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 COMPILE 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.

Advanced MPLS VPN Solutions, Revision 1.0: Student Guide

Table of Contents

Volume 1

Volume 2

5

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:

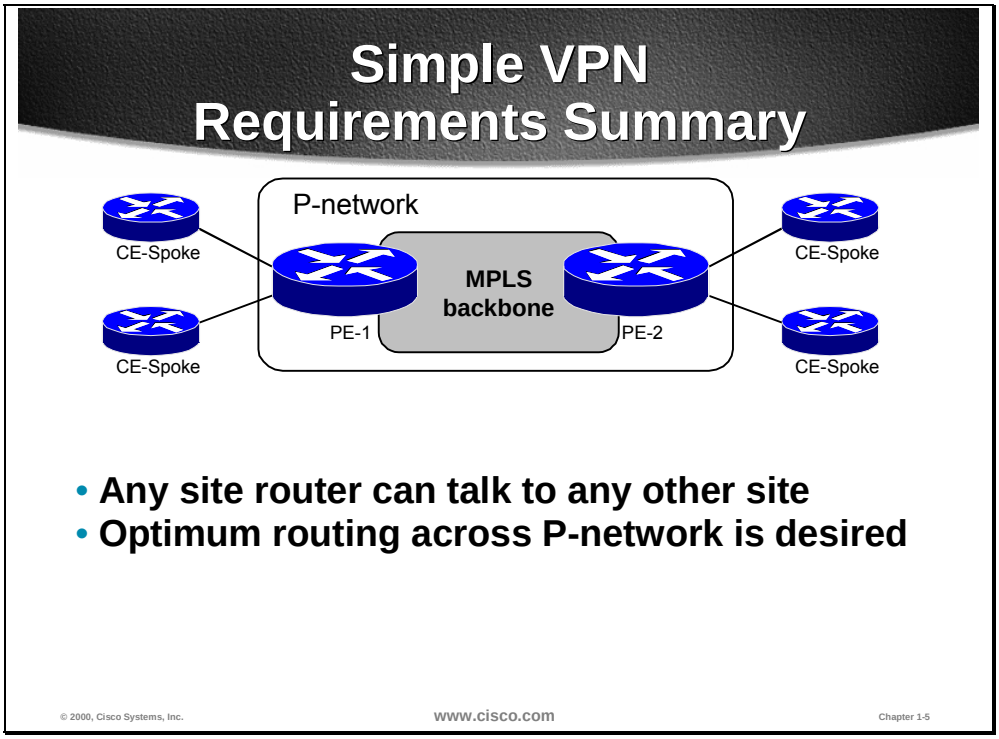
- Design and implement simple VPN solutions with optimal intra-VPN routing
- Design and implement various routing protocols within VPNs
- Design and implement central services VPN topologies
- Design and implement hub-and-spoke VPN topologies
- Design and implement VPN topology required for managed router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

