

AMVS

Advanced MPLS VPN Solutions

Volume 2

Version 1.0

Student Guide

Text Part Number: 97-0625-01

The products and specifications, configurations, and other technical information regarding the products in this manual are subject to change without notice. All statements, technical information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. You must take full responsibility for their application of any products specified in this manual.

LICENSE

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE MANUAL, DOCUMENTATION, AND/OR SOFTWARE (“MATERIALS”). BY USING THE MATERIALS YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE, PROMPTLY RETURN THE UNUSED MATERIALS (WITH PROOF OF PAYMENT) TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Cisco Systems, Inc. (“Cisco”) and its suppliers grant to you (“You”) a nonexclusive and nontransferable license to use the Cisco Materials solely for Your own personal use. If the Materials include Cisco software (“Software”), Cisco grants to You a nonexclusive and nontransferable license to use the Software in object code form solely on a single central processing unit owned or leased by You or otherwise embedded in equipment provided by Cisco. You may make one (1) archival copy of the Software provided You affix to such copy all copyright, confidentiality, and proprietary notices that appear on the original. EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, YOU SHALL NOT: COPY, IN WHOLE OR IN PART, MATERIALS; MODIFY THE SOFTWARE; REVERSE COMPILER OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE MATERIALS.

You agree that aspects of the licensed Materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Cisco. You agree not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Cisco. You agree to implement reasonable security measures to protect such trade secrets and copyrighted Material. Title to the Materials shall remain solely with Cisco.

This License is effective until terminated. You may terminate this License at any time by destroying all copies of the Materials. This License will terminate immediately without notice from Cisco if You fail to comply with any provision of this License. Upon termination, You must destroy all copies of the Materials.

Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. You agree to comply strictly with all such regulations and acknowledge that it has the responsibility to obtain licenses to export, re-export, or import Software.

This License shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the Materials

Restricted Rights - Cisco’s software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions as set forth in subparagraph “C” of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the U.S. Government’s rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202.

DISCLAIMER OF WARRANTY. ALL MATERIALS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Cisco’s or its suppliers’ liability to You, whether in contract, tort (including negligence), or otherwise, exceed the price paid by You. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of

the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the TN3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

Cisco incorporates Fastmac and TrueView software and the RingRunner chip in some Token Ring products. Fastmac software is licensed to Cisco by Madge Networks Limited, and the RingRunner chip is licensed to Cisco by Madge NV. Fastmac, RingRunner, and TrueView are trademarks and in some jurisdictions registered trademarks of Madge Networks Limited. Copyright © 1995, Madge Networks Limited. All rights reserved.

XRemote is a trademark of Network Computing Devices, Inc. Copyright © 1989, Network Computing Devices, Inc., Mountain View, California. NCD makes no representations about the suitability of this software for any purpose.

The X Window System is a trademark of the X Consortium, Cambridge, Massachusetts. All rights reserved.

Access Registrar, AccessPath, Any to Any, Are You Ready, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, IQ Breakthrough, IQ Expertise, IQ FastTrack, IQ Readiness Scorecard, The IQ Logo, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, The Cell, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0005R)

Advanced MPLS VPN Solutions, Revision 1.0: Student Guide

Copyright © 2000, Cisco Systems, Inc.

All rights reserved. Printed in USA.

Table of Contents

Volume 1

ADVANCED MPLS VPN SOLUTIONS	1-1
Overview	1-1
Course Objectives	1-2
Course Objectives – Implementation	1-3
Course Objectives – Solutions	1-4
Prerequisites	1-5
Participant Role	1-7
General Administration	1-9
Sources of Information	1-10
MPLS VPN TECHNOLOGY	2-1
Overview	2-1
Objectives	2-1
Introduction to Virtual Private Networks	2-2
Objectives	2-2
Summary	2-8
Review Questions	2-8
Overlay and Peer-to-Peer VPN	2-9
Objectives	2-9
Overlay VPN Implementations	2-13
Summary	2-23
Review Questions	2-24
Major VPN Topologies	2-25
Objectives	2-25
VPN Categorizations	2-25
Summary	2-38
Review Questions	2-38
MPLS VPN Architecture	2-39
Objectives	2-39
Summary	2-60
Review Questions	2-61
MPLS VPN Routing Model	2-62
Objectives	2-62
Summary	2-78
Review Questions	2-78
MPLS VPN Packet Forwarding	2-79
Objectives	2-79
Summary	2-91
Review Questions	2-91
Lesson Summary	2-92
Answers to Review Questions	2-93
Introduction to Virtual Private Networks	2-93
Overlay and Peer-to-Peer VPN	2-93

