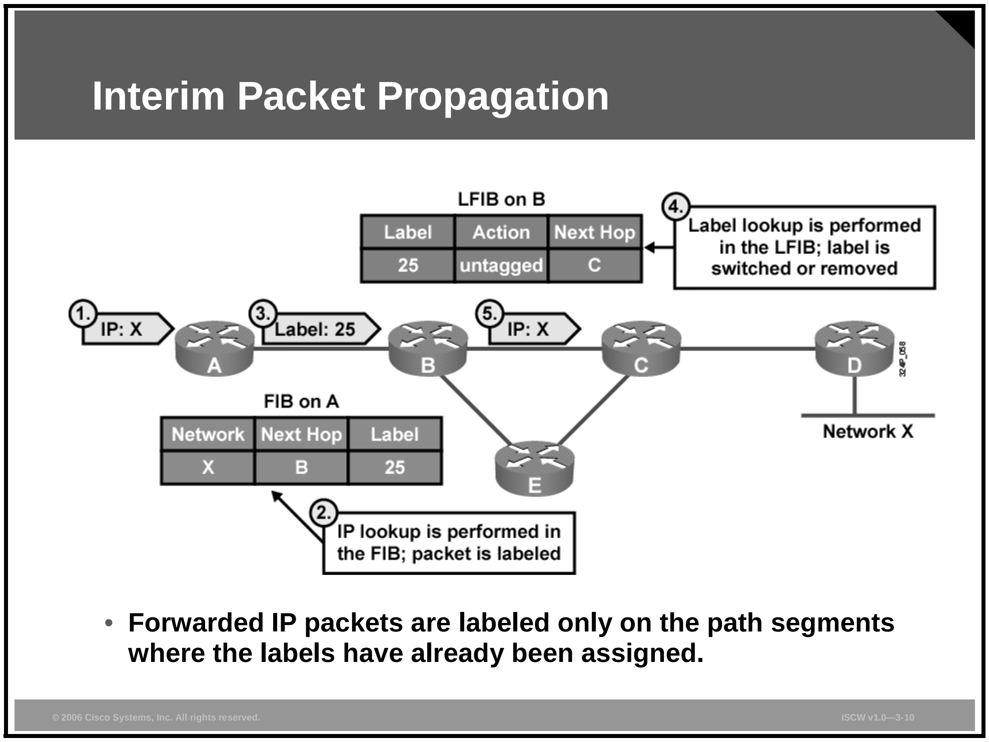
Label 25 is attached to the IP forwarding entry in the FIB table to enable the MPLS edge functionality (incoming IP packets are forwarded as labeled packets).

The local label in the LFIB table is mapped to outgoing label 25 instead of the untagged action (incoming labeled packets can be forwarded as labeled packets).

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

Interim Packet Propagation Through an MPLS Network

The question comes up of what happens if a packet arrives at an MPLS network before all routers have learned the label to network X.



Interim Packet Propagation

LFIB on B

Label	Action	Next Hop
25	untagged	C

4. Label lookup is performed in the LFIB; label is switched or removed

FIB on A

Network	Next Hop	Label
X	B	25

2. IP lookup is performed in the FIB; packet is labeled

- **Forwarded IP packets are labeled only on the path segments where the labels have already been assigned.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-10

The figure shows such an example:

Step 1 An unlabeled IP packet arrives at router A.

Step 2 The packet is forwarded based on the information found in the FIB table on router A.

Step 3 Label 25, found in the FIB table, is used to label the packet and it is forwarded to the next-hop router, router B.

Step 4 Router B must remove the label because LSR B has not yet received any next-hop label (the action in the LFIB is untagged).

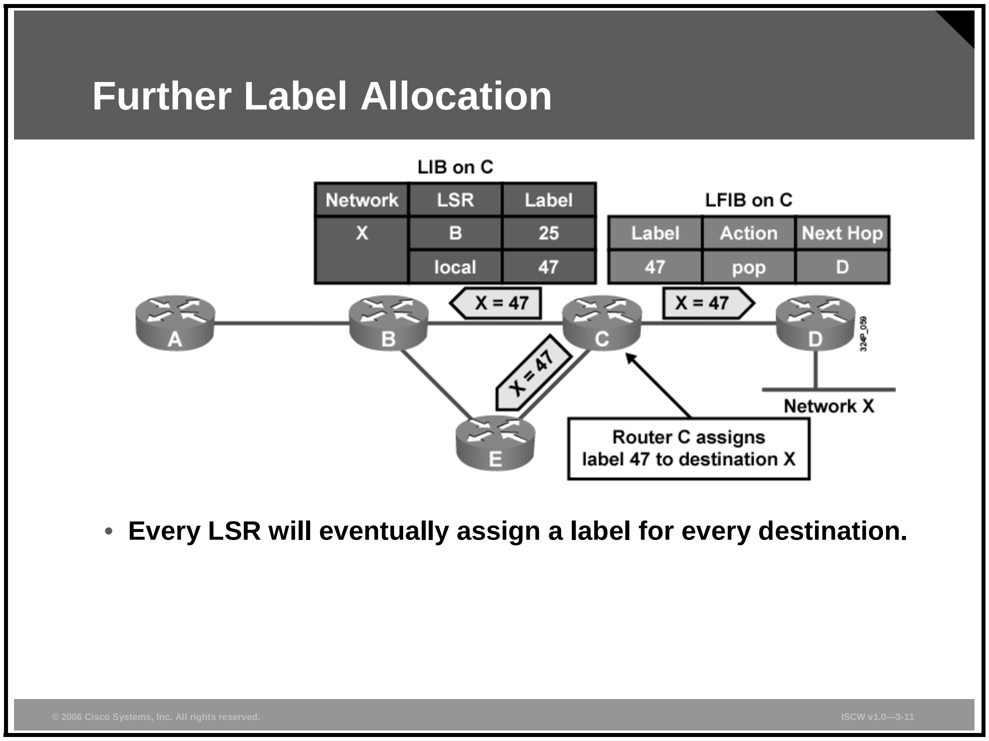
Step 5 The packet is then forwarded as a standard IP packet.

Router A performs an IP lookup (Cisco Express Forwarding [CEF] switching), whereas router B performs a label lookup (label switching) in which the label is removed and a normal IP packet is sent out of router B. This functionality allows MPLS to continue packet forwarding even though label distribution is not complete.

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

Further Label Allocation

Because all routers in an MPLS domain asynchronously do the same as routers A and B, a Label Switch Path (LSP) tunnel is generated, spanning from router A to router D.



Further Label Allocation

LIB on C

Network	LSR	Label
X	B	25
	local	47

LFIB on C

Label	Action	Next Hop
47	pop	D

Router C assigns label 47 to destination X

- **Every LSR will eventually assign a label for every destination.**

© 2006 Cisco Systems, Inc. All rights reserved.

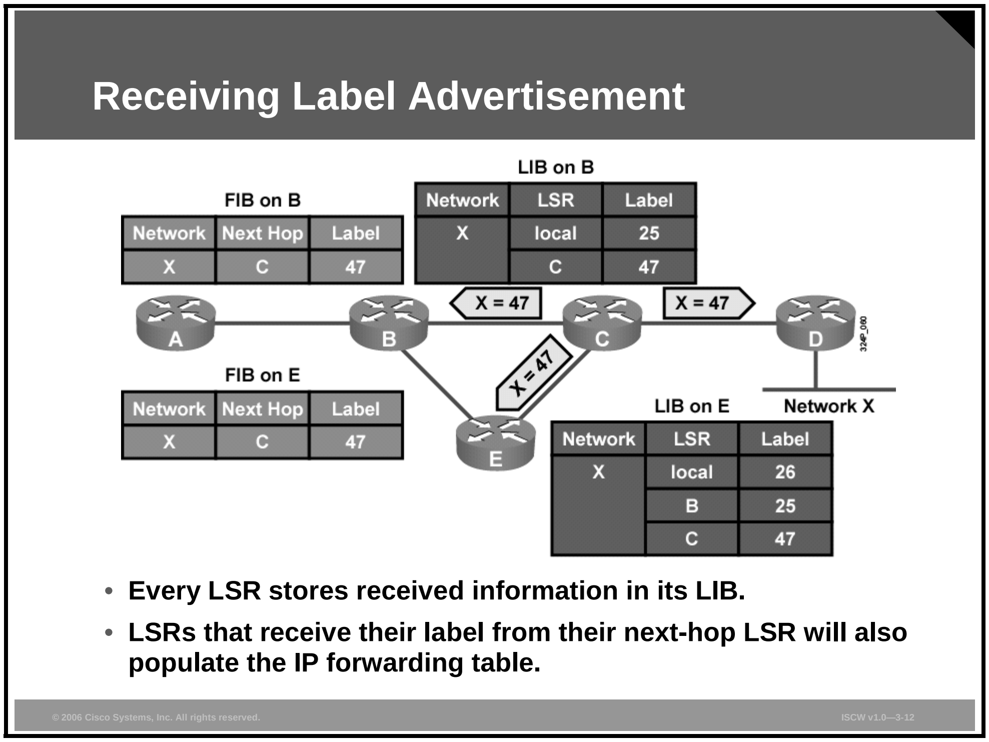
The figure illustrates how an LDP update, advertising label 47 for network X, from router C is sent to all adjacent routers, including router B.

Router D also advertises a label for network X. Since network X is directly connected to router D, it sends an implicit null label for this network. Because of this, the pop action for network X is used on router C, using a Penultimate Hop Popping (PHP) function. The packet sent to router D will not be labeled.

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

Receiving Label Advertisement

Router B can now map the entry for network X in its FIB and the local label 25 in its LFIB to the next-hop label 47 received from the downstream neighbor, router C.



Receiving Label Advertisement

FIB on B

Network	Next Hop	Label
X	C	47

LIB on B

Network	LSR	Label
X	local	25
	C	47

FIB on E

Network	Next Hop	Label
X	C	47

LIB on E

Network	LSR	Label
X	local	26
	B	25
	C	47

- **Every LSR stores received information in its LIB.**
- **LSRs that receive their label from their next-hop LSR will also populate the IP forwarding table.**

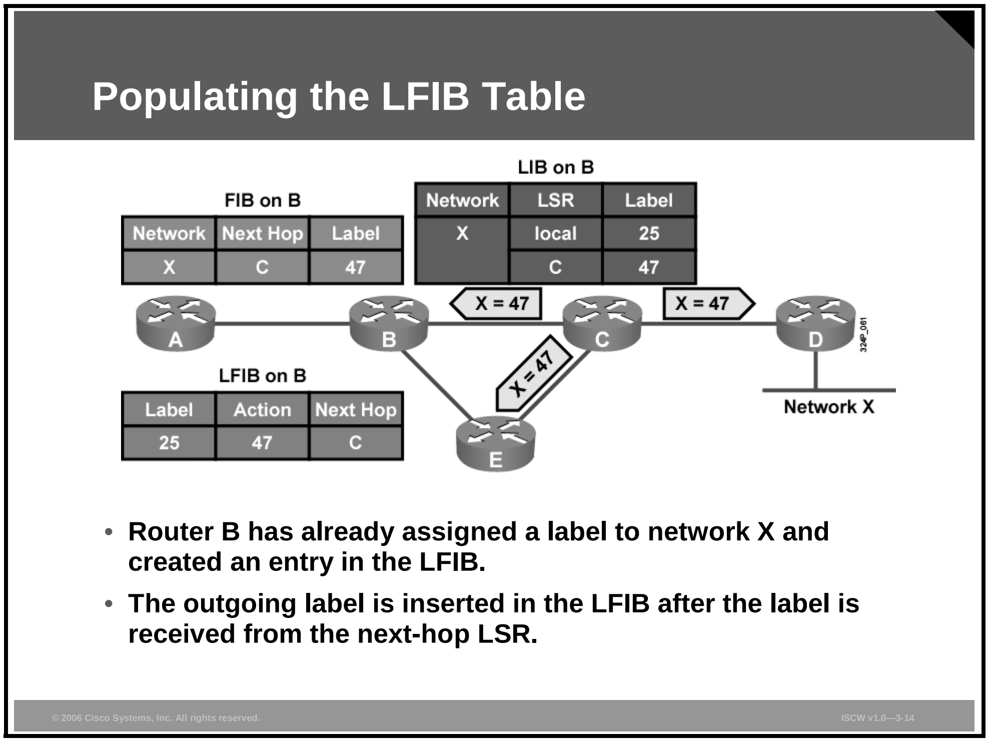
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-12

Router E has allocated label 26 for network X, and has received a label from router B (label 25) and a label from router C (label 47) for network X.

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

Populating the LFIB Table

This topic describes the process undertaken by routers to populate the LFIB database.



Populating the LFIB Table

FIB on B

Network	Next Hop	Label
X	C	47

LIB on B

Network	LSR	Label
X	local	25
	C	47

LFIB on B

Label	Action	Next Hop
25	47	C

- **Router B has already assigned a label to network X and created an entry in the LFIB.**
- **The outgoing label is inserted in the LFIB after the label is received from the next-hop LSR.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-14

An IGP is used to populate the routing tables in all routers in an MPLS domain. LDP is used to propagate labels for these networks. Each router determines its own shortest path by IGP.

LDP, which propagates labels for the networks, adds labels into the FIB and LFIB tables. Only those labels that come from the next-hop router are inserted into the LFIB table.

Router B has already assigned a label to network X and created an entry in the LFIB. The outgoing label is inserted in the LFIB after the label is received from the next-hop LSR.

After router C advertises label 47 to adjacent routers, the LSP tunnel for network X has two hops. The steps in establishing the LSP or LSP tunnel from router A to network X are as follows:

Step 1 On router A, network X is mapped to the next-hop label 25 (router B).

Step 2 On router B, label 25 is mapped to the next-hop label 47 (router C).

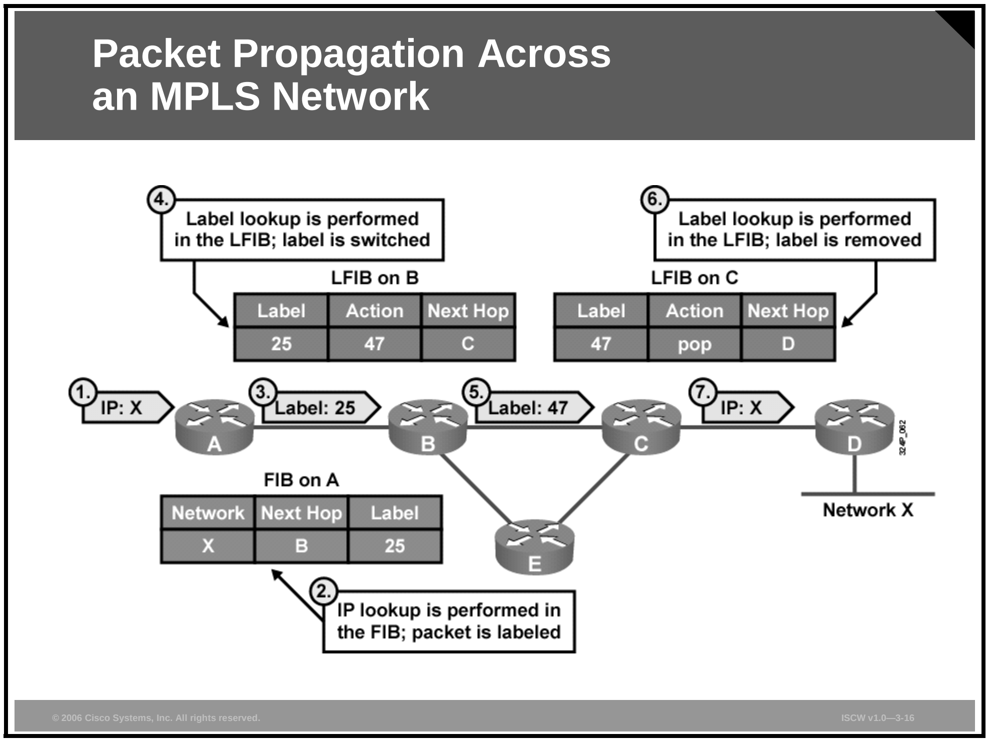
Step 3 Router C received an implicit null label for network X from router D. Label 47 is therefore mapped to the pop action.

Note In the figure, label distribution is from right to left, and packet forwarding is from left to right.

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

Packet Propagation Across an MPLS Network

This topic describes how IP packets cross an MPLS network.



Packet Propagation Across an MPLS Network

4. Label lookup is performed in the LFIB; label is switched

LFIB on B

Label	Action	Next Hop
25	47	C

6. Label lookup is performed in the LFIB; label is removed

LFIB on C

Label	Action	Next Hop
47	pop	D

FIB on A

Network	Next Hop	Label
X	B	25

2. IP lookup is performed in the FIB; packet is labeled

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-16

An incoming IP packet is forwarded by using the FIB table, and can be sent out as an IP packet or as a labeled IP packet. But an incoming labeled packet is forwarded by using the LFIB table and sent out as a labeled IP packet. If a router did not get a label from the next-hop router, the label is removed and an unlabeled IP packet is sent.

The figure illustrates how IP packets are propagated across an MPLS domain. The steps are as follows:

Step 1 A standard IP packet destined for network X arrives at router A.

Step 2 Router A labels a packet destined for network X by using the next-hop label 25 (CEF switching by using the FIB table).

Step 3 Router A sends the packet toward network X with the MPLS label 25.

Step 4 Router B swaps label 25 with label 47 using the LFIB.

Step 5 Router B forwards the packet to router C (label switching by using the LFIB table).

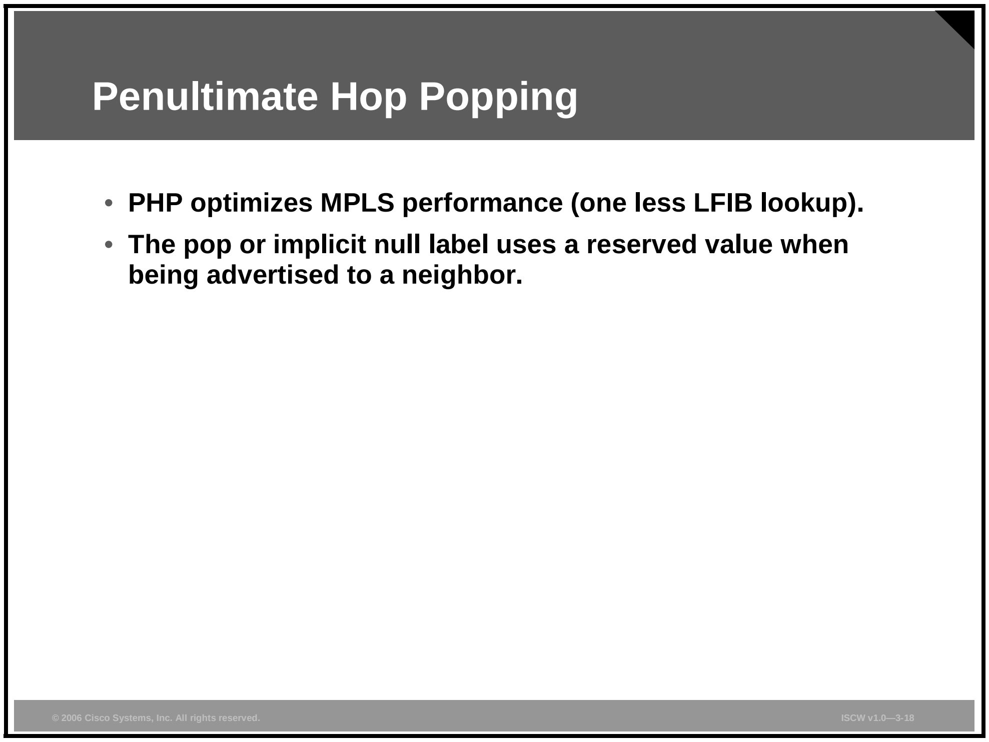
Step 6 Router C removes (pops) the label.

Step 7 Router C forwards the unlabeled packet to router D (label removed by using the LFIB table).

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

Penultimate Hop Popping

This topic describes the efficiency that is added to an MPLS network with PHP enabled.



Penultimate Hop Popping

- **PHP optimizes MPLS performance (one less LFIB lookup).**
- **The pop or implicit null label uses a reserved value when being advertised to a neighbor.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-18

PHP optimizes MPLS performance by reducing the number of table lookups on the egress router.

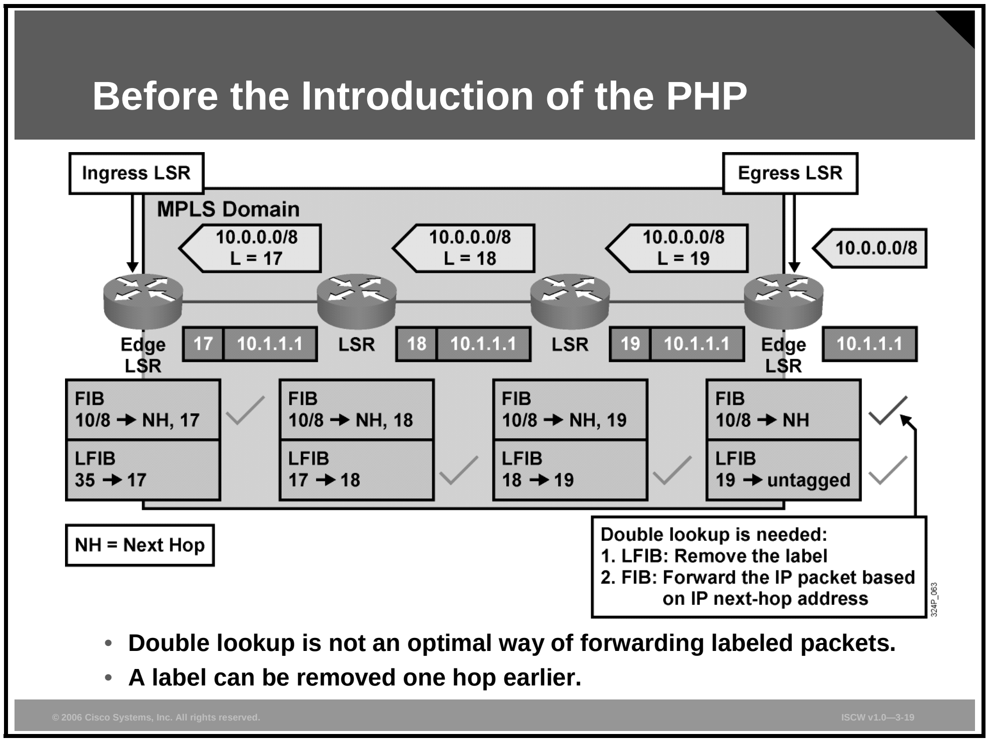
When the downstream router realizes that it is the final node in the label switched path, it can distribute the label value of 3 to the upstream router at the time the path is established. The upstream router makes the next-hop determination for the packet based on the inbound label it receives and forwards the packet without a label. This allows the downstream node to perform a single lookup.

Note A pop label is encoded with a value of 3 for LDP. This label instructs upstream routers to remove the label instead of swapping it with label 3. The display in the LIB table of the router will be *imp-null* rather than the value of 3.

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

Example: Before the Introduction of the PHP

The figure illustrates how labels are propagated and used in a typical frame mode MPLS network.



Before the Introduction of the PHP

Double lookup is needed:
1. LFIB: Remove the label
2. FIB: Forward the IP packet based on IP next-hop address

- **Double lookup is not an optimal way of forwarding labeled packets.**
- **A label can be removed one hop earlier.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-19

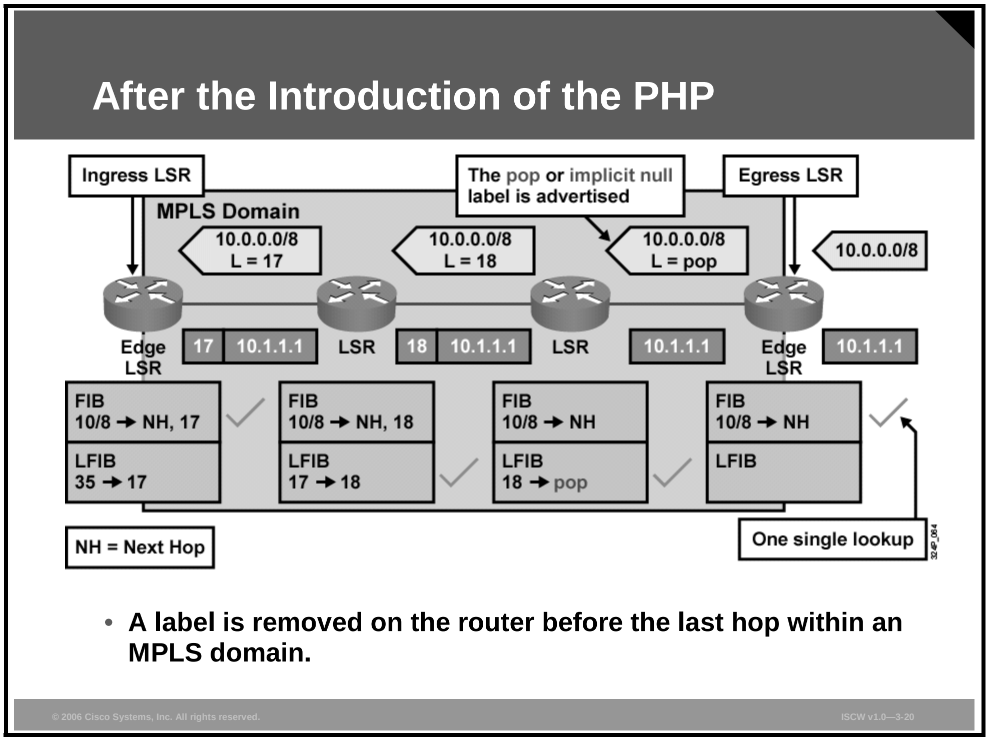
The check marks show which tables are used on individual routers. The egress router in this example must do a lookup in the LFIB table to determine whether the label must be removed and if a further lookup in the FIB table is required.

PHP removes the requirement for a double lookup to be performed on egress LSRs.

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

Example: After the Introduction of the PHP

This figure illustrates how a predefined label pop, which corresponds to the pop action in the LFIB, is propagated on the first hop or the last hop, depending on the perspective.



After the Introduction of the PHP

- **A label is removed on the router before the last hop within an MPLS domain.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-20

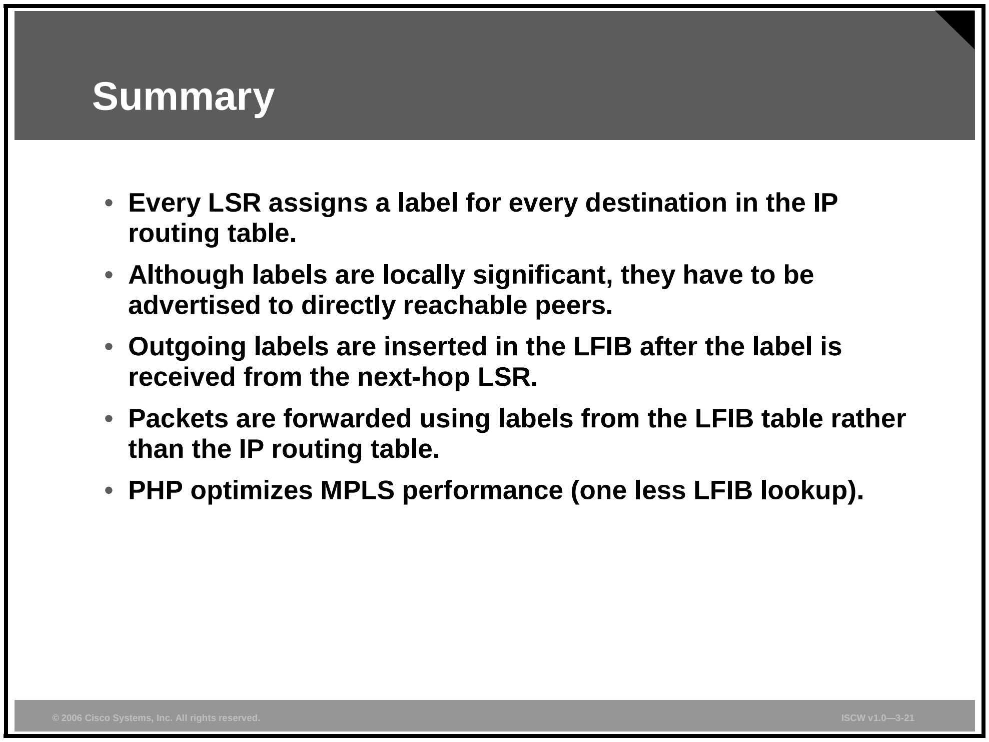
The term pop means to remove the top label in the MPLS label stack instead of swapping it with the next-hop label. The last router before the egress router, therefore, removes the top label.

PHP slightly optimizes MPLS performance by eliminating one LFIB lookup at the egress edge LSR.

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

Summary

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



Summary

- Every LSR assigns a label for every destination in the IP routing table.
- Although labels are locally significant, they have to be advertised to directly reachable peers.
- Outgoing labels are inserted in the LFIB after the label is received from the next-hop LSR.
- Packets are forwarded using labels from the LFIB table rather than the IP routing table.
- PHP optimizes MPLS performance (one less LFIB lookup).

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-21

References

For additional information, refer to these resources:

- RFC 3031: *Multiprotocol Label Switching Architecture* at http://www.ietf.org/rfc/rfc3031.txt
- RFC 3036: *LDP Specification* at http://www.ietf.org/rfc/rfc3036.txt

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

Lesson 3

Implementing Frame Mode MPLS

Overview

Cisco Express Forwarding (CEF) must be running as a prerequisite to running Multiprotocol Label Switching (MPLS) on a Cisco router. This lesson describes how to configure IP CEF switching and frame mode MPLS on Cisco IOS platforms. The lesson also describes the mandatory configuration tasks and commands.

Objectives

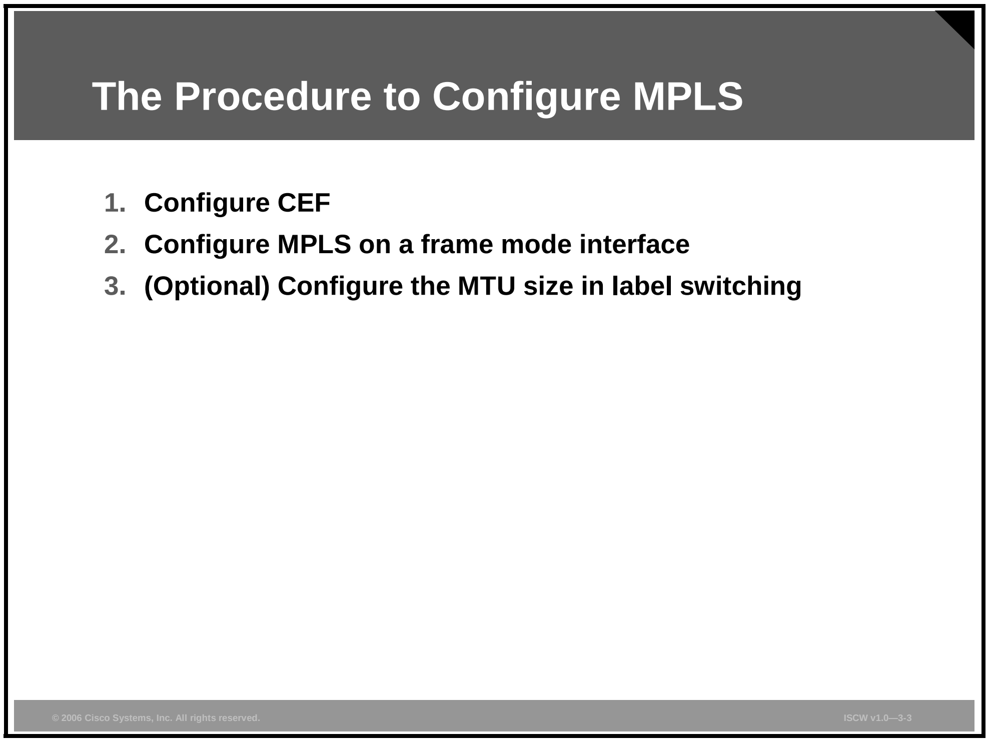
Upon completing this lesson, you will be able to describe the steps that are required to successfully implement MPLS. This ability includes being able to meet these objectives:

- Describe the procedure for configuring frame mode MPLS on a Cisco IOS router
- Enable IP CEF on a router as a step in implementing frame mode MPLS
- Enable MPLS on a frame mode interface as a step in implementing frame mode MPLS
- Configure the MTU size in label switching as a step in implementing frame mode MPLS

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

The Procedure to Configure MPLS

This topic describes the procedure for configuring frame mode MPLS on a Cisco IOS router.



The Procedure to Configure MPLS

1. **Configure CEF**
2. **Configure MPLS on a frame mode interface**
3. **(Optional) Configure the MTU size in label switching**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-3

To configure MPLS, follow these steps:

Step 1 **Configure CEF:** CEF must be running as a prerequisite to running MPLS on a Cisco router.

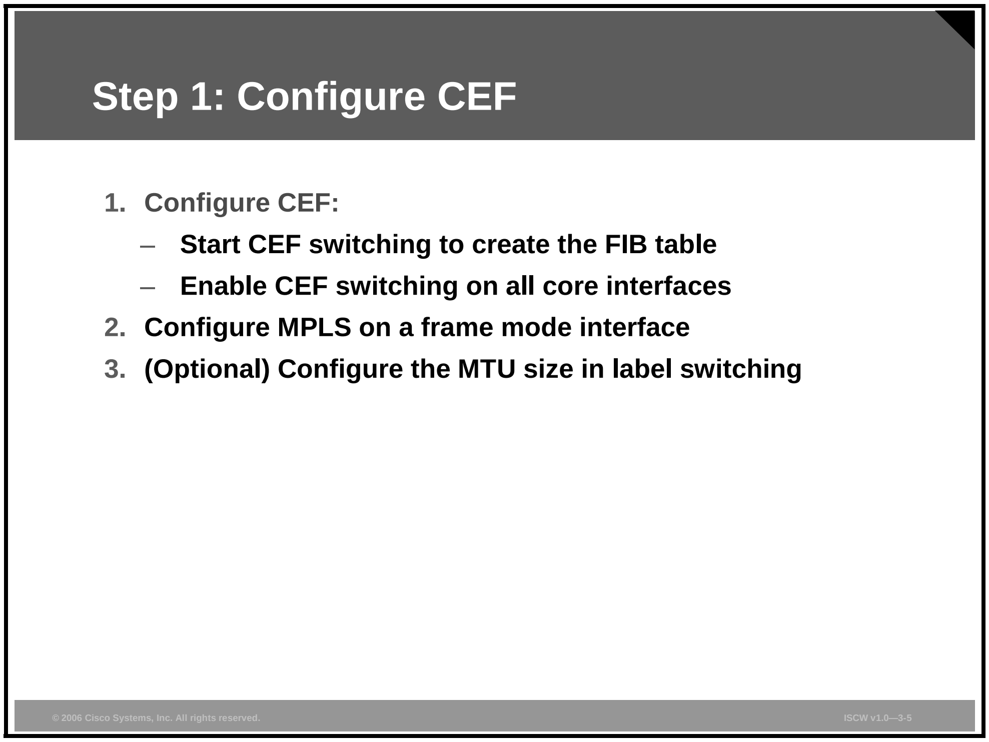
Step 2 **Configure MPLS on a frame mode interface:** All MPLS backbone interfaces should be enabled for MPLS.

Step 3 **Configure the maximum transmission unit (MTU) size in label switching:** To prevent labeled packets from exceeding the maximum size, you may need to increase the MTU on the MPLS interface.

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

Configuring IP CEF

This topic describes how to configure IP CEF.



Step 1: Configure CEF

1. Configure CEF:
   - Start CEF switching to create the FIB table
   - Enable CEF switching on all core interfaces
2. Configure MPLS on a frame mode interface
3. (Optional) Configure the MTU size in label switching

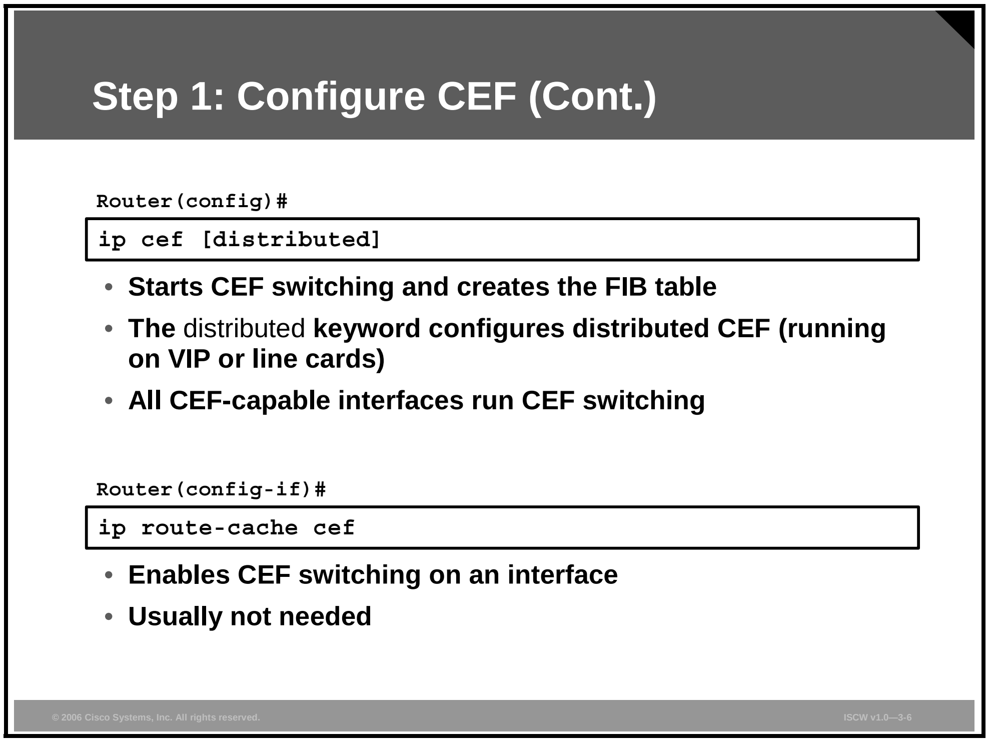
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-5

To enable MPLS, you must first enable CEF switching.

You should enable CEF switching globally or on individual interfaces. Enabling CEF globally on a router is more common—this will enable CEF on all interfaces.

In situations in which you want to have control over the range of labels assigned by Label Distribution Protocol (LDP), you may need to establish the range for the label pool.

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



Step 1: Configure CEF (Cont.)

Router(config)#

```
ip cef [distributed]
```

- **Starts CEF switching and creates the FIB table**
- **The** distributed **keyword configures distributed CEF (running on VIP or line cards)**
- **All CEF-capable interfaces run CEF switching**

Router(config-if)#

```
ip route-cache cef
```

- **Enables CEF switching on an interface**
- **Usually not needed**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-6

To enable CEF, use the **ip cef** command in global configuration mode.

ip cef [**distributed**]

ip cef Parameter

Parameter	Description
`distributed`	(Optional) Enables the distributed CEF operation. Distributes the CEF information to the line cards. The line cards perform express forwarding. CEF is enabled by default only on these platforms: ■ CEF is enabled on the Cisco 7100 series router. ■ CEF is enabled on the Cisco 7200 series router. ■ CEF is enabled on the Cisco 7500 series Internet router. ■ Distributed CEF is enabled on the Cisco 6500 series router. ■ Distributed CEF is enabled on the Cisco 12000 series Internet router.

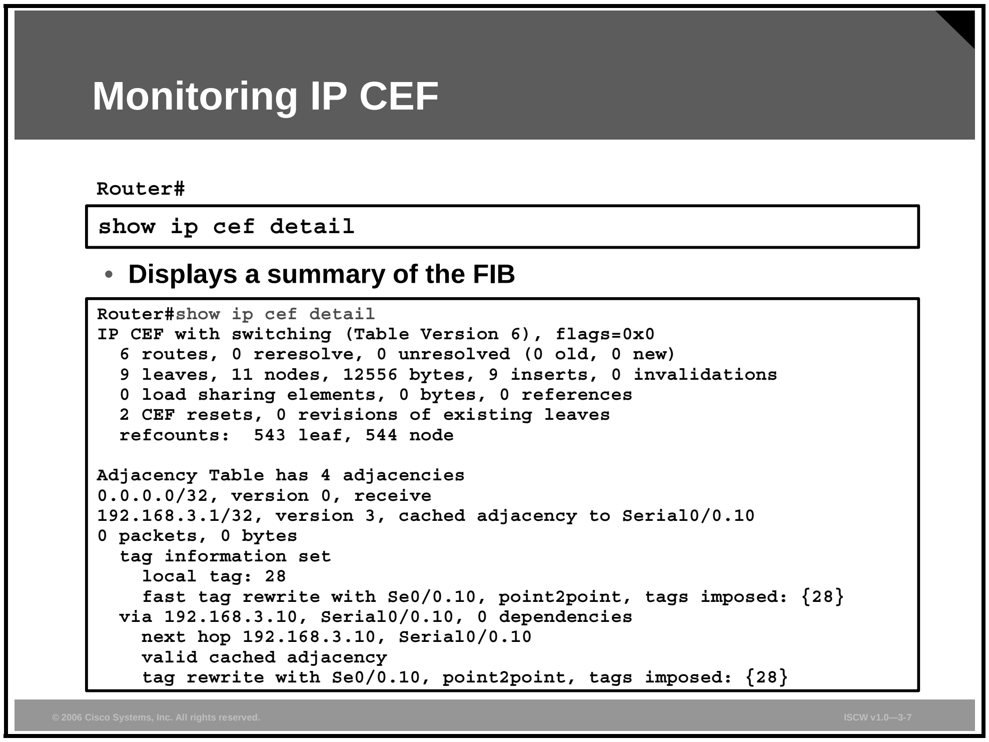
To enable CEF operation on an interface after the CEF operation has been disabled, use the **ip route-cache cef** command in interface configuration mode. The **ip route-cache cef** command does not have any parameters.

When standard CEF or distributed CEF operations are enabled globally, all interfaces that support CEF are enabled by default.

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

Monitoring IP CEF

To display entries in the Forwarding Information Base (FIB) or to display a summary of the FIB, use the **show ip cef** command in user EXEC or privileged EXEC mode.



Monitoring IP CEF

```
Router#
show ip cef detail
```

- **Displays a summary of the FIB**

```
Router#show ip cef detail
IP CEF with switching (Table Version 6), flags=0x0
  6 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
  9 leaves, 11 nodes, 12556 bytes, 9 inserts, 0 invalidations
  0 load sharing elements, 0 bytes, 0 references
  2 CEF resets, 0 revisions of existing leaves
  refcounts:  543 leaf, 544 node

Adjacency Table has 4 adjacencies
0.0.0.0/32, version 0, receive
192.168.3.1/32, version 3, cached adjacency to Serial0/0.10
0 packets, 0 bytes
  tag information set
    local tag: 28
    fast tag rewrite with Se0/0.10, point2point, tags imposed: {28}
  via 192.168.3.10, Serial0/0.10, 0 dependencies
    next hop 192.168.3.10, Serial0/0.10
    valid cached adjacency
    tag rewrite with Se0/0.10, point2point, tags imposed: {28}
```

© 2006 Cisco Systems, Inc. All rights reserved.

The **show if cef** command has several different parameters.

show ip cef [**unresolved** | **summary**]

show ip cef [*network* [*mask* [**longer-prefixes**]]] [**detail**]

show ip cef [*type number*] [**detail**]

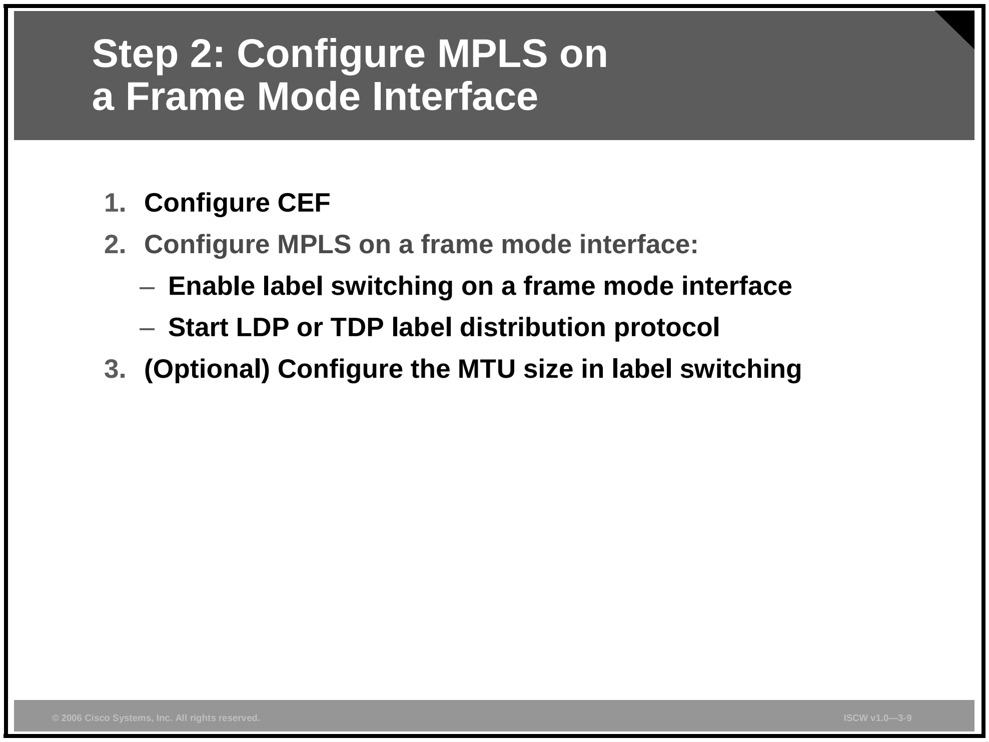
show ip cef Parameters

Parameter	Description
`unresolved`	(Optional) Displays unresolved FIB entries
`summary`	(Optional) Displays a summary of the FIB
`network`	(Optional) Displays the FIB entry for the specified destination network
`mask`	(Optional) Displays the FIB entry for the specified destination network and mask
`longer-prefixes`	(Optional) Displays the FIB entries for all the specific destinations
`detail`	(Optional) Displays detailed FIB entry information
`type number`	(Optional) Interface type and number for which to display FIB entries

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

Configuring MPLS on a Frame Mode Interface

This topic describes how to enable MPLS on a frame mode interface.



Step 2: Configure MPLS on a Frame Mode Interface

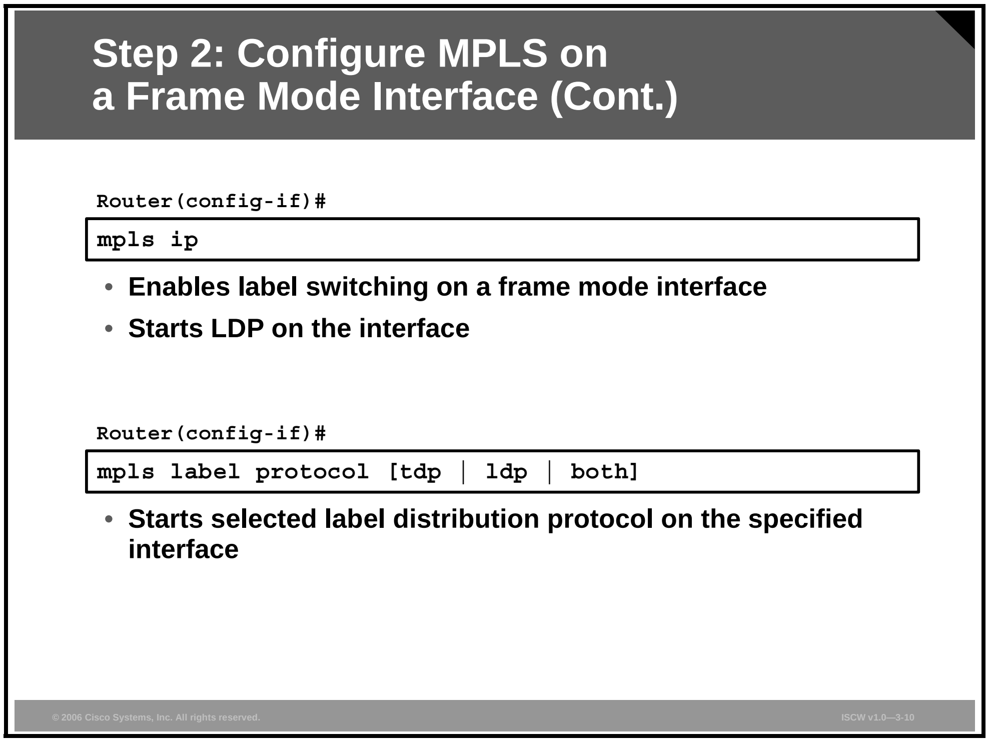
1. **Configure CEF**
2. **Configure MPLS on a frame mode interface:**
   - **Enable label switching on a frame mode interface**
   - **Start LDP or TDP label distribution protocol**
3. **(Optional) Configure the MTU size in label switching**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-9

Enable Tag Distribution Protocol (TDP) or Label Distribution Protocol (LDP) on the interface by using either tag switching or label switching. You enable the support for MPLS on a device by using **mpls ip** global configuration command, although this should be on by default, and then individually on every frame mode interface that participates in MPLS processes.

MPLS support is enabled by default in Cisco routers. MPLS can be disabled using the **no mpls ip** interface configuration command. You must configure MPLS individually on every frame mode interface that will participate in MPLS using the **mpls ip** command in interface configuration mode. After enabling MPLS on the interface, you must select the label distribution protocol using the **mpls label protocol** command in interface 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 self-study.



Step 2: Configure MPLS on a Frame Mode Interface (Cont.)

```
Router(config-if)#
mpls ip
```

- Enables label switching on a frame mode interface
- Starts LDP on the interface

```
Router(config-if)#
mpls label protocol [tdp | ldp | both]
```

- Starts selected label distribution protocol on the specified interface

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-10

To run MPLS on the interface, you must explicitly enable it and afterwards select the LDP.

TDP is Cisco proprietary protocol. Depending on the Cisco IOS version, when issuing a **show running-config** command, the **mpls ldp** commands will show up as **tag-switching** commands.

The default MPLS label distribution protocol changed from TDP to LDP. If no protocol is explicitly configured by the **mpls label protocol** command, LDP is the default label distribution protocol.

You can save the LDP configuration commands by using the **mpls ip** form of the command rather than the **tag-switching** form. Previously, commands were saved using the **tag-switching** form of the command, for backward compatibility.

To enable label switching of IP version 4 (IPv4) packets on an interface, use the **mpls ip** command in interface configuration mode. The **mpls ip** command does not have any parameters.

This command starts LDP on all interfaces on a Cisco router. To select TDP, you have to use **mpls label protocol tdp** command, globally or per interface.

By default, label switching of IPv4 packets is disabled on an interface.

To select which label distribution protocol will be used on an interface, use the **mpls label protocol** command in interface configuration mode.

mpls label protocol [**tdp** | **ldp** | **both**]

mpls label protocol Parameters

Parameter	Description
`tdp`	Enables TDP on an interface
`ldp`	Enables LDP on an interface
`both`	Enables TDP and LDP on an interface

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

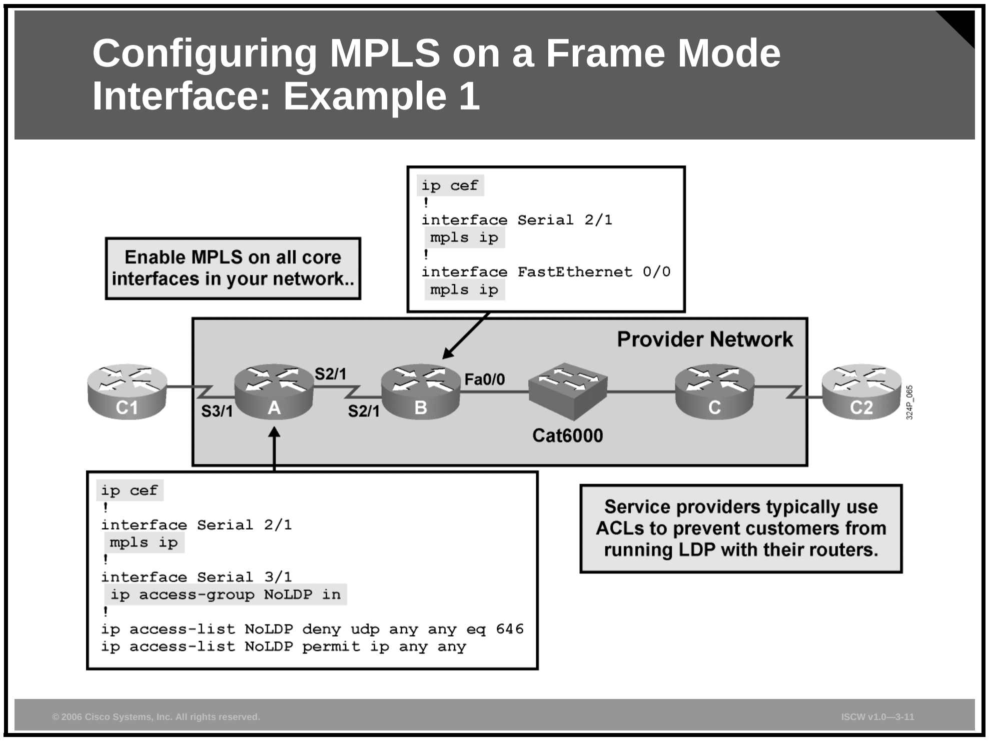
LDP is the default protocol on Cisco IOS software Release 12.4(3) and later. In the older releases, TDP was the default protocol.

Note For backward compatibility, using the **mpls** syntax will be entered as **tag-switching** syntax in the configuration by the Cisco IOS software.

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

Examples: Configuring MPLS on a Frame Mode Interface

The figure shows the configuration steps needed to enable MPLS on an edge label switch router (LSR). The configuration includes an access control list (ACL) that denies any attempt to establish an LDP session from an interface that is not enabled for MPLS. In the example in the figure, router A has “NoLDP” ACL on Serial 3/1 interface, which is not enabled for MPLS.



Configuring MPLS on a Frame Mode Interface: Example 1

```
ip cef
!
interface Serial 2/1
 mpls ip
!
interface FastEthernet 0/0
 mpls ip
```

Enable MPLS on all core interfaces in your network..

```
ip cef
!
interface Serial 2/1
 mpls ip
!
interface Serial 3/1
 ip access-group NoLDP in
!
ip access-list NoLDP deny udp any any eq 646
ip access-list NoLDP permit ip any any
```

Service providers typically use ACLs to prevent customers from running LDP with their routers.

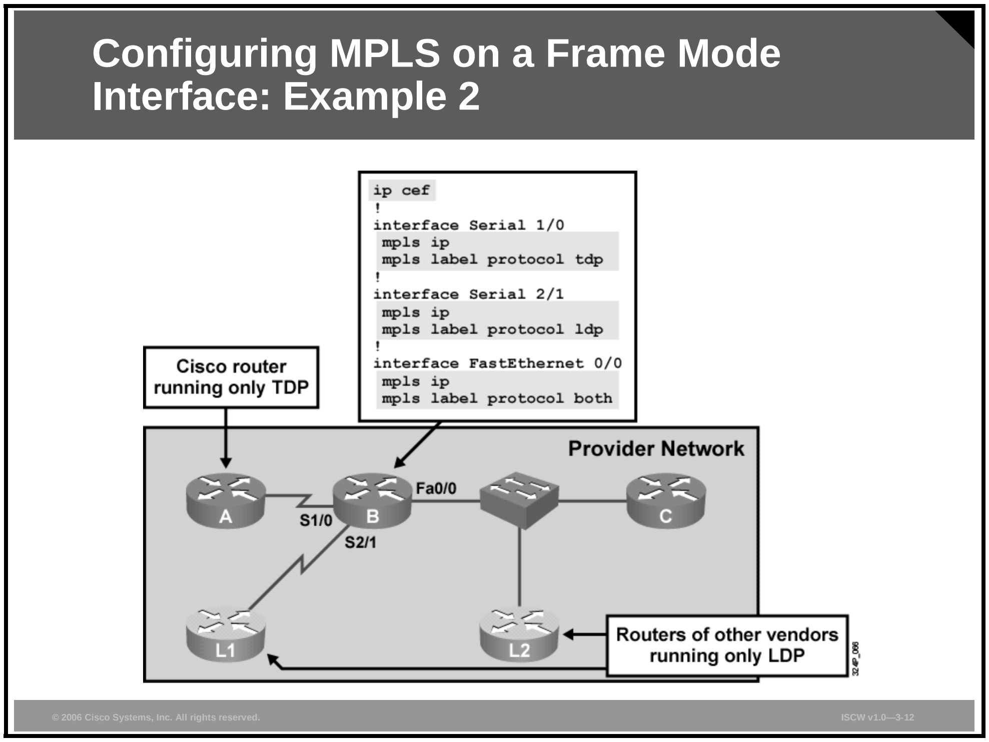
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-11

You must globally enable CEF switching, which automatically enables CEF on all interfaces that support it.

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

Non-backbone (non-MPLS) interfaces have an input ACL that denies TCP sessions on the well-known port number 711 (TDP uses TCP port 711). If using LDP, filter on UDP port 646, (LDP uses UDP port 646). This is just as a precaution because without the **mpls ip** command on the interface, LDP cannot be established on Serial 3/1.

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 self-study.



Configuring MPLS on a Frame Mode Interface: Example 2

```
ip cef
!
interface Serial 1/0
 mpls ip
 mpls label protocol tdp
!
interface Serial 2/1
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet 0/0
 mpls ip
 mpls label protocol both
```

Cisco router running only TDP
Provider Network
A
S1/0
B
Fa0/0
S2/1
C
L1
L2
Routers of other vendors running only LDP
324P_088

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-12

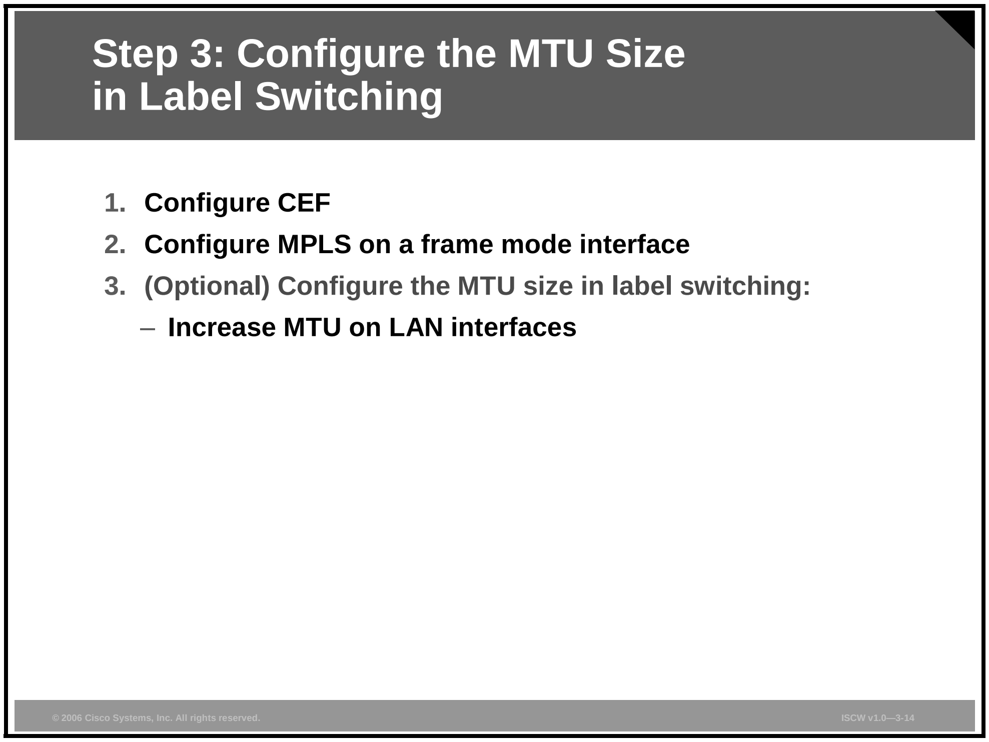
When combining Cisco routers with equipment of other vendors, you may need to use standard LDP. TDP can be replaced by LDP on point-to-point interfaces. However, you can also use both protocols on shared media if some devices do not support TDP.

Label switching is more or less independent of the distribution protocol, so there should be no problem in mixing the two protocols. TDP and LDP are functionally very similar, and both populate the Label Information Base (LIB) table.

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

Configuring the MTU Size in Label Switching

This topic describes how to configure the MTU size in label switching.



Step 3: Configure the MTU Size in Label Switching

1. **Configure CEF**
2. **Configure MPLS on a frame mode interface**
3. **(Optional) Configure the MTU size in label switching:**
   - **Increase MTU on LAN interfaces**

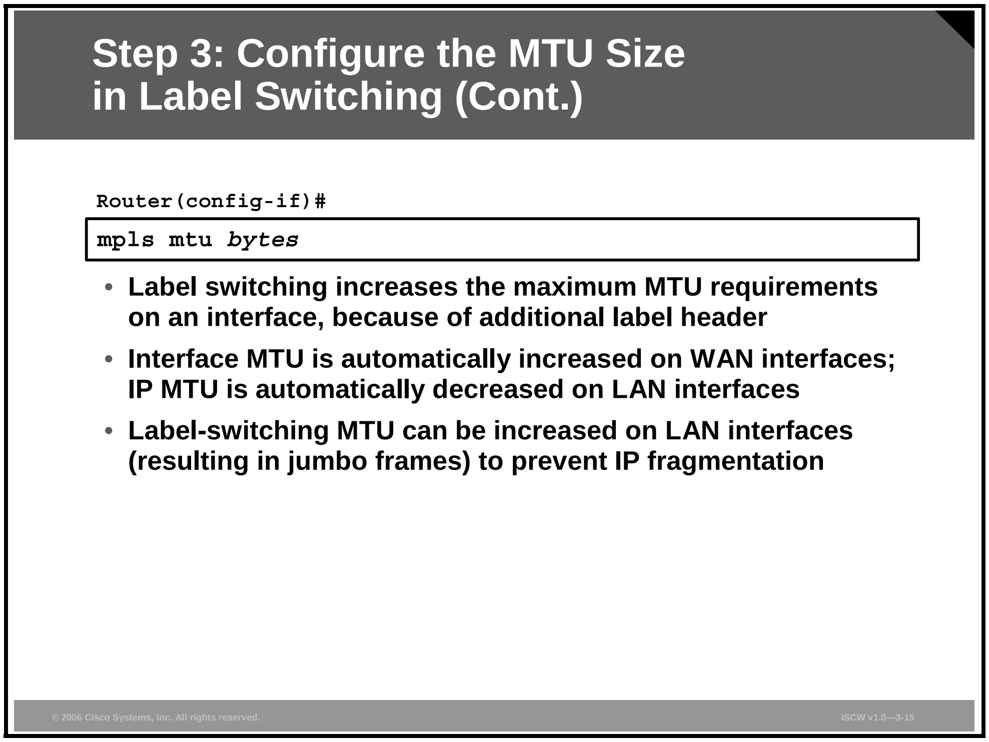
© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-14

Optionally, you may change the maximum size of labeled packets. Because of the additional label header, increase the MTU on LAN interfaces to prevent IP fragmentation.

The MPLS MTU size has to be increased on all routers attached to a LAN segment. The default MTU size on the LAN segments is 1500 bytes. The size of the MPLS MTU depends on the application you are running with MPLS. When you are using pure MPLS in the backbone, MTU size will increase for one label header only to 1504 bytes. When you are implementing MPLS VPN, MTU size has to increase for two label headers to 1508 bytes. With MPLS VPN with Traffic Engineering (TE), the MTU size should increase for three label headers to 1512 bytes.

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



Step 3: Configure the MTU Size in Label Switching (Cont.)

```
Router(config-if)#
mpls mtu bytes
```

- **Label switching increases the maximum MTU requirements on an interface, because of additional label header**
- **Interface MTU is automatically increased on WAN interfaces; IP MTU is automatically decreased on LAN interfaces**
- **Label-switching MTU can be increased on LAN interfaces (resulting in jumbo frames) to prevent IP fragmentation**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-15

One way of preventing labeled packets from exceeding the maximum size (and being fragmented as a result) is to increase the MTU size of labeled packets for all segments in the Label Switch Path (LSP) tunnel. The problem will typically occur on LAN switches, where it is more likely that a device does not support oversized packets (also called jumbo frames or, sometimes, giants or baby giants). Some devices support jumbo frames, and some need to be configured to support them.

Label switching increases the maximum MTU requirements on an interface because of the additional label headers.

The interface MTU is automatically increased on WAN interfaces, but not on LAN interfaces. Because MTU is not automatically increased on LAN interfaces, you have to increase it manually using **mpls mtu** command.

To set the per-interface MTU for labeled packets, use the **mpls mtu** interface configuration command.

mpls mtu *bytes*

mpls mtu Parameter

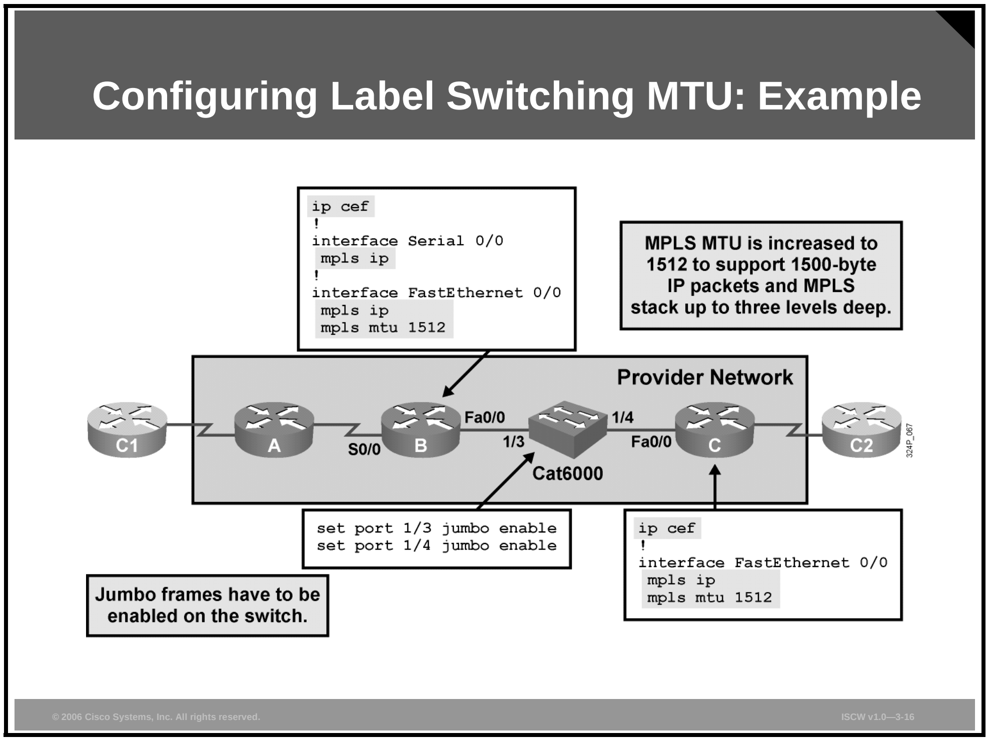
Parameter	Description
bytes	MTU in bytes

The minimum MTU is 64 bytes. The maximum depends on the type of interface medium.

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

Example: Configuring Label Switching MTU

The figure shows the label switching MTU configuration example.



Configuring Label Switching MTU: Example

```
ip cef
!
interface Serial 0/0
 mpls ip
!
interface FastEthernet 0/0
 mpls ip
 mpls mtu 1512
```

MPLS MTU is increased to 1512 to support 1500-byte IP packets and MPLS stack up to three levels deep.

```
set port 1/3 jumbo enable
set port 1/4 jumbo enable
```

Jumbo frames have to be enabled on the switch.

```
ip cef
!
interface FastEthernet 0/0
 mpls ip
 mpls mtu 1512
```

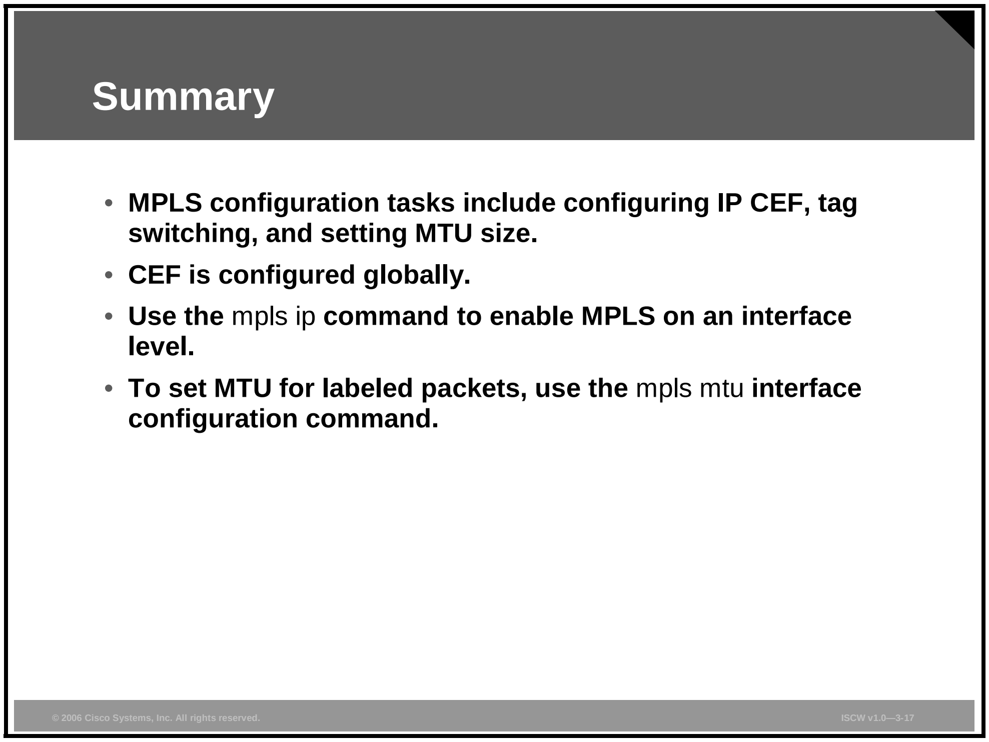
© 2006 Cisco Systems, Inc. All rights reserved.

The MPLS MTU size has to be increased on all routers attached to a LAN segment (routers B and C). Additionally, the LAN switch (Cat6000) that is used to implement switched LAN segments needs to be configured to support jumbo frames.

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

Summary

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



Summary

- **MPLS configuration tasks include configuring IP CEF, tag switching, and setting MTU size.**
- **CEF is configured globally.**
- **Use the** mpls ip **command to enable MPLS on an interface level.**
- **To set MTU for labeled packets, use the** mpls mtu **interface configuration command.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-17

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

Lesson 4

Describing MPLS VPN Technology

Overview

This lesson describes virtual private networks (VPNs) and the terminology introduced by Multiprotocol Label Switching (MPLS) VPN architecture. It is important to understand the background of VPNs, because you should be able to determine the need for a VPN and explain how MPLS VPNs can save time and money.

This lesson explains the differences between the overlay and peer-to-peer VPN models, how they are implemented, and the benefits and drawbacks of each implementation.

The MPLS VPN architecture is explained, as well as route information propagation, route distinguishers (RDs), route targets (RTs), and virtual routing tables.

This lesson explains the routing requirements for MPLS VPNs and how routing tables appear on provider edge (PE) routers. The lesson also discusses MPLS VPN end-to-end information flow, multiprotocol Border Gateway Protocol (MPBGP), updates, how the far-end VPN label is sent to the ingress PE router, and how that information is shared.

Objectives

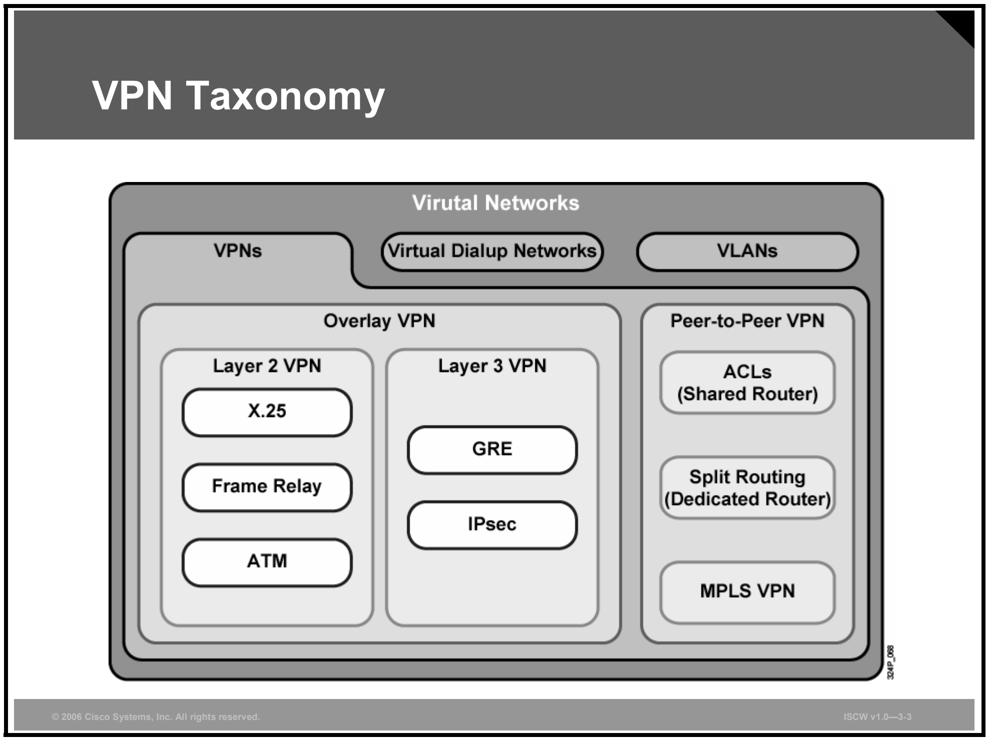
Upon completing this lesson, you will be able to explain the evolution of MPLS VPNs, and describe MPLS VPN routing and packet flow. This ability includes being able to meet these objectives:

- Explain MPLS VPN architecture, and how it improves on the traditional methods of overlay and peer-to-peer VPN
- Describe the components of an MPLS VPN and how they are interconnected to enable enterprise network connectivity between sites
- Identify how routing information is propagated across the P-network
- Identify the end-to-end flow of routing updates in an MPLS VPN
- Describe MPLS VPN packet forwarding

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

Defining MPLS VPN

This topic describes MPLS VPN architecture, and explains how it improves on the traditional methods of overlay and peer-to-peer VPN.



VPN Taxonomy

Virutal Networks

VPNs

Virtual Dialup Networks

VLANs

Overlay VPN

Layer 2 VPN

X.25

Frame Relay

ATM

Layer 3 VPN

GRE

IPsec

Peer-to-Peer VPN

ACLs (Shared Router)

Split Routing (Dedicated Router)

MPLS VPN

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-3

VPN Taxonomy

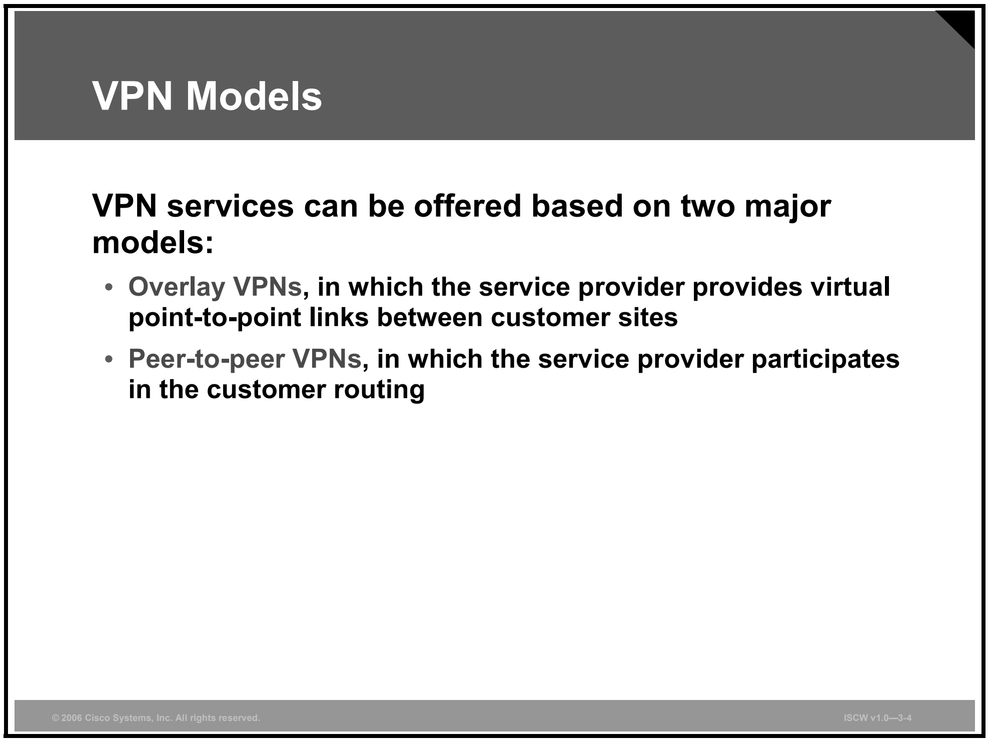
There are several different virtual networking concepts present in the data communications fields:

- VLANs allow you to implement isolated LANs over the same physical infrastructure.
- Virtual private dialup networks (VPDNs) allow you to use the dial-in infrastructure of a service provider for private dialup connections.
- VPNs allow you to use the shared infrastructure of a service provider to implement your private networks. There are basically these two implementation models:
  - Overlay VPNs, including technologies such as X.25, Frame Relay, ATM for Layer 2 Overlay VPN, and Generic Routing Encapsulation (GRE) and IPsec for Layer 3 Overlay VPN.
  - Peer-to-peer VPNs, implemented with routers and respective filters, with separate routers per customer, or with the MPLS VPN technology.

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

What Are the VPN Implementation Technologies?

Traditional VPN implementations were all based on the Layer 2 overlay model, in which the service provider sold virtual circuits (VCs) between customer sites as a replacement for dedicated point-to-point links. The Layer 2 overlay model had a number of drawbacks. To overcome these drawbacks (particularly in IP-based customer networks), a new model called the peer-to-peer VPN was introduced. In this model, the service provider actively participates in customer routing.



VPN Models

VPN services can be offered based on two major models:

- **Overlay VPNs, in which the service provider provides virtual point-to-point links between customer sites**
- **Peer-to-peer VPNs, in which the service provider participates in the customer routing**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-4

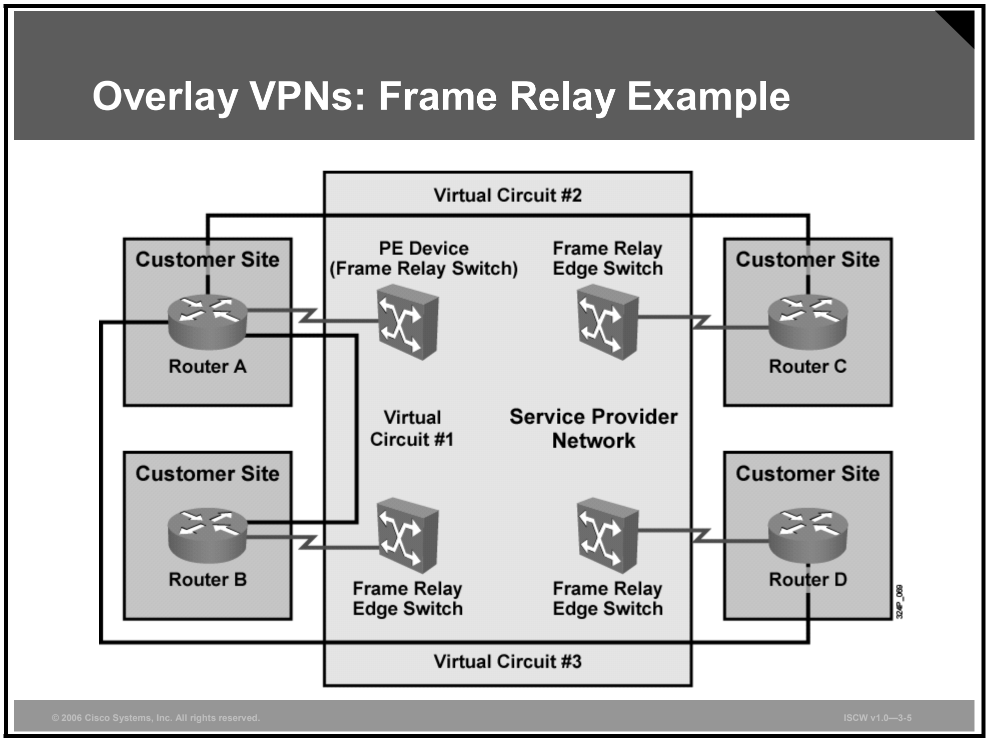
In the Layer 1 overlay VPN implementation, the service provider sells Layer 1 circuits (bit pipes) implemented with technologies such as ISDN, digital service level zero (DS0), E1, T1, Synchronous Digital Hierarchy (SDH), or SONET. The customer is responsible for Layer 2 encapsulation between customer devices and the transport of IP data across the infrastructure.

A Layer 2 VPN implementation is the traditional switched WAN model, implemented with technologies such as X.25, Frame Relay, ATM, and Switched Multimegabit Data Service (SMDS). The service provider is responsible for transport of Layer 2 frames between customer sites, and the customer is responsible for all higher layers.

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

Example: Layer 2 Overlay VPN—Frame Relay

The figure shows a typical Layer 2 overlay VPN implemented by a Frame Relay network.



Overlay VPNs: Frame Relay Example

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-5

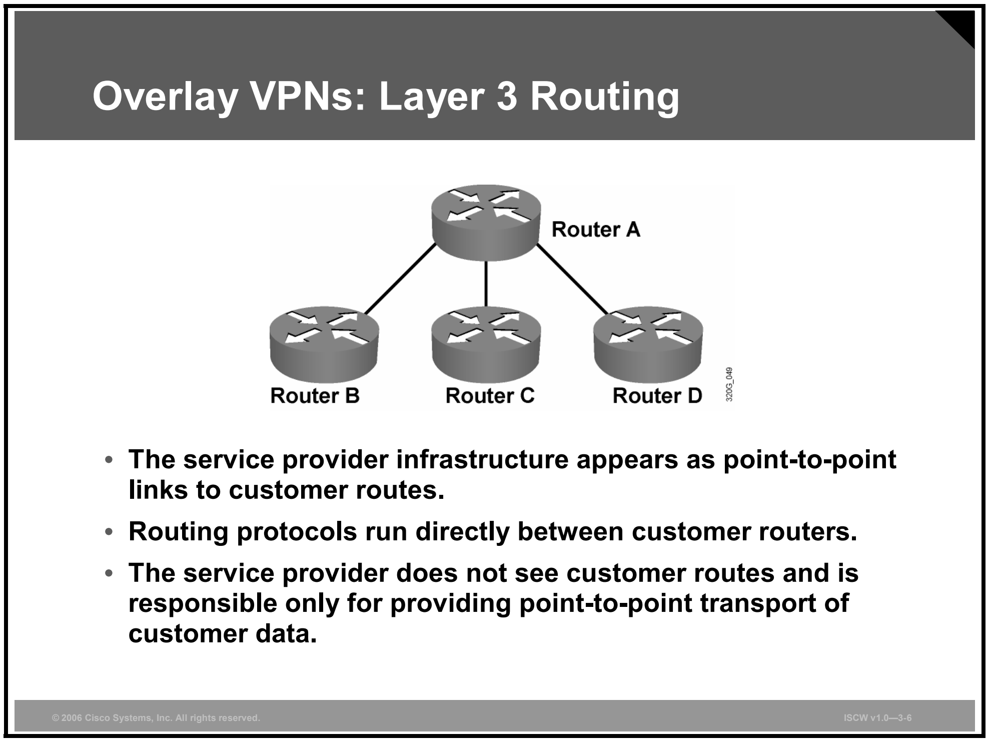
The customer needs to connect three sites to Site A (central site, or hub) and orders connectivity between Site A (hub) and Site B (spoke), between Site A and Site C (spoke), and between Site A and Site D (spoke). The service provider implements this request by providing three permanent virtual circuits (PVCs) across the Frame Relay network.

Note	The implementation displayed in this example does not provide full connectivity; data flow between spoke sites is through the hub.

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

Layer 3 Routing

From the Layer 3 perspective, the provider network (P-network) is invisible to the customer routers, which are linked with emulated point-to-point links. The routing protocol runs directly between customer routers that establish routing adjacencies and exchange routing information.



Overlay VPNs: Layer 3 Routing

- The service provider infrastructure appears as point-to-point links to customer routes.
- Routing protocols run directly between customer routers.
- The service provider does not see customer routes and is responsible only for providing point-to-point transport of customer data.

© 2006 Cisco Systems, Inc. All rights reserved.

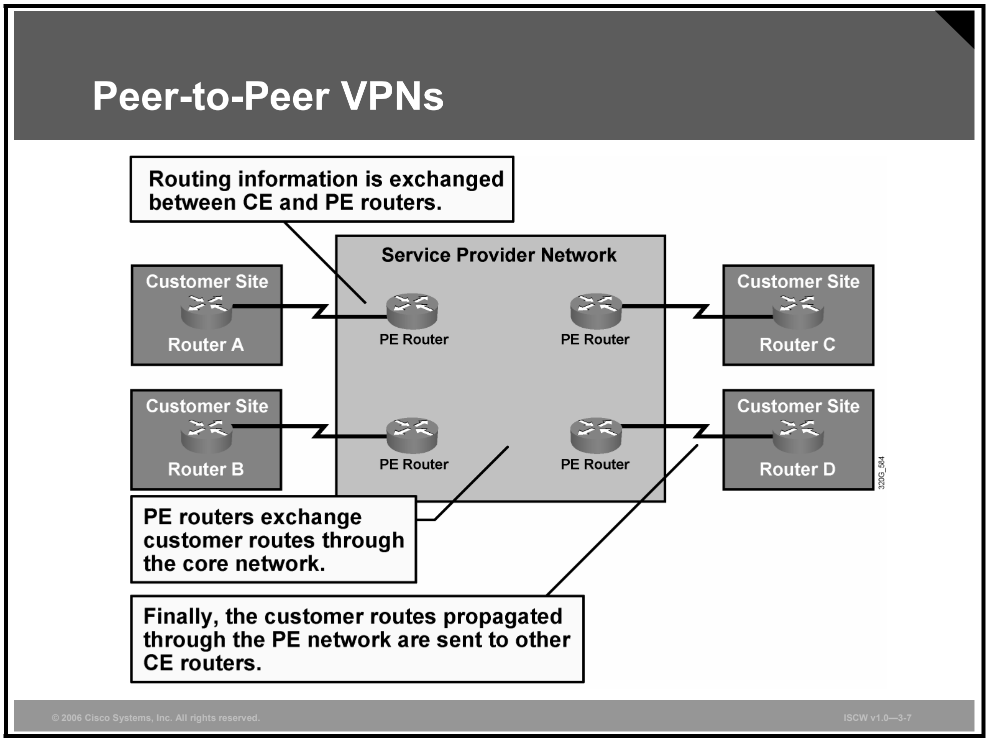
ISCW v1.0—3-6

The service provider is not aware of customer routing and has no information about customer routes. The responsibility of the service provider is simply point-to-point data transport between customer sites.

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

Example: Peer-to-Peer VPNs

The Layer 2 overlay VPN model has a number of drawbacks, most significantly the need for customers to establish point-to-point links or VCs between sites. The formula to calculate how many point-to-point links or VCs are needed is ([*n*]*[*n*-1])/2, where *n* is the number of sites to be connected.



Peer-to-Peer VPNs

Routing information is exchanged between CE and PE routers.

PE routers exchange customer routes through the core network.

Finally, the customer routes propagated through the PE network are sent to other CE routers.

© 2006 Cisco Systems, Inc. All rights reserved.

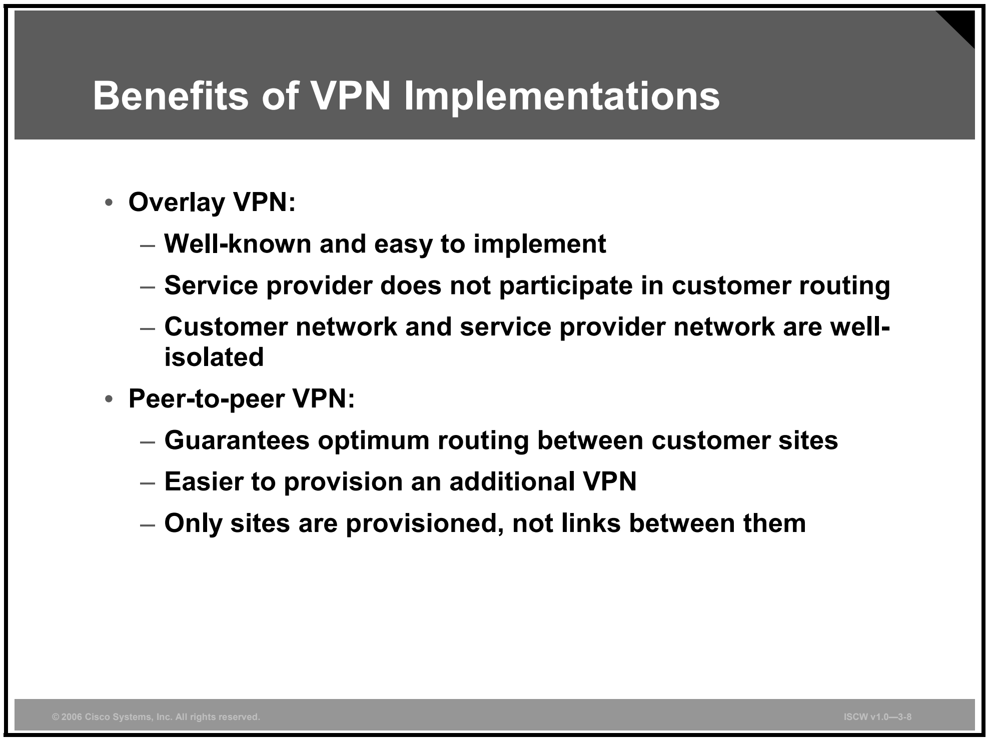
ISCW v1.0—3-7

For example, if you need to have full mesh connectivity between four sites, you will need a total of six point-to-point links or VCs. To overcome this drawback and provide the customer with optimum data transport across the service provider backbone, the peer-to-peer VPN concept was introduced. Here, the service provider actively participates in customer routing, accepting customer routes, transporting those customer routes across the service provider backbone, and finally propagating them to other customer sites.

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

Benefits of VPN Implementations

Each VPN model has a number of benefits.



Benefits of VPN Implementations

- Overlay VPN:
  - Well-known and easy to implement
  - Service provider does not participate in customer routing
  - Customer network and service provider network are well-isolated
- Peer-to-peer VPN:
  - Guarantees optimum routing between customer sites
  - Easier to provision an additional VPN
  - Only sites are provisioned, not links between them

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-8

For example, overlay VPNs have these advantages:

- Overlay VPNs are well-known and easy to implement from both customer and service provider perspectives.
- The service provider does not participate in customer routing, making the demarcation point between service provider and customer easier to manage.

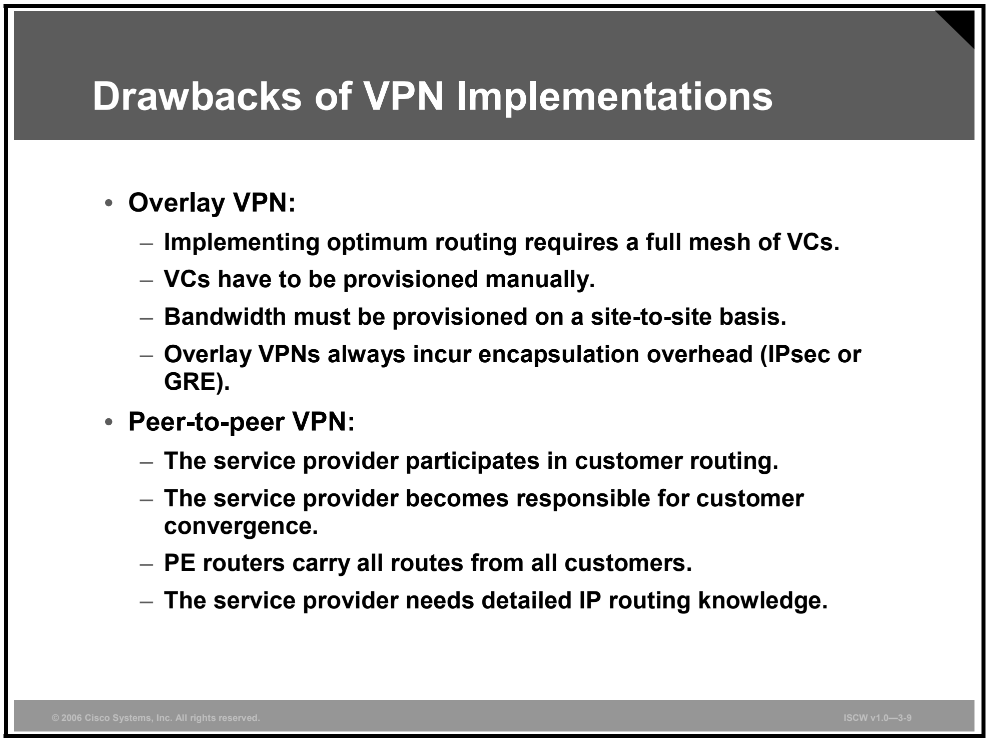
Peer-to-peer VPNs provide these benefits:

- Optimum routing between customer sites without any special design or configuration effort.
- Easy provisioning of additional VPNs or customer sites, because the service provider provisions only individual sites, not the links between individual customer sites.