Simple VPN with Optimal Intra-VPN Routing

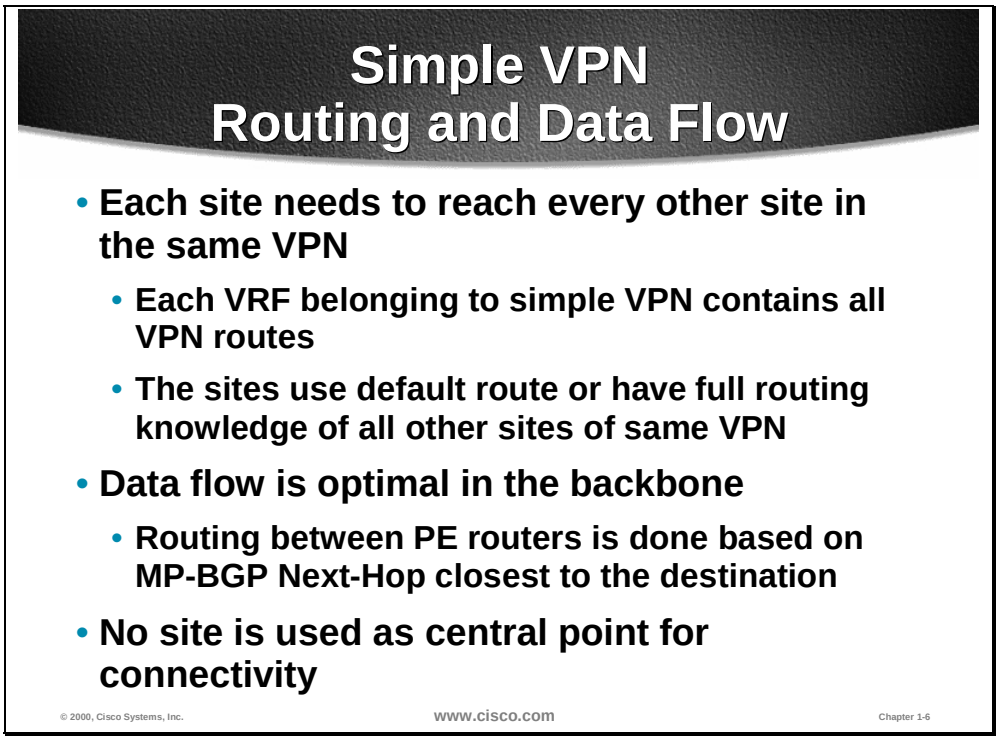
Objectives

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

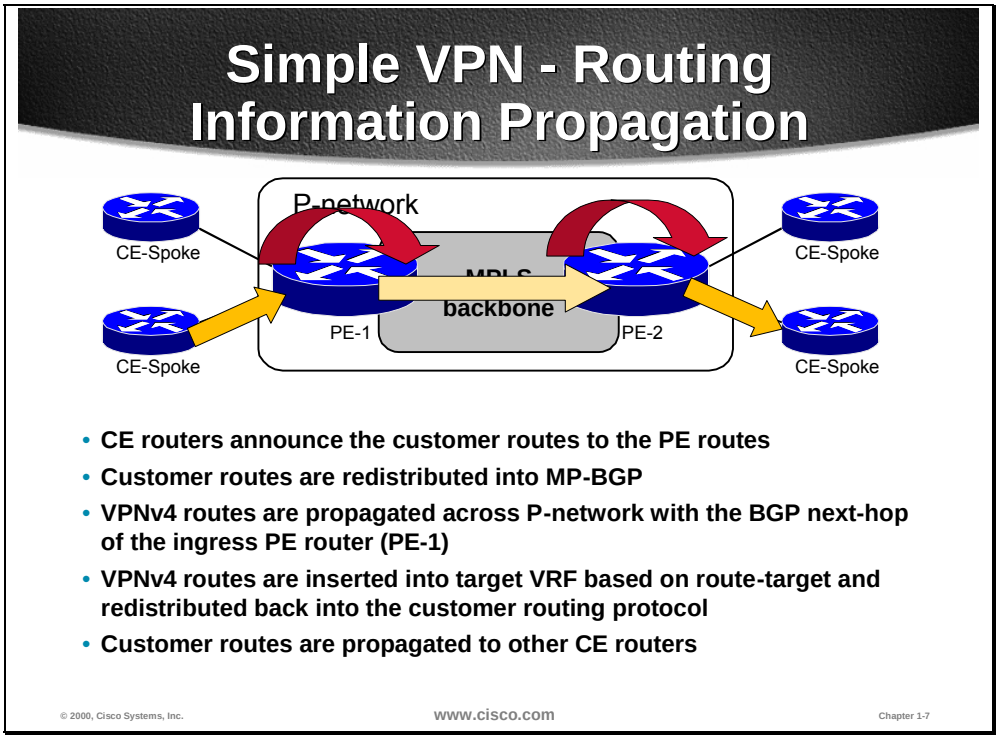
- Describe the requirements of simple VPN solutions
- Describe the routing model of these solutions
- Describe the optimal intra-VPN routing data flow
- Select the optimal PE-CE routing protocol based on user requirements
- Integrate the selected PE-CE routing protocol with the MPLS VPN backbone MP-BGP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



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.