Major VPN Topologies	2-94
MPLS VPN Architecture	2-94
MPLS VPN Routing Model	2-95
MPLS VPN Packet Forwarding	2-96

MPLS/VPN CONFIGURATION ON IOS PLATFORMS **3-1**

Overview	3-1
Objectives	3-1
MPLS/VPN Mechanisms in Cisco IOS	3-2
Objectives	3-2
Summary	3-16
Review Questions	3-16
Configuring Virtual Routing and Forwarding Table	3-17
Objectives	3-17
Summary	3-26
Review Questions	3-26
Configuring a Multi-Protocol BGP Session Between the PE Routers	3-27
Objectives	3-27
Summary	3-43
Review Questions	3-43
Configuring Routing Protocols Between PE and CE Routers	3-44
Objectives	3-44
Summary	3-55
Review Questions	3-55
Monitoring MPLS/VPN Operation	3-56
Objectives	3-56
Summary	3-82
Review Questions	3-82
Troubleshooting MPLS/VPN	3-83
Objectives	3-83
Summary	3-100
Review Questions	3-100
Advanced VRF Import/Export Features	3-101
Objectives	3-101
Summary	3-115
Review Questions	3-115
Advanced PE-CE BGP Configuration	3-116
Objectives	3-116
Summary	3-134
Review Questions	3-134

USING OSPF IN AN MPLS VPN ENVIRONMENT **4-1**

Overview	4-1
Objectives	4-1
Using OSPF as the PE-CE Protocol in an MPLS VPN Environment	4-2
Objectives	4-2
Summary	4-26
Review Questions	4-26
Configuring and Monitoring OSPF in an MPLS VPN Environment	4-27
Objectives	4-27
Summary	4-35
Review Questions	4-35

Summary	4-36
Answers to Review Questions	4-37
Using OSPF as the PE-CE Protocol in an MPLS VPN Environment	4-37
Configuring and Monitoring OSPF in an MPLS VPN Environment	4-37

Volume 2

MPLS VPN TOPOLOGIES	5-1
Overview	5-1
Objectives	5-1
Simple VPN with Optimal Intra-VPN Routing	5-2
Objectives	5-2
Summary	5-17
Review Questions	5-17
Using BGP as the PE-CE Routing Protocol	5-18
Objectives	5-18
Summary	5-23
Review Questions	5-23
Overlapping Virtual Private Networks	5-24
Objectives	5-24
Summary	5-33
Review Questions	5-33
Central Services VPN Solutions	5-34
Objectives	5-34
Summary	5-47
Review Questions	5-47
Hub-andSpoke VPN Solutions	5-48
Objectives	5-48
Summary	5-54
Review Questions	5-54
Managed CE-Router Service	5-55
Objectives	5-55
Summary	5-60
Review Questions	5-60
Chapter Summary	5-60
INTERNET ACCESS FROM A VPN	6-1
Overview	6-1
Objectives	6-1
Integrating Internet Access with the MPLS VPN Solution	6-2
Objectives	6-2
Summary	6-16
Review Questions	6-16
Design Options for Integrating Internet Access with MPLS VPN	6-17
Objectives	6-17
Summary	6-23
Review Questions	6-23
Leaking Between VPN and Global Backbone Routing	6-24
Objectives	6-24
Usability of Packet Leaking for Various Internet Access Services	6-32
Redundant Internet Access with Packet Leaking	6-36
Summary	6-38
Review Questions	6-38

Separating Internet Access from VPN Service	6-39
Objectives	6-39
Usability of Separated Internet Access for Various Internet Access Services	6-44
Summary	6-46
Review Questions	6-46
Internet Access Backbone as a Separate VPN	6-47
Objectives	6-47
Usability of Internet in a VPN Solution for Various Internet Access Services	6-52
Summary	6-56
Review Questions	6-57
Chapter Summary	6-57

