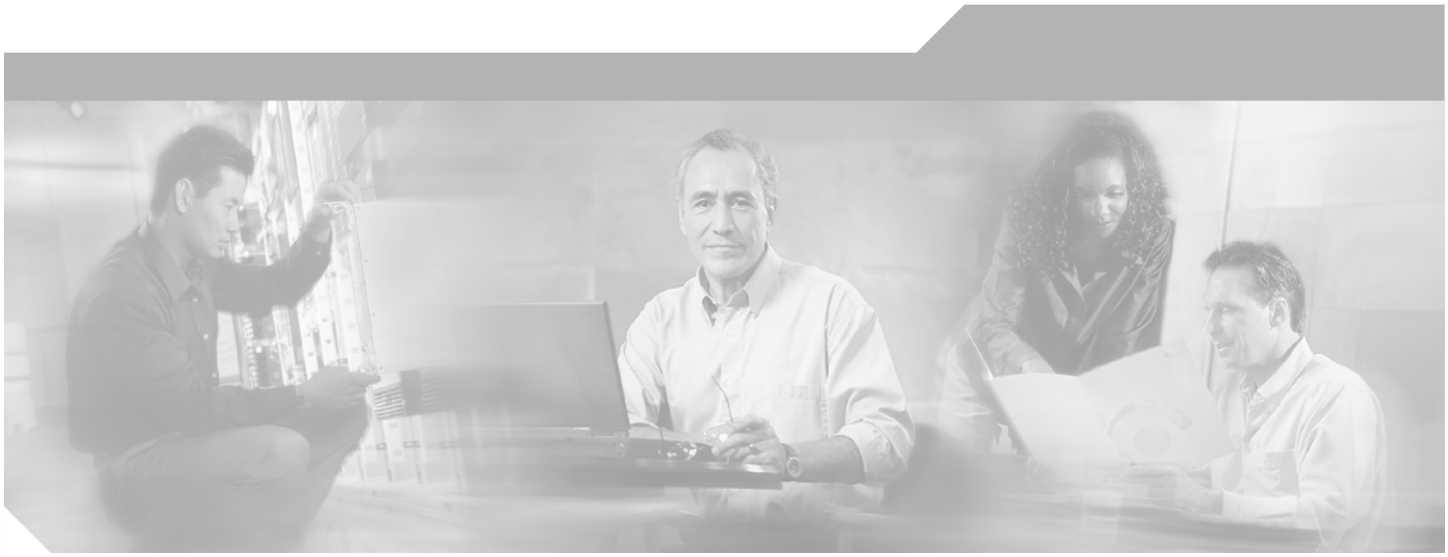


Cisco Remote Access to MPLS VPN Integration 2.0 Overview and Provisioning Guide

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

Customer Order Number:
Text Part Number: OL-2512-03

CONTENTS

Preface

This guide provides overview and provisioning information for a remote access to MPLS VPN integration solution. This preface has the following main subjects:

Document Objectives

This guide covers the three remote access to MPLS VPN network architectures: dial, DSL, and cable. The guide references features described in the Cisco IOS configuration guides and command references. Consult those documents for additional information.

Audience

This guide is meant for new and existing MPLS VPN service providers. It includes overview and configuration information designed to enable users to get their systems running as quickly as possible. However, it does not include extensive software configuration instructions. For more extensive software configuration information, refer to the Cisco IOS configuration guides and command references. See also the documents listed under Related Documentation, page xiii, and For More Information, page xvi.

This guide is intended primarily for the following audiences:

- Customers with technical networking background and experience
- Customers who support remote access users
- System administrators who are familiar with the fundamentals of router-based internetworking, but who may not be familiar with Cisco IOS software
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software

Document Organization

This document describes software installation and configuration procedures which are presented in the following chapters and appendices:

- This preface provides a summary of Remote Access to MPLS VPN Integration document objectives, organization and conventions, related documentation, and how to obtain documentation a technical assistance.
- Chapter 1, "Solution Overview," provides a brief description of the remote access solution at large, and a list of the integrated access technology methods covered.
- Chapter 2, "Overview of Dial Access to MPLS VPN Integration," describes each of the dial access methods and their required components.
- Chapter 3, "Provisioning Dial Access to MPLS VPN Integration," describes procedures for provisioning the various dial access methods and the associated applications.
- Chapter 4, "DSL Access to MPLS VPN Integration," provides both overview and provisioning information for remote access using DSL.
- Chapter 5, "Cable Access to MPLS VPN Integration," provides both overview and provisioning information for remote access using cable.
- Chapter 6, "AAA Radius Access to MPLS VPN Integration," describes Radius AAA requirements for Remote Access to MPLS VPN Integration.