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.



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)

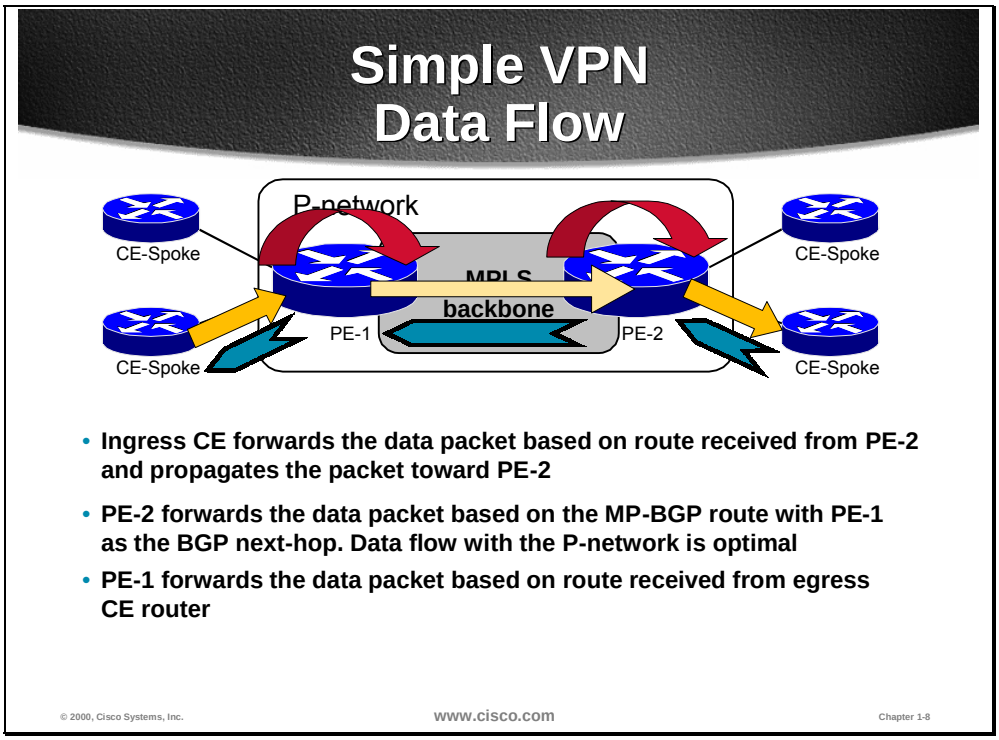
Note NLRI is a BGP term for a prefix (address and subnet mask)

- 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.