MPLS VPN DESIGN GUIDELINES **7-1**

Overview	7-1
Objectives	7-1
Backbone and PE-CE Link Addressing Scheme	7-2
Objectives	7-2
Summary	7-15
Review Questions	7-16
Backbone IGP Selection and Design	7-17
Objectives	7-17
Summary	7-30
Review Questions	7-31
Route Distinguisher and Route Target Allocation Schemes	7-32
Objective	7-32
Summary	7-37
Review Questions	7-37
End-to-End Convergence Issues	7-38
Objectives	7-38
Summary	7-52
Review Questions	7-52
Chapter Summary	7-53
Answers to Review Questions	7-54
Backbone and PE-CE Link Addressing Scheme	7-54
Backbone IGP Selection and Design	7-55
Route Distinguisher and Route Target Allocation Scheme	7-56
End-to-End Convergence Issues	7-56

LARGE-SCALE MPLS VPN DEPLOYMENT **8-1**

Overview	8-1
Objectives	8-1
MP-BGP Scalability Mechanisms	8-2
Objectives	8-2
Summary	8-12
Review Questions	8-12
Partitioned Route Reflectors	8-13
Objectives	8-13
Summary	8-28
Review Questions	8-28
Chapter Summary	8-29

MPLS VPN MIGRATION STRATEGIES **9-1**

Overview	9-1
Objective	9-1
Infrastructure Migration	9-2
Objective	9-2
Summary	9-9
Review Questions	9-9
Customer Migration to MPLS VPN service	9-10
Objective	9-10
Generic Customer Migration Strategy	9-11
Migration From Layer-2 Overlay VPN	9-13
Migration from GRE Tunnel-Based VPN	9-16
Migration from IPSec-Based VPN	9-19
Migration from L2F-Based VPN	9-20
Migration From Unsupported PE-CE Routing Protocol	9-22
Summary	9-26
Review Questions	9-26
Chapter Summary	9-26

INTRODUCTION TO LABORATORY EXERCISES **A-1**

Overview	A-1
Physical And Logical Connectivity	A-2
IP Addressing Scheme	A-5
Initial BGP Design	A-7
Notes Pages	A-8

LABORATORY EXERCISES—FRAME-MODE MPLS CONFIGURATION **B-1**

Overview	B-1
Laboratory Exercise B-1: Basic MPLS Setup	B-2
Objectives	B-2
Command list	B-2
Task 1: Configure MPLS in your backbone	B-2
Task 2: Remove BGP from your P-routers	B-2
Verification:	B-3
Review Questions	B-4
Laboratory Exercise B-2: Disabling TTL Propagation	B-5
Objective	B-5
Command list	B-5
Task: Disable IP TTL Propagation	B-5
Verification	B-5
Laboratory Exercise B-3: Conditional Label Advertising	B-6
Objective	B-6
Command list	B-6
Task: Configure Conditional Label Advertising	B-6
Verification	B-6
Review Questions	B-7

LABORATORY EXERCISES—MPLS VPN IMPLEMENTATION **C-1**

Overview	C-1
Laboratory Exercise C-1: Initial MPLS VPN Setup	C-2
Objectives	C-2
Background Information	C-2
Command list	C-3
Task 1: Configure multi-protocol BGP	C-3
Task 2: Configure Virtual Routing and Forwarding Tables	C-4
Additional Objective	C-5
Task 3: Configuring Additional CE routers	C-5
Verification	C-6
Laboratory Exercise C-2: Running OSPF Between PE and CE Routers	C-9
Objectives	C-9
Visual Objective	C-9
Command list	C-10
Task 1: Configure OSPF on CE routers	C-10
Task 2: Configure OSPF on PE routers	C-10
Verification	C-11
Task 3: Configure OSPF connectivity with additional CE routers	C-11
Verification	C-12
Laboratory Exercise C-3: Running BGP Between the PE and CE Routers	C-13
Objectives	C-13
Background Information	C-13
Command list	C-14
Task 1: Configure Additional PE-CE link	C-14
Task 2: Configure BGP as the PE-CE routing protocol	C-14
Verification	C-15
Task 3: Select Primary and Backup Link with BGP	C-16
Verification:	C-16
Task 4: Convergence Time Optimization	C-17
Verification	C-17