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

Drawbacks of VPN Implementations

Each VPN model also has a number of drawbacks.



Drawbacks of VPN Implementations

- **Overlay VPN:**
  - **Implementing optimum routing requires a full mesh of VCs.**
  - **VCs have to be provisioned manually.**
  - **Bandwidth must be provisioned on a site-to-site basis.**
  - **Overlay VPNs always incur encapsulation overhead (IPsec or GRE).**
- **Peer-to-peer VPN:**
  - **The service provider participates in customer routing.**
  - **The service provider becomes responsible for customer convergence.**
  - **PE routers carry all routes from all customers.**
  - **The service provider needs detailed IP routing knowledge.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-9

Overlay VPNs have these disadvantages:

- Layer 2 overlay VPNs require a full mesh of VCs between customer sites to provide optimum intersite routing.
- All VCs between customer sites have to be provisioned manually, and the bandwidth must be provisioned on a site-to-site basis (which is not always easy to achieve).
- The IP-based Layer 3 overlay VPN implementations (with IPsec or GRE) incur high encapsulation overhead—ranging from 20 to 80 bytes per transported datagram.

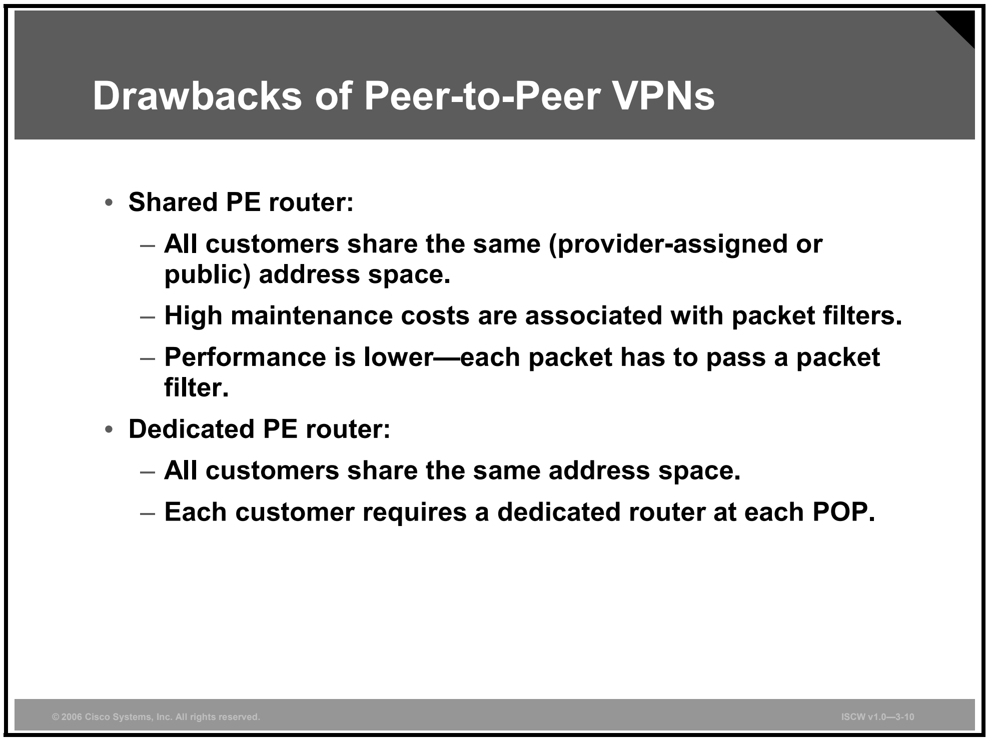
The major drawbacks of peer-to-peer VPNs arise from service provider involvement in customer routing, such as the following situations:

- The service provider becomes responsible for correct customer routing and for fast convergence of the customer network (C-network) following a link failure.
- The service provider PE routers have to carry all customer routes that were hidden from the service provider in the overlay VPN model.
- The service provider needs detailed IP routing knowledge, which is not readily available in traditional service provider teams.

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

Drawbacks of Peer-to-Peer VPNs

Pre-MPLS VPN implementations or peer-to-peer VPNs all share common drawbacks.



Drawbacks of Peer-to-Peer VPNs

- **Shared PE router:**
  - **All customers share the same (provider-assigned or public) address space.**
  - **High maintenance costs are associated with packet filters.**
  - **Performance is lower—each packet has to pass a packet filter.**
- **Dedicated PE router:**
  - **All customers share the same address space.**
  - **Each customer requires a dedicated router at each POP.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-10

Customers have to share the same global address space, either using their own public IP addresses or relying on provider-assigned IP addresses. In both cases, connecting a new customer to a peer-to-peer VPN service usually requires IP renumbering inside the C-network—an operation most customers are reluctant to perform.

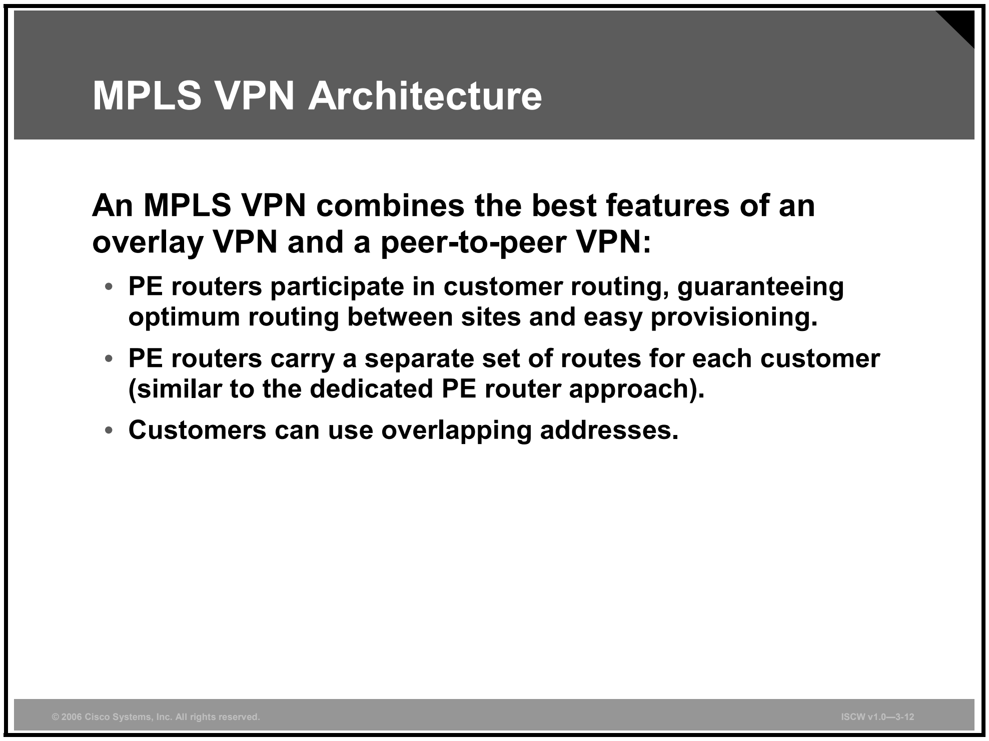
Peer-to-peer VPNs based on packet filters also incur high operational costs associated with packet filter maintenance and performance degradation because of heavy use of packet filters.

Peer-to-peer VPNs implemented with per-customer PE routers are easier to maintain and can provide optimum routing performance, but they are usually more expensive because every customer requires a dedicated router in every point of presence (POP). Therefore, this approach is usually used if the service provider has only a small number of large customers.

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

MPLS VPN Architecture

This topic describes the components of an MPLS VPN and how they are interconnected to enable enterprise network connectivity between sites.



MPLS VPN Architecture

An MPLS VPN combines the best features of an overlay VPN and a peer-to-peer VPN:

- **PE routers participate in customer routing, guaranteeing optimum routing between sites and easy provisioning.**
- **PE routers carry a separate set of routes for each customer (similar to the dedicated PE router approach).**
- **Customers can use overlapping addresses.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-12

The MPLS VPN architecture offers service providers a peer-to-peer VPN architecture that combines the best features of overlay VPNs (support for overlapping customer address spaces) with the best features of peer-to-peer VPNs.

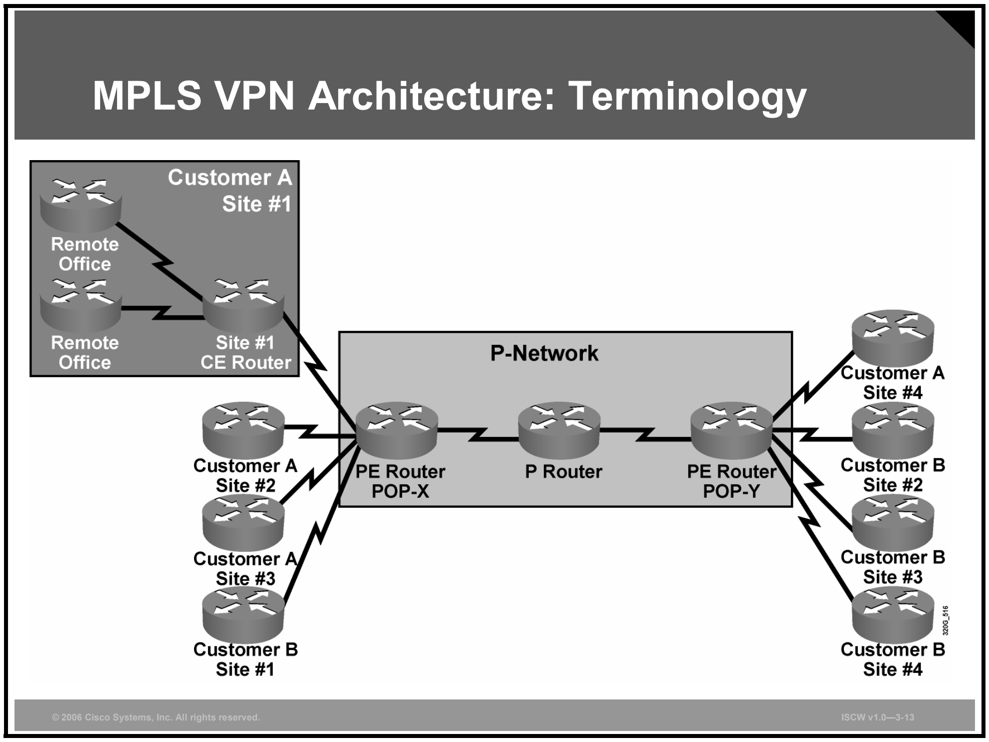
The following describes these characteristics:

- PE routers participate in customer routing, guaranteeing optimum routing between customer sites.
- PE routers use a separate virtual routing table for each customer, resulting in perfect isolation between customers.
- Customers can use overlapping addresses.

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

Terminology

MPLS VPN terminology divides the overall network into a customer-controlled part (the C-network) and a provider-controlled part (the P-network).



MPLS VPN Architecture: Terminology

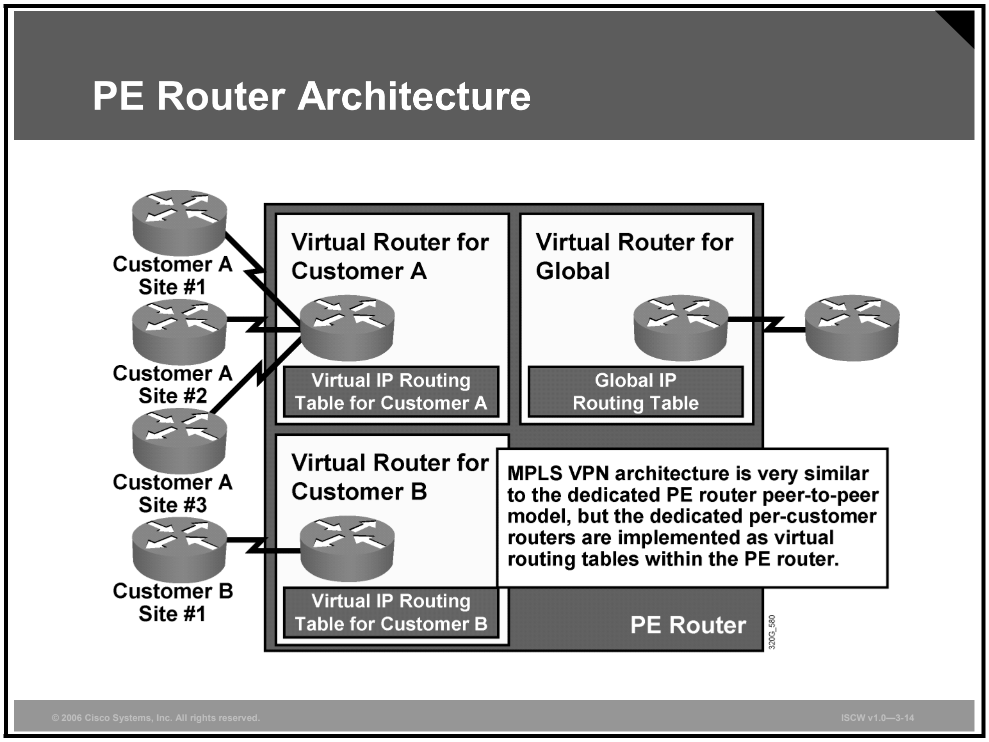
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-13

Contiguous portions of the C-network are called sites and are linked with the P-network via customer edge (CE) routers. The CE routers are connected to the PE routers, which serve as the edge devices of the P-network. The core devices in the P-network, the provider routers, provide transport across the provider backbone and do not carry customer routes.

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

PE Router Architecture

The architecture of a PE router in an MPLS VPN is very similar to the architecture of a POP in the dedicated PE router peer-to-peer model. The only difference is that the whole architecture is condensed into one physical device.



PE Router Architecture

MPLS VPN architecture is very similar to the dedicated PE router peer-to-peer model, but the dedicated per-customer routers are implemented as virtual routing tables within the PE router.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-14

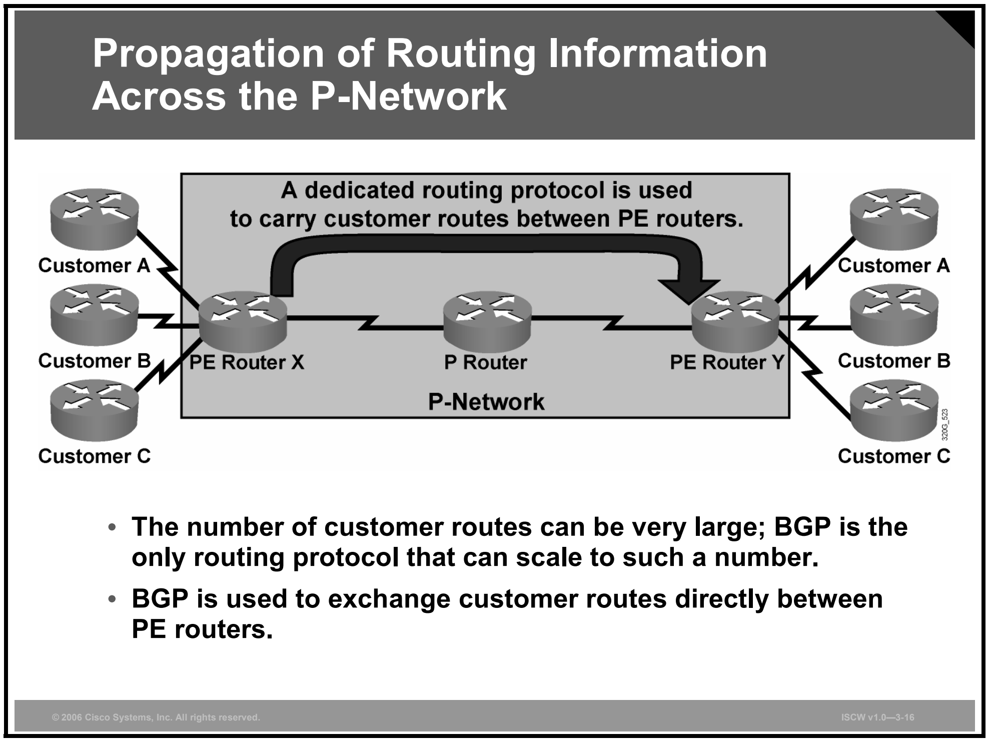
Each customer is assigned an independent routing table, or virtual routing and forwarding (VRF) table that corresponds to the dedicated PE router in the traditional peer-to-peer model. Routing across the provider backbone is performed by another routing process that uses a global IP routing table.

Note	Cisco IOS software implements isolation between customers via VRF tables. The whole PE router is still configured and managed as a single device, not as a set of virtual 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 self-study.*

Propagation of Routing Information Across the P-Network

This topic describes how routing information is propagated across the P-network.



Propagation of Routing Information Across the P-Network

- The number of customer routes can be very large; BGP is the only routing protocol that can scale to such a number.
- BGP is used to exchange customer routes directly between PE routers.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-16

Although VRFs provide isolation between customers, the data from these routing tables still needs to be exchanged between PE routers to enable data transfer between sites attached to different PE routers. Therefore, a routing protocol is needed that will transport all customer routes across the P-network, while maintaining the independence of individual customer address spaces.

The best solution to the customer route propagation issue is to run a single routing protocol between PE routers that will exchange all customer routes without the involvement of the P routers. This solution is scalable. These are some of the benefits of this approach:

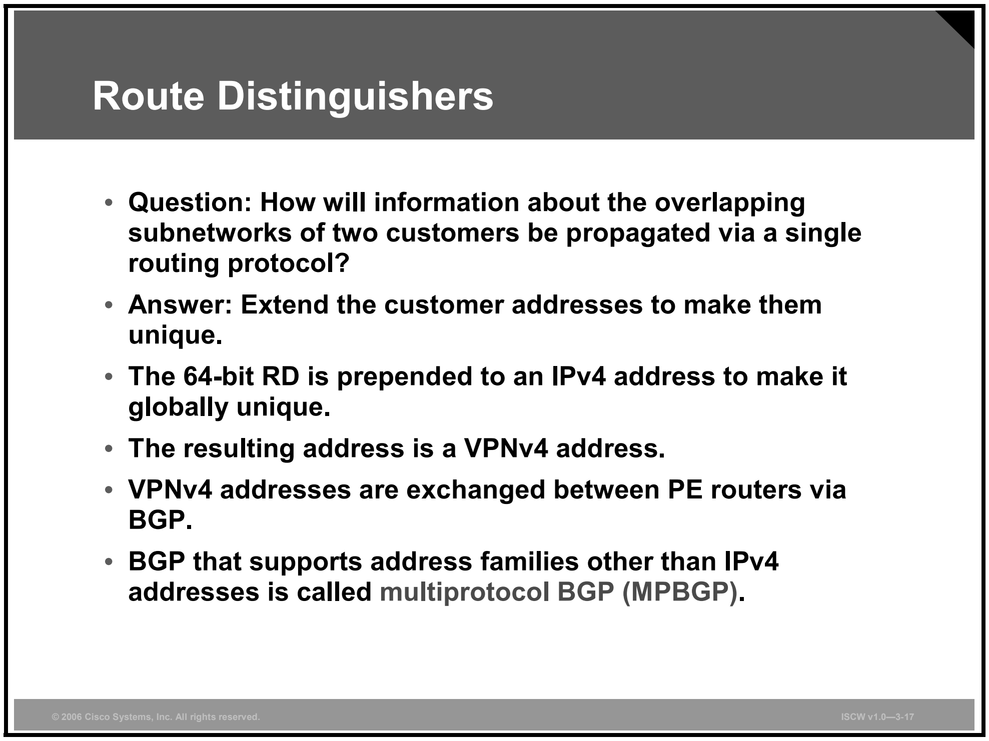
- The number of routing protocols running between PE routers does not increase with an increasing number of customers.
- The P routers do not carry customer routes.

The next design decision to be made is the choice of the routing protocol running between PE routers. Given that the total number of customer routes is expected to be very large, the only well-known protocol with the required scalability is Border Gateway Protocol (BGP). Therefore, BGP is used in MPLS VPN architecture to transport customer routes directly between PE 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 self-study.

Route Distinguishers

MPLS VPN architecture differs from traditional peer-to-peer VPN solutions in the support of overlapping customer address spaces.



Route Distinguishers

- **Question: How will information about the overlapping subnetworks of two customers be propagated via a single routing protocol?**
- **Answer: Extend the customer addresses to make them unique.**
- **The 64-bit RD is prepended to an IPv4 address to make it globally unique.**
- **The resulting address is a VPNv4 address.**
- **VPNv4 addresses are exchanged between PE routers via BGP.**
- **BGP that supports address families other than IPv4 addresses is called multiprotocol BGP (MPBGP).**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-17

With the deployment of a single routing protocol, BGP, to exchange all customer routes between PE routers, an important issue arises: how can BGP propagate several identical prefixes belonging to different customers between PE routers?

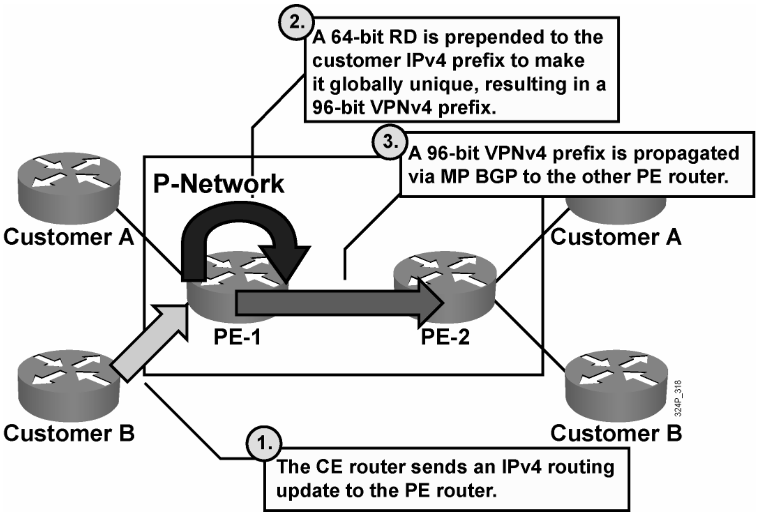
The only solution to this dilemma is the expansion of customer IP prefixes with a unique prefix that makes them unique even if they had previously overlapped. A 64-bit prefix called the RD is used in MPLS VPNs to convert non-unique 32-bit customer IPv4 addresses into 96-bit unique addresses that can be transported between PE routers.

The RD is used only to transform non-unique 32-bit customer IP version 4 (IPv4) addresses into unique 96-bit VPN version 4 (VPNv4) addresses (also called VPN IPv4 addresses).

VPNv4 addresses are exchanged only between PE routers; they are never used between CE routers. The BGP session between PE routers must therefore support the exchange of traditional IPv4 prefixes and the exchange of VPNv4 prefixes. A BGP session between PE routers must support multiple protocols, so an MPBGP session is established.

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

Route Distinguishers (Cont.)



2. A 64-bit RD is prepended to the customer IPv4 prefix to make it globally unique, resulting in a 96-bit VPNv4 prefix.

3. A 96-bit VPNv4 prefix is propagated via MP BGP to the other PE router.

1. The CE router sends an IPv4 routing update to the PE router.

© 2006 Cisco Systems, Inc. All rights reserved.

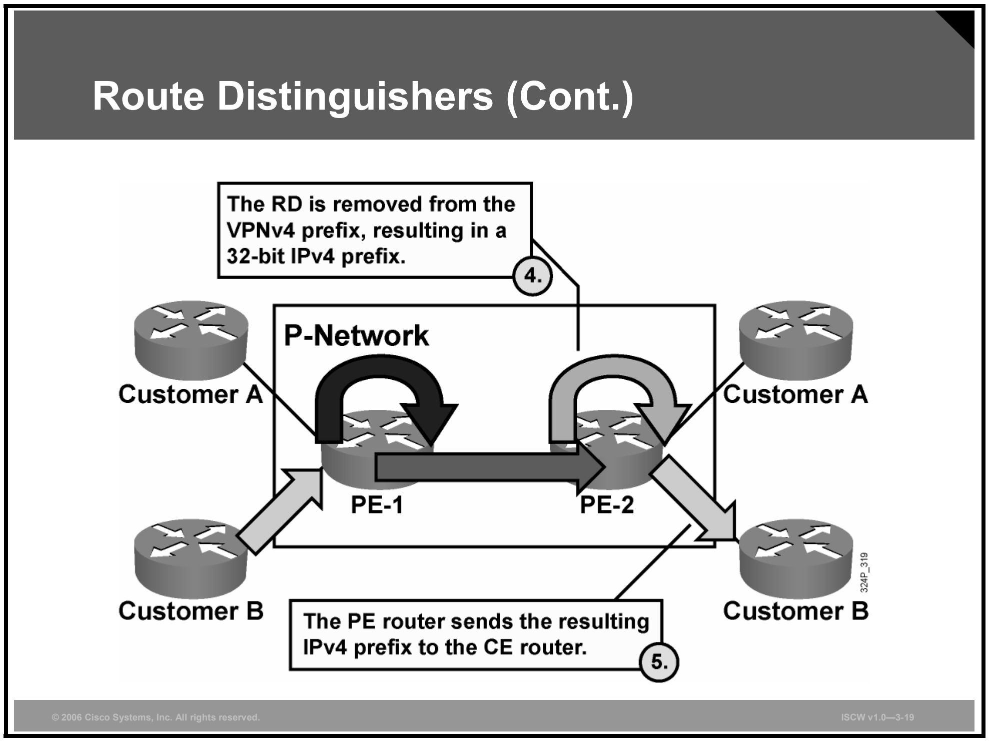
Customer route propagation across an MPLS VPN network is done using this process:

Step 1 The CE router sends an IPv4 routing update to the PE router.

Step 2 The PE router prepends a 64-bit RD to the IPv4 routing update, resulting in a globally unique 96-bit VPNv4 prefix.

Step 3 The VPNv4 prefix is propagated via an MPBGP session to other PE 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 self-study.



Route Distinguishers (Cont.)

The RD is removed from the VPNv4 prefix, resulting in a 32-bit IPv4 prefix. 4.

The PE router sends the resulting IPv4 prefix to the CE router. 5.

© 2006 Cisco Systems, Inc. All rights reserved.

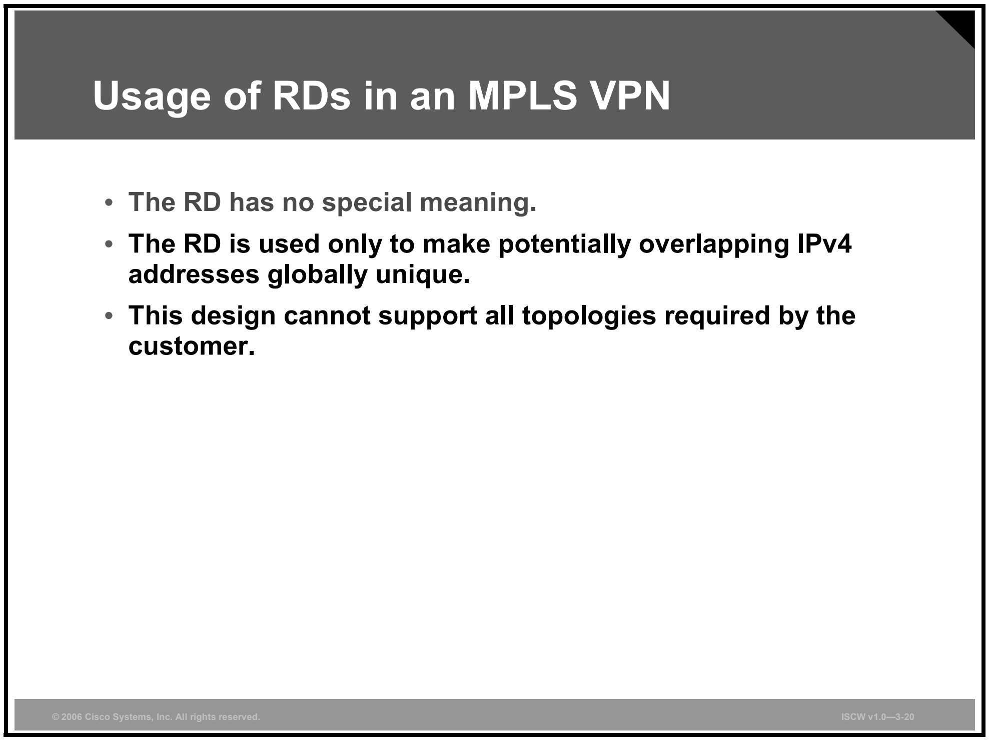
Step 4 The receiving PE routers strip the RD from the VPNv4 prefix, resulting in an IPv4 prefix.

Step 5 The IPv4 prefix is forwarded to other CE routers within an IPv4 routing 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 self-study.

Usage of RDs in an MPLS VPN

The RD has no special meaning or role in MPLS VPN architecture.



Usage of RDs in an MPLS VPN

- The RD has no special meaning.
- **The RD is used only to make potentially overlapping IPv4 addresses globally unique.**
- **This design cannot support all topologies required by the customer.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-20

The only function of the RD is to make overlapping IPv4 addresses globally unique.

Note	Because there has to be a unique one-to-one mapping between RD and VRFs, the RD could be viewed as the VRF identifier in the Cisco implementation of an MPLS VPN.

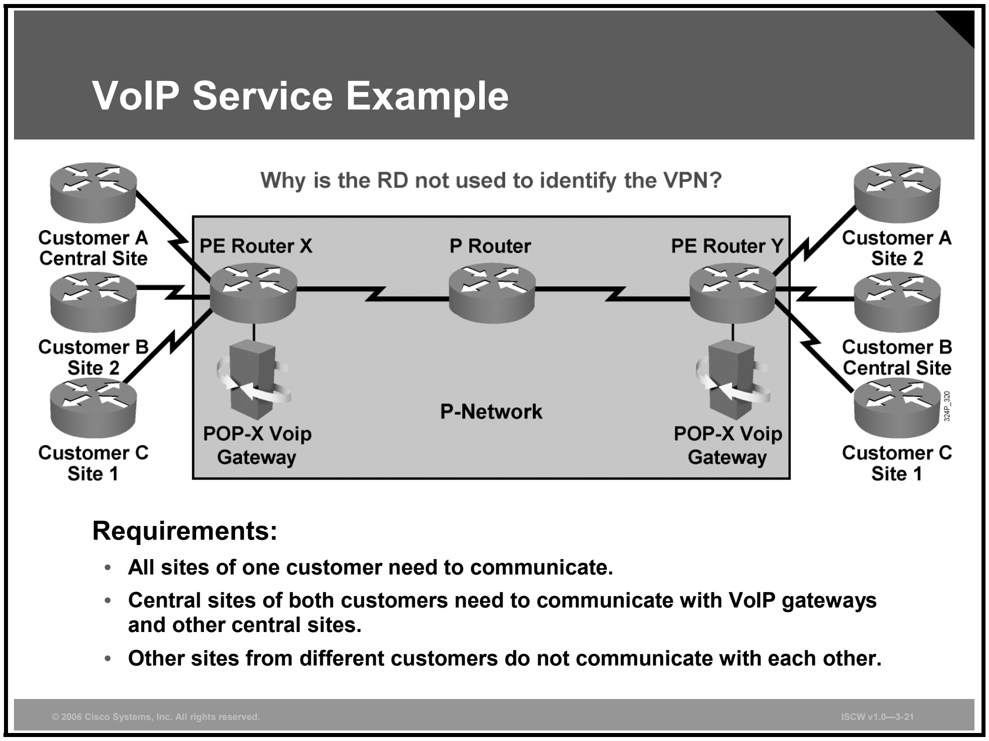
The RD is configured at the PE router as part of the setup of the VPN site. The RD is not configured on the CE and is not visible to the customer.

Simple VPN topologies require only one RD per customer, raising the possibility that the RD could serve as a VPN identifier. This design, however, would not allow implementation of more complex VPN topologies, such as when a customer site belongs to multiple VPNs.

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

VoIP Service in VPN Environment

To illustrate the need for a more versatile VPN indicator than the RD, consider the VoIP service.



VoIP Service Example

Why is the RD not used to identify the VPN?

Requirements:

- **All sites of one customer need to communicate.**
- **Central sites of both customers need to communicate with VoIP gateways and other central sites.**
- **Other sites from different customers do not communicate with each other.**

© 2006 Cisco Systems, Inc. All rights reserved.

The figure illustrates the need for a more versatile VPN indicator than the RD. The connectivity requirements of the VoIP service are as follows:

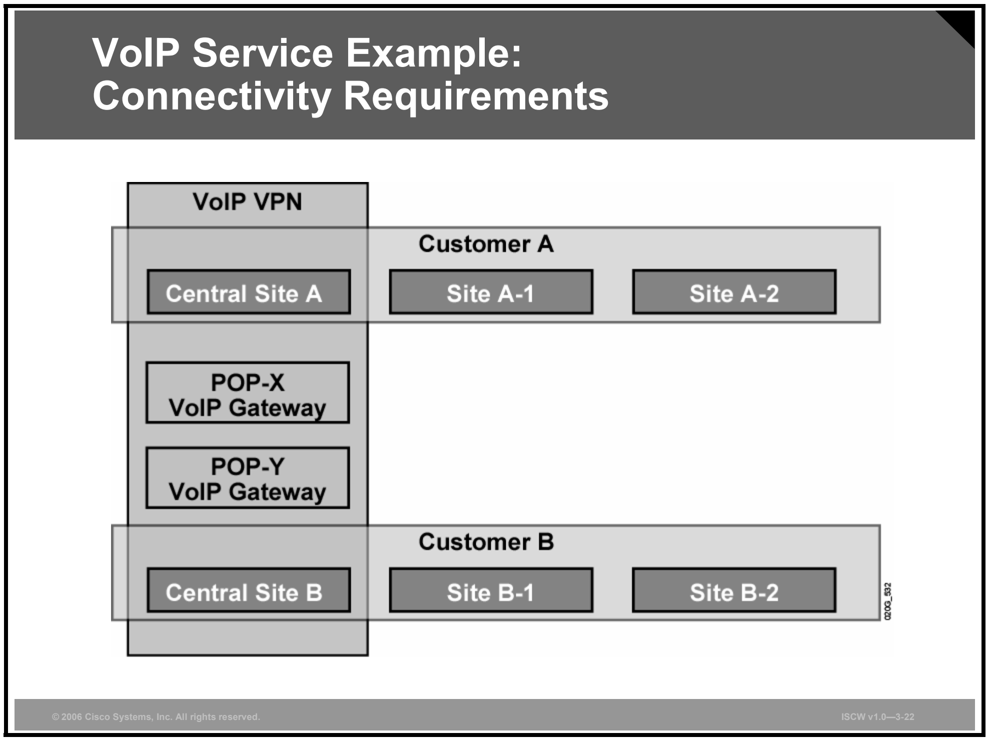
- All sites of a single customer need to communicate.
- The central sites of different customers subscribed to the VoIP service need to communicate with the VoIP gateways to originate and receive calls in the public voice network, and also with other central sites to exchange inter-company voice calls.

Note Additional security measures have to be put in place at central sites to ensure that the central sites exchange only VoIP calls with other central sites. Otherwise, the corporate network of a customer could be compromised by another customer who is using the VoIP 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 self-study.

Connectivity Requirements

The connectivity requirements of the VoIP service are illustrated in the figure.



VoIP Service Example:
Connectivity Requirements

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-22

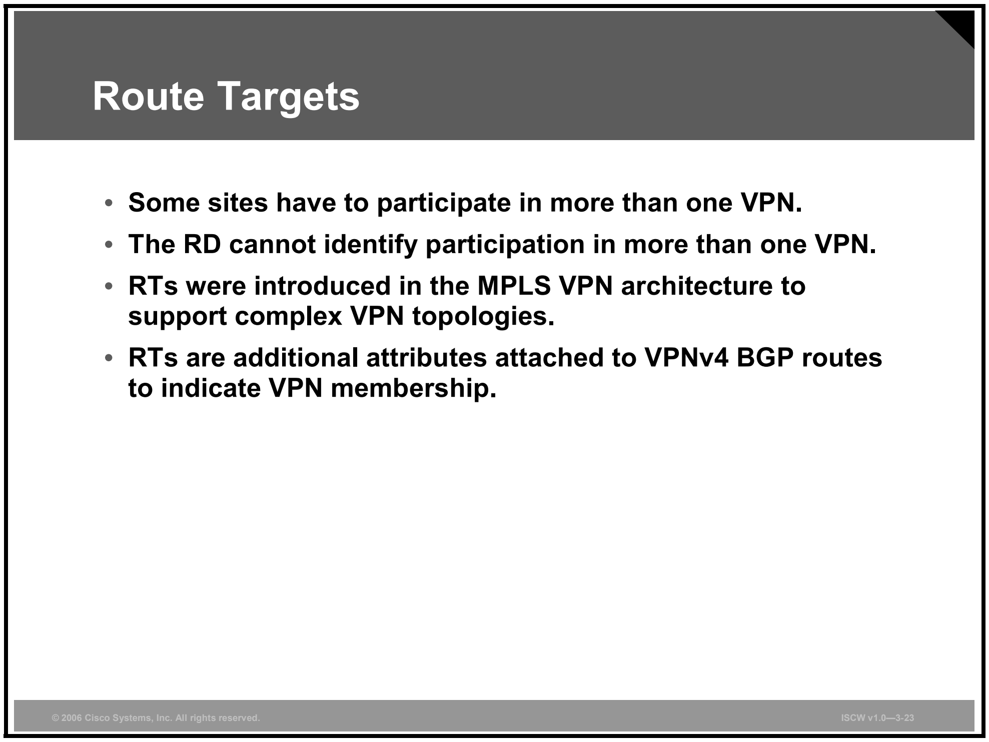
Three VPNs are needed to implement the desired connectivity: two customer VPNs (customer A and customer B) and a shared VoIP VPN, related as follows:

- Central site A participates in the customer A VPN and in the VoIP VPN.
- Central site B participates in the customer B VPN and in the VoIP VPN.
- Customer sites A-1 and A-2 participate in customer A VPN.
- Customer sites B-1 and B-2 participate in customer B VPN.

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

Route Targets

The RD (again, a single entity prepended to an IPv4 route) cannot indicate that a site participates in more than one VPN. A method is needed in which a set of VPN identifiers can be attached to a route to indicate its membership in several VPNs.



Route Targets

- **Some sites have to participate in more than one VPN.**
- **The RD cannot identify participation in more than one VPN.**
- **RTs were introduced in the MPLS VPN architecture to support complex VPN topologies.**
- **RTs are additional attributes attached to VPNv4 BGP routes to indicate VPN membership.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-23

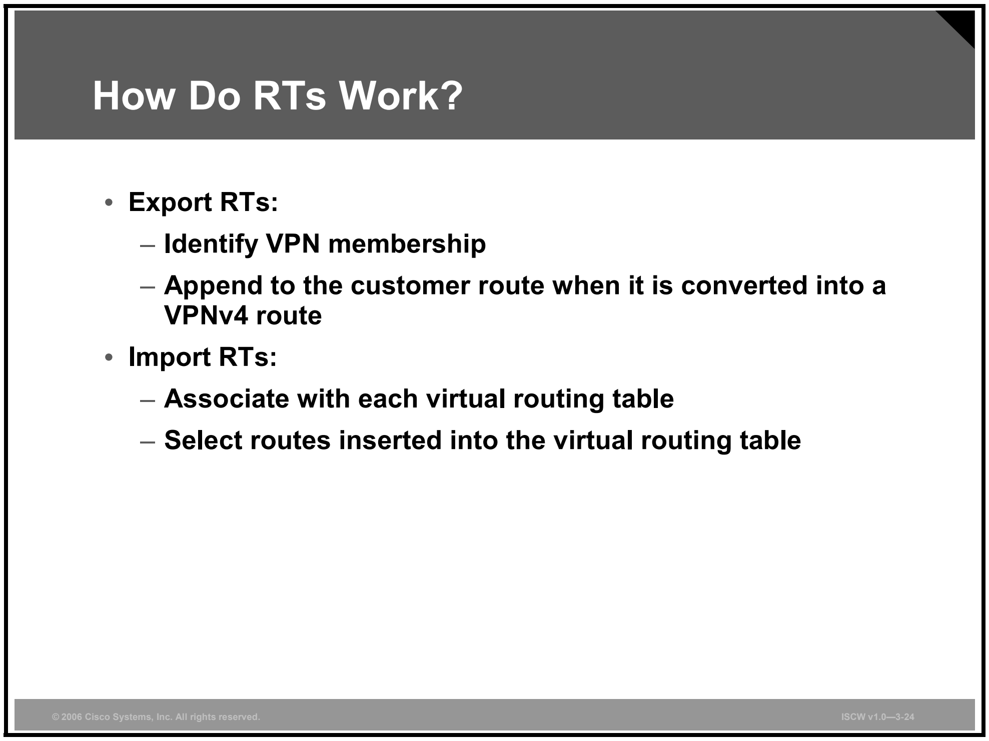
RTs were introduced into the MPLS VPN architecture to support the requirements for multi-VPN membership.

RTs are attributes that are attached to a VPNv4 BGP route to indicate its VPN membership.

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

How Do RTs Work?

MPLS VPN RTs are attached to a customer route at the moment that it is converted from an IPv4 route to a VPNv4 route by the PE router. The RTs attached to the route are called export RTs and are configured separately for each virtual routing table in a PE router. Export RTs identify a set of VPNs to which sites associated with the virtual routing table belong.



How Do RTs Work?

- **Export RTs:**
  - **Identify VPN membership**
  - **Append to the customer route when it is converted into a VPNv4 route**
- **Import RTs:**
  - **Associate with each virtual routing table**
  - **Select routes inserted into the virtual routing table**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-24

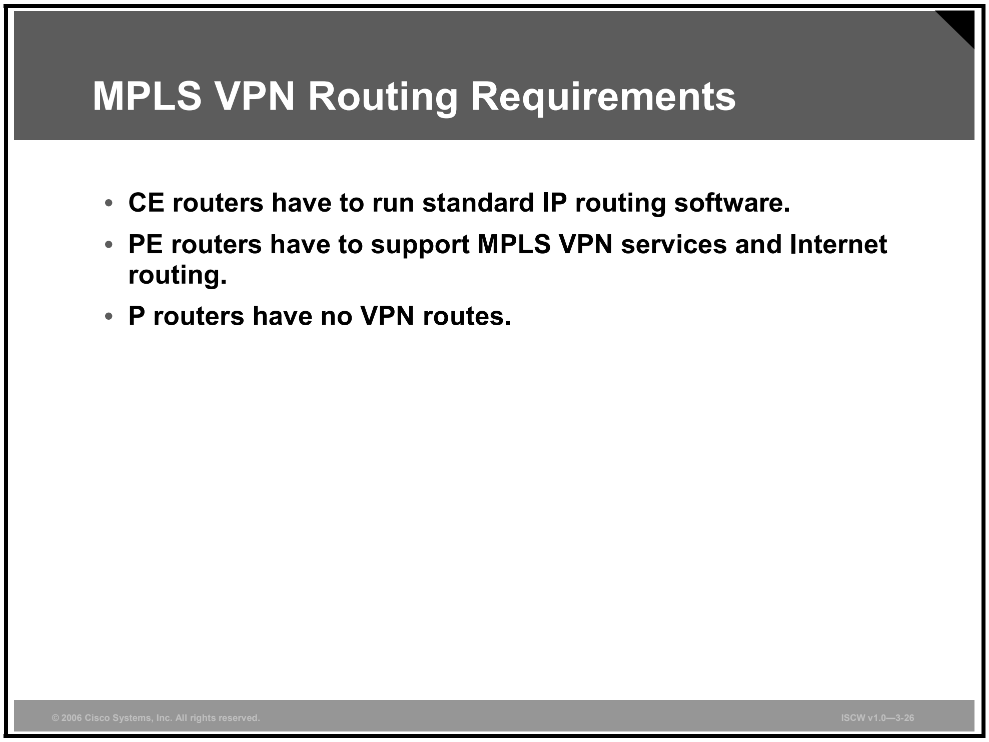
When the VPNv4 routes are propagated to other PE routers, those routers need to select the routes to import into their virtual routing tables. This selection is based on import RTs. Each virtual routing table in a PE router can have a number of configured import RTs that identify the set of VPNs from which the virtual routing table is accepting routes.

In overlapping VPN topologies, RTs are used to identify VPN membership. Advanced VPN topologies (for example, central services VPNs) use RTs in more complex scenarios.

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

End-to-End Routing Information Flow

This topic describes the end-to-end flow of routing updates in an MPLS VPN.



MPLS VPN Routing Requirements

- CE routers have to run standard IP routing software.
- PE routers have to support MPLS VPN services and Internet routing.
- P routers have no VPN routes.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—3-26

MPLS VPN Routing Requirements

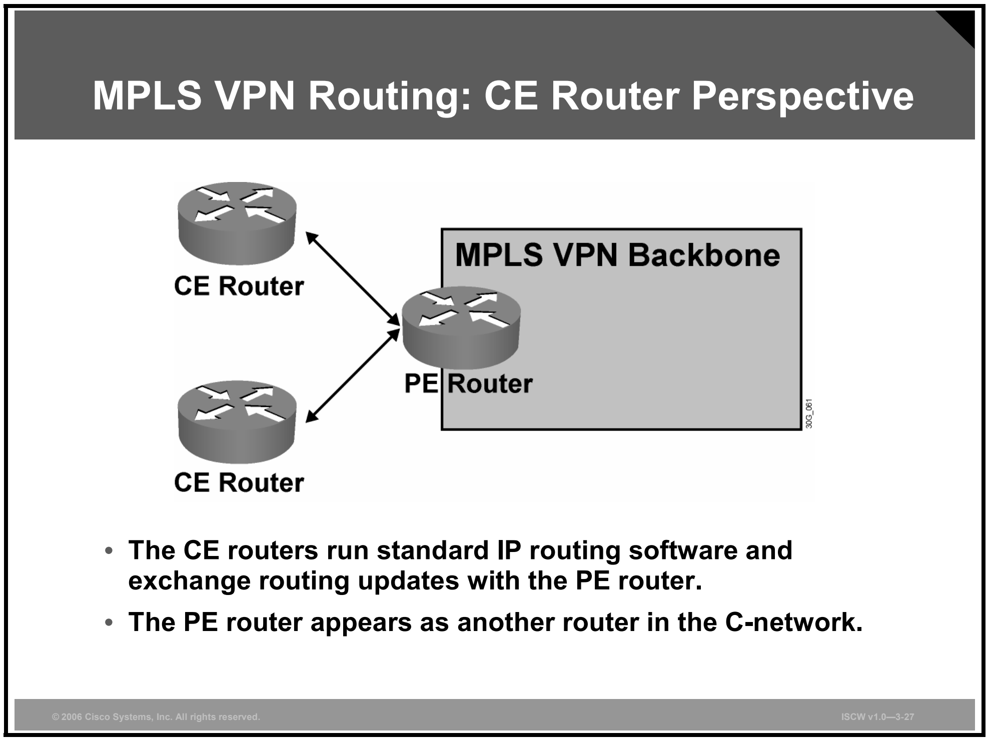
The designers of MPLS VPN technology were faced with these routing requirements:

- CE routers should not be MPLS VPN-aware; they should run standard IP routing software.
- PE routers must support MPLS VPN services and traditional Internet services.
- To make the MPLS VPN solution scalable, P routers must not carry VPN routes.

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

CE Router Perspective

The MPLS VPN backbone should look like a standard corporate backbone to the CE routers.



MPLS VPN Routing: CE Router Perspective

- **The CE routers run standard IP routing software and exchange routing updates with the PE router.**
- **The PE router appears as another router in the C-network.**

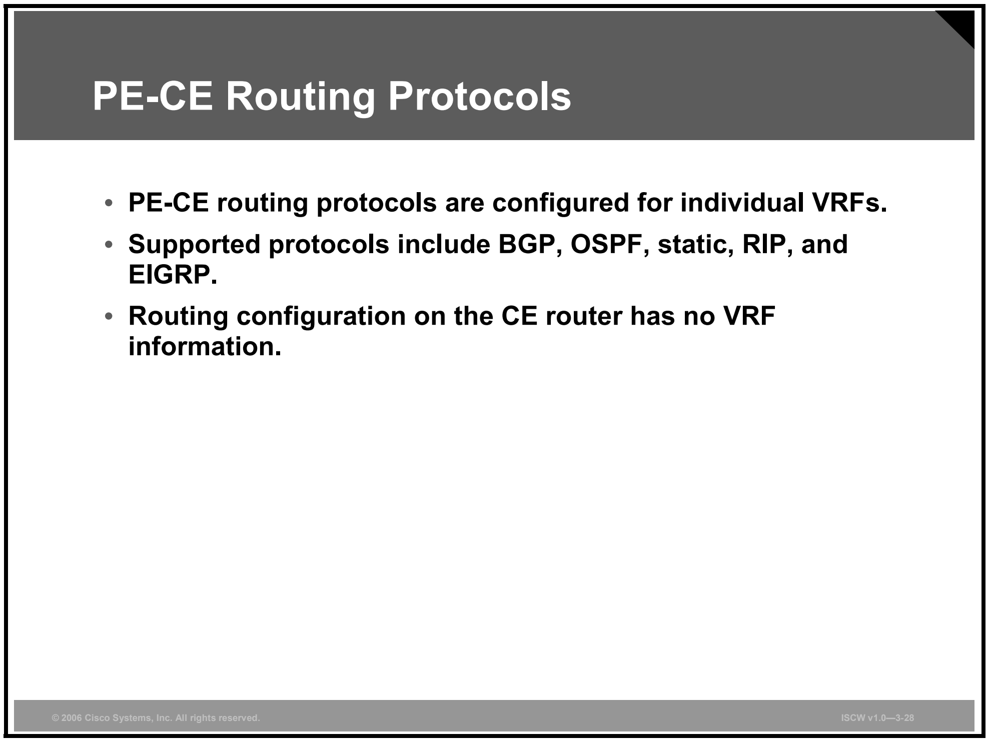
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-27

The CE routers run standard IP routing software and exchange routing updates with the PE routers, which appear to them as normal routers in the C-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 self-study.

PE-CE Routing Protocol

After you configure VRFs and establish MPBGP connectivity between PE routers, you have to configure routing protocols between the PE router and the attached CE routers. The PE-CE routing protocols on the PE router need to be configured for individual VRFs.



PE-CE Routing Protocols

- **PE-CE routing protocols are configured for individual VRFs.**
- **Supported protocols include BGP, OSPF, static, RIP, and EIGRP.**
- **Routing configuration on the CE router has no VRF information.**

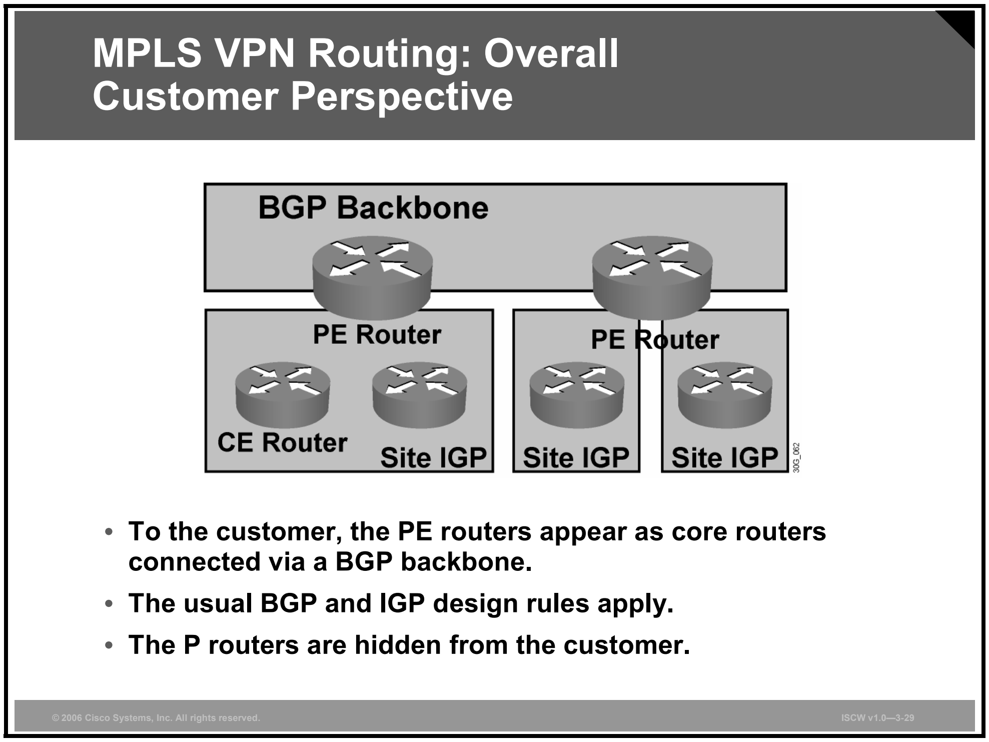
© 2006 Cisco Systems, Inc. All rights reserved.

Configuring routing protocol on the CE site is very simple. The customer has no information on VRFs configured on the provider site. Customer configuration is the same configuration as if routing between two devices in the C-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 self-study.

Overall Customer Perspective

From the customer perspective, the MPLS VPN backbone looks like an intra-company BGP backbone with PE routers performing route redistribution between individual sites and the core backbone.



MPLS VPN Routing: Overall Customer Perspective

- To the customer, the PE routers appear as core routers connected via a BGP backbone.
- The usual BGP and IGP design rules apply.
- The P routers are hidden from the customer.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-29

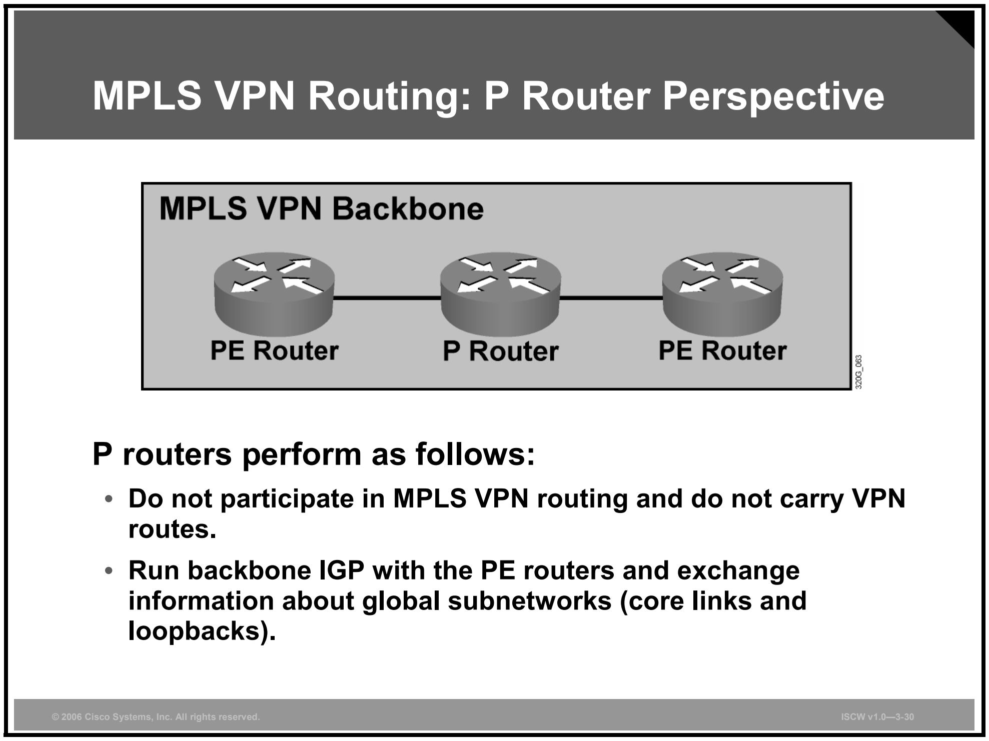
The standard design rules used for enterprise BGP backbones can be applied to the design of the C-network.

The P routers are hidden from the customer view; the internal topology of the BGP backbone is therefore transparent to the customer.

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

P Router Perspective

From the P router perspective, the MPLS VPN backbone looks even simpler—the P routers do not participate in MPLS VPN routing and do not carry VPN routes.



MPLS VPN Routing: P Router Perspective

P routers perform as follows:

- **Do not participate in MPLS VPN routing and do not carry VPN routes.**
- **Run backbone IGP with the PE routers and exchange information about global subnetworks (core links and loopbacks).**

© 2006 Cisco Systems, Inc. All rights reserved.

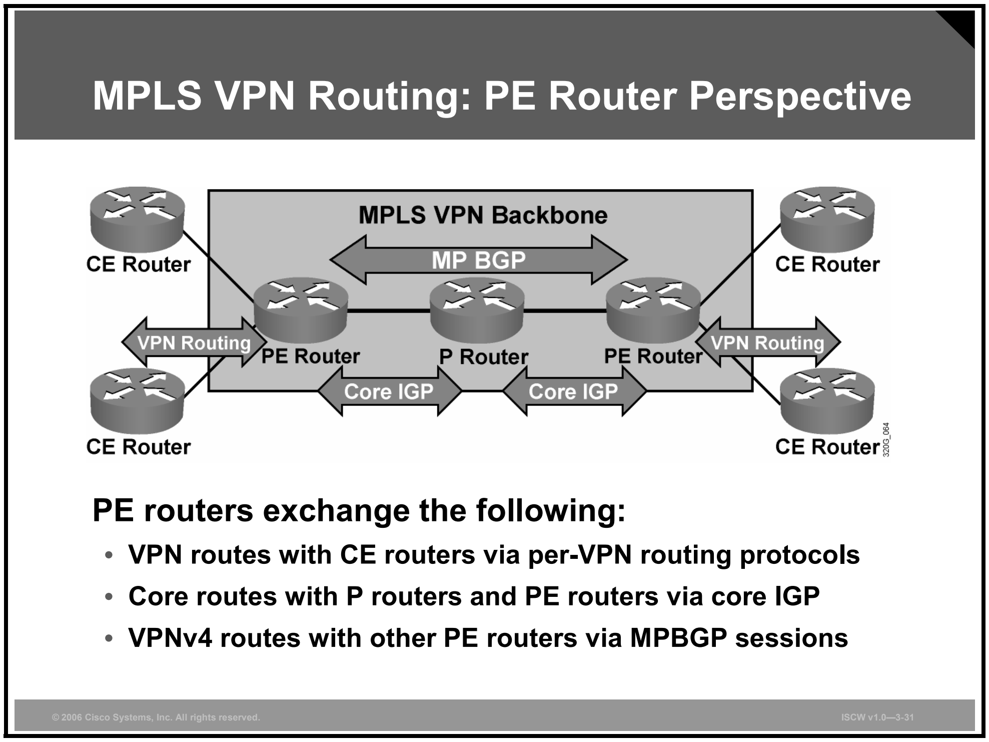
ISCW v1.0—3-30

The P routers run only a backbone Interior Gateway Protocol (IGP) with other P routers and with PE routers, and exchange information about core subnetworks and loopbacks. BGP deployment on P routers is not needed for proper MPLS VPN operation; it might be needed, however, to support traditional Internet connectivity that has not yet been migrated to MPLS.

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

PE Router Perspective

The PE routers are the only routers in MPLS VPN architecture that see all routing aspects of the MPLS VPN.



MPLS VPN Routing: PE Router Perspective

PE routers exchange the following:

- **VPN routes with CE routers via per-VPN routing protocols**
- **Core routes with P routers and PE routers via core IGP**
- **VPNv4 routes with other PE routers via MPBGP sessions**

© 2006 Cisco Systems, Inc. All rights reserved.

PE routers are able to exchange the following:

- IPv4 VPN routes with CE routers via various routing protocols running in the VRF tables of the PE.

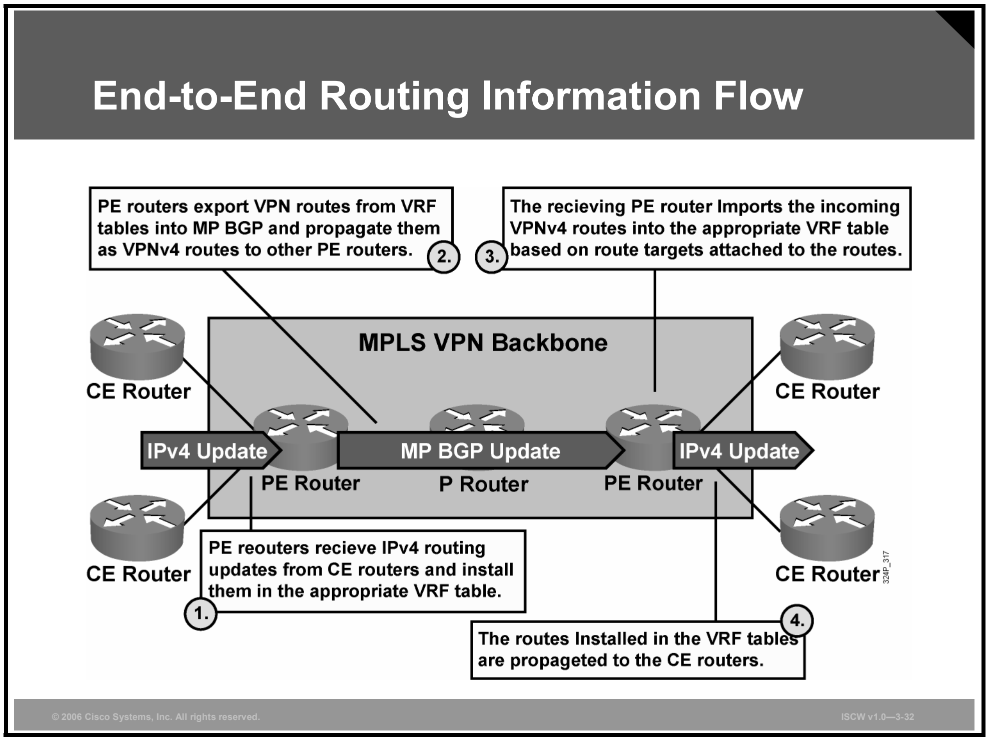
Note Static routing can also be used between the CE and PE.

- VPNv4 routes via MPBGP sessions with other PE routers
- Core routes with P routers and other PE routers via core IGP

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

Identifying End-to-End Routing Update Flow

This figure provides an overview of end-to-end routing information flow in an MPLS VPN network.



End-to-End Routing Information Flow

2. PE routers export VPN routes from VRF tables into MP BGP and propagate them as VPNv4 routes to other PE routers.

3. The recieving PE router Imports the incoming VPNv4 routes into the appropriate VRF table based on route targets attached to the routes.

1. PE reouters recieve IPv4 routing updates from CE routers and install them in the appropriate VRF table.

4. The routes Installed in the VRF tables are propageted to the CE routers.

© 2006 Cisco Systems, Inc. All rights reserved.   ISCW v1.0—3-32

These steps describe the stages of routing information flow—from the IPv4 routing updates entering the MPLS VPN backbone through their propagation as VPNv4 routes across the backbone:

Step 1 PE routers receive IPv4 routing updates from the CE routers and install them in the appropriate VRF table.

Step 2 The customer routes from VRF tables are exported as VPNv4 routes into MPBGP and propagated to other PE routers.

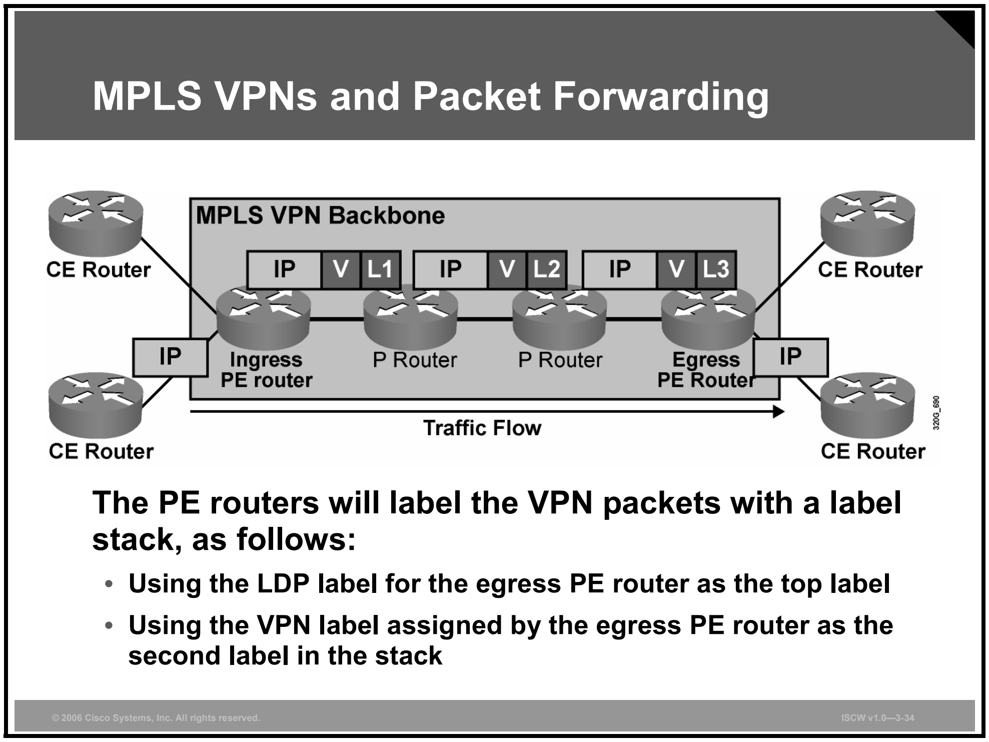
Step 3 The PE routers receiving MPBGP updates import the incoming VPNv4 routes into their VRF tables based on RTs attached to the incoming routes and on import RTs configured in the VRF tables.

Step 4 The VPNv4 routes installed in the VRF tables are converted to IPv4 routes and then propagated to the CE 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 self-study.

MPLS VPNs and Packet Forwarding

This topic describes MPLS VPN packet forwarding.



MPLS VPNs and Packet Forwarding

The PE routers will label the VPN packets with a label stack, as follows:

- **Using the LDP label for the egress PE router as the top label**
- **Using the VPN label assigned by the egress PE router as the second label in the stack**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-34

You can use an MPLS label stack to tell the egress PE router what to do with the VPN packet. When using the label stack, the ingress PE router labels the incoming IP packet with two labels:

- The top label in the stack is the Label Distribution Protocol (LDP) label for the egress PE router. This label guarantees that the packet will traverse the MPLS VPN backbone and arrive at the egress PE router.
- The second label in the stack is assigned by the egress PE router and tells the router how to forward the incoming VPN packet. The second label could point directly toward an outgoing interface, in which case the egress PE router would perform label lookup only on the VPN packet. The second label could also point to a VRF table, in which case the egress PE router would first perform a label lookup to find the target VRF table and then perform an IP lookup within the VRF table.

Both methods are used in Cisco IOS software. The second label in the stack points toward an outgoing interface whenever the CE router is the next hop of the VPN route. The second label in the stack points to the VRF table for aggregate VPN routes, VPN routes pointing to a null interface, and routes for directly connected VPN interfaces.

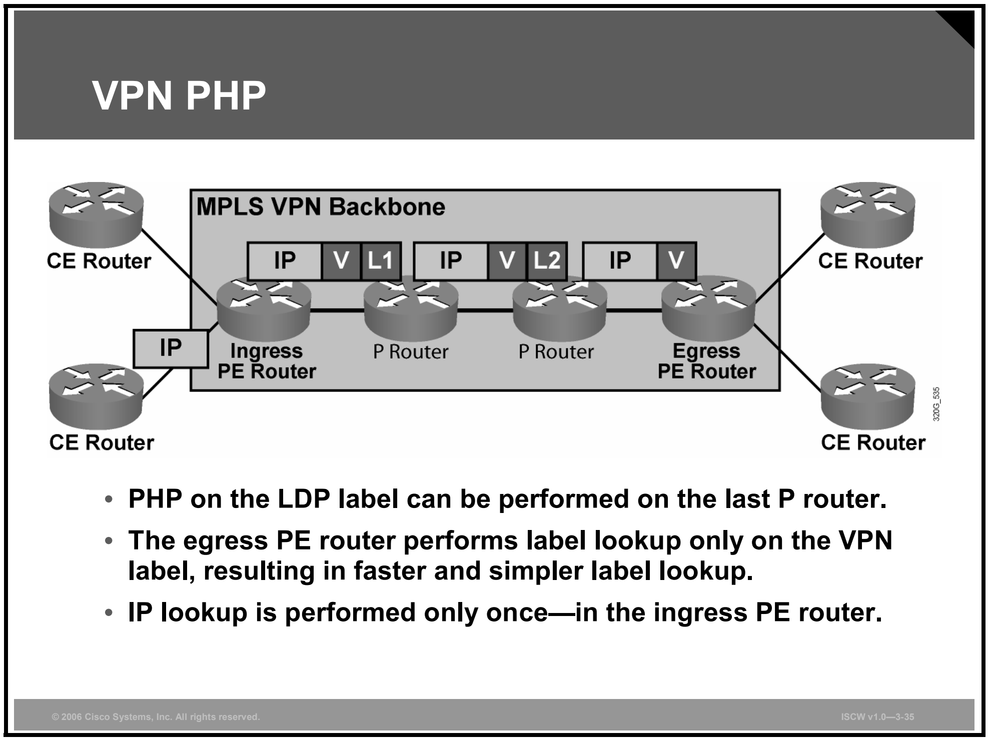
The two-level MPLS label stack satisfies these MPLS VPN forwarding requirements:

- The P routers perform label switching on the LDP-assigned label toward the egress PE router.
- The egress PE router performs label switching on the second label (which it has previously assigned), and either forwards the IP packet toward the CE router or performs another IP lookup in the VRF table pointed to by the second label in the stack.

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

VPN PHP

Penultimate Hop Popping (PHP), the removal of the top label in the stack on the hop prior to the egress router, can be performed in frame-based MPLS networks.



VPN PHP

- PHP on the LDP label can be performed on the last P router.
- The egress PE router performs label lookup only on the VPN label, resulting in faster and simpler label lookup.
- IP lookup is performed only once—in the ingress PE router.

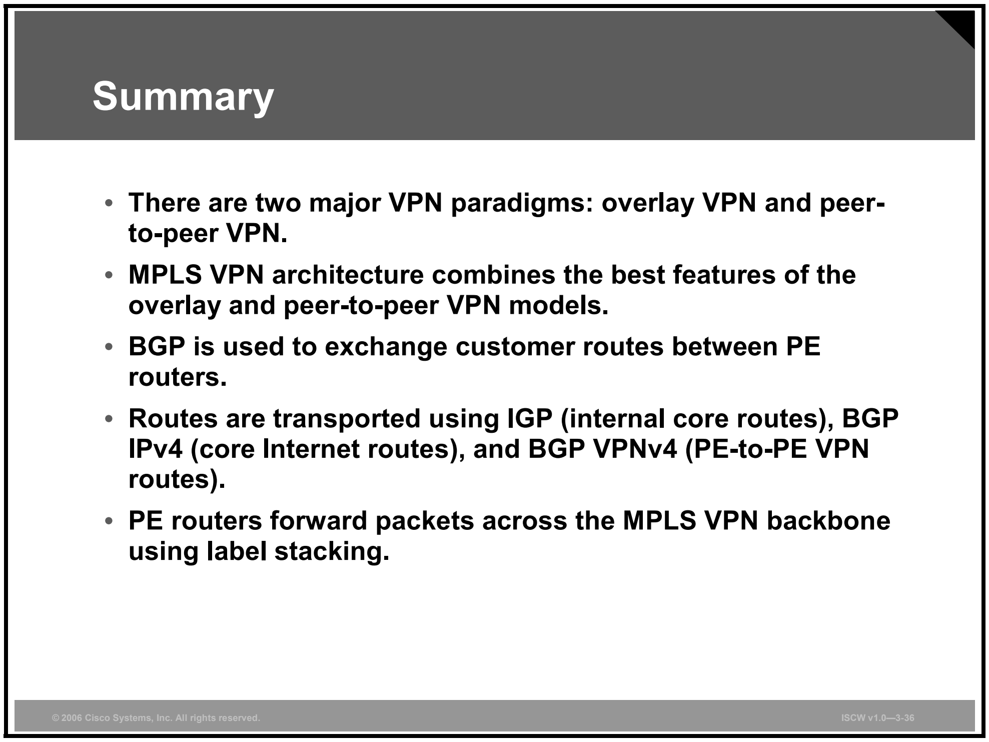
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-35

In these networks, the last P router in the Label Switch Path (LSP) tunnel pops the LDP label, as previously requested by the egress PE router through LDP, and the PE router receives a labeled packet that contains only the VPN label. In most cases, a single label lookup performed on that packet in the egress PE router is enough to forward the packet toward the CE router. The full IP lookup through the Forwarding Information Base (FIB) is performed only once, in the ingress PE router, even without PHP.

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

Summary

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



Summary

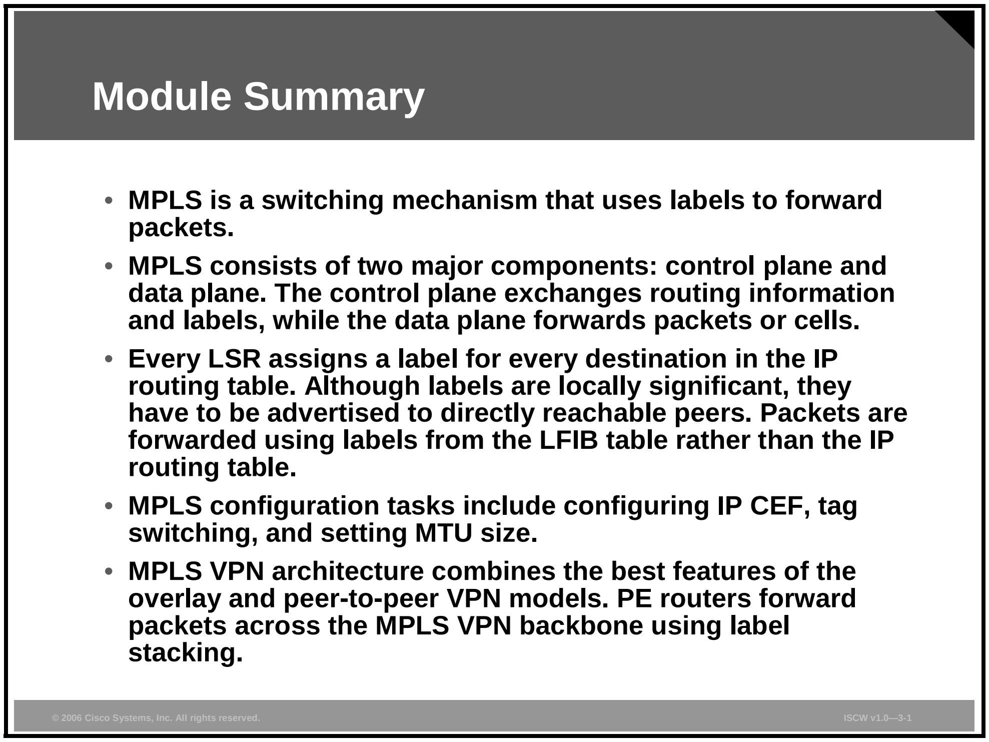
- There are two major VPN paradigms: overlay VPN and peer-to-peer VPN.
- MPLS VPN architecture combines the best features of the overlay and peer-to-peer VPN models.
- BGP is used to exchange customer routes between PE routers.
- Routes are transported using IGP (internal core routes), BGP IPv4 (core Internet routes), and BGP VPNv4 (PE-to-PE VPN routes).
- PE routers forward packets across the MPLS VPN backbone using label stacking.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-36

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

Module Summary

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



Module Summary

- MPLS is a switching mechanism that uses labels to forward packets.
- MPLS consists of two major components: control plane and data plane. The control plane exchanges routing information and labels, while the data plane forwards packets or cells.
- Every LSR assigns a label for every destination in the IP routing table. Although labels are locally significant, they have to be advertised to directly reachable peers. Packets are forwarded using labels from the LFIB table rather than the IP routing table.
- MPLS configuration tasks include configuring IP CEF, tag switching, and setting MTU size.
- MPLS VPN architecture combines the best features of the overlay and peer-to-peer VPN models. PE routers forward packets across the MPLS VPN backbone using label stacking.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—3-1

Multiprotocol Label Switching (MPLS) forwards packets based on labels. In an MPLS network, labels are assigned and distributed. Label information is populated in the Label Information Base (LIB), Forwarding Information Base (FIB), and Label Forwarding Information Base (LFIB) tables. The two major virtual private network (VPN) design options—overlay VPN and peer-to-peer VPN—have many benefits and drawbacks. MPLS VPN architecture combines the best features of the overlay and peer-to-peer VPN models.

References

For additional information, refer to these resources:

- RFC 3031: *Multiprotocol Label Switching Architecture* at http://www.ietf.org/rfc/rfc3031.txt
- RFC 3032: *MPLS Label Stack Encoding* at http://www.ietf.org/rfc/rfc3032.txt
- RFC 3036: *LDP Specification* at http://www.ietf.org/rfc/rfc3036.txt

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-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) Which three of these statements are true? (Choose three.) (Source: Introducing MPLS Networks)

A) MPLS uses labels to forward packets.
B) MPLS is used to forward IP packets only.
C) MPLS labels can correspond to a Layer 3 destination address, QoS, source address, or Layer 2 circuit.
D) MPLS does not require a routing table lookup on core routers.
E) MPLS requires a routing table lookup on core routers.
F) MPLS replaces IP header with label.
G) MPLS label header consists of 32 bytes.

Q2) The LDP is the responsibility of the _____. (Source: Introducing MPLS Networks)

A) data plane
B) forwarding plane
C) system plane
D) control plane

Q3) How many bits does the MPLS label header consists of? (Source: Introducing MPLS Networks)

A) 64
B) 32
C) 16
D) 8

Q4) Which two of these statements are true? (Choose two.) (Source: Introducing MPLS Networks)

A) An edge LSR is a device that primarily inserts labels on packets or removes labels.
B) An LSR is a device that primarily labels packets or removes labels.
C) An LSR is a device that forwards packets primarily based on labels.
D) An edge LSR is a device that forwards packets primarily based on labels.
E) LSRs are usually capable of doing label switching only.

Q5) Which of these terms is best described as “a simple label-based forwarding engine”? (Source: Introducing MPLS Networks)

A) control plane
B) ground plane
C) data plane
D) routing plane

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

Q6) When an IP packet is to be label-switched as it traverses an MPLS network, which table is used to perform the label switching? (Source: Assigning MPLS Labels to Packets)

A) LIB
B) FIB
C) RIB
D) LFIB

Q7) Which two tables contain label information? (Choose two.) (Source: Assigning MPLS Labels to Packets)

A) LIB
B) main IP routing table
C) BGP table
D) LFIB
E) LDP neighbor table

Q8) Which statement is correct? (Source: Assigning MPLS Labels to Packets)

A) An IP forwarding table resides on the data plane, LDP runs on the control plane, and an IP routing table resides on the data plane.
B) An IP forwarding table resides on the data plane, LDP runs on the control plane, and an IP routing table resides on the control plane.
C) An IP forwarding table resides on the control plane, LDP runs on the control plane, and an IP routing table resides on the data plane.
D) An IP forwarding table resides on the control plane, LDP runs on the control plane, and an IP routing table resides on the control plane.

Q9) Which statement is correct? (Source: Assigning MPLS Labels to Packets)

A) An incoming IP packet is forwarded by using the FIB table, and can be sent out as an IP packet or as a labeled IP packet.
B) An incoming IP packet is forwarded by using the FIB table, and can be sent out only as an IP packet.
C) An incoming IP packet is forwarded by using the FIB table, and can be sent out only as a labeled IP packet.
D) An incoming IP packet is forwarded by using the LIB table, and can be sent out as an IP packet or as a labeled IP packet.

Q10) Which of these statements best describes PHP? (Source: Assigning MPLS Labels to Packets)

A) PHP works only for TDP and not for LDP.
B) PHP works only for LDP and not for TDP.
C) PHP optimizes MPLS performance.
D) PHP is configurable and is disabled by default.

Q11) Which of the following is *not* a mandatory step to enable MPLS? (Source: Implementing Frame Mode MPLS)

A) Enable CEF switching.
B) Configure the MTU size for labeled packets.
C) Enable label switching on a frame mode interface.

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

Q12) Which command is used to enable CEF on a Cisco router? (Source: Implementing Frame Mode MPLS)

A) `Router#ip cef`
B) `Router>ip cef`
C) `Router(config)#cef`
D) `Router(config)#ip cef`

Q13) Which command is used to enable MPLS in Cisco IOS software? (Source: Implementing Frame Mode MPLS)

A) `Router#mpls ip`
B) `Router>ip mpls`
C) `Router(config)#ip mpls`
D) `Router(config-if)#mpls ip`

Q14) The MPLS MTU is increased to _____ to support 1500-B IP packets and MPLS stacks up to three levels deep. (Source: Implementing Frame Mode MPLS)

Q15) Which VPN type does *not* require the SP to participate in customer routing? (Source: MPLS VPN Technology)

A) overlay
B) peer-to-peer
C) MPLS VPN
D) overlay-to-overlay

Q16) Which two network elements are contained in the provider network? (Choose two.) (Source: MPLS VPN Technology)

A) P device
B) CE device
C) PE device
D) CE router
E) customer core router

Q17) Which well-known routing protocol can scale to a very large number of routes? (Source: MPLS VPN Technology)

A) BGP
B) RIP
C) OSPF
D) EIGRP

Q18) In which two ways do MPLS VPNs support overlapping customer address spaces between different customers? (Choose two.) (Source: MPLS VPN Technology)

A) by implementing unique RDs for each customer
B) by implementing unique RTs for each customer
C) by implementing different LSPs for each customer
D) by implementing virtual routing tables for each customer
E) by using different routing protocols in the provider network for each customer

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

Module Self-Check Answer Key

Q1)	A, C, D
Q2)	D
Q3)	B
Q4)	A, C
Q5)	C
Q6)	D
Q7)	A, D
Q8)	B
Q9)	A
Q10)	C
Q11)	B
Q12)	D
Q13)	D
Q14)	1,512
Q15)	A
Q16)	A, C
Q17)	A
Q18)	A, D

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

Module 4

IPsec VPNs

Overview

Virtual private networks (VPNs) use advanced encryption techniques and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets.

Cisco offers a wide range of VPN products, from VPN-optimized routers and firewalls to dedicated VPN concentrators that are used to create VPN solutions that meet the requirements of any organization.

This module describes the fundamental terms used with IPsec VPNs, and describes different types of IPsec VPNs and their configurations in detail. Generic Routing Encapsulation (GRE) tunnels and Cisco VPN Client for Windows are also introduced.

Module Objectives

Upon completing this module, you will be able to describe and configure a site-to-site IPsec VPN. This ability includes being able to meet these objectives:

- Describe the fundamental concepts, technologies, and terms used with IPsec VPNs
- Describe IPsec site-to-site VPN operations
- Describe the procedure to configure a site-to-site IPsec VPN with preshared key authentication using SDM, and explain the resulting CLI configurations
- Explain GRE encapsulations, operations, and configurations
- Describe the procedure to configure VPN backup interfaces
- Describe the procedure to configure and verify a Cisco Easy VPN Server and an IPsec VPN, configured with Cisco Easy VPN, using SDM to support remote access VPNs
- Describe, configure, and verify the Cisco VPN Client on a Windows PC

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

Lesson 1

Understanding IPsec Components and IPsec VPN Features

Overview

This lesson describes the protocols and standards required to enable secure communication using IPsec. To successfully design and implement a virtual private network (VPN) deployment, you must understand IPsec basic functionality and the protocols used.

Objectives

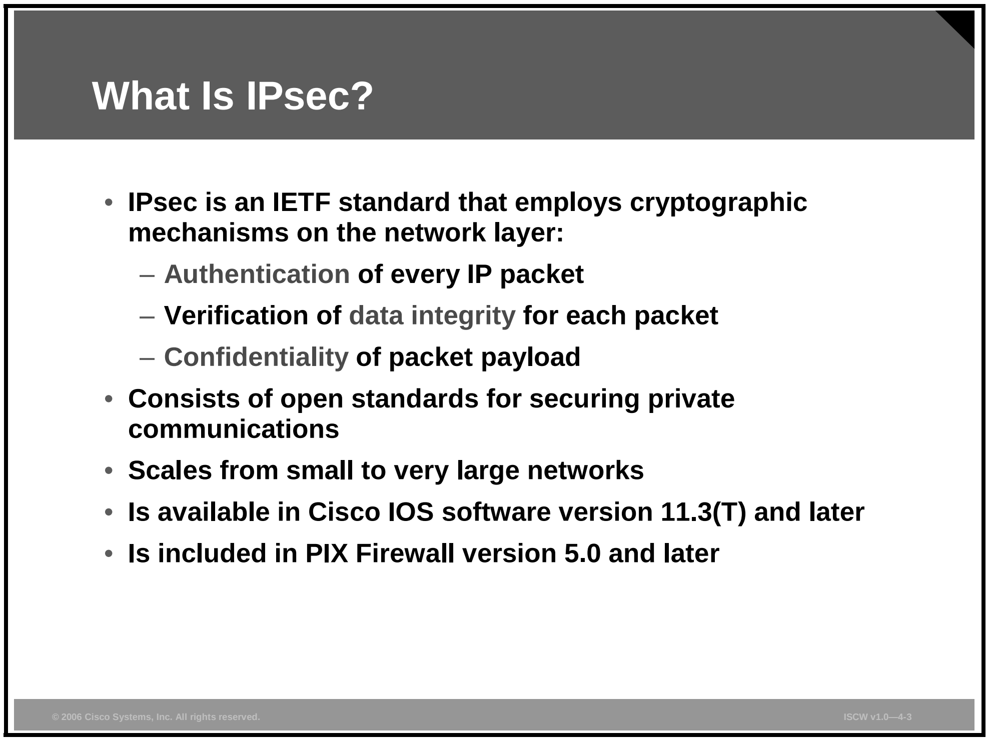
Upon completing this lesson, you will be able to describe the fundamental concepts, technologies, and terms used with IPsec VPNs. This ability includes being able to meet these objectives:

- Describe the IPsec protocol and its basic functions, and the advantages of IPsec VPNs versus other types of VPNs
- Explain the IKE protocols
- Describe IKE functionality
- Describe the two protocols that are used for IPsec
- Describe message authentication and integrity check
- Explain the differences and the functionality between symmetric and asymmetric encryption algorithms
- Describe the PKI

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

IPsec Overview

This topic describes the IPsec protocol and its basic functions, and the advantages of IPsec VPNs over other types of VPNs.



What Is IPsec?

- **IPsec is an IETF standard that employs cryptographic mechanisms on the network layer:**
  - **Authentication of every IP packet**
  - **Verification of data integrity for each packet**
  - **Confidentiality of packet payload**
- **Consists of open standards for securing private communications**
- **Scales from small to very large networks**
- **Is available in Cisco IOS software version 11.3(T) and later**
- **Is included in PIX Firewall version 5.0 and later**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-3

IPsec provides a mechanism for secure data transmission over IP networks, ensuring *confidentiality*, *integrity*, and *authenticity* of data communications over unprotected networks such as the Internet. IPsec encompasses a suite of protocols and is not bound to any specific encryption or authentication algorithms, key generation technique, or security association (SA). IPsec provides the rules while existing algorithms provide the encryption, authentication, key management, and so on.

Definition and Protocols

IPsec is a set of security protocols and algorithms used to secure data at the network layer. A companion security architecture specifies how IPsec secures data.

Following is a long and growing list of current RFCs that concern IPsec:

- RFC 1829: The ESP DES-CBC Transform
- RFC 1851: The ESP Triple DES Transform
- RFC 2085: HMAC-MD5 IP Authentication with Replay Prevention
- RFC 2207: RSVP Extensions for IPsec Data Flows
- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2402: IP Authentication Header
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2406: IP Encapsulating Security Payload (ESP)

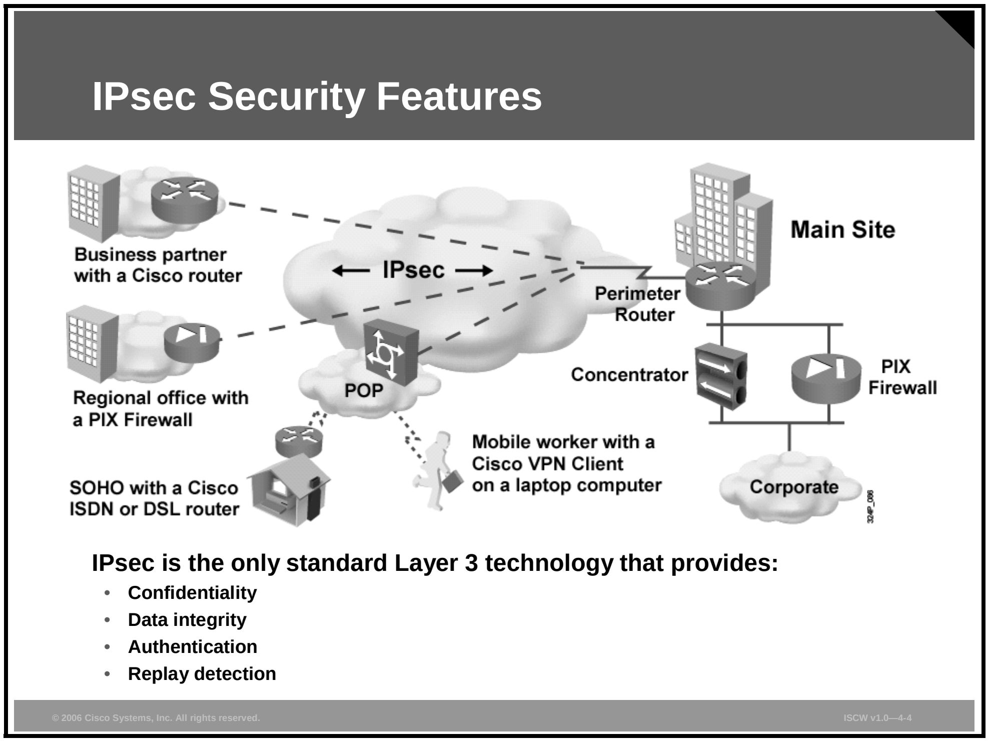
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 2539: Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
- RFC 2631: Diffie-Hellman Key Agreement Method
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 2875: Diffie-Hellman Proof-of-Possession Algorithms
- RFC 3070: Layer Two Tunneling Protocol (L2TP) over Frame Relay
- RFC 3104: RSIP Support for End-to-End IPsec
- RFC 3145: L2TP Disconnect Cause Information
- RFC 3193: Securing L2TP Using IPsec
- RFC 3301: Layer Two Tunneling Protocol (L2TP): ATM access network extensions

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

IPsec Security Features

IPsec acts at the network layer, protecting and authenticating IP packets between IPsec devices (peers), such as Cisco PIX Firewalls, Cisco routers, the Cisco Secure VPN Client, and other IPsec-compliant products.



IPsec Security Features

Business partner with a Cisco router
← IPsec →
Main Site
Perimeter Router
Regional office with a PIX Firewall
POP
Concentrator
PIX Firewall
SOHO with a Cisco ISDN or DSL router
Mobile worker with a Cisco VPN Client on a laptop computer
Corporate
324P_086

IPsec is the only standard Layer 3 technology that provides:

- **Confidentiality**
- **Data integrity**
- **Authentication**
- **Replay detection**

© 2006 Cisco Systems, Inc. All rights reserved.