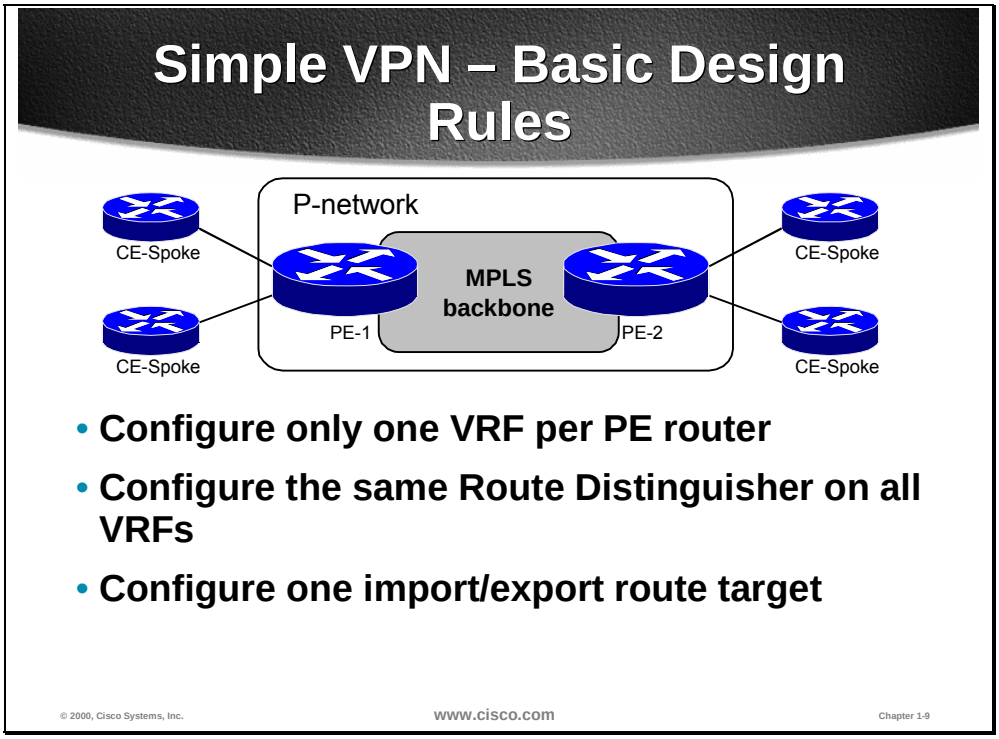
The MPLS VPN core network is not visible to the CE routers. The BGP part of the routing information propagation is only seen as slower convergence.



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.



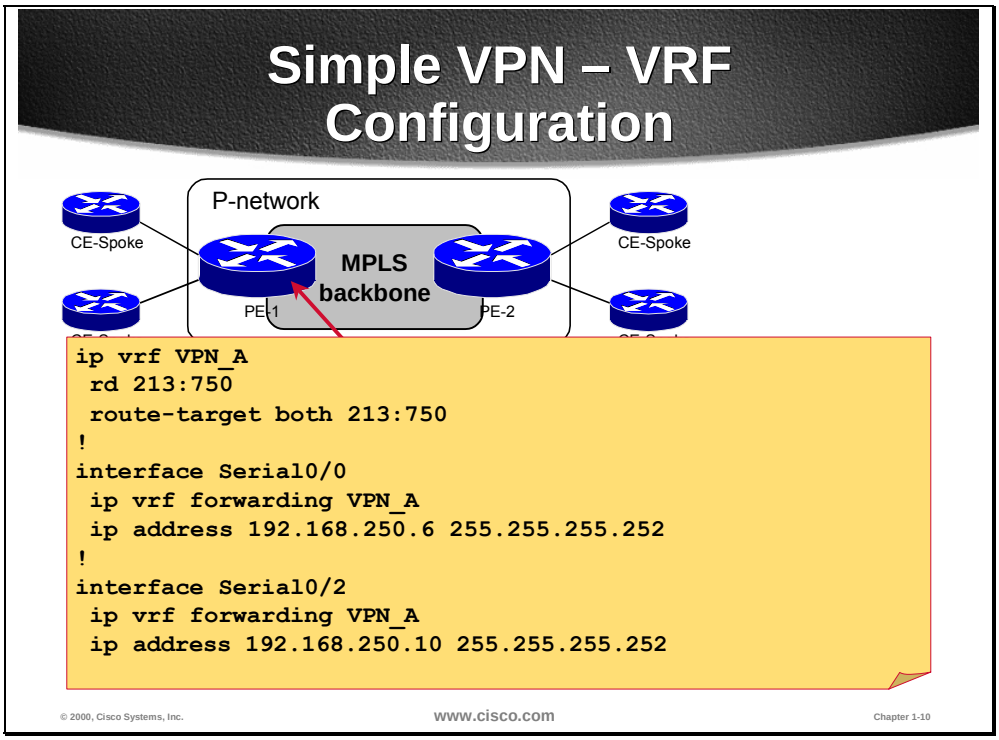
To optimize performance, reduce configuration efforts and conserve memory on the PE router on which you should minimize the number of VRFs per router.

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.



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.