LABORATORY EXERCISES—MPLS VPN TOPOLOGIES **D-1**

Overview	D-1
Laboratory Exercise D-1: Overlapping VPN Topology	D-2
Objective	D-2
Visual Objective	D-2
Command list	D-3
Task 1: Design your VPN solution	D-4
Task 2: Remove WGxA1/WGxB1 from existing VRFs	D-4
Task 3: Configure new VRFs for WGxA1 and WGxB1	D-4
Verification:	D-4
Laboratory Exercise D-2: Common Services VPN	D-8
Objective	D-8
Background Information	D-9
Command list	D-10
Task 1: Design your Network Management VPN	D-10
Task 2: Create Network Management VRF	D-10
Verification	D-11
Task 3: Establish connectivity between NMS VRF and other VRFs	D-11
Verification	D-11
Task 4: Establish routing between WGxPE2 and the NMS router	D-12

Verification	D-13
Laboratory Exercise D-3: Internet Connectivity Through Route Leaking	D-14
Objective	D-14
Visual Objective	D-14
Command list	D-15
Task 1: Cleanup from the previous VPN exercises	D-15
Task 2: Configure route leaking between customer VPN and the Internet	D-15
Verification	D-16
Additional exercise: Fix intra-VPN routing	D-17
Laboratory Exercise D-4: Separate Interface for Internet Connectivity	D-18
Objective	D-18
Visual Objective	D-19
Command list	D-20
Task 1: Cleanup from the previous exercise	D-20
Verification	D-21
Task 2: Establishing connectivity in the global routing table	D-21
Task 3: Routing between the PE-router and the CE-router	D-21
Verification	D-22
Laboratory Exercise D-5: Internet in a VPN	D-23
Objective	D-23
Visual Objective	D-23
Command list	D-24
Task 1: Design your Internet VPN	D-24
Task 2: Migrate Internet routers in a VPN	D-24
Verification	D-25
Additional Task: Direct Internet connectivity for all CE-routers	D-26
Verification	D-26

INITIAL LABORATORY CONFIGURATION E-1

Overview	E-1
Laboratory Exercise E-1: Initial Core Router Configuration	E-2
Objective	E-2
Task: Configure Initial Router Configuration	E-2
Verification	E-3
Laboratory Exercise E-2: Initial Customer Router Configuration	E-4
Objective	E-4
Task: Configure Customer Routers	E-4
Verification	E-5
Laboratory Exercise E-3: Basic ISP Setup	E-6
Objective	E-6
Task 1: Configure IS-IS in your backbone	E-6
Task 2: Configure BGP in your backbone	E-6
Task 3: Configure Customer Routing	E-6
Task 4: Peering with other Service Providers	E-7
Task 5: Establishing Network Management Connectivity	E-7
Verification	E-7

INITIAL ROUTER CONFIGURATION F-1

Overview	F-1
Router WGxPE1	F-2
Router WGxPE2	F-4

Router WGxPE3	F-6
Router WGxPE4	F-8
Router WGxP	F-10
Router WGxA1	F-12
Router WGxA2	F-14
Router WGxB1	F-15
Router WGxB2	F-17

MPLS VPN Topologies

Overview

This chapter describes the most commonly used MPLS VPN topologies and the design and implementation issues associated with them.

It includes the following topics:

- Simple VPN with optimal Intra-VPN routing
- Using BGP as the PE-CE routing protocol
- Overlapping Virtual Private Networks
- Central Services VPN solutions
- Hub-and-Spoke VPN solutions
- Managed CE Router Service

Objectives

Upon completion of this chapter, you will be able to perform the following tasks:

- Design and implement simple VPN solutions with optimal intra-VPN routing
- Design and implement various routing protocols within VPNs
- Design and implement central services VPN topologies
- Design and implement hub-and-spoke VPN topologies
- Design and implement VPN topology required for managed router services

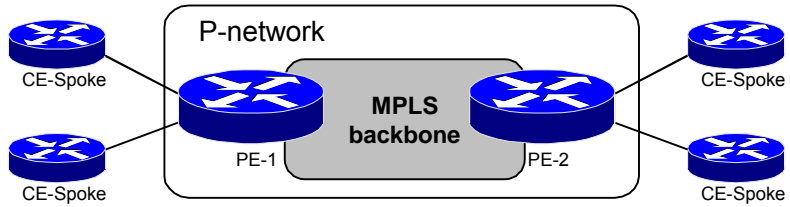
Simple VPN with Optimal Intra-VPN Routing