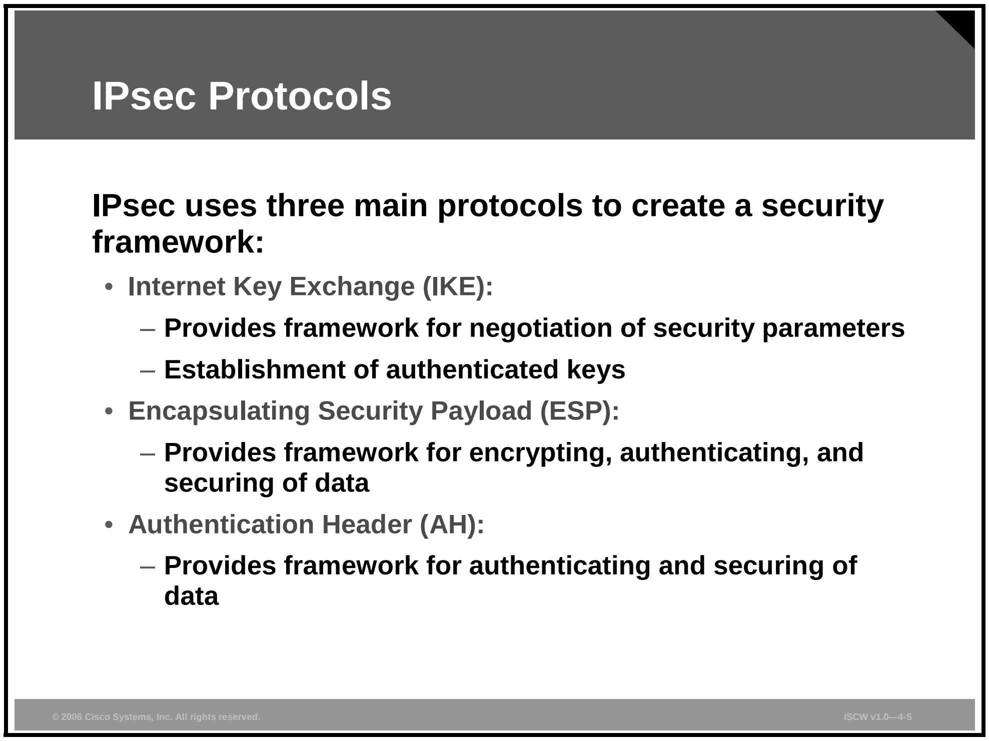
IPsec provides these features:

- **Data confidentiality:** The IPsec sender can encrypt packets before transmitting them across a network, thereby preventing anyone from eavesdropping on the communication. If intercepted, the communications cannot be read.
- **Data integrity:** The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that there has been no alteration to the data during transmission.
- **Data origin authentication:** The IPsec receiver can authenticate the source of the IPsec packets sent. This service is dependent upon the data integrity service.
- **Anti-replay:** Anti-replay protection verifies that each packet is unique, not duplicated. IPsec packets are protected by comparing the sequence number of the received packets and a sliding window on the destination host, or security gateway. A packet whose sequence number is before the sliding window is considered late, or a duplicate. Late and duplicate packets are dropped.

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

IPsec Protocols

The IPsec standard provides a method to manage authentication and data protection between multiple peers engaging in secure data transfer. IPsec includes a protocol for exchanging keys, called Internet Key Exchange (IKE) and two IPsec IP protocols, Encapsulating Security Payload (ESP) and Authentication Header (AH).



IPsec Protocols

IPsec uses three main protocols to create a security framework:

- Internet Key Exchange (IKE):
  - Provides framework for negotiation of security parameters
  - Establishment of authenticated keys
- Encapsulating Security Payload (ESP):
  - Provides framework for encrypting, authenticating, and securing of data
- Authentication Header (AH):
  - Provides framework for authenticating and securing of data

© 2006 Cisco Systems, Inc. All rights reserved.　ISCW v1.0—4-5

IPsec uses three main protocols to create a security framework:

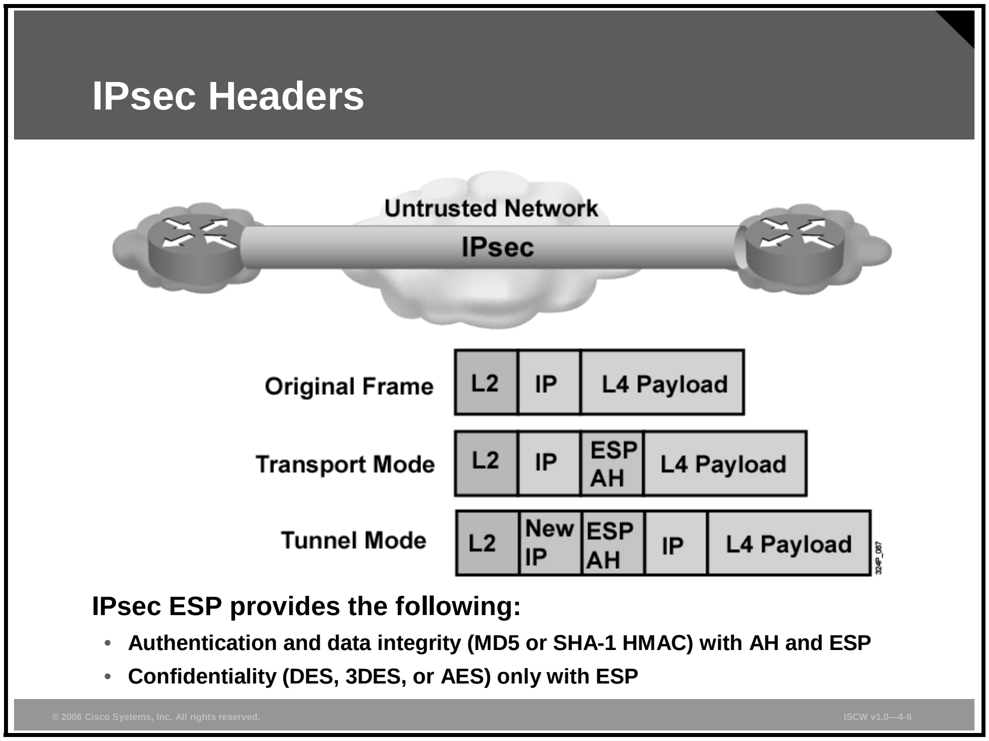
- **IKE:** Provides a framework for the negotiation of security parameters and establishes authenticated keys. IPsec uses symmetrical encryption algorithms for data protection, which are more efficient and easier to implement in hardware than other types of algorithms. These algorithms need a secure method of key exchange to ensure data protection. The IKE protocols provide the capability for secure key exchange.
- **ESP:** Provides a framework for encrypting, authenticating, and securing of data. ESP is a security protocol, which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected. The ESP protocol is mainly used in the IPsec.
- **AH:** Provides a framework for authenticating and securing of data. AH is a security protocol, which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram). The AH protocol is not very often used in IPsec because it has been replaced by ESP.

Note RFC 2401 defines the architecture for IPsec, including the framework and the services provided. RFC 2401 also defines how the services work together and how and where to use them. Other RFCs define individual protocols. Beyond these protocols are the implementation specifics, such as the exact encryption algorithm and the key length used for ESP.

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

IPsec Headers

IPsec provides authentication, integrity, and encryption via the insertion of one or both of two specific headers, AH or ESP, into the IP datagram.



IPsec Headers

Original Frame: L2 | IP | L4 Payload

Transport Mode: L2 | IP | ESP AH | L4 Payload

Tunnel Mode: L2 | New IP | ESP AH | IP | L4 Payload

IPsec ESP provides the following:

- **Authentication and data integrity (MD5 or SHA-1 HMAC) with AH and ESP**
- **Confidentiality (DES, 3DES, or AES) only with ESP**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-6

The AH provides authentication and integrity checks on the IP datagram. Authentication means the packet was definitely sent by the apparent sender. Integrity means the packet was not changed.

The ESP header provides information that indicates encryption of the datagram payload contents. The ESP header also provides authentication and integrity checks.

AH and ESP are used between two hosts. These hosts may be end stations or gateways.

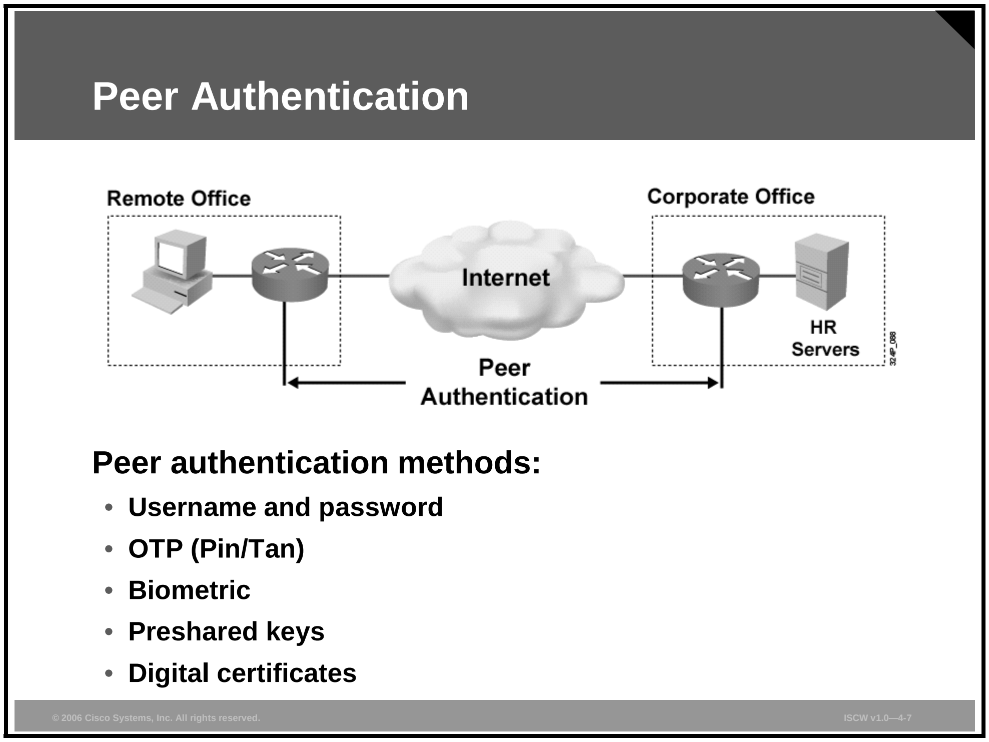
Note AH and ESP provide services to transport layer protocols such as TCP and User Datagram Protocol (UDP). AH and ESP are Internet protocols and are assigned numbers 51 (AH) and 50 (ESP) by the Internet Assigned Numbers Authority (IANA).

AH and ESP solutions require a standards-based way to secure data from eavesdropping and modification. IPsec has a choice of different encryptions (Data Encryption Standard [DES], Triple Data Encryption Standard [3DES], Advanced Encryption Standard [AES]) so that users may choose the strength of their data protection. IPsec also has several hash methods to choose from (Hash-based Message Authentication Code [HMAC], Message Digest 5 [MD5], Secure Hash Algorithm 1 [SHA-1]), each giving different levels of protection.

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

Peer Authentication

When conducting business long distance, you need to know who is at the other end of the phone, e-mail, or fax. The same is true of VPN networking. The device on the other end of the VPN tunnel must be authenticated before the communications path is considered secure.



Peer Authentication

Peer authentication methods:

- Username and password
- OTP (Pin/Tan)
- Biometric
- Preshared keys
- Digital certificates

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-7

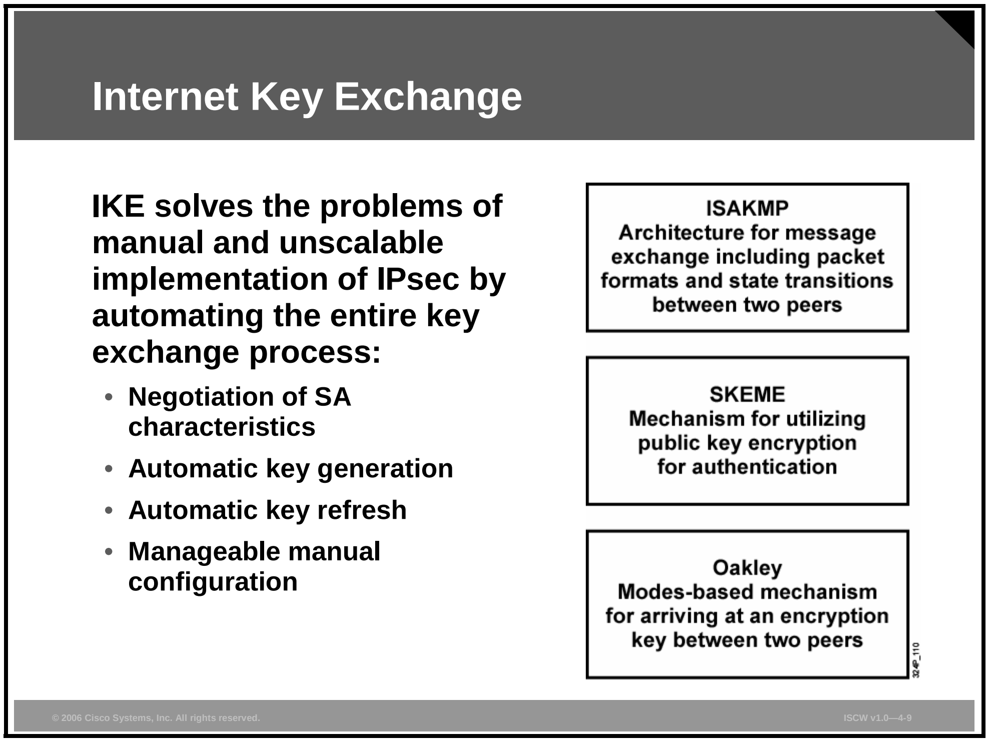
There are these authentication methods:

- **Username and password:** Uses the predefined usernames and passwords for different users or systems.
- **One Time Password (OTP) (Pin/Tan):** A stronger authentication method using passwords that are generated for each authentication.
- **Biometric:** Biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes.
- **Preshared keys:** A secret key value that is manually entered into each peer and used to authenticate the peer.
- **Digital certificates:** Use the exchange of digital certificates to authenticate the peers.

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

Internet Key Exchange

This topic describes the IKE protocols.



Internet Key Exchange

IKE solves the problems of manual and unscalable implementation of IPsec by automating the entire key exchange process:

- **Negotiation of SA characteristics**
- **Automatic key generation**
- **Automatic key refresh**
- **Manageable manual configuration**

ISAKMP
Architecture for message exchange including packet formats and state transitions between two peers

SKEME
Mechanism for utilizing public key encryption for authentication

Oakley
Modes-based mechanism for arriving at an encryption key between two peers

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-9

To implement a VPN solution with encryption, the periodic changing of encryption keys is necessary. Failure to change these keys makes the network susceptible to brute force attacks. IPsec solves this problem with the IKE protocol, which uses two other protocols to authenticate a peer and generate keys. The IKE protocol uses a mathematical routine called a Diffie-Hellman exchange to generate symmetrical keys to be used by two IPsec peers. IKE also manages the negotiation of other security parameters, such as data to be protected, strength of the keys, hash methods used, and whether packets are protected from replay. IKE uses UDP port 500.

IKE negotiates an SA, which is an agreement between two peers engaging in an IPsec exchange and consists of these required parameters necessary to establish successful communication:

- **Oakley:** A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm. You can find the standard in RFC 2412: *The OAKLEY Key Determination Protocol*.
- **ISAKMP:** A protocol framework that defines the mechanics of implementing a key exchange protocol and negotiation of a security policy. ISAKMP is defined in the standard in RFC 2408.
- **Skeme:** A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

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

IKE Features

IKE automatically negotiates IPsec SAs and enables IPsec secure communications without costly manual preconfiguration. (An SA is an agreement between two peers and consists of all required parameters necessary to establish successful communications)

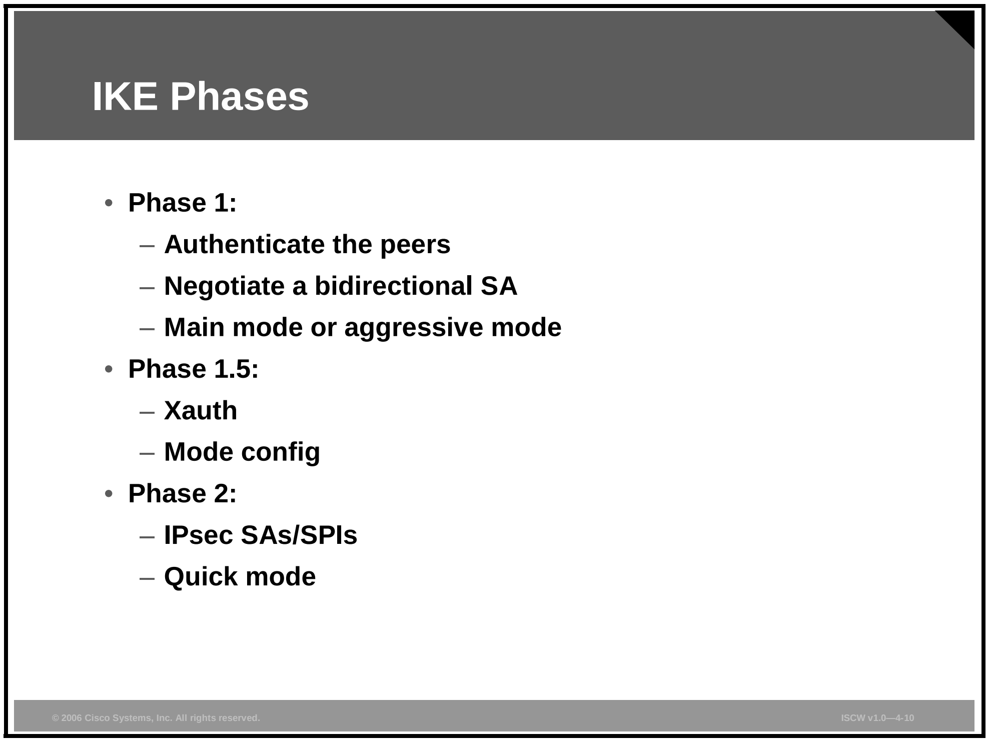
IKE includes these features:

- Eliminates the need to manually specify all of the IPsec security parameters at both peers
- Allows specification for a lifetime for the IPsec SA
- Allows encryption keys to change during IPsec sessions
- Allows IPsec to provide anti-replay services
- Permits certification authority (CA) support for a manageable, scalable IPsec implementation
- Allows dynamic authentication of peers

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

IKE Phases

IKE is executed in two phases to establish a secure communication channel between two peers.



IKE Phases

- **Phase 1:**
  - **Authenticate the peers**
  - **Negotiate a bidirectional SA**
  - **Main mode or aggressive mode**
- **Phase 1.5:**
  - **Xauth**
  - **Mode config**
- **Phase 2:**
  - **IPsec SAs/SPIs**
  - **Quick mode**

© 2006 Cisco Systems, Inc. All rights reserved.

IKE Phase 1

Phase 1 is the initial negotiation of SAs between two IPsec peers. Optionally, phase 1 can also include an authentication in which each peer is able to verify the identity of the other. This conversation between two IPsec peers can be subject to eavesdropping with no significant vulnerability of the keys being recovered. Phase 1 SAs are bidirectional; data may be sent and received using the same key material generated. Two modes are available for phase 1 SA negotiations: main mode or aggressive mode.

IKE Phase 1.5 (optional)

To further authenticate VPN participants (clients), you can use a protocol called Extended Authentication (Xauth), which provides user authentication of IPsec tunnels within the IKE protocol. Additionally, you can exchange other parameters between the peers. Mode configuration is used to deliver parameters such as IP address and DNS address to the client.

Phase 1.5 is optional.

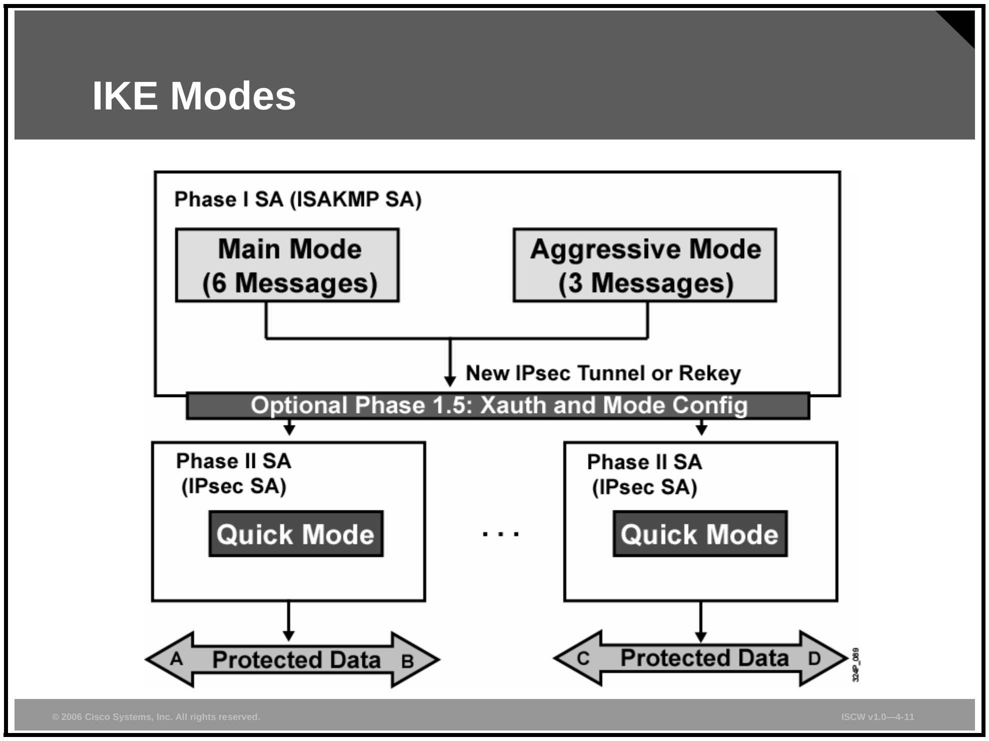
IKE Phase 2

Phase 2 SAs are negotiated by the IKE process (ISAKMP) on behalf of other services such as IPsec, which need key material for operation. Because the SAs used by IPsec are unidirectional, separate key exchanges are needed for data flowing in the forward direction and the reverse direction. The two peers have already agreed upon the transform sets, hash methods, and other parameters during the phase 1 negotiation. Quick mode is the method used for the phase 2 SA negotiations.

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

IKE Modes

IKE can use main mode, aggressive mode, or quick mode.



IKE Modes

Phase I SA (ISAKMP SA)

Main Mode (6 Messages)

Aggressive Mode (3 Messages)

New IPsec Tunnel or Rekey

Optional Phase 1.5: Xauth and Mode Config

Phase II SA (IPsec SA)

Quick Mode

. . .

Phase II SA (IPsec SA)

Quick Mode

A Protected Data B

C Protected Data D

324P_089

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-11

Main Mode

In the main mode, an IKE session begins with the initiator sending a proposal or proposals to the responder. These proposals define which encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced. Multiple proposals can be sent in one offering. The first exchange between nodes establishes the basic security policy. The responder chooses the appropriate proposal and sends it to the initiator. The next exchange passes Diffie-Hellman public keys and other data. All further negotiation is encrypted within the IKE SA. The third exchange authenticates the ISAKMP session. Once the IKE SA is established, IPsec negotiation (quick mode) begins.

Aggressive Mode

The aggressive mode squeezes the IKE SA negotiation into three packets, with all data required for the SA passed by the initiator. The responder sends the proposal, key material, and identification, and authenticates the session in the next packet. The initiator replies by authenticating the session. Negotiation is quicker, and the initiator and responder ID pass in plaintext.

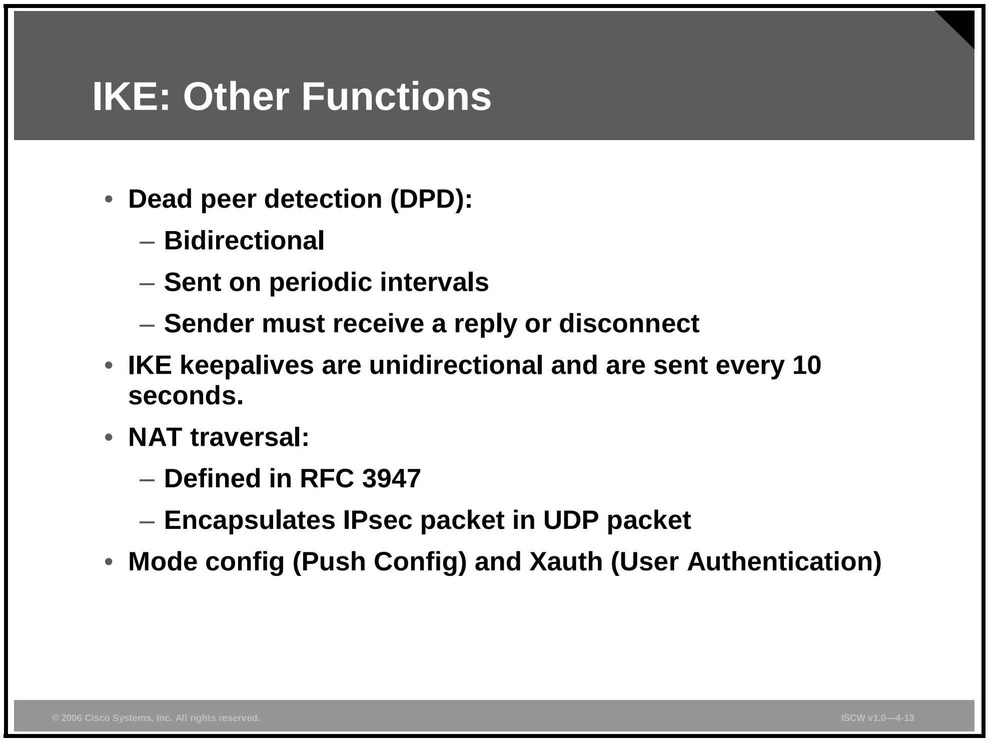
Quick Mode

The quick mode IPsec negotiation is similar to an aggressive mode IKE negotiation, except negotiation must be protected within an IKE SA. Quick mode negotiates the SA for the data encryption and manages the key exchange for that IPsec SA.

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

IKE: Other Functions

This topic describes additional functionality available within IKE.



IKE: Other Functions

- **Dead peer detection (DPD):**
  - **Bidirectional**
  - **Sent on periodic intervals**
  - **Sender must receive a reply or disconnect**
- **IKE keepalives are unidirectional and are sent every 10 seconds.**
- **NAT traversal:**
  - **Defined in RFC 3947**
  - **Encapsulates IPsec packet in UDP packet**
- **Mode config (Push Config) and Xauth (User Authentication)**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-13

There are some additional functions that can be delivered by IKE, which are used to verify if the peer device is still active, to pass IPsec through Network Address Translation (NAT) devices, or to exchange additional configuration parameters.

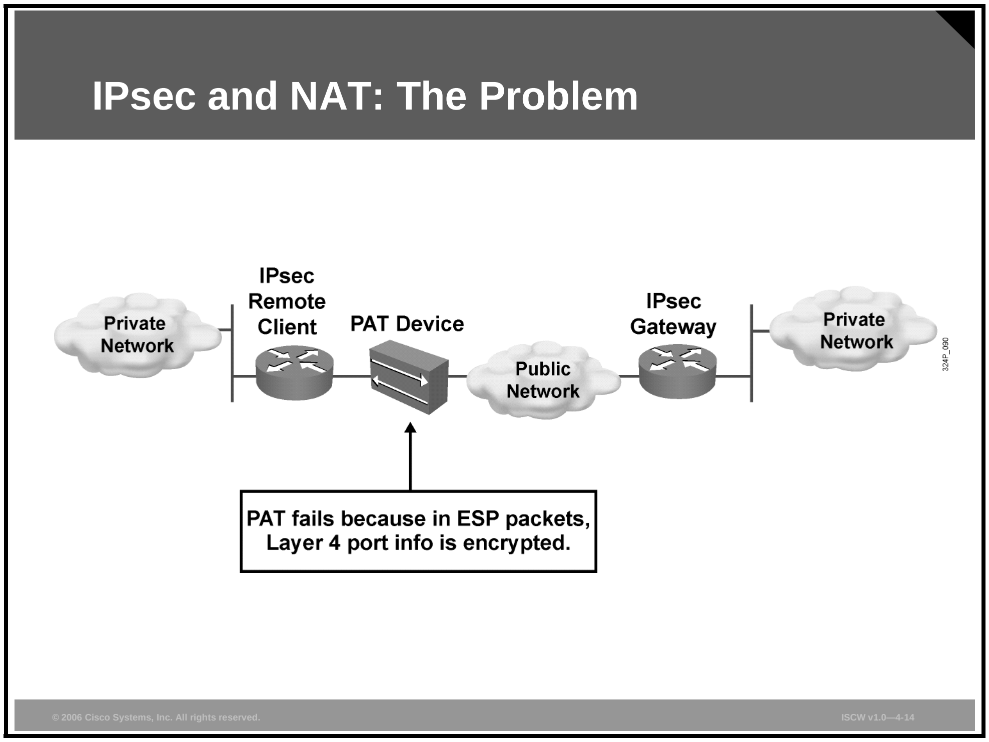
Dead peer detection (DPD) and Cisco IOS keepalives function on the basis of a timer. If the timer is set for 10 seconds, the router will send a “hello” message every 10 seconds (unless, of course, the router receives a “hello” message from the peer). The benefit of IOS keepalives and periodic DPD is earlier detection of dead peers. However, IOS keepalives and periodic DPD rely on periodic messages that have to be sent with considerable frequency. The result of sending frequent messages is that the communicating peers must encrypt and decrypt more packets.

Note	The default operation of DPD is on-demand. With on-demand DPD, messages are sent on the basis of traffic patterns. If a router has no traffic to send, it never sends a DPD message. If a peer is dead and the router never has any traffic to send to the peer, the router will not find out until the IKE or IPsec SA has to be rekeyed (the liveliness of the peer is unimportant if the router is not trying to communicate with the peer).

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

NAT Traversal

A standard IPsec VPN tunnel will not work if there are one or more NAT or Port Address Translation (PAT) points in the delivery path of the IPsec packet.



IPsec and NAT: The Problem

PAT fails because in ESP packets, Layer 4 port info is encrypted.

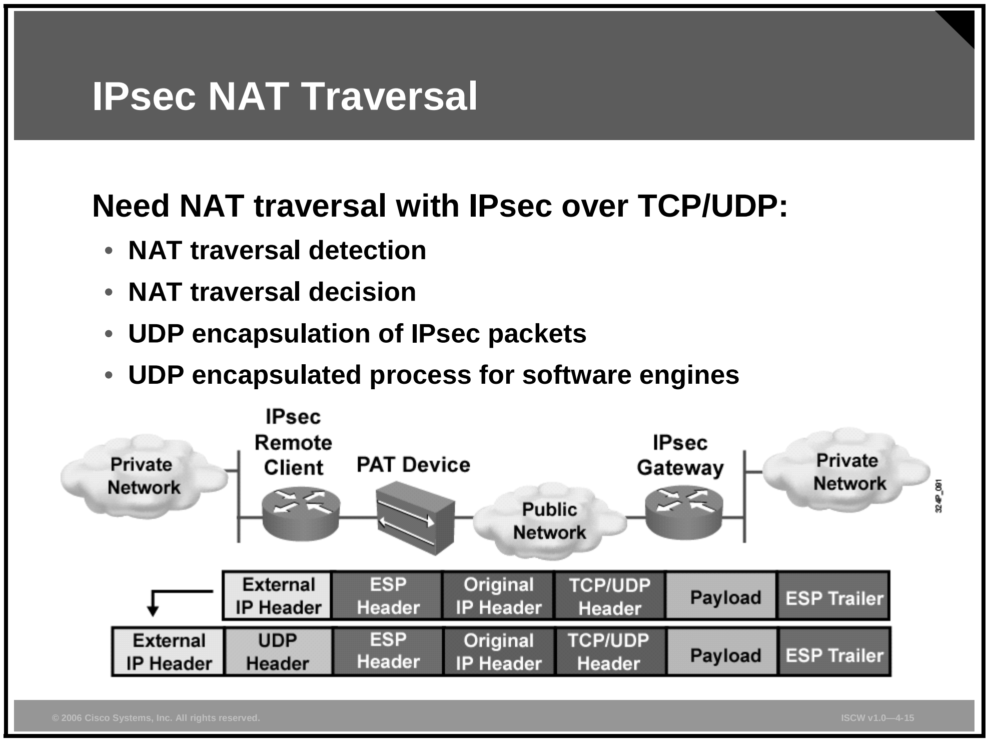
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-14

The IPsec VPN tunnel will not work if there are no port numbers in the IPsec headers that can be used to create and maintain translation tables. The Layer 4 port information is encrypted and therefore cannot be read.

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

IPsec NAT Traversal

The IPsec NAT traversal feature, which was introduced in Cisco IOS software Release 12.2(13)T, enables IPsec traffic to travel through NAT or PAT devices in the network by encapsulating IPsec packets in a UDP wrapper.



IPsec NAT Traversal

Need NAT traversal with IPsec over TCP/UDP:

- NAT traversal detection
- NAT traversal decision
- UDP encapsulation of IPsec packets
- UDP encapsulated process for software engines

External IP Header	ESP Header	Original IP Header	TCP/UDP Header	Payload	ESP Trailer

External IP Header	UDP Header	ESP Header	Original IP Header	TCP/UDP Header	Payload	ESP Trailer

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-15

NAT traversal is negotiated with these factors:

- NAT traversal detection
- NAT traversal decision
- UDP encapsulation of IPsec packets for NAT traversal
- UDP encapsulated process for software engines

NAT Traversal Detection

During IKE phase 1 negotiation, two types of NAT detection occur before IKE quick mode begins: NAT support and NAT existence along the network path. To detect NAT support, the vendor ID string is exchanged with the remote peer. The remote peer sends a vendor ID string payload to its peer to indicate that this version supports NAT traversal. Thereafter, NAT existence along the network path can be determined.

NAT traversal enables an IPsec device to find any NAT device between two IPsec peers. To detect whether a NAT device exists along the network path, the peers send a payload with hashes of the IP address and port of both the source and destination address from each end. The hashes are sent as a series of NAT discovery (NAT-D) payloads. If, upon receipt, both ends recalculate the hashes and the hashes match the payload hash, each peer knows that no NAT device exists on the network path between them. If the payload hash and recalculated hashes do not match (that is, someone translated the address or port), then each peer needs to perform NAT traversal to get the IPsec packet through 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 self-study.

NAT Traversal Decision

While IKE phase 1 detects NAT support and NAT existence along the network path, IKE phase 2 decides whether or not the peers at both ends will use NAT traversal. Quick mode SA payload is used for NAT traversal negotiation.

UDP Encapsulation of IPsec Packets

In addition to allowing IPsec packets to traverse across NAT devices, UDP encapsulation also addresses many incompatibility issues between IPsec, NAT, and PAT. The resolved issues are as follows:

- **Incompatibility between IPsec ESP and PAT:** If PAT found a legislative IP address and port, it would drop the ESP packet. To prevent an ESP packet drop, UDP encapsulation is used to hide the ESP packet behind the UDP header. Therefore, PAT treats the ESP packet as a UDP packet, processing the ESP packet as a normal UDP packet.
- **Incompatibility between checksums and NAT:** In the new UDP header, the checksum value is always zero. This value prevents an intermediate device from validating the checksum against the packet checksum, thereby resolving the checksum issue because NAT changes the IP source and destination addresses.
- **Incompatibility between fixed IKE destination ports and PAT:** PAT changes the port address in the new UDP header for translation and leaves the original payload unchanged.

UDP Encapsulated Process for Software Engines: Transport Mode and Tunnel Mode ESP Encapsulation

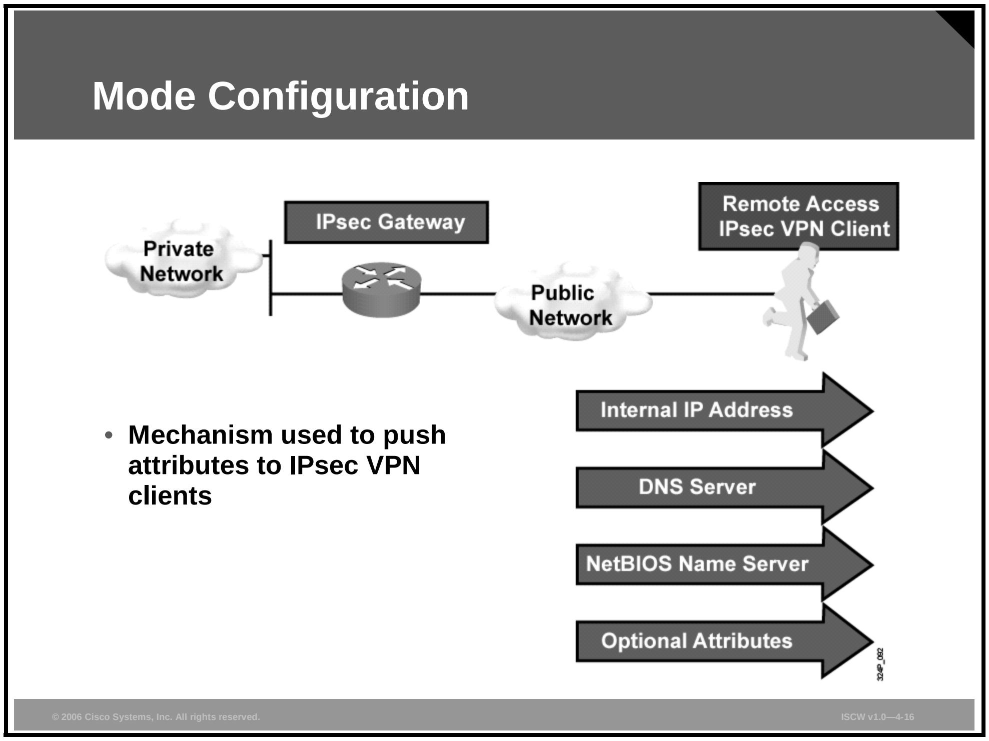
After the IPsec packet is encrypted by a hardware accelerator or a software crypto engine, a UDP header and a non-IKE marker (which is eight bytes in length) are inserted between the original IP header and ESP header. The total length, protocol, and checksum fields are changed to match this modification.

Note NAT keepalives can be used to keep the dynamic NAT mapping alive during a connection between two peers. NAT keepalives are UDP packets with an unencrypted payload of one byte. By default, there are no NAT keepalives sent.

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

Mode Configuration Option

Mode configuration is an option for pushing system parameters (for example, IP address and DNS attributes) to the peer, which is usually the client in a remote access VPN.



Mode Configuration

- **Mechanism used to push attributes to IPsec VPN clients**

© 2006 Cisco Systems, Inc. All rights reserved.

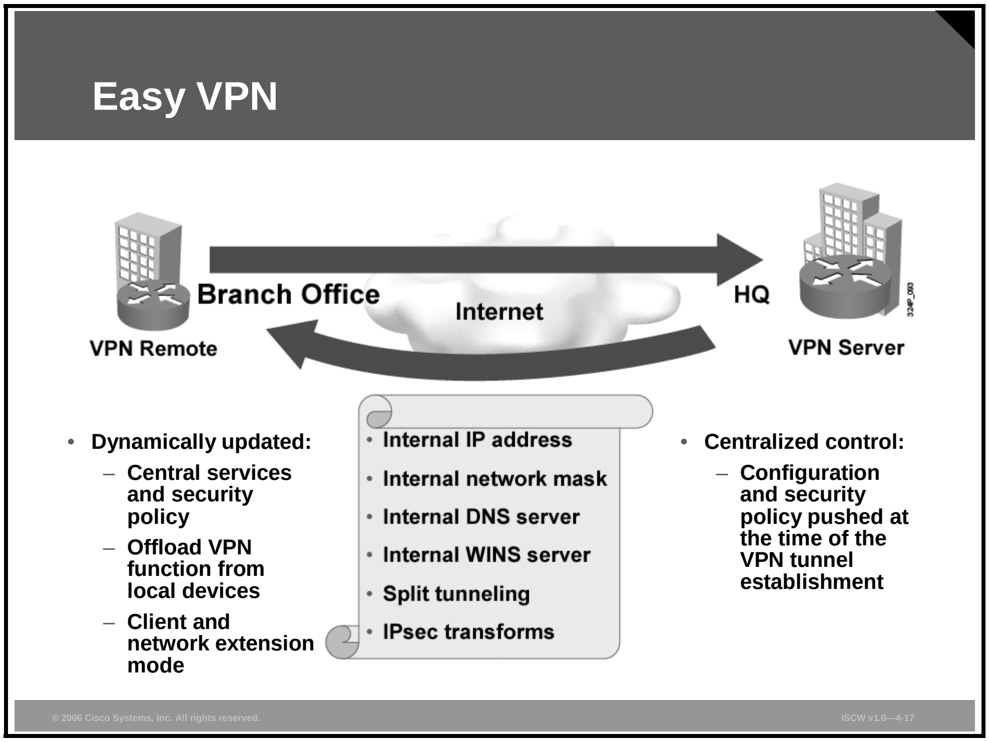
ISCW v1.0—4-16

The mode configuration option is heavily used for Easy VPN. Easy VPN allows remote clients to receive security policies from an Easy VPN Server, minimizing configuration requirements at the client.

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

Easy VPN

Cisco Easy VPN greatly simplifies VPN deployment for remote offices and teleworkers. The Cisco Easy VPN solution centralizes VPN management across all Cisco VPN devices, thus reducing the management complexity of VPN deployments.



Easy VPN

- Dynamically updated:
  - Central services and security policy
  - Offload VPN function from local devices
  - Client and network extension mode

- Internal IP address
- Internal network mask
- Internal DNS server
- Internal WINS server
- Split tunneling
- IPsec transforms

- Centralized control:
  - Configuration and security policy pushed at the time of the VPN tunnel establishment

© 2006 Cisco Systems, Inc. All rights reserved.

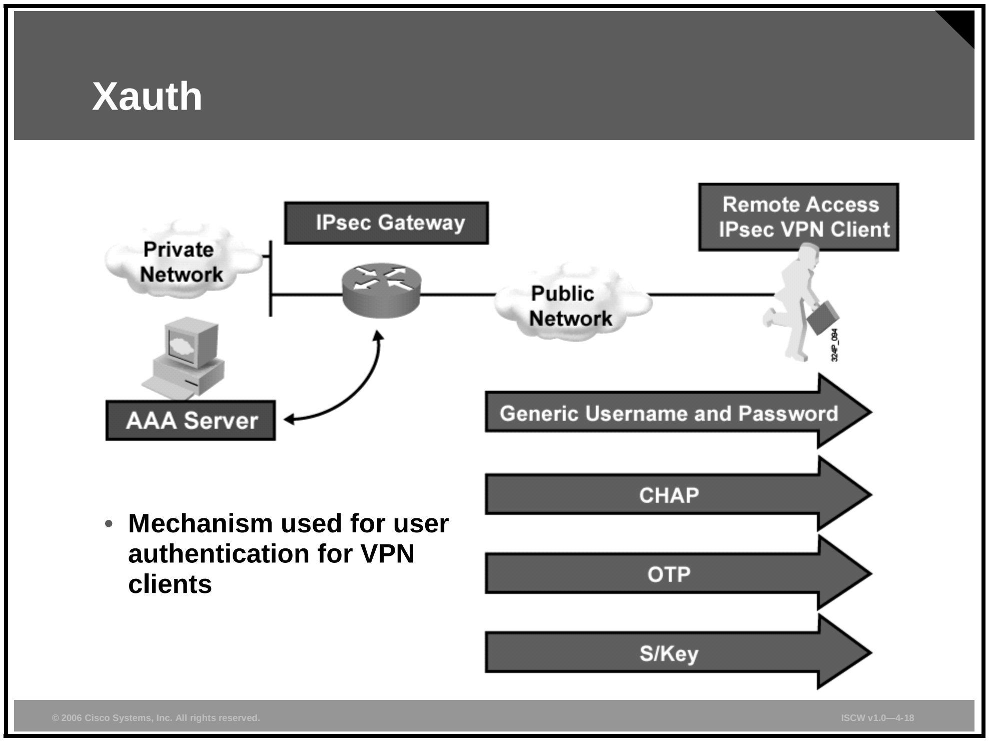
Cisco Easy VPN consists of these two components:

- **Cisco Easy VPN Remote:** The Cisco Easy VPN Remote component allows Cisco IOS routers, Cisco PIX Security Appliances, Cisco VPN 3002 hardware clients, and the Cisco VPN Client to receive security policies upon a VPN tunnel connection from a Cisco Easy VPN Server, minimizing configuration requirements at the remote location. This cost-effective solution is ideal for remote offices with little IT support or for large customer premises equipment (CPE) deployments where it is impractical to individually configure multiple remote devices. This feature makes VPN configuration as easy as entering a password, which minimizes local IT support, increases productivity, and lowers costs.
- **Cisco Easy VPN Server:** The Cisco Easy VPN Server allows Cisco IOS routers, Cisco PIX Security Appliances, and Cisco VPN 3000 Concentrators to act as VPN headend devices in site-to-site or remote-access VPNs, where the remote office devices are using the Cisco Easy VPN Remote feature. This feature pushes security policies defined at the central site to the remote VPN device, helping to ensure that those connections have up-to-date policies in place before the connection is established. Additionally, a device enabled with the Cisco Easy VPN Server can terminate VPN tunnels initiated by mobile remote workers running the Cisco VPN Client software on PCs. This flexibility allows mobile and remote workers to access critical data and applications on their corporate intranet.

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

Extended Authentication

Xauth is based on the IKE protocol. Xauth allows authentication, authorization, and accounting (AAA) methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange.



Xauth

- **Mechanism used for user authentication for VPN clients**

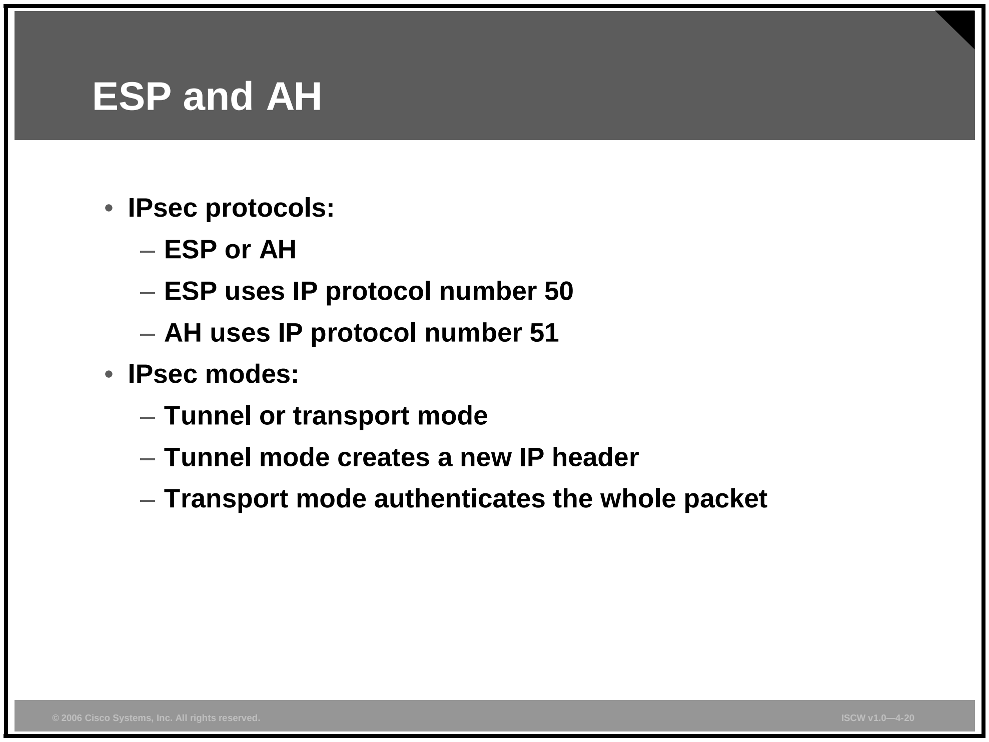
© 2006 Cisco Systems, Inc. All rights reserved.

Xauth does not replace IKE. IKE allows for device authentication while Xauth allows for user authentication, which occurs after IKE device authentication. A user authentication option can be a generic username and password, Challenge Handshake Authentication Protocol (CHAP), OTPs, or Secure Key (S/Key).

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

ESP and AH

This topic describes the two protocols used for IPsec and IPsec modes.



ESP and AH

- **IPsec protocols:**
  - **ESP or AH**
  - **ESP uses IP protocol number 50**
  - **AH uses IP protocol number 51**
- **IPsec modes:**
  - **Tunnel or transport mode**
  - **Tunnel mode creates a new IP header**
  - **Transport mode authenticates the whole packet**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-20

These two IP protocols are used in the IPsec standard:

- **ESP:** The ESP header (IP protocol 50) forms the core of the IPsec protocol. This protocol, in conjunction with an agreed-upon encryption method or transform set, protects data by rendering it undecipherable. This protocol protects only the data portion of the packet. It can optionally also provide for authentication of the protected data.
- **AH:** The other part of IPsec is formed by the AH protocol (IP protocol 51). The AH does not protect data in the usual sense by hiding the data, but it adds a tamper-evident seal to the data. It also protects fields in the IP header carrying the data, including the address fields of the IP header. The AH protocol should not be used alone when there is a requirement for data confidentiality.

IPsec has two methods of forwarding data across a network: tunnel mode and transport mode, which differ in their application as well as in the amount of overhead added to the passenger packet, as follows:

- **Tunnel mode:** Tunnel mode works by encapsulating and protecting an entire IP packet. Because tunnel mode encapsulates or hides the IP header of the packet, a new IP header must be added for the packet to be successfully forwarded. The encrypting devices themselves own the IP addresses used in this new header. These addresses can be specified in the configuration in Cisco IOS routers. Tunnel mode may be employed with either ESP or AH or both. Tunnel mode results in an additional packet expansion of approximately 20 bytes because of the new IP header.

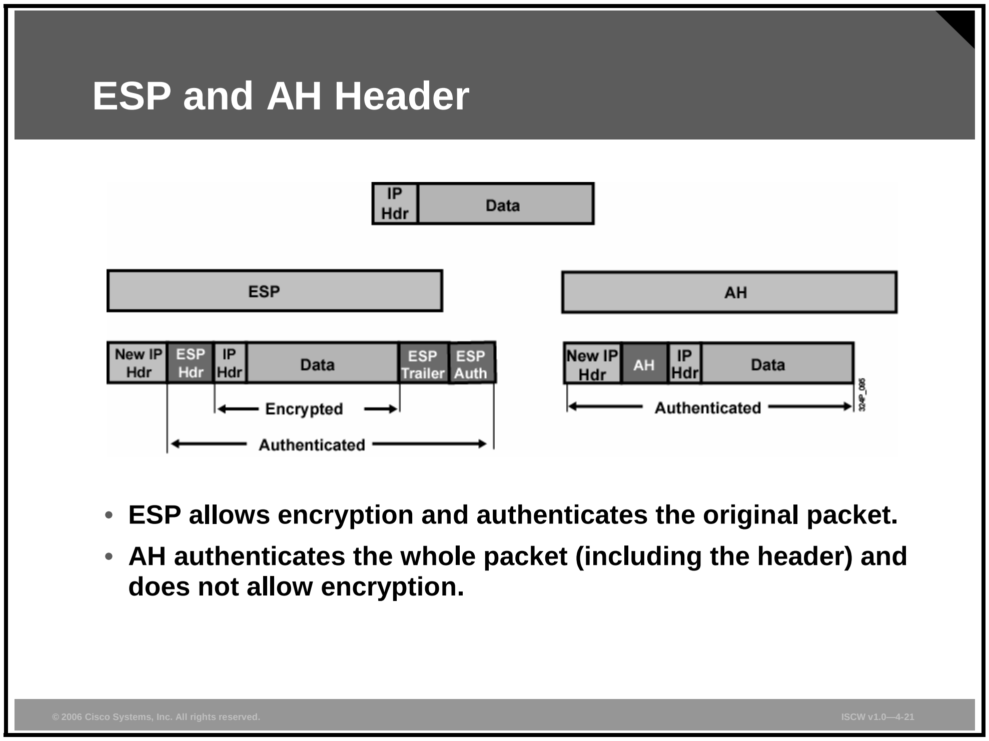
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

- **Transport mode:** Because packet expansion can be a concern during the forwarding of small packets, a second forwarding method is also possible. IPsec transport mode works by inserting the ESP header between the IP header and the next protocol or the Transport layer of the packet. Both IP addresses of the two network nodes whose traffic is being protected by IPsec are visible. This mode of IPsec can sometimes be susceptible to traffic analysis. However, because there is no additional IP header added, the result is less packet expansion. Transport mode can be deployed with either ESP or AH or both. This mode works well with Generic Routing Encapsulation (GRE) because GRE already hides the addresses of the end stations by adding its own IP header.

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

ESP and AH Header

This section describes the ESP and AH headers.



ESP and AH Header

- **ESP allows encryption and authenticates the original packet.**
- **AH authenticates the whole packet (including the header) and does not allow encryption.**

© 2006 Cisco Systems, Inc. All rights reserved.

You can achieve AH authentication by applying a keyed one-way hash function to the packet, creating a hash or message digest. The hash is combined with the text and transmitted. Changes in any part of the packet that occur during transit are detected by the receiver when it performs the same one-way hash function on the received packet and compares the value of the message digest that the sender has supplied. The fact that the one-way hash also involves the use of a symmetric key between the two systems means that authenticity is guaranteed.

ESP provides confidentiality by encrypting the payload. The default algorithm for IPsec is 56-bit DES. Cisco products also support the use of 3DES for stronger encryption.

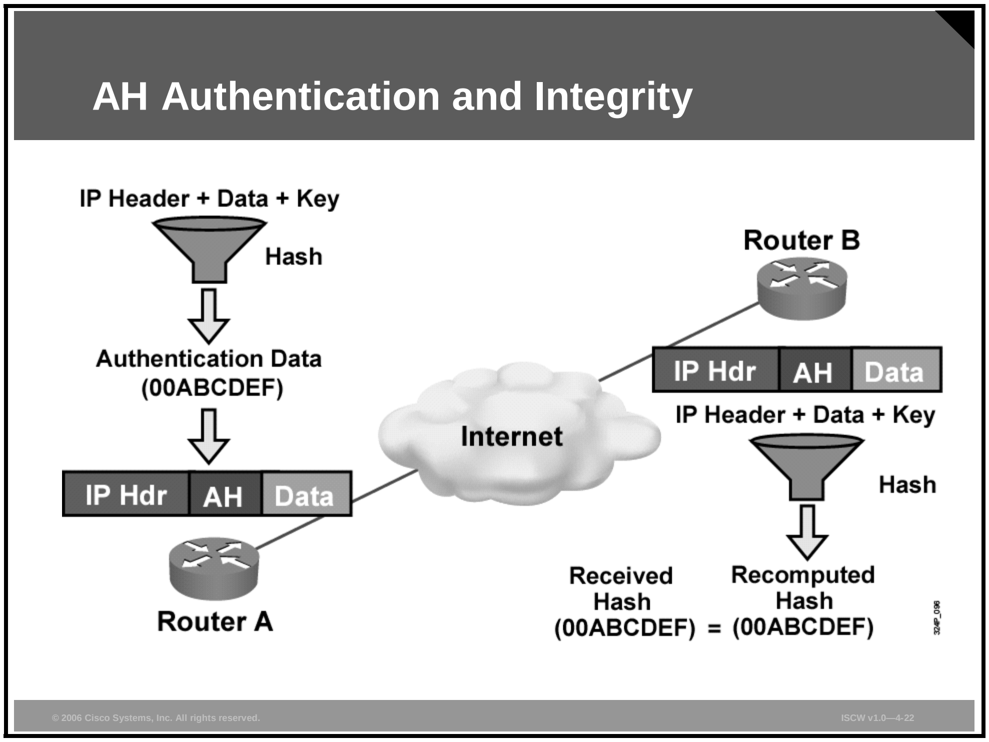
You can use ESP alone or in combination with AH. ESP with AH also provides integrity and authentication of the datagrams. First, the payload is encrypted. Next, the encrypted payload is sent through a hash algorithm: MD5 or SHA-1. The hash provides origin authentication and data integrity for the data payload.

Alternatively, ESP may also enforce anti-replay protection by requiring that a receiving host set the replay bit in the header to indicate that the packet has been seen.

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

AH Authentication and Integrity

The AH function is applied to the entire datagram, except for any mutable IP header fields that change in transit, such as Time to Live [TTL] fields that are modified by the routers along the transmission path.



AH Authentication and Integrity

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-22

AH works as follows:

Step 1 The IP header and data payload is hashed.

Step 2 The hash is used to build an AH header, which is appended to the original packet.

Step 3 The new packet is transmitted to the IPsec peer router.

Step 4 The peer router hashes the IP header and data payload.

Step 5 The peer router extracts the transmitted hash from the AH header.

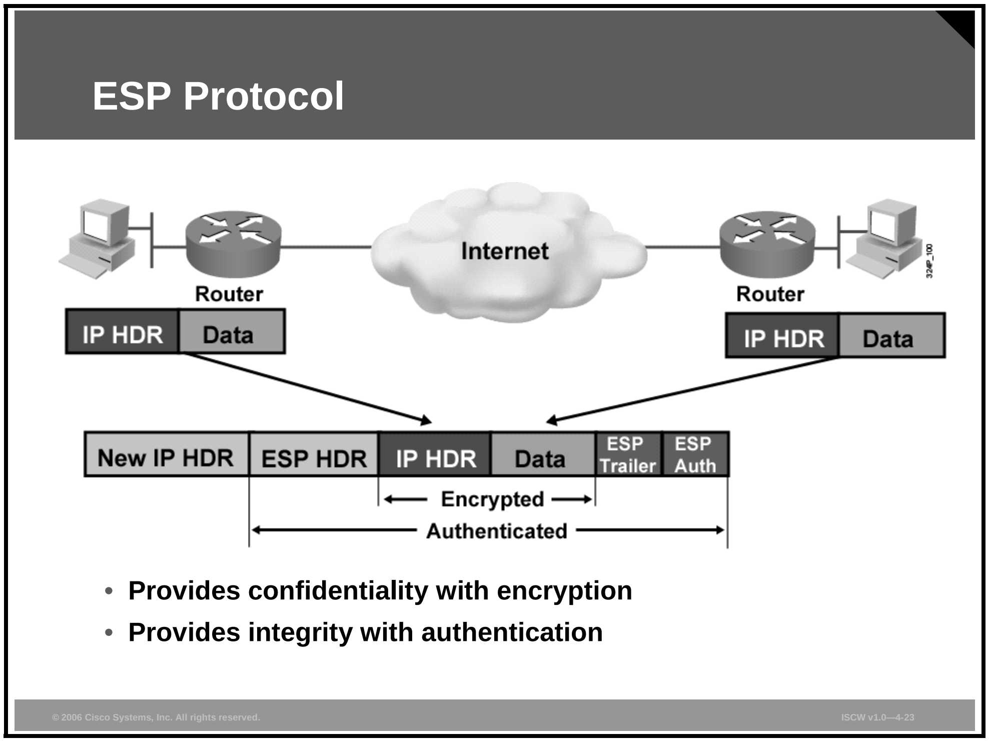
Step 6 The peer router compares the two hashes. The hashes must exactly match. Even if one bit is changed in the transmitted packet, the hash output on the received packet will change and the AH header will not match.

AH supports MD5 and SHA-1 algorithms.

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

ESP Protocol

Between two security gateways, the original payload is well protected because the entire original IP datagram is encrypted. An ESP header and trailer are added to the encrypted payload. With ESP authentication, the encrypted IP datagram and the ESP header or trailer are included in the hashing process. Lastly, a new IP header is appended to the front of the authenticated payload. The new IP address is used to route the packet through the Internet.



ESP Protocol

- Provides confidentiality with encryption
- Provides integrity with authentication

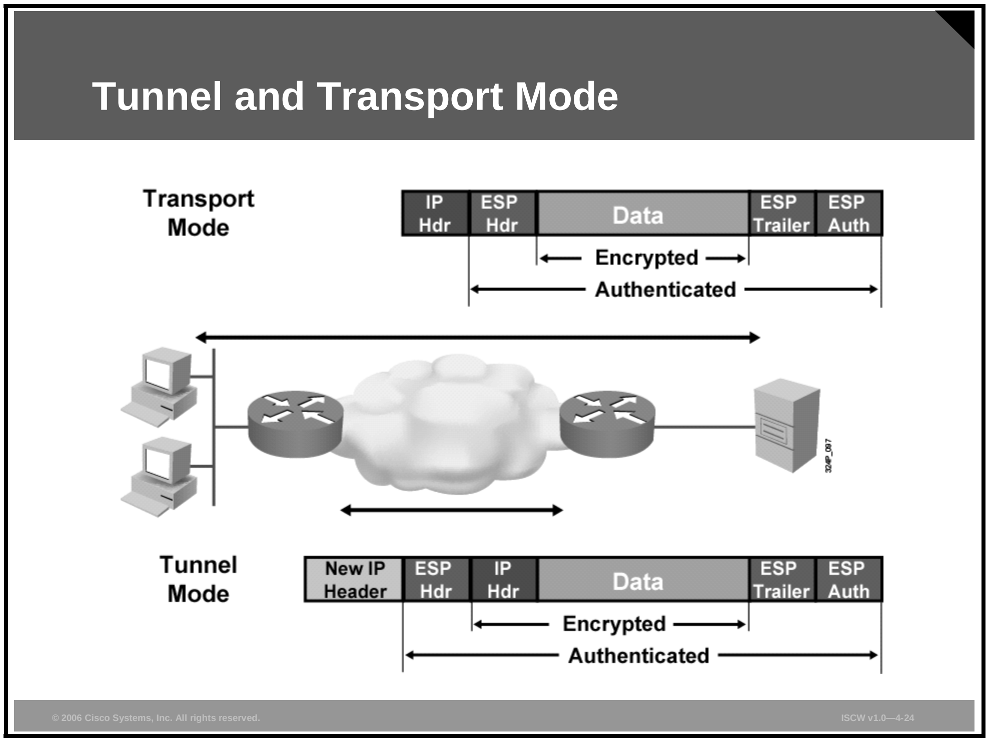
© 2006 Cisco Systems, Inc. All rights reserved.

When both ESP authentication and encryption are selected, encryption is performed first before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can authenticate inbound packets. By doing this, it can detect the problems and potentially reduce the impact of denial of service (DoS) 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 self-study.

Tunnel and Transport Mode

This section describes the tunnel and transport mode.



Tunnel and Transport Mode

Transport Mode

IP Hdr | ESP Hdr | Data | ESP Trailer | ESP Auth

Encrypted

Authenticated

Tunnel Mode

New IP Header | ESP Hdr | IP Hdr | Data | ESP Trailer | ESP Auth

Encrypted

Authenticated

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-24

Transport mode protects the payload of the packet, higher layer protocols, but leaves the original IP address in the clear. The original IP address is used to route the packet through the Internet. ESP transport mode is used between two hosts. Transport mode provides security to the higher layer protocols only.

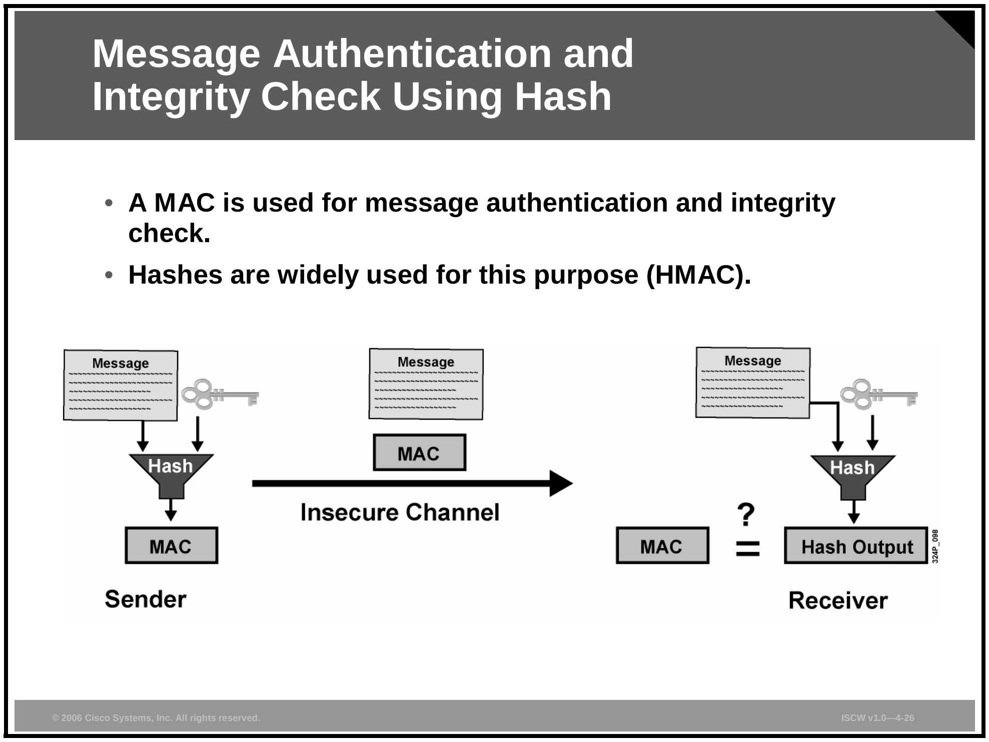
ESP tunnel mode is used between a host and a security gateway or between two security gateways. For gateway-to-gateway applications, rather than load IPsec on all the computers at the remote and corporate offices, it is easier to have the security gateways perform the IP-in-IP encryption and encapsulation.

In the IPsec remote access application, ESP tunnel mode is used. At a home office, there may be no router to perform the IPsec encapsulation and encryption. In the example in the figure, the IPsec client running on the PC performs the IPsec IP-in-IP encapsulation and encryption. At the corporate office, the router de-encapsulates and decrypts the packet.

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

Message Authentication and Integrity Check

This topic describes message authentication and integrity check.



Message Authentication and Integrity Check Using Hash

- **A MAC is used for message authentication and integrity check.**
- **Hashes are widely used for this purpose (HMAC).**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-26

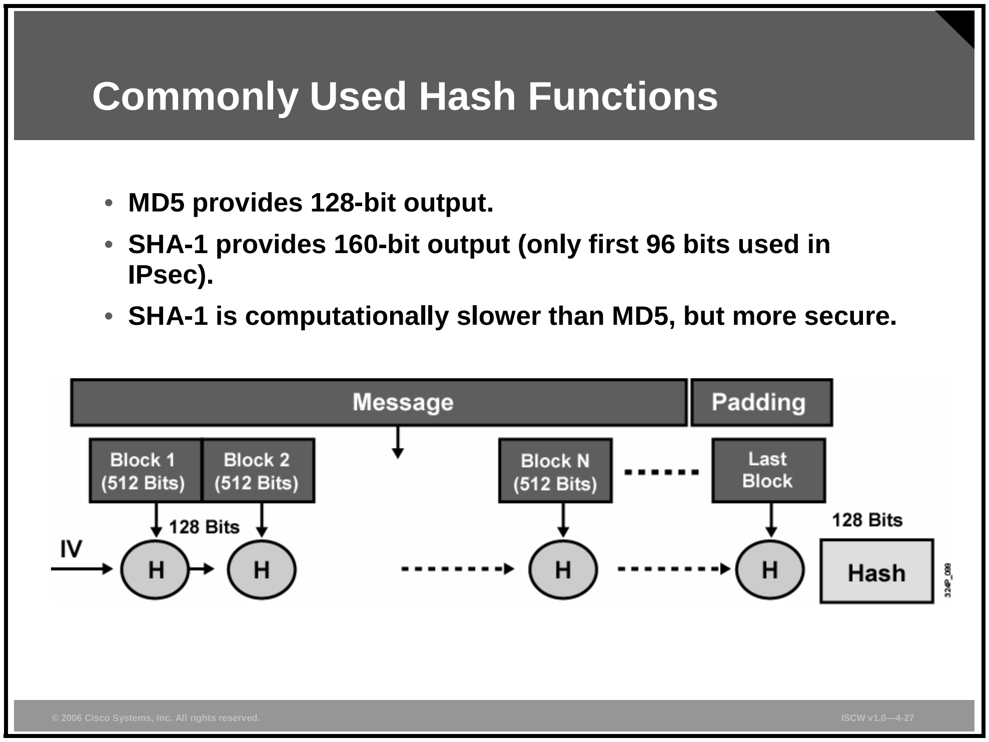
VPN data is transported over the public Internet. Potentially, this data could be intercepted and modified. To guard against this, each message has a hash attached to the message. A hash guarantees the integrity of the original message. If the transmitted hash matches the received hash, the message has not been tampered with. However, if there is no match, the message was altered.

The HMAC is used for message authentication and integrity check. HMAC can be used with any iterative cryptographic hash function, for example, MD5 or SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. HMAC also uses a secret key for calculation and verification of the message authentication values. MD5 and SHA-1 are examples of such hash 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 self-study.

Commonly Used Hash Functions

There are two hash functions for IPsec: MD5 and SHA-1. MD5 is well known from various uses in Cisco components, such as hashing passwords in the Cisco IOS. Both hash functions take some variable length input message and create a fixed-length hash.



Commonly Used Hash Functions

- MD5 provides 128-bit output.
- SHA-1 provides 160-bit output (only first 96 bits used in IPsec).
- SHA-1 is computationally slower than MD5, but more secure.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-27

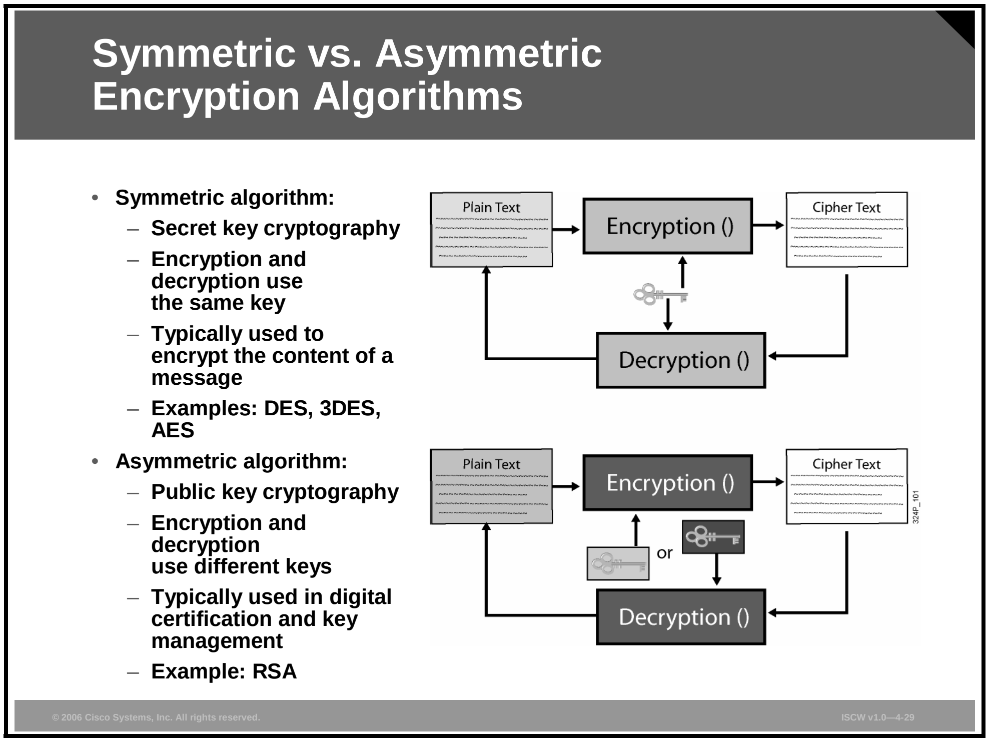
MD5 creates a 128-bit hash, while SHA-1 creates a 160-bit hash. In the case of SHA-1, only 96 bits of this hash are used for IPsec.

The initialization vector (IV) is used as an initial value to start creating a hash.

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

Symmetric and Asymmetric Encryption Algorithms

This topic describes symmetric and asymmetric encryption algorithms.



Symmetric vs. Asymmetric Encryption Algorithms

- Symmetric algorithm:
  - Secret key cryptography
  - Encryption and decryption use the same key
  - Typically used to encrypt the content of a message
  - Examples: DES, 3DES, AES
- Asymmetric algorithm:
  - Public key cryptography
  - Encryption and decryption use different keys
  - Typically used in digital certification and key management
  - Example: RSA

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-29

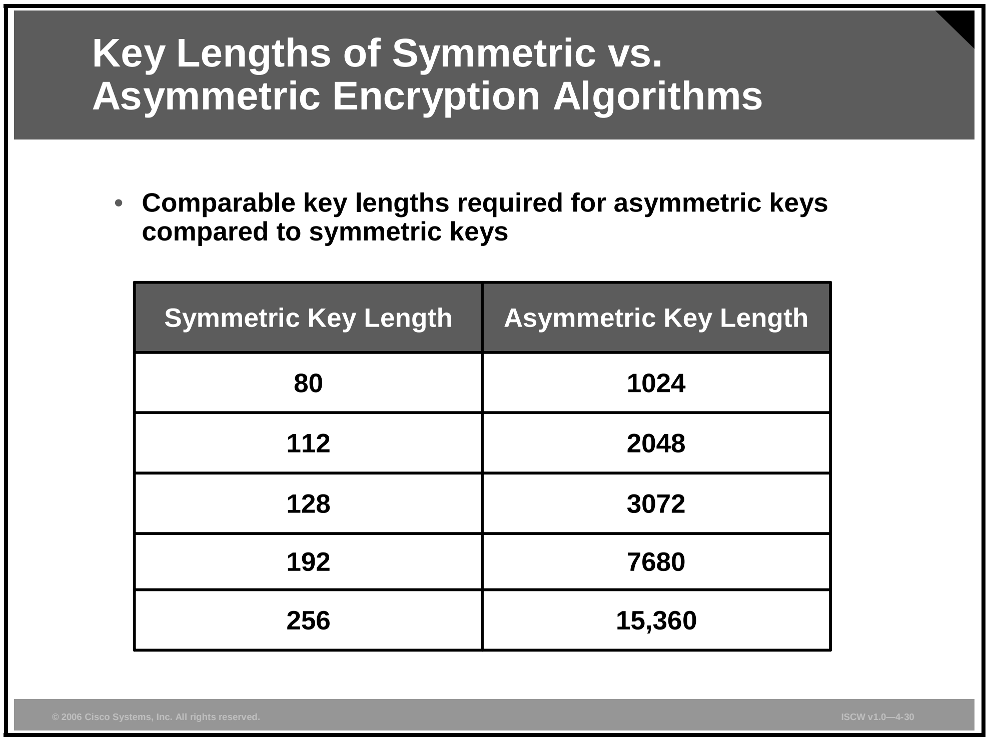
The purpose of encryption is to make data unreadable for everyone except those specified. A mathematical function is applied to the plain text and converts it to an encrypted cipher. These two types of mathematical functions are used:

- **Symmetric Encryption:** Symmetric encryption was the only option prior to 1976, when asymmetric encryption was introduced. With symmetric encryption, the sender and the receiver use the same secret key to encrypt and decrypt the message. This secret key is exchanged between the peers in a secret manner and must stay secret.
- **Asymmetric Encryption:** In 1976, a new idea was introduced into the field of cryptography. This idea allows the use of different keys for encryption and decryption. Even knowing one of the keys will not allow a hacker to deduce the second key. One key is used to encrypt the message, while the other key is used to decrypt the message. It is not possible to encrypt and decrypt with the same key.

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

Key Lengths of Symmetric and Asymmetric Encryption Algorithms

The table shows how symmetric key lengths can be compared to asymmetric key lengths.



Key Lengths of Symmetric vs. Asymmetric Encryption Algorithms

- **Comparable key lengths required for asymmetric keys compared to symmetric keys**

Symmetric Key Length	Asymmetric Key Length
80	1024
112	2048
128	3072
192	7680
256	15,360

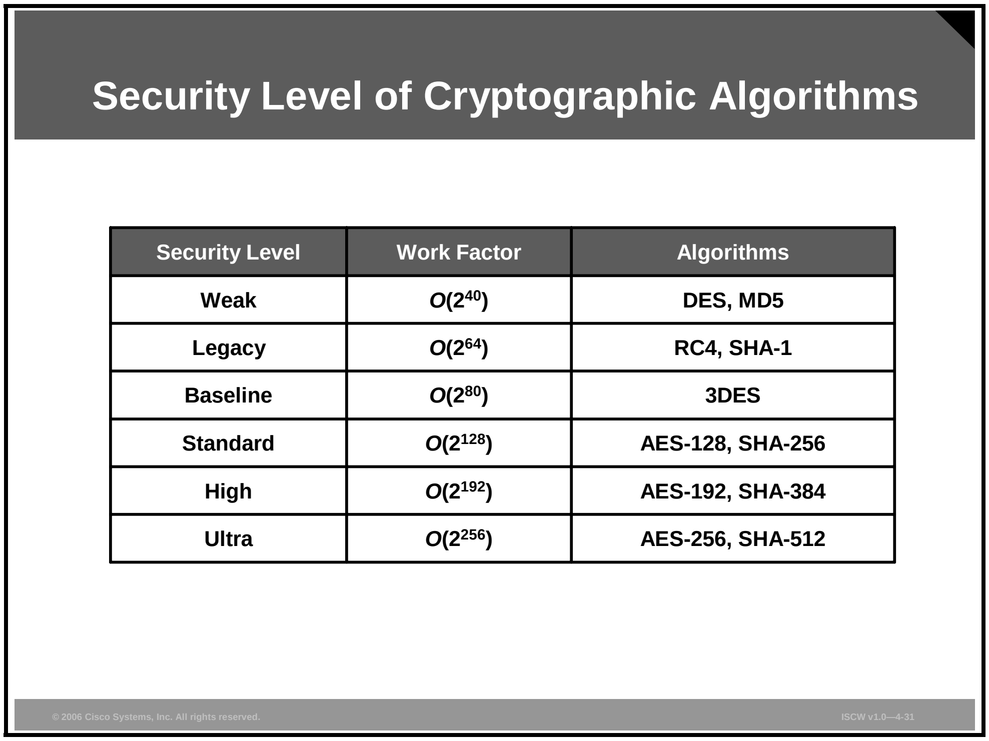
© 2006 Cisco Systems, Inc. All rights reserved.

A symmetric algorithm using a 256-bit key is comparable to an asymmetric algorithm using a 15,360-bit key. The longer the key, the more processing power 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 self-study.

Security Level of Cryptographic Algorithms

The table shows the differences in security levels between various algorithms.



Security Level of Cryptographic Algorithms

Security Level	Work Factor	Algorithms
Weak	***O*(2⁴⁰)**	**DES, MD5**
Legacy	***O*(2⁶⁴)**	**RC4, SHA-1**
Baseline	***O*(2⁸⁰)**	**3DES**
Standard	***O*(2¹²⁸)**	**AES-128, SHA-256**
High	***O*(2¹⁹²)**	**AES-192, SHA-384**
Ultra	***O*(2²⁵⁶)**	**AES-256, SHA-512**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-31

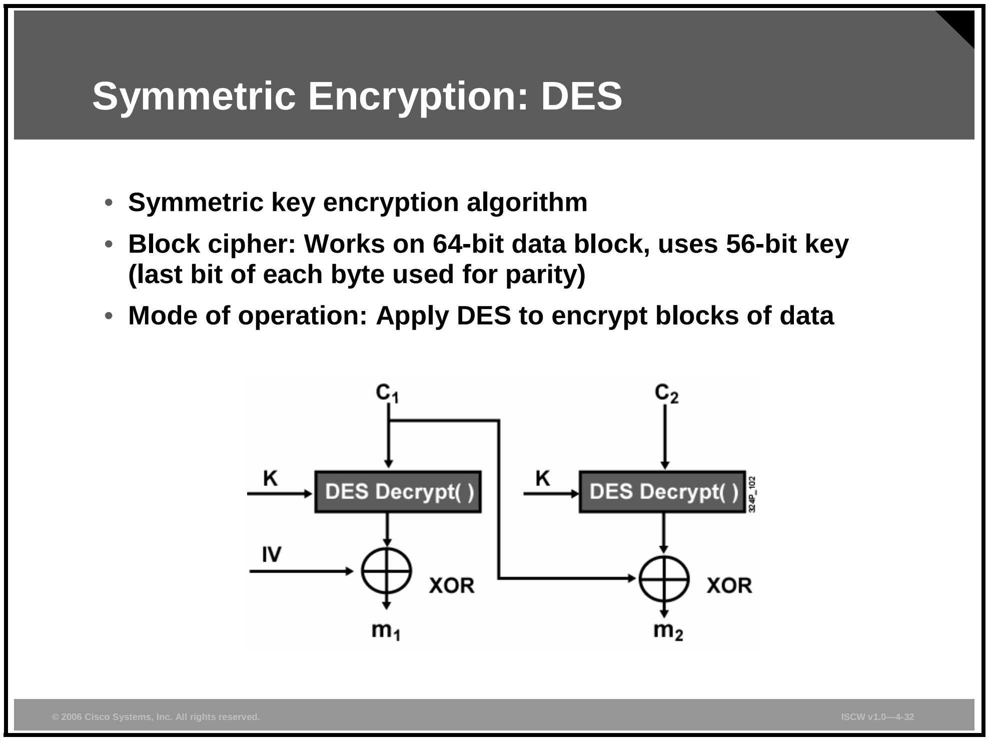
The algorithms listed in the table are all symmetric encryption algorithms. Work factor (O) represents the strength of the algorithm. In addition to these encryption algorithms, there are other encryption algorithms available, such as the following:

- **SEAL:** A stream cipher developed by Phillip Rogaway and Don Coppersmith. Version 3 was published in September 1997. SEAL is patented in the United States by IBM.
- **Skipjack:** A block cipher developed by the National Security Agency (NSA) and published in June 1998.

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

Symmetric Encryption: DES

The DES is a cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. The algorithm was initially controversial, with classified design elements and a relatively short key length. DES consequently came under intense academic scrutiny, and motivated the modern understanding of block ciphers and their cryptanalysis.



Symmetric Encryption: DES

- **Symmetric key encryption algorithm**
- **Block cipher: Works on 64-bit data block, uses 56-bit key (last bit of each byte used for parity)**
- **Mode of operation: Apply DES to encrypt blocks of data**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-32

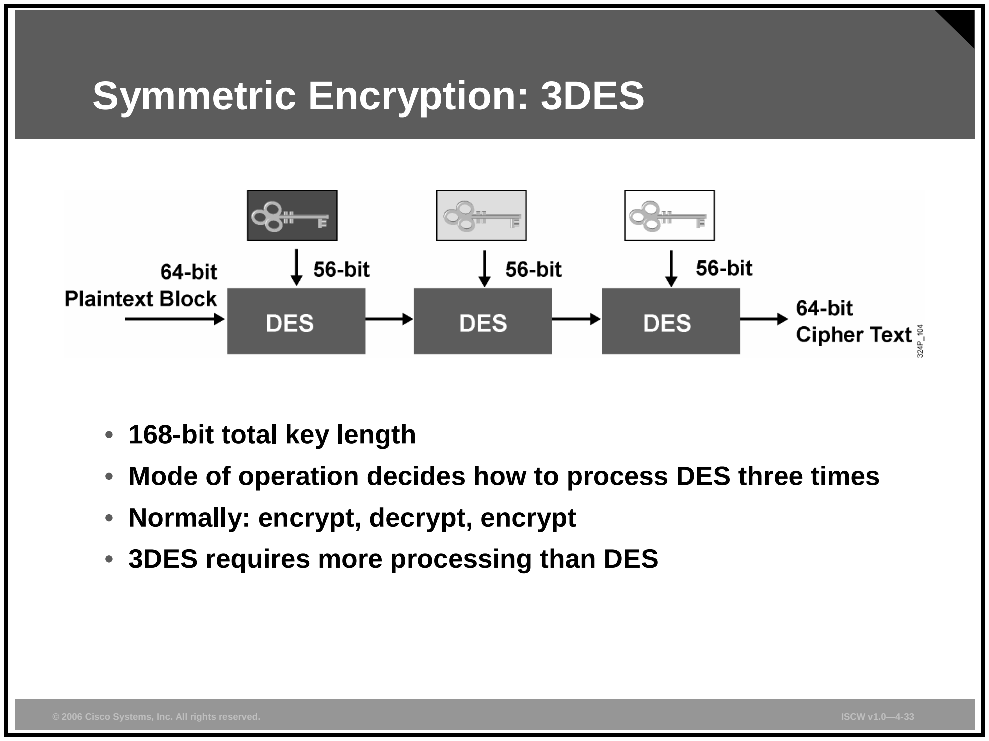
DES is now considered to be insecure for many applications, mainly due to the 56-bit key size being too small. DES keys have been broken in less than 24 hours. There are also some analytical results that demonstrate theoretical weaknesses in the cipher. The algorithm is believed to be secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the AES.

In some documentation, DES is referred to as the Data Encryption Algorithm (DEA).

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

Symmetric Encryption: 3DES

Triple DES (also 3DES or DESede) is a block cipher formed from the DES cipher. It was developed by Walter Tuchman (the leader of the DES development team at IBM) in 1978 and is specified in FIPS Pub 46-3. There are several ways to use DES three times; not all are 3DES and not all are as secure.



Symmetric Encryption: 3DES

- 168-bit total key length
- Mode of operation decides how to process DES three times
- Normally: encrypt, decrypt, encrypt
- 3DES requires more processing than DES

© 2006 Cisco Systems, Inc. All rights reserved.

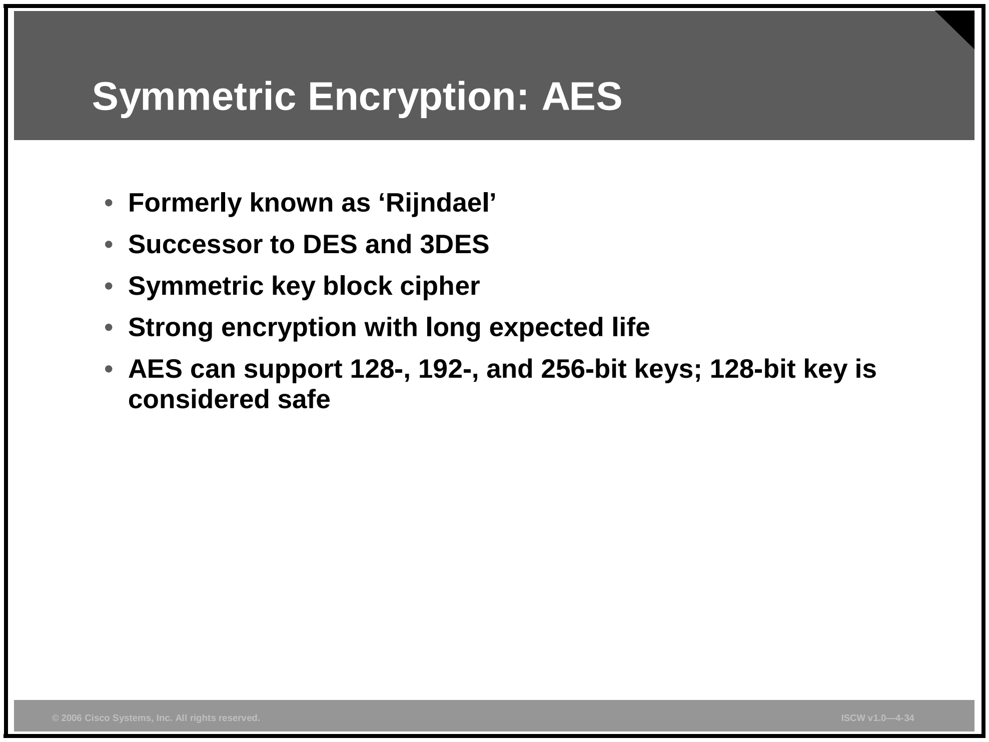
3DES is defined as performing a DES encryption, then a DES decryption, and then a DES encryption again.

3DES has a key length of 168 bits (three 56-bit DES keys), but it has an effective key size of 112 bits.

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

Symmetric Encryption: AES

AES, also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It is expected to be used worldwide and analyzed extensively, as was the case with its predecessor, DES. AES was adopted by National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001 after a five-year standardization process.



Symmetric Encryption: AES

- **Formerly known as 'Rijndael'**
- **Successor to DES and 3DES**
- **Symmetric key block cipher**
- **Strong encryption with long expected life**
- **AES can support 128-, 192-, and 256-bit keys; 128-bit key is considered safe**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-34

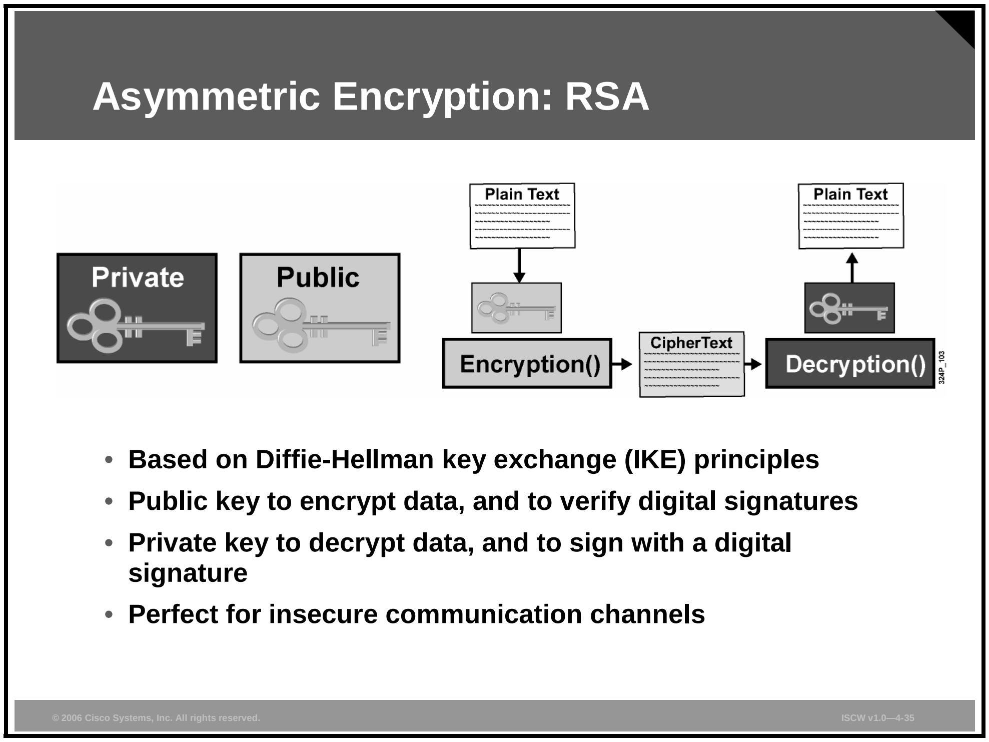
The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted to the AES selection process under the name "Rijndael". AES is not exactly the same as the original Rijndael because Rijndael supports a larger range of block and key sizes; AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits.

Up to 2005, no successful attacks against AES have been recognized. The NSA reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for U.S. government nonclassified data. In June 2003, the U.S. government announced that AES may be used for classified information. This marks the first time that the public has had access to a cipher approved by NSA for top secret information. It is interesting to note that many public products use 128-bit secret keys by default.

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

Asymmetric Encryption: RSA

There are various asymmetric algorithms used for IPsec, two of which, Diffie-Hellman and RSA, are given to show the main difference between symmetric algorithms and asymmetric algorithms.



Asymmetric Encryption: RSA

- Based on Diffie-Hellman key exchange (IKE) principles
- Public key to encrypt data, and to verify digital signatures
- Private key to decrypt data, and to sign with a digital signature
- Perfect for insecure communication channels

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-35

The Diffie-Hellman key agreement was invented in 1976 during collaboration between Whitfield Diffie and Martin Hellman, and was the first practical method for establishing a shared secret over an unprotected communications channel. The method was followed shortly afterwards by RSA, named after its designers: Rivest, Shamir, and Adelman.

RSA is an algorithm for public key encryption and was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography.

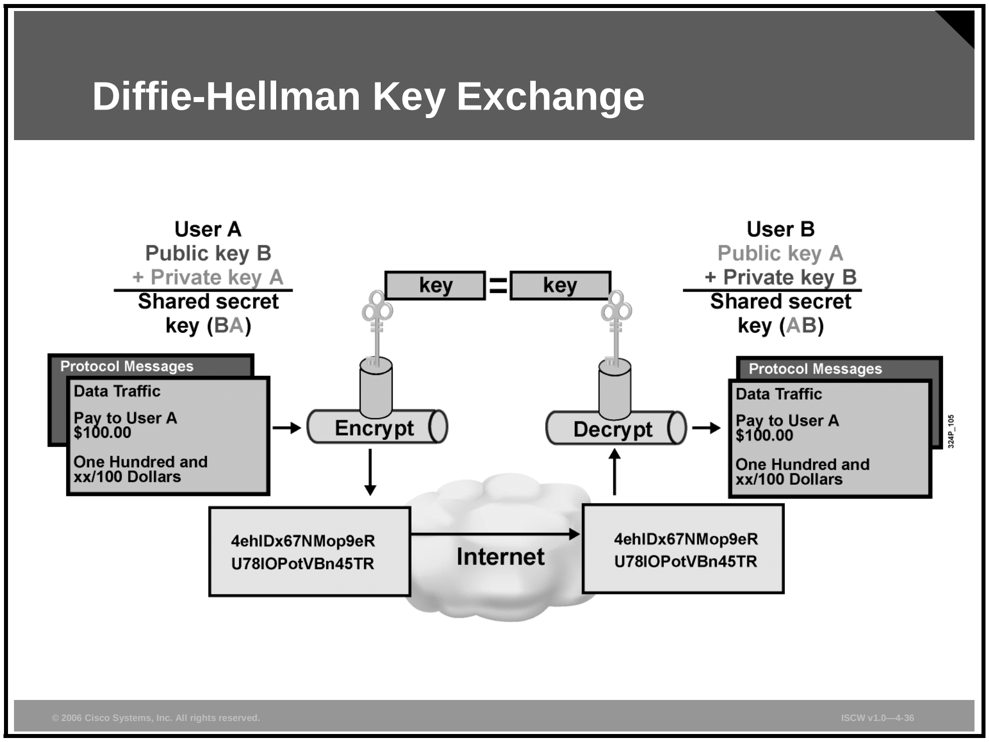
The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring very large numbers, and the RSA problem. Full decryption of an RSA cipher text is thought to be impossible because both of these problems are difficult, and no efficient algorithm exists for solving them. No polynomial-time method for factoring large integers on a classical computer has yet been found, but it has not been proven that none exists.