Document Conventions

This publication uses the following conventions to display instructions and information.

Interactive examples showing prompts (`AS5800(config-line)#`) are used in procedures to show exactly what the prompt should look like when you enter a command, and what happens after you enter a command. Examples showing sample output from a **show running-config** or **show startup-config** (without prompts) command are included in the configuration sections.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the action described saves time*. You can save time by performing the action described in the paragraph.

Tip Means the following information will help you solve a problem.

Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, may harm you. A warning symbol precedes each warning statement. To see translations of safety warnings pertaining to the Cisco AS5850, refer to the *Regulatory Compliance and Safety Information* document that shipped with your system.

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that aCisco.commpanied this device.**

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document Regulatory Compliance and Safety Information (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).

Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui aCisco.commpagne cet appareil.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, oCisco.comrre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che aCisco.commpagna questo dispositivo.

Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.

¡Advertencia! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.

Related Documentation

The Cisco Remote Access to MPLS VPN Integration 2.0 Documentation Set

In addition to this guide, the Cisco Remote Access to MPLS VPN Integration 2.0 documentation set includes:

- *Troubleshooting Cisco Remote Access to MPLS VPN Integration 2.0*
  http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/rampls2/trblsht/index.htm
- *Cisco Remote Access to MPLS VPN Integration 2.0 Release Notes*
  http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/rampls2/relnote/index.htm

Reference Documentation

The following platform specific hardware component reference documentation is available on Cisco.com or Cisco's Universal CD.

MPLS VPNSC References

The following Cisco MPLS VPN Solution Center reference documentation is available on Cisco.com or Cisco's Universal Documentation CD.

MPLS VPN Solution Center Documentation

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/index.htm

Network Management References

The following Cisco network management reference documentation is available on Cisco.com or Cisco's Universal Documentation CD.

Cisco Access Registrar

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

Cisco DSL Manager

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cdm/index.htm

Cisco Network Registrar

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnr/index.htm

Cisco 6400 Service Connection Manager

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/scm/index.htm

Cisco IP Manager

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ip_mgr/index.htm

NetFlow FlowAnalyzer (see Network Data Analyzer)
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfa/index.htm

NetFlow FlowCollector
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfc/index.htm

DSL Routers

Cisco 600 Series CPE Products
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c600s/index.htm

Cisco 600 Series Installation and Operation Guide
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c600s/600inop/index.htm

Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis1700/confgnts/confnt.htm

Access Servers

Cisco Access Servers and Access Routers
http://www.cisco.com/univercd/cc/td/doc/product/access/index.htm

Dial Solutions Quick Configuration Guide
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/dsqcg3/index.htm

AS5300
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm

AS5800
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/index.htm

Aggregation/Home Gateway/PE Routers

Cisco 6400 Universal Access Concentrator
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/index.htm

Cisco 7200 Series Routers
http://www.cisco.com/univercd/cc/td/doc/product/core/index.htm

Cisco 7500 Series Routers
http://www.cisco.com/univercd/cc/td/doc/product/core/index.htm

IOS for Cisco DSLAMs with NI-2
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/ios_dsl/index.htm

ViewRunner Management Software
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/vrmgtsw/index.htm

Cisco IOS

The following Cisco IOS reference documentation is available on Cisco.com or Cisco's Universal Documentation CD.

Cisco IOS Software Configuration

http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm

Cisco SSG IOS on the NRP

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/relnote/6400uac/rn120dc7.htm

MPLS VPN Overviews and Configurations

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt4/index.htm

Internetworking Technology Overviews

The following internetworking technology reference documentation is available on Cisco.com or Cisco's Universal Documentation CD.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm

Virtual Private Networks (VPNs) Overview

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm

Digital Subscriber Line Technology

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/adsl.htm

Access VPDN Dial-in Using L2TP

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/l2tp/index.htm

Access VPN Solutions Using Tunneling Technology

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/vpn_soln/index.htm

Tag Switching (Labeling)

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/tagswtch.htm

Cisco Secure VPN Client Solutions Guide

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/index.htm

Introduction to WAN Technologies

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm

Internetwork Troubleshooting Guides

http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm

Internetworking Terms and Acronyms

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

For More Information

For information on MPLS, use the following resources:

- MPLS Resource Center (http://www.mplsrc.com/)
- *MPLS: Technologies and Applications* by Bruce S. Davie and Yakov Rekhter
- *Switching in IP Networks: IP Switching, Tag Switching, and Related Technologies* by Bruce S. Davie, Paul Dooley, and Yakov Rekhter
- *CSM Brochure,* Literature Number 953088
- *New World Operations Advertorial,* Literature Number 952807
- *CSM Advertorial,* Literature Number 952937
- *CSM Demo CD-ROM,* Literature Number 952319

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Solution Overview

This section provides component overviews and a technological perspective of a remote access to Multiprotocol Label Switching (MPLS) virtual private network (VPN) end-to-end solution, implemented over a shared infrastructure.

Introduction

Using MPLS VPN technology, a service provider can create scalable and efficient VPNs across the core of its network for each customer. This solution integrates various access VPN services with MPLS VPN in the service provider's core. This permits the service provider to offer bundled end-to-end VPN service to their ISP customers and enterprise customers.

Remote access technologies in the remote access to MPLS VPN solution include dial, DSL (digital subscriber line), cable, and wireless.

Methods of Dial access covered in this integration solution include:

- L2TP Dial-In
- Direct ISDN PE Dial-In
- Dial Backup
- L2TP Dial-Out
- Direct ISDN PE Dial-Out

Methods of DSL access covered in this integration solution include:

- RFC 1483 Routing Integration, page 4-2
- RFC 1483 Routed Bridge Encapsulation to MPLS VPN Integration, page 4-8
- PPPoX Remote Access SSG to MPLS VPN Integration, page 4-19
- PPPoX Remote Access to MPLS VPN Integration, page 4-30
- DSL L2TP to MPLS VPN Integration, page 4-40

Methods of cable access covered in this integration solution include:

- Cable DOCSIS 1.0 SID to MPLS VPN Integration, page 5-1

Note SSG is an example of a provider service function applied to a session.

Technology Overviews

This chapter includes an overview of the basic core MPLS technology:

Overviews of access technologies are covered in their own sections or chapters:

The Cisco IOS Command Line Interface (CLI) overview is summarized in the following section:

MPLS Summary

Multiprotocol Label Switching (MPLS) is an emerging IETF protocol standard, pioneered by Cisco as tag switching between layer 2 and 3. The key element of MPLS is that packet/cell forwarding is performed using labels, or label values, instead of IP header information, regardless of the network type. When troubleshooting MPLS, network packet forwarding uses labels, hop by hop, so you must look to the label tables for routing information. Labels are assigned a particular destination at the ingress, or entry point, of the MPLS network. They are placed on top of or in front of the IP packet. Each router along the path will forward the “tagged” or MPLS packets based on label value, not IP information.

Refer to the Cisco IOS documentation suite for conceptual MPLS overview and configuration details at http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt4/index.htm

IP Forwarding

IP forwarding is a hop by hop routing process where every node, or router, in the network, has to maintain packet destination information in local routing tables. Each router has to have a routing entry for any given IP packet destination, or the packet gets dropped.

With IP forwarding, the following process takes place:

1. A routing protocol (e.g. OSPF, IS-IS, BGP) establishes reachability to destination networks.

   Note Transit providers do not do default routing. They need a full routing table in every core router, full BGP mesh, route reflectors or confederations.

2. An ingress router receives a packet, and performs a lookup in the IP forwarding table at each hop.
3. The packet is delivered to destination.

IP Forwarding is performed based on the longest prefix match of the destination address. A longest match, or a default route, should be present in the forwarding table

MPLS Forwarding

IP forwarding is a hop by hop routing process where every node, or router, in the network, has to maintain packet destination information in local routing tables. Each router has to have a routing entry for any given IP packet destination, or the packet gets dropped.

With MPLS forwarding, the following process takes place:

1. Existing routing protocols (e.g. OSPF, IS-IS) establish reachability to destination networks.
2. Label Distribution Protocol (LDP) establishes tag to destination network mappings.
3. Ingress label edge router receives packet, performs layer 3 value-added services, and "label" packets.
4. Label switches, switch tagged packets, using label swapping.
5. Label edge router, at egress, removes the tag, and delivers the packet.