Objectives

Upon completion of this section, you will be able to perform the following tasks:

- Describe the requirements of simple VPN solutions
- Describe the routing model of these solutions
- Describe the optimal intra-VPN routing data flow
- Select the optimal PE-CE routing protocol based on user requirements
- Integrate the selected PE-CE routing protocol with the MPLS VPN backbone MP-BGP routing

Simple VPN Requirements Summary



- Any site router can talk to any other site
- Optimum routing across P-network is desired

© 2000, Cisco Systems, Inc.

www.cisco.com

Chapter 1-5

In contrast with other VPN technologies, MPLS VPN supports optimum any-to-any connectivity between customer sites (equivalent to the full mesh of overlay VPN networks) without the end customer having to manually configure anything. The provider only needs to configure the VPN in the Provider Edge (PE) routers. The so-called “hub-and-spoke” topology, which was primarily used to reduce the cost of the network, is no longer needed. The interconnection of CE sites is done automatically by using BGP and an IGP to find the shortest path.

Simple VPN Routing and Data Flow

- **Each site needs to reach every other site in the same VPN**
 - **Each VRF belonging to simple VPN contains all VPN routes**
 - **The sites use default route or have full routing knowledge of all other sites of same VPN**
- **Data flow is optimal in the backbone**
 - **Routing between PE routers is done based on MP-BGP Next-Hop closest to the destination**
- **No site is used as central point for connectivity**

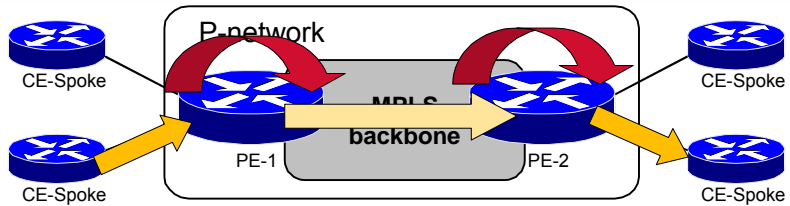
© 2000, Cisco Systems, Inc.

www.cisco.com

Chapter 1-6

MPLS VPN architecture by default provides optimal routing between CE sites. A CE site can have full internal routing for its VPN or just a default route pointing to the PE router. The PE routers, however, need to have full routing information for the MPLS VPN network in order to provide connectivity and optimal routing. A MP-BGP next-hop address is used to find a label for a VPN destination network and the backbone IGP provides the optimal routing towards the next-hop address.

Simple VPN - Routing Information Propagation



- CE routers announce the customer routes to the PE routes
- Customer routes are redistributed into MP-BGP
- VPNv4 routes are propagated across P-network with the BGP next-hop of the ingress PE router (PE-1)
- VPNv4 routes are inserted into target VRF based on route-target and redistributed back into the customer routing protocol
- Customer routes are propagated to other CE routers

© 2000, Cisco Systems, Inc.

www.cisco.com

Chapter 1-7

When a Customer Edge (CE) router announces a network through an IGP, the PE router will redistribute and export it into Multiprotocol BGP, converting an IPv4 address into a VPNv4 address. The following list contains the most significant changes that happen with redistribution and export:

- IPv4 Network Layer Reachability Information (NLRI) is converted into VPNv4 NLRI by pre-pending a route distinguisher (for example, a route distinguisher 12:13 could be prepended to an IPv4 prefix 10.0.0.0/8 resulting in a VPNv4 prefix 12:13:10:10.0.0.0/8)

Note NLRI is a BGP term for a prefix (address and subnet mask)

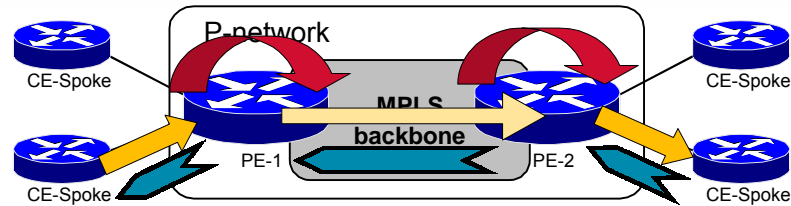
- VPNv4 NLRI also contains a label that will be used to identify the outgoing interface or the VRF where a routing lookup should be performed
- A *route target* extended community is added based on the VRF configuration

The PE router will forward VPN_IPv4 networks to all other PE routers that will use the route target community to identify the VRFs where this information has to be imported. The received VPN label will be used as the second label and the BGP next-hop label (learned via LDP) will be used as the top label for packets going to CE routers connected to distant PE routers.