As of 2005, the largest number factored by general-purpose methods was 663 bits long, using state-of-the-art distributed methods. RSA keys are typically 1024–2048 bits long.

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

Diffie-Hellman Key Exchange

DES, 3DES, MD5, and SHA require a symmetric shared secret key to perform encryption and decryption. The question is how do the encrypting and decrypting devices get the shared secret key? The keys could be sent via e-mail, courier, overnight express, or public key exchange. The easiest method is Diffie-Hellman public key exchange. The Diffie-Hellman key agreement is a public key encryption method that provides a way for two peers to establish a shared secret key that only they know, although they are communicating over an insecure channel.



Diffie-Hellman Key Exchange

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-36

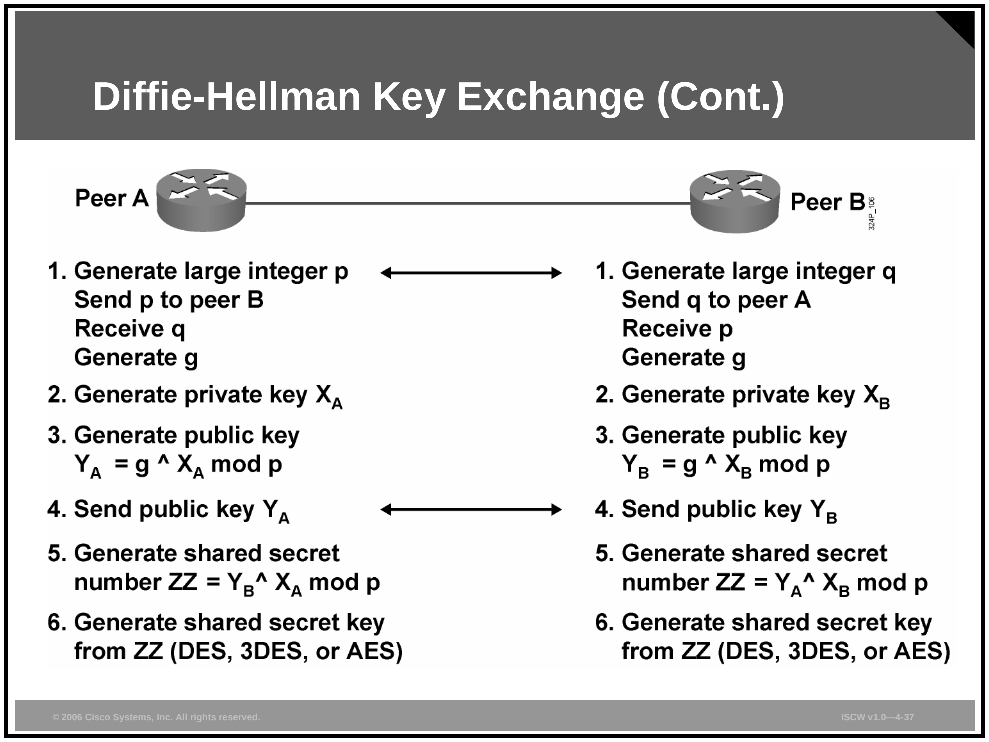
Public key cryptosystems rely on a two-key system:

- *Public key*, which is exchanged between end users
- *Private key*, which is kept secret by the original owners

The Diffie-Hellman public key algorithm states that if user A and user B exchange public keys and a calculation is performed on their individual private key and on the public key of the other peer, the end result of the process is an identical shared key. The shared key will be used to encrypt and decrypt the data.

Security is not an issue with the Diffie-Hellman key exchange. Although someone may know a user’s public key, the shared secret cannot be generated because the private key never becomes public knowledge.

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



Diffie-Hellman Key Exchange (Cont.)

Peer A	Peer B
1. Generate large integer p Send p to peer B Receive q Generate g	1. Generate large integer q Send q to peer A Receive p Generate g
2. Generate private key X_A	2. Generate private key X_B
3. Generate public key $Y_A = g \wedge X_A \bmod p$	3. Generate public key $Y_B = g \wedge X_B \bmod p$
4. Send public key Y_A	4. Send public key Y_B
5. Generate shared secret number $ZZ = Y_B \wedge X_A \bmod p$	5. Generate shared secret number $ZZ = Y_A \wedge X_B \bmod p$
6. Generate shared secret key from ZZ (DES, 3DES, or AES)	6. Generate shared secret key from ZZ (DES, 3DES, or AES)

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-37

The Diffie-Hellman key exchange is a public key exchange method that provides a way for two IPsec peers to establish a shared secret key that only they know, although they are communicating over an insecure channel.

With Diffie-Hellman, each peer generates a public and private key pair. The private key generated by each peer is kept secret and never shared. The public key is calculated from the private key by each peer and is exchanged over the insecure channel. Each peer combines the public key of the other peer with its own private key, and computes the same shared secret number. The shared secret number is then converted into a shared secret key. The shared secret key is never exchanged over the insecure channel.

The following steps explain the Diffie-Hellman process:

Step 1 The Diffie-Hellman process starts with each peer generating a large prime integer, p and q. Each peer sends the other its prime integer over the insecure channel. For example, peer A sends p to peer B. Routers select a minimum value from p and q, to determine a common p value. Each peer then uses the p value to generate g, a primitive root of p.

Step 2 Each peer generates a private Diffie-Hellman key: peer A generates X_A and peer B generates X_B.

Step 3 Each peer generates a public Diffie-Hellman key. The local private key is combined with the prime number p and the primitive root g in each peer to generate a public key, Y_A for peer A and Y_B for peer B. The formula for peer A is $Y_A = g \wedge X_A \bmod p$. The formula for peer B is $Y_B = g \wedge X_B \bmod p$. The exponentiation is computationally expensive.

Note The character ^ denotes exponentiation (g to the power of X_A); mod denotes modulus.

Step 4 The public keys Y_A and Y_B are exchanged in public.

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

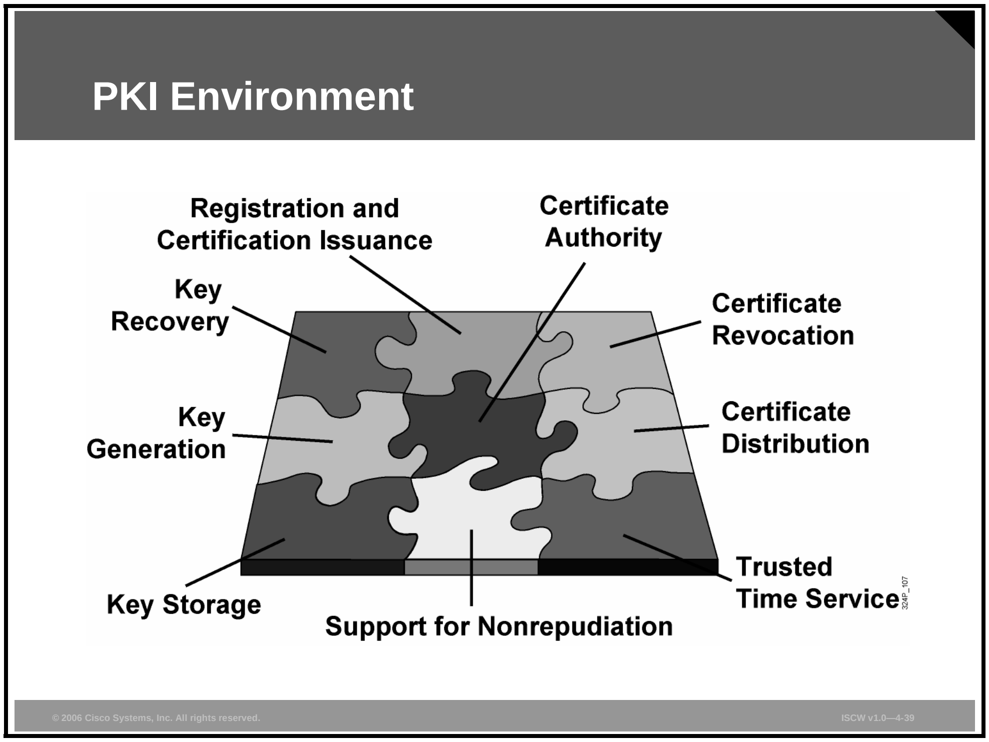
Step 5 Each peer generates a shared secret number (ZZ) by combining the public key received from the opposite peer with its own private key. The formula for peer A is $ZZ = (Y_B \wedge X_A) \bmod p$. The formula for peer B is $ZZ = (Y_A \wedge X_B) \bmod p$. The ZZ values are identical in each peer. Anyone who knows p or g, or the Diffie-Hellman public keys, cannot guess or easily calculate the shared secret value—largely because of the difficulty in factoring large prime numbers.

Step 6 Shared secret number ZZ is used in the derivation of the encryption and authentication symmetrical keys.

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

PKI Environment

This topic describes the public key infrastructure (PKI).



PKI Environment

Registration and Certification Issuance

Certificate Authority

Key Recovery

Certificate Revocation

Key Generation

Certificate Distribution

Key Storage

Support for Nonrepudiation

Trusted Time Service

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-39

A PKI provides a hierarchical framework for managing digital security attributes of entities that will engage in secured communications. In addition to human users, there are encryption gateways, secure web servers, and other resources that require close control of identity and encryption.

A PKI consists of these entities:

- Peers communicating on a secure network
- At least one CA that grants and maintains certificates
- Digital certificates, which contain information such as the certificate validity period, peer identity information, encryption keys that are used for secure communications, and the signature of the issuing CA
- An optional registration authority (RA) to offload the CA by processing enrollment requests. Certificate enrollment is the process of obtaining a certificate from a CA.
- A distribution mechanism, such as Lightweight Directory Access Protocol (LDAP) or HTTP, for certificate revocation lists (CRLs)

PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or device) participating in the secured communications is enrolled in the PKI in a process in which the entity generates an RSA key pair (one private key and one public key) and has their identity validated by a trusted entity (also known as a CA or trust point).

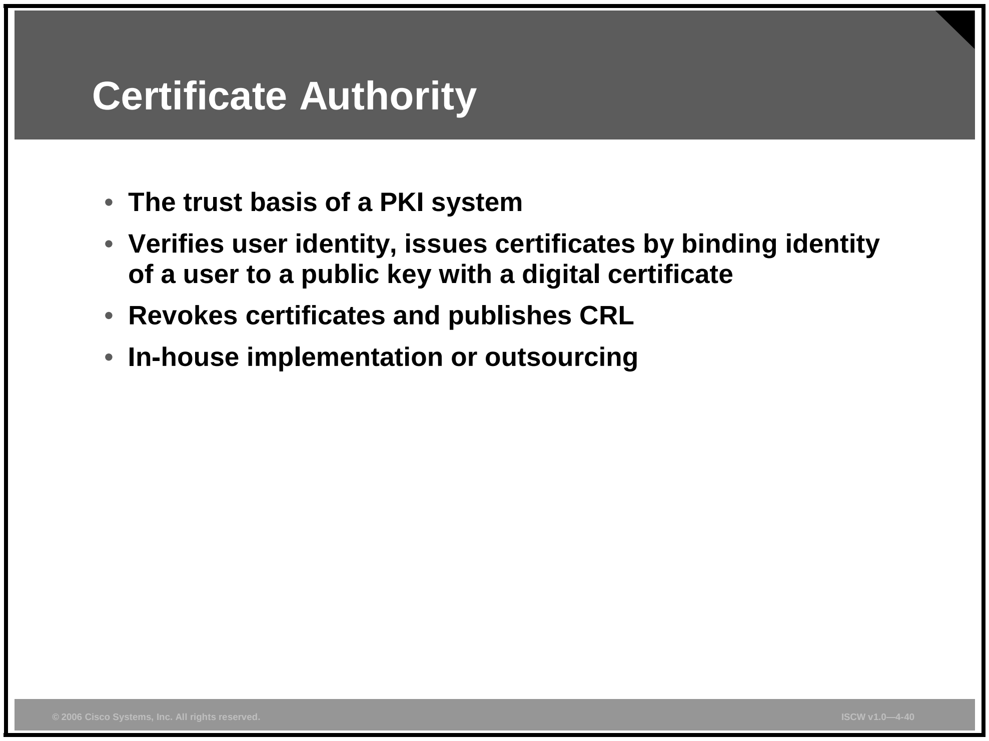
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

After enrolling in a PKI, each peer (also known as end host) in a PKI is granted a digital certificate that has been issued by a CA. When peers must negotiate a secured communication session, they exchange digital certificates. Based on the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

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

Certificate Authority

A CA, also known as a trustpoint, manages certificate requests and issues certificates to participating network devices. These services, managing certificate requests and issuing certificates, provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.



Certificate Authority

- **The trust basis of a PKI system**
- **Verifies user identity, issues certificates by binding identity of a user to a public key with a digital certificate**
- **Revokes certificates and publishes CRL**
- **In-house implementation or outsourcing**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-40

You can use a CA provided by a third-party CA vendor, or you can use an internal CA, which is the Cisco IOS Certificate Server.

Hierarchical PKI: Multiple CAs

You can set up a PKI in a hierarchical framework to support multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. The subordinate CAs within the hierarchy can be enrolled with either the root CA or with another subordinate CA. These enrollment options enable multiple tiers of CAs to be configured. Within a hierarchical PKI, all enrolled peers can validate the certificate of each other if the peers share a trusted root CA certificate or a common subordinate CA.

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

Multiple CAs provide users with added flexibility and reliability. For example, subordinate CAs can be placed in branch offices while the root CA is at the office headquarters. Also, different granting policies can be implemented per CA, so you can set up one CA to automatically grant certificate requests while another CA within the hierarchy requires each certificate request to be manually granted.

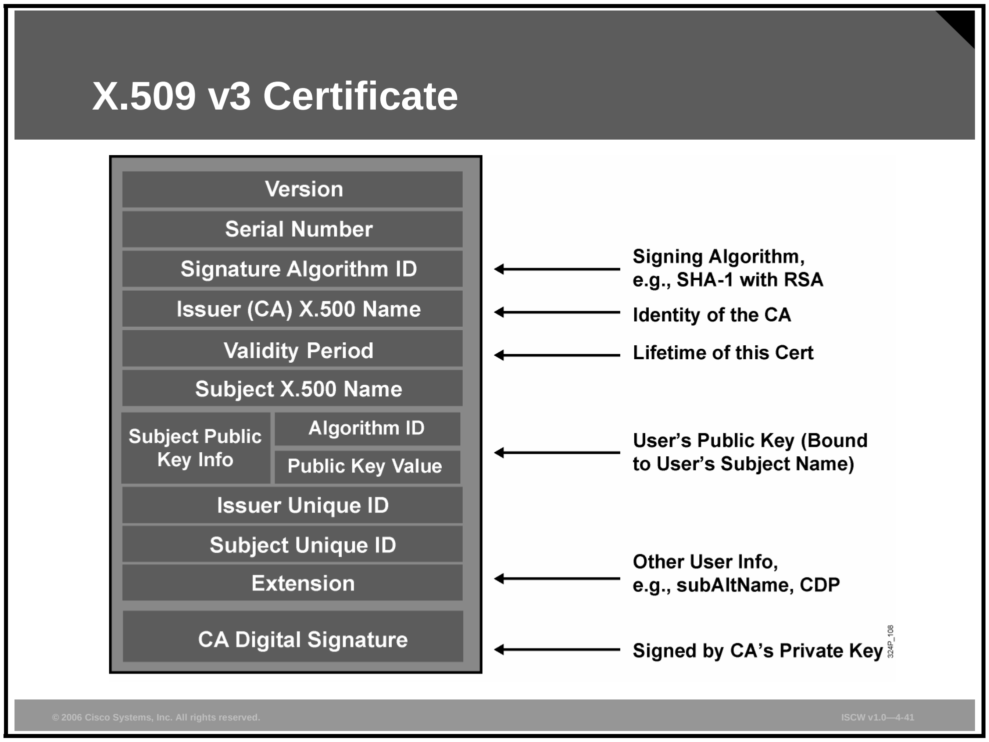
Scenarios in which at least a two-tier CA is recommended are as follows:

- Large and very active networks in which a large number of certificates are revoked and reissued. A multiple tier CA helps to control the size of the CRLs.
- When online enrollment protocols are used, the root CA can be kept offline with the exception of issuing subordinate CA certificates. This scenario provides added security for the root CA.

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

X.509 v3 Certificate

Certificates can be used for the large-scale use of public key cryptography. Securely exchanging secret keys among users becomes impractical for large networks.



X.509 v3 Certificate

Version

Serial Number

Signature Algorithm ID — Signing Algorithm, e.g., SHA-1 with RSA

Issuer (CA) X.500 Name — Identity of the CA

Validity Period — Lifetime of this Cert

Subject X.500 Name

Subject Public Key Info: Algorithm ID, Public Key Value — User's Public Key (Bound to User's Subject Name)

Issuer Unique ID

Subject Unique ID

Extension — Other User Info, e.g., subAltName, CDP

CA Digital Signature — Signed by CA's Private Key

324P_108

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-41

A certificate may be revoked if it is discovered that its related private key has been compromised, or if the relationship between an entity and a public key, embedded in the certificate, is discovered to be incorrect or has changed; this might occur, for example, if a person changes jobs or names. A revocation is a rare occurrence, but that possibility means that when a certificate is trusted, the user should always check its validity. You can check its validity by comparing it against a CRL—a list of revoked or cancelled certificates. Ensuring that such a list is up-to-date and accurate is a core function in a centralized PKI. To be effective, the certificate must be readily available to anyone and must be updated frequently. The other way to check certificate validity is to query the CA using the Online Certificate Status Protocol (OCSP) to know the status of a specific certificate.

The structure of a X.509 v3 digital certificate is as follows:

- Certificate
  - — Version
  - — Serial Number
  - — Algorithm ID
  - — Issuer
  - — Validity:
    - Not Before
    - Not After
  - — Subject

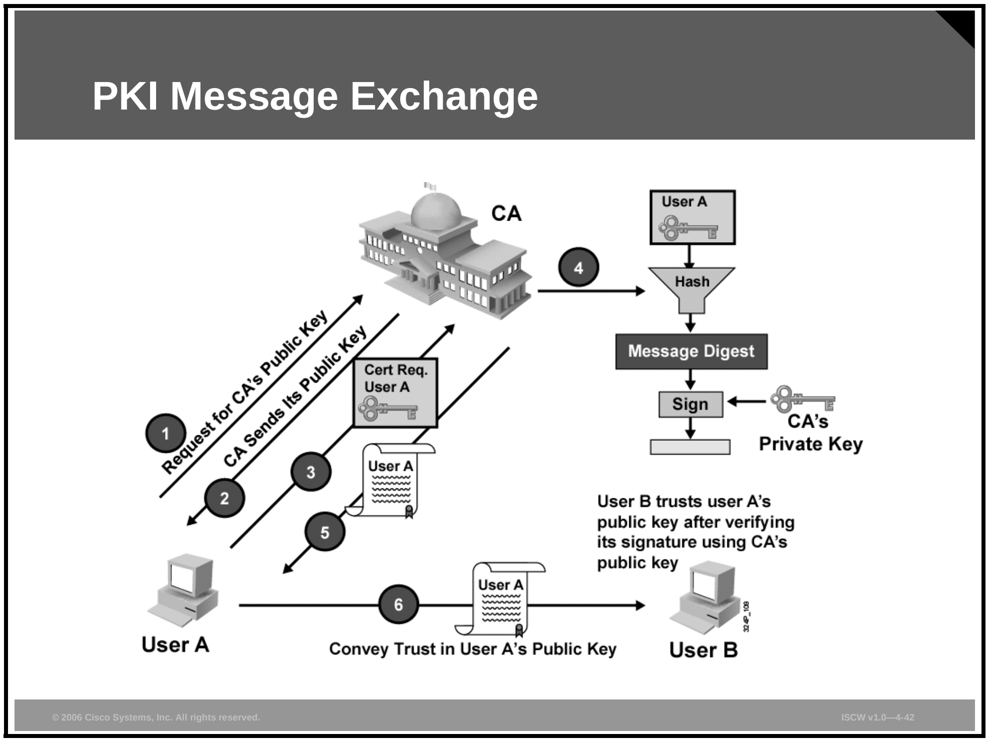
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (Optional)
  - Subject Unique Identifier (Optional)
  - Extensions (Optional)
- Certificate Signature Algorithm
- Certificate Signature

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

PKI Message Exchange

Certificate enrollment is the process of obtaining a certificate from a CA. Each end host that wants to participate in the PKI must obtain a certificate.



PKI Message Exchange

CA
User A
Hash
Message Digest
Sign
CA's Private Key
4
Request for CA's Public Key
CA Sends Its Public Key
Cert Req. User A
User A
1
2
3
5
User B trusts user A's public key after verifying its signature using CA's public key
User A
6
User A
Convey Trust in User A's Public Key
User B

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-42

Certificate enrollment occurs with these steps between the end host requesting the certificate and the CA:

Step 1 The end host generates an RSA key pair and requests the public key of the CA.

Step 2 The CA sends its public key to the end host.

Step 3 The end host generates a certificate request and forwards it to the CA (or the RA, if applicable). The CA receives the certificate enrollment request, and, depending on your network configuration, one of the following options occurs:

A) Manual intervention is required to approve the request.
B) The end host is configured to automatically request a certificate from the CA.

Thus, operator intervention is no longer required at the time the enrollment request is sent to the CA server.

Step 4 After the request is approved, the CA signs the request with its private key.

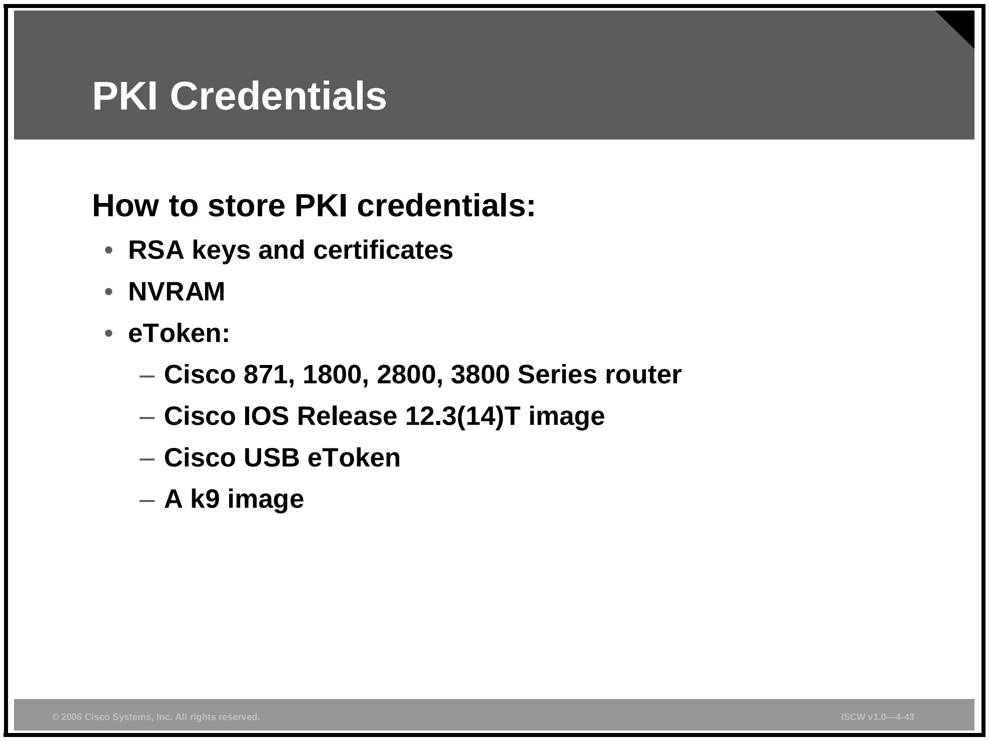
Step 5 The CA returns the completed certificate to the end host. The end host writes the certificate to a storage area such as NVRAM.

Step 6 The end host uses the certificate for communication with other communication partners.

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

PKI Credentials

PKI credentials, such as RSA keys and certificates, can be stored in a location other than NVRAM, the default location on the router.



PKI Credentials

How to store PKI credentials:

- **RSA keys and certificates**
- **NVRAM**
- **eToken:**
  - **Cisco 871, 1800, 2800, 3800 Series router**
  - **Cisco IOS Release 12.3(14)T image**
  - **Cisco USB eToken**
  - **A k9 image**

© 2006 Cisco Systems, Inc. All rights reserved.

Selected Cisco platforms now support Smartcard technology in a Universal Serial Bus (USB) key form (also known as an Aladdin USB eToken key). An eToken provides secure configuration distribution and allows users to store VPN credentials for deployment.

Before you can use an eToken, you should have the following system requirements:

- A Cisco 871 router, Cisco 1800 Series, Cisco 2800 Series, or a Cisco 3800 Series router
- At least a Cisco IOS Release 12.3(14)T image running on any of the supported platforms
- A Cisco supported USB eToken
- A Cisco IOS image with k9 code

An eToken is a Smartcard with a USB interface. The eToken can securely store any type of file within its available 32-KB storage space. Configuration files that are stored on the eToken can be encrypted and accessed only via a user PIN. The router will not load the configuration file unless the proper PIN has been configured for secure deployment of router configuration files.

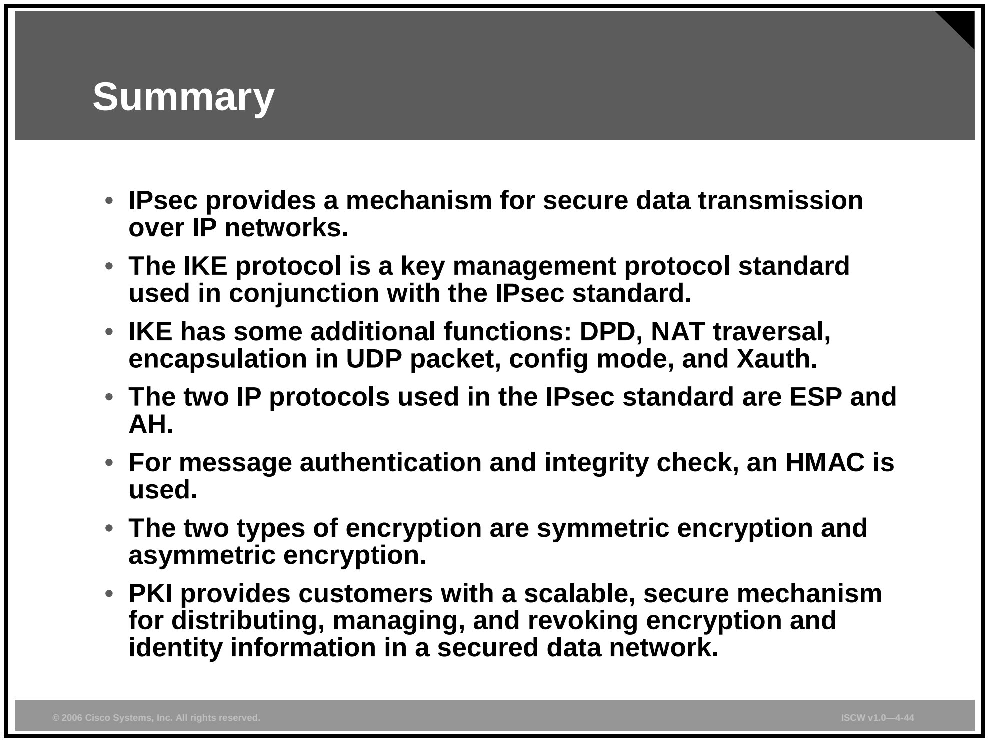
After you plug the eToken into the router, you must log into the eToken; thereafter, you can change default settings, such as the user PIN (default: 1234567890) and the allowed number of failed login attempts before future logins are refused (default: 15 attempts).

After you have successfully logged into the eToken, you can copy files from the router on to the eToken via the **copy** command. By default, after the eToken is removed from the router, all associated RSA keys are removed; IPsec tunnels are not torn down until the next IKE negotiation period.

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

Summary

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



Summary

- IPsec provides a mechanism for secure data transmission over IP networks.
- The IKE protocol is a key management protocol standard used in conjunction with the IPsec standard.
- IKE has some additional functions: DPD, NAT traversal, encapsulation in UDP packet, config mode, and Xauth.
- The two IP protocols used in the IPsec standard are ESP and AH.
- For message authentication and integrity check, an HMAC is used.
- The two types of encryption are symmetric encryption and asymmetric encryption.
- PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network.

© 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 self-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 self-study.

Lesson 2

Implementing Site-to-Site IPsec VPN Operations

Overview

This lesson describes how to successfully design and implement an IPsec virtual private network (VPN) between Cisco routers and explains the five steps of IPsec configuration.

Objectives

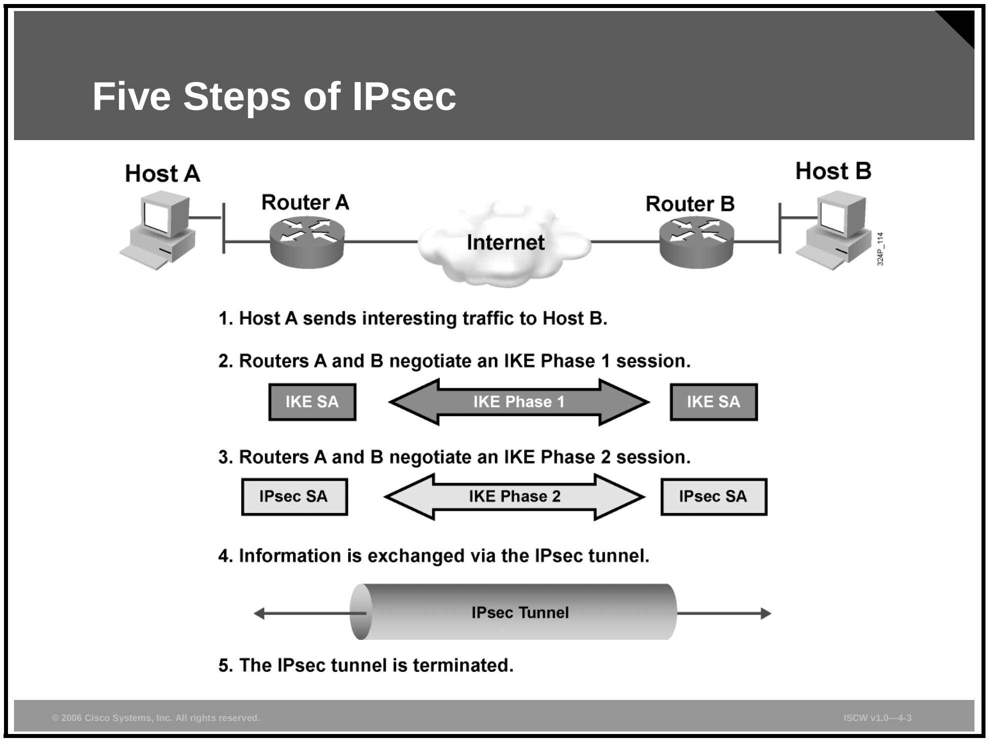
Upon completing this lesson, you will be able to describe IPsec site-to-site VPN operations. This ability includes being able to meet these objectives:

- Describe the five steps of IPsec operation
- Explain the procedure to configure IPsec
- Describe the configuration of the ISAKMP parameters
- Describe the configuration to define the IPsec transform set, the crypto ACL, and the crypto map
- Describe the configuration to apply the crypto map to the interface
- Describe the configuration of the interface ACL for IPsec

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

Site-to-Site IPsec VPN Operations

This topic describes the five steps of IPsec operation.



Five Steps of IPsec

1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE Phase 1 session.

3. Routers A and B negotiate an IKE Phase 2 session.

4. Information is exchanged via the IPsec tunnel.

5. The IPsec tunnel is terminated.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-3

The goal of IPsec is to protect data with the necessary security and algorithms. The figure shows only one of two bidirectional IPsec security associations (SAs). IPsec operation can be broken down into five primary steps:

Step 1 **Interesting traffic initiates the IPsec process:** Traffic is deemed interesting when the VPN device recognizes that the traffic you want to send must be protected.

Step 2 **Internet Key Exchange (IKE) Phase 1:** IKE authenticates IPsec peers and negotiates IKE SAs during this phase, setting up a secure communications channel for negotiating IPsec SAs in Phase 2.

Step 3 **IKE Phase 2:** IKE negotiates IPsec SA parameters and sets up matching IPsec SAs in the peers. These security parameters are used to protect data and messages that are exchanged between endpoints.

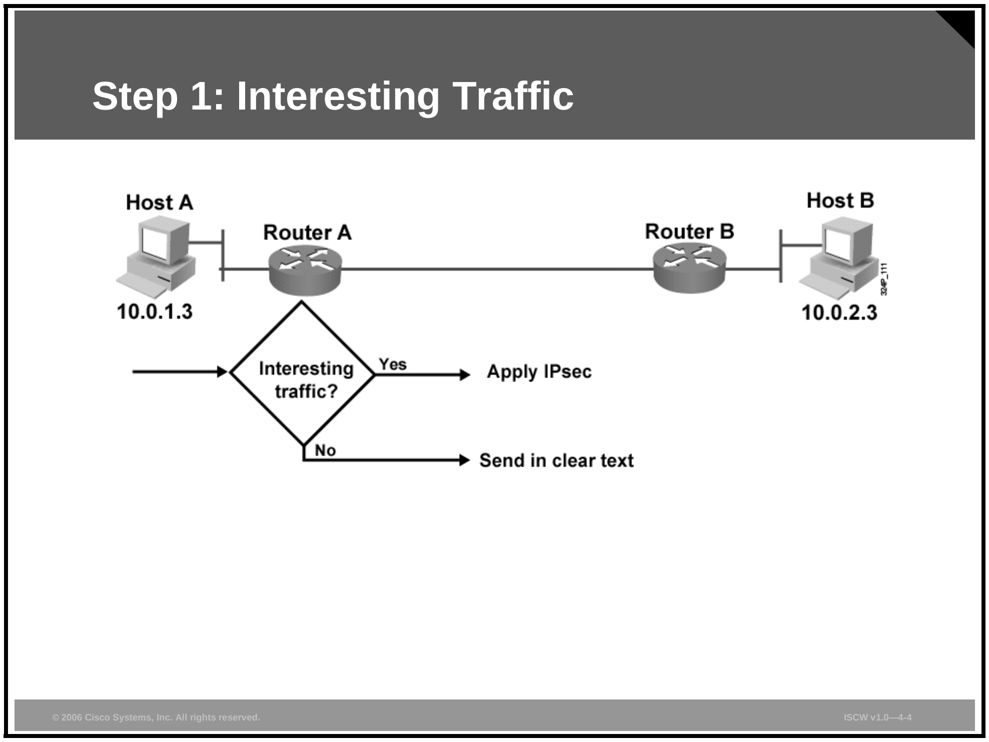
Step 4 **Data transfer:** Data is transferred between IPsec peers, based on the IPsec parameters and keys stored in the SA database.

Step 5 **IPsec tunnel termination:** IPsec SAs terminate through deletion or by timing out.

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

Step 1: Interesting Traffic Initiates the IPsec Process

Determining what traffic needs to be protected is done as part of formulating a security policy for using a VPN.



Step 1: Interesting Traffic

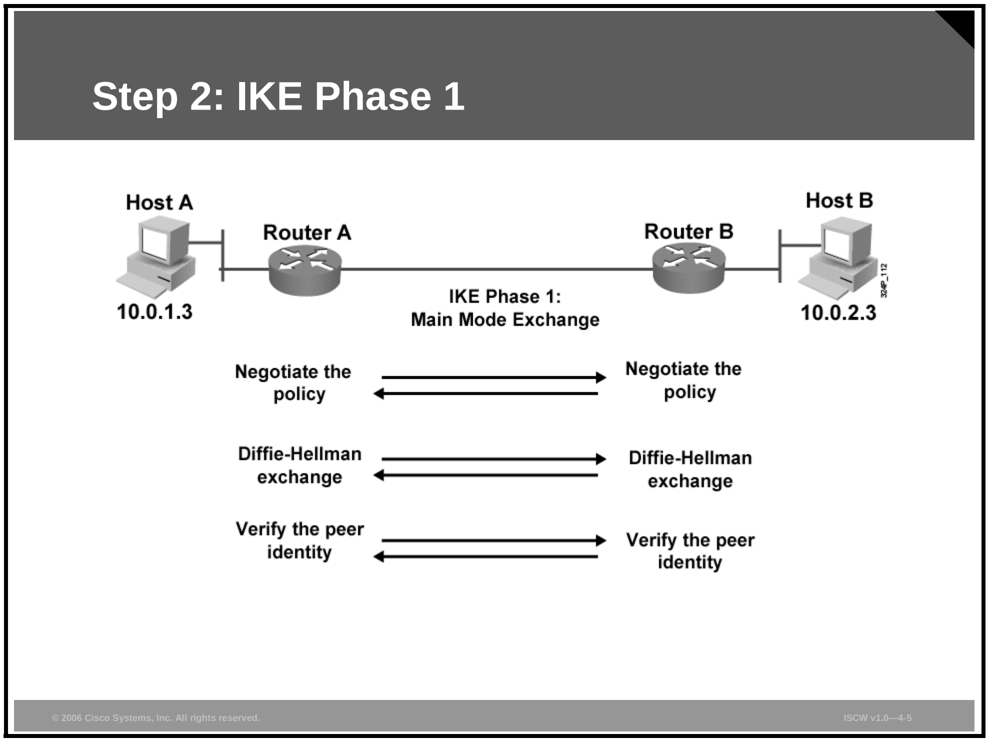
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-4

The policy is used to determine what traffic needs to be protected and what traffic can be sent in the clear. For every inbound and outbound datagram, there are two choices: apply IPsec, or bypass IPsec and send the datagram in clear text. For every datagram protected by IPsec, the system administrator must specify the security services applied to the datagram. The security policy database specifies the IPsec protocols, modes, and algorithms applied to the traffic. The services are then applied to traffic destined to each particular IPsec peer. With the VPN Client, you use menu windows to select connections that you want secured by IPsec. When interesting traffic transits the IPsec client, the client initiates the next step in the process, negotiating an IKE Phase 1 exchange.

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

Step 2: IKE Phase 1

The basic purpose of IKE Phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. IKE Phase 1 occurs in two modes: main mode and aggressive mode.



Step 2: IKE Phase 1

Host A

Router A

Router B

Host B

10.0.1.3

IKE Phase 1:
Main Mode Exchange

10.0.2.3

Negotiate the policy → ← Negotiate the policy

Diffie-Hellman exchange → ← Diffie-Hellman exchange

Verify the peer identity → ← Verify the peer identity

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-5

The main mode has three two-way exchanges between the initiator and receiver:

- **First exchange:** The algorithms and hashes used to secure the IKE communications are negotiated and agreed upon between peers.
- **Second exchange:** Uses a Diffie-Hellmann exchange to generate shared secret keys and pass nonces, which are random numbers sent to the other party, signed, and returned to prove their identity. The shared secret key is used to generate all the other encryption and authentication keys.
- **Third exchange:** Verifies the identity of the other side by authenticating the remote peer.

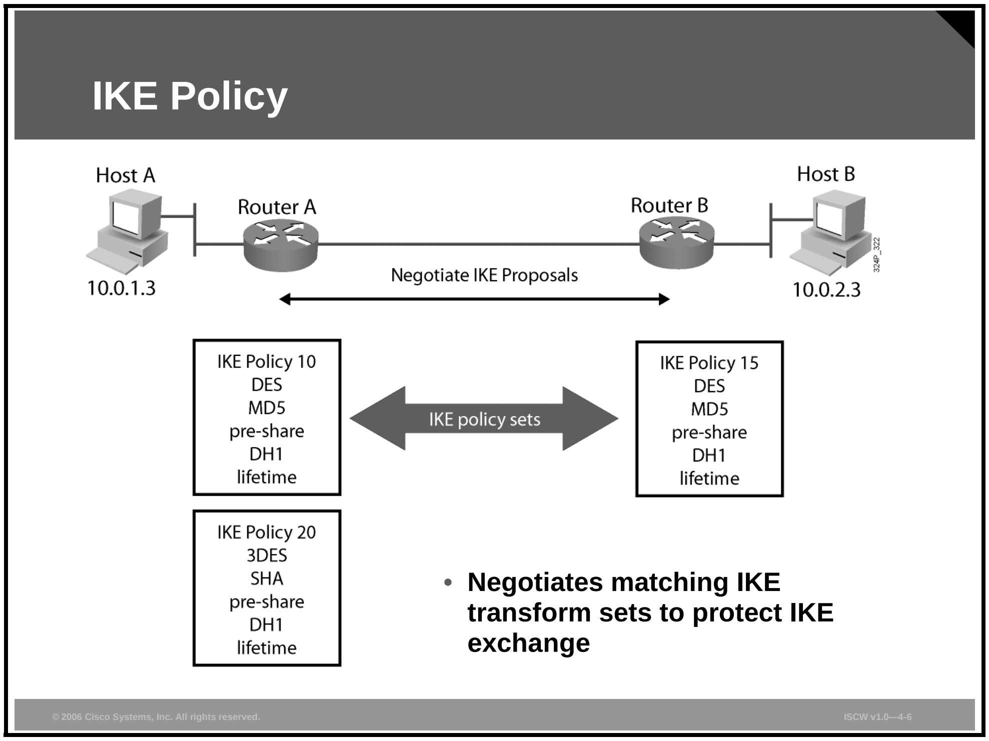
The main outcome of the main mode is a secure communication path for subsequent exchanges between the peers. Without proper authentication, it is possible that you might establish a secure communication channel with a hacker who will steal your sensitive material.

In the aggressive mode, fewer exchanges are done and with fewer packets. Most of the actions occur during the first exchange: the IKE policy set negotiation; the Diffie-Hellmann public key generation; a nonce, which the other party signs; and an identity packet, which can be used to verify the identity of the other party via a third party. The receiver sends everything back that is needed to complete the exchange. The only action left is for the initiator to confirm the exchange.

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

IKE Policy

When trying to make a secure connection between host A and host B through the Internet, IKE security proposals are exchanged between router A and router B. The proposals identify the IPsec protocol being negotiated (for example, Encapsulating Security Payload [ESP]). Under each proposal, the originator must delineate which algorithms are employed in the proposal (for example, Data Encryption Standard [DES] with Message Digest 5 [MD5]). Rather than negotiate each algorithm individually, the algorithms are grouped into sets, called IKE transform sets. A transform set describes which encryption algorithm, authentication algorithm, mode, and key length are proposed. These IKE proposals and transform sets are exchanged during the IKE main mode first exchange phase. If a transform set match is found between peers, the main mode continues. If no match is found, the tunnel is torn down.



IKE Policy

Host A

10.0.1.3

Router A

Negotiate IKE Proposals

Router B

Host B

10.0.2.3

IKE Policy 10
DES
MD5
pre-share
DH1
lifetime

IKE policy sets

IKE Policy 15
DES
MD5
pre-share
DH1
lifetime

IKE Policy 20
3DES
SHA
pre-share
DH1
lifetime

- **Negotiates matching IKE transform sets to protect IKE exchange**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-6

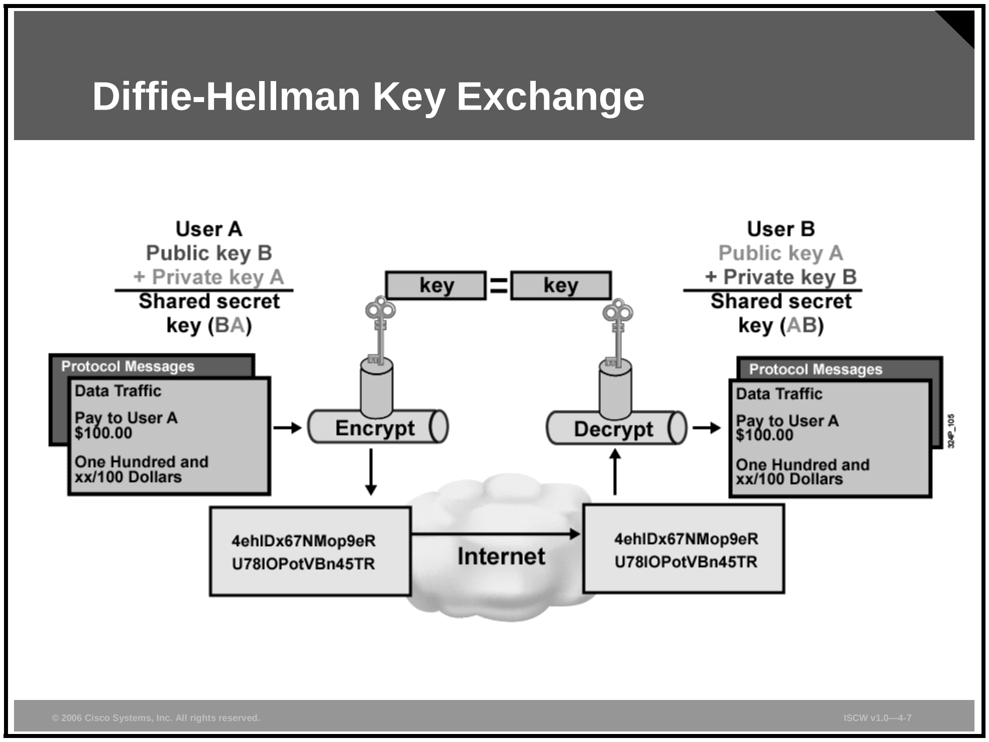
In the figure, Router A sends IKE policies 10 and 20 to Router B. Router B compares its IKE policies, policy 15, with those received from Router A. In this instance, there is a match: Router A’s policy 10 matches Router B’s policy 15.

In a point-to-point application, each end may only need a single IKE policy defined. However, in a hub and spoke environment, the central site may require multiple IKE policies defined to satisfy all the remote peers.

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

Diffie-Hellman Key Exchange

Diffie-Hellmann key exchange is a public key exchange method that provides a way for two peers to establish a shared secret key over an insecure communications path. There are several different Diffie-Hellmann algorithms, or groups defined, Diffie-Hellmann groups 1–7. A group number defines an algorithm and unique values. For example, group 1 defines a modular exponentiation (MODP) algorithm with a 768-bit prime number. Group 2 defines a MODP algorithm with a 1024-bit prime number. During IKE Phase 1, the group is negotiated between peers. Between Cisco VPN devices, either group 1 or group 2 is supported.



Diffie-Hellman Key Exchange

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-7

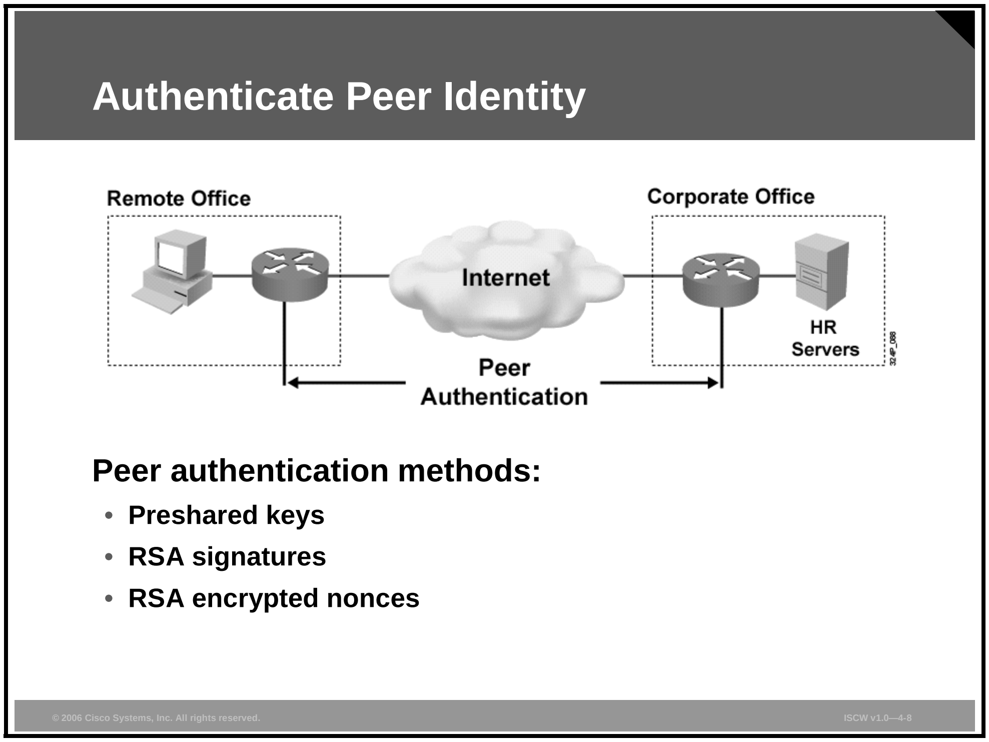
After the group negotiations are completed, the shared secret key is calculated, SKEYID. The shared secret key, SKEYID, is used in the derivation of three other keys: SKEYID_a, SKEYID_e, and SKEYID_d. Each key has a separate purpose. SKEYID_a is the keying material used during the authentication process. The SKEYID_e key is the keying material used in the encryption process and the SKEY_d key is keying material used to derive keys for non-Internet Security Association and Key Management Protocol (non-ISAKMP) SAs. All four keys are calculated during IKE Phase 1.

In the example, User A and User B each establishes their own private key, and from the private key they calculate their public keys, which are exchanged. From their own private key and the public key of the other peer, they calculate a shared secret key which is used for encryption and decryption.

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

Authenticate Peer Identity

When conducting business over the Internet, the device on the other end of a VPN tunnel must be authenticated before the communications path is considered secure. The last exchange of IKE Phase 1 is used to authenticate the remote peer.



Authenticate Peer Identity

Peer authentication methods:

- **Preshared keys**
- **RSA signatures**
- **RSA encrypted nonces**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-8

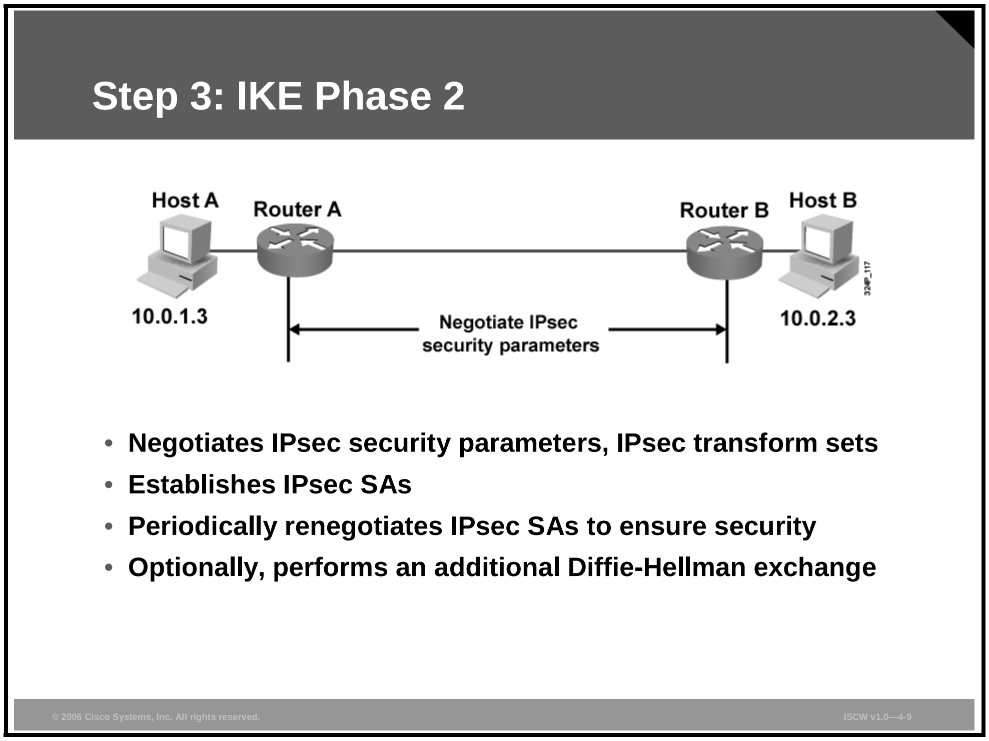
There are these three data origin authentication methods:

- **Preshared keys:** A secret key value entered into each peer manually, used to authenticate the peer
- **RSA signatures:** Uses the exchange of digital certificates to authenticate the peers
- **RSA encrypted nonces:** Nonces (a random number generated by each peer) are encrypted and then exchanged between peers. The two nonces are used during a peer authentication process.

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

Step 3: IKE Phase 2

The purpose of IKE Phase 2 is to negotiate the IPsec security parameters used to secure the IPsec tunnel.



Step 3: IKE Phase 2

- **Negotiates IPsec security parameters, IPsec transform sets**
- **Establishes IPsec SAs**
- **Periodically renegotiates IPsec SAs to ensure security**
- **Optionally, performs an additional Diffie-Hellman exchange**

© 2006 Cisco Systems, Inc. All rights reserved.

These functions are performed in IKE Phase 2:

- Negotiation of IPsec security parameters and IPsec transform sets
- Establishment of IPsec SAs
- Periodic renegotiation of IPsec SAs to ensure security
- Optionally, performance of an additional Diffie-Hellmann exchange

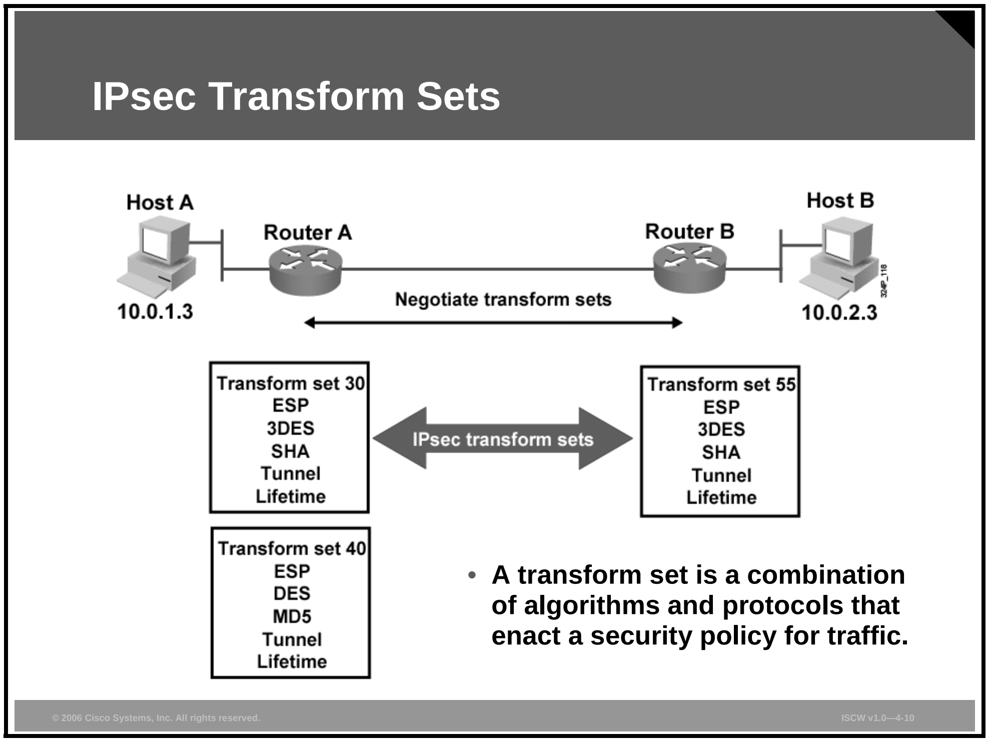
IKE Phase 2 has one mode, called quick mode. Quick mode occurs after IKE has established the secure tunnel in Phase 1. Quick mode negotiates a shared IPsec transform, derives shared secret keying material used for the IPsec security algorithms, and establishes IPsec SAs. Quick mode exchanges nonces that are used to generate new shared secret key material and to prevent replay attacks from generating bogus SAs.

Quick mode is also used to renegotiate a new IPsec SA when the IPsec SA lifetime expires. Quick mode is used to refresh the keying material used to create the shared secret key based on the keying material derived from the Diffie-Hellmann exchange in Phase 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 self-study.

IPsec Transform Sets

The ultimate goal of IKE Phase 2 is to establish a secure IPsec session between endpoints. Before that can happen, each pair of endpoints negotiates the level of security required (for example, encryption and authentication algorithms for the session). Rather than negotiate each protocol individually, the protocols are grouped into an IPsec transform set. IPsec transform sets are exchanged between peers during quick mode. If a match is found between sets, IPsec session establishment continues. If no match is found, the session is torn down.



IPsec Transform Sets

Host A

10.0.1.3

Router A

Negotiate transform sets

Router B

Host B

10.0.2.3

324P_118

Transform set 30
ESP
3DES
SHA
Tunnel
Lifetime

IPsec transform sets

Transform set 55
ESP
3DES
SHA
Tunnel
Lifetime

Transform set 40
ESP
DES
MD5
Tunnel
Lifetime

- **A transform set is a combination of algorithms and protocols that enact a security policy for traffic.**

© 2006 Cisco Systems, Inc. All rights reserved.

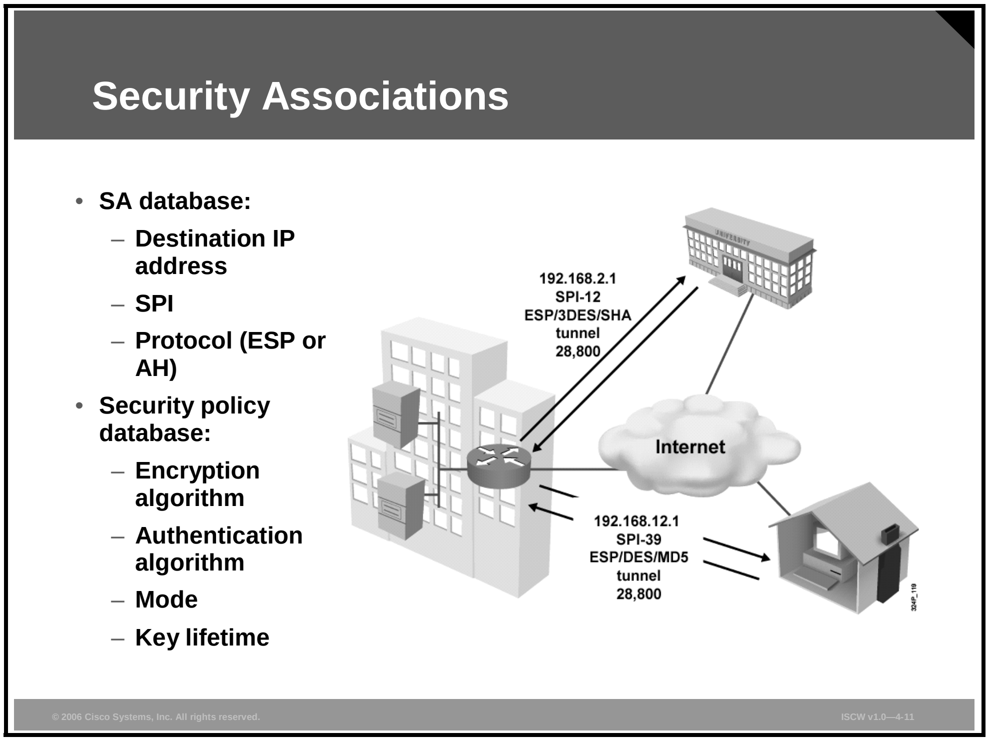
ISCW v1.0—4-10

In the example, Router A sends IPsec transform set 30 and 40 to Router B. Router B compares its set, transform set 55, with those received from Router A. In this instance, there is a match. The Router A transform set 30 matches the Router B transform set 55. These encryption and authentication algorithms form an SA. The transform set 40 on router A is not 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 self-study.

Security Associations

When security services are agreed upon between peers, each VPN peer device enters the information in a Security Policy Database (SPD). The information includes the encryption and authentication algorithm, destination IP address, transport mode, key lifetime, and so on. This information is referred to as the SA. An SA is a one-way logical connection that provides security to all traffic traversing the connection. Because most traffic is bidirectional, two SAs are required: one for inbound traffic and one for outbound traffic. The VPN device indexes the SA with a number, a Security Parameter Index (SPI). Rather than send the individual parameters of the SA across the tunnel, the source gateway, or host, inserts the SPI into the ESP header. When the IPsec peer receives the packet, it looks up the destination IP address, IPsec protocol, and SPI in its security association database (SAD), and then processes the packet according to the algorithms listed under the SPD.



Security Associations

- **SA database:**
  - **Destination IP address**
  - **SPI**
  - **Protocol (ESP or AH)**
- **Security policy database:**
  - **Encryption algorithm**
  - **Authentication algorithm**
  - **Mode**
  - **Key lifetime**

The IPsec SA is a compilation of the SAD and SPD. SAD is used to identify the SA destination IP address, IPsec protocol, and SPI number.

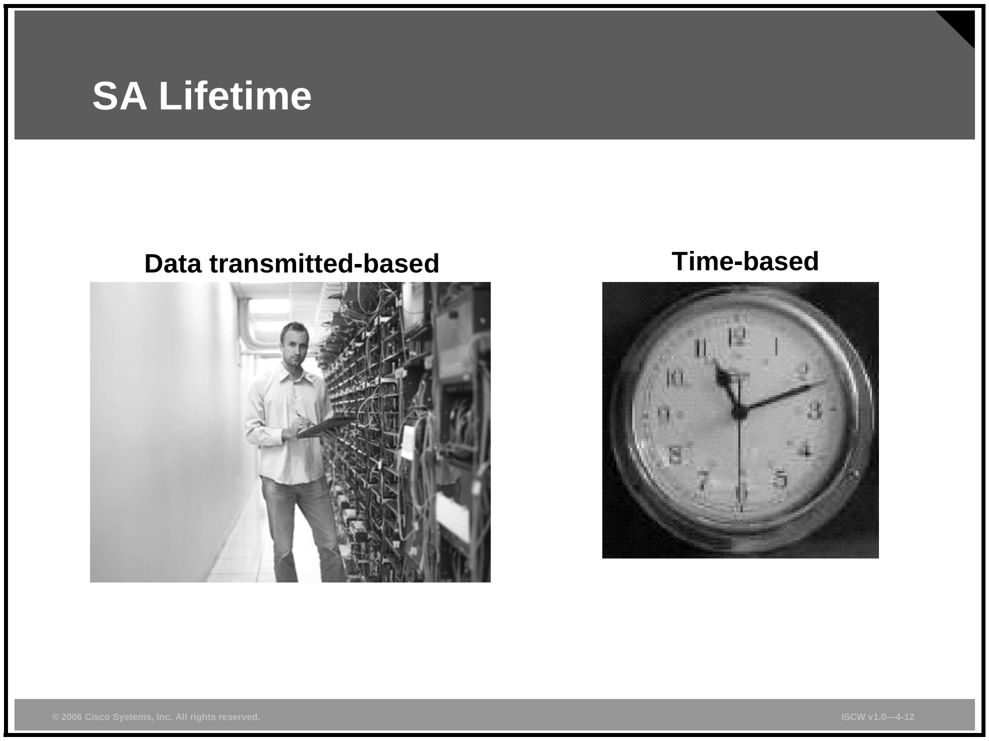
The SPD defines the security services applied to the SA, encryption and authentication algorithms, and mode and key lifetime.

For example, in the corporate-to-bank connection, the security policy provides a very secure tunnel using Triple Data Encryption Standard (3DES), Secure Hash Algorithm 1 (SHA-1), tunnel mode, and a key lifetime of 28,800. The SAD value is 192.168.2.1, ESP, and SPI-12. For the remote user accessing e-mails, a less secure policy is negotiated using DES, MD5, tunnel mode, and a key lifetime of 28,800. The SAD values are a destination IP address of 192.168.12.1, ESP, and SPI-39.

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

SA Lifetime

To maintain adequate security, you should change the SA and keys periodically.



SA Lifetime

Data transmitted-based

Time-based

© 2006 Cisco Systems, Inc. All rights reserved.

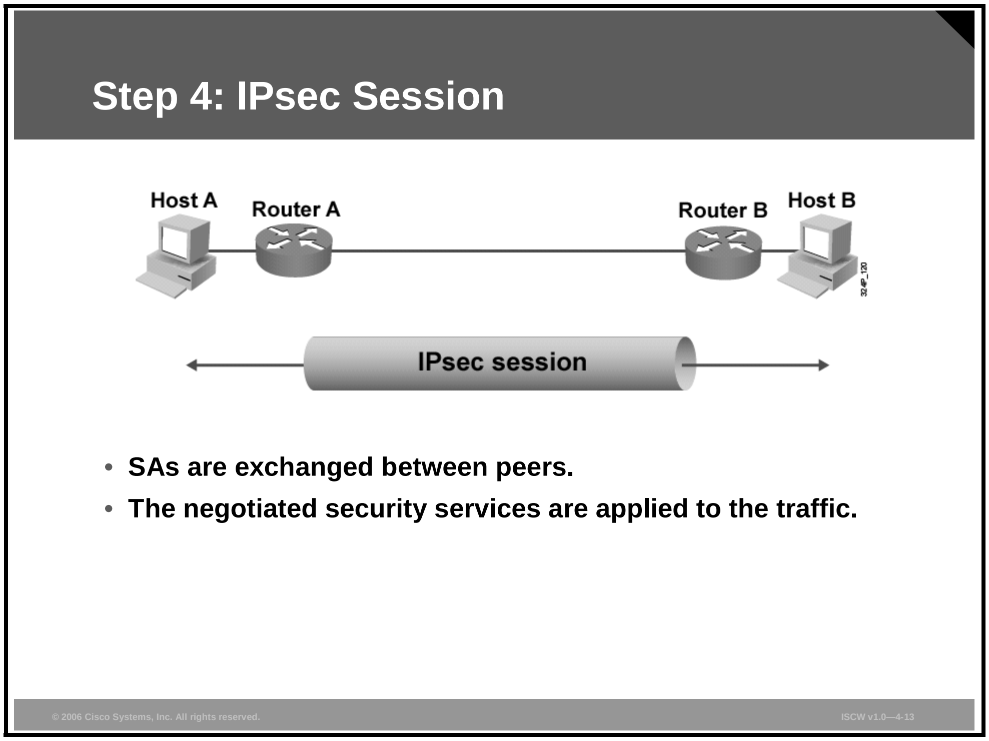
ISCW v1.0—4-12

There are two parameters of an SA lifetime: type and duration. The first parameter is lifetime type. How is the lifetime measured? Is it measured by the number of bytes transmitted or the amount of time transpired? The second parameter is the unit of measure: kilobytes of data or seconds of time. For example, a lifetime could be based on 10,000 kilobytes of data transmitted or 28,800 seconds of time expired. The keys and SAs remain active until their lifetime expires or until some external event—the client drops the tunnel—causes them to be deleted.

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

Step 4: Data Transfer

After IKE Phase 2 is complete and quick mode has established IPsec SAs, traffic is exchanged between host A and host B via a secure tunnel.



Step 4: IPsec Session

- SAs are exchanged between peers.
- The negotiated security services are applied to the traffic.

© 2006 Cisco Systems, Inc. All rights reserved.

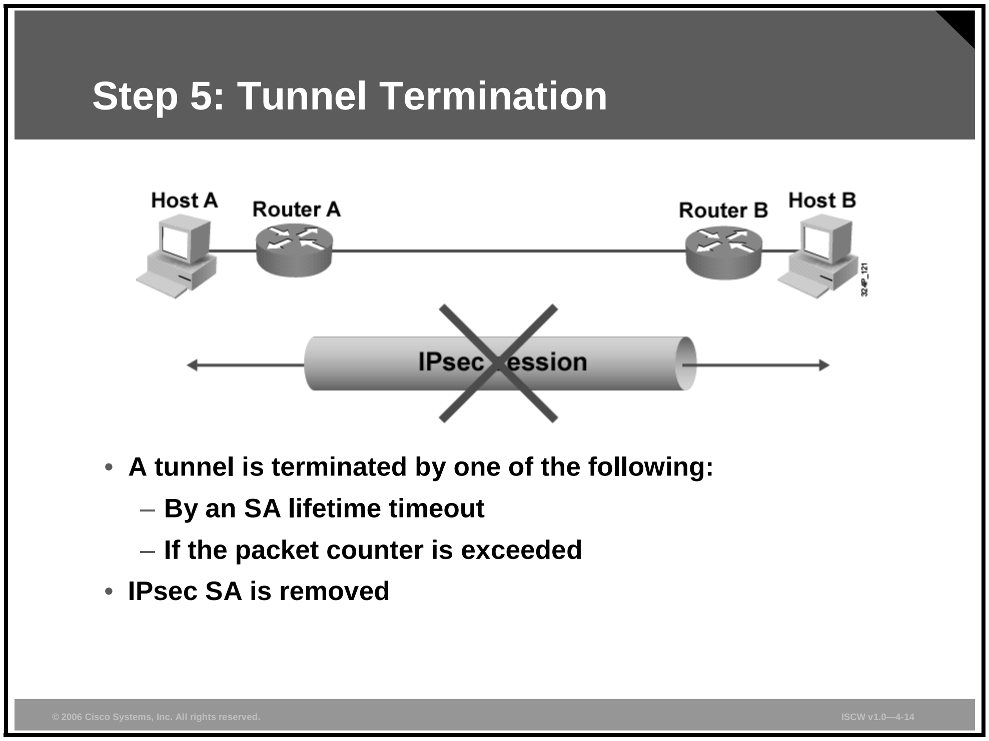
ISCW v1.0—4-13

Interesting traffic is encrypted and decrypted according to the security services specified in the IPsec SA.

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

Step 5: IPsec Tunnel Termination

IPsec SAs terminate through deletion or by timing out.



Step 5: Tunnel Termination

- **A tunnel is terminated by one of the following:**
  - **By an SA lifetime timeout**
  - **If the packet counter is exceeded**
- **IPsec SA is removed**

© 2006 Cisco Systems, Inc. All rights reserved.

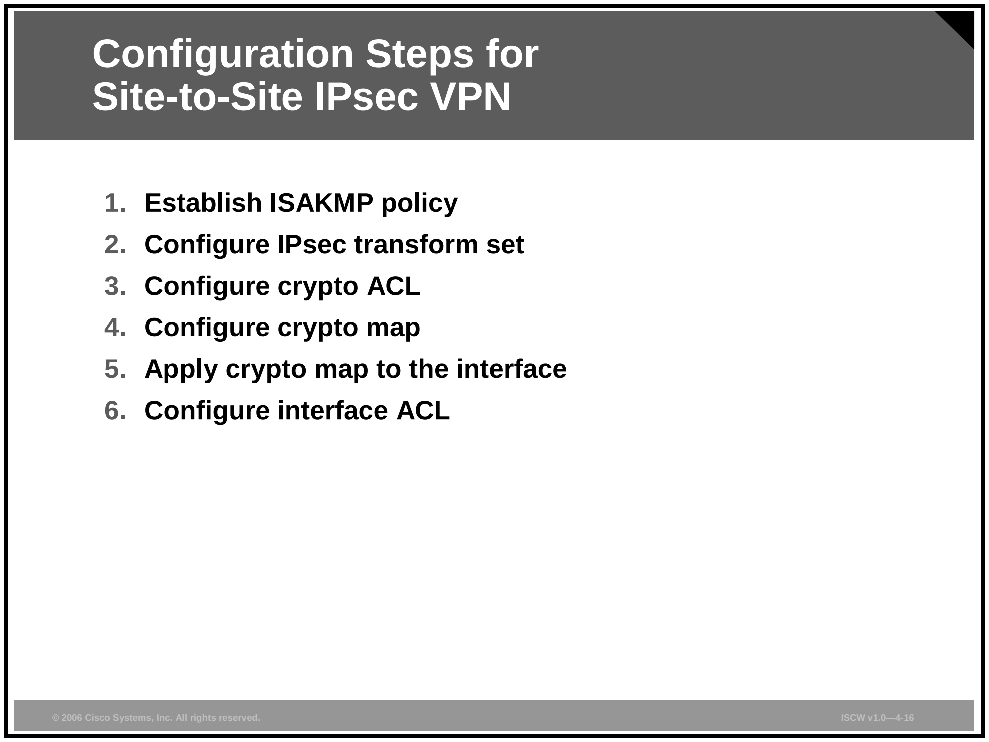
ISCW v1.0—4-14

An SA can time out when a specified number of seconds has elapsed or when a specified number of bytes has passed through the tunnel. When the SAs terminate, the keys are also discarded. When subsequent IPsec SAs are needed for a flow, IKE performs a new Phase 2, and, if necessary, a new Phase 1 negotiation. A successful negotiation results in new SAs and new keys. New SAs are usually established before the existing SAs expire, so that a given flow can continue uninterrupted.

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

Configuring IPsec

This topic describes the tasks to configure IPsec.



Configuration Steps for Site-to-Site IPsec VPN

1. **Establish ISAKMP policy**
2. **Configure IPsec transform set**
3. **Configure crypto ACL**
4. **Configure crypto map**
5. **Apply crypto map to the interface**
6. **Configure interface ACL**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-16

The steps to configure a site-to-site IPsec VPN are as follows:

Step 1 Configure the ISAKMP policy required to establish an IKE tunnel.

Step 2 Define the IPsec transform set. The definition of the transform set defines the parameters used for the IPsec tunnel, such as encryption and integrity algorithms.

Step 3 Create a crypto access control list (ACL). The crypto ACL defines which traffic should be sent through the IPsec tunnel.

Step 4 Create a crypto map. The crypto map maps the previously configured parameters together and defines the IPsec peer device.

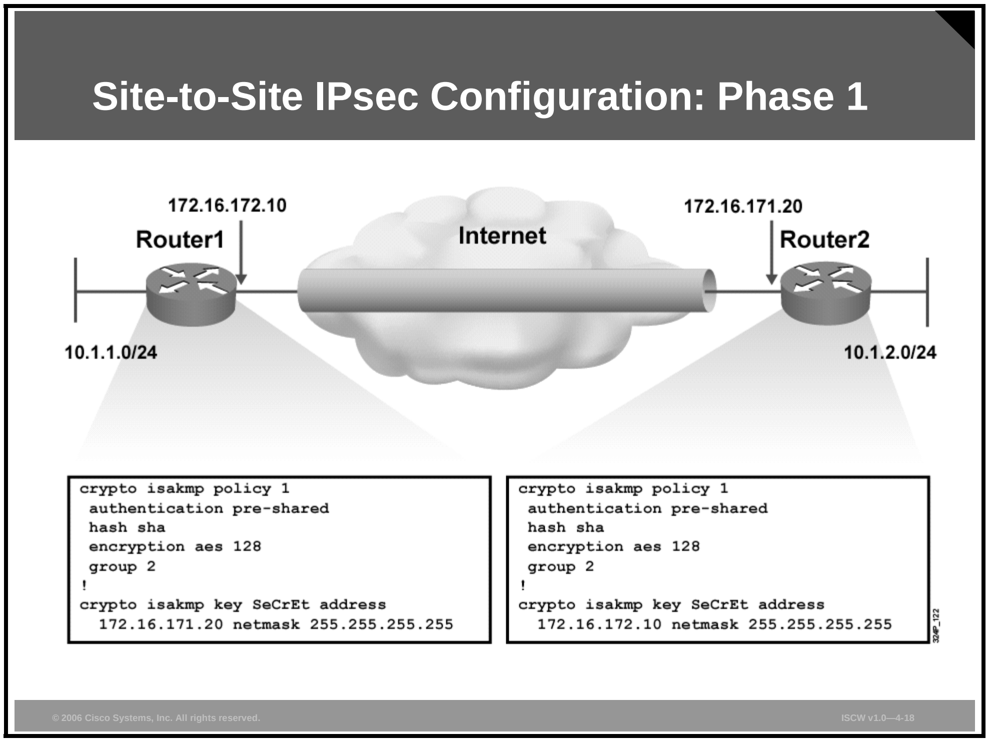
Step 5 Apply the crypto map. The crypto map is applied to the outgoing interface of the VPN device.

Step 6 Configure an ACL and apply it to the interface. Usually there are some restrictions on the interface which is used for VPN traffic, such as blocking all traffic which is not IPsec or IKE.

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

Site-to-Site IPsec Configuration: Phase 1

This topic describes the configuration of the ISAKMP parameters.



Site-to-Site IPsec Configuration: Phase 1

```
crypto isakmp policy 1
 authentication pre-shared
 hash sha
 encryption aes 128
 group 2
!
crypto isakmp key SeCrEt address
  172.16.171.20 netmask 255.255.255.255
```

```
crypto isakmp policy 1
 authentication pre-shared
 hash sha
 encryption aes 128
 group 2
!
crypto isakmp key SeCrEt address
  172.16.172.10 netmask 255.255.255.255
```

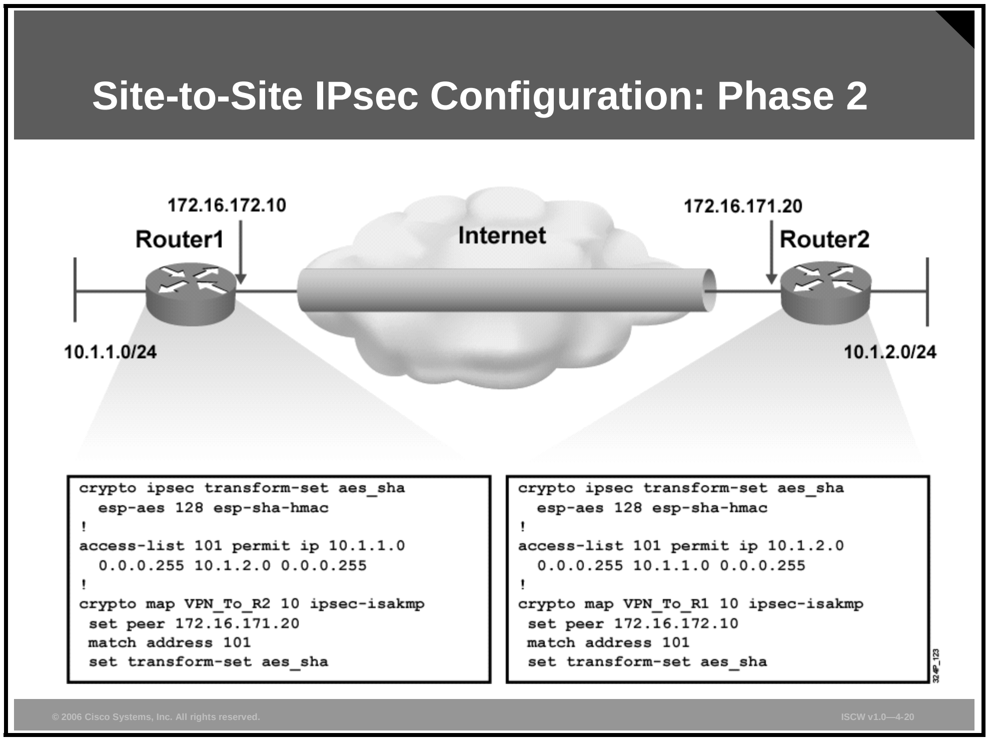
© 2006 Cisco Systems, Inc. All rights reserved.

The first step when configuring a site-to-site IPsec VPN is establishment of ISAKMP policy. The figure shows the configuration of the ISAKMP parameters. In the example, preshared authentication is used with the key “SeCrEt” to the IPsec peer.

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

Site-to-Site IPsec Configuration: Phase 2

This topic describes the configuration to define the IPsec transform set, the crypto ACL, and the crypto map.



Site-to-Site IPsec Configuration: Phase 2

```
crypto ipsec transform-set aes_sha
  esp-aes 128 esp-sha-hmac
!
access-list 101 permit ip 10.1.1.0
  0.0.0.255 10.1.2.0 0.0.0.255
!
crypto map VPN_To_R2 10 ipsec-isakmp
 set peer 172.16.171.20
 match address 101
 set transform-set aes_sha
```

```
crypto ipsec transform-set aes_sha
  esp-aes 128 esp-sha-hmac
!
access-list 101 permit ip 10.1.2.0
  0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map VPN_To_R1 10 ipsec-isakmp
 set peer 172.16.172.10
 match address 101
 set transform-set aes_sha
```

The next step when configuring a site-to-site IPsec VPN is configuration of an IPsec transform set, a crypto access list, and a crypto map. The configuration defines the crypto ACL. This ACL states a “permit” entry for the traffic which should be sent into the IPsec tunnel. If packets are not matching, they are just not encrypted but they are not dropped.

After the parameters are defined, they are mapped with the crypto map configuration. The crypto map (for example, VPN_To_R2) maps the configured ACL with the transform set (IPsec parameters). Additionally, it defines the IP address of the IPsec peer.

Crypto map entries created for IPsec pull together the various parts used to set up IPsec SAs, including the following:

- Which traffic should be protected by IPsec (per a crypto ACL)
- The granularity of the flow to be protected by a set of SAs
- Where IPsec-protected traffic should be sent (who the remote IPsec peer is)
- The local address to be used for the IPsec traffic (optional)
- What IPsec security should be applied to this traffic (selecting from a list of one or more transform sets)

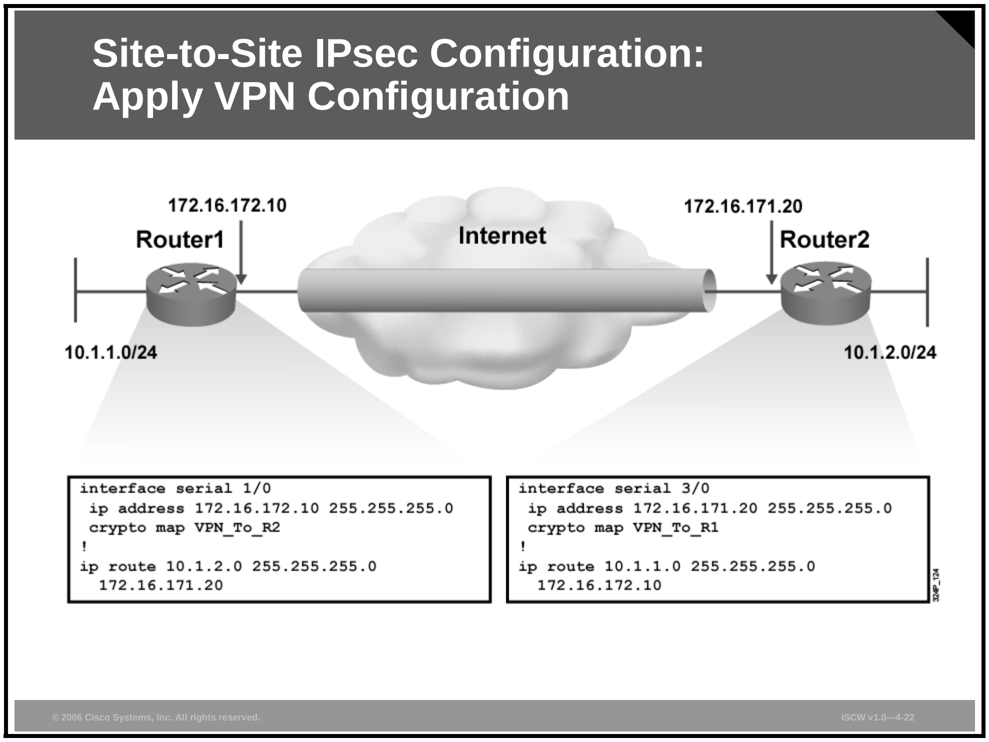
Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set.

All IP traffic passing through the interface in which the crypto map is applied is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, an SA is negotiated with the remote peer according to the parameters included in the crypto map entry.

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

Site-to-Site IPsec Configuration: Apply VPN Configuration

This topic describes the configuration to apply the crypto map to the interface.



Site-to-Site IPsec Configuration:
Apply VPN Configuration

```
interface serial 1/0
 ip address 172.16.172.10 255.255.255.0
 crypto map VPN_To_R2
!
ip route 10.1.2.0 255.255.255.0
  172.16.171.20
```

```
interface serial 3/0
 ip address 172.16.171.20 255.255.255.0
 crypto map VPN_To_R1
!
ip route 10.1.1.0 255.255.255.0
  172.16.172.10
```

© 2006 Cisco Systems, Inc. All rights reserved.

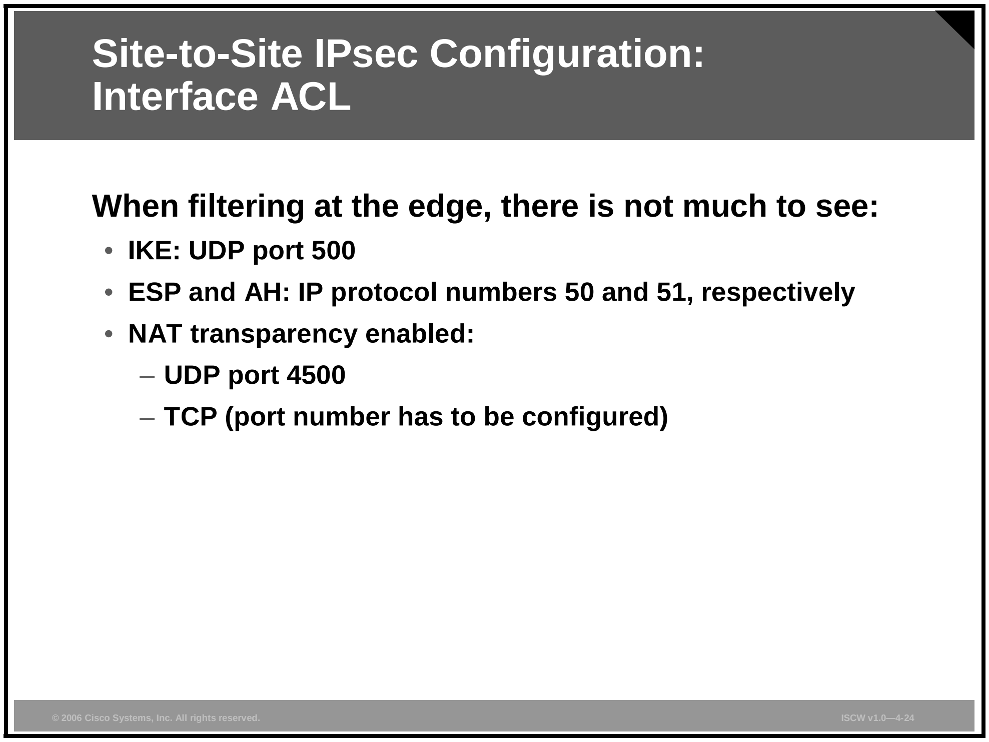
ISCW v1.0—4-22

In the last part of the IPsec configuration, the crypto map is applied to the interface. The crypto map is placed on the outgoing interface of the VPN tunnel. The example also shows static route configuration for packets to be sent into the tunnel.

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

Site-to-Site IPsec Configuration: Interface ACL

This topic describes how to configure an interface ACL for IPsec.



Site-to-Site IPsec Configuration: Interface ACL

When filtering at the edge, there is not much to see:

- **IKE: UDP port 500**
- **ESP and AH: IP protocol numbers 50 and 51, respectively**
- **NAT transparency enabled:**
  - **UDP port 4500**
  - **TCP (port number has to be configured)**

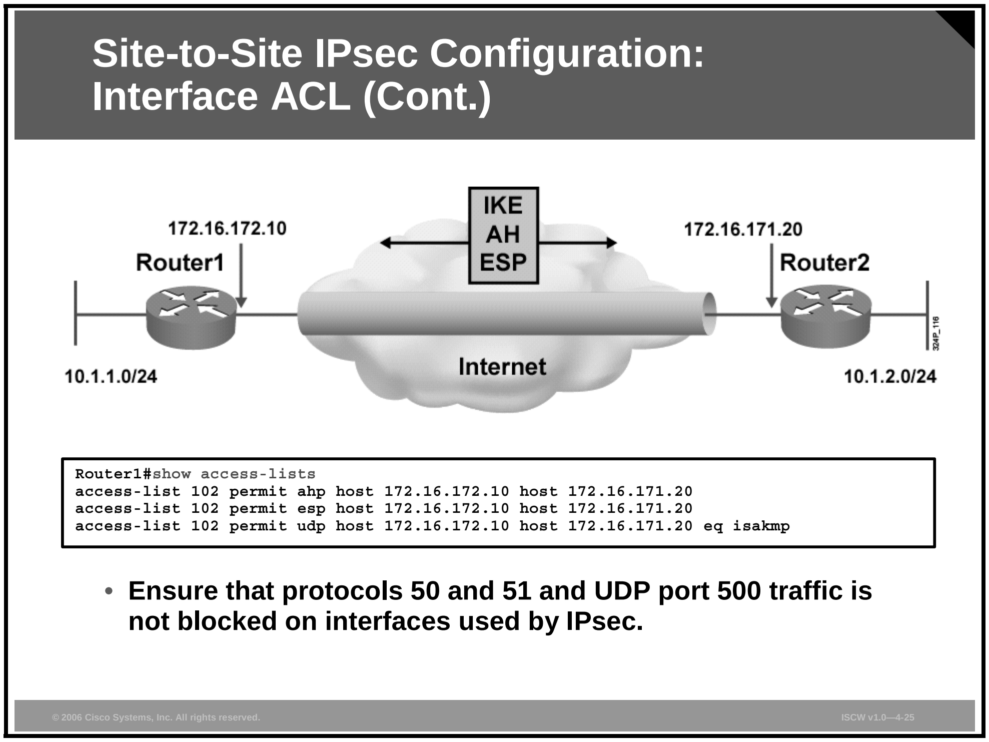
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-24

In a typical scenario, using only IPsec VPN on the router interface, any traffic not passing the secured IPsec VPN would be blocked. To block traffic, you can define an ACL and apply it to all incoming packets on your IPsec interface. Usually you have to enable only the IPsec protocols (protocol 50 for ESP or protocol 51 for Authentication Header [AH]) and IKE (User Datagram Protocol [UDP] port 500).

If there is any dynamic routing done on the interface, do not forget to permit the routing traffic.

The IPsec NAT Traversal feature is required for passing the IPsec traffic through devices using Network Address Translation (NAT) or Port Address Translation (PAT). This is accomplished by wrapping (encapsulating) the IPsec packet with a UDP header.

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



Site-to-Site IPsec Configuration: Interface ACL (Cont.)

```
Router1#show access-lists
access-list 102 permit ahp host 172.16.172.10 host 172.16.171.20
access-list 102 permit esp host 172.16.172.10 host 172.16.171.20
access-list 102 permit udp host 172.16.172.10 host 172.16.171.20 eq isakmp
```

- **Ensure that protocols 50 and 51 and UDP port 500 traffic is not blocked on interfaces used by IPsec.**

© 2006 Cisco Systems, Inc. All rights reserved.

Ensure that your ACLs are configured so that ISAKMP, ESP, and AH traffic is not blocked at interfaces used by IPsec. ISAKMP uses UDP port 500, ESP is assigned IP protocol number 50, and AH is assigned IP protocol number 51. In some cases, you might need to follow these steps to add a statement to the ACLs on the perimeter router to explicitly permit this traffic:

Step 1 Examine the current ACL configuration at the perimeter router to determine if it will block IPsec traffic.

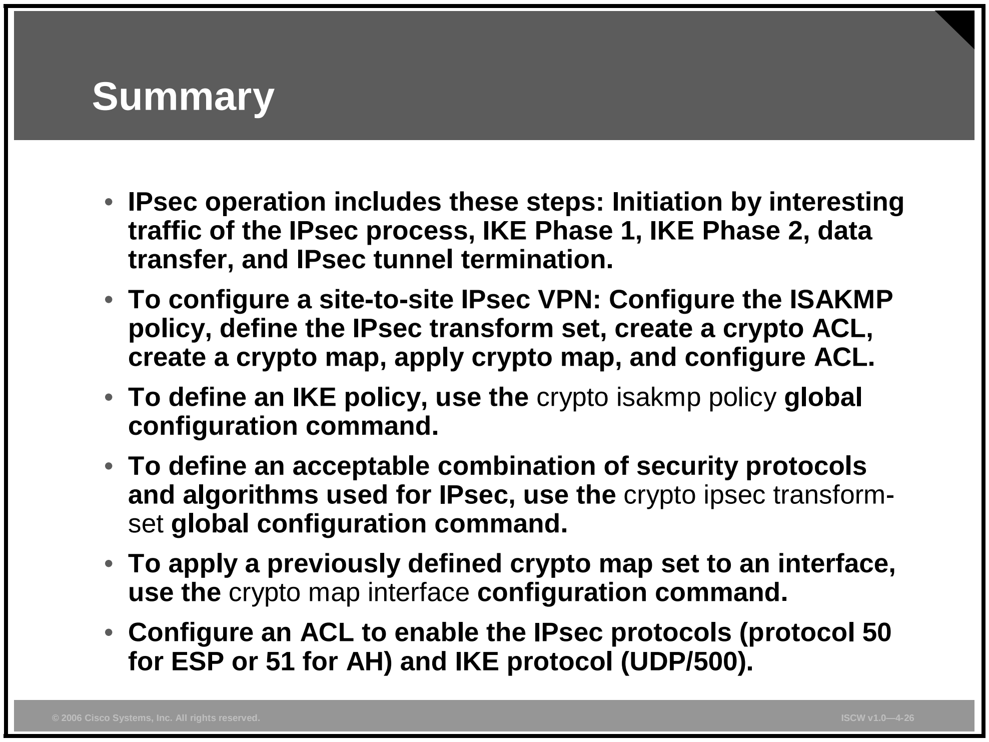
Step 2 Add ACL entries to permit IPsec traffic. To do this, copy the existing ACL configuration and paste it into a text editor.