MPLS VPN Summary

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) is an IP network infrastructure delivering private network services over a public infrastructure using a layer 3 backbone which:

- is scalable for easy provisioning
- provides controlled access and QoS
- is easily configurable for customers
- includes global as well as non-unique private address space
- supports large scale VPN services
- increases value add by the VPN Service Provider
- decreases service provider cost of providing VPN services
- enables VPN Service Provider with mechanisms general enough to support a wide range of VPN customers (see RFC2547)

Refer to the Cisco IOS documentation for conceptual MPLS VPN overview and configuration details at http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt4/index.htm

Cisco MPLS VPN Solution Center Summary

Cisco Virtual Private Network (VPN) Solutions Center offers Multiprotocol Label Switching (MPLS) VPN service providers a customized service and network layers FCAPS (fault, configuration management, accounting, performance, security) management solution facilitating rapid service deployment. It provides a carrier-grade network and service management solution integrated with CSM applications and consisting of functional modules developed to support:

- **Provisioning:** A provisioning module supports scheduled VPN service provisioning. The provisioning module translates simple order entry information to complex Cisco IOSÆ commands. An auditing system ensures the integrity of networks.
- **Accounting:** An accounting module collects usage data and generates reports.
- **Service Level Monitoring (SLA):** An SLA module that monitors specific SLAs and generates performance reports to validate whether SLAs are met.

- **Application Programming Interface (API):** APIs supports application integration and Operations Support System (OSS) integration.
- **Graphical User Interface (GUI):** A user-friendly interface supports various management functions.
- **Billing:** Cisco VPNSC integrates with third-party applications to provide usage-based billing to support VPN services.
- **Fault Management:** Cisco VPNSC integrates with third-party applications to provide service-level fault management functions. Element-and-network-level alarms and events are correlated with service-level information to generate VPN aware messages.
- **Performance Management:** Cisco VPNSC integrates with third-party applications to provide service-level-performance management functions. Sophisticated VPN performance reports are generated.

Note For more information on the VPN Solution Center features and benefits, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Cisco VPN Solutions Center is integrated with third-party applications to provide planning, security, and other management functions for the following benefits:

- **Improved Time-to-Market:** Cisco VPNSC automates provisioning. MPLS VPN Services can be turned on in hours instead of days or weeks.
- **Improved Network Quality:** Cisco VPNSC allows service providers to minimize configuration errors by automating the error-prone manual provisioning process. The auditing function provides a secondary validation level before activating services.
- **Reduced Operation Costs:** Cisco VPNSC automates labor-intensive network and service management processes.
- **Reduced Ownership Costs:** No need to develop MPLS VPN custom management services. Use Cisco VPNSC as a stand-alone or integrated solution. Cisco VPNSC supports evolving MPLS VPN technology that includes new hardware and software releases.

Cisco VPN SC Installation

During installation, the install script checks for VPNSC required solaris patches and prompts you to install them if they are not in place. Ensure these patches are installed before using the install script again. These patches can be downloaded from the sun site.

The install script also prompts you for Orbix software and requires the name and path of the browser. It also prompts you for the e-mail address for mailing watchdog alerts. Use the default port of 7500 for the TIBCO Rendezvous.

Cisco MPLS VPN SC Initialization

Every VPN created by VPNSC is created and deleted using a Service Request that has a request ID.

Before creating a Service Request:

1. Define network elements (Targets)

   Targets are any device to be managed by the VPNSC. Typically these will be of type Cisco router, whether CE or PE.

   a. Import the router (target) configuration files from a directory:

      VPNConsole > Setup > Create Targets from Router Configurations

   b. Specify the directory containing configurations, the network name (a container for targets), and a domain name (optional).

   c. Complete the target definitions by adding description and password information in the Network window.

      This operation can be performed for individual targets, or multiple targets can be updated simultaneously. Targets can be added or deleted from the Networks window.

2. Define provider admin domain

   The PAD is made up of all the “Regions” managed by VPN SC. To define a PAD,

   a. Specify a BGP autonomous region number, the PE routers with each region, and the IP address pools for numbered and unnumbered links.

      VPN Console > Setup > New Provider Administrative Domain

3. Create VPN customer definition.

   a. Specify customer information, customer sites, and associated CE devices to define a VPN customer.

      VPNConsole > Setup > New VPN Customer

   b. Specify name and contact information in the VPN Customer window.

   c. Title each site and “Add” CE devices in the Customer Site window.

4. Define the VPN.

   a. Select a VPN name and topology to define a VPN. Typically, the VPN named is relative to the customer.