The PE router will then redistribute the VPN_IPv4 network into the IGP used between the PE and the CE and send it to the CE router.

The MPLS VPN core network is not visible to the CE routers. The BGP part of the routing information propagation is only seen as slower convergence.

Simple VPN Data Flow



- Ingress CE forwards the data packet based on route received from PE-2 and propagates the packet toward PE-2
- PE-2 forwards the data packet based on the MP-BGP route with PE-1 as the BGP next-hop. Data flow with the P-network is optimal
- PE-1 forwards the data packet based on route received from egress CE router

© 2000, Cisco Systems, Inc.

www.cisco.com

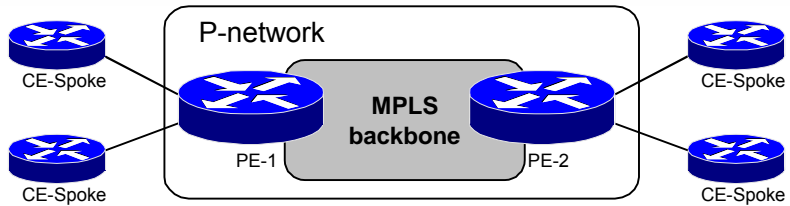
Chapter 1-8

In the slide above, the CE router finds the destination in its IP routing table (learned through IGP or based on a static default route). PE-2 has learned about the destination through MP-BGP and labels each packet from the CE router with the VPN label (second label) and the next-hop label (top label).

The core routers are doing label switching based on the top label. The last core router before PE-1 will pop the top label (penultimate hop popping). PE-1 will identify the outgoing interface or the VRF by looking at the second label, which at this time is the top and only label. The packet sent to the CE is no longer labeled.

Note Please refer to **MPLS VPN Technology** lesson for more information on MPLS VPN packet forwarding.

Simple VPN – Basic Design Rules



- **Configure only one VRF per PE router**
- **Configure the same Route Distinguisher on all VRFs**
- **Configure one import/export route target**

© 2000, Cisco Systems, Inc.

www.cisco.com

Chapter 1-9

To optimize performance, reduce configuration efforts and conserve memory on the PE router on which you should minimize the number of VRFs per router.

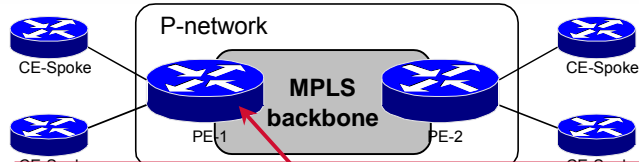
Using one VRF per VPN per PE router will reduce memory requirements and CPU load. This is possible because the routing requirements for all CE routers in the same VPN are the same. Using one VRF per VPN can also improve convergence between CE routers connected to the same PE router.

Using the same route distinguisher for VRFs that are used for the same VPN will also conserve memory.

Only one route target is needed for a simple VPN. Any additional route targets are unnecessary and will consume at least 64 bits per routing update.

Using the same route distinguisher and route target for a simple VPN helps to ease the management, monitoring, and troubleshooting of the MPLS VPN network.

Simple VPN – VRF Configuration



```
ip vrf VPN_A
 rd 213:750
 route-target both 213:750
 !
interface Serial0/0
 ip vrf forwarding VPN_A
 ip address 192.168.250.6 255.255.255.252
 !
interface Serial0/2
 ip vrf forwarding VPN_A
 ip address 192.168.250.10 255.255.255.252
```

© 2000, Cisco Systems, Inc.

www.cisco.com

Chapter 1-10

In the example above, we have two interfaces in the same VRF. We are using the same numbering scheme for route distinguishers and route targets.

Note There is no routing configuration in this example. This example only shows how to create a virtual router (VRF – virtual routing and forwarding instance) and to assign interfaces to it.