The example in the figure represents an ACL where AH, ESP, and ISAKMP protocols are permitted between two hosts. The protocol keyword of **esp** equals the ESP protocol (number 50), the keyword of **ahp** equals the AH protocol (number 51), and the **isakmp** keyword equals UDP port 500.

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

Summary

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



Summary

- **IPsec operation includes these steps: Initiation by interesting traffic of the IPsec process, IKE Phase 1, IKE Phase 2, data transfer, and IPsec tunnel termination.**
- **To configure a site-to-site IPsec VPN: Configure the ISAKMP policy, define the IPsec transform set, create a crypto ACL, create a crypto map, apply crypto map, and configure ACL.**
- **To define an IKE policy, use the** crypto isakmp policy **global configuration command.**
- **To define an acceptable combination of security protocols and algorithms used for IPsec, use the** crypto ipsec transform-set **global configuration command.**
- **To apply a previously defined crypto map set to an interface, use the** crypto map interface **configuration command.**
- **Configure an ACL to enable the IPsec protocols (protocol 50 for ESP or 51 for AH) and IKE protocol (UDP/500).**

© 2006 Cisco Systems, Inc. All rights reserved.　ISCW v1.0—4-26

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

Lesson 3

Configuring IPsec Site-to-Site VPN Using SDM

Overview

This lesson describes the configuration steps to implement an IPsec site-to-site virtual private network (VPN) using the Cisco Security Device Manager (SDM).

Objectives

Upon completing this lesson, you will be able to describe the procedure to configure a site-to-site IPsec VPN with preshared key authentication using SDM, and explain the resulting command-line interface (CLI) configurations. This ability includes being able to meet these objectives:

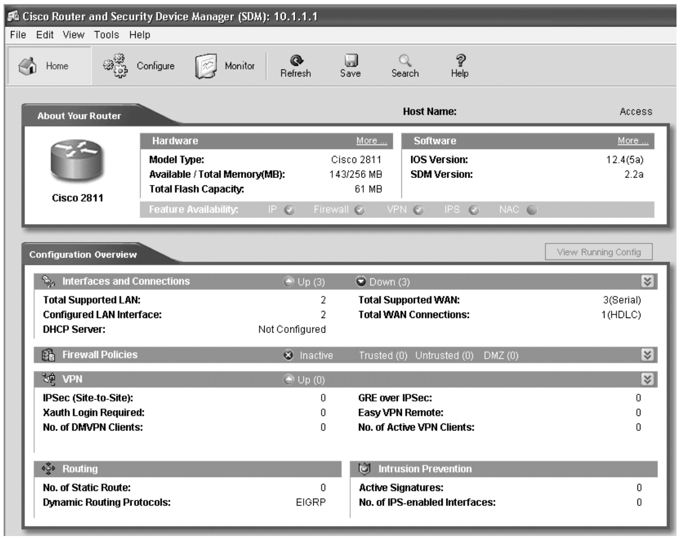
- Describe how to navigate the site-to-site VPN wizard interface
- Describe the components that will be configured by the SDM site-to-site VPN wizard
- Explain how to launch the site-to-site VPN wizard
- Explain how to set the parameters of the site-to-site VPN tunnel
- Explain how SDM sets IKE policies
- Explain how to select a transform set and associate additional transform sets as required
- Explain how to define the traffic that the VPN protects
- Explain how to complete the configuration by viewing the settings in the Summary window

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

Introducing the SDM VPN Wizard Interface

This topic describes how to navigate the site-to-site VPN wizard interface.

Cisco Router and SDM



Cisco Router and Security Device Manager (SDM): 10.1.1.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
More ...
More ...
View Running Config

About Your Router

Host Name: Access

Cisco 2811

Hardware

Model Type: Cisco 2811
Available / Total Memory(MB): 143/256 MB
Total Flash Capacity: 61 MB

Software

IOS Version: 12.4(5a)
SDM Version: 2.2a

Feature Availability: IP ✓ Firewall ✓ VPN ✓ IPS ✓ NAC ●

Configuration Overview

Interfaces and Connections ▲ Up (3) ▼ Down (3)

Total Supported LAN: 2
Configured LAN Interface: 2
DHCP Server: Not Configured
Total Supported WAN: 3(Serial)
Total WAN Connections: 1(HDLC)

Firewall Policies ☒ Inactive Trusted (0) Untrusted (0) DMZ (0)

VPN ▲ Up (0)

IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0

Routing

No. of Static Route: 0
Dynamic Routing Protocols: EIGRP

Intrusion Prevention

Active Signatures: 0
No. of IPS-enabled Interfaces: 0

© 2006 Cisco Systems, Inc. All rights reserved.

The main page of the SDM consists of two sections:

- **About Your Router:** This section displays the hardware and software configuration of the router.
- **Configuration Overview:** This section displays basic traffic statistics.

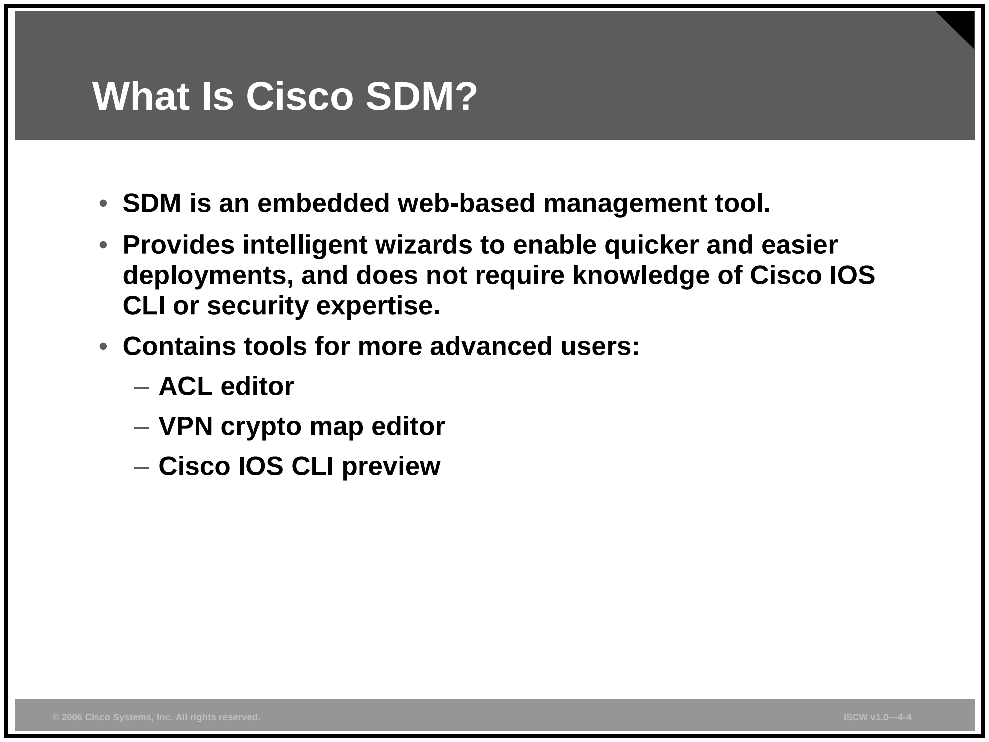
There are two important icons in the top horizontal navigation bar:

- The **Configure** icon enters the configuration page.
- The **Monitor** icon enters the page where the status of the tunnels, interfaces, and device can be monitored.

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

Security Device Manager

SDM is an easy-to-use Internet browser-based device management tool that is embedded within the Cisco IOS 800–3800 Series routers at no cost.



What Is Cisco SDM?

- SDM is an embedded web-based management tool.
- Provides intelligent wizards to enable quicker and easier deployments, and does not require knowledge of Cisco IOS CLI or security expertise.
- Contains tools for more advanced users:
  - ACL editor
  - VPN crypto map editor
  - Cisco IOS CLI preview

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-4

SDM simplifies router and security configuration through the use of intelligent wizards to enable customers and partners to quickly and easily deploy, configure, and monitor a Cisco access router.

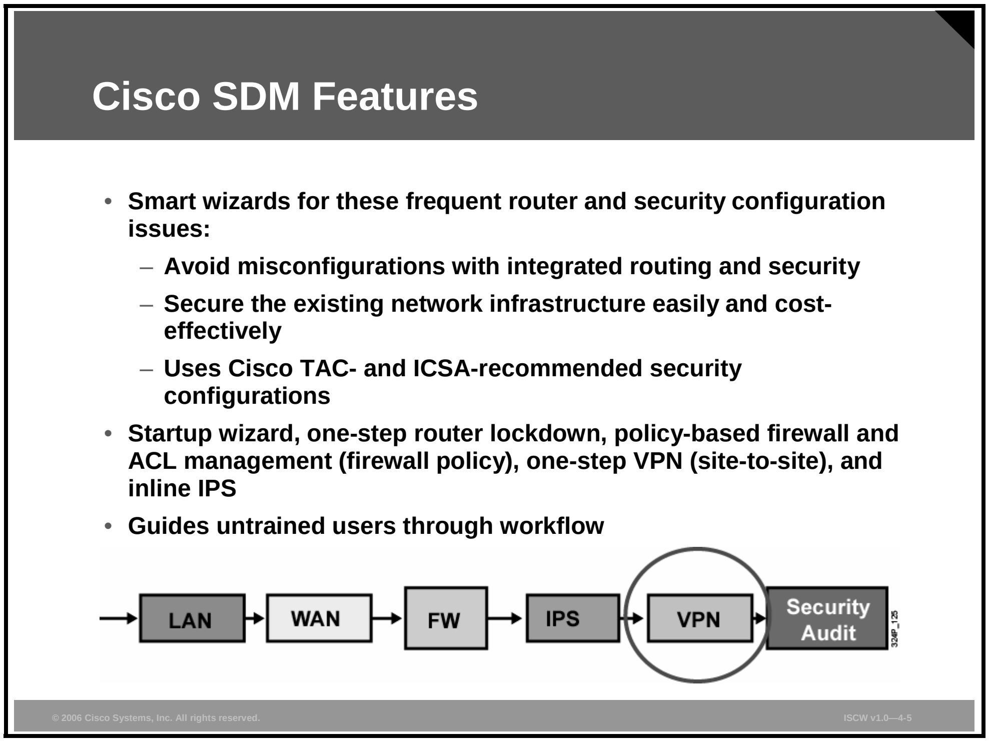
SDM is designed for resellers and network administrators of small- to medium-sized businesses, who are proficient in LAN fundamentals and basic network design but have little or no experience with the Cisco IOS CLI, or may not be security experts.

SDM also assists advanced users. It contains several time-saving tools, such as an access control list (ACL) editor, VPN crypto map editor, Cisco IOS CLI preview, and many more.

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

Cisco SDM Features

SDM has a unique Security Audit wizard that provides a comprehensive router security audit. SDM uses Cisco Technical Assistance Center (TAC) and Internet Computer Security Association (ICSA) recommended security configurations as its basis for comparisons and default settings.



Cisco SDM Features

- Smart wizards for these frequent router and security configuration issues:
  - Avoid misconfigurations with integrated routing and security
  - Secure the existing network infrastructure easily and cost-effectively
  - Uses Cisco TAC- and ICSA-recommended security configurations
- Startup wizard, one-step router lockdown, policy-based firewall and ACL management (firewall policy), one-step VPN (site-to-site), and inline IPS
- Guides untrained users through workflow

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-5

Other intelligent wizards are also available for these tasks:

- Autodetect misconfigurations and propose fixes
- Provide strong security and verify configuration entries
- Use device and interface-specific defaults

Examples of SDM wizards include the following:

- Startup wizard for initial router configuration
- One-step router lockdown wizard to harden the router
- Policy-based firewall and access-list management to easily configure firewall settings based on policy rules
- One-step site-to-site VPN wizard

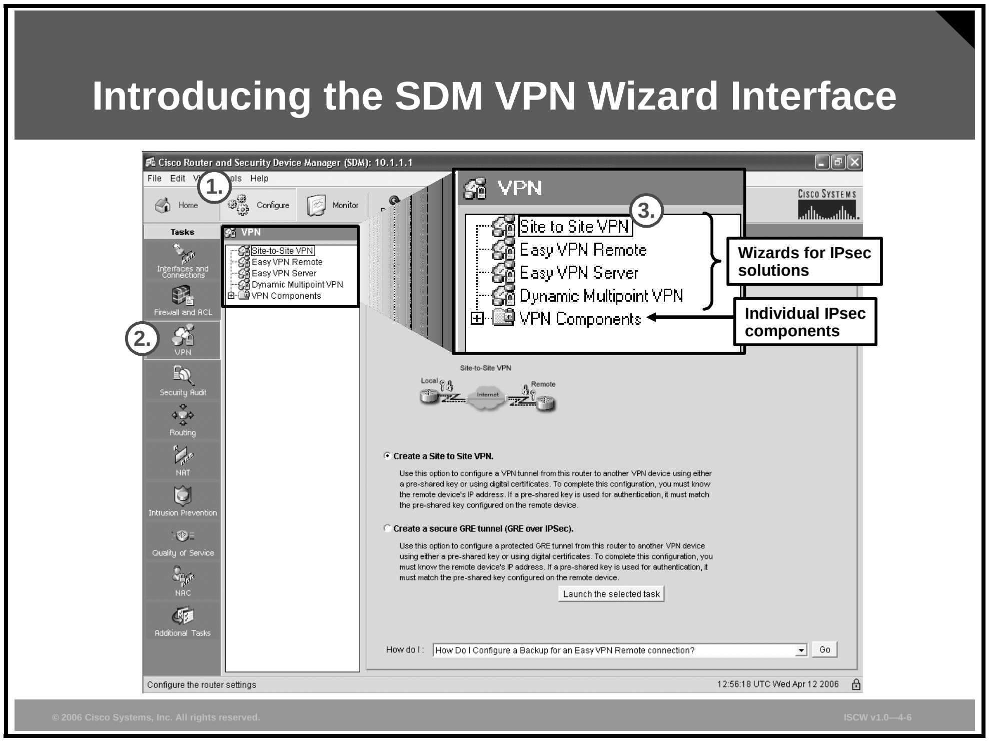
Use the SDM wizards to provide a quick deployment. A suggested workflow is given in the lower part of the screens to guide untrained users through the process.

Begin with configuring LAN, WAN, firewall, intrusion prevention system (IPS), and VPN, and finish with a security audit.

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

Introducing the SDM VPN Wizard Interface

The VPN configuration page lists VPN wizards that help implement different types of IPsec VPNs.



Introducing the SDM VPN Wizard Interface

● **Create a Site to Site VPN.**

Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

○ **Create a secure GRE tunnel (GRE over IPSec).**

Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

How do I : How Do I Configure a Backup for an Easy VPN Remote connection?

12:56:18 UTC Wed Apr 12 2006

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-6

To select and start a VPN wizard, follow this procedure:

Step 1 Click the **Configure** icon in the top horizontal navigation bar to enter the configuration page.

Step 2 Click the **VPN** icon in the left vertical navigation bar to open the VPN page.

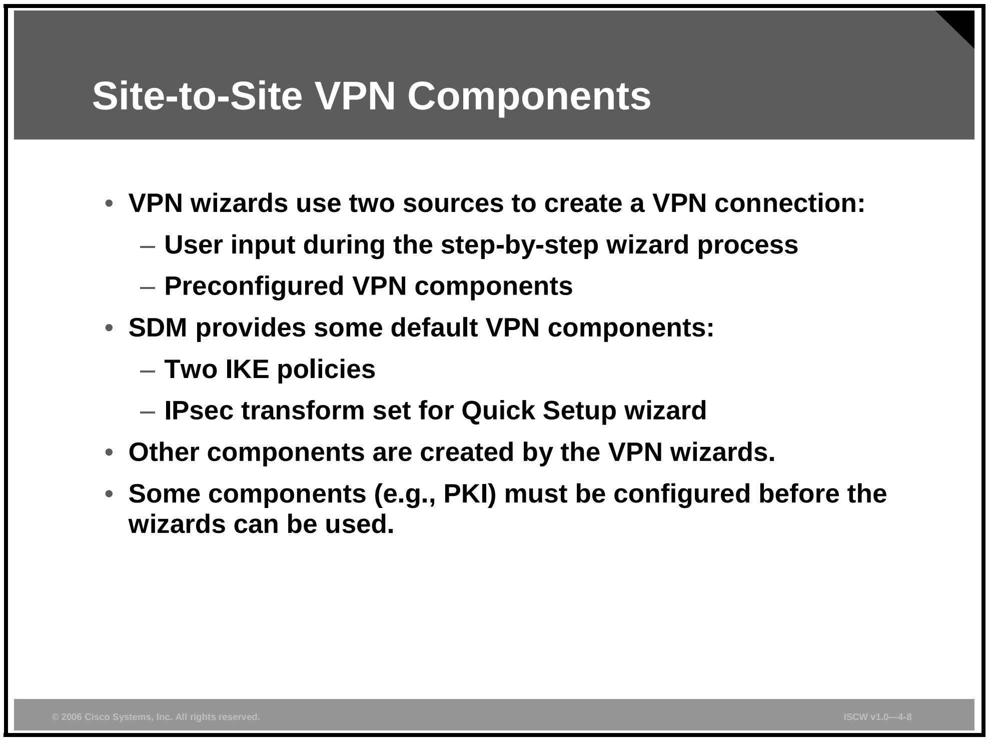
Step 3 Choose the **Site to Site VPN** wizard from the list.

Here you can create two types of site-to-site VPNs: classic and Generic Routing Encapsulation (GRE) over IPsec.

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

Site-to-Site VPN Components

This topic describes the components and the resulting Cisco IOS configuration that will be configured by the SDM site-to-site VPN wizard.



Site-to-Site VPN Components

- **VPN wizards use two sources to create a VPN connection:**
  - **User input during the step-by-step wizard process**
  - **Preconfigured VPN components**
- **SDM provides some default VPN components:**
  - **Two IKE policies**
  - **IPsec transform set for Quick Setup wizard**
- **Other components are created by the VPN wizards.**
- **Some components (e.g., PKI) must be configured before the wizards can be used.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-8

The VPN wizards of the SDM use two sources to create a VPN connection:

- User input during the step-by-step wizard process
- Preconfigured VPN components

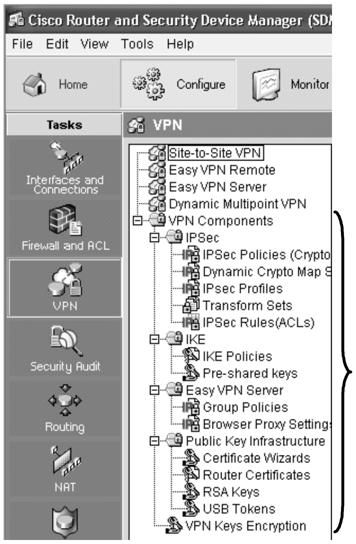
The SDM provides some default VPN components:

- Two Internet Key Exchange (IKE) policies
- IPsec transform set for the Quick Setup wizard

Other components are created by the VPN wizards during the step-by-step configuration process. Some components must be configured before the wizards can be used (for example, Public Key Infrastructure [PKI]).

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

Site-to-Site VPN Components (Cont.)



Individual IPsec components used to build VPNs

- **Two main components:**
  - **IPsec**
  - **IKE**
- **Two optional components:**
  - **Group Policies for Easy VPN server functionality**
  - **Public Key Infrastructure for IKE authentication using digital certificates**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-9

The figure illustrates the VPN navigation bar, which contains two major sections:

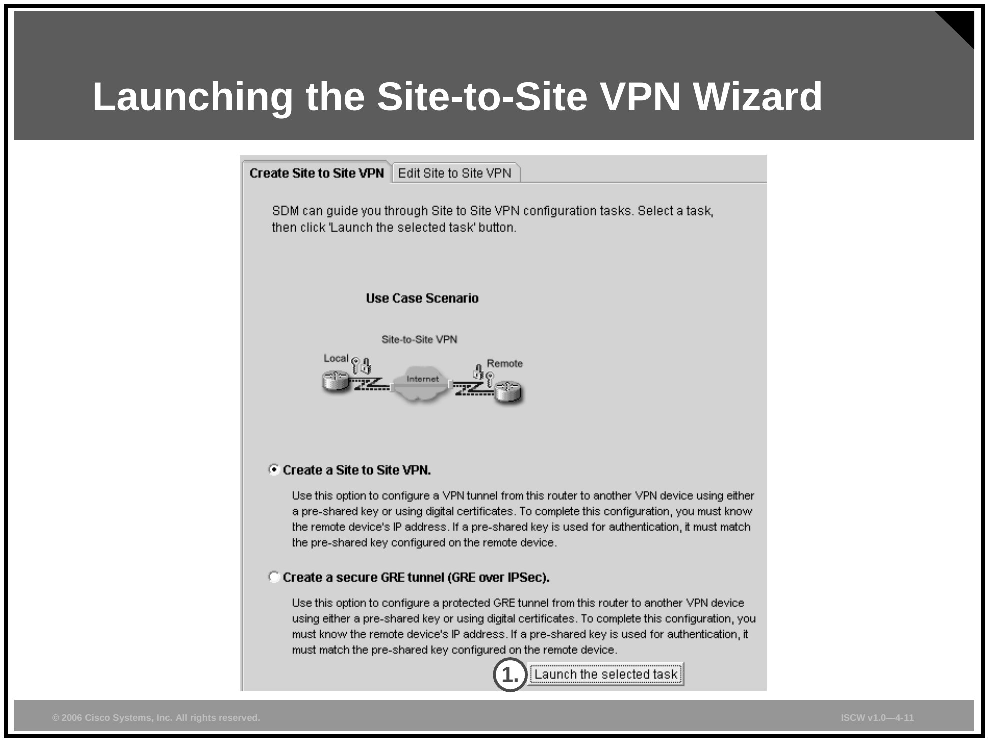
- VPN wizards, at the top:
  - Site-to-Site VPN
  - Easy VPN Remote
  - Easy VPN Server
  - Dynamic Multipoint VPN
- Individual IPsec components below:
  - Main components:
    - IPSec
    - IKE
  - Optional components:
    - Group Policies (for easy VPN server functionality)
    - Public Key Infrastructure (for IKE authentication using digital certificates)
  - The VPN Key Encryption Settings window appears if the Cisco IOS image on your router supports Type 6 encryption, also referred to as VPN key encryption. You can use this window to specify a master key to use when encrypting VPN keys, such as preshared keys, Easy VPN keys, and Xauth keys. When encrypted, these keys will not be readable by someone viewing the router configuration file.

The VPN wizards are used to simplify the configuration of individual VPN components. The individual IPsec components section can be used later to modify some parameters that may have been misconfigured during the VPN wizard step-by-step 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 self-study.

Launching the Site-to-Site VPN Wizard

This topic describes how to launch the site-to-site VPN wizard.



Launching the Site-to-Site VPN Wizard

SDM can guide you through Site to Site VPN configuration tasks. Select a task, then click 'Launch the selected task' button.

Use Case Scenario

● **Create a Site to Site VPN.**

Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

○ **Create a secure GRE tunnel (GRE over IPSec).**

Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

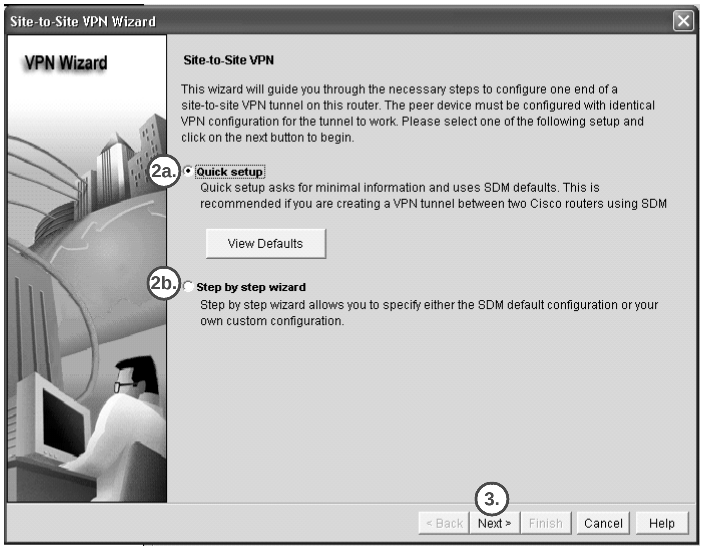
© 2006 Cisco Systems, Inc. All rights reserved.

Use a web browser to connect to an HTTP server of a router. Select the VPN wizard by choosing **Configure > VPN > Site to Site VPN**. To create and configure a classic site-to-site VPN:

Step 1 Click the **Create a Site to Site VPN** radio button and click the **Launch the selected task** button.

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

Launching the Site-to-Site VPN Wizard (Cont.)



Site-to-Site VPN

This wizard will guide you through the necessary steps to configure one end of a site-to-site VPN tunnel on this router. The peer device must be configured with identical VPN configuration for the tunnel to work. Please select one of the following setup and click on the next button to begin.

● **Quick setup**
Quick setup asks for minimal information and uses SDM defaults. This is recommended if you are creating a VPN tunnel between two Cisco routers using SDM

○ **Step by step wizard**
Step by step wizard allows you to specify either the SDM default configuration or your own custom configuration.

© 2006 Cisco Systems, Inc. All rights reserved.

Step 2 A window will open, asking you which wizard mode to use:

a. The **Quick setup** uses SDM-default IKE policies and IPsec transform sets.

b. The **Step by step wizard** allows you to specify all the details.

Step 3 Click the **Next** button to configure the parameters of the VPN connection.

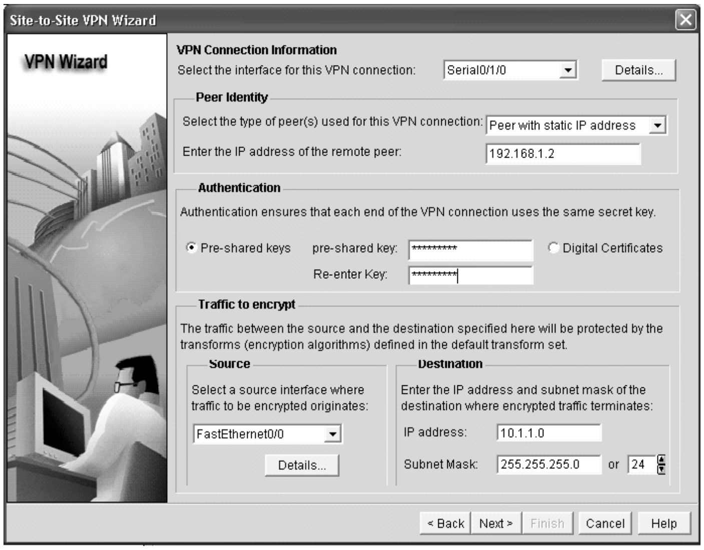
© 2006 Cisco Systems, Inc.

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 self-study.

Quick Setup

The first of the two wizard modes is the quick setup, which requires a single window to complete the configuration of the VPN.

Quick Setup



Site-to-Site VPN Wizard

VPN Wizard

VPN Connection Information

Select the interface for this VPN connection: Serial0/1/0

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 192.168.1.2

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

● Pre-shared keys pre-shared key: ********* ○ Digital Certificates

Re-enter Key: *********

Traffic to encrypt

The traffic between the source and the destination specified here will be protected by the transforms (encryption algorithms) defined in the default transform set.

Source

Select a source interface where traffic to be encrypted originates: FastEthernet0/0

Destination

Enter the IP address and subnet mask of the destination where encrypted traffic terminates:

IP address: 10.1.1.0

Subnet Mask: 255.255.255.0 or 24

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-13

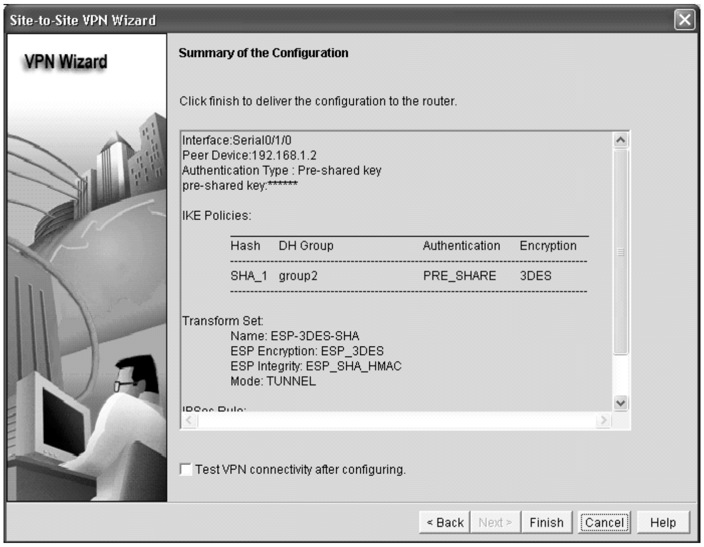
The quick setup includes these parameters:

- Outside interface
- IP address of the peer
- Authentication method:
  - Preshared keys (specify the secret)
  - Digital certificates (select a certificate that was created earlier)
- Traffic to encrypt:
  - Coming from IP subnet configured on the selected source interface
  - Going to defined remote IP subnet

When done, click the **Next** button to proceed.

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

Quick Setup (Cont.)



Summary of the Configuration

Click finish to deliver the configuration to the router.

```
Interface:Serial0/1/0
Peer Device:192.168.1.2
Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

          Hash    DH Group                 Authentication    Encryption
          -------------------------------------------------------------
          SHA_1   group2                   PRE_SHARE         3DES
          -------------------------------------------------------------

Transform Set:
          Name: ESP-3DES-SHA
          ESP Encryption: ESP_3DES
          ESP Integrity: ESP_SHA_HMAC
          Mode: TUNNEL

IPSec Rule:
```

□ Test VPN connectivity after configuring.

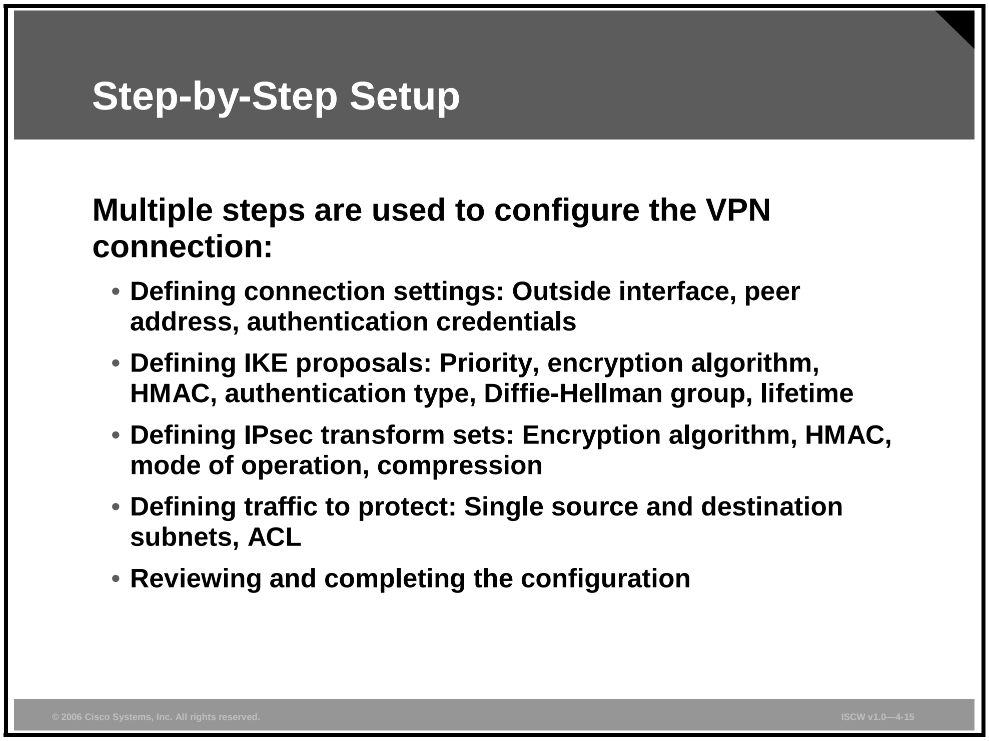
© 2006 Cisco Systems, Inc. All rights reserved.

A window opens, summarizing all the parameters of the site-to-site VPN connection that you configured. Click the **Back** button if you wish to change any of the parameters, or the **Finish** button to apply the parameters.

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

Step-by-Step Setup

The second of the two wizard modes is the step-by-step wizard, which requires multiple steps to configure the VPN connection.



Step-by-Step Setup

Multiple steps are used to configure the VPN connection:

- **Defining connection settings: Outside interface, peer address, authentication credentials**
- **Defining IKE proposals: Priority, encryption algorithm, HMAC, authentication type, Diffie-Hellman group, lifetime**
- **Defining IPsec transform sets: Encryption algorithm, HMAC, mode of operation, compression**
- **Defining traffic to protect: Single source and destination subnets, ACL**
- **Reviewing and completing the configuration**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-15

The step-by-step setup includes these parameters:

- **Connection settings:** Outside interface, peer address, and authentication credentials
- **IKE proposals:** IKE proposal priority, encryption algorithm (Data Encryption Standard [DES], Triple Data Encryption Standard [3DES], Advanced Encryption Standard [AES], or Software Encryption Algorithm [SEAL]), Hashed Message Authentication Code (HMAC) (Secure Hash Algorithm 1 [SHA-1] or Message Digest 5 [MD5]), IKE authentication method (preshared secrets or digital certificates), Diffie-Hellman group (1, 2, or 5), and IKE lifetime
- **IPsec transform sets:** Encryption algorithm (DES, 3DES, AES, or SEAL), HMAC (SHA-1 or MD5), mode of operation (tunnel or transport), and compression
- **Traffic to protect:** Defining single source and destination subnets, or an ACL for more complex VPNs

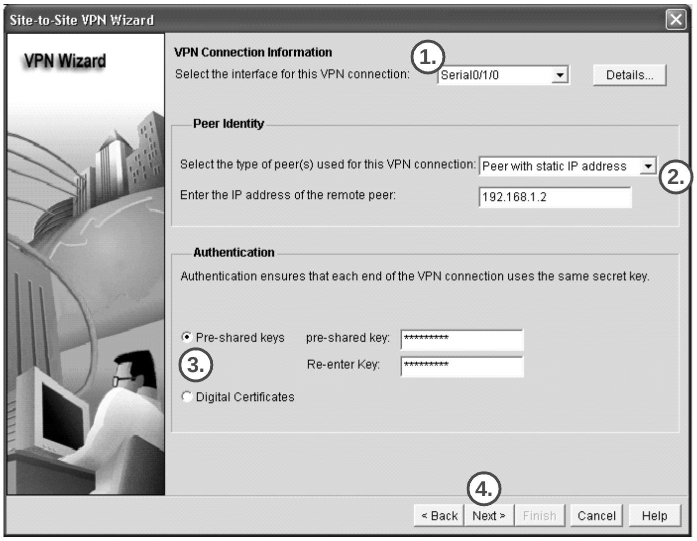
The last task of the step-by-step wizard is reviewing and completing the configuration.

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 self-study.

Connection Settings

This topic describes how to identify the IP address or host name of the remote site that will terminate the VPN tunnel, how to specify the router interface to use, and how to enter the preshared key that both routers will use to authenticate each other.

Connection Settings



Site-to-Site VPN Wizard

VPN Wizard

VPN Connection Information

Select the interface for this VPN connection: Serial0/1/0 [Details...]

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 192.168.1.2

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

● Pre-shared keys pre-shared key: ********* Re-enter Key: *********

○ Digital Certificates

< Back | Next > | Finish | Cancel | Help

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-17

The first task in the step-by-step setup is to configure the connection:

Step 1 Choose the outside interface for towards the IPsec peer over the untrusted network.

Step 2 Specify the IP address of the peer.

Step 3 Choose the authentication method and specify credentials. Use long and random preshared keys to prevent brute-force and dictionary attacks against IKE.

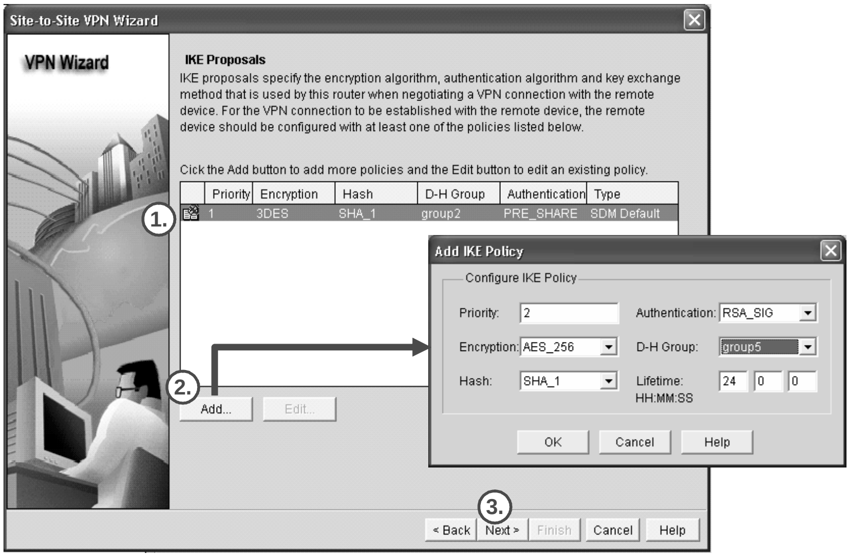
Step 4 Click the **Next** button to proceed to the next task.

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

IKE Proposals

This topic explains how SDM sets IKE policies.

IKE Proposals



Site-to-Site VPN Wizard

VPN Wizard

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Cick the Add button to add more policies and the Edit button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	SDM Default

Add IKE Policy

Configure IKE Policy

Priority: 2

Encryption: AES_256

Hash: SHA_1

Authentication: RSA_SIG

D-H Group: group5

Lifetime: HH:MM:SS 24 0 0

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-19

The second task in the step-by-step setup is to configure IKE proposals:

Step 1 You can use the IKE proposal predefined by SDM.

Step 2 If you want to use a custom IKE proposal, define it by clicking the **Add** button and specifying the required parameters:

— IKE proposal priority

— Encryption algorithm

— HMAC

— IKE authentication method

— Diffie-Hellman group

— IKE lifetime

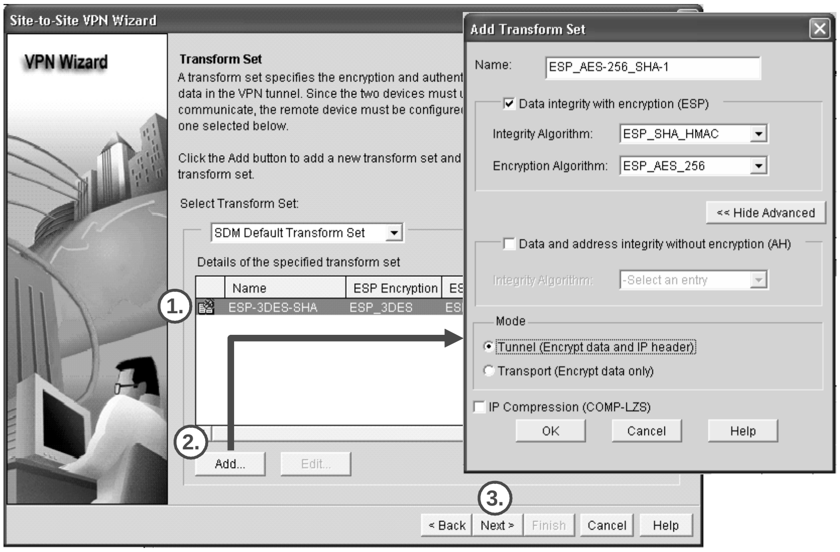
Step 3 When you are finished with adding IKE policies, click the **Next** button to proceed to the next task.

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

Transform Set

This topic describes how to select a transform set and associate additional transform sets to the VPN connection.

Transform Set



Site-to-Site VPN Wizard

VPN Wizard

Transform Set

A transform set specifies the encryption and authent data in the VPN tunnel. Since the two devices must u communicate, the remote device must be configure one selected below.

Click the Add button to add a new transform set and transform set.

Select Transform Set: SDM Default Transform Set

Details of the specified transform set

Name	ESP Encryption	ES
ESP-3DES-SHA	ESP_3DES	ES

Add Transform Set

Name: ESP_AES-256_SHA-1

☑ Data integrity with encryption (ESP)

Integrity Algorithm: ESP_SHA_HMAC

Encryption Algorithm: ESP_AES_256

☐ Data and address integrity without encryption (AH)

Integrity Algorithm: -Select an entry

Mode

● Tunnel (Encrypt data and IP header)

○ Transport (Encrypt data only)

☐ IP Compression (COMP-LZS)

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-21

The third task in the step-by-step setup is configuring a transform set:

Step 1 You can use the IPsec transform set predefined by SDM.

Step 2 If you want to use a custom IPsec transform set, define it by clicking the **Add** button and specifying these parameters:

— Transform set name

— Encryption algorithm

— HMAC

— Mode of operation

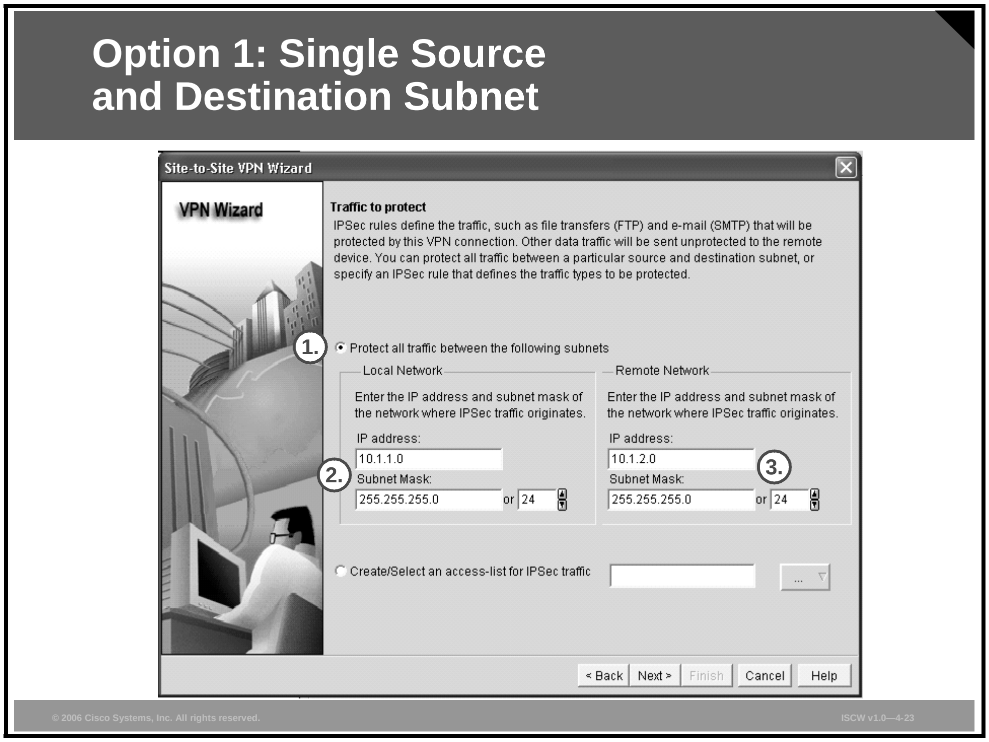
— Optional compression

Step 3 When finished, click the **Next** button to proceed to the next task.

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

Defining What Traffic to Protect

This topic describes how to define the traffic that the VPN protects.



Option 1: Single Source and Destination Subnet

Site-to-Site VPN Wizard

VPN Wizard

Traffic to protect

IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

1. ● Protect all traffic between the following subnets

Local Network

Enter the IP address and subnet mask of the network where IPSec traffic originates.

IP address: 10.1.1.0

2. Subnet Mask: 255.255.255.0 or 24

Remote Network

Enter the IP address and subnet mask of the network where IPSec traffic originates.

IP address: 10.1.2.0

3. Subnet Mask: 255.255.255.0 or 24

○ Create/Select an access-list for IPSec traffic

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-23

Option 1: Single Source and Destination Subnet

To define the traffic that needs protection, you can use the simple mode, allowing protection of traffic between one pair of IP subnets.

To protect traffic between a particular pair of IP subnets, follow these steps:

Step 1 Click the **Protect all traffic between the following subnets** radio button.

Step 2 Define IP address and subnet mask of the local network where IPsec traffic originates.

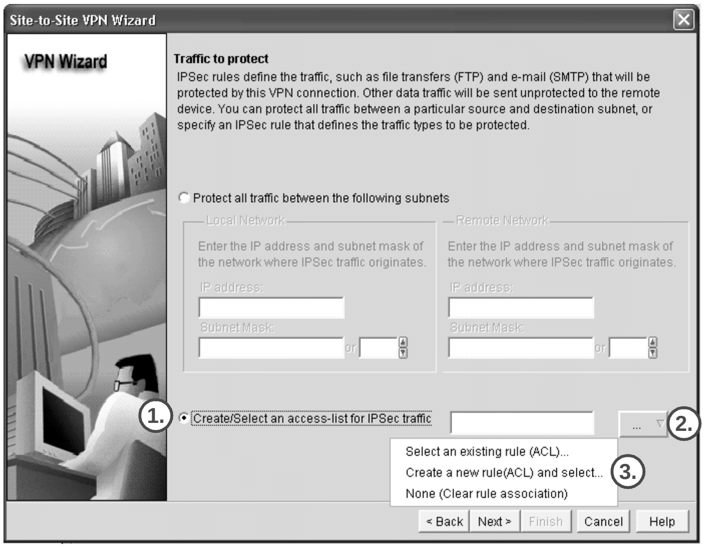
Step 3 Define IP address and subnet mask of the remote network where IPsec traffic is sent.

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

Option 2: Using an ACL

Alternatively, you can use an ACL to define a more complex set of proxy identities.

Option 2: Using an ACL



Site-to-Site VPN Wizard

Traffic to protect

IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

○ Protect all traffic between the following subnets

Local Network: Enter the IP address and subnet mask of the network where IPSec traffic originates.

Remote Network: Enter the IP address and subnet mask of the network where IPSec traffic originates.

● Create/Select an access-list for IPSec traffic

VPN Wizard
IP address:
Subnet Mask:
or
1.
...
2.
Select an existing rule (ACL)...
Create a new rule(ACL) and select...
None (Clear rule association)
3.
< Back
Next >
Finish
Cancel
Help

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-24

To specify an IPsec rule that defines the traffic types to be protected, follow these steps:

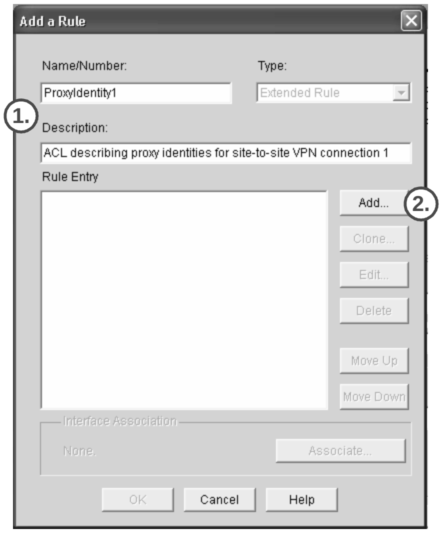
Step 1 Click the **Create/Select an access-list for IPSec traffic** radio button.

Step 2 Click the **...** button on the right to choose an existing ACL or create a new one.

Step 3 If an ACL you would like to use already exists, choose **Select an existing rule (ACL)** option. If you would like to create a new ACL, choose **Create a new rule(ACL) and select** option.

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

Option 2: Using an ACL (Cont.)


Add a Rule

Name/Number: ProxyIdentity1

Type: Extended Rule

Description: ACL describing proxy identities for site-to-site VPN connection 1

Interface Association: None.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-25

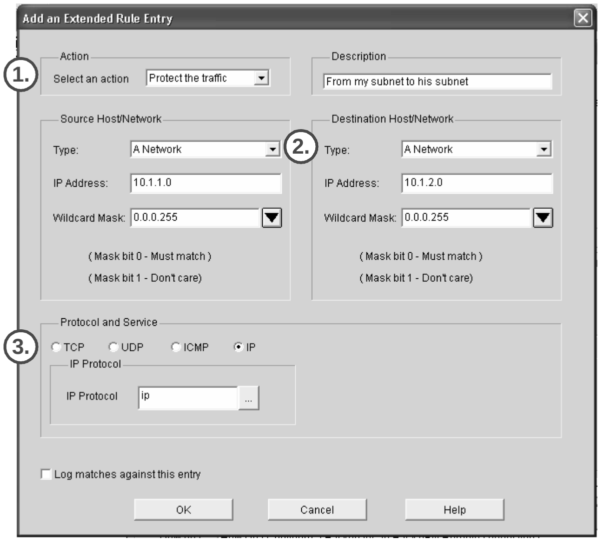
When creating a new ACL to define traffic that needs protection, you will be presented with a window listing the created access rule entries. To create a new rule, follow these steps:

Step 1 Give the access rule a name and description.

Step 2 Click the **Add** button to start adding rule entries.

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

Option 2: Using an ACL (Cont.)



Add an Extended Rule Entry

Action

Select an action: Protect the traffic

Description: From my subnet to his subnet

Source Host/Network

Type: A Network

IP Address: 10.1.1.0

Wildcard Mask: 0.0.0.255

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

Destination Host/Network

Type: A Network

IP Address: 10.1.2.0

Wildcard Mask: 0.0.0.255

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

Protocol and Service

○ TCP ○ UDP ○ ICMP ● IP

IP Protocol

IP Protocol: ip

□ Log matches against this entry

OK Cancel Help

© 2006 Cisco Systems, Inc. All rights reserved.

Follow these steps to configure a new rule entry:

Step 1 Select an action and write a description of the rule entry.

Step 2 Each rule entry defines one pair of source and destination addresses or networks.

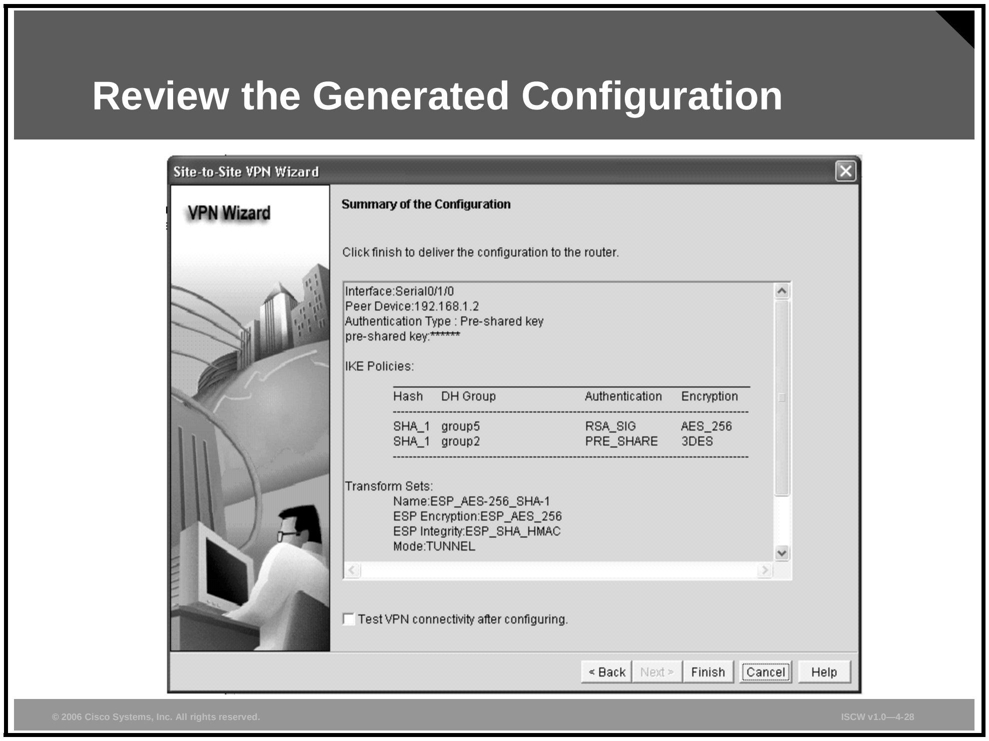
Note You must use wildcard bits instead of subnet masks.

Step 3 Optionally, you can provide protection for individual Open Systems Interconnection (OSI) Layer 4 protocols by selecting the required protocol radio box (TCP or UDP) and the required port numbers. If the rule applies to all IP traffic, leave the default radio button setting (IP).

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

Completing the Configuration

This topic describes how to complete the configuration by viewing the settings in the Summary window.



Review the Generated Configuration

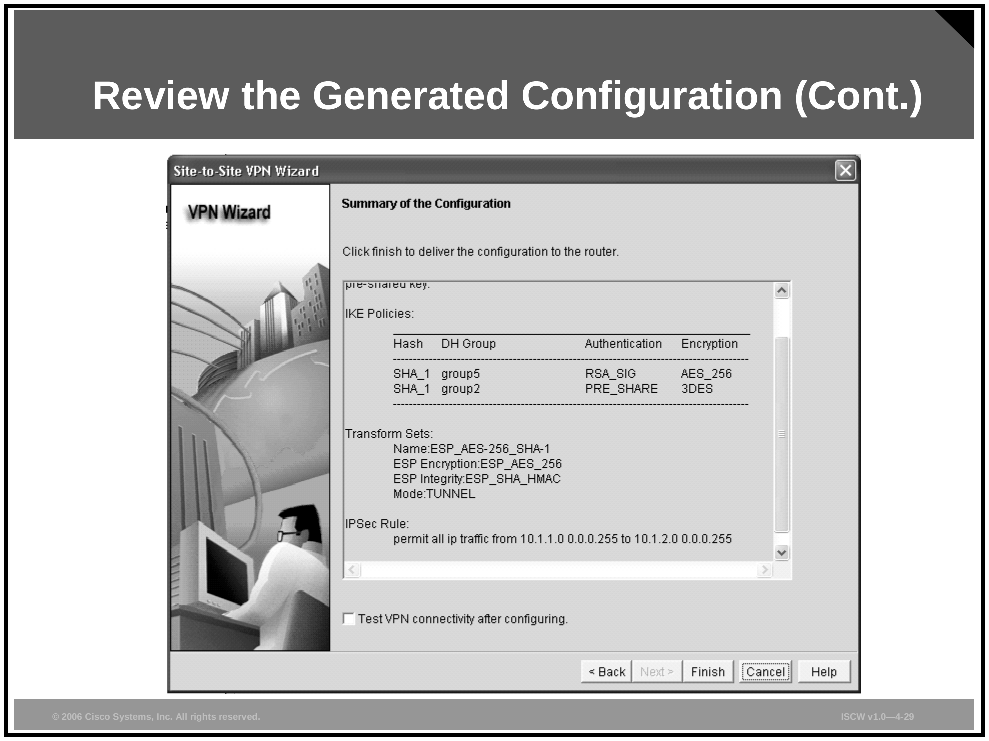
Summary of the Configuration

Click finish to deliver the configuration to the router.

```
Interface:Serial0/1/0
Peer Device:192.168.1.2
Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

         Hash    DH Group                    Authentication    Encryption
         -----------------------------------------------------------------
         SHA_1   group5                      RSA_SIG           AES_256
         SHA_1   group2                      PRE_SHARE         3DES
         -----------------------------------------------------------------

Transform Sets:
         Name:ESP_AES-256_SHA-1
         ESP Encryption:ESP_AES_256
         ESP Integrity:ESP_SHA_HMAC
         Mode:TUNNEL
```

□ Test VPN connectivity after configuring.

© 2006 Cisco Systems, Inc. All rights reserved.



Review the Generated Configuration (Cont.)

Summary of the Configuration

Click finish to deliver the configuration to the router.

```
pre-shared key:
IKE Policies:

         Hash    DH Group                    Authentication    Encryption
         -----------------------------------------------------------------
         SHA_1   group5                      RSA_SIG           AES_256
         SHA_1   group2                      PRE_SHARE         3DES
         -----------------------------------------------------------------

Transform Sets:
         Name:ESP_AES-256_SHA-1
         ESP Encryption:ESP_AES_256
         ESP Integrity:ESP_SHA_HMAC
         Mode:TUNNEL

IPSec Rule:
         permit all ip traffic from 10.1.1.0 0.0.0.255 to 10.1.2.0 0.0.0.255
```

□ Test VPN connectivity after configuring.

© 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 self-study.

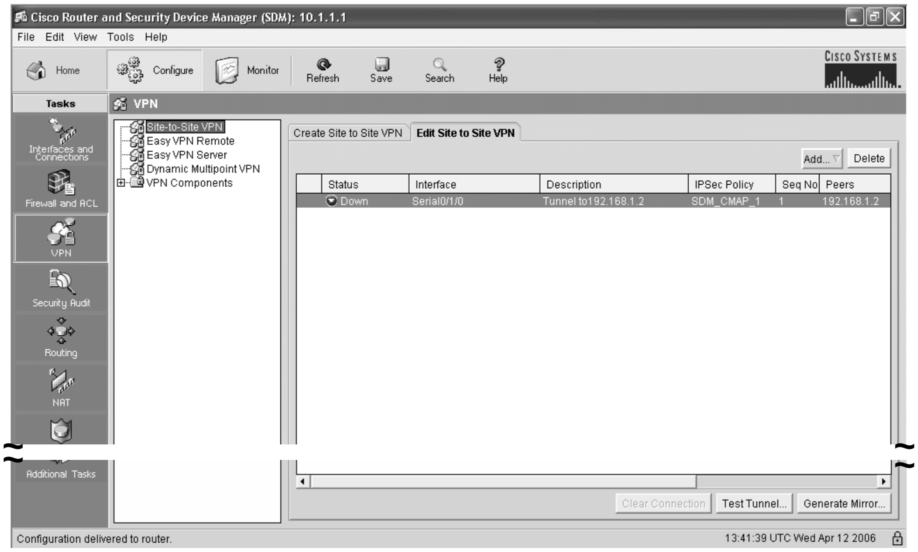
At the end of the step-by-step setup, the wizard presents a summary of the configured parameters. Click the **Back** button to go back and modify the configuration in case you have made a mistake. Click the **Finish** button to complete the configuration.

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 self-study.

Test Tunnel Configuration and Operation

After the site-to-site tunnel has been created, you can immediately see its status by clicking the **Edit Site to Site VPN** tab.

Test Tunnel Configuration and Operation



Status	Interface	Description	IPSec Policy	Seq No	Peers
Down	Serial0/1/0	Tunnel to192.168.1.2	SDM_CMAP_1	1	192.168.1.2

Configuration delivered to router.

13:41:39 UTC Wed Apr 12 2006

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-30

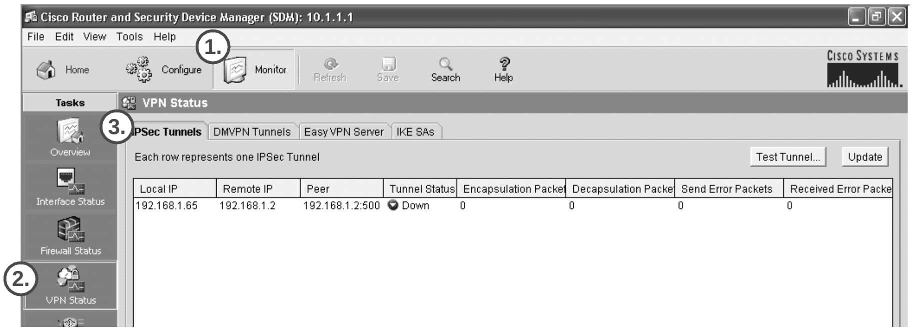
You can click the **Test Tunnel** button to run a test to determine the configuration correctness of the tunnel. You can also click the **Generate Mirror** button to generate a mirroring configuration that is required on the other end of the tunnel. This is useful if the other router does not have SDM and you have to use the CLI to configure the tunnel.

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

Monitor Tunnel Operation

The monitoring page can be used to display the status of the tunnel.

Monitor Tunnel Operation



Each row represents one IPSec Tunnel

Local IP	Remote IP	Peer	Tunnel Status	Encapsulation Packet	Decapsulation Packe	Send Error Packets	Received Error Packe
192.168.1.65	192.168.1.2	192.168.1.2:500	● Down	0	0	0	0

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-31

To see all IPsec tunnels, their parameters, and status, follow this procedure:

Step 1 Click the **Monitor** icon in the top navigation bar.

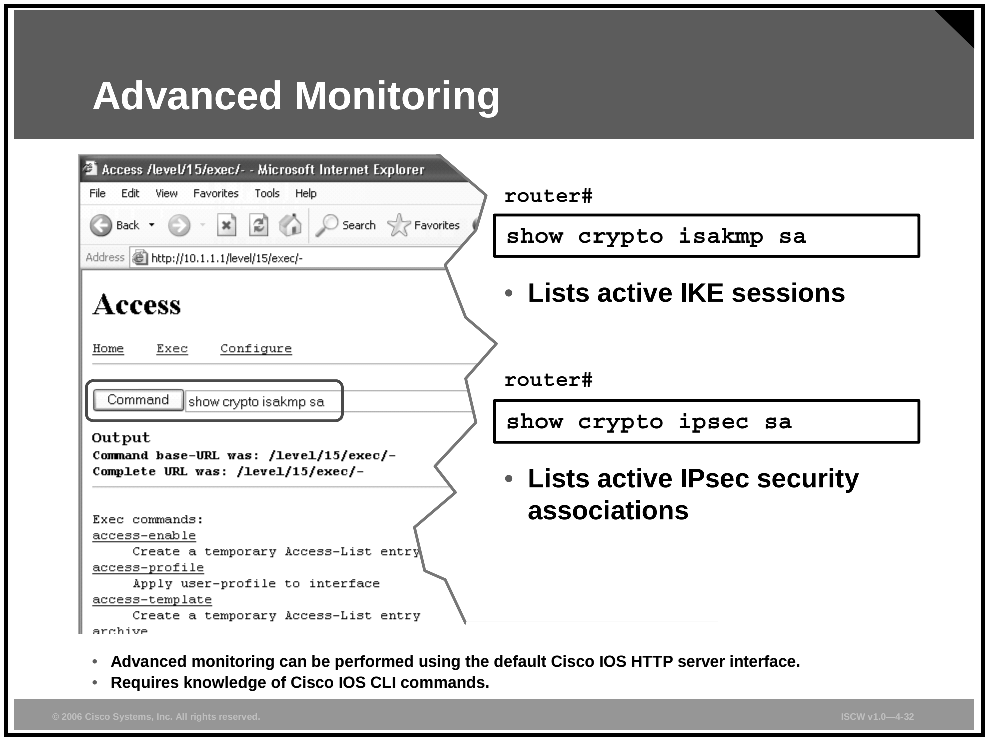
Step 2 Click the **VPN Status** icon in the left vertical navigation bar.

Step 3 Click the **IPSec Tunnels** tab.

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

Advanced Monitoring

The basic Cisco IOS web interface also allows you to use the web interface to enter Cisco IOS CLI commands to monitor and troubleshoot the router.



Advanced Monitoring

Access /level/15/exec/- - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://10.1.1.1/level/15/exec/-
Access
Home
Exec
Configure
Command

show crypto isakmp sa

```
Output
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-

Exec commands:
access-enable
     Create a temporary Access-List entry
access-profile
     Apply user-profile to interface
access-template
     Create a temporary Access-List entry
archive
```

```
router#
show crypto isakmp sa
```

- **Lists active IKE sessions**

```
router#
show crypto ipsec sa
```

- **Lists active IPsec security associations**

- **Advanced monitoring can be performed using the default Cisco IOS HTTP server interface.**
- **Requires knowledge of Cisco IOS CLI commands.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-32

The table lists two of the most useful **show** commands for determining the status of IPsec VPN connections.

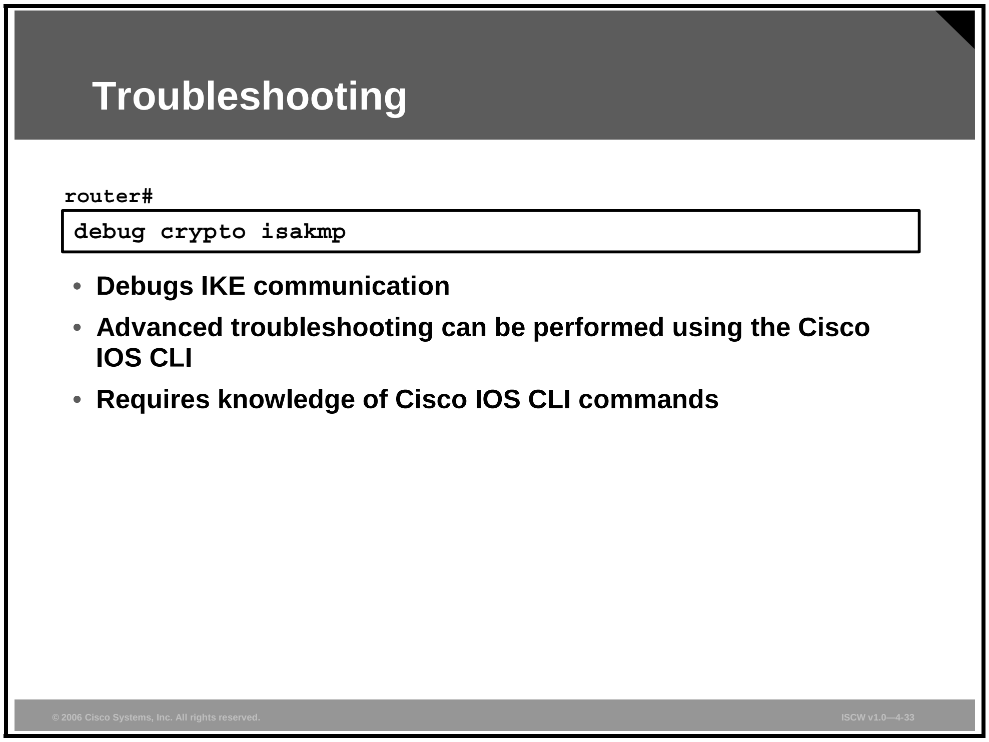
show Commands

Command	Description
`show crypto isakmp sa`	To display all current IKE security associations (SAs), use the **show crypto isakmp sa** command in EXEC mode. QM_IDLE status indicates an active IKE SA.
`show crypto ipsec sa`	To display the settings used by current SAs, use the **show crypto ipsec sa** command in EXEC mode. Non-zero encryption and decryption statistics can indicate a working set of IPsec SAs.

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

Troubleshooting

You should use a terminal to connect to the Cisco IOS router if you want to use debugging commands to troubleshoot VPN connectivity.



Troubleshooting

```
router#
debug crypto isakmp
```

- **Debugs IKE communication**
- **Advanced troubleshooting can be performed using the Cisco IOS CLI**
- **Requires knowledge of Cisco IOS CLI commands**

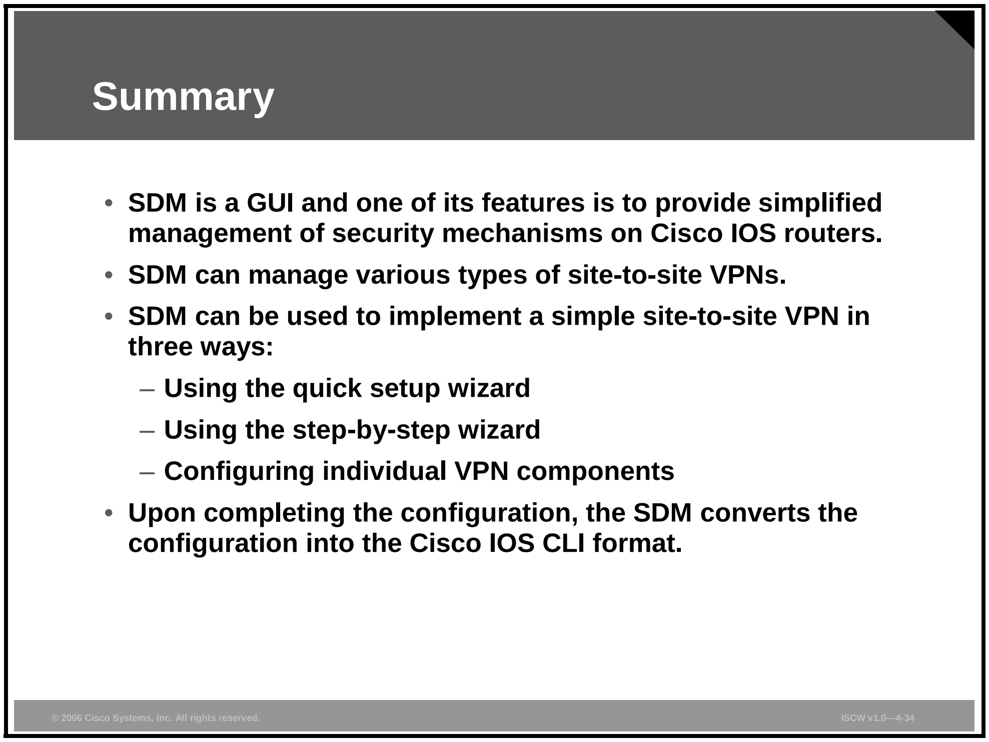
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-33

The **debug crypto isakmp** EXEC command displays detailed information about the IKE Phase 1 and Phase 2 negotiation processes.

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

Summary

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



Summary

- **SDM is a GUI and one of its features is to provide simplified management of security mechanisms on Cisco IOS routers.**
- **SDM can manage various types of site-to-site VPNs.**
- **SDM can be used to implement a simple site-to-site VPN in three ways:**
  - **Using the quick setup wizard**
  - **Using the step-by-step wizard**
  - **Configuring individual VPN components**
- **Upon completing the configuration, the SDM converts the configuration into the Cisco IOS CLI format.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-34

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

Lesson 4

Configuring GRE Tunnels over IPsec

Overview

This lesson describes the configuration steps required to implement site-to-site virtual private networks (VPNs) using Generic Routing Encapsulation (GRE) over IPsec and the Cisco Security Device Manager (SDM).

Objectives

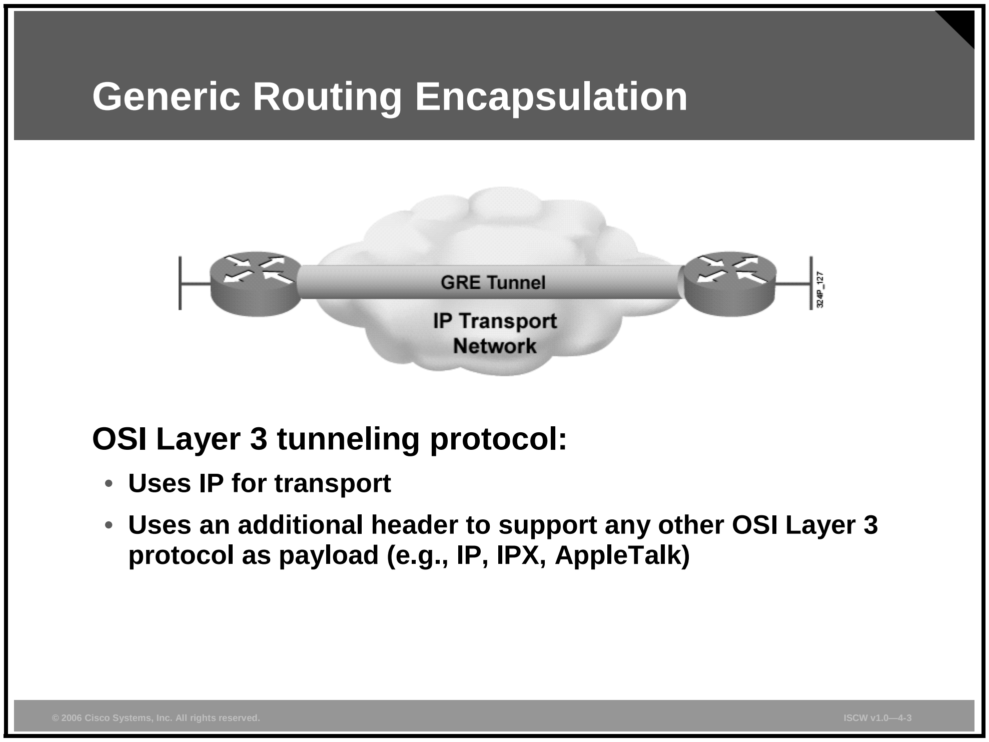
Upon completing this lesson, you will be able to explain GRE encapsulations, operations, and configurations. This ability includes being able to meet these objectives:

- Describe GRE
- Explain the purpose of a secure GRE tunnel
- Describe the components that will be configured by the SDM site-to-site VPN secure GRE tunnel wizard
- Explain how to configure a backup GRE-over-IPsec tunnel that the router can use when the primary tunnel fails
- Explain how to select the authentication method to be used on the VPN
- Explain how to configure IKE using the SDM wizard
- Explain how to configure the IPsec transform set using the SDM wizard
- Explain how to configure dynamic or static routing over the GRE and IPsec tunnel
- Explain how to complete the configuration by viewing the settings in the Summary window

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

Generic Routing Encapsulation

This topic describes GRE and how it is used to support VPN routing.



Generic Routing Encapsulation

OSI Layer 3 tunneling protocol:

- **Uses IP for transport**
- **Uses an additional header to support any other OSI Layer 3 protocol as payload (e.g., IP, IPX, AppleTalk)**

© 2006 Cisco Systems, Inc. All rights reserved.

GRE is a tunneling protocol initially developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

Routing protocols are often used across the tunnel to enable dynamic exchange or routing information in the virtual network.

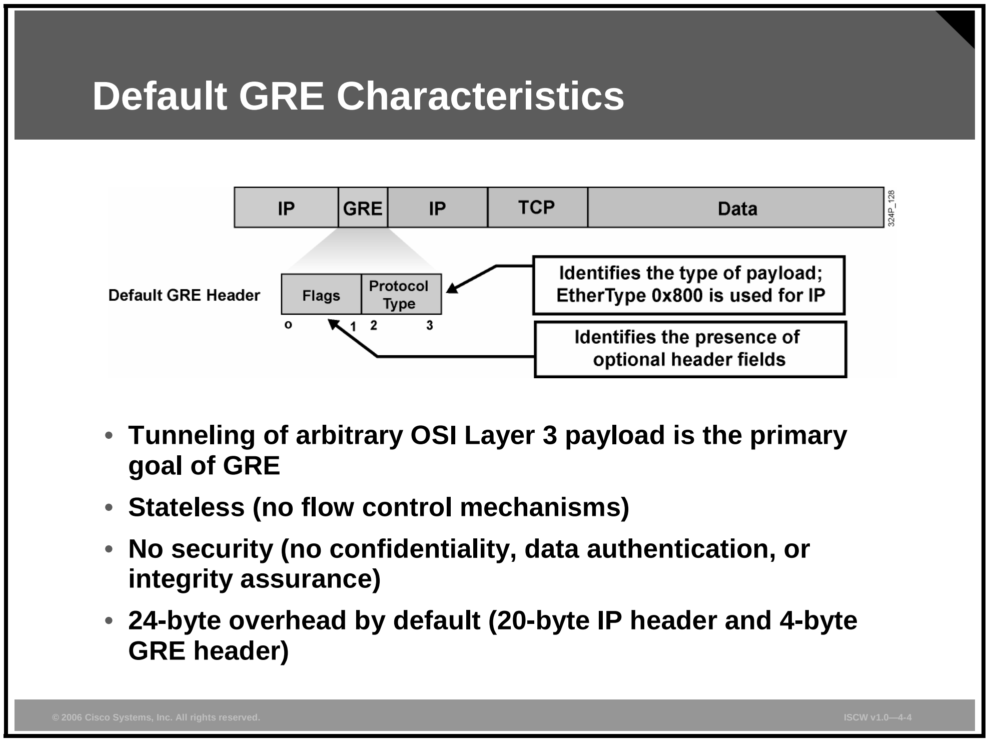
The multiprotocol functionality is provided by adding an additional GRE header between the payload and the tunneling IP header.

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

Default GRE Characteristics

GRE is now a standard tunneling method described by these Internet Engineering Task Force (IETF) standards:

- RFC 1701 and RFC 2784, describing a general-purpose GRE that can also be used by non-IP protocols in the transport network
- RFC 1702, describing how GRE can be used to transport arbitrary Layer 3 payloads over IP networks
- RFC 3147, describing GRE over Connectionless Network Service (CLNS) networks
- RFC 4023, describing Multiprotocol Label Switching (MPLS) encapsulation inside GRE



Default GRE Characteristics

Identifies the type of payload; EtherType 0x800 is used for IP

Identifies the presence of optional header fields

- **Tunneling of arbitrary OSI Layer 3 payload is the primary goal of GRE**
- **Stateless (no flow control mechanisms)**
- **No security (no confidentiality, data authentication, or integrity assurance)**
- **24-byte overhead by default (20-byte IP header and 4-byte GRE header)**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-4

GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any Open Systems Interconnection (OSI) Layer 3 protocol.

GRE itself is completely stateless—it does not include any flow control mechanisms, by default.

GRE also does not include any strong security mechanisms to protect its payload.

The GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.

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

Basic GRE Header

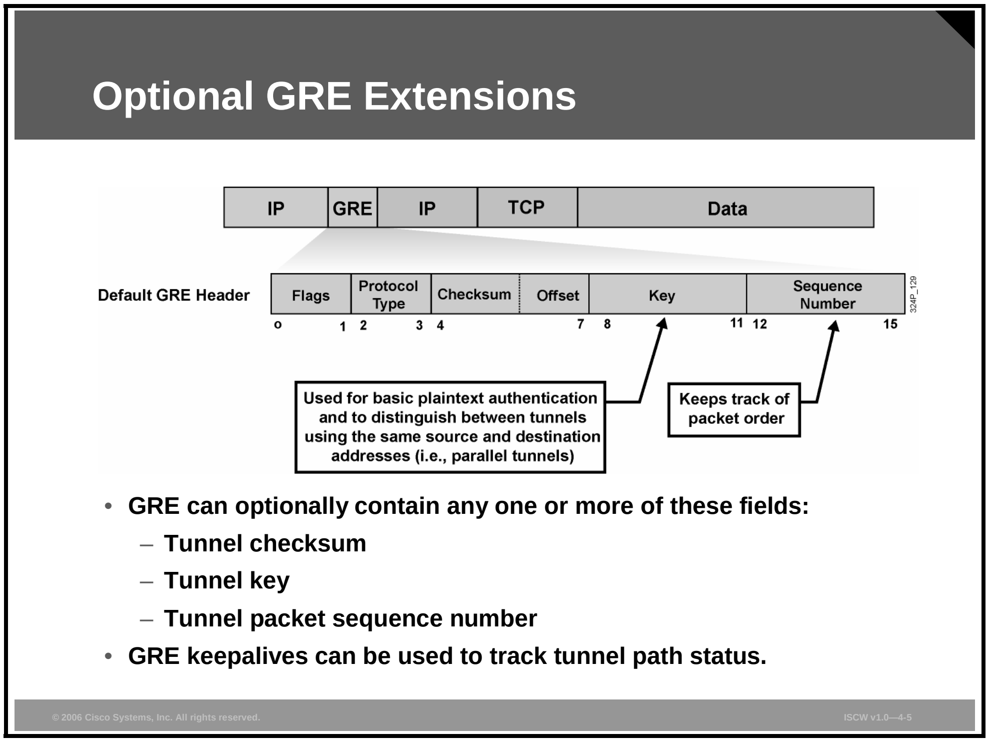
The GRE tunnel header contains at least two 2-byte mandatory fields:

- **GRE flags:** The GRE flags are encoded in the first two octets. Bit 0 is the most significant bit, and bit 15 is the least significant bit. Some of the GRE flags include the following:
  - **Checksum Present (bit 0):** If the Checksum Present bit is set to 1, the optional Checksum field is present in the GRE header.
  - **Key Present (bit 2):** If the Key Present bit is set to 1, it indicates that the optional Key field is present in the GRE header.
  - **Sequence Number Present (bit 3):** If the Sequence Number Present bit is set to 1, it indicates that the optional Sequence Number field is present in the GRE header.
  - **Version Number (bits 13–15):** The Version Number indicates the GRE implementation version. A value of 0 is typically used for basic GRE implementation. Point-to-Point Tunneling Protocol (PPTP) uses Version 1.
- **Protocol Type:** The Protocol Type field contains the protocol type of the payload packet. In general, the value will be the Ethernet protocol type field for the packet. For IP, the hexadecimal value of 0x800 is used. This field enables the GRE to tunnel any OSI Layer 3 protocol.

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

Optional GRE Extensions

The GRE tunnel header can contain additional optional header information, depending on the flags in the first two bytes of the GRE header.



Optional GRE Extensions

Used for basic plaintext authentication and to distinguish between tunnels using the same source and destination addresses (i.e., parallel tunnels)

Keeps track of packet order

- GRE can optionally contain any one or more of these fields:
  - Tunnel checksum
  - Tunnel key
  - Tunnel packet sequence number
- GRE keepalives can be used to track tunnel path status.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-5

Optional header information can include the following:

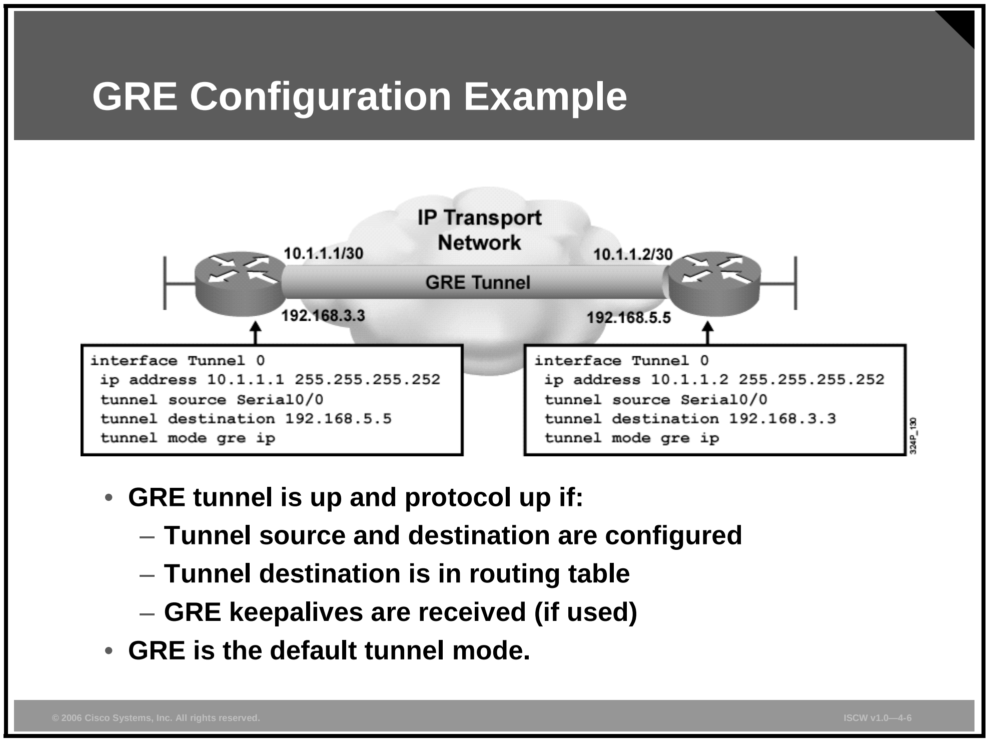
- **Tunnel checksum:** Used to detect packet corruption. This option is not used often because checksums are also used on other layers in the protocol stack, typically to ensure the accuracy of the GRE packets.
- **Tunnel key:** Can be used for two purposes:
  - It can be used for basic plaintext authentication of packets, in which only the two GRE endpoints share a secret number that enables the tunnel to operate properly. However, anyone in the packet path can easily see the key and be able to spoof tunnel packets.
  - A more common usage of the tunnel key is when two routers want to establish parallel tunnels sourced from the same IP address. The tunnel key is then used to distinguish between GRE packets belonging to different tunnels.
- **Tunnel sequence number:** To ensure that GRE packets are accepted only if they arrive in correct order.

Cisco IOS also supports a proprietary keepalive mechanism that can be used to detect failures in the GRE tunnel path or detect a failed GRE peer.

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

GRE Configuration Example

This section shows how to configure a basic GRE tunnel.



GRE Configuration Example

```
interface Tunnel 0
 ip address 10.1.1.1 255.255.255.252
 tunnel source Serial0/0
 tunnel destination 192.168.5.5
 tunnel mode gre ip
```

```
interface Tunnel 0
 ip address 10.1.1.2 255.255.255.252
 tunnel source Serial0/0
 tunnel destination 192.168.3.3
 tunnel mode gre ip
```

- **GRE tunnel is up and protocol up if:**
  - **Tunnel source and destination are configured**
  - **Tunnel destination is in routing table**
  - **GRE keepalives are received (if used)**
- **GRE is the default tunnel mode.**

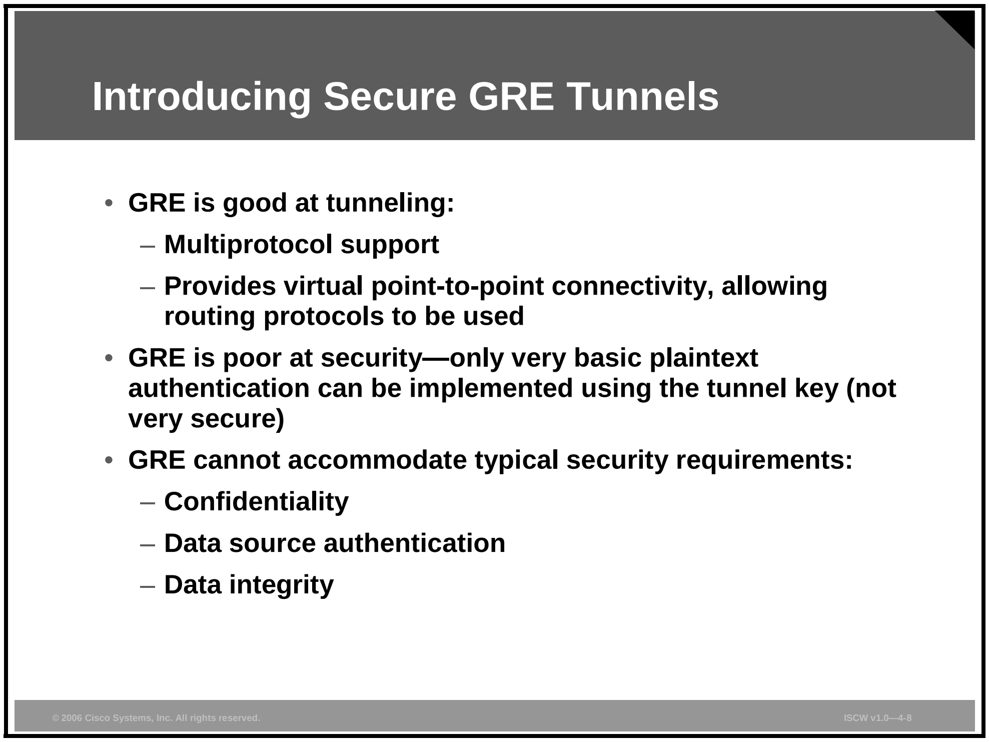
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-6

The sample configuration illustrates a basic GRE tunnel configuration built with SDM between a pair of routers. The virtual point-to-point connection is configured with the IP subnet 10.1.1.0/30. Both routers use the IP address of their outbound interface as tunnel sources. The two routers must be configured by mirroring IP addresses (that is, the tunnel source on one router must be specified as the tunnel destination on the other 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 self-study.

Introducing Secure GRE Tunnels

This topic explains the purpose of a secure GRE tunnel (GRE-over-IPsec).



Introducing Secure GRE Tunnels

- **GRE is good at tunneling:**
  - **Multiprotocol support**
  - **Provides virtual point-to-point connectivity, allowing routing protocols to be used**
- **GRE is poor at security—only very basic plaintext authentication can be implemented using the tunnel key (not very secure)**
- **GRE cannot accommodate typical security requirements:**
  - **Confidentiality**
  - **Data source authentication**
  - **Data integrity**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-8

The main function of GRE is to provide powerful yet simple tunneling. It supports any OSI Layer 3 protocol as payload, for which it provides virtual point-to-point connectivity. It also allows the usage of routing protocols across the tunnel.

The main limitation of GRE is that it lacks strong security functionality. It only provides basic plaintext authentication using the tunnel key, which is not secure, and tunnel source and destination addresses. A reasonably secure VPN requires these characteristics that are not provided by GRE:

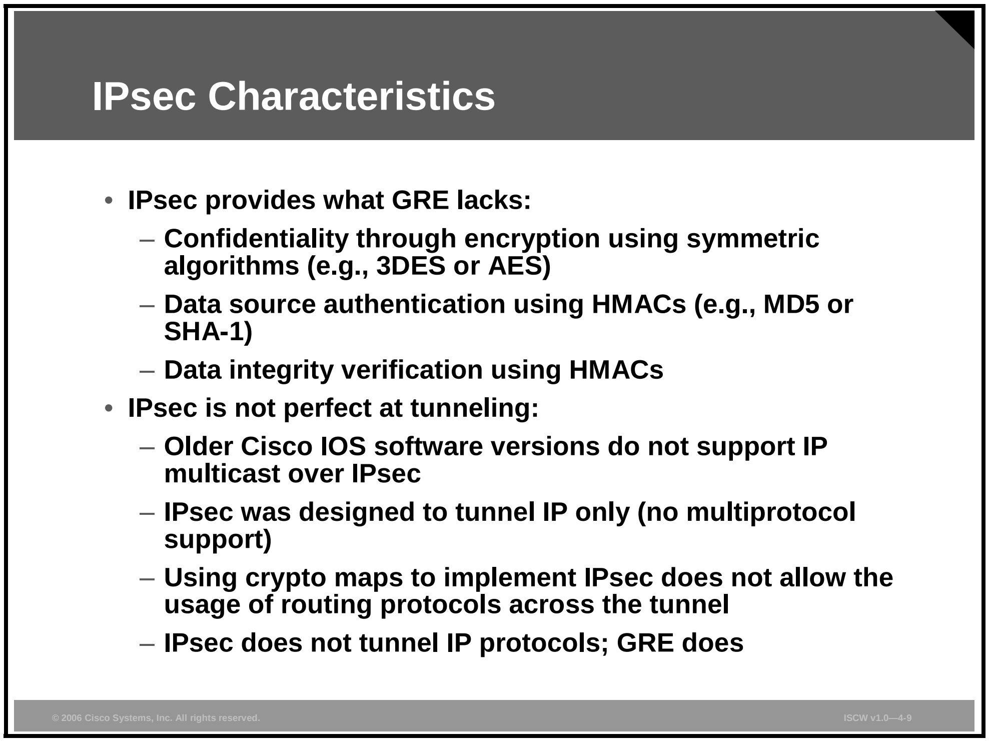
- Cryptographically strong confidentiality (that is, encryption)
- Data source authentication that is not vulnerable to man-in-the-middle attacks
- Data integrity assurance that is not vulnerable to man-in-the-middle attacks and spoofing

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

IPsec Characteristics

IPsec was designed to provide the tunneling characteristics that GRE lacks:

- Confidentiality through encryption using symmetric algorithms (for example, Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES])
- Data source authentication using Hash-based Message Authentication Codes (HMACs) (for example, Message Digest 5 [MD5] or Secure Hash Algorithm 1 [SHA-1])
- Data integrity verification using HMACs



IPsec Characteristics

- **IPsec provides what GRE lacks:**
  - **Confidentiality through encryption using symmetric algorithms (e.g., 3DES or AES)**
  - **Data source authentication using HMACs (e.g., MD5 or SHA-1)**
  - **Data integrity verification using HMACs**
- **IPsec is not perfect at tunneling:**
  - **Older Cisco IOS software versions do not support IP multicast over IPsec**
  - **IPsec was designed to tunnel IP only (no multiprotocol support)**
  - **Using crypto maps to implement IPsec does not allow the usage of routing protocols across the tunnel**
  - **IPsec does not tunnel IP protocols; GRE does**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-9

IPsec, however, was primarily intended to provide the above services to IP traffic only. The development of Cisco IOS software is removing the limitations, but multiprotocol support will always require an additional tunneling protocol.