      VPNConsole > Setup > New VPN Definition

   b. CERC tab creation of a hub-and-spoke or full mesh topology.

Cisco MPLS VPN SC Provisioning

To provision using the Cisco MPLS VPN SC you create and deploy service requests.

VPNSC is task schedule oriented. These tasks are saved and can be reused. Task examples are:

- Deploying all service requests
- Deploying all new service requests
- Auditing existing service requests for configuration and routing information
- Collecting configuration files from devices
- Collecting netflow information from a netflow collector
- Creating SLA probes on routers

Creating Service Requests

To create a service request, perform the following:

1. Initialize the VPN Solution Center PAD, Region, IP address pool, PEs, Customer, Sites, CEs, VPNs, and CE routing communities.
2. Create a PE to CE Service Request.
3. Add the VPN Service Wizard to define the service.
   a. Choose a CE
   b. Choose a PE
   c. Define the VPN membership of the CE
   d. Choose the routing protocol between PE-CE
   e. Select a protocol if redistributed on this link
   f. Choose the PE and CE interfaces
   g. Enter layer 2 information (i.e. DLCI)
   h. Choose an addressing scheme
   i. Select a CoS profile if required
   j. Verify the service information
4. Configure routing protocols.

   Static between PE and CE

   a. Specify subnets on PE to reach CE addresses
   b. Specify subnets on CE to reach other Customer Sites
   c. Optional - Default routing on CE to other Sites

   RIP between PE and CE

   a. Optional - Specify default route from PE to CE
   b. Redistribute routing protocols from Customer into VPN

   BGP between PE and CE

   a. Specify BGP AS on CE
   b. Redistribute routing protocols from Customer into VPN

c. Redistribute connected option

OSPF

a. OSPF Process ID

b. OSPF Area Number

Redistributed Connected and Static by Default from VRF into VPN

5. Exporting configlets.
   a. Configlets can be saved as text files

      Provision > Export SR configlets

   b. Review configlets prior to deployment as verification

Deploying Service Requests

Defined service requests are queued and wait in the "Requested" state. Requested SRs can be deployed in batches, or individually, by a scheduled task, or immediately.

- To immediately deploy a single SR, select:
  a. **Provisioning > List all Service Requests**
  b. Select an SR from list and deploy
- To schedule or deploy many SRs, select:
  a. **Provisioning > Deploy Service Requests**
- View Task Logs to verify task completion.
- Deployment steps are:
  a. Upload PE Configuration (read from network)
  b. Upload CE Configuration
  c. Create MPLS/VPN Configlet based on uploaded configuration
  d. Download CE configuration (write to network)
  e. Download PE configuration
  f. Upload PE Configuration (read from network)
  g. Upload CE Configuration
  h. After Deployment List all Service Requests - requests in "Pending State" if not audited upon deployment

Equipment and Software Selection

The following Cisco remote access to MPLS VPN Integration solution hardware elements are supported. Refer to the "Reference Documentation" section on page xiii for platform specific documentation URLs, IOS configuration URLs, MPLS VPNSC reference URLs, and technology overview URLs.

- NAS Platforms
  - Cisco AS5300
  - Cisco AS5800
  - Cisco AS5850
  - Cisco 3660 & 3640 (LAC)
- Virtual Home Gateway (VHG) Provider Edge (PE) Routers:
  - Cisco 7200
  - Cisco 7500
  - Cisco 6400 (LNS)
  - Cisco uBR7200
  - Cisco MGX 8850 with route-processor module (RPM-PR)
- DSL Equipment
  - Cisco 827
  - Cisco 6130
  - Cisco 6xx (DSL Modem)
  - Cisco 7500 for DSL routed-bridge encapsulation remote access
  - Cisco MGX 8850 with route-processor module (RPM-PR) for DSL routed-bridge encapsulation remote access
- Cable Subscriber Equipment
  - Cisco uBR924
- Access Networks: LAN, ATM
- Core Network
  - IP MPLS network
  - ATM MPLS network
- Radius Server: Access Register Release 1.5
- Management Platforms: RPMS

The following Cisco remote access to MPLS VPN Integration solution software elements are supported.

- VPNSC 2.1
- Netflow Collector 3.0
- RPMS 1.0
- SCM 1.2
- CIC 2.0
- IOS Feature: Overlapping IP address Pools
- CNR 3.5

- CSRC 1.0(2)

Cisco IOS Software Fundamentals

Cisco MPLS VPN access provider, service provider, and customer CPE, CE, PE, concentrator, access server, aggregation, gateway, and headend hardware components use Cisco IOS software. Cisco IOS software provides the capability to configure Cisco routers and switches using command-line interface (CLI) commands.