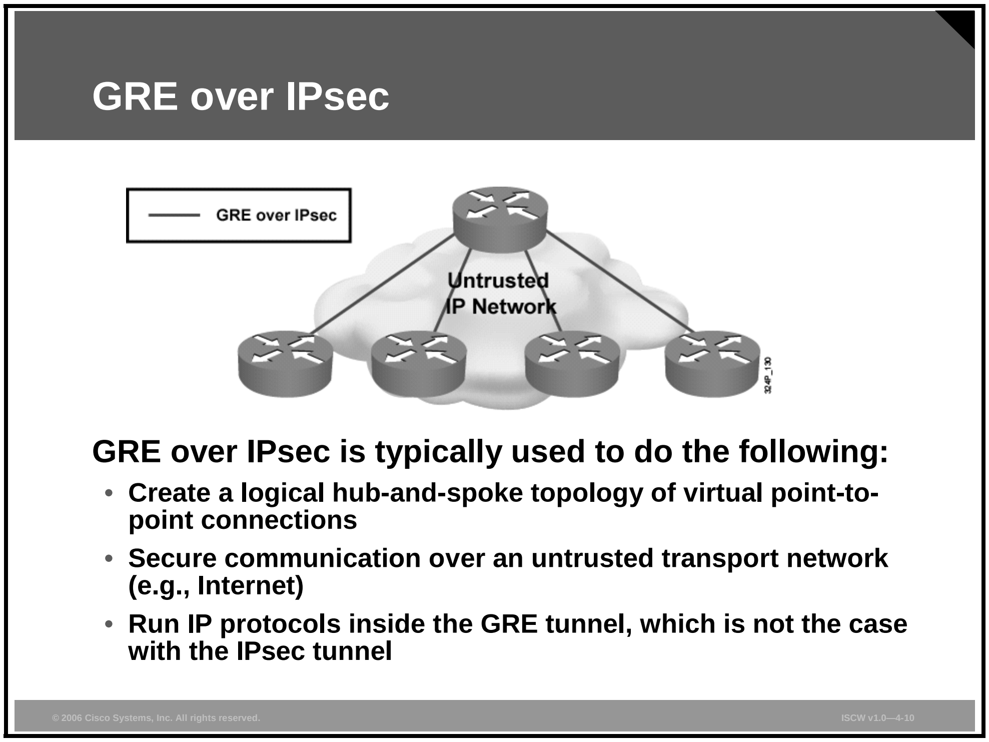
The usage of crypto maps does not provide a virtual interface in which an address can be configured and a routing protocol can be run to dynamically exchange routing information.

Note Cisco IOS software Release 12.4(4)T and newer can now encrypt multicast using a crypto map and an access list. Older software required GRE tunneling to provide support for multicast.

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

GRE over IPsec

Most implementations of point-to-point GRE over IPsec are implemented in a hub-and-spoke topology because it uses the minimum number of tunnels required to still provide full connectivity between VPN sites.



GRE over IPsec

GRE over IPsec is typically used to do the following:

- **Create a logical hub-and-spoke topology of virtual point-to-point connections**
- **Secure communication over an untrusted transport network (e.g., Internet)**
- **Run IP protocols inside the GRE tunnel, which is not the case with the IPsec tunnel**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-10

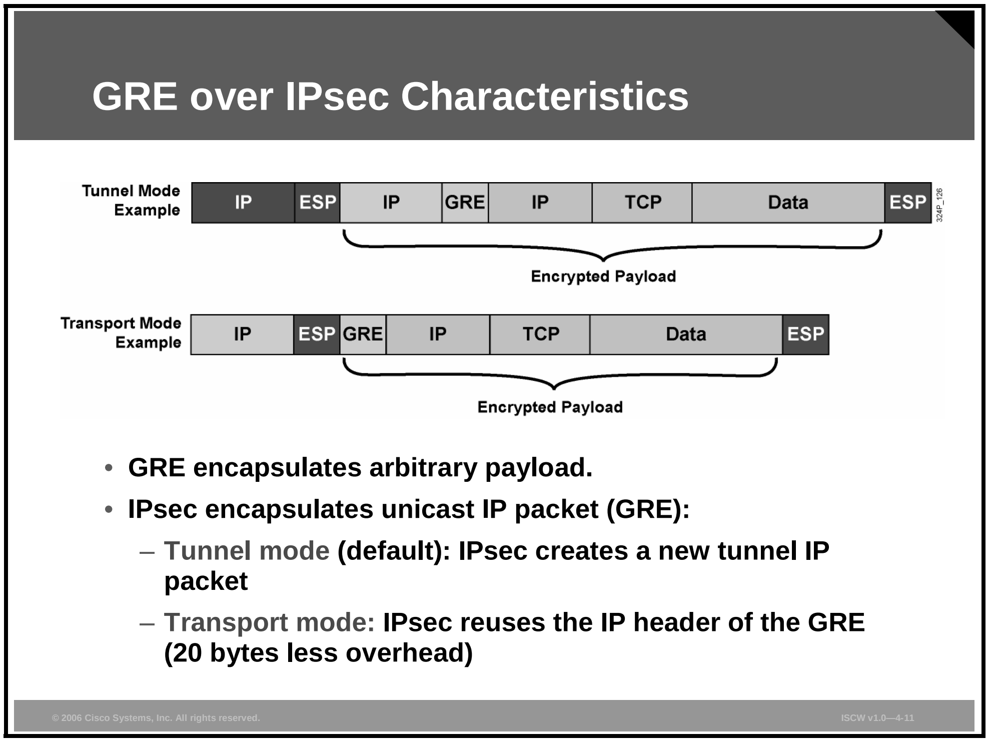
The hub-and-spoke topology minimizes the management overhead associated with the maintenance of the IPsec tunnels. Also, most enterprises have concentric traffic patterns, thus are not interested in managing more tunnels than necessary.

GRE over IPsec is typically used to provide an emulated WAN (by using GRE) over an untrusted transport network (for example, the Internet) in which communication is protected using IPsec.

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

GRE over IPsec Characteristics

The image illustrates the combination of GRE and IPsec.



GRE over IPsec Characteristics

- **GRE encapsulates arbitrary payload.**
- **IPsec encapsulates unicast IP packet (GRE):**
  - **Tunnel mode (default): IPsec creates a new tunnel IP packet**
  - **Transport mode: IPsec reuses the IP header of the GRE (20 bytes less overhead)**

© 2006 Cisco Systems, Inc. All rights reserved.

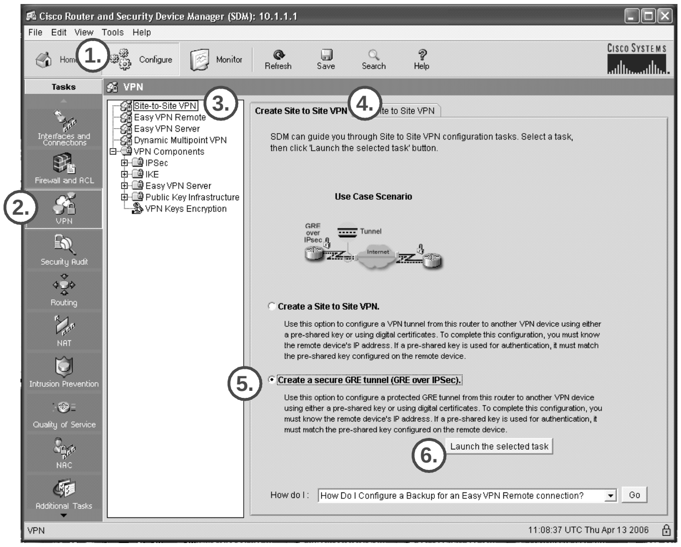
The top figure shows the tunnel mode in which both tunneling technologies (IPsec and GRE) introduce their own tunnel IP header. The bottom figure illustrates the usage of transport mode in which IPsec reuses the IP header of the packet that it is protecting, and thus reduces the overhead.

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

Configuring GRE over IPsec Site-to-Site Tunnel Using SDM

This topic describes the components and resulting Cisco IOS configuration that will be configured by the SDM site-to-site VPN secure GRE tunnel wizard.

Configuring GRE over IPsec Site-to-Site Tunnel Using SDM



SDM can guide you through Site to Site VPN configuration tasks. Select a task, then click 'Launch the selected task' button.

○ **Create a Site to Site VPN.**

Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

● **Create a secure GRE tunnel (GRE over IPSec).**

Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

© 2006 Cisco Systems, Inc. All rights reserved.

To create a GRE over IPsec site-to-site VPN, follow this procedure:

Step 1 Use a web browser to connect to an HTTP server of a router. Click the **Configure** icon in the top horizontal navigation bar to enter the configuration page.

Step 2 Click the **VPN** icon in the left vertical navigation bar to open the VPN page.

Step 3 Choose the **Site to Site VPN** wizard in the menu.

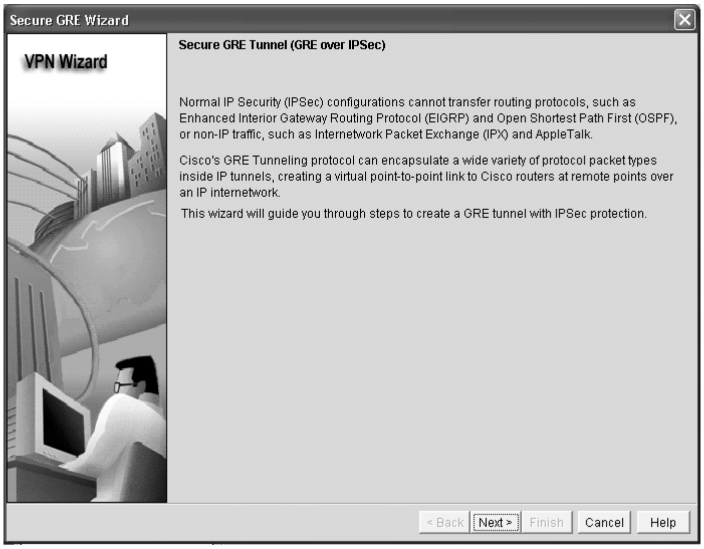
Step 4 Click the **Create Site to Site VPN** tab in the section on the right.

Step 5 Click the **Create a Secure GRE tunnel (GRE over IPSec)** radio button.

Step 6 Click the **Launch the selected task** button to start the wizard that will guide you through the configuration steps.

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

Configuring GRE over IPsec Site-to-Site Tunnel Using SDM (Cont.)



Secure GRE Tunnel (GRE over IPSec)

Normal IP Security (IPSec) configurations cannot transfer routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), or non-IP traffic, such as Internetwork Packet Exchange (IPX) and AppleTalk.

Cisco's GRE Tunneling protocol can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

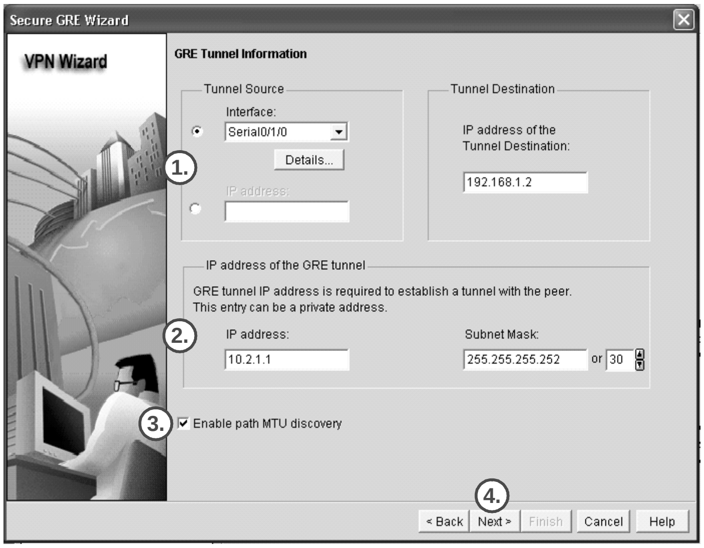
This wizard will guide you through steps to create a GRE tunnel with IPSec protection.

© 2006 Cisco Systems, Inc. All rights reserved.

The first window that the wizard displays gives a brief overview of GRE and its benefits when combined with IPsec.

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

Configuring GRE over IPsec Site-to-Site Tunnel Using SDM (Cont.)



Secure GRE Wizard

VPN Wizard

GRE Tunnel Information

Tunnel Source

● Interface: Serial0/1/0

○ IP address:

Tunnel Destination

IP address of the Tunnel Destination: 192.168.1.2

IP address of the GRE tunnel

GRE tunnel IP address is required to establish a tunnel with the peer. This entry can be a private address.

IP address: 10.2.1.1

Subnet Mask: 255.255.255.252 or 30

☑ Enable path MTU discovery

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-15

The figure illustrates these configuration steps for implementing a GRE tunnel:

Step 1 The GRE tunnel *source* IP address is taken from a configured interface or manually specified. It must still be a valid IP address configured on one of the interfaces on the router. Also, define the tunnel *destination* IP address.

Step 2 Define the inner IP address and subnet mask that are applied to the virtual point-to-point link.

Step 3 Optionally, enable Path MTU Discovery (PMTUD) to let the router determine the maximum transmission unit (MTU) for the virtual interface using Internet Control Message Protocol (ICMP). ICMP unreachables must be permitted by all filters and firewalls in the path between the two tunnel endpoints to allow PMTUD to work.

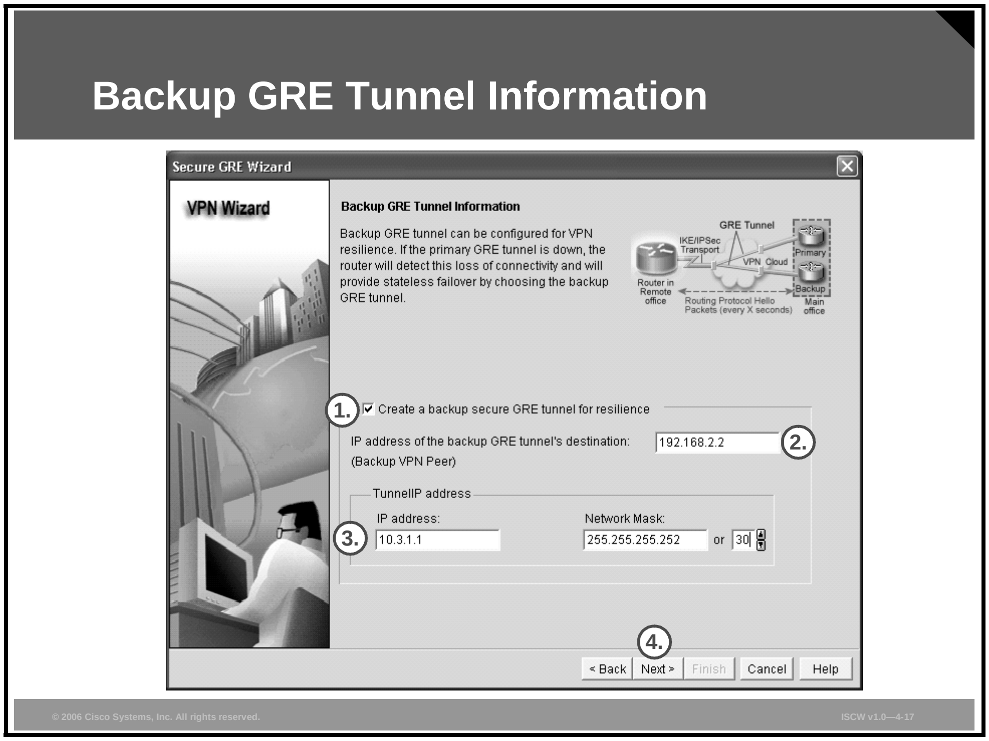
Note The PMTUD is enabled by default.

Step 4 Click the **Next** button to proceed to the next task.

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

Backup GRE Tunnel Information

This topic describes how to configure a backup GRE-over-IPsec tunnel that the router can use when the primary tunnel fails.



Backup GRE Tunnel Information

Secure GRE Wizard

VPN Wizard

Backup GRE Tunnel Information

Backup GRE tunnel can be configured for VPN resilience. If the primary GRE tunnel is down, the router will detect this loss of connectivity and will provide stateless failover by choosing the backup GRE tunnel.

1. ☑ Create a backup secure GRE tunnel for resilience

IP address of the backup GRE tunnel's destination: (Backup VPN Peer) 192.168.2.2 2.

TunnelIP address

3. IP address: 10.3.1.1 Network Mask: 255.255.255.252 or 30

4.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-17

Optionally, you can create a second GRE tunnel that will be used in case the primary tunnel fails:

Step 1 Check **Create a backup secure GRE tunnel for resilience**.

Step 2 Define the IP address of the backup VPN peer.

Step 3 Define the inner IP address and the subnet mask for the logical tunnel interface.

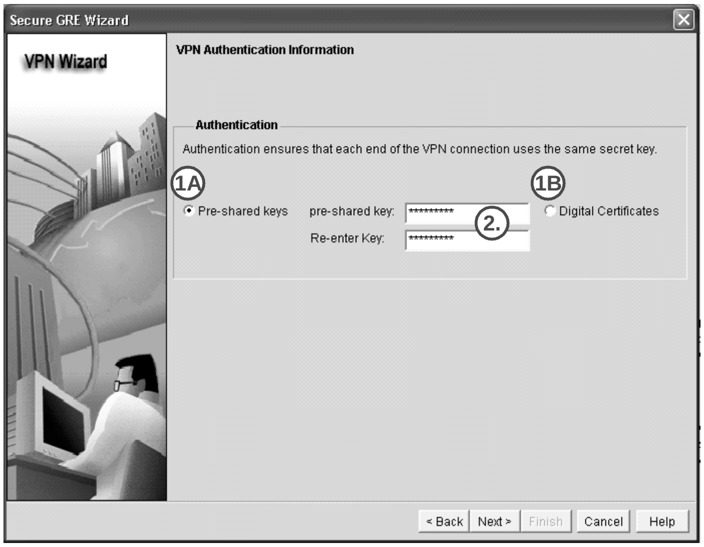
Step 4 Click the **Next** button to proceed to the next task.

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

VPN Authentication Information

This topic describes how to select the authentication method to be used on the VPN.

VPN Authentication Information



Secure GRE Wizard

VPN Wizard

VPN Authentication Information

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

● Pre-shared keys pre-shared key: ********* Re-enter Key: *********

○ Digital Certificates

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-19

After the GRE tunnel parameters have been defined, the wizard proceeds with the configuration of IPsec-specific parameters:

Step 1 Click the radio button for the desired authentication method:

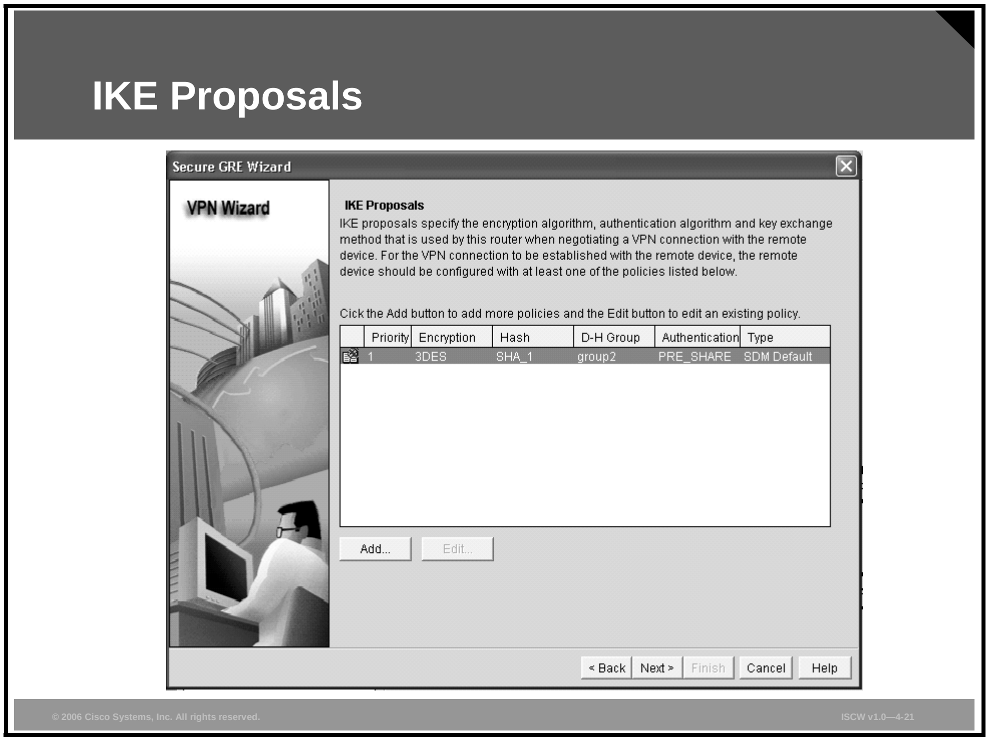
A) Preshared keys
B) Digital certificates

Step 2 If preshared keys are used for authentication, then specify a long and random preshared secret.

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

IKE Proposals

This topic describes the procedure to configure Internet Key Exchange (IKE) using the SDM wizard.



IKE Proposals

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Cick the Add button to add more policies and the Edit button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	SDM Default

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-21

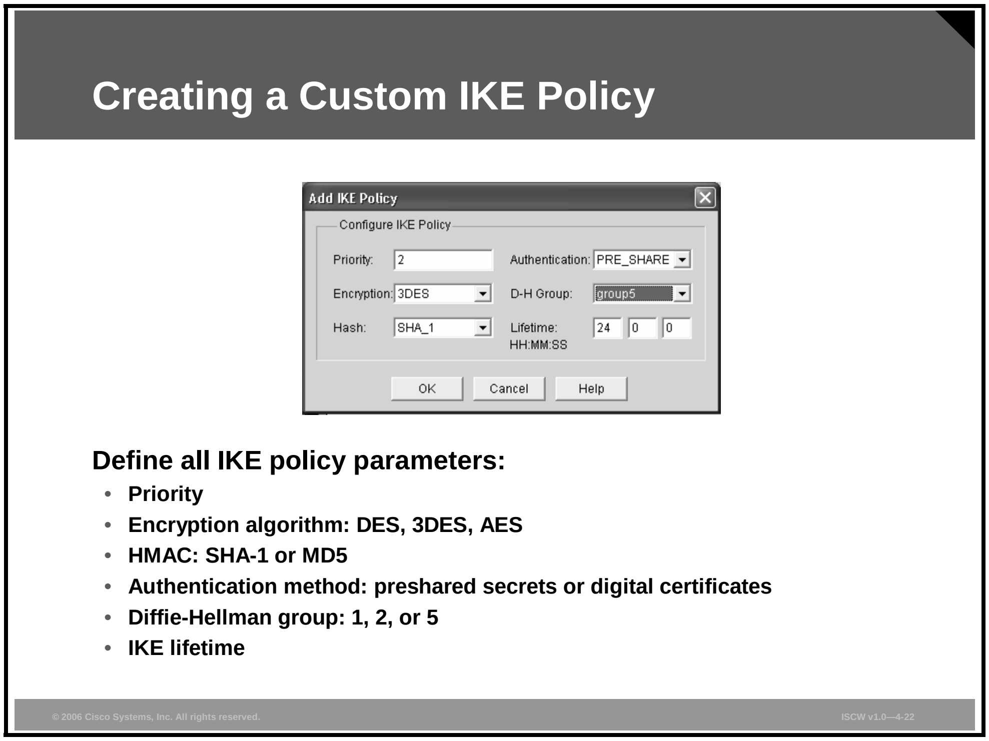
Use a predefined IKE policy, or click the **Add** button to create a custom IKE policy. You can also modify the existing policies by selecting them and clicking the **Edit** button.

When finished, click the **Next** button to proceed to the next task.

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

Creating a Custom IKE Policy

When adding a new or editing an existing IKE policy, define the required parameters.



Creating a Custom IKE Policy

Priority: 2

Encryption: 3DES

Hash: SHA_1

Authentication: PRE_SHARE

D-H Group: group5

Lifetime: HH:MM:SS 24 0 0

Define all IKE policy parameters:

- **Priority**
- **Encryption algorithm: DES, 3DES, AES**
- **HMAC: SHA-1 or MD5**
- **Authentication method: preshared secrets or digital certificates**
- **Diffie-Hellman group: 1, 2, or 5**
- **IKE lifetime**

© 2006 Cisco Systems, Inc. All rights reserved.

The required parameters are:

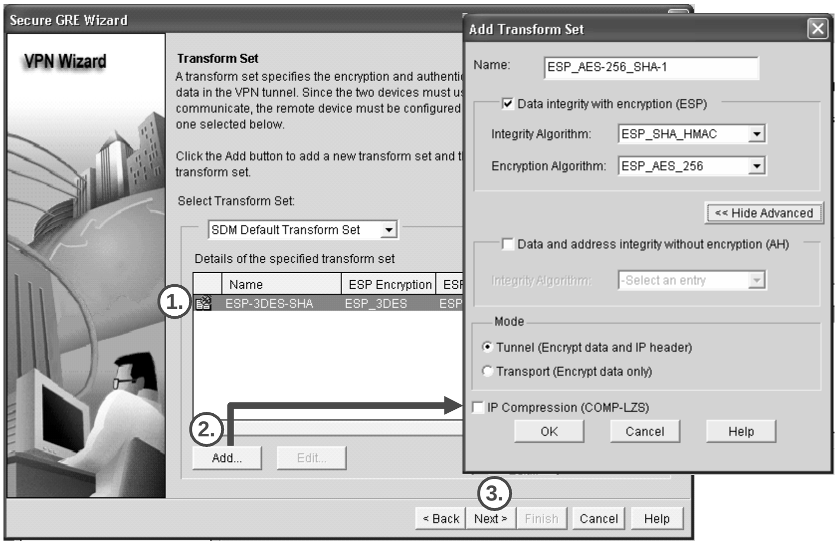
- IKE proposal priority
- Encryption algorithm (most commonly 3DES or AES; you can also use Software Encryption Algorithm [SEAL] to improve crypto performance on routers without hardware IPsec accelerators; DES is no longer advised because it can be broken in a relatively short time)
- HMAC (SHA-1 or MD5)
- Authentication method (preshared secrets or digital certificates)
- Diffie-Hellman group (1, 2, or 5)
- IKE lifetime

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

Transform Set

This topic describes the procedure to configure the IPsec transform set using the SDM wizard.

Transform Set



Transform Set

A transform set specifies the encryption and authenti data in the VPN tunnel. Since the two devices must u communicate, the remote device must be configured one selected below.

Click the Add button to add a new transform set and t transform set.

Select Transform Set: SDM Default Transform Set

Details of the specified transform set

Name	ESP Encryption	ESI
ESP-3DES-SHA	ESP_3DES	ESP

Name: ESP_AES-256_SHA-1

☑ Data integrity with encryption (ESP)

Integrity Algorithm: ESP_SHA_HMAC

Encryption Algorithm: ESP_AES_256

□ Data and address integrity without encryption (AH)

Integrity Algorithm: -Select an entry

Mode

● Tunnel (Encrypt data and IP header)

○ Transport (Encrypt data only)

□ IP Compression (COMP-LZS)

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-24

When creating IPsec transform set, you should use the same set of algorithms as with the configured IKE policy, following this procedure:

Step 1 You can use the IPsec transform set predefined by SDM.

Step 2 If you want to use a custom IPsec transform set, define it by clicking the **Add** button and specifying these parameters:

- Transform set name
- Encryption algorithm
- HMAC
- Mode of operation
- Optional compression

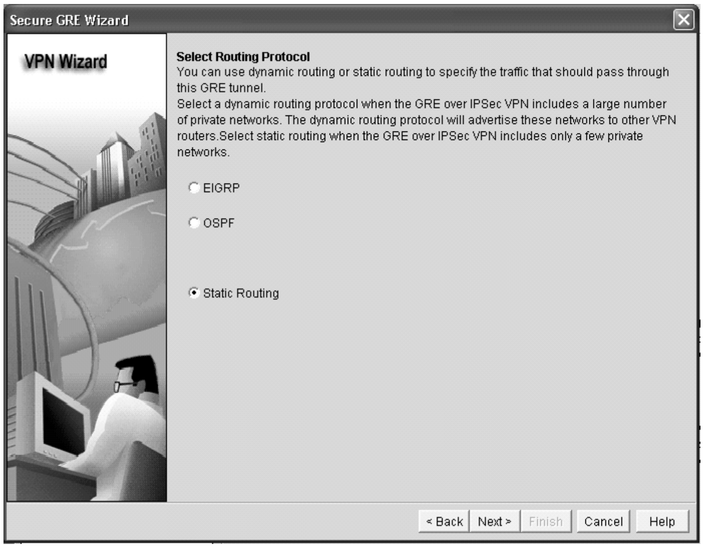
Step 3 When finished, click the **Next** button to proceed to the next task.

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

Routing Information

This topic explains how to configure dynamic or static routing over the GRE and IPsec tunnel.

Routing Information



Secure GRE Wizard

Select Routing Protocol

You can use dynamic routing or static routing to specify the traffic that should pass through this GRE tunnel.

Select a dynamic routing protocol when the GRE over IPSec VPN includes a large number of private networks. The dynamic routing protocol will advertise these networks to other VPN routers.Select static routing when the GRE over IPSec VPN includes only a few private networks.

○ EIGRP

○ OSPF

● Static Routing

© 2006 Cisco Systems, Inc. All rights reserved.

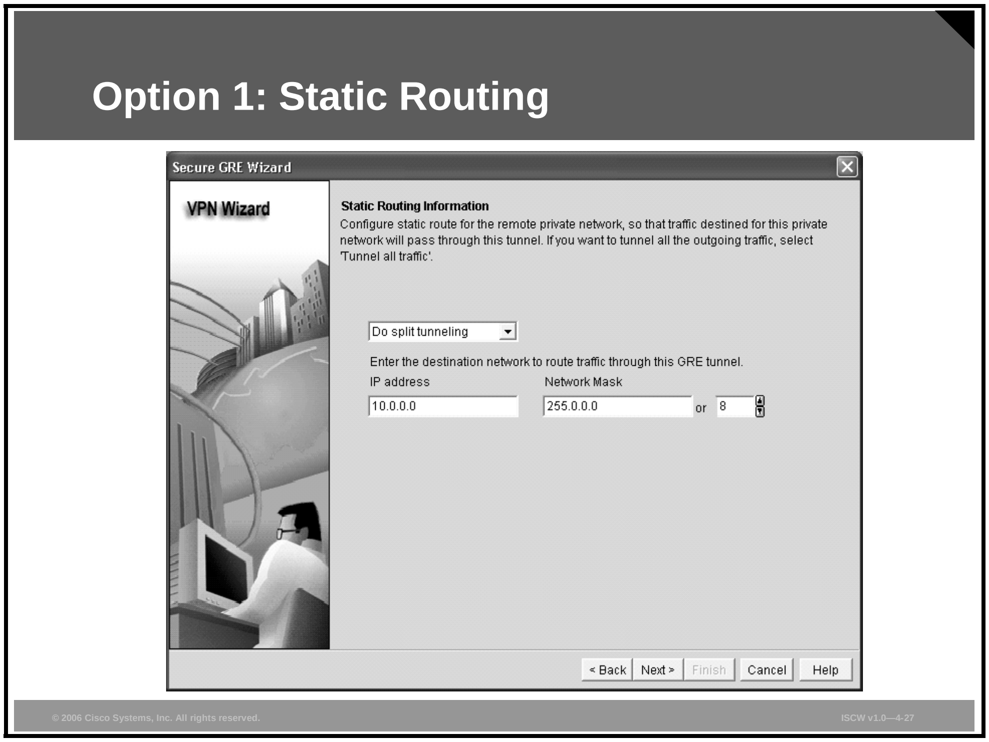
ISCW v1.0—4-26

A GRE tunnel supports multicast across the addressed point-to-point link. Static routing is typically used for simple stub sites with a single GRE over IPsec tunnel. With more complex topologies in which sites are using backup tunnels or have multiple IP subnets, you should enable a routing protocol to dynamically distribute the routing information as well as detect failures and reroute to backup tunnels.

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

Option 1: Static Routing

The figure illustrates the configuration of static routing.



Option 1: Static Routing

Secure GRE Wizard

Static Routing Information
Configure static route for the remote private network, so that traffic destined for this private network will pass through this tunnel. If you want to tunnel all the outgoing traffic, select 'Tunnel all traffic'.

Do split tunneling

Enter the destination network to route traffic through this GRE tunnel.

IP address: 10.0.0.0
Network Mask: 255.0.0.0 or 8

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-27

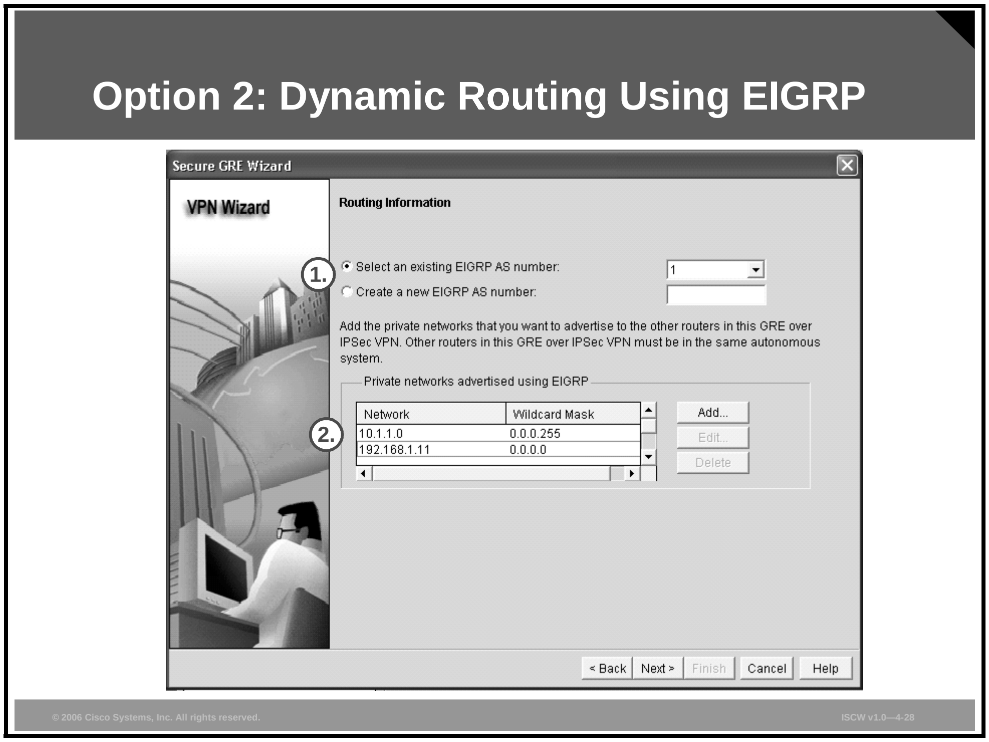
Disable split tunneling by choosing the **Tunnel all traffic** option, which results in a default route pointing into the tunnel.

Alternatively, you can choose the **Do split tunneling** option, and specify the IP address and subnet mask of the destination that is reachable through the tunnel. All other destinations are reachable by bypassing the tunnel.

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

Option 2: Dynamic Routing Using EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is often used for dynamic routing in VPNs.



Option 2: Dynamic Routing Using EIGRP

Secure GRE Wizard

VPN Wizard

Routing Information

● Select an existing EIGRP AS number: 1

○ Create a new EIGRP AS number:

Add the private networks that you want to advertise to the other routers in this GRE over IPSec VPN. Other routers in this GRE over IPSec VPN must be in the same autonomous system.

Private networks advertised using EIGRP

Network	Wildcard Mask
10.1.1.0	0.0.0.255
192.168.1.11	0.0.0.0

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-28

The figure illustrates the steps for configuring EIGRP across the tunnel:

Step 1 Select an existing or define a new EIGRP autonomous system (AS) number.

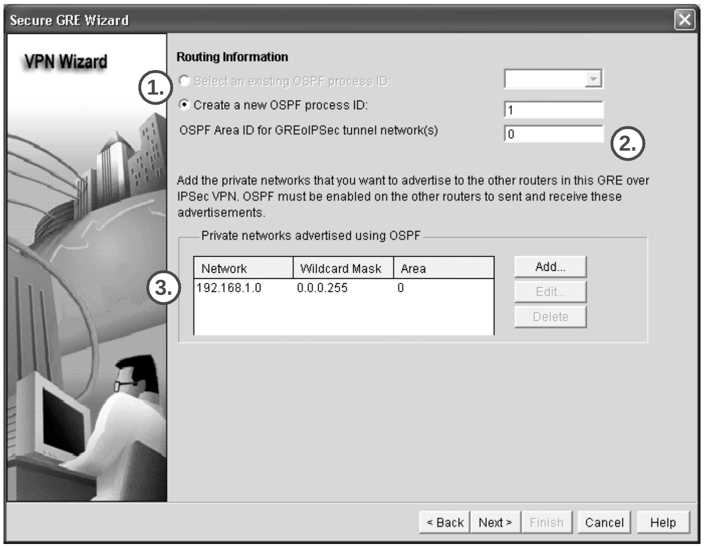
Step 2 Define one or more local subnets to be advertised to EIGRP neighbors.

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

Option 3: Dynamic Routing Using OSPF

The other protocol that can be used for dynamic routing in VPNs is Open Shortest Path First (OSPF).

Option 3: Dynamic Routing Using OSPF



Routing Information

○ Select an existing OSPF process ID:

● Create a new OSPF process ID: 1

OSPF Area ID for GREoIPSec tunnel network(s) 0

Add the private networks that you want to advertise to the other routers in this GRE over IPSec VPN. OSPF must be enabled on the other routers to sent and receive these advertisements.

Private networks advertised using OSPF

Network	Wildcard Mask	Area
192.168.1.0	0.0.0.255	0

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-29

The figure illustrates the steps to configure OSPF across the tunnel:

Step 1 Select an existing or define a new OSPF process number.

Step 2 Define an OSPF area number for the tunnels.

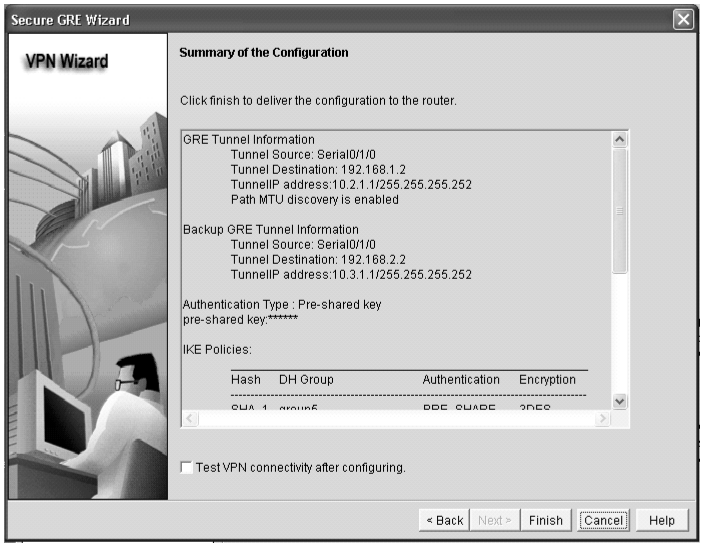
Step 3 Define one or more local subnets to be advertised to OSPF neighbors. An area number must also be specified for each subnet.

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 self-study.

Completing the Configuration

This topic describes how to complete the configuration by viewing the settings in the Summary window.

Review the Generated Configuration



Summary of the Configuration

Click finish to deliver the configuration to the router.

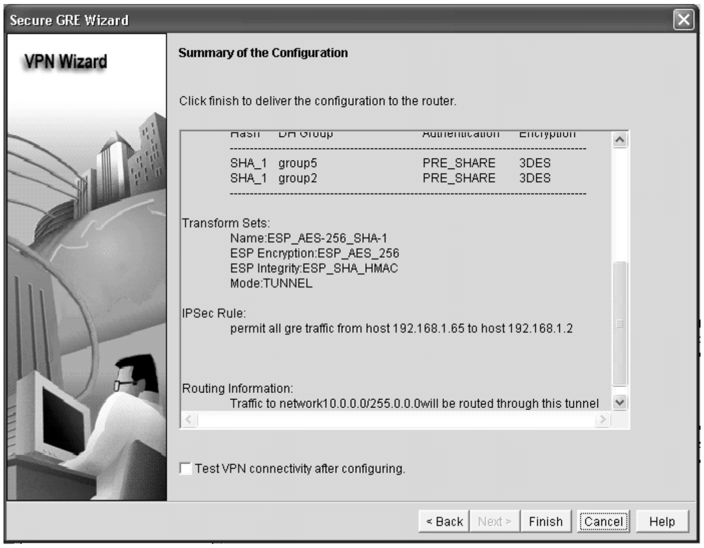
```
GRE Tunnel Information
          Tunnel Source: Serial0/1/0
          Tunnel Destination: 192.168.1.2
          TunnelIP address:10.2.1.1/255.255.255.252
          Path MTU discovery is enabled

Backup GRE Tunnel Information
          Tunnel Source: Serial0/1/0
          Tunnel Destination: 192.168.2.2
          TunnelIP address:10.3.1.1/255.255.255.252

Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:
          ____________________________________________________________
          Hash    DH Group                 Authentication   Encryption
          ------------------------------------------------------------
          SHA_1   group5                   PRE_SHARE        3DES
```

☐ Test VPN connectivity after configuring.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-31

Review the Generated Configuration (Cont.)



Summary of the Configuration

Click finish to deliver the configuration to the router.

```
          Hash    DH Group                 Authentication   Encryption
          ------------------------------------------------------------
          SHA_1   group5                   PRE_SHARE        3DES
          SHA_1   group2                   PRE_SHARE        3DES
          ------------------------------------------------------------

Transform Sets:
          Name:ESP_AES-256_SHA-1
          ESP Encryption:ESP_AES_256
          ESP Integrity:ESP_SHA_HMAC
          Mode:TUNNEL

IPSec Rule:
          permit all gre traffic from host 192.168.1.65 to host 192.168.1.2



Routing Information:
          Traffic to network10.0.0.0/255.0.0.0will be routed through this tunnel
```

☐ Test VPN connectivity after configuring.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-32

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

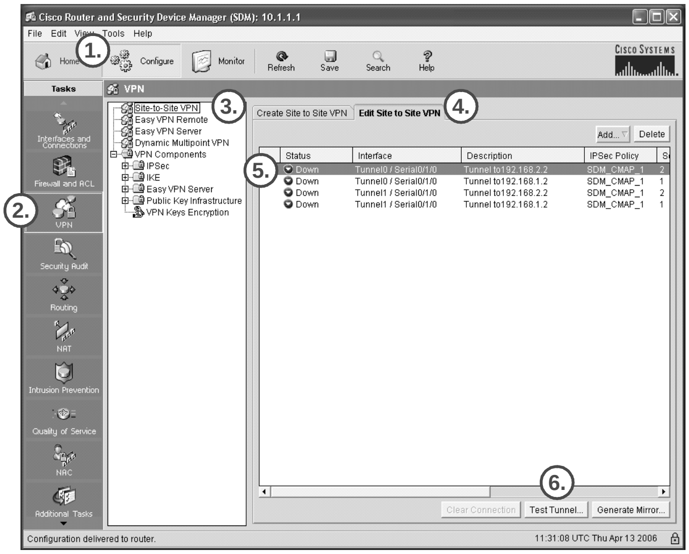
At the end, the wizard will present a summary of the configured parameters. You can go back to correct the configuration in case you have made a mistake. Click the **Finish** button to complete the configuration.

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 self-study.

Test Tunnel Configuration and Operation

After creating the GRE over IPsec site-to-site tunnel, you can immediately see its status.

Test Tunnel Configuration and Operation



Status	Interface	Description	IPSec Policy	S
Down	Tunnel0 / Serial0/1/0	Tunnel to192.168.2.2	SDM_CMAP_1	2
Down	Tunnel0 / Serial0/1/0	Tunnel to192.168.1.2	SDM_CMAP_1	1
Down	Tunnel1 / Serial0/1/0	Tunnel to192.168.2.2	SDM_CMAP_1	2
Down	Tunnel1 / Serial0/1/0	Tunnel to192.168.1.2	SDM_CMAP_1	1

Configuration delivered to router.

11:31:08 UTC Thu Apr 13 2006

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-33

You can also run a test to determine the configuration correctness of the tunnel, or generate a mirroring configuration that is required on the other end of the tunnel. This is useful if the other router does not have SDM and you have to use the command-line interface (CLI) to configure the tunnel.

To test the tunnel, follow this procedure:

Step 1 Click the **Configure** icon in the top horizontal navigation bar to enter the configuration page.

Step 2 Click the **VPN** icon in the left vertical navigation bar to open the VPN page.

Step 3 Choose the **Site to Site VPN** wizard from the list in the middle section.

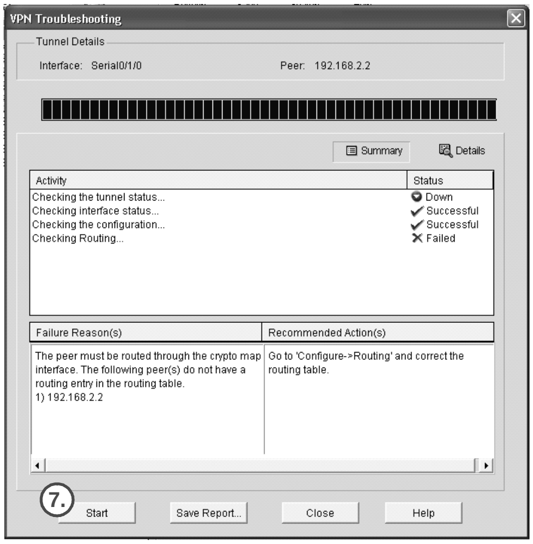
Step 4 Click the **Edit Site to Site VPN** tab in the section on the right side.

Step 5 Choose the tunnel that you want to test.

Step 6 Click the **Test Tunnel** button.

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

Test Tunnel Configuration and Operation (Cont.)



Tunnel Details

Interface: Serial0/1/0 Peer: 192.168.2.2

Activity	Status
Checking the tunnel status...	● Down
Checking interface status...	✓ Successful
Checking the configuration...	✓ Successful
Checking Routing...	✗ Failed

Failure Reason(s)	Recommended Action(s)
The peer must be routed through the crypto map interface. The following peer(s) do not have a routing entry in the routing table. 1) 192.168.2.2	Go to 'Configure->Routing' and correct the routing table.

© 2006 Cisco Systems, Inc. All rights reserved.

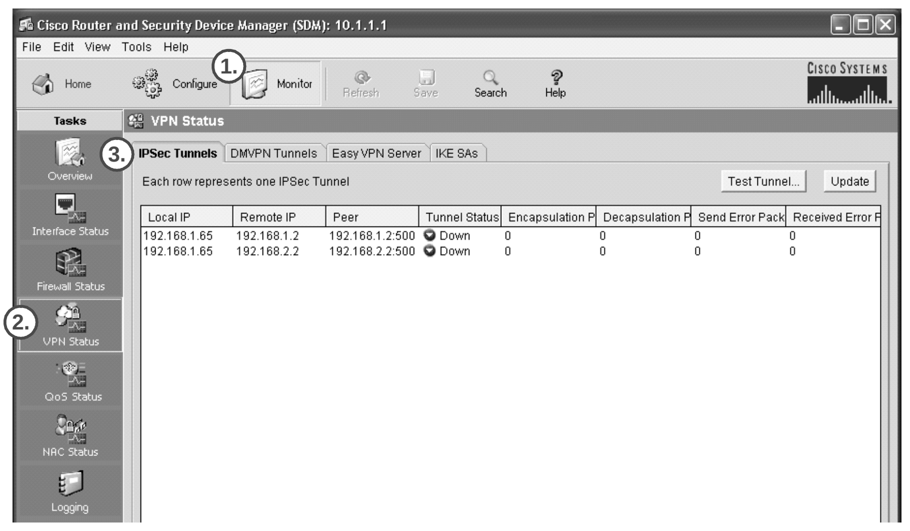
Step 7 Click the **Start** button and wait until the test is completed. For each failed task, the reason and recommended actions to resolve the issue are listed in the bottom part of the window.

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

Monitor Tunnel Operation

Use the monitoring page to display the status of the tunnel.

Monitor Tunnel Operation



Each row represents one IPSec Tunnel

Local IP	Remote IP	Peer	Tunnel Status	Encapsulation P	Decapsulation P	Send Error Pack	Received Error F
192.168.1.65	192.168.1.2	192.168.1.2:500	Down	0	0	0	0
192.168.1.65	192.168.2.2	192.168.2.2:500	Down	0	0	0	0

© 2006 Cisco Systems, Inc. All rights reserved.

To see all IPsec tunnels, their parameters, and status, follow this procedure:

Step 1 Click the **Monitor** icon in the top horizontal navigation bar.

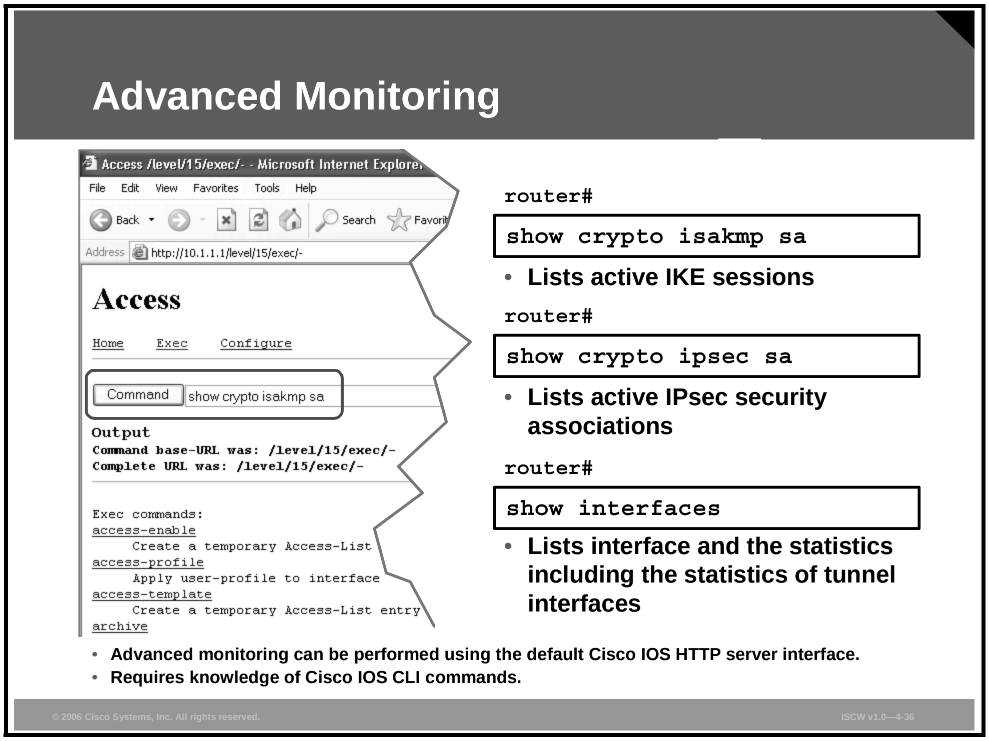
Step 2 Click the **VPN Status** icon in the left vertical navigation bar.

Step 3 Click the **IPSec Tunnels** tab.

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

Advanced Monitoring

The basic Cisco IOS web interface also allows you to use the web interface to enter Cisco IOS CLI commands to monitor and troubleshoot the router.



Advanced Monitoring

Access /level/15/exec/- - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorit
Address http://10.1.1.1/level/15/exec/-
Access
Home Exec Configure
Command

```
show crypto isakmp sa

Output
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-

Exec commands:
access-enable
     Create a temporary Access-List
access-profile
     Apply user-profile to interface
access-template
     Create a temporary Access-List entry
archive
```

```
router#
show crypto isakmp sa
```

- Lists active IKE sessions

```
router#
show crypto ipsec sa
```

- Lists active IPsec security associations

```
router#
show interfaces
```

- Lists interface and the statistics including the statistics of tunnel interfaces

- Advanced monitoring can be performed using the default Cisco IOS HTTP server interface.
- Requires knowledge of Cisco IOS CLI commands.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-36

The table lists three of the most useful **show** commands to determine the status of IPsec VPN connections.

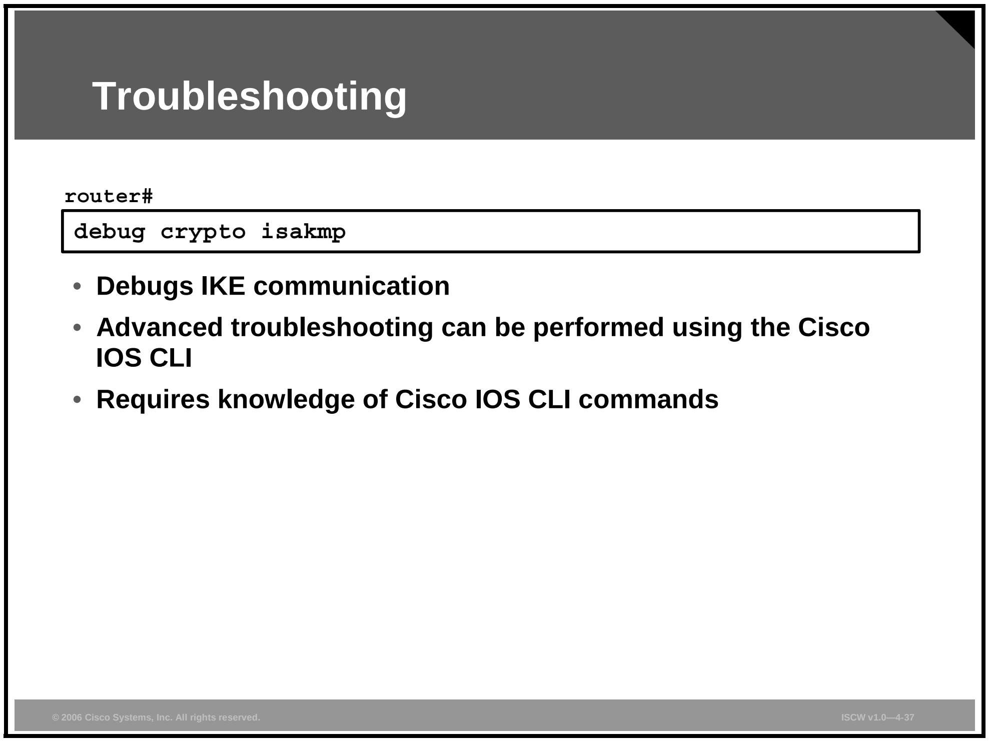
show Commands

Command	Description
`show crypto isakmp sa`	To display all current IKE SAs, use the **show crypto isakmp sa** command in EXEC mode. QM_IDLE status indicates an active IKE SA.
`show crypto ipsec sa`	To display the settings used by current SAs, use the **show crypto ipsec sa** command in EXEC mode. Non-zero encryption and decryption statistics can indicate a working set of IPsec SAs.
`show interfaces`	Display statistics for all interfaces configured on the router, including the tunnel 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 self-study.

Troubleshooting

You should use a terminal to connect to the Cisco IOS router if you want to use debugging commands to troubleshoot VPN connectivity.



Troubleshooting

```
router#
debug crypto isakmp
```

- **Debugs IKE communication**
- **Advanced troubleshooting can be performed using the Cisco IOS CLI**
- **Requires knowledge of Cisco IOS CLI commands**

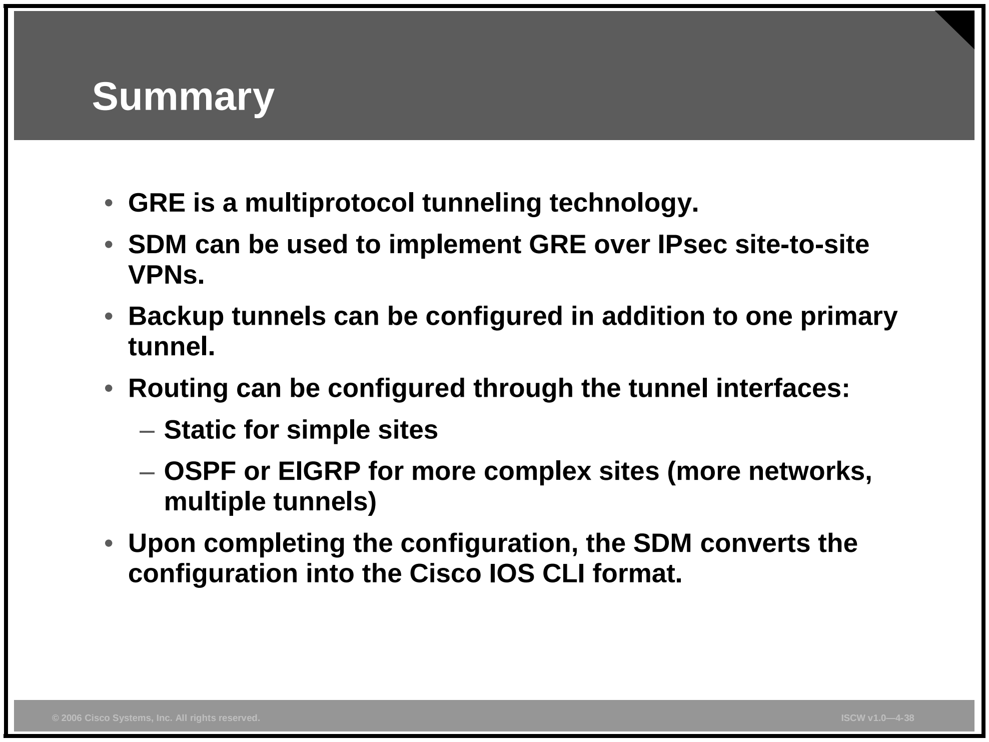
© 2006 Cisco Systems, Inc. All rights reserved.

The **debug crypto isakmp** EXEC command displays detailed information about the IKE Phase 1 and Phase 2 negotiation processes.

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

Summary

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



Summary

- GRE is a multiprotocol tunneling technology.
- SDM can be used to implement GRE over IPsec site-to-site VPNs.
- Backup tunnels can be configured in addition to one primary tunnel.
- Routing can be configured through the tunnel interfaces:
  - Static for simple sites
  - OSPF or EIGRP for more complex sites (more networks, multiple tunnels)
- Upon completing the configuration, the SDM converts the configuration into the Cisco IOS CLI format.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-38

References

For additional information, refer to these resources:

- Complete information about EtherType values at: http://www.iana.org/assignments/ethernet-numbers
- Information about GRE at: http://www.ietf.org/rfc/rfc1701.txt

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

Lesson 5

Configuring High-Availability Options

Overview

This lesson describes some of the possible designs used to provide a highly-available IPsec virtual private network (VPN). The lesson describes the backup peer option that uses Hot Standby Routing Protocol (HSRP) to provide redundant devices, and stateless failover and HSRP with Stateful Switchover (SSO) to provide stateful failover for IPsec VPN sessions.

Objectives

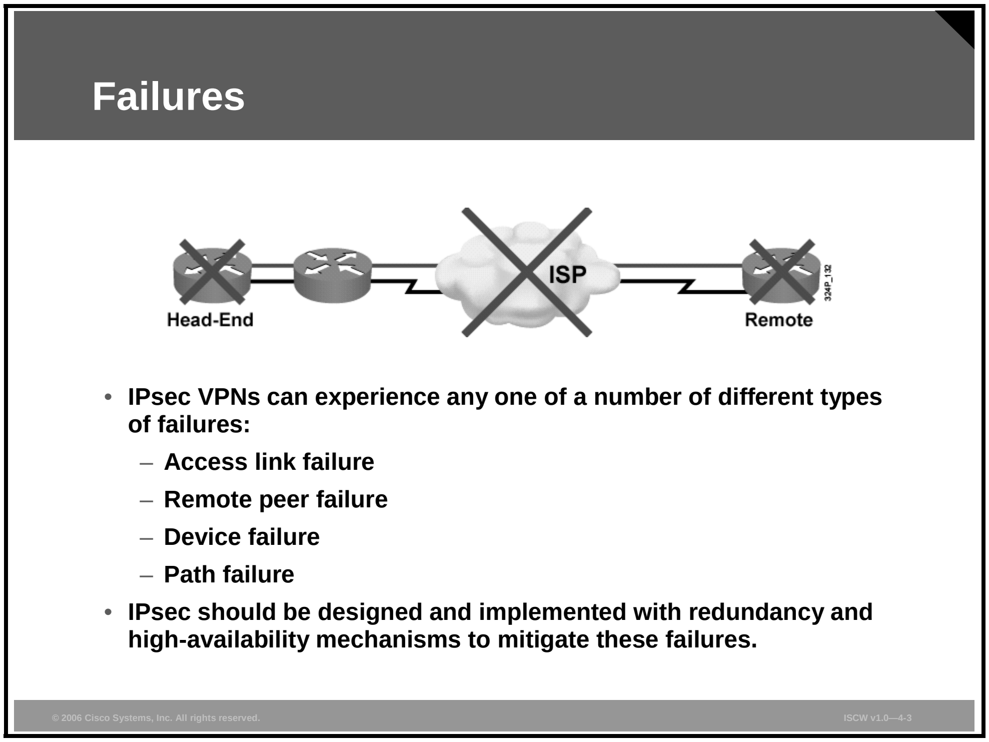
Upon completing this lesson, you will be able to describe the procedure to configure VPN backup interfaces. This ability includes being able to meet these objectives:

- Explain how high availability of IPsec VPNs is achieved
- Explain the failover option of backup IPsec peers
- Explain the use of HSRP for IOS IPsec VPN resiliency
- Explain IPsec stateful failover
- Explain how to back up a WAN connection by using an IPsec VPN

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

High Availability for IOS IPsec VPNs

This topic describes high availability for Cisco IOS IPsec VPNs.


Head-End
ISP
Remote
324P_132

Failures

- **IPsec VPNs can experience any one of a number of different types of failures:**
  - **Access link failure**
  - **Remote peer failure**
  - **Device failure**
  - **Path failure**
- **IPsec should be designed and implemented with redundancy and high-availability mechanisms to mitigate these failures.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-3

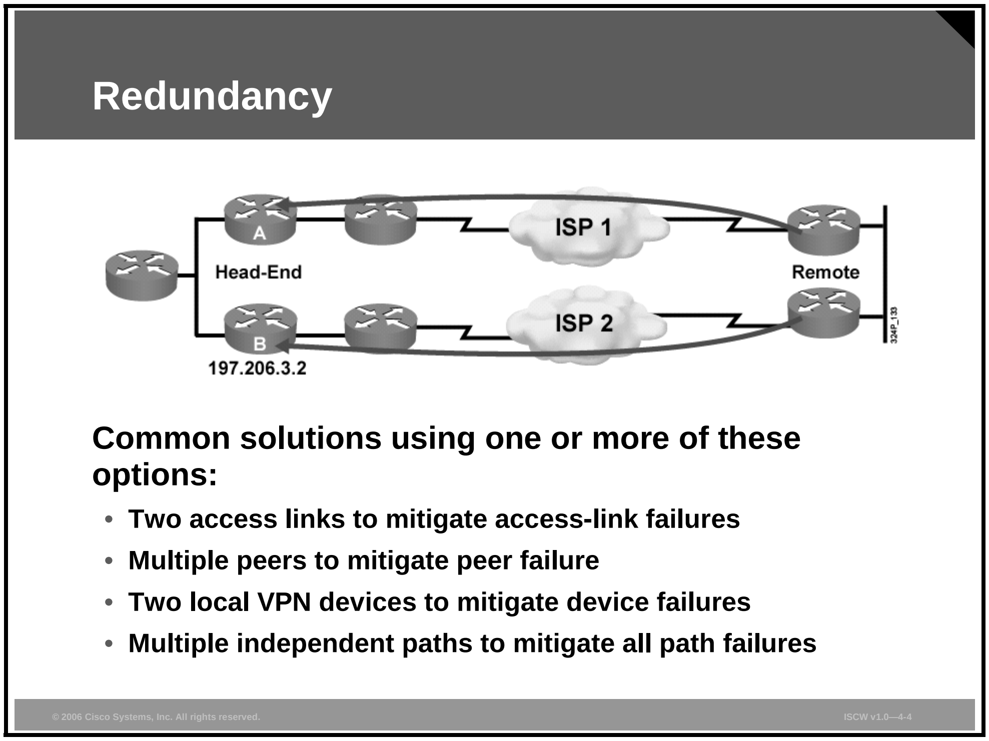
IPsec-based VPNs provide connectivity between distant sites using an untrusted transport network. Network connectivity consists of links, devices, or sometimes just paths across networks whose topology is not known. Any of these components can fail, making the VPN inoperable.

IPsec VPNs requiring high availability should be designed and implemented with redundancy in order to survive failures.

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

Redundancy

The figure illustrates an implementation of IPsec in which maximum failover is configured.



Redundancy

Common solutions using one or more of these options:

- **Two access links to mitigate access-link failures**
- **Multiple peers to mitigate peer failure**
- **Two local VPN devices to mitigate device failures**
- **Multiple independent paths to mitigate all path failures**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-4

The duplication techniques must be coupled with high-availability mechanisms.

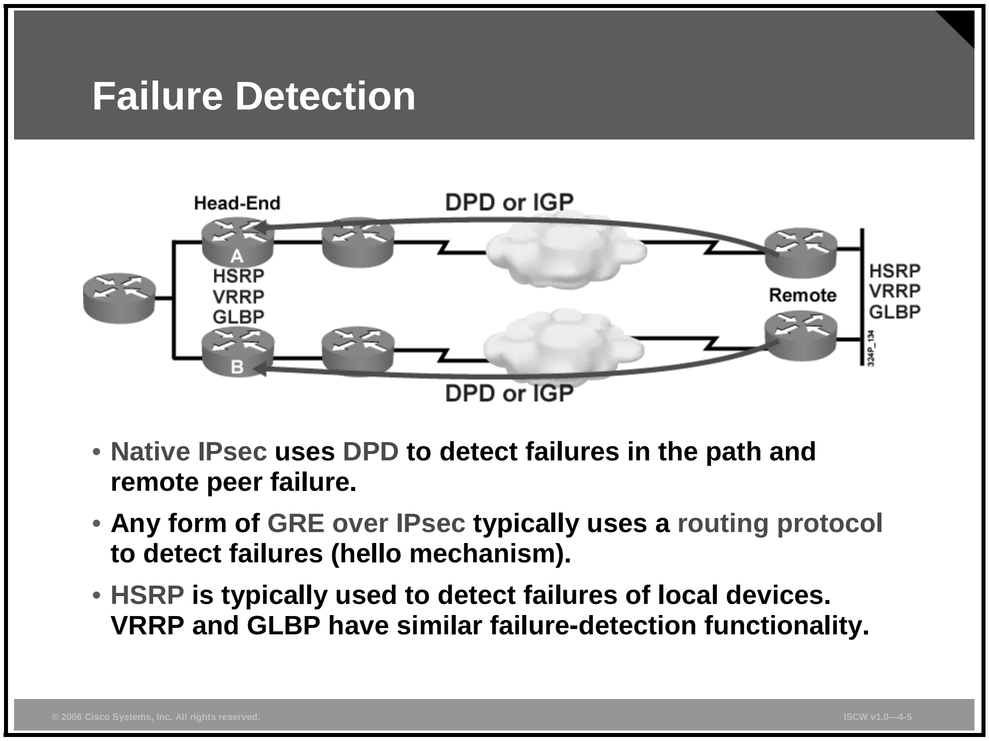
The figure illustrates an implementation of IPsec in which every component has been duplicated in order for the solution to survive any possible single failure:

- Two access links are used on both ends to mitigate a failure of any access link.
- The remote site is configured with two remote peers in case any one of them fails.
- Both sites use two VPN gateways to mitigate local device failures.
- Multiple independent paths are used between remote sites to mitigate an unknown failure anywhere in any of the paths.

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

Failure Detection

The figure illustrates the usage of HA mechanisms to detect failures and reroute to secondary paths.



Failure Detection

- **Native IPsec uses DPD to detect failures in the path and remote peer failure.**
- **Any form of GRE over IPsec typically uses a routing protocol to detect failures (hello mechanism).**
- **HSRP is typically used to detect failures of local devices. VRRP and GLBP have similar failure-detection functionality.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-5

Failures in the IPsec path are typically detected using one of these two mechanisms:

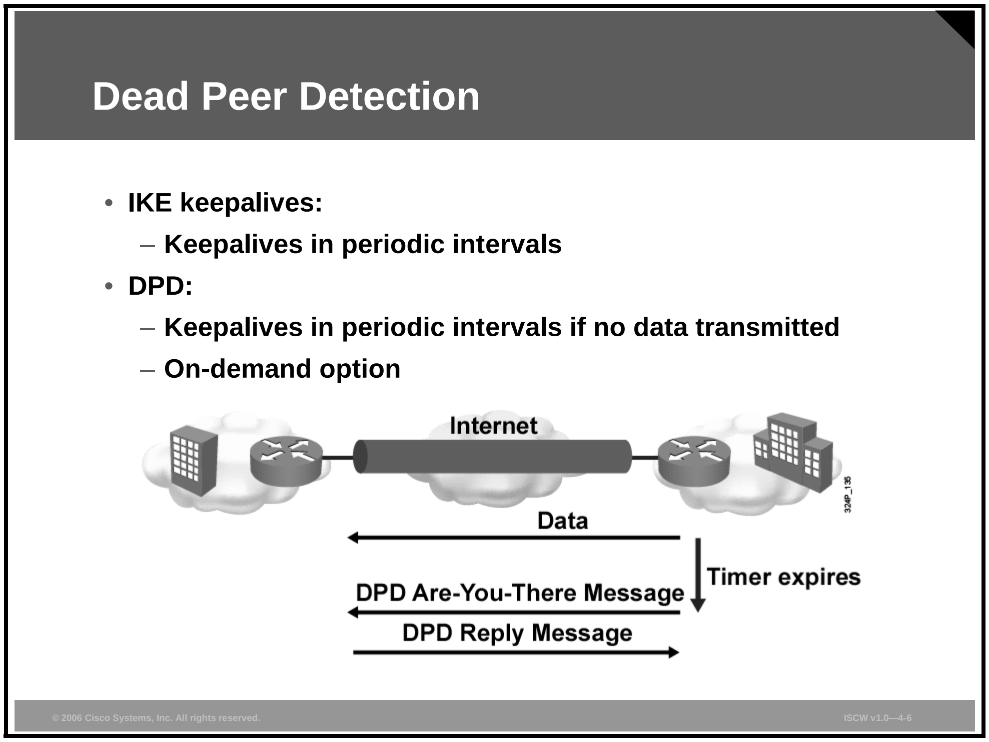
- Dead peer detection (DPD), which is a native Internet Key Exchange (IKE) mechanism similar to old proprietary IKE keepalives.
- Alternatively, any routing protocol running across the IPsec tunnel will detect failures using the hello mechanism of the routing protocol.

Detecting failures of local devices is typically achieved by using the Cisco-proprietary HSRP. Virtual Router Redundancy Protocol (VRRP) is a standardized version of HSRP, and Gateway Load Balancing Protocol (GLBP) is a protocol that can provide load balancing across all the devices in the failover group (all devices are active).

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

How DPD and Cisco IOS Keepalive Features Work

DPD and Cisco IOS keepalives function on the basis of a timer. If the timer is set for 10 seconds, the router will send a hello message every 10 seconds (unless, of course, the router receives a hello message from the peer). The benefit of IOS keepalives and periodic DPD is earlier detection of dead peers. However, IOS keepalives and periodic DPD rely on periodic messages that have to be sent with considerable frequency. The result of sending frequent messages is that the communicating peers must encrypt and decrypt more packets.



Dead Peer Detection

- **IKE keepalives:**
  - **Keepalives in periodic intervals**
- **DPD:**
  - **Keepalives in periodic intervals if no data transmitted**
  - **On-demand option**

© 2006 Cisco Systems, Inc. All rights reserved.   ISCW v1.0—4-6

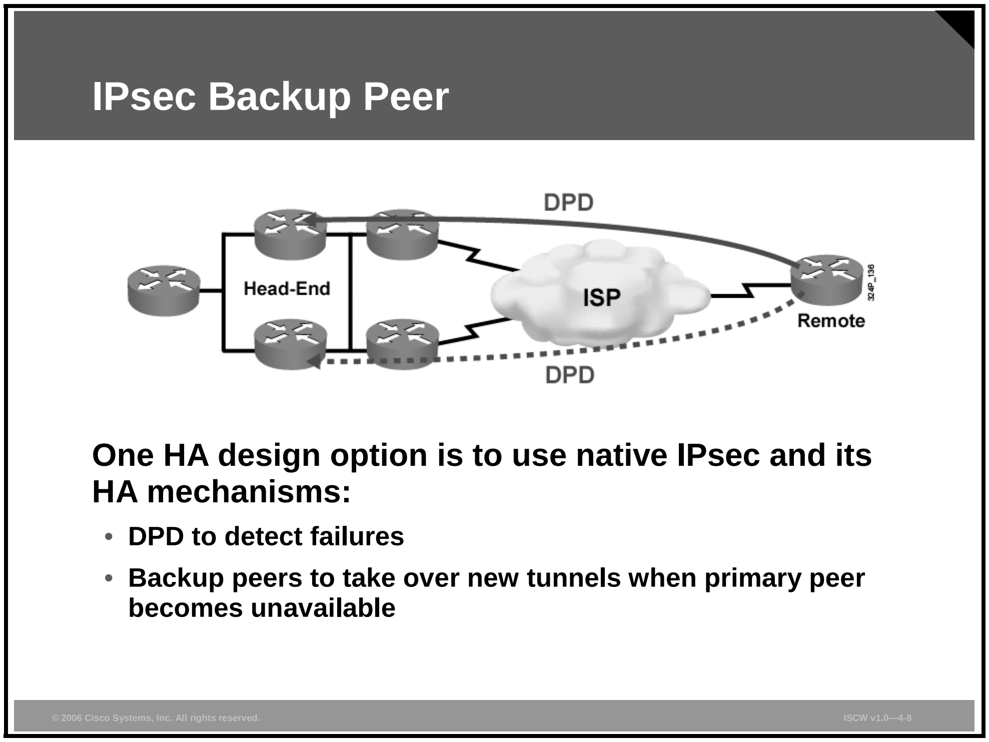
DPD also has an on-demand approach. The contrasting on-demand approach is the default. With on-demand DPD, messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message. If a peer is dead and the router never has any traffic to send to the peer, the router will not find out until the IKE or IPsec security association (SA) has to be rekeyed (the liveliness of the peer is unimportant if the router is not trying to communicate with the peer). On the other hand, if the router has traffic to send to the peer, and the peer does not respond, the router will initiate a DPD message to determine the state of the peer.

Note In Cisco IOS software Release 12.2(8)T, the Cisco proprietary keepalives were replaced with standard DPD. Two peers may still use proprietary keepalives if one of them has an older Cisco IOS software release.

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

IPsec Backup Peer

This topic describes IPsec backup peers.



IPsec Backup Peer

One HA design option is to use native IPsec and its HA mechanisms:

- **DPD to detect failures**
- **Backup peers to take over new tunnels when primary peer becomes unavailable**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-8

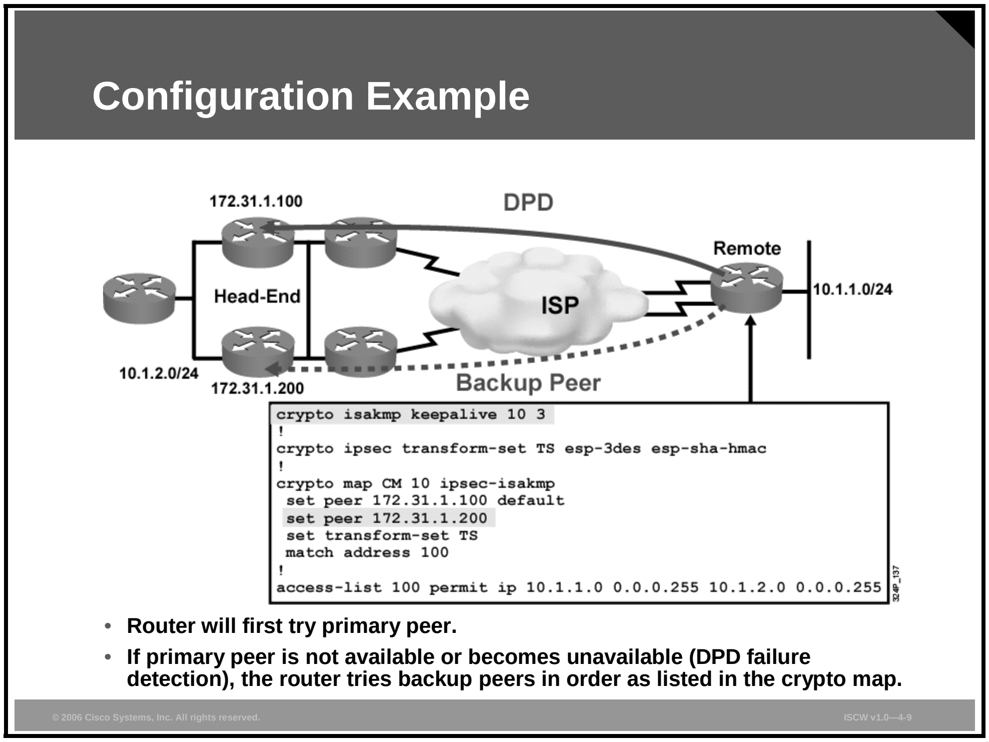
Using DPD and Cisco IOS Keepalive Features with Multiple Peers in the Crypto Map

DPD and IOS keepalive features can be used in conjunction with multiple peers in the crypto map to allow for stateless failover. DPD allows the router to detect a dead IKE peer, and when the router detects the dead state, the router deletes the IPsec and IKE SAs to the peer. If you configure multiple peers, the router will switch over to the next listed peer for a stateless failover.

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

Configuration Example

The figure illustrates a sample configuration where DPD is enabled with a 10-second frequency and a 3-second retry frequency.



Configuration Example

```
crypto isakmp keepalive 10 3
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto map CM 10 ipsec-isakmp
 set peer 172.31.1.100 default
 set peer 172.31.1.200
 set transform-set TS
 match address 100
!
access-list 100 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
```

- **Router will first try primary peer.**
- **If primary peer is not available or becomes unavailable (DPD failure detection), the router tries backup peers in order as listed in the crypto map.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-9

The crypto map is configured with a backup peer that will be used when DPD determines that the primary peer is no longer responding.

Note When the **crypto isakmp keepalive** command is configured, the IOS software negotiates the use of proprietary IOS keepalives or standard DPDs, depending on which protocol the peer supports.

crypto isakmp keepalive

To allow the gateway to send DPD messages to the peer, use the **crypto isakmp keepalive** command in global configuration mode. To disable keepalives, use the **no** form of this command.

crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]

crypto isakmp keepalive **Parameters**

Parameter	Description
seconds	Number of seconds between DPD messages; the range is from 10 to 3600 seconds. If you do not specify a time interval, you will receive an error message.
retries	(Optional) Number of seconds between DPD retries if the DPD message fails; the range is from 2 to 60 seconds. If unspecified, the default is 2 seconds.
periodic	(Optional) DPD messages are sent at regular intervals.

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

Parameter	Description
`on-demand`	(Optional) The default behavior. DPD retries are sent on demand. Note that because this option is the default, the **on-demand** keyword does not appear in configuration output.

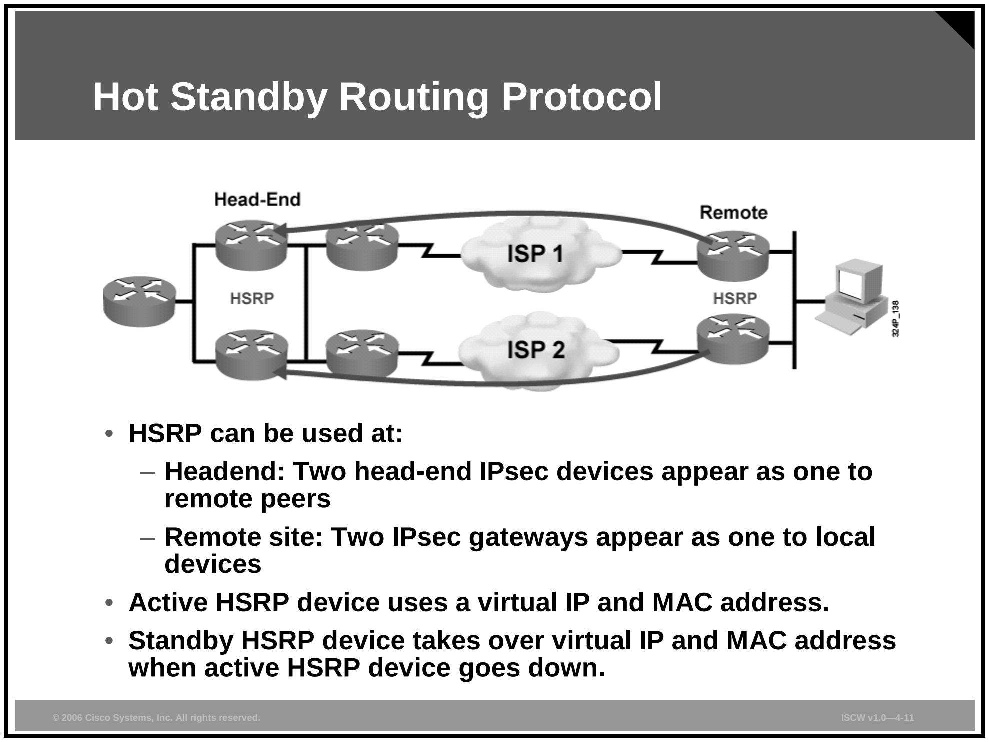
DPD is a keepalive scheme that allows the router to query the liveliness of its IKE peer.

Use the **periodic** keyword to configure your router so that DPD messages are forced at regular intervals. This forced approach results in earlier detection of dead peers than with the on-demand approach. If you do not configure the periodic option, the router defaults to the on-demand approach.

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

Hot Standby Routing Protocol

This topic describes HSRP.



Hot Standby Routing Protocol

- HSRP can be used at:
  - Headend: Two head-end IPsec devices appear as one to remote peers
  - Remote site: Two IPsec gateways appear as one to local devices
- Active HSRP device uses a virtual IP and MAC address.
- Standby HSRP device takes over virtual IP and MAC address when active HSRP device goes down.

© 2006 Cisco Systems, Inc. All rights reserved.

HSRP Operation

A large class of legacy hosts that do not support dynamic router discovery are typically configured with a default gateway (router). Running a dynamic router discovery mechanism on every host may not be feasible for a number of reasons, including administrative overhead, processing overhead, security issues, or lack of a protocol implementation for some platforms. HSRP provides failover services to these hosts.

Using HSRP, a set of routers works in concert to present the illusion of a single virtual router to the hosts on the LAN. This set of routers is known as an *HSRP group* or a *standby group*. A single router elected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the *active router*. Another router is elected as the *standby router*. In the event that the active router fails, the standby router assumes the packet-forwarding duties of the active router. Although an arbitrary number of routers may run HSRP, only the active router forwards the packets sent to the virtual router.

To minimize network traffic, only the active and standby routers send periodic HSRP messages after the protocol has completed the election process. If the active router fails, the standby router takes over as the active router. If the standby router fails or becomes the active router, another router is elected as the standby router.

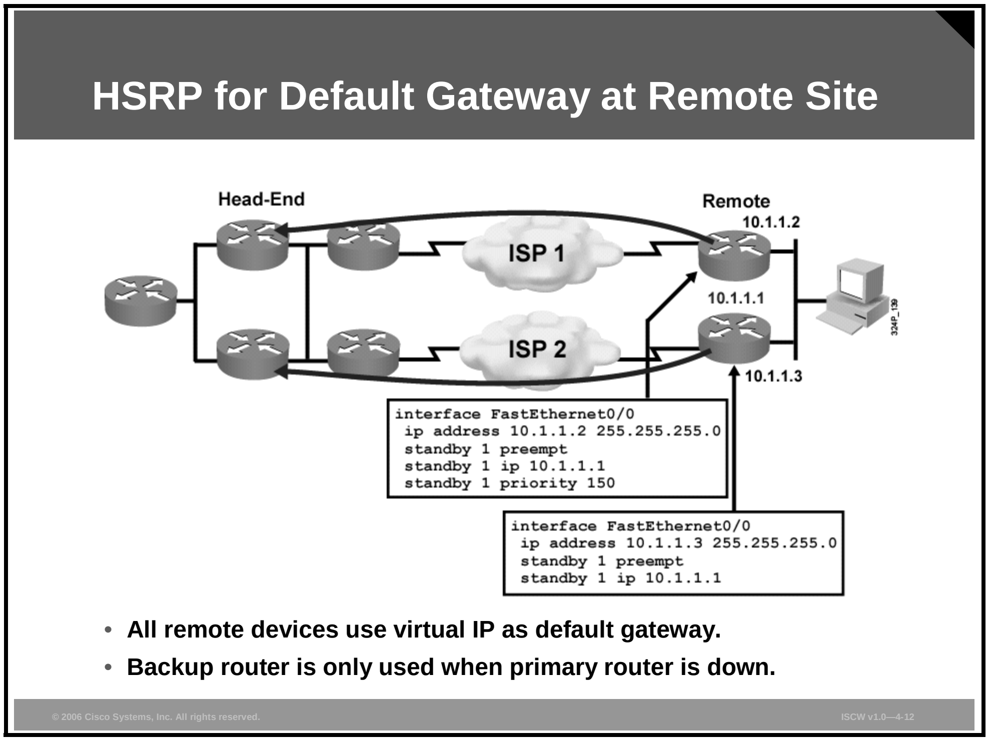
On a particular LAN, multiple hot standby groups may coexist and overlap. Each standby group emulates a single virtual router. The individual routers may participate in multiple groups. In this case, the router maintains separate state and timers for each group.

Each standby group has a single, well-known MAC address as well as an IP address.

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

HSRP for Default Gateway at Remote Site

The figure illustrates the usage of HSRP at remote sites where devices behind the pair of IPsec gateways are configured with a static default gateway.



HSRP for Default Gateway at Remote Site

```
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.0
 standby 1 preempt
 standby 1 ip 10.1.1.1
 standby 1 priority 150
```

```
interface FastEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 standby 1 preempt
 standby 1 ip 10.1.1.1
```

- **All remote devices use virtual IP as default gateway.**
- **Backup router is only used when primary router is down.**

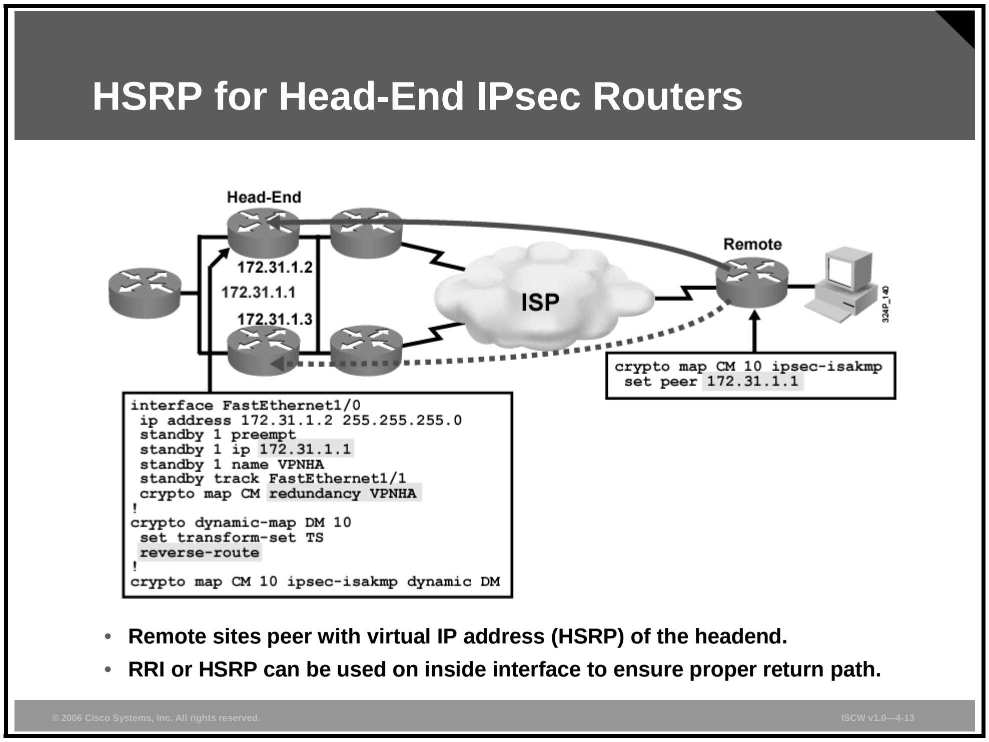
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-12

To ensure that a single device failure can be mitigated, the default gateway points to an HSRP virtual IP address, thus ensuring that the default IP gateway is always present.

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

HSRP for Headend IPsec Routers

The figure illustrates the usage of HSRP to make the pair of headend VPN routers appear as a single device. A failure of the primary device will result in the IPsec tunnels failing, but the remote sites will reestablish the tunnels to the other router using the same peer address.



HSRP for Head-End IPsec Routers

```
crypto map CM 10 ipsec-isakmp
 set peer 172.31.1.1
```

```
interface FastEthernet1/0
 ip address 172.31.1.2 255.255.255.0
 standby 1 preempt
 standby 1 ip 172.31.1.1
 standby 1 name VPNHA
 standby track FastEthernet1/1
 crypto map CM redundancy VPNHA
!
crypto dynamic-map DM 10
 set transform-set TS
 reverse-route
!
crypto map CM 10 ipsec-isakmp dynamic DM
```

- **Remote sites peer with virtual IP address (HSRP) of the headend.**
- **RRI or HSRP can be used on inside interface to ensure proper return path.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-13

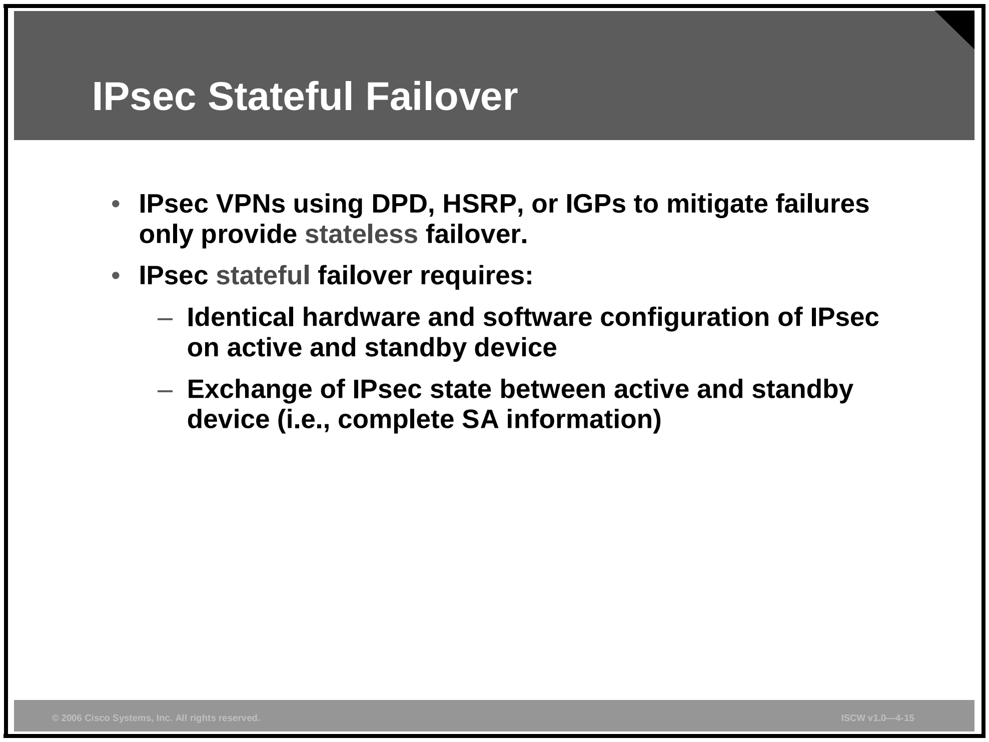
Devices behind the headend VPN routers can find the return path toward remote sites using one of these two mechanisms:

- HSRP on the inside interface, configured similarly to the HSRP on the outside interface
- Reverse Route Injection (RRI) to inject remote networks into an Interior Gateway Protocol (IGP) and distribute it to other routers 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 self-study.

IPsec Stateful Failover

This topic describes IPsec stateful failover.



IPsec Stateful Failover

- **IPsec VPNs using DPD, HSRP, or IGPs to mitigate failures only provide stateless failover.**
- **IPsec stateful failover requires:**
  - **Identical hardware and software configuration of IPsec on active and standby device**
  - **Exchange of IPsec state between active and standby device (i.e., complete SA information)**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-15

Stateless failover means that when there is a failure, a tunnel will typically go down and will have to be reestablished.

To provide a *stateful* failover, a pair of devices must run in a virtually identical environment (same hardware, software, configuration, and so forth) and exchange live information about IPsec SAs.

Restrictions for Stateful Failover for IPsec

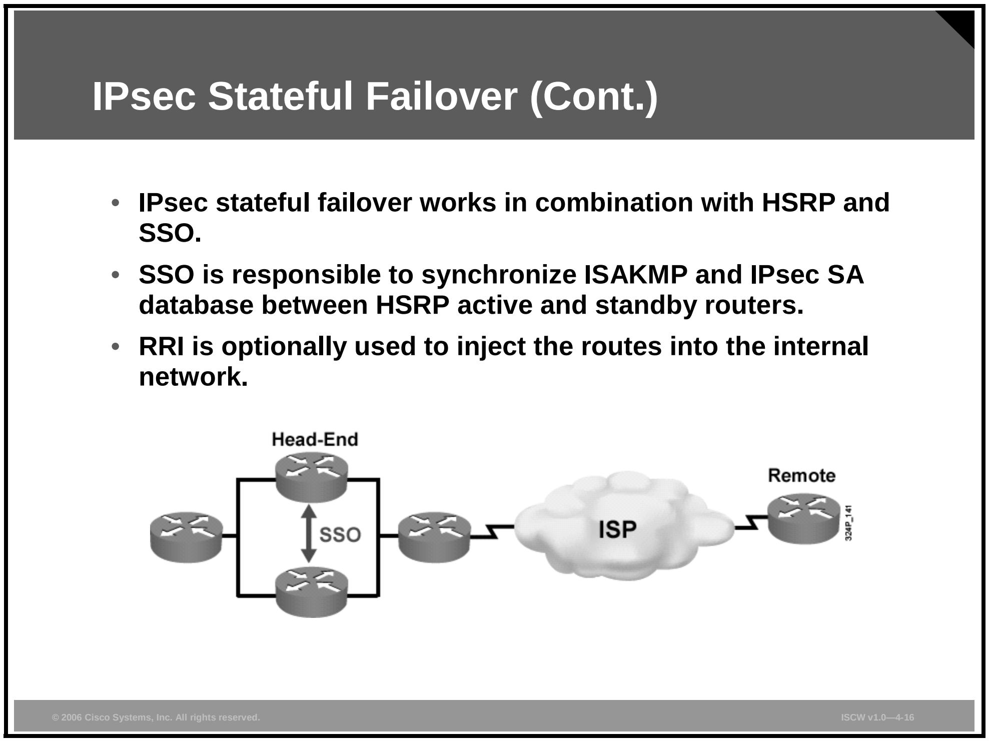
When configuring redundancy for a VPN, these restrictions exist:

- Both the active and standby devices must run the identical Cisco IOS software release, and both the active and standby devices must be connected via hub or switch.
- Only the VPN Acceleration Module (VAM), VPN Acceleration Module 2 (VAM2), and AIM-VPN/HPII hardware encryption accelerators are supported.
- Only “box-to-box” failover is supported; that is, intrachassis failover is currently not supported.
- WAN interfaces between the active (primary) router and the standby (secondary) router are not supported. HSRP requires inside interfaces and outside interfaces to be connected via LANs.
- Load balancing is not supported; that is, no more than one device in a redundancy group can be active at any given time.
- Stateful failover of IPsec with Layer 2 Tunneling Protocol (L2TP) is not supported.
- IKE keepalives are not supported. Enabling this functionality will cause the connection to be torn down after the standby router assumes ownership control. However, DPD and periodic DPD are supported.

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

- IPsec idle timers are not supported when used with stateful failover.
- A stateful failover crypto map applied to an interface in a virtual routing and forwarding (VRF) instance is not supported. However, VRF-aware IPsec features are supported when a stateful failover crypto map is applied to an interface in the global VRF.
- Stateful failover is not compatible or interoperable with the State Synchronization Protocol (SSP) version of stateful failover (which is available in Cisco IOS software Release 12.2YX1 and Cisco IOS software Release 12.2SU).

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



IPsec Stateful Failover (Cont.)

- **IPsec stateful failover works in combination with HSRP and SSO.**
- **SSO is responsible to synchronize ISAKMP and IPsec SA database between HSRP active and standby routers.**
- **RRI is optionally used to inject the routes into the internal network.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-16

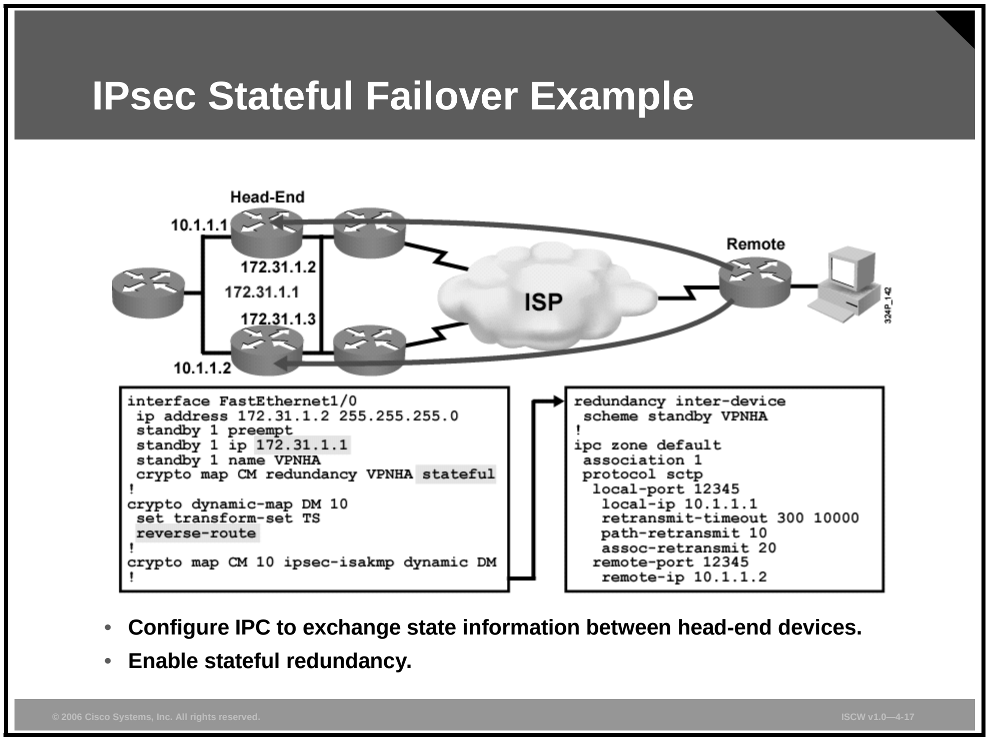
Stateful failover for IPsec, introduced in Cisco IOS software Release 12.3(11)T, enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent to the user and does not require adjustment or reconfiguration of any remote peer.

Stateful failover for IPsec is designed to work in conjunction with SSO and HSRP. HSRP provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from failures in network edge devices or access circuits. That is, HSRP monitors both the inside and outside interfaces so that if either interface goes down, the whole router is deemed to be down and ownership of IKE and IPsec SAs is passed to the standby router (which transitions to the HSRP active state). SSO allows the active and standby routers to share IKE and IPsec state information so that each router has enough information to become the active router at any time. To configure stateful failover for IPsec, you should enable HSRP, assign a virtual IP address, and enable the SSO protocol.

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

IPsec Stateful Failover Example

The figure illustrates a configuration for IPsec stateful failover.



IPsec Stateful Failover Example

```
interface FastEthernet1/0
 ip address 172.31.1.2 255.255.255.0
 standby 1 preempt
 standby 1 ip 172.31.1.1
 standby 1 name VPNHA
 crypto map CM redundancy VPNHA stateful
!
crypto dynamic-map DM 10
 set transform-set TS
 reverse-route
!
crypto map CM 10 ipsec-isakmp dynamic DM
!
```

```
redundancy inter-device
 scheme standby VPNHA
!
ipc zone default
 association 1
 protocol sctp
  local-port 12345
   local-ip 10.1.1.1
   retransmit-timeout 300 10000
   path-retransmit 10
   assoc-retransmit 20
  remote-port 12345
   remote-ip 10.1.1.2
```

- **Configure IPC to exchange state information between head-end devices.**
- **Enable stateful redundancy.**

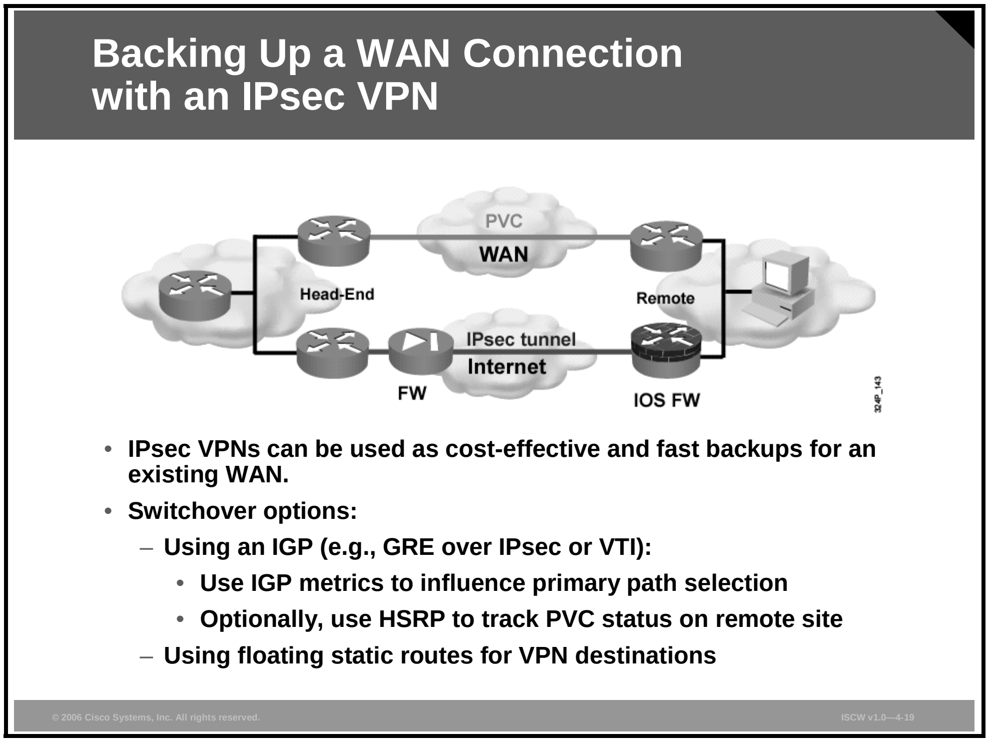
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-17

In the figure, the crypto map redundancy is configured with the **stateful** keyword, which requires HSRP to be configured in combination with SSO. The right part of the configuration example shows how the HSRP profile named VPNHA is configured to exchange IPsec state with the other HSRP router using Stream Control Transmission Protocol (SCTP) on source and destination port 12345.

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

Backing Up a WAN Connection with an IPsec VPN

This topic describes how you can back up a WAN connection by using an IPsec VPN.



Backing Up a WAN Connection with an IPsec VPN

- IPsec VPNs can be used as cost-effective and fast backups for an existing WAN.
- Switchover options:
  - Using an IGP (e.g., GRE over IPsec or VTI):
    - Use IGP metrics to influence primary path selection
    - Optionally, use HSRP to track PVC status on remote site
  - Using floating static routes for VPN destinations

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-19

The figure illustrates a scenario in which the WAN is backed up by an IPsec VPN. A failure of the primary permanent virtual circuit (PVC) should result in the two sites rerouting onto the IPsec VPN. This can easily be achieved if the same routing protocol, which is used in the WAN, is also deployed over the IPsec VPN. IGP metric tuning (for example, interface delay for Enhanced Interior Gateway Routing Protocol [EIGRP] or per-interface Open Shortest Path First [OSPF] cost) can be used to influence the primary and backup path selection.

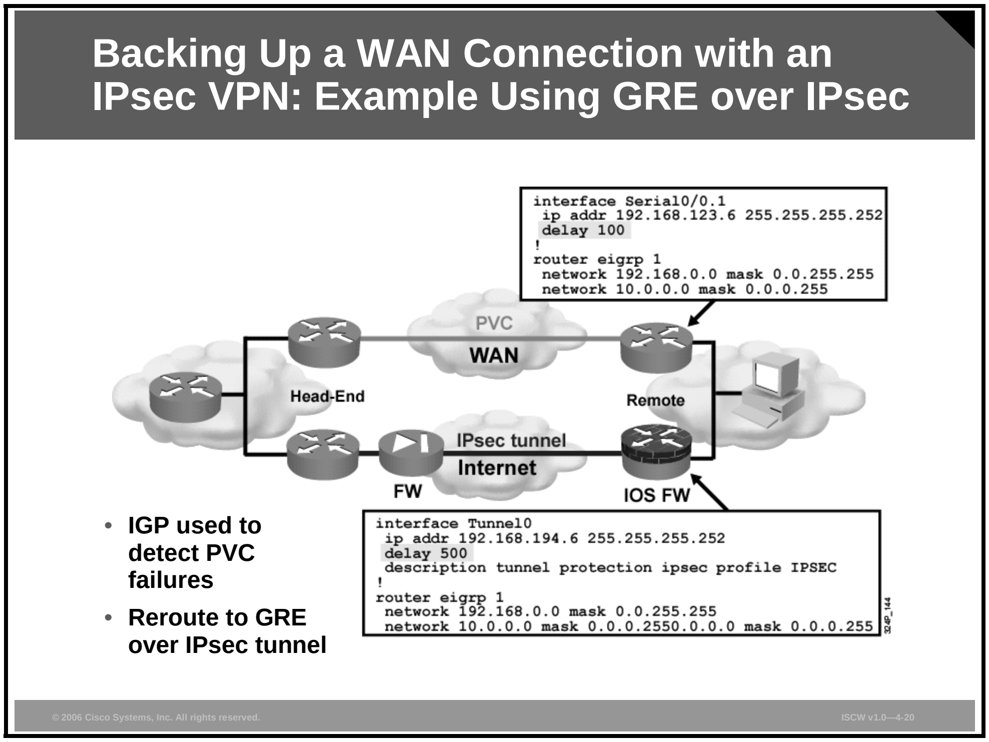
Note In order to run an IGP across an IPsec tunnel, you should use GRE over IPsec which provides a virtual point-to-point link. Alternatively, you can use a newer method in which virtual interfaces are used with native IPsec (no additional GRE headers are used).

An alternative is to use native IPsec and configure floating static routes (that is, routes with high administrative distance and, optionally, that are locally redistributed using a very high cost) for VPN destination that point to the Internet. A lost route from the WAN will result in the usage of the floating static route towards the Internet in which a crypto map will capture and encrypt the 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 self-study.

Backing Up a WAN Connection with an IPsec VPN: Example Using GRE over IPsec

The figure illustrates a partial example configuration in which GRE over IPsec tunnels are used to enable the usage of the WAN IGP across the VPN links.



Backing Up a WAN Connection with an IPsec VPN: Example Using GRE over IPsec

```
interface Serial0/0.1
 ip addr 192.168.123.6 255.255.255.252
 delay 100
!
router eigrp 1
 network 192.168.0.0 mask 0.0.255.255
 network 10.0.0.0 mask 0.0.0.255
```

```
interface Tunnel0
 ip addr 192.168.194.6 255.255.255.252
 delay 500
 description tunnel protection ipsec profile IPSEC
!
router eigrp 1
 network 192.168.0.0 mask 0.0.255.255
 network 10.0.0.0 mask 0.0.0.2550.0.0.0 mask 0.0.0.255
```

- **IGP used to detect PVC failures**
- **Reroute to GRE over IPsec tunnel**

© 2006 Cisco Systems, Inc. All rights reserved.

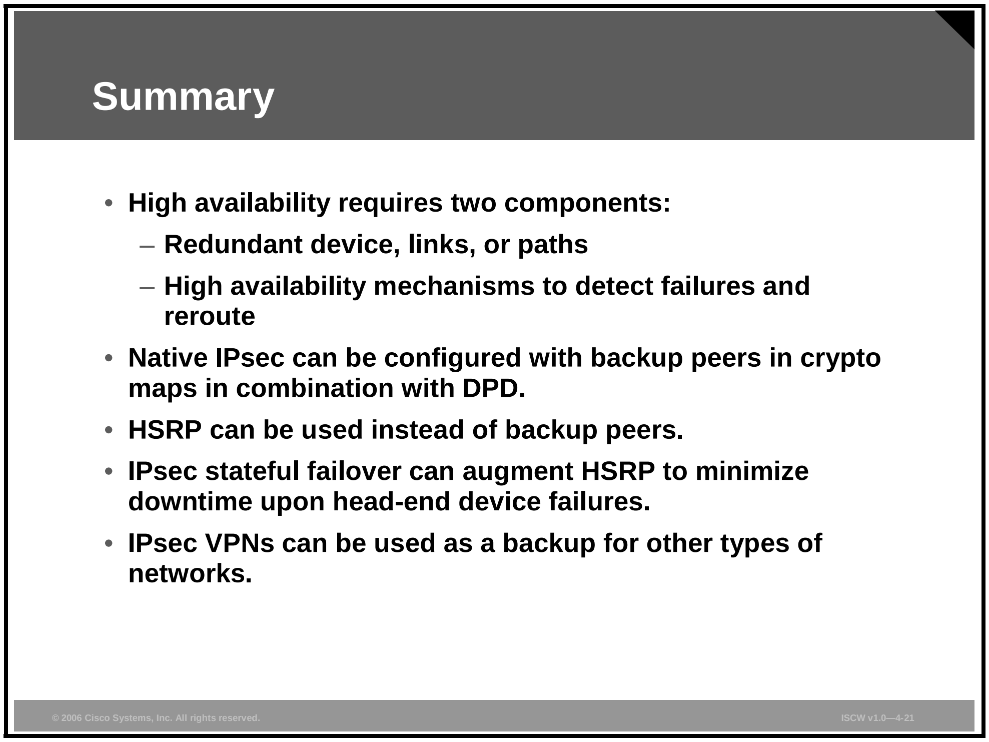
ISCW v1.0—4-20

The VPN links, however, are configured with longer delay to influence the EIGRP process to prefer the primary WAN link as long as it is functional.

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

Summary

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



Summary

- High availability requires two components:
  - Redundant device, links, or paths
  - High availability mechanisms to detect failures and reroute
- Native IPsec can be configured with backup peers in crypto maps in combination with DPD.
- HSRP can be used instead of backup peers.
- IPsec stateful failover can augment HSRP to minimize downtime upon head-end device failures.
- IPsec VPNs can be used as a backup for other types of networks.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-21

References

For additional information, refer to these resources:

- *Stateful Failover for IPSec* at http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d03f2.html

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

Lesson 6

Configuring Cisco Easy VPN and Easy VPN Server Using SDM

Overview

This lesson describes the configuration steps needed to configure a Cisco Easy virtual private network (VPN) Server using the Cisco Security Device Manager (SDM).

Objectives

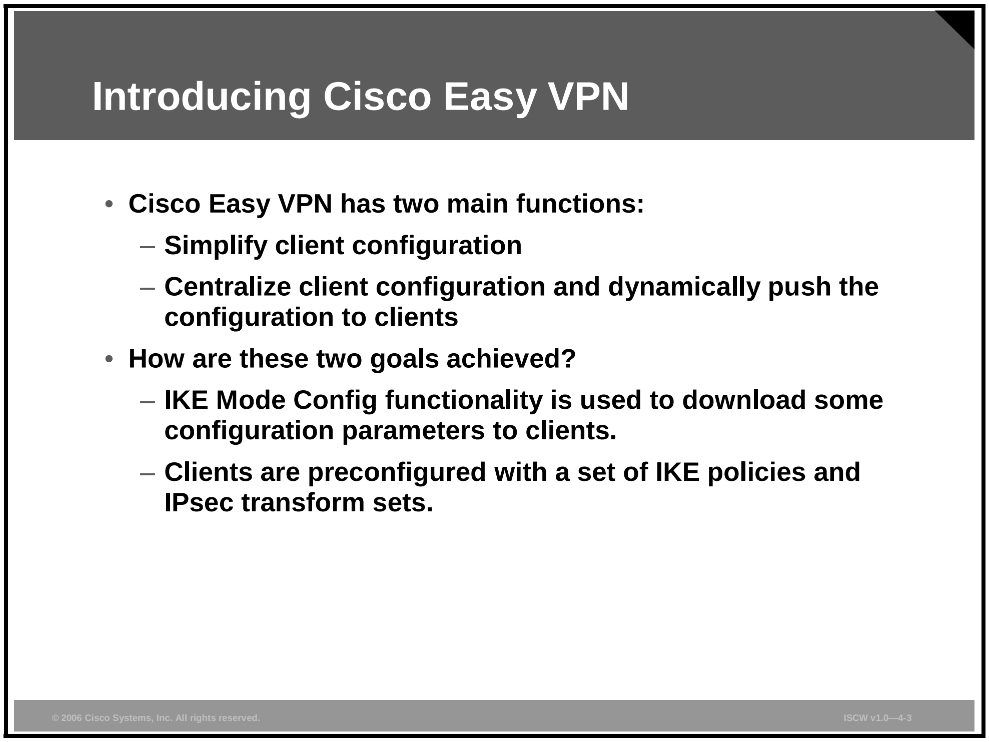
Upon completing this lesson, you will be able to describe the procedure to configure and verify a Cisco Easy VPN Server and an IPsec VPN, configured with Cisco Easy VPN, using SDM to support remote access VPNs. This ability includes being able to meet these objectives:

- Explain the general operation of Cisco Easy VPN including its benefits and the role of each of its components
- Describe the functionality provided by Cisco Easy VPN Server, explain the concept of dynamic crypto maps, and describe the functionality provided by Easy VPN Remote
- List the steps required to configure Cisco Easy VPN Server using SDM
- Describe each of the steps required to configure Cisco Easy VPN Server using SDM
- Explain how to configure IKE using the SDM wizard
- Explain how to configure the IPsec transform set using the SDM wizard
- Describe the locations where Easy VPN group policies can be stored
- Describe the locations where user records for Xauth can be stored
- Configure local group policies
- Explain how to complete the configuration by viewing the settings in the Summary window

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

Introducing Cisco Easy VPN

This topic describes the role of each component of Cisco Easy VPN.



Introducing Cisco Easy VPN

- **Cisco Easy VPN has two main functions:**
  - **Simplify client configuration**
  - **Centralize client configuration and dynamically push the configuration to clients**
- **How are these two goals achieved?**
  - **IKE Mode Config functionality is used to download some configuration parameters to clients.**
  - **Clients are preconfigured with a set of IKE policies and IPsec transform sets.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-3

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN Server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 Concentrator, a Cisco PIX Firewall, or a Cisco IOS router that supports the Cisco Unity Client protocol.

After the Cisco Easy VPN Server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN Remote client, such as a Cisco 800 Series router or a Cisco 1700 Series router. When the Easy VPN Remote initiates the VPN tunnel connection, the Cisco Easy VPN Server pushes the IPsec policies to the Easy VPN Remote client and creates the corresponding VPN tunnel connection.

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

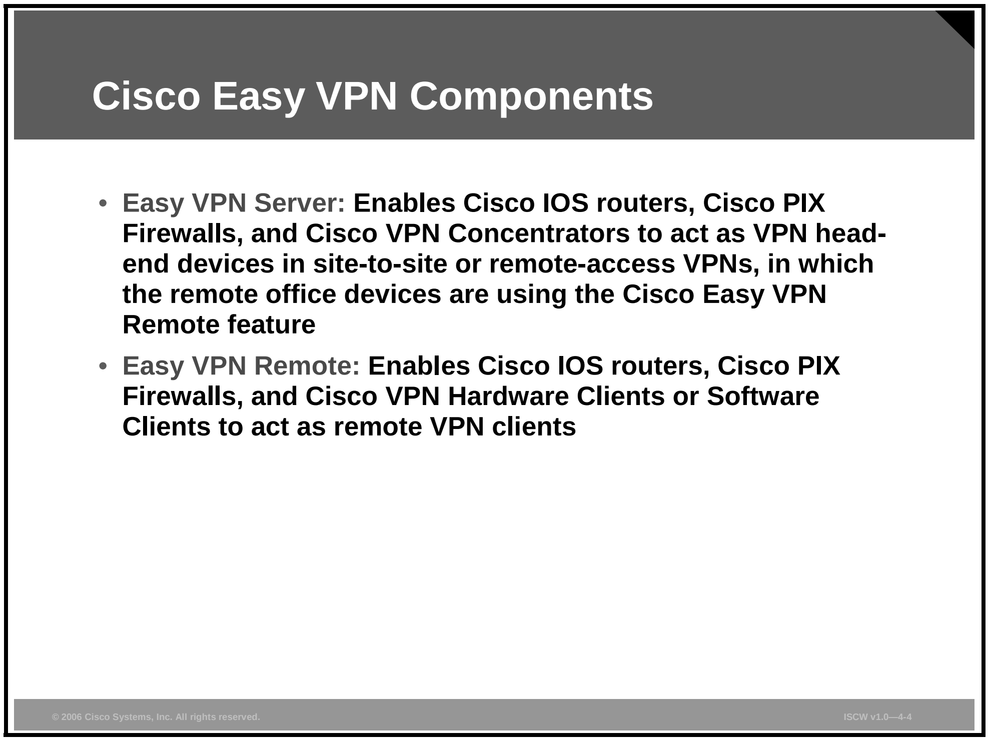
The Cisco Easy VPN Remote feature provides for automatic management of these details:

- Negotiating tunnel parameters, such as addresses, algorithms, and lifetime
- Establishing tunnels according to the parameters that were set
- Automatically creating the Network Address Translation (NAT) or Port Address Translation (PAT) and associated access control lists (ACLs) that are needed, if any
- Authenticating users—that is, ensuring that users are who they say they are—by usernames, group names, and passwords
- Managing security keys for encryption and decryption
- Authenticating, encrypting, and decrypting data through the tunnel

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

Cisco Easy VPN Components

Cisco Easy VPN consists of two components: Cisco Easy VPN Server and Cisco Easy VPN Remote.



Cisco Easy VPN Components

- Easy VPN Server: **Enables Cisco IOS routers, Cisco PIX Firewalls, and Cisco VPN Concentrators to act as VPN head-end devices in site-to-site or remote-access VPNs, in which the remote office devices are using the Cisco Easy VPN Remote feature**
- Easy VPN Remote: **Enables Cisco IOS routers, Cisco PIX Firewalls, and Cisco VPN Hardware Clients or Software Clients to act as remote VPN clients**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-4

Cisco Easy VPN Server

Cisco Easy VPN Server enables Cisco IOS routers, Cisco PIX Firewalls, and Cisco VPN 3000 Series Concentrators to act as VPN headend devices in site-to-site or remote-access VPNs, in which the remote office devices use the Easy VPN Remote feature. Using this feature, security policies defined at the headend are pushed to the remote VPN device, ensuring that those connections have up-to-date policies in place before the connection is established.

In addition, an Easy VPN Server-enabled device can terminate IPsec tunnels initiated by mobile remote workers running VPN Client software on PCs. This flexibility makes it possible for mobile and remote workers, such as salespeople on the road or telecommuters, to access their headquarters intranet, where critical data and applications exist.

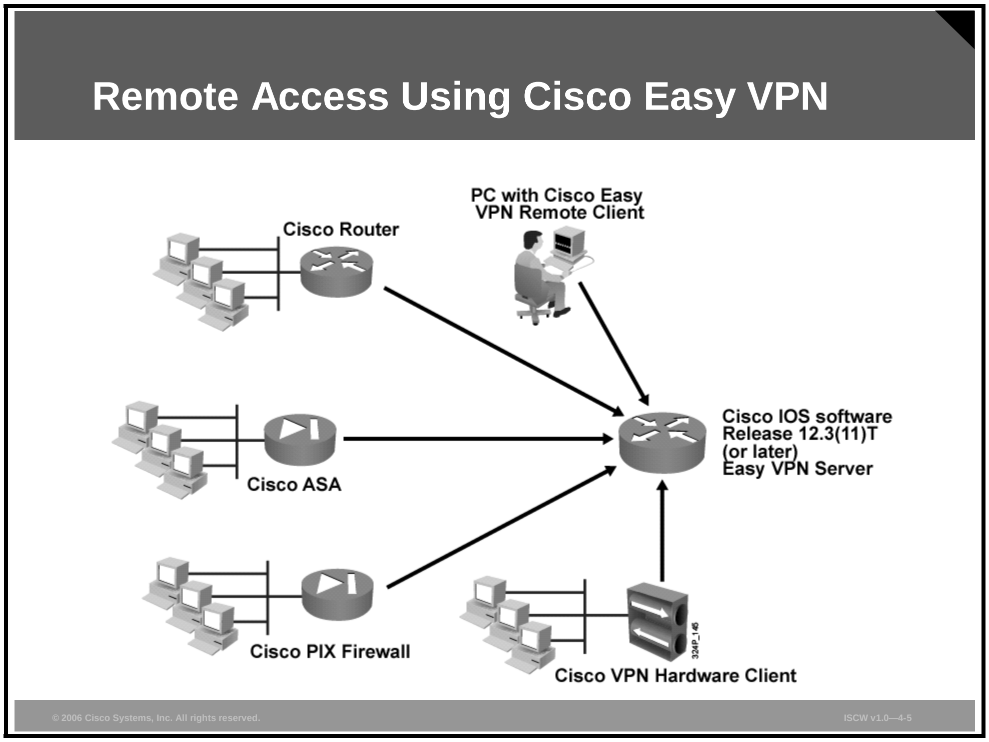
Cisco Easy VPN Remote

Cisco Easy VPN Remote enables Cisco IOS routers, Cisco PIX Firewalls, and Cisco VPN 3002 Hardware Clients or Software Clients to act as remote VPN clients. These devices can receive security policies from an Easy VPN Server, minimizing VPN configuration requirements at the remote location. This cost-effective solution is ideal for remote offices with little information technology (IT) support or for large customer premises equipment (CPE) deployments where it is impractical to individually configure multiple remote devices. This feature makes VPN configuration as easy as entering a password, which increases productivity and lowers costs because the need for local IT support is minimized.

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

Remote Access Using Cisco Easy VPN

In the example in the figure, the VPN gateway is a Cisco IOS router running the Easy VPN Server feature. Remote Cisco IOS routers and VPN Software Clients connect to the Cisco IOS router Easy VPN Server for access to the corporate intranet.



Remote Access Using Cisco Easy VPN

PC with Cisco Easy VPN Remote Client
Cisco Router
Cisco IOS software Release 12.3(11)T (or later) Easy VPN Server
Cisco ASA
Cisco PIX Firewall
Cisco VPN Hardware Client
324P_145

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-5

Restrictions for Cisco Easy VPN Remote

Required Easy VPN Servers

The Cisco Easy VPN Remote feature requires that the destination peer be a Cisco IOS Easy VPN Server or VPN concentrator that supports the Cisco Easy VPN Server feature. At the time of publication, this includes the following platforms when running the indicated software releases:

- **Cisco 831, Cisco 836, Cisco 837, Cisco 851, Cisco 857, Cisco 871, Cisco 876, Cisco 877, and Cisco 878 routers:** Cisco IOS Software Release 12.2(8)T or later release. Cisco 800 Series routers are not supported in Cisco IOS Software Release 12.3(7)XR, but they are supported in Cisco IOS Software Release 12.3(7)XR2.
- **Cisco 1700 Series:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 2600 Series:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 3620:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 3640:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 3660:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 7100 Series VPN routers:** Cisco IOS Software Release 12.2(8)T or later release.

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

- **Cisco 7200 Series routers:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 7500 Series routers:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco PIX 500 Series:** Cisco IOS Software Release 6.2 or later release.
- **Cisco VPN 3000 Series:** Cisco IOS Software Release 3.11 or later release.

Only ISAKMP Policy Group 2 Supported on Easy VPN Servers

The Cisco Unity Client protocol supports only Internet Security Association and Key Management Protocol (ISAKMP) policies that use Diffie-Hellman group 2 (1024-bit Diffie-Hellman) Internet Key Exchange (IKE) negotiation, so the Cisco Easy VPN Server being used with the Cisco Easy VPN Remote feature must be configured for a group 2 ISAKMP policy. The Easy VPN Server cannot be configured for ISAKMP group 1 or group 5 when being used with a Cisco Easy VPN client.

Transform Sets Supported

To ensure a secure tunnel connection, the Cisco Easy VPN Remote feature does not support transform sets that provide encryption without authentication (esp-des and esp-3des) or transform sets that provide authentication without encryption (esp-null esp-sha-hmac and esp-null esp-md5-hmac).

Note The Cisco Unity Client protocol does not support Authentication Header (AH) authentication, but it does support Encapsulating Security Payload (ESP).

Dial Backup for Easy VPN Remotes

Line status-based backup is not supported in this feature.

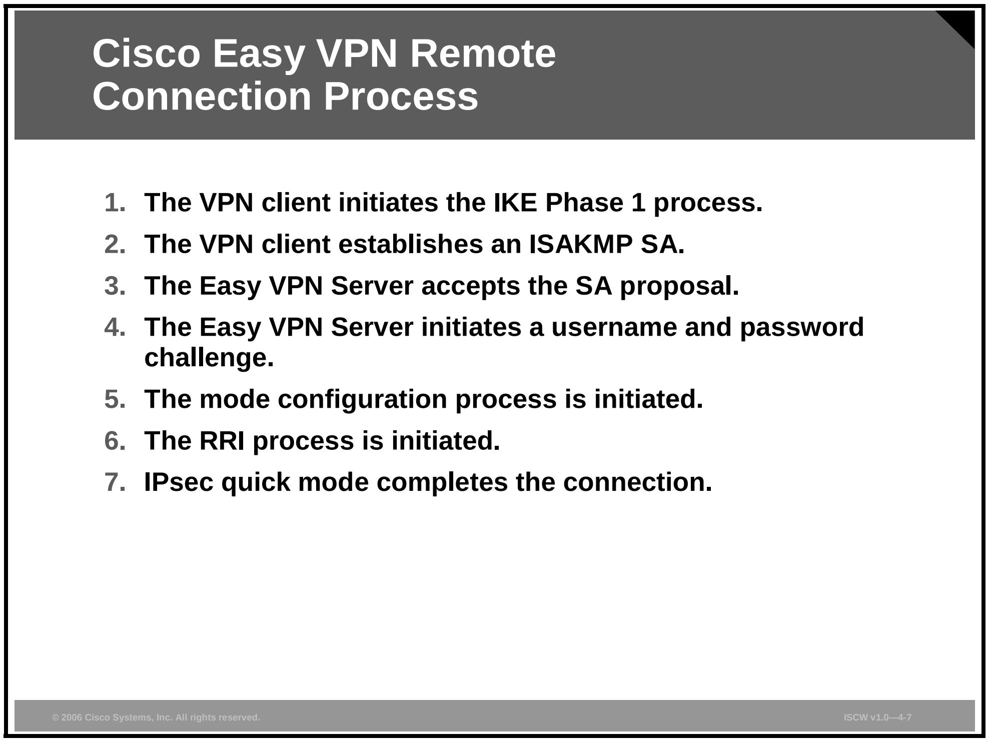
NAT Interoperability Support

NAT interoperability is not supported in client mode with split tunneling.

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

Describe Easy VPN Server and Easy VPN Remote

This topic describes IKE phases, including additional steps between Phases 1 and 2 in which Xauth is used for additional user authentication and mode configuration is used to dynamically configure clients with various parameters.



Cisco Easy VPN Remote Connection Process

1. The VPN client initiates the IKE Phase 1 process.
2. The VPN client establishes an ISAKMP SA.
3. The Easy VPN Server accepts the SA proposal.
4. The Easy VPN Server initiates a username and password challenge.
5. The mode configuration process is initiated.
6. The RRI process is initiated.
7. IPsec quick mode completes the connection.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-7

When an Easy VPN Remote client initiates a connection with an Easy VPN Server gateway, the “conversation” that occurs between peers generally consists of these steps:

Step 1 The VPN Client initiates the IKE Phase 1 process.

Step 2 The VPN Client establishes an ISAKMP security association (SA).

Step 3 The Easy VPN Server accepts the SA proposal.

Step 4 The Easy VPN Server initiates a username and password challenge.

Step 5 The mode configuration process is initiated.

Step 6 The Reverse Route Injection (RRI) process is initiated.

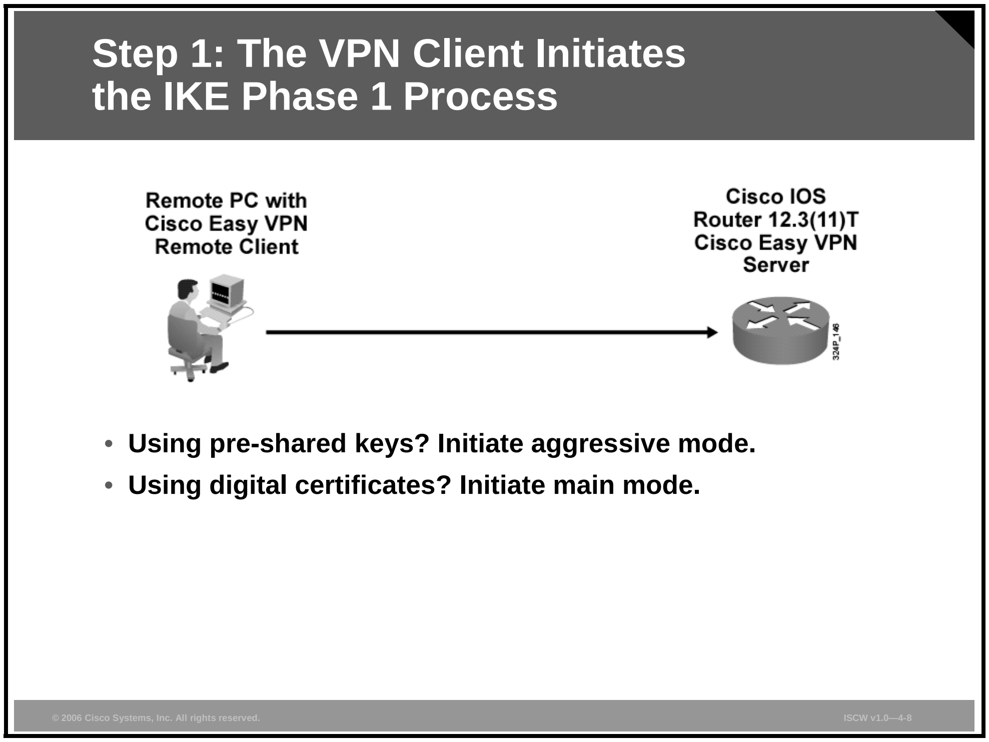
Step 7 IPsec quick mode completes the connection.

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

Step 1: The VPN Client Initiates the IKE Phase 1 Process

There are two ways to perform authentication, and the VPN Client must consider the following when initiating IKE Phase 1:

- If a preshared key is to be used for authentication, the VPN Client initiates aggressive mode. When preshared keys are used, the accompanying group name entered in the configuration GUI (ID_KEY_ID) is used to identify the group profile associated with this VPN Client.
- If digital certificates are to be used for authentication, the VPN Client initiates main mode. When digital certificates are used, the organizational unit field of a distinguished name is used to identify the group profile.



Step 1: The VPN Client Initiates the IKE Phase 1 Process

Remote PC with Cisco Easy VPN Remote Client
Cisco IOS Router 12.3(11)T Cisco Easy VPN Server
324P_146

- **Using pre-shared keys? Initiate aggressive mode.**
- **Using digital certificates? Initiate main mode.**

© 2006 Cisco Systems, Inc. All rights reserved.

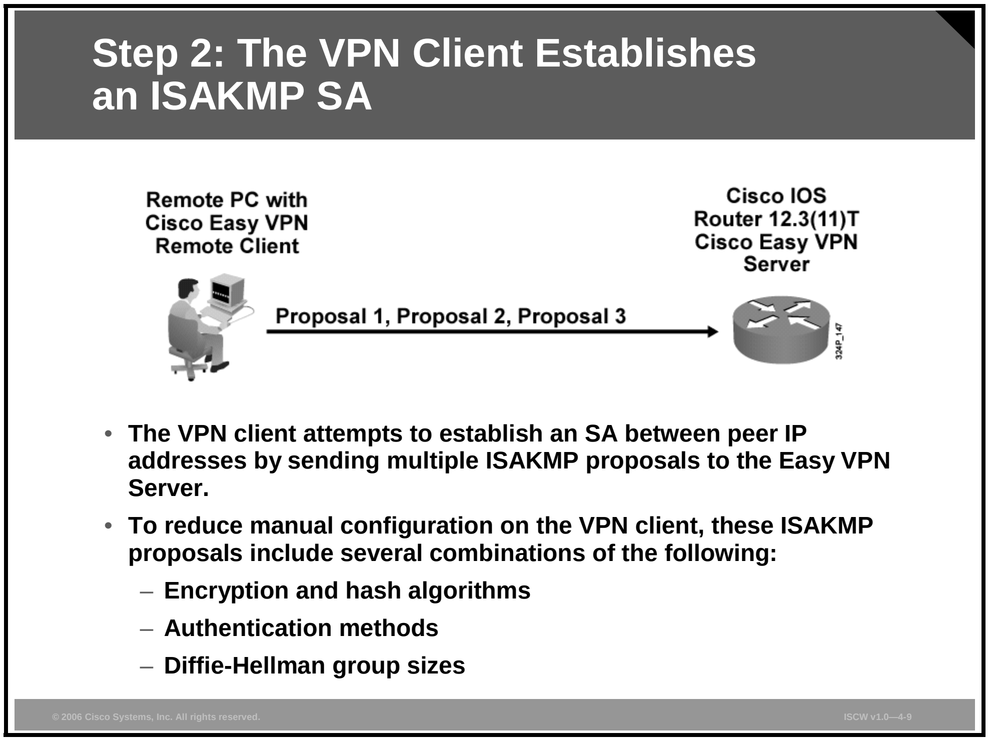
ISCW v1.0—4-8

Because the VPN Client may be configured for preshared key authentication, which initiates IKE aggressive mode, you should change the identity of the Cisco IOS VPN device via the **crypto isakmp identity hostname** command. This action does not affect certificate authentication via IKE main 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 self-study.

Step 2: The VPN Client Establishes an ISAKMP SA

This section describes how the VPN Client establishes an ISAKMP SA.



Step 2: The VPN Client Establishes an ISAKMP SA

Remote PC with Cisco Easy VPN Remote Client
Cisco IOS Router 12.3(11)T Cisco Easy VPN Server
Proposal 1, Proposal 2, Proposal 3
324P_147

- The VPN client attempts to establish an SA between peer IP addresses by sending multiple ISAKMP proposals to the Easy VPN Server.
- To reduce manual configuration on the VPN client, these ISAKMP proposals include several combinations of the following:
  - Encryption and hash algorithms
  - Authentication methods
  - Diffie-Hellman group sizes

© 2006 Cisco Systems, Inc. All rights reserved.

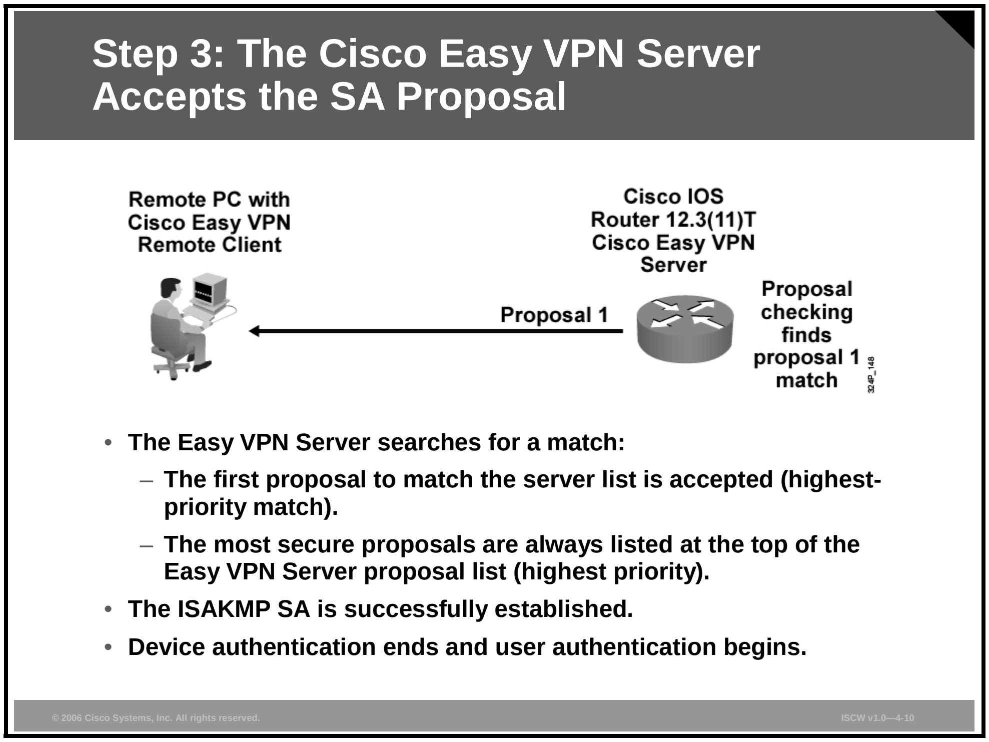
ISCW v1.0—4-9

To reduce the amount of manual configuration on the VPN Client, ISAKMP proposals include every combination of encryption and hash algorithms, authentication methods, and Diffie-Hellman group sizes.

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

Step 3: The Cisco Easy VPN Server Accepts the SA Proposal

This section describes how the Cisco Easy VPN Server accepts the SA proposal.



Step 3: The Cisco Easy VPN Server Accepts the SA Proposal

Remote PC with Cisco Easy VPN Remote Client
Cisco IOS Router 12.3(11)T Cisco Easy VPN Server
Proposal 1
Proposal checking finds proposal 1 match
324P_148

- **The Easy VPN Server searches for a match:**
  - **The first proposal to match the server list is accepted (highest-priority match).**
  - **The most secure proposals are always listed at the top of the Easy VPN Server proposal list (highest priority).**
- **The ISAKMP SA is successfully established.**
- **Device authentication ends and user authentication begins.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-10

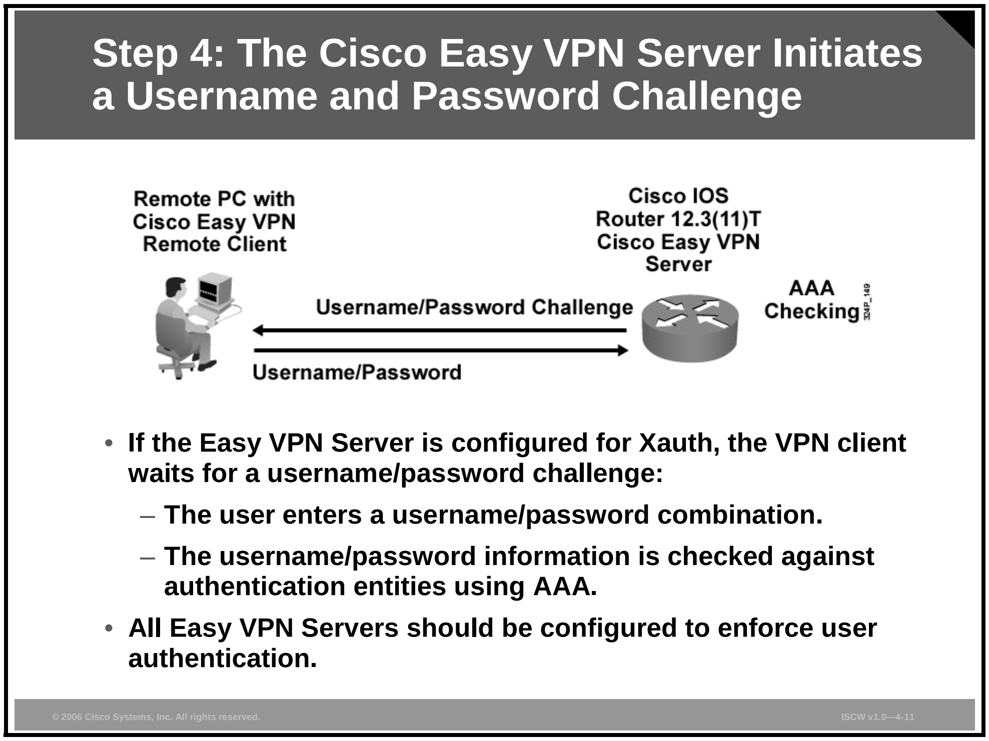
ISAKMP policy is global for the Easy VPN Server and can consist of several proposals. In the case of multiple proposals, the Easy VPN Server will use the first match, so you should always have your most secure policies listed first.

Device authentication ends and user authentication begins at this point.

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

Step 4: The Cisco Easy VPN Server Initiates a Username and Password Challenge

This section describes how the Easy VPN Server initiates a username and password challenge.



Step 4: The Cisco Easy VPN Server Initiates a Username and Password Challenge

Remote PC with Cisco Easy VPN Remote Client
Cisco IOS Router 12.3(11)T Cisco Easy VPN Server
Username/Password Challenge
Username/Password
AAA Checking
324P_149

- **If the Easy VPN Server is configured for Xauth, the VPN client waits for a username/password challenge:**
  - **The user enters a username/password combination.**
  - **The username/password information is checked against authentication entities using AAA.**
- **All Easy VPN Servers should be configured to enforce user authentication.**

© 2006 Cisco Systems, Inc. All rights reserved.

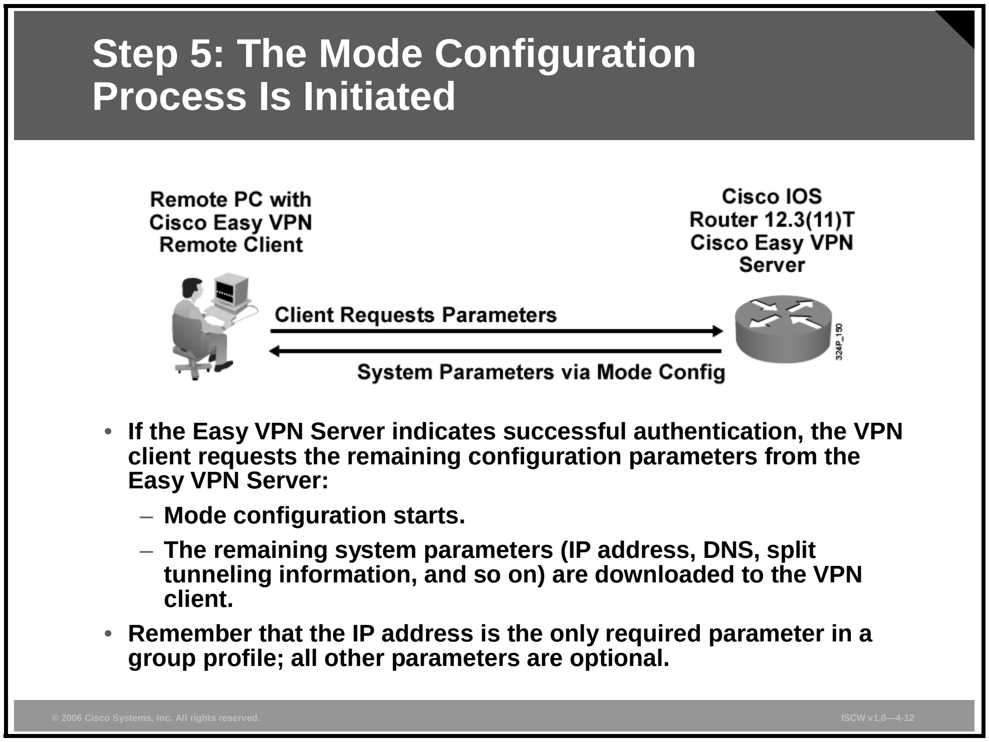
The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy.

VPN devices that are configured to handle remote VPN clients should always be configured to enforce user 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 self-study.

Step 5: The Mode Configuration Process Is Initiated

This section describes how the mode configuration process is initiated.



Step 5: The Mode Configuration Process Is Initiated

Remote PC with Cisco Easy VPN Remote Client

Cisco IOS Router 12.3(11)T Cisco Easy VPN Server

Client Requests Parameters

System Parameters via Mode Config

324P_150

- If the Easy VPN Server indicates successful authentication, the VPN client requests the remaining configuration parameters from the Easy VPN Server:
  - Mode configuration starts.
  - The remaining system parameters (IP address, DNS, split tunneling information, and so on) are downloaded to the VPN client.
- Remember that the IP address is the only required parameter in a group profile; all other parameters are optional.

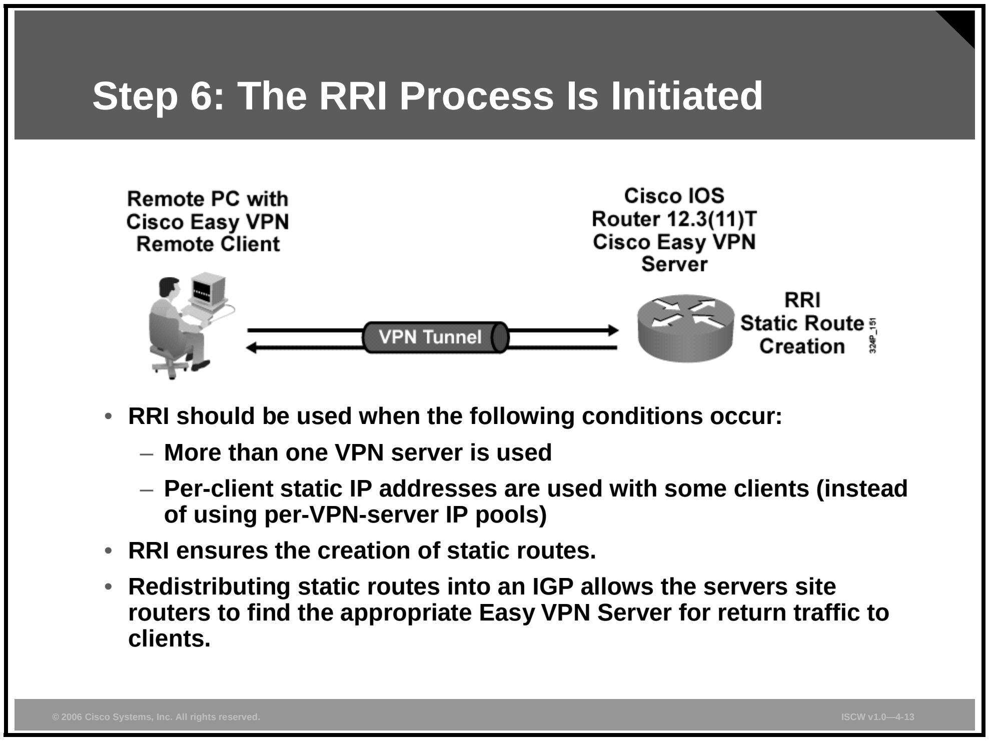
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-12

The remaining system parameters (IP address, Domain Name System [DNS], split tunnel attributes, and so on) are pushed to the VPN client at this time using mode configuration. The IP address is the only required parameter in a group profile; all other parameters are optional.

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

Step 6: The RRI Process Is Initiated

This section describes how the Reverse Route Injection (RRI) process is initiated.



Step 6: The RRI Process Is Initiated

Remote PC with Cisco Easy VPN Remote Client
Cisco IOS Router 12.3(11)T Cisco Easy VPN Server
VPN Tunnel
RRI Static Route Creation
324P_151

- RRI should be used when the following conditions occur:
  - More than one VPN server is used
  - Per-client static IP addresses are used with some clients (instead of using per-VPN-server IP pools)
- RRI ensures the creation of static routes.
- Redistributing static routes into an IGP allows the servers site routers to find the appropriate Easy VPN Server for return traffic to clients.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-13

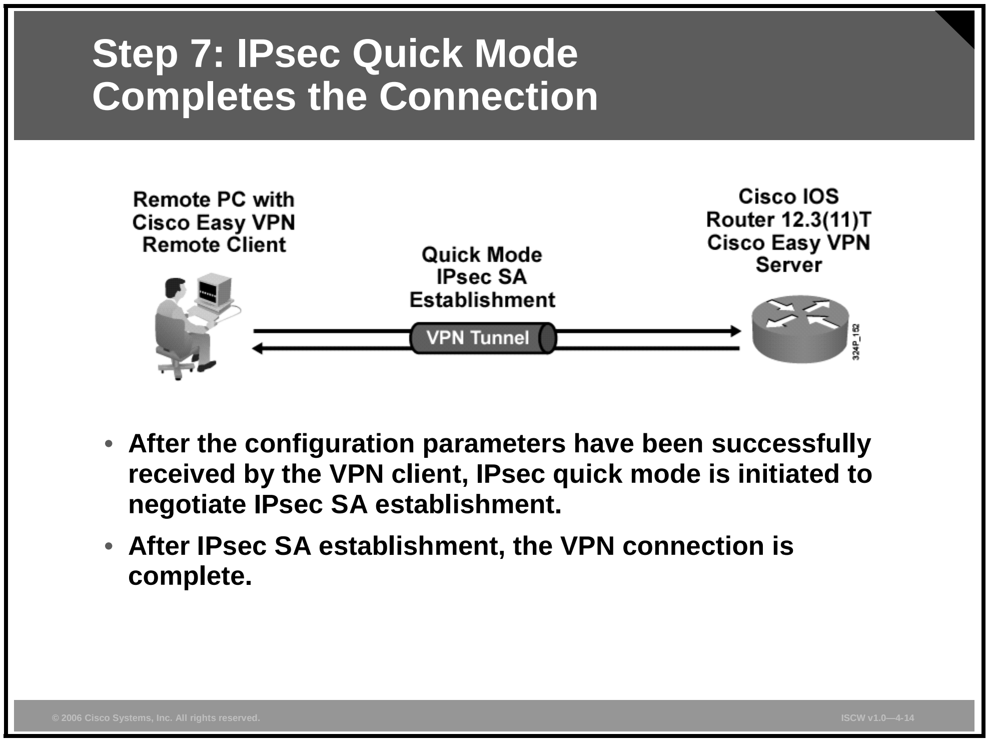
RRI ensures that a static route is created on the Cisco Easy VPN Server for the internal IP address of each VPN client.

Note	It is recommended that you enable RRI on the dynamic crypto map when per-user IP addresses are used and when more than one Easy VPN Server is used. Redistributing RRI routes into an Interior Gateway Protocol (IGP) allows the server site to properly find the return path to the clients.

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

Step 7: IPsec Quick Mode Completes the Connection

This section describes how the IPsec quick mode completes the connection.



Step 7: IPsec Quick Mode Completes the Connection

Remote PC with Cisco Easy VPN Remote Client

Quick Mode IPsec SA Establishment

VPN Tunnel

Cisco IOS Router 12.3(11)T Cisco Easy VPN Server

324P_152

- After the configuration parameters have been successfully received by the VPN client, IPsec quick mode is initiated to negotiate IPsec SA establishment.
- After IPsec SA establishment, the VPN connection is complete.

© 2006 Cisco Systems, Inc. All rights reserved.

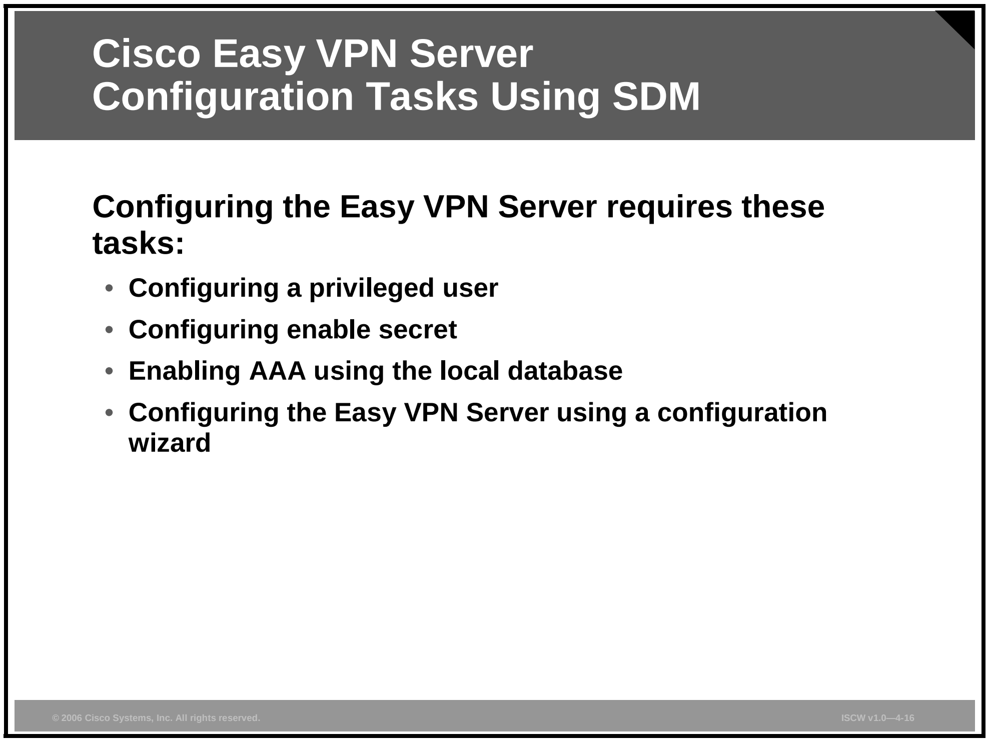
ISCW v1.0—4-14

After IPsec SAs have been created, the connection is complete.

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

Cisco Easy VPN Server Configuration Tasks

This topic describes the steps required to configure Cisco Easy VPN Server using SDM.



Cisco Easy VPN Server Configuration Tasks Using SDM

Configuring the Easy VPN Server requires these tasks:

- **Configuring a privileged user**
- **Configuring enable secret**
- **Enabling AAA using the local database**
- **Configuring the Easy VPN Server using a configuration wizard**

© 2006 Cisco Systems, Inc. All rights reserved.

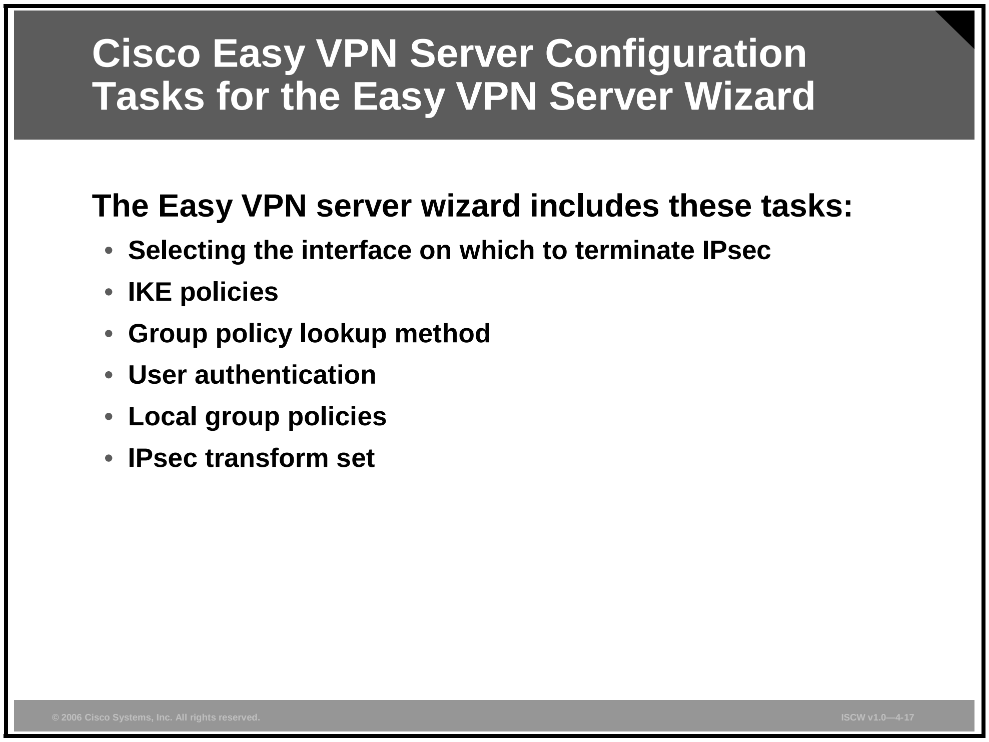
Configuring Easy VPN Server functionality using the SDM consists of two parts:

- Configuring prerequisites, such as AAA, privileged users, and enable secret
- Configuring the Easy VPN Server using the provided 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 self-study.

Cisco Easy VPN Server Configuration Tasks for the Easy VPN Server Wizard

This section describes how the Easy VPN Server wizard guides you through the configuration steps.



Cisco Easy VPN Server Configuration Tasks for the Easy VPN Server Wizard

The Easy VPN server wizard includes these tasks:

- **Selecting the interface on which to terminate IPsec**
- **IKE policies**
- **Group policy lookup method**
- **User authentication**
- **Local group policies**
- **IPsec transform set**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-17

The Easy VPN Server wizard guides you through a set of steps which includes the configuration of these parameters:

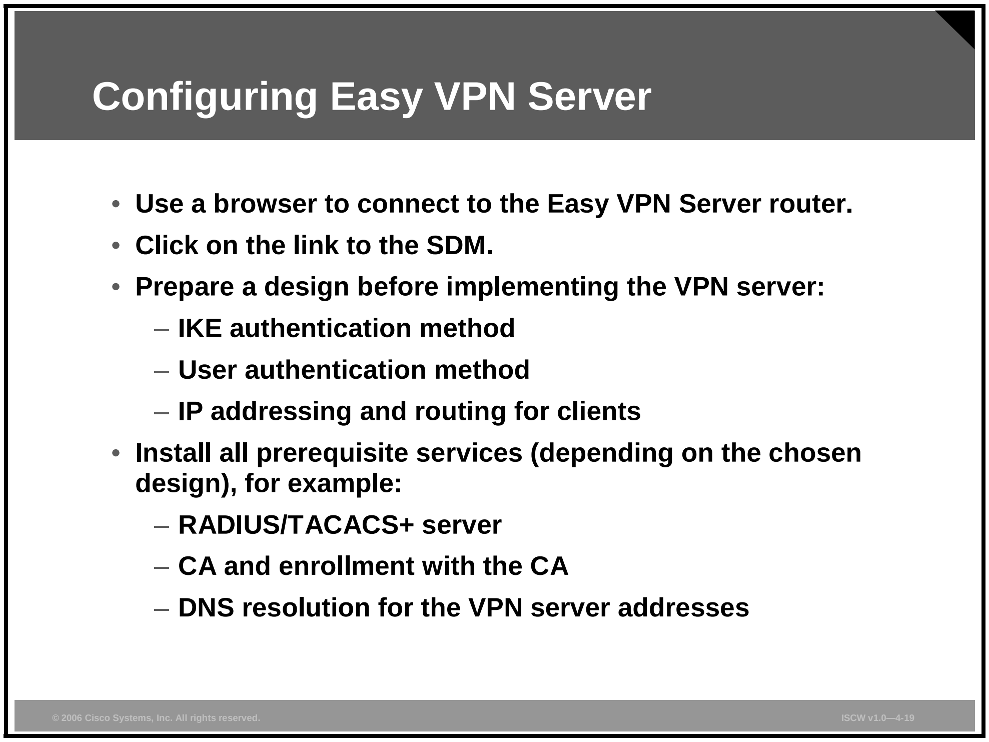
- Selecting the interface on which to terminate IPsec tunnels
- IKE policies (for example, encryption algorithm, Hash-based Message Authentication Code (HMAC), priority, lifetime, and Diffie-Hellman group)
- Group policy lookup method (local, RADIUS, or TACACS+)
- User authentication (local or RADIUS)
- Local group policies (such as name, preshared secret, DNS servers, and split tunneling)

IPsec transform set (for example, encryption algorithm, HMAC, and mode of operation)

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

Configuring Easy VPN Server

This topic describes each of the steps required to configure Cisco Easy VPN Server.



Configuring Easy VPN Server

- **Use a browser to connect to the Easy VPN Server router.**
- **Click on the link to the SDM.**
- **Prepare a design before implementing the VPN server:**
  - **IKE authentication method**
  - **User authentication method**
  - **IP addressing and routing for clients**
- **Install all prerequisite services (depending on the chosen design), for example:**
  - **RADIUS/TACACS+ server**
  - **CA and enrollment with the CA**
  - **DNS resolution for the VPN server addresses**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-19

Use a browser to connect to the Easy VPN Server router, where you can follow the link to the SDM.

Before starting with the configuration, you should prepare a VPN design and prepare these parameters required for the configuration:

- IKE authentication method
- User authentication method
- IP addressing and routing for clients

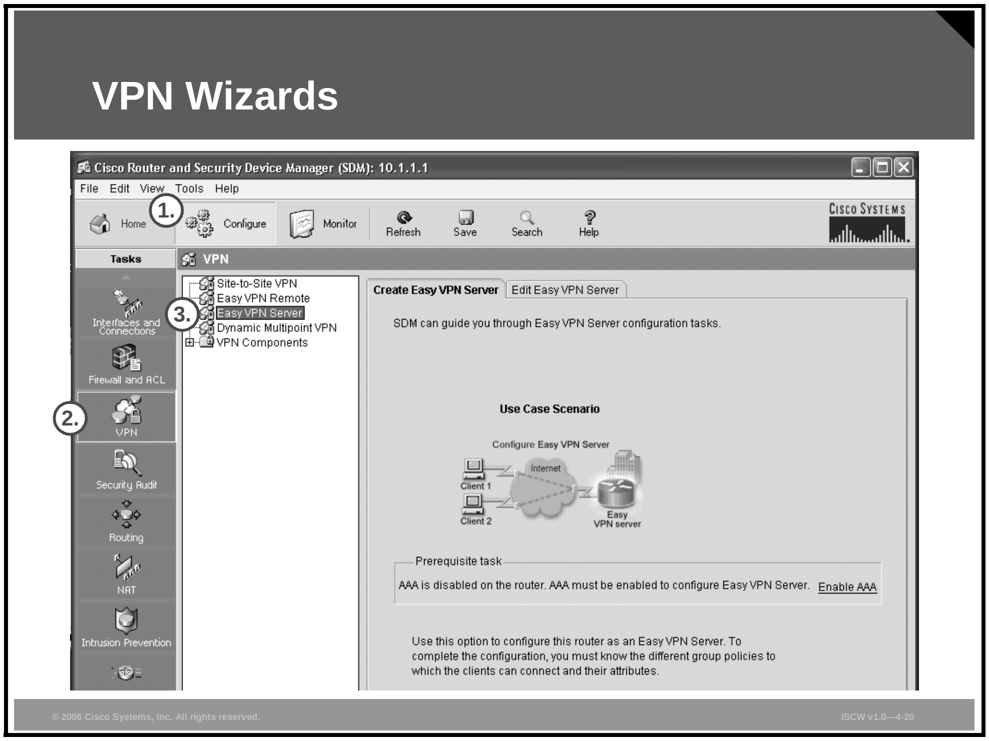
You should also install these prerequisite services, depending on the chosen design:

- RADIUS or TACACS+ server installation and configuration.
- CA installation and configuration if the public key infrastructure (PKI) is used for authentication. The router should also be enrolled with the CA to get the CA certificate and the identity certificate of the router that can later be used to enable PKI for the VPN.
- DNS resolution for the addresses of the VPN servers.
- Network Time Protocol (NTP) for the PKI to operate properly.

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

VPN Wizards

The VPN configuration page lists VPN wizards that help implement different type of IPsec-based VPNs. Select the Easy VPN Server page.



VPN Wizards

SDM can guide you through Easy VPN Server configuration tasks.

AAA is disabled on the router. AAA must be enabled to configure Easy VPN Server.

Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-20

Navigate to the Easy VPN Server page by following this procedure:

Step 1 Click the **Configure** icon in the toolbar at the top of the window.

Step 2 Click the **VPN** icon in the Tasks toolbar on the left side of the window.

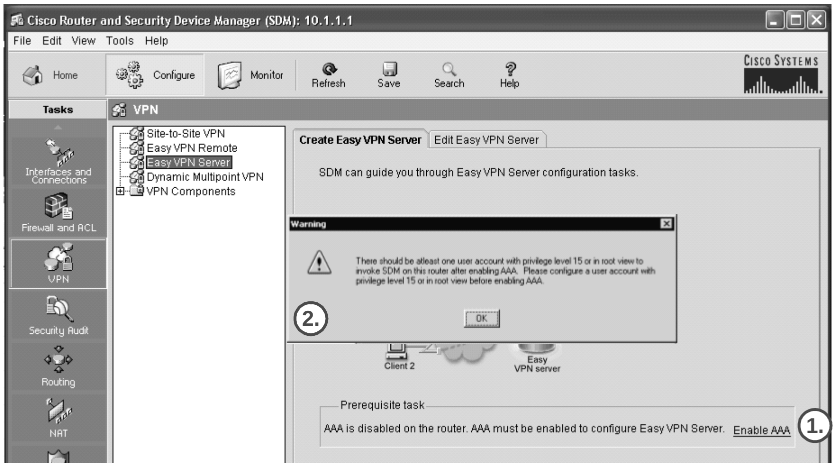
Step 3 Choose the **Easy VPN Server** option in the middle part of the window.

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

Enabling AAA

If you have not configured AAA, the wizard will ask you to configure it.

Enabling AAA



SDM can guide you through Easy VPN Server configuration tasks.

There should be atleast one user account with privilege level 15 or in root view to invoke SDM on this router after enabling AAA. Please configure a user account with privilege level 15 or in root view before enabling AAA.

AAA is disabled on the router. AAA must be enabled to configure Easy VPN Server.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-21

If AAA is disabled on the router, you have to configure it before Easy VPN Server configuration begins. To do so, follow this procedure:

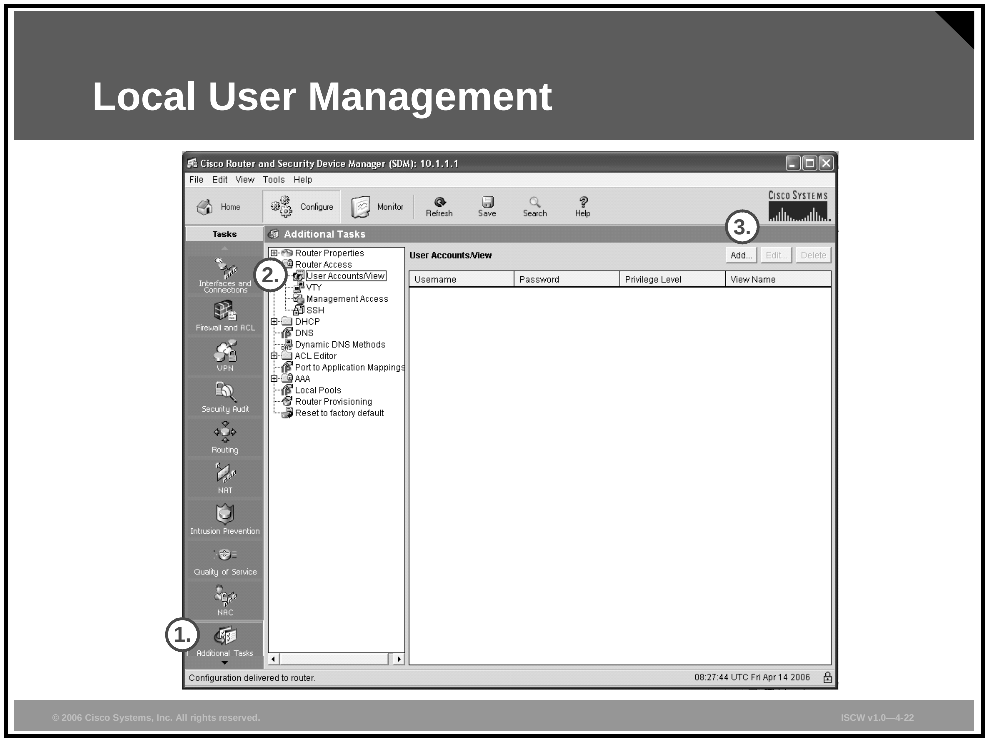
Step 1 Click the **Enable AAA** link at the bottom of the Create Easy VPN Server tab.

Step 2 A warning window opens, warning you to configure a user account with privilege level 15 before enabling AAA. Click **OK** to the warning window.

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

Local User Management

The figure illustrates the location where you must create an administrative user.



Local User Management

To create an administrative user, follow this procedure:

Step 1 Click the **Additional Tasks** icon in the Tasks toolbar on the left side of the window.

Step 2 Click the **User Accounts/View** option under the **Router Access** option in the middle part of the window.

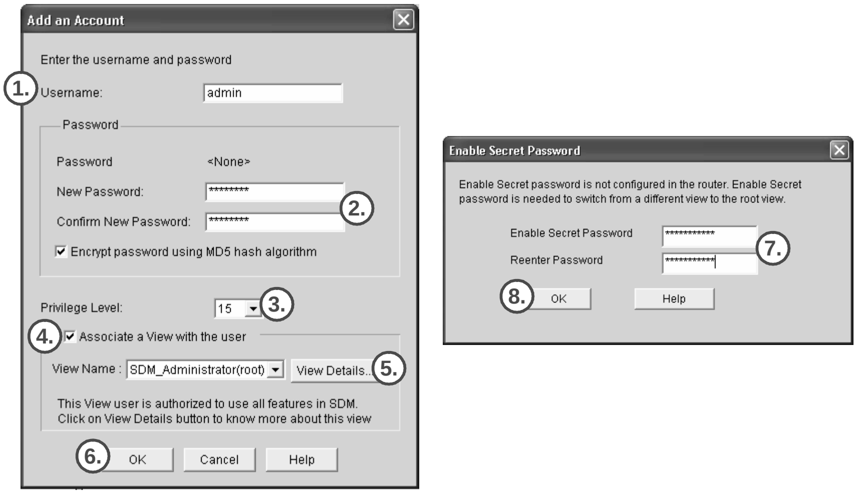
Step 3 Click **Add** in the top right side of the window to add a user.

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 self-study.

Creating Users

An **Add an Account** window opens.

Creating Users



Add an Account

Enter the username and password

Username: admin

Password

Password <None>

New Password: *********

Confirm New Password: *********

☑ Encrypt password using MD5 hash algorithm

Privilege Level: 15

☑ Associate a View with the user

View Name : SDM_Administrator(root)

This View user is authorized to use all features in SDM.
Click on View Details button to know more about this view

Enable Secret Password

Enable Secret password is not configured in the router. Enable Secret password is needed to switch from a different view to the root view.

Enable Secret Password ************

Reenter Password ************

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-23

To add parameters for the new user, follow this procedure:

Step 1 Give the administrative user a username.

Step 2 Select a good password.

Step 3 Make sure that the user has privilege level 15.

Step 4 You should assign this user to have the SDM administrative role by selecting the **SDM_Administrator (root)** option in the View Name drop-down menu.

Step 5 Click **View Details** to review the details of the currently chosen role. When done, click **OK**.

Step 6 Click **OK**.

Step 7 If the enable secret password is not configured on your router, you will be asked to enter the enable secret password.

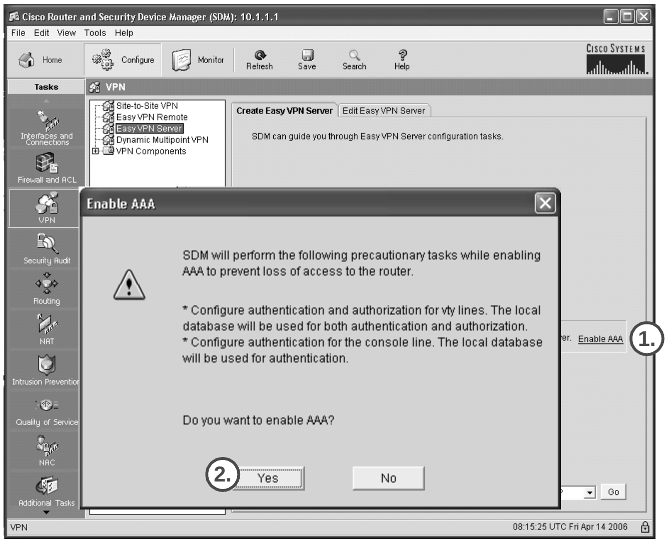
Step 8 Click **OK**.

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

Enabling AAA

This section describes how to enable AAA.

Enabling AAA



SDM can guide you through Easy VPN Server configuration tasks.

Enable AAA

SDM will perform the following precautionary tasks while enabling AAA to prevent loss of access to the router.

* Configure authentication and authorization for vty lines. The local database will be used for both authentication and authorization.
* Configure authentication for the console line. The local database will be used for authentication.

Do you want to enable AAA?

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-24

Finally, you can return to the Easy VPN Server wizard and enable AAA services:

Step 1 Click the **Enable AAA** link on the Create Easy VPN Server tab to enable AAA services.

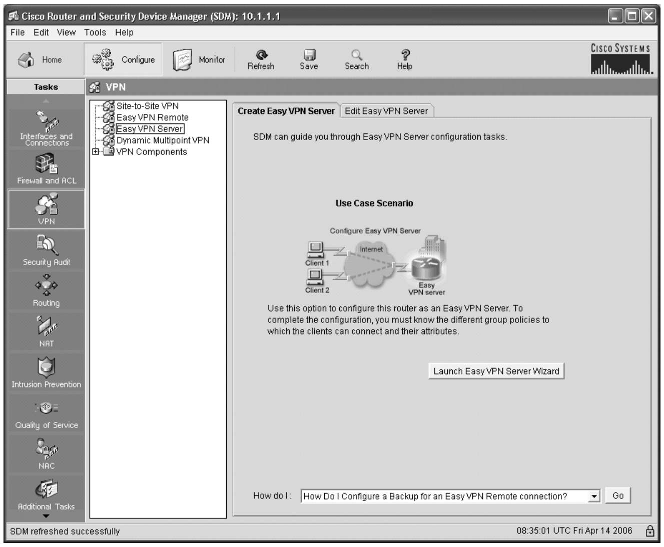
Step 2 An Enable AAA window opens. Click **Yes** to enable AAA.

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

Starting the Easy VPN Server Wizard

This section describes how to start Easy VPN Server wizard.

Starting the Easy VPN Server Wizard



Cisco Router and Security Device Manager (SDM): 10.1.1.1

SDM can guide you through Easy VPN Server configuration tasks.

Use Case Scenario

Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes.

How do I : How Do I Configure a Backup for an Easy VPN Remote connection?

SDM refreshed successfully

08:35:01 UTC Fri Apr 14 2006

© 2006 Cisco Systems, Inc. All rights reserved.

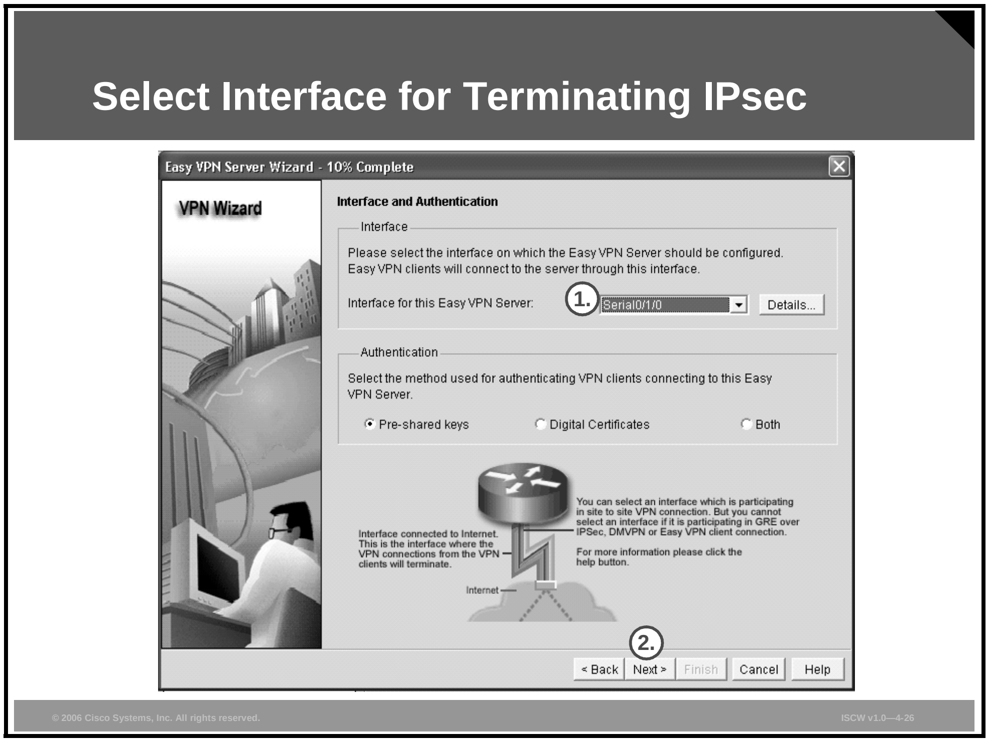
ISCW v1.0—4-25

Once the AAA services are enabled, click **Launch Easy VPN Server Wizard** on the Create Easy VPN Server tab to start the Easy VPN Server 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 self-study.

Select Interface for Terminating IPsec

This section describes how to select the outside interface.



Select Interface for Terminating IPsec

Easy VPN Server Wizard - 10% Complete

VPN Wizard

Interface and Authentication

Interface

Please select the interface on which the Easy VPN Server should be configured. Easy VPN clients will connect to the server through this interface.

1. Interface for this Easy VPN Server: Serial0/1/0 [Details...]

Authentication

Select the method used for authenticating VPN clients connecting to this Easy VPN Server.

● Pre-shared keys ○ Digital Certificates ○ Both

Interface connected to Internet. This is the interface where the VPN connections from the VPN clients will terminate.

You can select an interface which is participating in site to site VPN connection. But you cannot select an interface if it is participating in GRE over IPSec, DMVPN or Easy VPN client connection.

For more information please click the help button.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-26

The Interface and Authentication window opens. Here you can select the outside interface toward the IPsec peer over the untrusted network:

Step 1 Select the interface in the **Interface for this Easy VPN Server** drop-down menu.

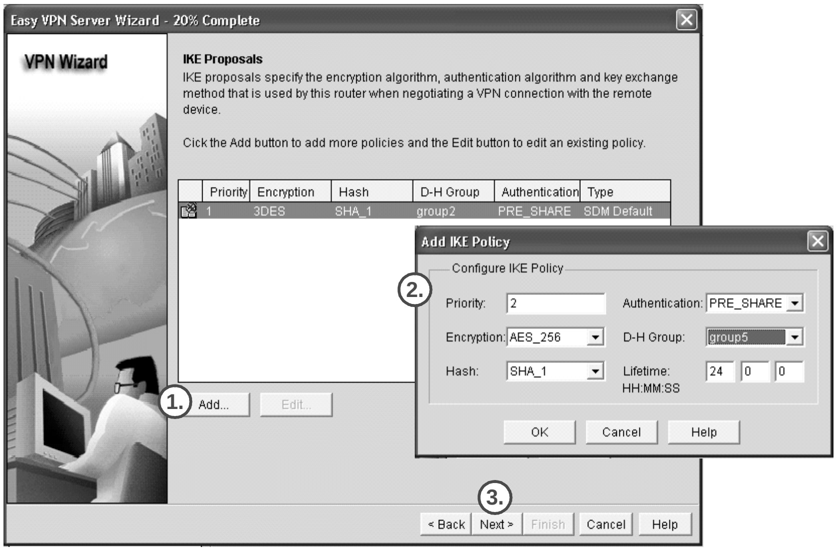
Step 2 Click **Next** to continue.

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

IKE Proposals

This topic describes the procedure to configure IKE using the SDM wizard.

IKE Proposals



Easy VPN Server Wizard - 20% Complete

VPN Wizard

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device.

Click the Add button to add more policies and the Edit button to edit an existing policy.

Priority	Encryption	Hash	D-H Group	Authentication	Type
1	3DES	SHA_1	group2	PRE_SHARE	SDM Default

Add IKE Policy

Configure IKE Policy

Priority: 2

Authentication: PRE_SHARE

Encryption: AES_256

D-H Group: group5

Hash: SHA_1

Lifetime: HH:MM:SS 24 0 0

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-28

When configuring IKE proposals, you can use the IKE proposal predefined by SDM or add a custom IKE proposal specifying these required parameters:

- IKE proposal priority
- Diffie-Hellman group (1, 2, or 5)
- Encryption algorithm (Data Encryption Standard [DES], Triple Data Encryption Standard [3DES], Advanced Encryption Standard [AES], or Software Encryption Algorithm [SEAL])
- HMAC (Secure Hash Algorithm 1 [SHA-1] or Message Digest 5 [MD5])
- IKE lifetime

After selecting the interface for terminating IPsec, configure the IKE proposals:

Step 1 In the IKE Proposals window, click **Add** to add an IKE proposal.

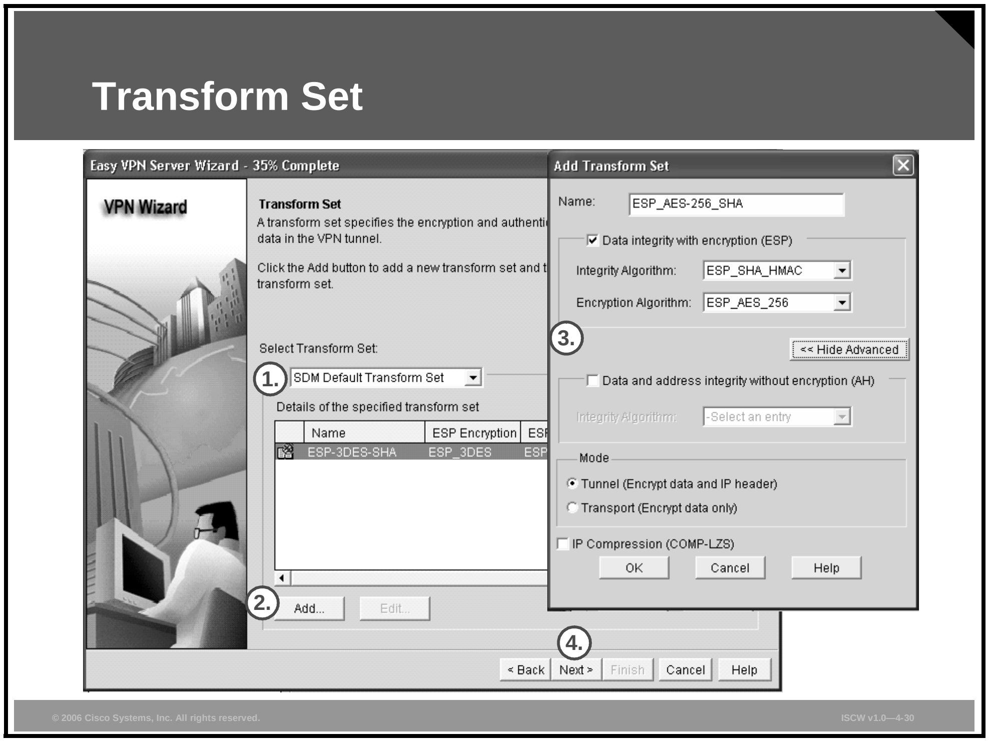
Step 2 An Add IKE Policy window opens. Enter IKE parameters and click **OK** when you are done.

Step 3 Click **Next** to continue.

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

Transform Set

This topic describes the procedure to configure the IPsec transform set using the SDM wizard.



Transform Set

Easy VPN Server Wizard - 35% Complete

Transform Set

A transform set specifies the encryption and authenti
data in the VPN tunnel.

Click the Add button to add a new transform set and t
transform set.

Select Transform Set: SDM Default Transform Set

Details of the specified transform set

Name	ESP Encryption	ESP
ESP-3DES-SHA	ESP_3DES	ESP

Add Transform Set

Name: ESP_AES-256_SHA

☑ Data integrity with encryption (ESP)

Integrity Algorithm: ESP_SHA_HMAC

Encryption Algorithm: ESP_AES_256

☐ Data and address integrity without encryption (AH)

Integrity Algorithm: -Select an entry

Mode

● Tunnel (Encrypt data and IP header)

○ Transport (Encrypt data only)

☐ IP Compression (COMP-LZS)

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-30

IPsec transform set configuration requires these parameters:

- Transform set name
- Encryption algorithm (DES, 3DES, AES, or SEAL)
- HMAC (SHA-1 or MD5)
- Optional compression
- Mode of operation (tunnel or transport)

The next step in configuring an Easy VPN Server is configuration of a transform set:

Step 1 In the Transform Set window, select a transform set in the **Select Transform Set** drop-down menu.

Step 2 Click **Add** to add an IPsec transform set.

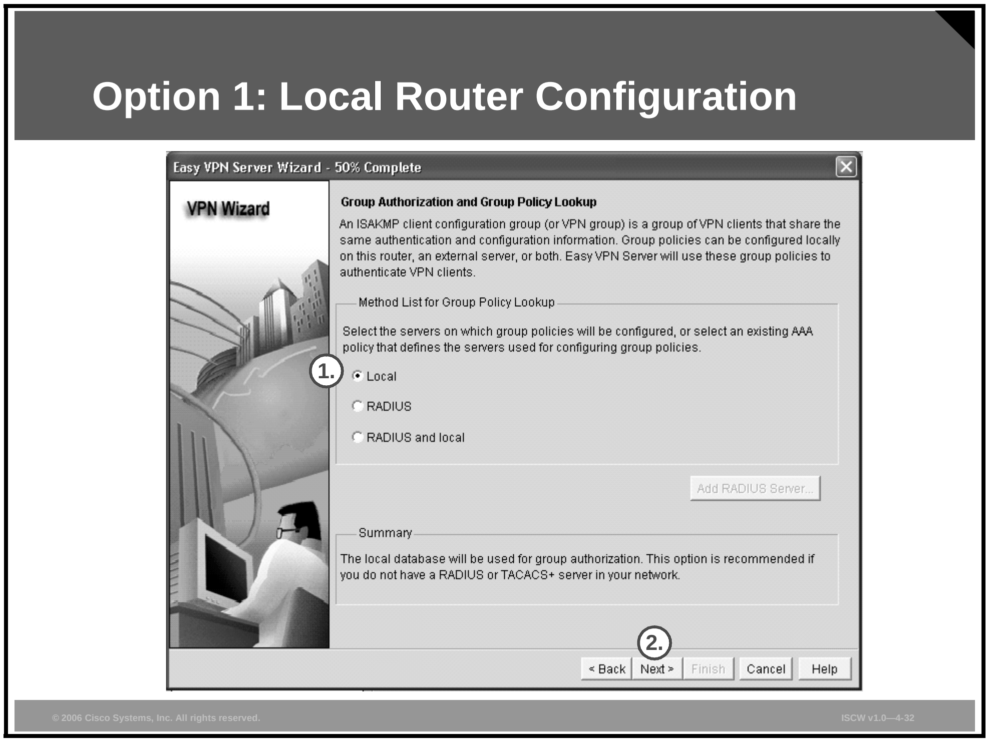
Step 3 An Add Transform Set window opens. Enter IPsec transform set parameters and click **OK**.

Step 4 Click **Next** to continue.

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

Group Policy Configuration Location

This topic describes the locations where you can store Easy VPN group policies.



Option 1: Local Router Configuration

Easy VPN Server Wizard - 50% Complete

Group Authorization and Group Policy Lookup

An ISAKMP client configuration group (or VPN group) is a group of VPN clients that share the same authentication and configuration information. Group policies can be configured locally on this router, an external server, or both. Easy VPN Server will use these group policies to authenticate VPN clients.

Method List for Group Policy Lookup

Select the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies.

1. ● Local

○ RADIUS

○ RADIUS and local

Summary

The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACS+ server in your network.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-32

The figure illustrates the page on which you select the location where Easy VPN group policies will be stored:

- *Local* means that all the groups will be in the router configuration in NVRAM.
- *RADIUS* means that the router will use RADIUS server for group authorization.
- *RADIUS and local* means that the router will also be able to look up policies stored in a AAA server database reachable via RADIUS.

Option 1: Local Router Configuration

The first option is to configure the group policies on the local server:

Step 1 In the Group Authorization and Group Policy Lookup window, click the **Local** radio button in the Method List for Group Policy Lookup section.

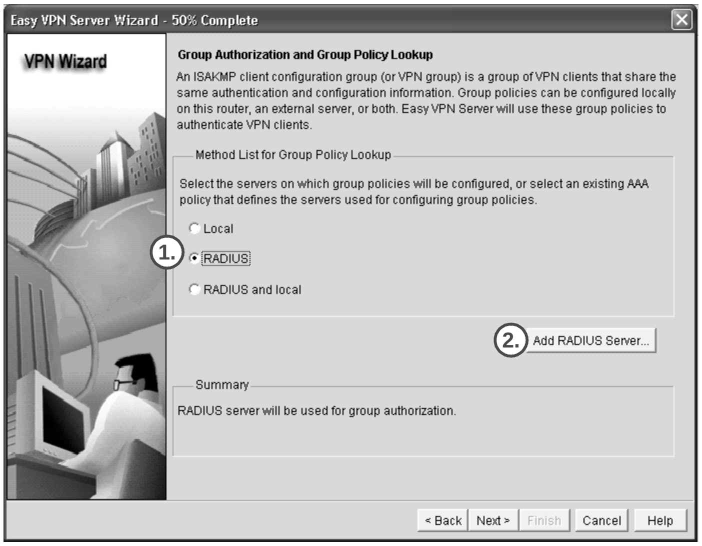
Step 2 Click **Next** to continue.

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

Option 2: External Location via RADIUS

This section describes the second option for group authorization.

Option 2: External Location via RADIUS



Easy VPN Server Wizard - 50% Complete

Group Authorization and Group Policy Lookup

An ISAKMP client configuration group (or VPN group) is a group of VPN clients that share the same authentication and configuration information. Group policies can be configured locally on this router, an external server, or both. Easy VPN Server will use these group policies to authenticate VPN clients.

Method List for Group Policy Lookup

Select the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies.

○ Local

1. ● RADIUS

○ RADIUS and local

2. Add RADIUS Server...

Summary

RADIUS server will be used for group authorization.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-33

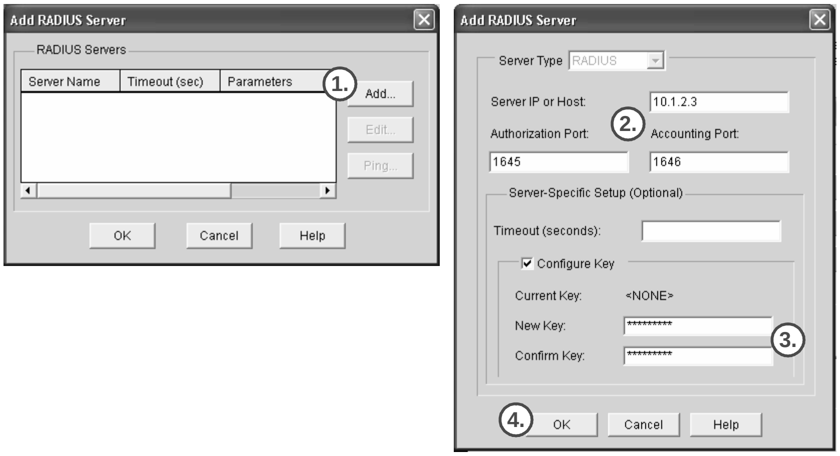
The second option is using RADIUS server for group authorization:

Step 1 In the Group Authorization and Group Policy Lookup window, click the **RADIUS** radio button in the Method List for Group Policy Lookup section.

Step 2 Click **Add RADIUS Server** to add a RADIUS 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 self-study.

Option 2: External Location via RADIUS (Cont.)



Server Type: RADIUS

Server IP or Host: 10.1.2.3

Authorization Port: 1645

Accounting Port: 1646

Timeout (seconds):

☑ Configure Key

Current Key: <NONE>

New Key: *********

Confirm Key: *********

© 2006 Cisco Systems, Inc. All rights reserved.

An Add RADIUS Server window opens:

Step 1 Click **Add** to add RADIUS server parameters.

Step 2 Specify the IP address of the server, RADIUS authorization port, and RADIUS authentication port (use ports 1645 and 1646 for Cisco Secure Access Control Server [ACS], and ports 1812 and 1813 for other RADIUS servers).

Step 3 You should use a key to authenticate individual RADIUS messages. To configure the key, select the **Configure Key** check box and enter the key twice.

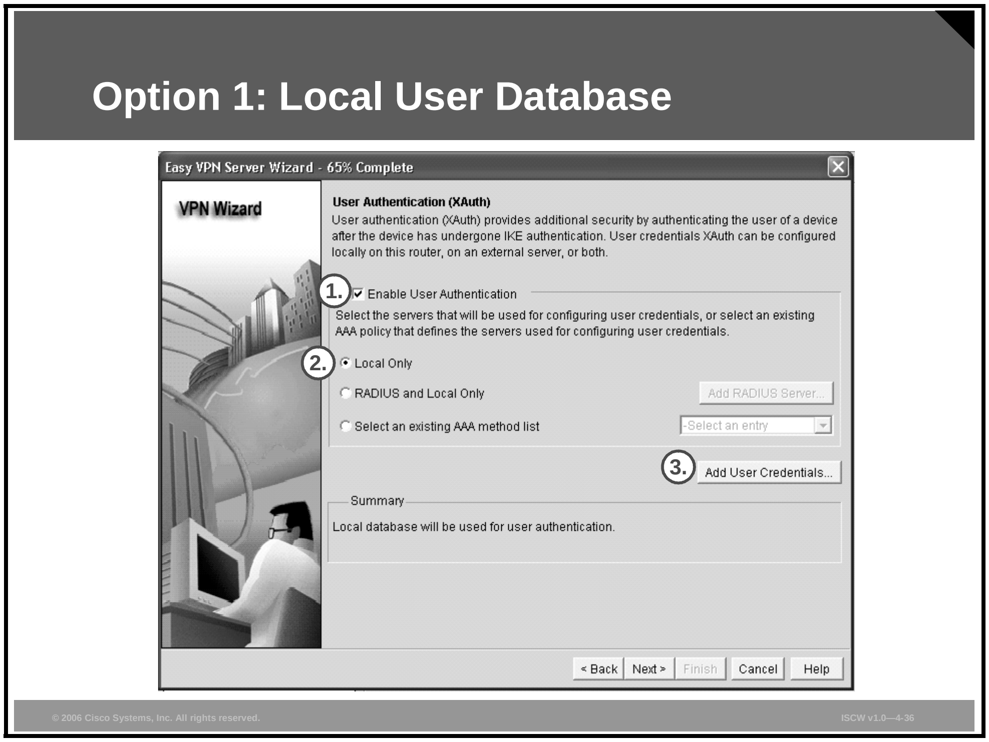
Step 4 Click **OK**.

When you are back on the Group Authorization and Group Policy Lookup window, click **Next** to continue.

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

User Authentication

This topic describes the locations where you store user records for Xauth.



Option 1: Local User Database

Easy VPN Server Wizard - 65% Complete

User Authentication (XAuth)

User authentication (XAuth) provides additional security by authenticating the user of a device after the device has undergone IKE authentication. User credentials XAuth can be configured locally on this router, on an external server, or both.

1. ☑ Enable User Authentication

Select the servers that will be used for configuring user credentials, or select an existing AAA policy that defines the servers used for configuring user credentials.

2. ● Local Only

○ RADIUS and Local Only

○ Select an existing AAA method list

3. Add User Credentials...

Summary

Local database will be used for user authentication.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-36

The figure illustrates the page on which you select the location where user records for Xauth will be stored.

Option 1: Local User Database

To store the user records to a local user database:

Step 1 In the User Authentication (XAuth) window, select the **Enable User Authentication** check box.

Step 2 Click the **Local Only** radio button. The *Local Only* option means that all users will be in the router configuration in NVRAM.

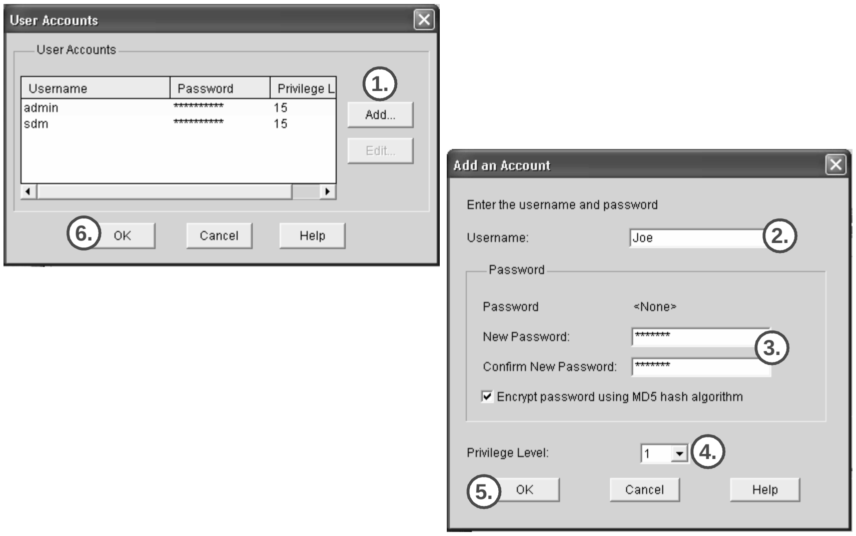
Step 3 Add users by clicking **Add User Credentials**.

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

Adding Users

This section describes how to configure VPN users.

Local User Database—Adding Users



User Accounts

Username	Password	Privilege L
admin	**********	15
sdm	**********	15

Add an Account

Enter the username and password

Username: Joe

Password

Password <None>

New Password: *******

Confirm New Password: *******

☑ Encrypt password using MD5 hash algorithm

Privilege Level: 1

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-37

A User Accounts window opens. Follow this procedure to add a new user account:

Step 1 Click **Add**.

Step 2 An Add an Account window opens. Enter username in the **Username** field.

Step 3 Enter password and confirm it.

Step 4 Use default privilege level 1 for VPN users.

Step 5 Click **OK**.

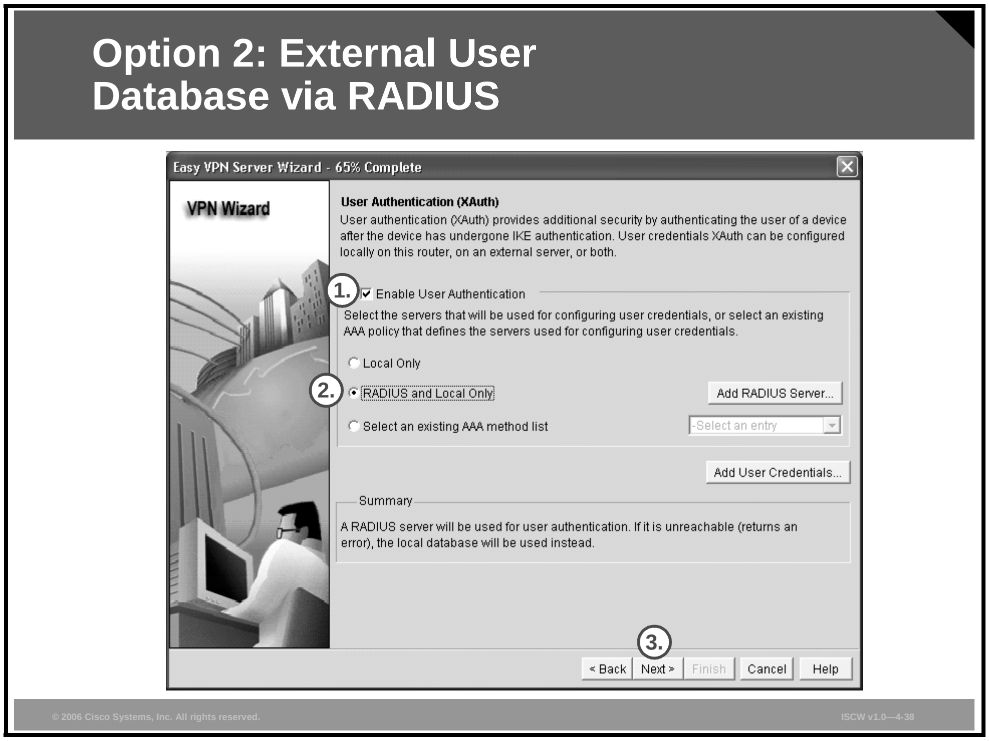
Step 6 Click **OK** in the User Accounts window.

When you are back on the User Authentication (XAuth) window, click **Next** to continue.

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

Option 2: External User Database via RADIUS

If RADIUS is used for user authentication you can use a previously configured RADIUS server or define a new one.



Option 2: External User Database via RADIUS

Easy VPN Server Wizard - 65% Complete

VPN Wizard

User Authentication (XAuth)

User authentication (XAuth) provides additional security by authenticating the user of a device after the device has undergone IKE authentication. User credentials XAuth can be configured locally on this router, on an external server, or both.

1. ☑ Enable User Authentication

Select the servers that will be used for configuring user credentials, or select an existing AAA policy that defines the servers used for configuring user credentials.

○ Local Only

2. ● RADIUS and Local Only

○ Select an existing AAA method list

Summary

A RADIUS server will be used for user authentication. If it is unreachable (returns an error), the local database will be used instead.

3.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-38

Follow these steps to store the user records to a RADIUS and local user database:

Step 1 In the User Authentication (XAuth) window, select the **Enable User Authentication** check box.

Step 2 Click the **RADIUS and Local Only** radio button.

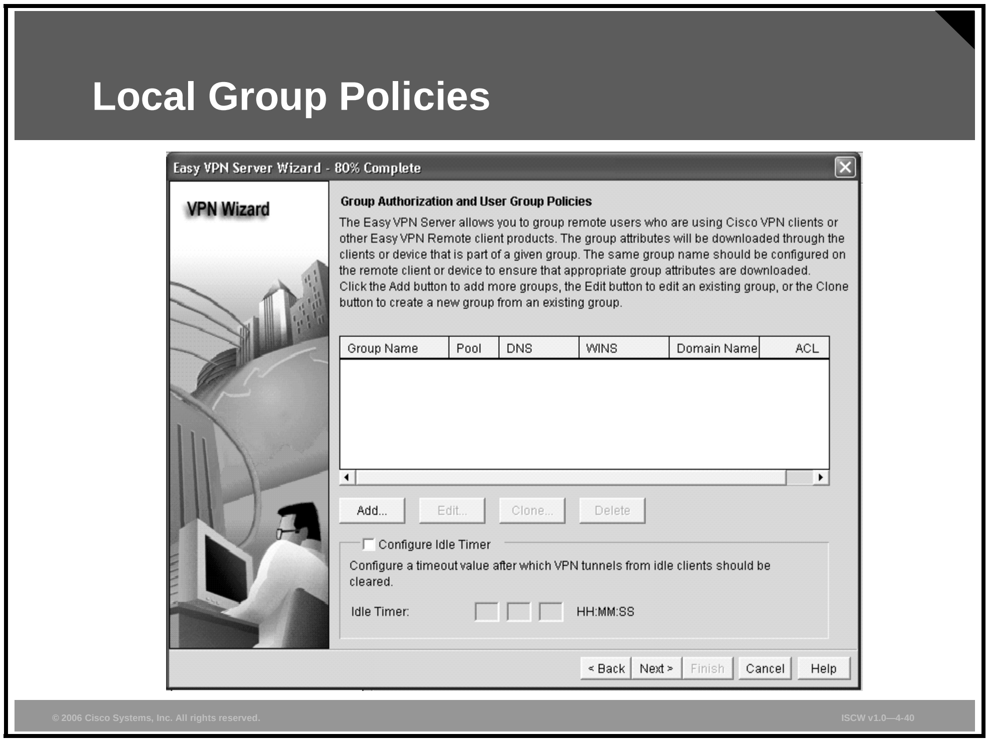
Step 3 Click **Next** to continue.

Alternatively, you can select a previously configured AAA authentication template by clicking the **Select an existing AAA method list** radio button.

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

Local Group Policies

This topic describes how to configure local group policies.



Local Group Policies

Group Authorization and User Group Policies

The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other Easy VPN Remote client products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured on the remote client or device to ensure that appropriate group attributes are downloaded.
Click the Add button to add more groups, the Edit button to edit an existing group, or the Clone button to create a new group from an existing group.

Group Name	Pool	DNS	WINS	Domain Name	ACL

☐ Configure Idle Timer

Configure a timeout value after which VPN tunnels from idle clients should be cleared.

Idle Timer: □ □ □ HH:MM:SS

© 2006 Cisco Systems, Inc. All rights reserved.

The figure illustrates the page on which local group policies can be configured.

In the Group Authorization and User Group Policies window, click **Add** to add a group policy.

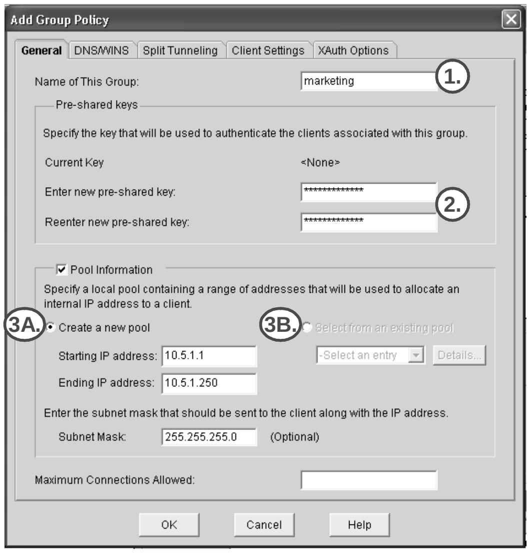
You can skip this step if you intend to store group policies on an AAA server (useful when you are managing a large number of VPN servers).

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

General Parameters

This section describes how to set general parameters.

General Parameters



Name of This Group: marketing

Pre-shared keys

Specify the key that will be used to authenticate the clients associated with this group.

Current Key <None>

Enter new pre-shared key: **************

Reenter new pre-shared key: **************

☑ Pool Information

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

● Create a new pool ○ Select from an existing pool

Starting IP address: 10.5.1.1 -Select an entry Details...

Ending IP address: 10.5.1.250

Enter the subnet mask that should be sent to the client along with the IP address.

Subnet Mask: 255.255.255.0 (Optional)

Maximum Connections Allowed:

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-41

Use the General tab to configure the minimum required parameters for a functional group policy:

Step 1 Define a name of the group.

Step 2 Enter the preshared secret for the group.

Step 3 Specify an IP address pool from which addresses will be taken and assigned to clients. You have these two options:

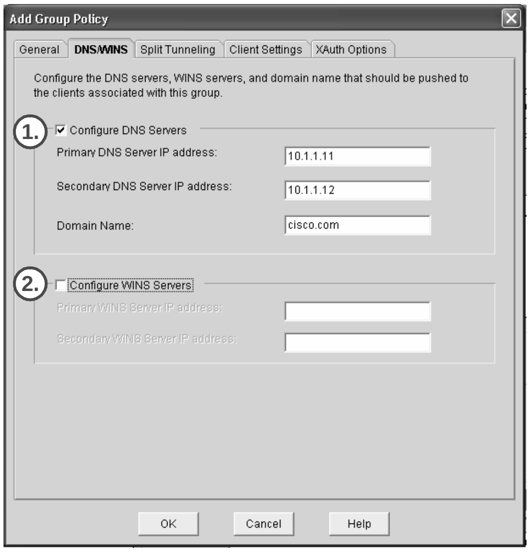
A) Create a new pool
B) Select from an existing pool

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

Domain Name System

This section describes how to configure a DNS.

Domain Name System



Add Group Policy

Configure the DNS servers, WINS servers, and domain name that should be pushed to the clients associated with this group.

1. ☑ Configure DNS Servers

Primary DNS Server IP address: 10.1.1.11

Secondary DNS Server IP address: 10.1.1.12

Domain Name: cisco.com

2. □ Configure WINS Servers

Primary WINS Server IP address:

Secondary WINS Server IP address:

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-42

Select the DNS/WINS tab to configure the DNS and WINS servers:

Step 1 You should specify any internal DNS servers that may be required by clients in order to be able to resolve hostnames that are only reachable inside the VPN.

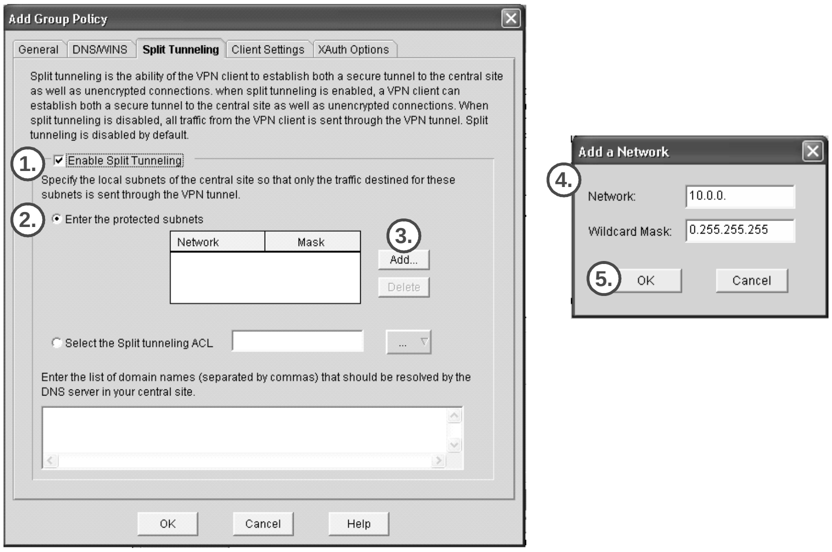
Step 2 The same applies to WINS servers.

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

Split Tunneling

You should keep split tunneling disabled (default) to prevent any compromised client PC from becoming a proxy between the Internet and the VPN.

Split Tunneling



Add Group Policy

General | DNS/WINS | Split Tunneling | Client Settings | XAuth Options

Split tunneling is the ability of the VPN client to establish both a secure tunnel to the central site as well as unencrypted connections. when split tunneling is enabled, a VPN client can establish both a secure tunnel to the central site as well as unencrypted connections. When split tunneling is disabled, all traffic from the VPN client is sent through the VPN tunnel. Split tunneling is disabled by default.

☑ Enable Split Tunneling

Specify the local subnets of the central site so that only the traffic destined for these subnets is sent through the VPN tunnel.

● Enter the protected subnets

Network	Mask

Add... Delete

○ Select the Split tunneling ACL

Enter the list of domain names (separated by commas) that should be resolved by the DNS server in your central site.

OK Cancel Help

Add a Network

Network: 10.0.0.

Wildcard Mask: 0.255.255.255

OK Cancel

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-43

If, however, split tunneling is required, you should complete one of the following two configuration options on the Split Tunneling tab:

Step 1 Check the **Enable Split Tunneling** check box.

Step 2 Click the **Enter the protected subnets** radio button.

Step 3 Click **Add** to add a network**.**

Step 4 In the Add a Network window, define protected networks (all other destinations will be reachable by bypassing the tunnel).

Step 5 Click **OK**.

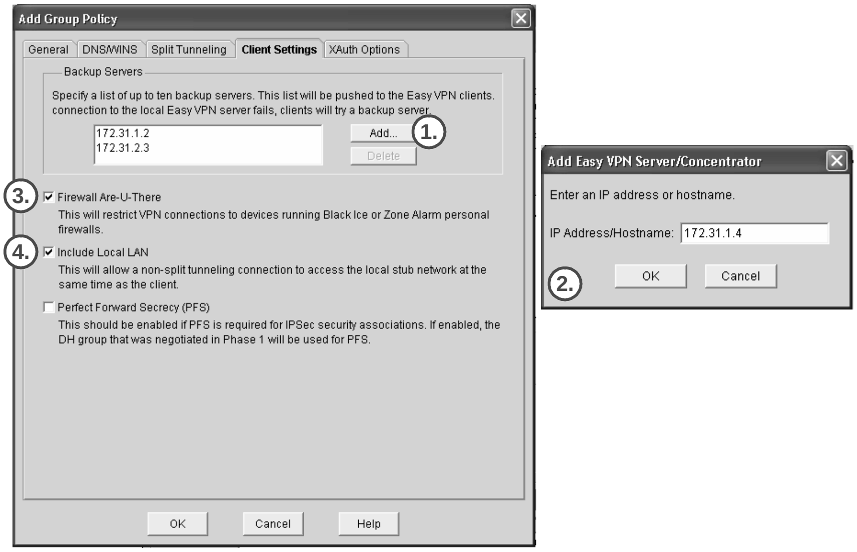
Alternatively, click the **Select the Split tunneling ACL** radio button to use an existing ACL or create a new ACL to configure split tunneling.

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

Advanced Options

This section describes how to configure advanced options.

Advanced Options



Backup Servers

Specify a list of up to ten backup servers. This list will be pushed to the Easy VPN clients. connection to the local Easy VPN server fails, clients will try a backup server.

172.31.1.2
172.31.2.3

☑ Firewall Are-U-There

This will restrict VPN connections to devices running Black Ice or Zone Alarm personal firewalls.

☑ Include Local LAN

This will allow a non-split tunneling connection to access the local stub network at the same time as the client.

☐ Perfect Forward Secrecy (PFS)

This should be enabled if PFS is required for IPSec security associations. If enabled, the DH group that was negotiated in Phase 1 will be used for PFS.

Enter an IP address or hostname.

IP Address/Hostname: 172.31.1.4

© 2006 Cisco Systems, Inc. All rights reserved.

On the Client Settings tab, you can also define a list of backup servers that will be pushed to the client:

Step 1 Click **Add**.

Step 2 In the Add Easy VPN Server/Concentrator window, enter an IP address or hostname and click **OK**.

Step 3 Select the **Firewall Are-U-There** check box.

Step 4 Select the **Include Local LAN** check box.

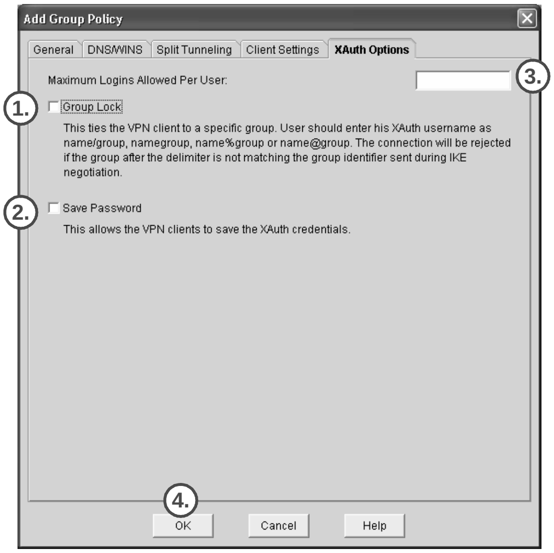
© 2006 Cisco Systems, Inc.

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 self-study.

Xauth Options

This section describes how to configure user authentication.

Xauth Options



Maximum Logins Allowed Per User:

□ Group Lock

This ties the VPN client to a specific group. User should enter his XAuth username as name/group, namegroup, name%group or name@group. The connection will be rejected if the group after the delimiter is not matching the group identifier sent during IKE negotiation.

□ Save Password

This allows the VPN clients to save the XAuth credentials.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-45

Configure user authentication using Xauth with these additional options on the XAuth Options tab:

Step 1 Select the **Group Lock** check box to statically tie a user to a VPN group where users will have to use group name as part of the Xauth username.

Step 2 Select the **Save Password** check box to allow user to save the password in the VPN client.

Step 3 Type the maximum number of concurrent logins to prevent multiple users from sharing the same account at the same time to the Maximum Logins Allowed Per User field.

Step 4 Click **OK**.

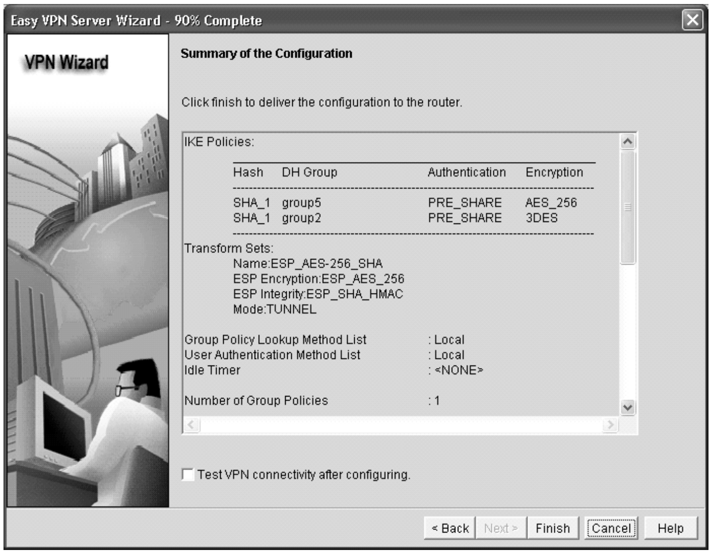
When you are back on the Group Authorization and User Group Policies window, click **Next** to continue.

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

Completing the Configuration

This topic describes how to complete the configuration by viewing the settings in the Summary of the Configuration window.

Review the Generated Configuration



Summary of the Configuration

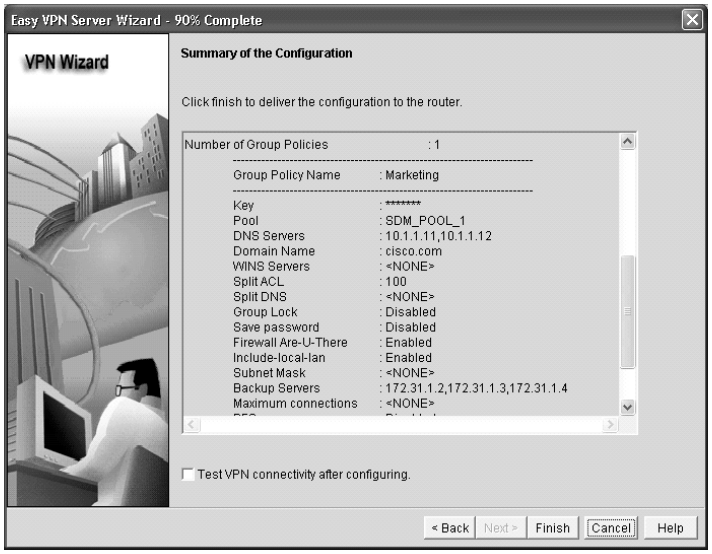
Click finish to deliver the configuration to the router.

```
IKE Policies:

          ____________________________________________________________
          Hash     DH Group                 Authentication   Encryption
          -------------------------------------------------------------
          SHA_1    group5                   PRE_SHARE        AES_256
          SHA_1    group2                   PRE_SHARE        3DES
          -------------------------------------------------------------
Transform Sets:
          Name:ESP_AES-256_SHA
          ESP Encryption:ESP_AES_256
          ESP Integrity:ESP_SHA_HMAC
          Mode:TUNNEL

Group Policy Lookup Method List         : Local
User Authentication Method List         : Local
Idle Timer                              : <NONE>

Number of Group Policies                : 1
```

☐ Test VPN connectivity after configuring.

© 2006 Cisco Systems, Inc. All rights reserved.

Review the Generated Configuration (Cont.)



Summary of the Configuration

Click finish to deliver the configuration to the router.

```
Number of Group Policies                : 1
          ------------------------------------------------
          Group Policy Name         : Marketing
          ------------------------------------------------
          Key                       : *******
          Pool                      : SDM_POOL_1
          DNS Servers               : 10.1.1.11,10.1.1.12
          Domain Name               : cisco.com
          WINS Servers              : <NONE>
          Split ACL                 : 100
          Split DNS                 : <NONE>
          Group Lock                : Disabled
          Save password             : Disabled
          Firewall Are-U-There      : Enabled
          Include-local-lan         : Enabled
          Subnet Mask               : <NONE>
          Backup Servers            : 172.31.1.2,172.31.1.3,172.31.1.4
          Maximum connections       : <NONE>
```

☐ Test VPN connectivity after configuring.

© 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 self-study.

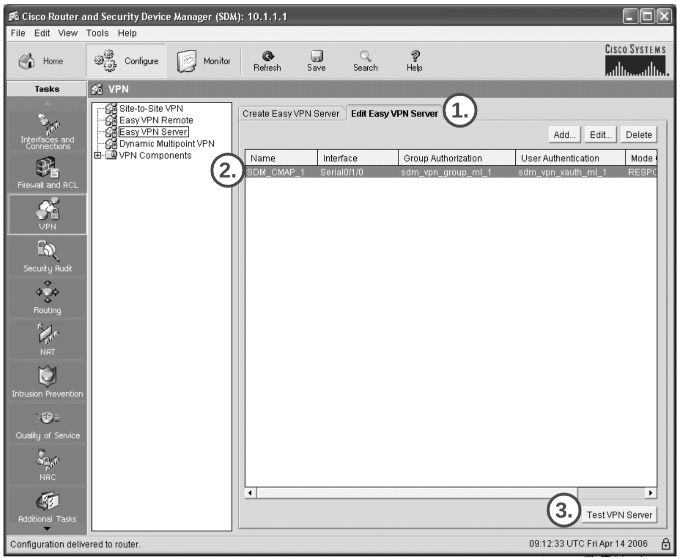
The wizard will present a summary of the configured parameters. You can go back to correct the configuration in case you have made a mistake. Otherwise, click **Finish** to apply the configuration to the router.

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 self-study.

Verify the Easy VPN Server Configuration

This section describes how to verify Easy VPN Server configuration.

Verify the Easy VPN Server Configuration



Name	Interface	Group Authorization	User Authentication	Mode
SDM_CMAP_1	Serial0/1/0	sdm_vpn_group_ml_1	sdm_vpn_xauth_ml_1	RESPO

Configuration delivered to router.

09:12:33 UTC Fri Apr 14 2006

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-49

Once the Easy VPN Server configuration is created, you can run a test to determine the configuration sanity of the tunnel:

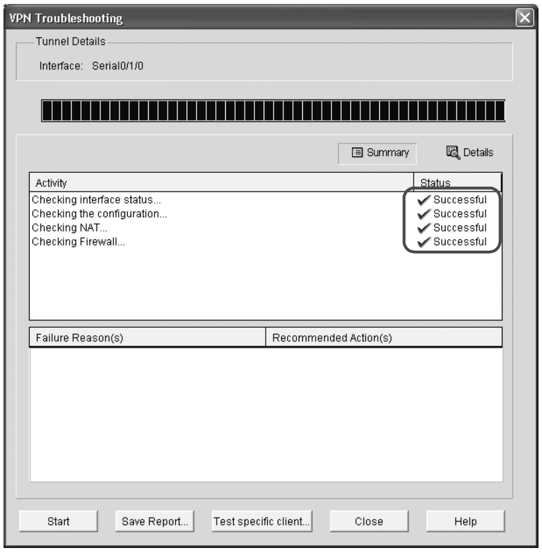
Step 1 Click the **Edit Easy VPN Server** tab.

Step 2 Choose an Easy VPN server configuration.

Step 3 Click the **Test VPN Server** button to run the test.

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

Verify the Easy VPN Server Configuration (Cont.)



VPN Troubleshooting

Tunnel Details

Interface: Serial0/1/0

Activity	Status
Checking interface status...	✓ Successful
Checking the configuration...	✓ Successful
Checking NAT...	✓ Successful
Checking Firewall...	✓ Successful

Failure Reason(s)	Recommended Action(s)

© 2006 Cisco Systems, Inc. All rights reserved.

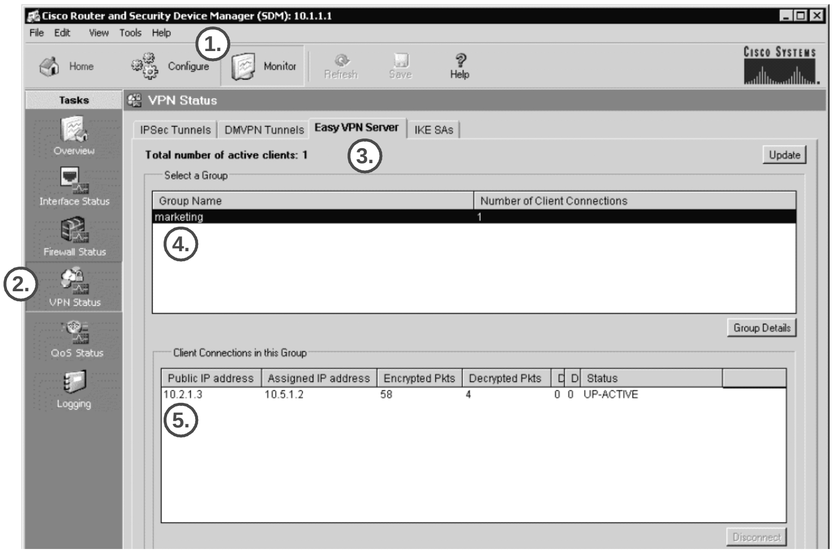
Start the test by clicking **Start** in the VPN Troubleshooting window. The status of each tested activity should be “Successful.”

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

Monitoring Easy VPN Server

This section describes how to monitor Easy VPN Server.

Monitoring Easy VPN Server



Total number of active clients: 1

Group Name	Number of Client Connections
marketing	1

Public IP address	Assigned IP address	Encrypted Pkts	Decrypted Pkts	D	D	Status
10.2.1.3	10.5.1.2	58	4	0	0	UP-ACTIVE

© 2006 Cisco Systems, Inc. All rights reserved.

Use the monitoring page to display the status of the tunnel and the currently logged-in users.

Step 1 Select the **Monitor** icon in the toolbar at the top of the window.

Step 2 Click the **VPN Status** icon in the Tasks toolbar at the left side of the window.

Step 3 Select **Easy VPN Server** tab.

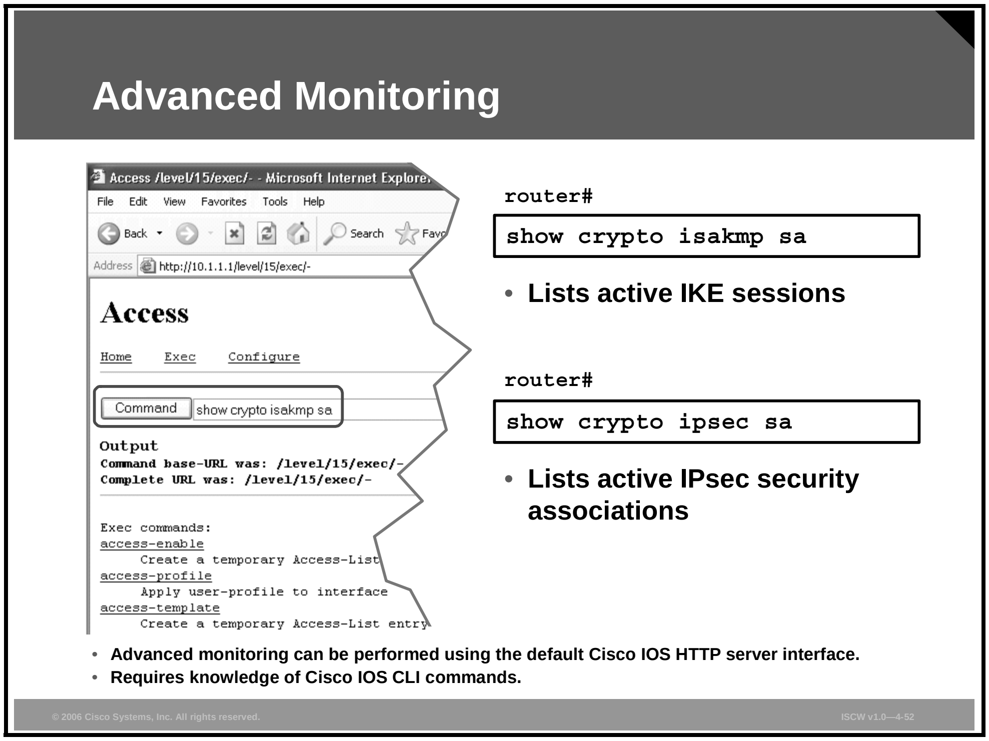
Step 4 Select a group name in the **Select a Group** section.

Step 5 Verify the client connections in the **Client Connections in this Group** section.

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

Advanced Monitoring

The basic Cisco IOS web interface also allows you to use the web interface to enter Cisco IOS command-line interface (CLI) commands to monitor and troubleshoot the router.



Advanced Monitoring

Access /level/15/exec/- - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favo
Address http://10.1.1.1/level/15/exec/-
Access
Home Exec Configure
Command

show crypto isakmp sa

```
Output
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-

Exec commands:
access-enable
     Create a temporary Access-List
access-profile
     Apply user-profile to interface
access-template
     Create a temporary Access-List entry
```

```
router#
show crypto isakmp sa
```

- Lists active IKE sessions

```
router#
show crypto ipsec sa
```

- Lists active IPsec security associations

- Advanced monitoring can be performed using the default Cisco IOS HTTP server interface.
- Requires knowledge of Cisco IOS CLI commands.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-52

The table lists two of the most useful **show** commands to determine the status of IPsec VPN connections.

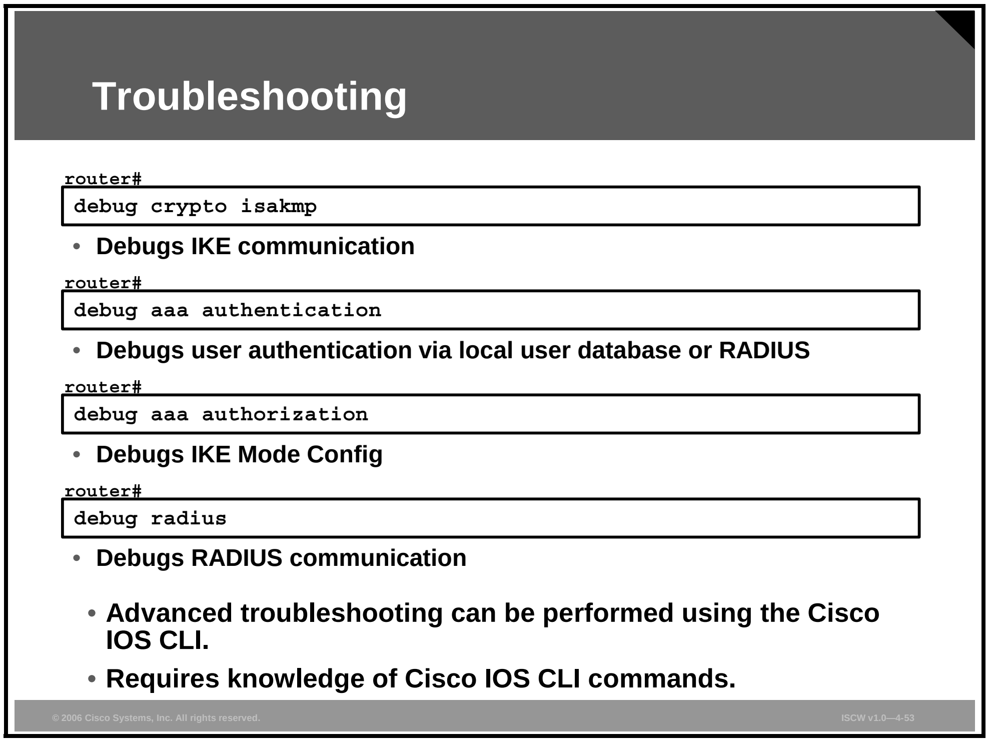
show Commands

Command	Description
`show crypto isakmp sa`	To display all current IKE SAs, use the **show crypto isakmp sa** command in EXEC mode. QM_IDLE status indicates an active IKE SA.
`show crypto ipsec sa`	To display the settings used by current SAs, use the **show crypto ipsec sa** command in EXEC mode. Non-zero encryption and decryption statistics can indicate a working set of IPsec SAs.

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

Troubleshooting

You should use a terminal to connect to the Cisco IOS router if you want to use debugging commands to troubleshoot VPN connectivity. The **debug crypto isakmp** command displays detailed information about the IKE Phase 1 and Phase 2 negotiation processes.



Troubleshooting

```
router#
debug crypto isakmp
```

- **Debugs IKE communication**

```
router#
debug aaa authentication
```

- **Debugs user authentication via local user database or RADIUS**

```
router#
debug aaa authorization
```

- **Debugs IKE Mode Config**

```
router#
debug radius
```

- **Debugs RADIUS communication**

- **Advanced troubleshooting can be performed using the Cisco IOS CLI.**
- **Requires knowledge of Cisco IOS CLI commands.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-53

To display messages about IKE events, use the **debug crypto isakmp** command in EXEC mode.

To debug the authentication and authorization of Easy VPN tunnels, you can use the commands listed in the table.

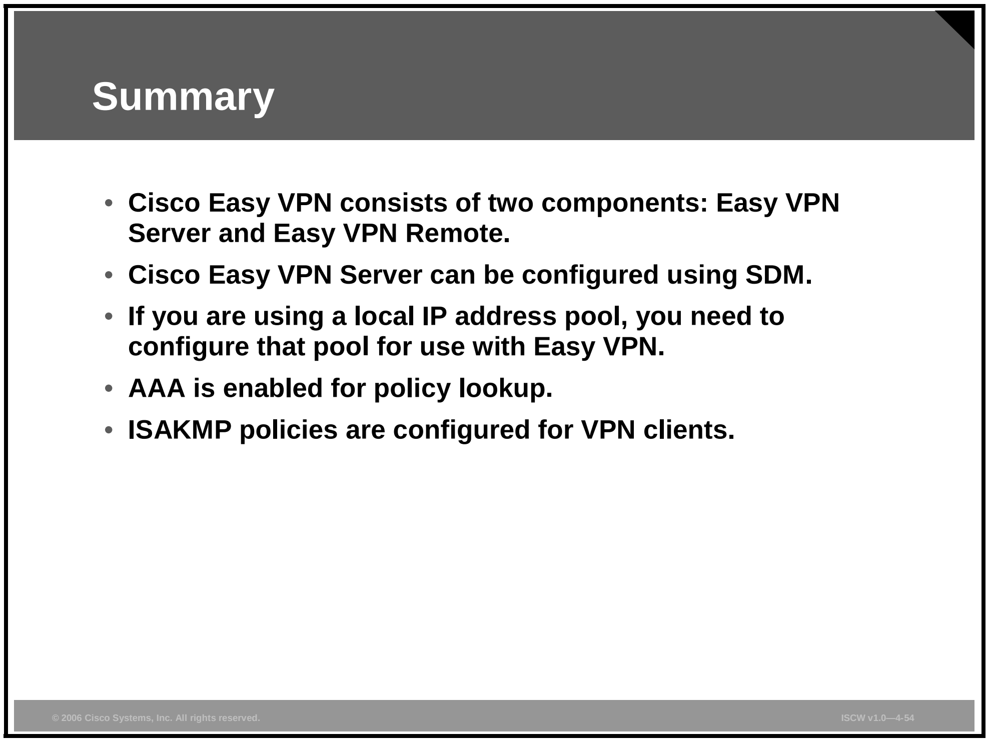
debug Commands

Command	Description
`debug aaa authentication`	Use for troubleshooting user authentication
`debug aaa authorization`	Use for troubleshooting group policy configuration access via RADIUS
`debug radius`	Use to troubleshoot RADIUS communication

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

Summary

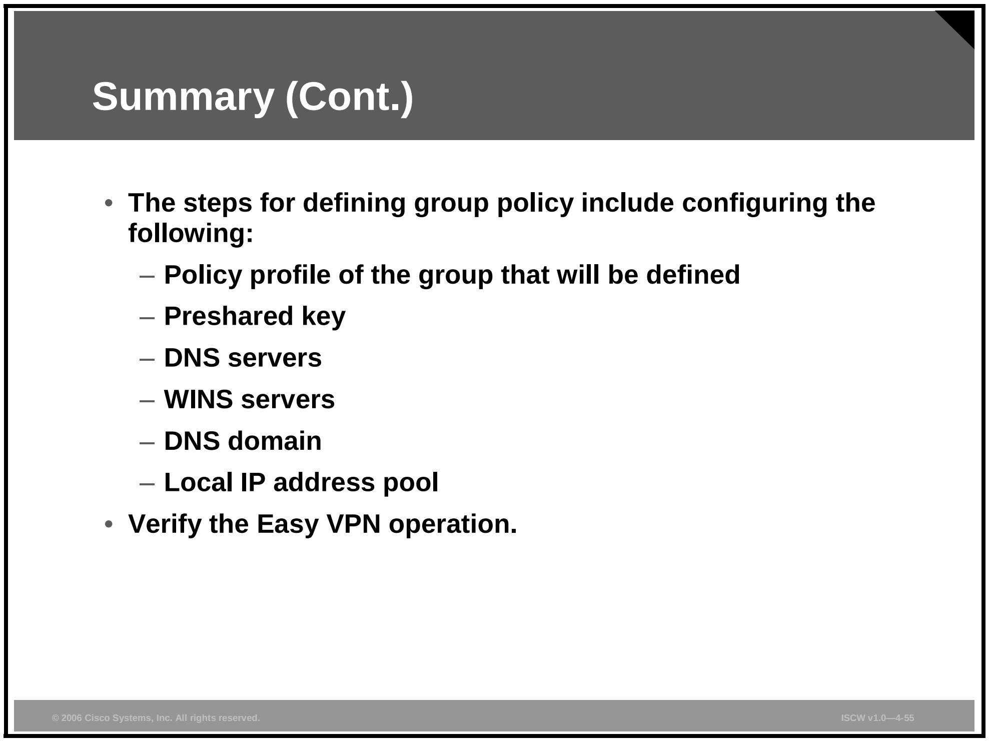
This topic summarizes the key points that were discussed in this lesson.



Summary

- Cisco Easy VPN consists of two components: Easy VPN Server and Easy VPN Remote.
- Cisco Easy VPN Server can be configured using SDM.
- If you are using a local IP address pool, you need to configure that pool for use with Easy VPN.
- AAA is enabled for policy lookup.
- ISAKMP policies are configured for VPN clients.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-54



Summary (Cont.)

- The steps for defining group policy include configuring the following:
  - Policy profile of the group that will be defined
  - Preshared key
  - DNS servers
  - WINS servers
  - DNS domain
  - Local IP address pool
- Verify the Easy VPN operation.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-55

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

References

For additional information, refer to these resources:

- *Cisco Router and Security Device Manager Version 2.2 User's Guide* at: http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_book09186a00804bfd82.html

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

Lesson 7

Implementing the Cisco VPN Client

Overview

The Cisco virtual private network (VPN) Client for Windows (or VPN Client) is software that runs on a Microsoft Windows-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN Server on an enterprise network or with a service provider, creates a secure connection over the Internet. This lesson describes the process of setting up a Cisco VPN Client on a laptop to create a secure connection, called a tunnel, between your computer and a private network.

Objectives

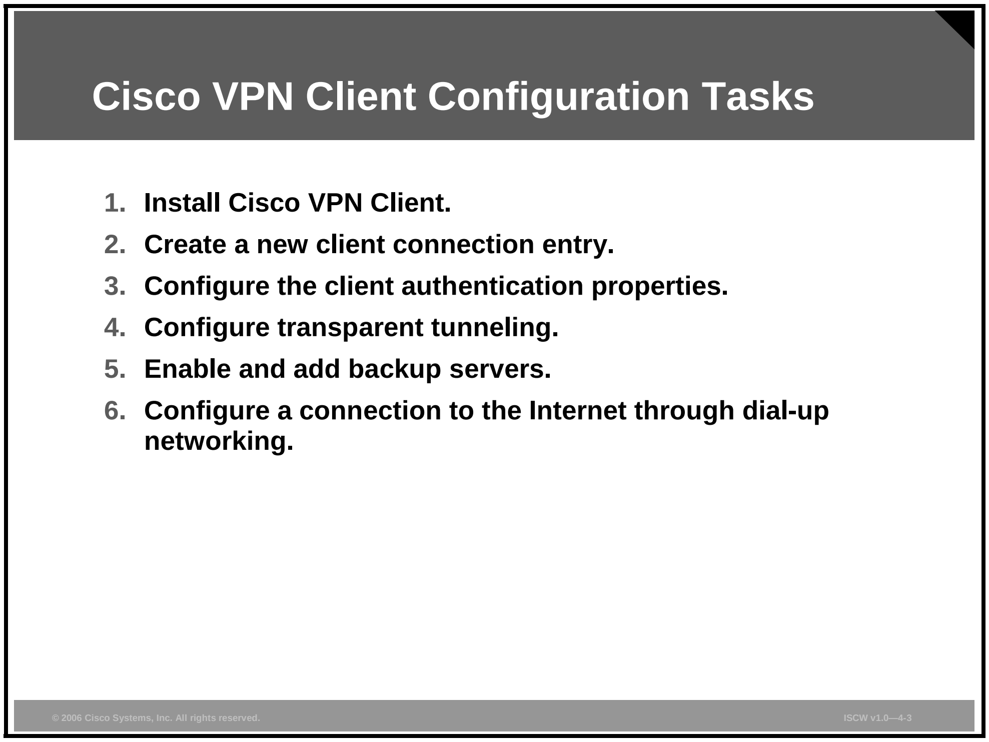
Upon completing this lesson, you will be able to describe, configure, and verify the Cisco VPN Client on a Windows PC. This ability includes being able to meet these objectives:

- List the steps required to configure the software VPN client on a PC
- Describe each of the steps required to configure Cisco VPN Client

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

Cisco VPN Client Configuration Tasks

This topic describes the steps required to configure the software VPN client on a PC.



Cisco VPN Client Configuration Tasks

1. **Install Cisco VPN Client.**
2. **Create a new client connection entry.**
3. **Configure the client authentication properties.**
4. **Configure transparent tunneling.**
5. **Enable and add backup servers.**
6. **Configure a connection to the Internet through dial-up networking.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-3

Complete these tasks to configure the Cisco VPN Client for Easy VPN Remote access:

Step 1 Install a Cisco VPN Client on the remote user PC.

Step 2 Create a new client connection entry.

Step 3 Configure client authentication properties.

Step 4 Configure transparent tunneling.

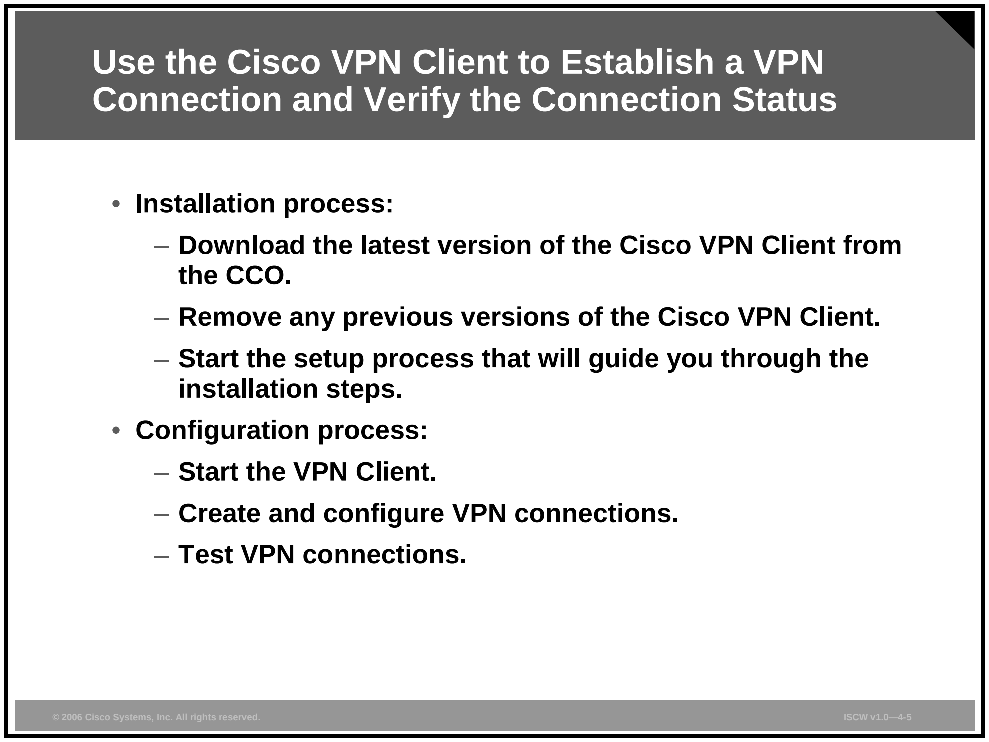
Step 5 Enable and add backup servers.

Step 6 Configure a connection to the Internet through dial-up networking.

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

Use the Cisco VPN Client to Establish a VPN Connection and Verify the Connection Status

This topic describes the steps required to configure Cisco Easy VPN Client.



Use the Cisco VPN Client to Establish a VPN Connection and Verify the Connection Status

- **Installation process:**
  - **Download the latest version of the Cisco VPN Client from the CCO.**
  - **Remove any previous versions of the Cisco VPN Client.**
  - **Start the setup process that will guide you through the installation steps.**
- **Configuration process:**
  - **Start the VPN Client.**
  - **Create and configure VPN connections.**
  - **Test VPN connections.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-5

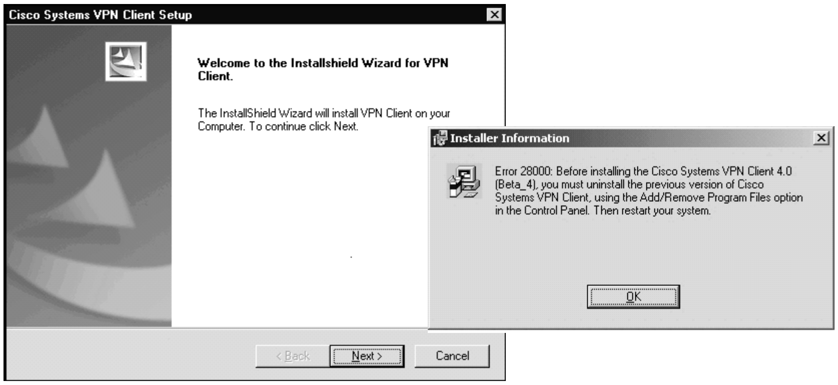
To enable Microsoft Windows operating systems to use native IPsec, add IPsec client software that supports it. The Cisco VPN Client software can be used to achieve that.

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

Task 1: Install Cisco VPN Client

You can install the VPN Client on your system by using either of two applications: InstallShield or Microsoft Windows Installer (MSI). Both applications use installation wizards to walk you through the installation.

Task 1: Install Cisco VPN Client



Cisco Systems VPN Client Setup

Welcome to the Installshield Wizard for VPN Client.

The InstallShield Wizard will install VPN Client on your Computer. To continue click Next.

Installer Information

Error 28000: Before installing the Cisco Systems VPN Client 4.0 (Beta_4), you must uninstall the previous version of Cisco Systems VPN Client, using the Add/Remove Program Files option in the Control Panel. Then restart your system.

© 2006 Cisco Systems, Inc. All rights reserved.

This topic describes how to install the VPN Client on your PC and includes the following:

- Verifying system requirements
- Gathering the information that you need
- Installing the VPN Client through InstallShield
- Installing the VPN Client through MSI

If you have not removed a previously installed VPN Client, when you execute the **vpnclient_en.exe** command or **vpnclient_en.msi** command, an error message displays. You must uninstall the previously installed VPN Client before proceeding with the new installation.

To remove a VPN Client installed with MSI, use the Windows Add/Remove Programs located in the control panel. To remove a VPN Client installed with InstallShield, choose **Start > Programs > Cisco Systems VPN Client > Uninstall Client**.

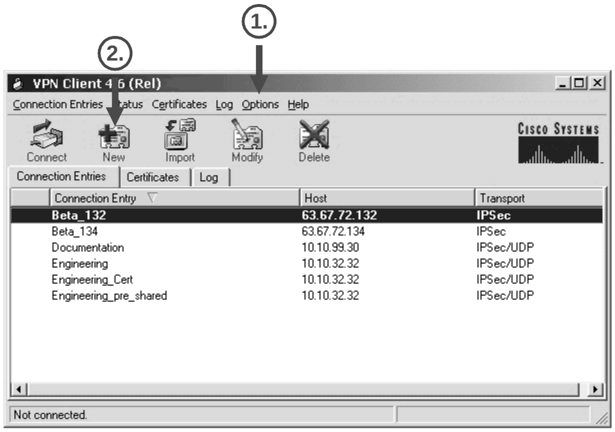
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Task 2: Create a New Client Connection Entry

To use the VPN Client, you must create at least one connection entry that includes this information:

- The VPN device (the remote server) to access.
- Preshared keys—the IPsec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPsec algorithms that your VPN Client uses.
- Certificates—the name of the certificate that you are using for authentication.
- Optional parameters that govern VPN Client operation and connection to the remote network.

Task 2: Create a New Client Connection Entry



Connection Entry	Host	Transport
Beta_132	**63.67.72.132**	**IPSec**
Beta_134	63.67.72.134	IPSec
Documentation	10.10.99.30	IPSec/UDP
Engineering	10.10.32.32	IPSec/UDP
Engineering_Cert	10.10.32.32	IPSec/UDP
Engineering_pre_shared	10.10.32.32	IPSec/UDP

Not connected.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-7

You can create multiple connection entries if you use your VPN Client to connect to multiple networks (though not simultaneously) or if you belong to more than one VPN remote access group.

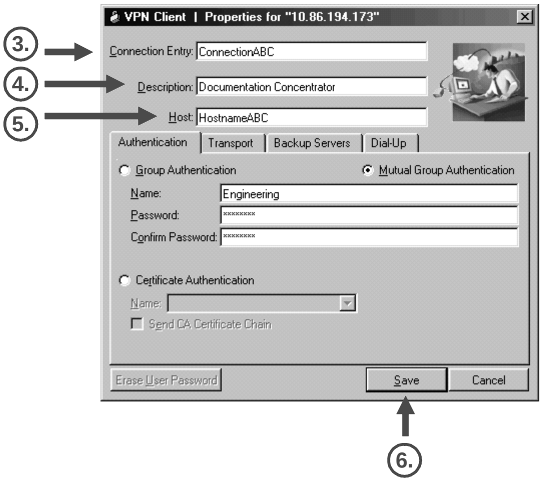
To create a new connection entry, start the VPN Client by choosing **Start > Programs > Cisco Systems VPN Client > VPN Client** and follow this procedure:

Step 1 The VPN Client application starts and displays the advanced mode main window. If this is not the case and the simple mode window is displayed, choose **Options > Advanced Mode** or press **Ctrl-M**.

Step 2 Click the **New** icon in the toolbar. Alternatively, you can choose **New** in the **Connection Entries** menu. The VPN Client displays a form.

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

Task 2: Create a New Client Connection Entry (Cont.)



VPN Client | Properties for "10.86.194.173"

Connection Entry: ConnectionABC

Description: Documentation Concentrator

Host: HostnameABC

○ Group Authentication ● Mutual Group Authentication

Name: Engineering

Password: ********

Confirm Password: ********

○ Certificate Authentication

Name:

□ Send CA Certificate Chain

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-8

Step 3 Enter a unique name for this new connection in the **Connection Entry** field. You can use any name to identify this connection; for example, Engineering. This name can contain spaces, and it is not case-sensitive.

Step 4 Enter a description of this connection in the **Description** field. This field is optional, but it helps further identify this connection; for example, Connection to Engineering remote server.

Step 5 Enter the host name or IP address of the remote VPN device that you want to access in the **Host** field.

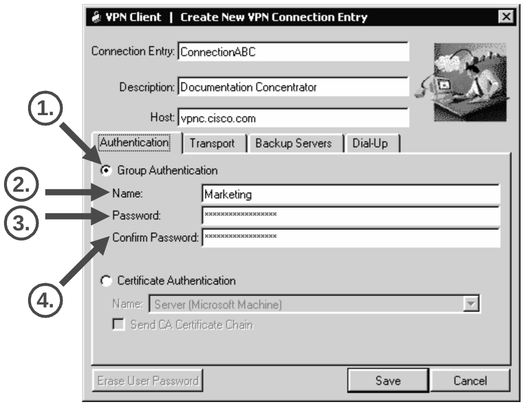
Step 6 Save the connection entry by clicking the **Save** button.

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

Task 3: Configure Client Authentication Properties

Under the Authentication tab, enter the information for the method that you want to use. You can connect as part of a group (configured on a VPN device) or by supplying an identity digital certificate.

Task 3: Configure Client Authentication Properties



Connection Entry: ConnectionABC

Description: Documentation Concentrator

Host: vpnc.cisco.com

● Group Authentication

Name: Marketing

Password: ****************

Confirm Password: ****************

○ Certificate Authentication

Name: Server (Microsoft Machine)

□ Send CA Certificate Chain

Authentication options:

- **Group preshared secrets (group name and group secret)**
- **Mutual authentication (import CA certificate first; group name and secret)**
- **Digital certificates (enroll with the CA first; select the certificate)**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-9

Group Authentication

The network administrator usually configures group authentication for you. If this is not the case, complete this procedure:

Step 1 Select the **Group Authentication** radio button.

Step 2 In the **Name** field, enter the name of the IPsec group to which you belong. This entry is case-sensitive.

Step 3 In the **Password** field, enter the password (which is also case-sensitive) for your IPsec group. The field displays only asterisks.

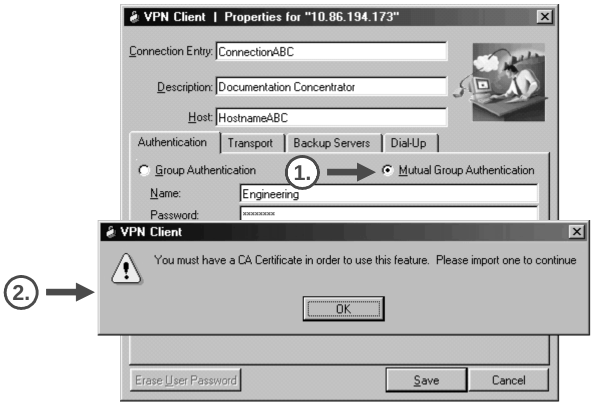
Step 4 Verify your password by entering it again in the **Confirm Password** field.

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

Mutual Group Authentication

Another option is to use mutual group authentication.

Mutual Group Authentication



VPN Client | Properties for "10.86.194.173"

Connection Entry: ConnectionABC

Description: Documentation Concentrator

Host: HostnameABC

You must have a CA Certificate in order to use this feature. Please import one to continue

- Mutual authentication should be used instead of group preshared secrets.
- Group preshared secrets are vulnerable to man-in-the-middle attacks if the attacker knows the group preshared secret.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-10

To use mutual group authentication, you need a root certificate that is compatible with the central-site VPN installed on your system:

Step 1 Your network administrator can load a root certificate on your system during installation. When you select the **Mutual Group Authentication** radio button, the VPN Client software verifies whether you have a root certificate installed.

Step 2 If you do not have a root certificate installed, the VPN Client prompts you to install one. Before you continue, you must import a root certificate.

When you have installed a root certificate (if required), follow the steps for group authentication.

Certificate Authentication

For certificate authentication, click the **Certificate Authentication** radio button and choose the name of the certificate you are using from the menu. If the field reads "No Certificates Installed" and is shaded, then you must enroll for a certificate before you can use this feature.

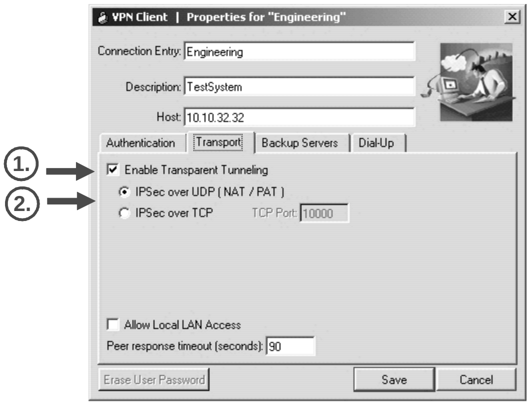
Note The procedure for certificate authentication varies according to the type of certificate you are using.

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

Task 4: Configure Transparent Tunneling

Next, configure transparent tunneling by completing the fields on the Transport tab.

Task 4: Configure Transparent Tunneling



VPN Client | Properties for "Engineering"

Connection Entry: Engineering

Description: TestSystem

Host: 10.10.32.32

☑ Enable Transparent Tunneling

● IPSec over UDP (NAT / PAT)

○ IPSec over TCP TCP Port: 10000

□ Allow Local LAN Access

Peer response timeout (seconds): 90

- **On by default.**
- **NAT-T enables IPsec and IKE over a standard UDP port 4500, allowing the VPN Client to be behind a NAT or PAT device.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-11

Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translation (PAT). Transparent tunneling encapsulates Protocol 50 (Encapsulating Security Payload, or ESP) traffic within UDP packets and can allow both Internet Security Association and Key Management Protocol (ISAKMP) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices or firewalls. The most common application for transparent tunneling is behind a home router performing PAT.

The VPN Client also sends keepalives frequently, ensuring that the mappings on the devices are kept active.

Not all devices support multiple simultaneous connections. Some devices cannot map additional sessions to unique source ports. Be sure to check with the vendor of your device to verify whether this limitation exists. Some vendors support Protocol 50 PAT (IPsec passthrough), which might let you operate without enabling transparent tunneling.

To use transparent tunneling, the central-site group in the Cisco VPN device must be configured to support it. For an example, refer to the **Cisco VPN 3000 Concentrator Manager > Configuration > User Management > Groups > Add > IPsec** tab (or refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration*, or Help in the VPN 3000 Concentrator Manager browser). Follow this procedure to use transparent tunneling:

Step 1 The transparent tunneling parameter is enabled by default. To disable this parameter, uncheck the **Enable Transparent Tunneling** check box. It is recommended that you always keep this parameter checked.

Step 2 Select a mode of transparent tunneling, over User Datagram Protocol (UDP) or over TCP. The mode that you use must match the mode used by the secure gateway to which you are connecting. Either mode operates properly through a PAT device.

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

Multiple simultaneous connections might work better with TCP, and if you are in an extranet environment, TCP mode is preferable. UDP does not operate with stateful firewalls, so in this case, you should use TCP.

Using IPsec over UDP (NAT/PAT)

To enable IPsec over UDP (NAT or PAT), click the **IPsec over UDP (NAT/PAT)** radio button. With UDP, the port number is negotiated. UDP is the default mode.

Using IPsec over TCP (NAT/PAT/Firewall)

To enable IPsec over TCP, click the **IPsec over TCP** radio button. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is 10000.

Allowing Local LAN Access

In a multiple-network interface card (NIC) configuration, local LAN access pertains only to network traffic on the interface on which the tunnel was established. The Allow Local LAN Access parameter gives you access to the resources on your local LAN (printer, fax, shared files, or other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your client system goes through the IPsec connection to the secure gateway.

To enable this feature, check the **Allow Local LAN Access** check box; to disable it, uncheck the check box. If the local LAN that you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

A network administrator at the central site configures a list of networks at the client side that you can access. You can access up to 10 networks when this feature is enabled. When the Allow Local LAN Access feature is enabled and you are connected to a central site, all traffic from your system goes through the IPsec tunnel except traffic to the networks excluded from doing so (in the network list).

When this feature is enabled and configured on the VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking at the routing table.

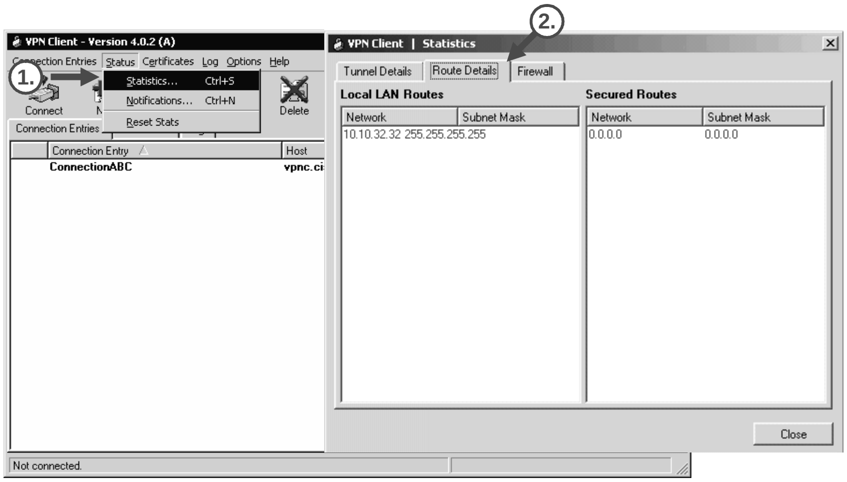
The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Routing Table

The Statistics window provides information about the following:

- Tunnel details
- Routing table
- Personal firewall

Routing Table



Local LAN Routes

Network	Subnet Mask
10.10.32.32	255.255.255.255

Secured Routes

Network	Subnet Mask
0.0.0.0	0.0.0.0

- **The Statistics window provides information about tunnel details, routing table, and personal firewall.**

© 2006 Cisco Systems, Inc. All rights reserved.

To display the routing table, complete these steps:

Step 1 Choose **Status > Statistics.**

Step 2 Select the **Route Details** tab from the Statistics dialog box.

The routing table shows local LAN routes that do not traverse the IPsec tunnel, and secured routes that do traverse the IPsec tunnel to a central-site device. The routes in the local LAN routes column are for locally available resources.

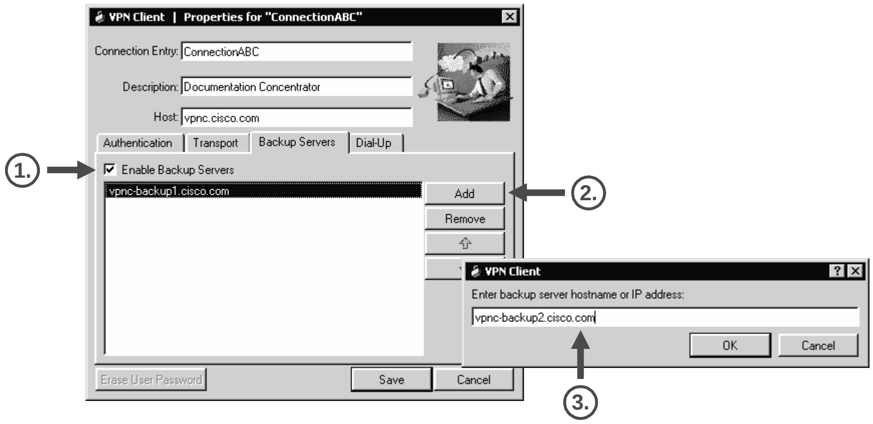
Note This feature works on only one NIC, the same NIC as the tunnel.

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

Task 5: Enable and Add Backup Servers

The private network may include one or more backup VPN servers to use if the primary server is not available. Your system administrator tells you whether to enable backup servers. Information on backup servers can download automatically from the VPN Concentrator, or you can manually enter this information.

Task 5: Enable and Add Backup Servers



Connection Entry: ConnectionABC

Description: Documentation Concentrator

Host: vpnc.cisco.com

☑ Enable Backup Servers

vpnc-backup1.cisco.com

Enter backup server hostname or IP address:

vpnc-backup2.cisco.com

- **List backup VPN servers to be used in case the primary VPN server is not reachable.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-13

To enable backup servers from the VPN Client, click the **Backup Servers** tab and complete these steps:

Step 1 Check the **Enable Backup Servers** check box. This box is not checked by default.

Step 2 Click **Add** to enter the backup server address.

Step 3 Enter the host name or IP address of the backup server, using a maximum of 255 characters.

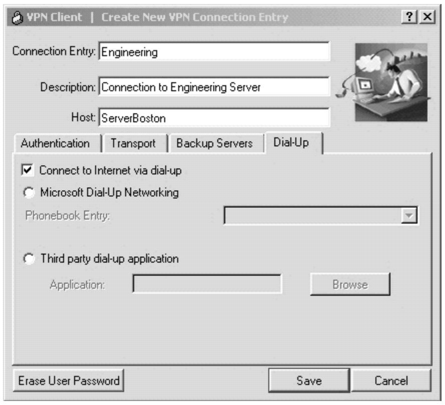
To add more backup devices, repeat these three steps.

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

Task 6: Configure Connection to the Internet Through Dial-Up Networking

The final task is configuring the dial-up connection to the Internet.

Task 6: Configure Connection to the Internet Through Dial-Up Networking


VPN Client | Create New VPN Connection Entry

Connection Entry: Engineering

Description: Connection to Engineering Server

Host: ServerBoston

☑ Connect to Internet via dial-up

○ Microsoft Dial-Up Networking

Phonebook Entry:

○ Third party dial-up application

Application:

- **Optionally, tie a VPN connection to a dial-up connection defined in the Networking section of Windows.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-14

To connect to a private network using a dial-up connection, complete these steps:

Step 1 Use a dial-up connection to your Internet service provider (ISP) to connect to the Internet.

Step 2 Use the VPN Client to connect to the private network through the Internet.

To enable and configure this feature, check the **Connect to Internet via dial-up** check box. This box is not checked by default.

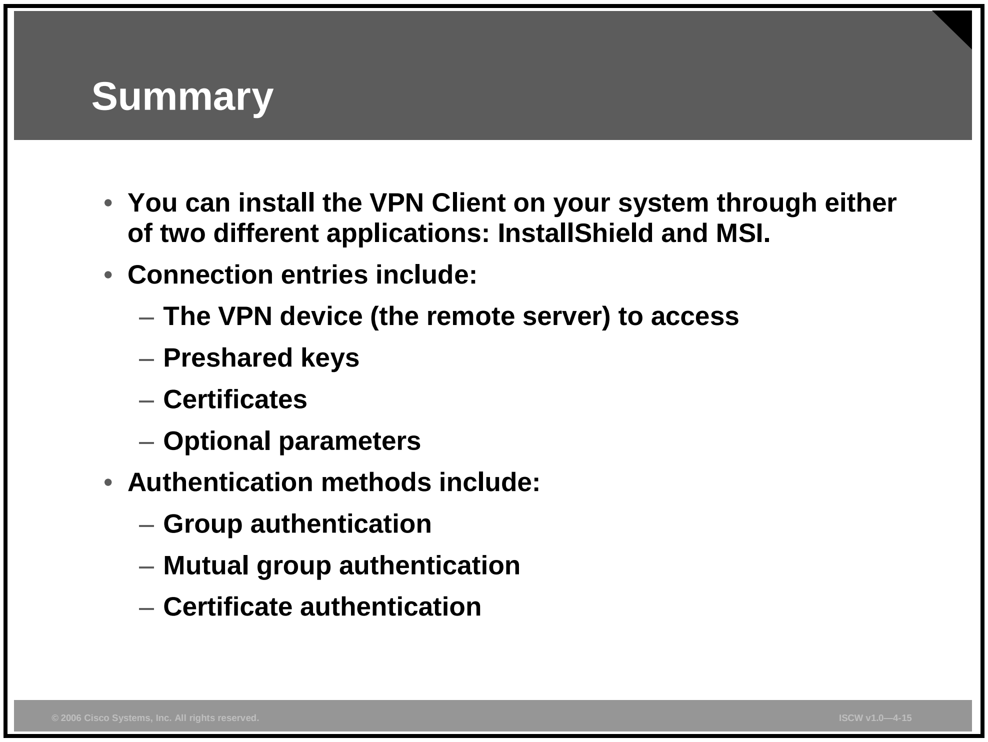
You can connect to the Internet using the VPN Client application in either of the following ways:

- Microsoft Dial-Up Networking
- Third-party dial-up application

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

Summary

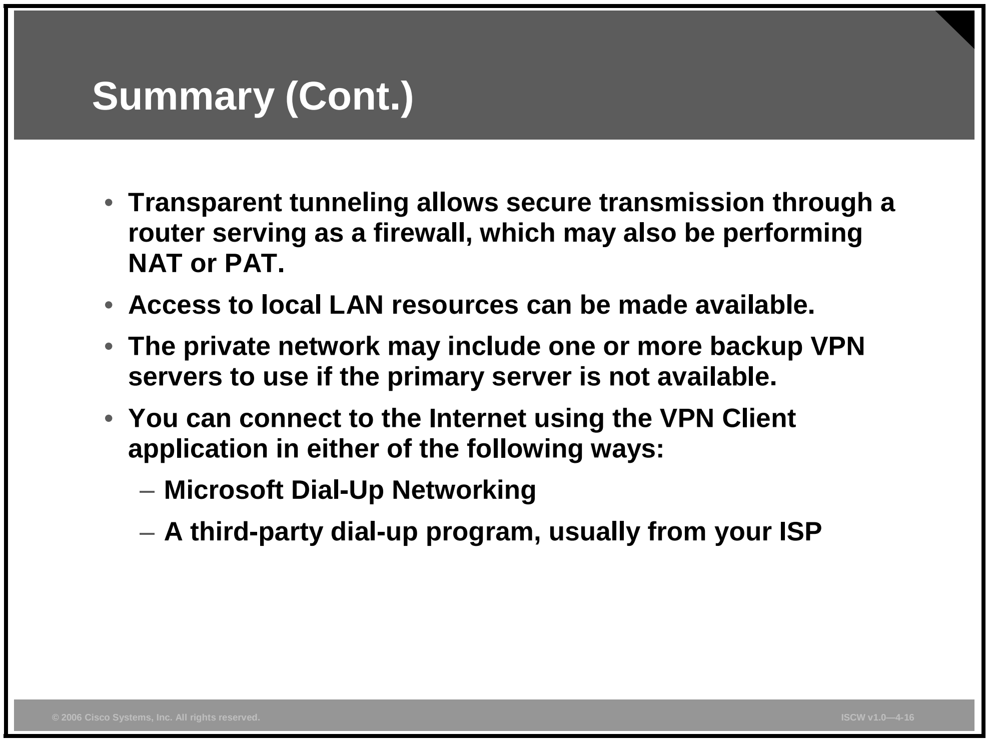
This topic summarizes the key points that were discussed in this lesson.



Summary

- You can install the VPN Client on your system through either of two different applications: InstallShield and MSI.
- Connection entries include:
  - The VPN device (the remote server) to access
  - Preshared keys
  - Certificates
  - Optional parameters
- Authentication methods include:
  - Group authentication
  - Mutual group authentication
  - Certificate authentication

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-15



Summary (Cont.)

- Transparent tunneling allows secure transmission through a router serving as a firewall, which may also be performing NAT or PAT.
- Access to local LAN resources can be made available.
- The private network may include one or more backup VPN servers to use if the primary server is not available.
- You can connect to the Internet using the VPN Client application in either of the following ways:
  - Microsoft Dial-Up Networking
  - A third-party dial-up program, usually from your ISP

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-16

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

References

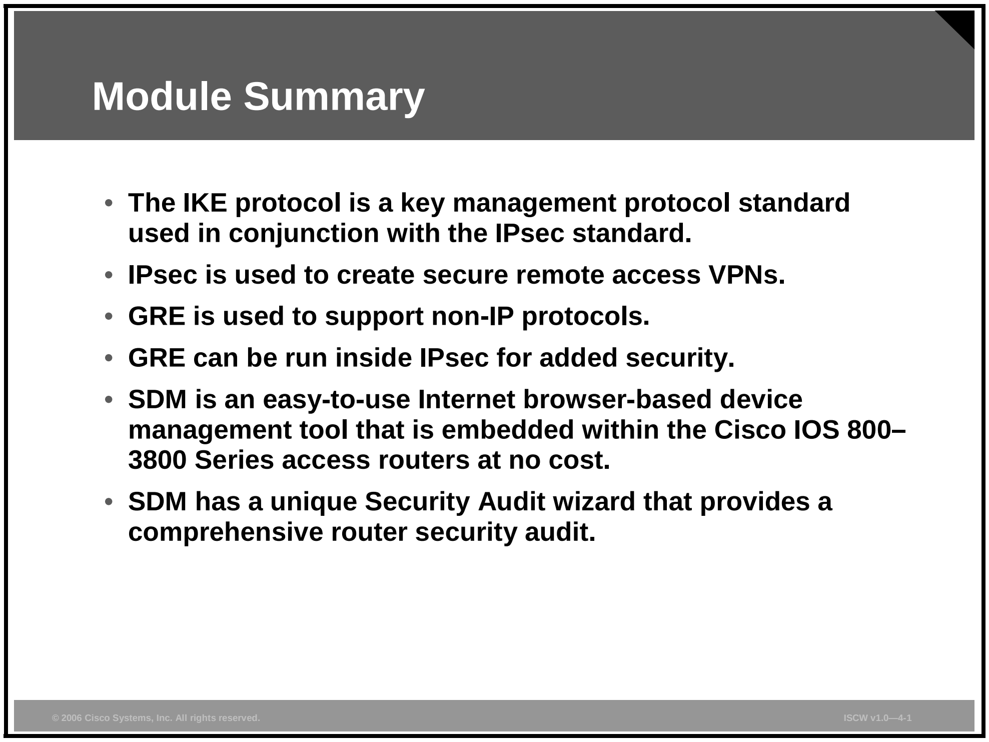
For additional information, refer to these resources:

- *VPN Client User Guide for Windows, Release 4.6* at: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/4_6/ugwin/

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

Module Summary

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

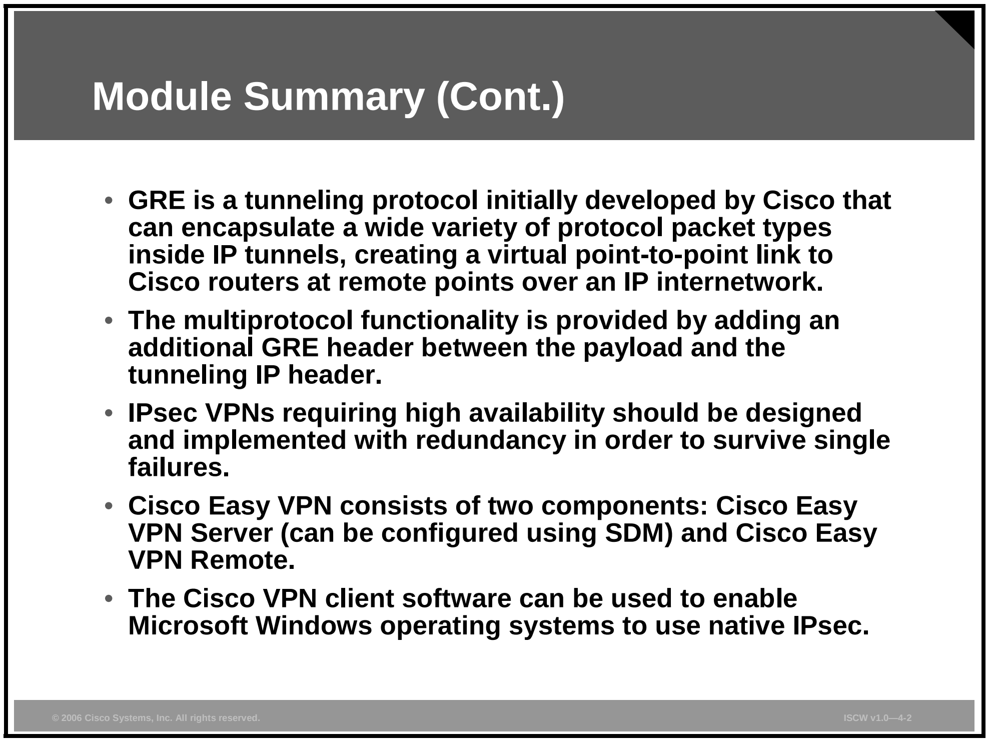


Module Summary

- The IKE protocol is a key management protocol standard used in conjunction with the IPsec standard.
- IPsec is used to create secure remote access VPNs.
- GRE is used to support non-IP protocols.
- GRE can be run inside IPsec for added security.
- SDM is an easy-to-use Internet browser-based device management tool that is embedded within the Cisco IOS 800–3800 Series access routers at no cost.
- SDM has a unique Security Audit wizard that provides a comprehensive router security audit.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-1



Module Summary (Cont.)

- GRE is a tunneling protocol initially developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.
- The multiprotocol functionality is provided by adding an additional GRE header between the payload and the tunneling IP header.
- IPsec VPNs requiring high availability should be designed and implemented with redundancy in order to survive single failures.
- Cisco Easy VPN consists of two components: Cisco Easy VPN Server (can be configured using SDM) and Cisco Easy VPN Remote.
- The Cisco VPN client software can be used to enable Microsoft Windows operating systems to use native IPsec.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—4-2

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

This module described the fundamental terms used with IPsec VPNs, and describes different types of IPsec VPNs and their configurations in detail. Generic Routing Encapsulation (GRE) tunnels and Cisco VPN Client for Windows are also introduced.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-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) At which OSI layer does IPsec operate? (Source: Understanding IPsec Components and IPsec VPN Features)

A) physical layer
B) data link layer
C) network layer
D) transport layer
E) session layer
F) presentation layer
G) application layer

Q2) Which IPsec mode adds a new IP header to the packet? (Source: Understanding IPsec Components and IPsec VPN Features)

A) aggressive mode
B) tunnel mode
C) transport mode
D) main mode
E) quick mode

Q3) The same SA is used for inbound and outbound traffic. (Source: Implementing Site-to-Site IPsec VPN Operations)

A) true
B) false

Q4) What kind of IKE proposals can be used when configuring IPsec site-to-site VPN using SDM? (Source: Configuring IPsec on a Site-to-Site VPN Using SDM)

A) only preconfigured
B) preconfigured or custom
C) only custom

Q5) What kind of IPsec transform sets can be used when configuring IPsec site-to-site VPN using SDM? (Source: Configuring IPsec on a Site-to-Site VPN Using SDM)

A) only preconfigured
B) preconfigured or custom
C) only custom

Q6) ACLs can be used to define which traffic needs protection. (Source: Configuring IPsec on a Site-to-Site VPN Using SDM)

A) true
B) false

Q7) Which security mechanism does GRE include to protect its payload? (Source: Configuring GRE Tunnels over IPsec)

A) IPsec
B) AH
C) ESP
D) none

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

Q8) Which mechanism does native IPsec use to detect failure of the remote peer? (Source: Configuring High-Availability Options)

A) DPD
B) HSRP
C) GLBP
D) VRRP

Q9) Which two components comprise Cisco Easy VPN? (Choose two.) (Source: Configuring Cisco Easy VPN and Easy VPN Server Using SDM)

A) Cisco Easy VPN Client
B) Cisco Easy VPN Server
C) Cisco Easy VPN Firewall
D) Cisco Easy VPN Remote
E) Cisco Easy VPN Local

Q10) Which three methods can be used for user authentication? (Choose three.) (Source: Implementing the Cisco VPN Client)

A) single-user authentication
B) group authentication
C) mutual group authentication
D) certificate 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 self-study.

Module Self-Check Answer Key

Q1)	C
Q2)	B
Q3)	B
Q4)	B
Q5)	B
Q6)	A
Q7)	D
Q8)	A
Q9)	B, D
Q10)	B, C, D

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