Keep in mind the following when configuring your Cisco IOS software:

- Use the question mark (?) and arrow keys to help enter commands.
- Each command mode restricts you to a set of commands.
- Enter the keyword **no** before a command to disable a feature; for example, **no ip routing**.
- Save configuration changes to NVRAM so they are not lost in a system reload or power outage.
- Use the forward slash (/) command syntax to identify interface and port locations (*slot/port*). The slot identification number is the first number identified in the command syntax.

Note Cisco IOS software is feature specific and licensed on an "as is" basis without warranty of any kind, either expressed or implied. The version of Cisco IOS software used in this guide varies depending on configuration requisites for presentation purposes, and should not be construed as the Cisco IOS software version of choice for your system or internetwork environment. Consult your Cisco sales representative regarding your Cisco IOS requirements.

User Interface Command Modes

Cisco routers/servers are configured from user interfaces, known as ports, which provide hardware connectivity. They are accessed from the console port on a router or Telnet into a router interface from another host. Typical interfaces are Serial 0 (S0), Serial 1 (S1), and Ethernet (E0). Token Ring interfaces are referenced as (T0) and FDDI interfaces use (F0).

Command Modes

When using the CLI, a command interpreter, called EXEC, is employed by the operating system to translate any command and execute its operation. This command interpreter has two access modes, user and privileged, which provide security to the respective command levels. Each command mode restricts you to a subset of mode-specific commands.

User mode provides restricted access and limits router configuration or troubleshooting. At this level, miscellaneous functionality is performed, such as viewing system information, obtaining basic router status, changing terminal settings, or establishing remote device connectivity.

Privileged mode includes user mode functionality and provides unrestricted access. It is used exclusively for router configuration, debugging, setting operating system (OS) parameters, and retrieving detailed router status information.

There are many modes of configuration within privileged mode that determine the type of configuration desired, such as interface configuration (`AS5800(config-if)#`), line configuration (`AS5800(config-line)#`), and controller configuration (`AS5800(config-controller)#`). Each configuration command mode restricts you to a subset of mode specific commands.

In the following command sequence, command prompts are automatically modified to reflect command mode changes. A manual carriage return is implied at the end of each line item.

```
AS5800> enable
AS5800# configure terminal
AS5800(config)# interface ethernet 0/0
AS5800(config-if)# line 0/0
AS5800(config-line)# controller e1 0/0
AS5800(config-controller)# exit
AS5800(config)# exit
AS5800#
%SYS-5-CONFIG_I: Configured from console by console
AS5800#
```

The last message is an example of a system response. Press **Enter** to get the `AS5800#` prompt.

Table 1-1lists common configuration modes. Configure global parameters in global configuration mode, interface parameters in interface configuration mode, and line parameters in line configuration mode.

Table 1-1 Common Command Modes

Command Mode	Prompt	Access Method	Escape Method
User EXEC	`AS5800>`	Log in.	Use the **exit** or **logout** command to leave the command line interface.
Privileged EXEC	`AS5800#`	From user EXEC mode, enter the **enable** command.	Use the **disable** command to escape back to user EXEC mode. Use the **exit** or **logout** command to leave the command line interface.
Global configuration	`AS5800(config)#`	From privileged EXEC mode, enter the **configure terminal** command.	Use the **exit** or **end** (Ctrl-Z) command to escape to privileged EXEC mode.
Interface configuration	`AS5800(config-if)#`	Enter the **interface** type and number command, such as **interface ethernet 0/0/0**.	Use the **exit** command to escape to global configuration mode. Use the **end** (Ctrl-Z) command to escape directly to privileged EXEC mode.
Line configuration	`AS5800(config-line)#`	Enter the **line** start-number end-number command, such as **line 0/0/1 0/0/48**.	Use the **exit** command to escape to global configuration mode. Use the **end** (Ctrl-Z) command to escape directly to privileged EXEC mode.
Controller configuration	`AS5800(config-control)#`	Enter the **controller** name and number command, such as **controller t1 0/0/0**.	Use the **exit** command to escape to global configuration mode. Use the **end** (Ctrl-Z) command to escape directly to privileged EXEC mode.

Context-Sensitive Help

Context-sensitive help is available at any command prompt. Enter a question mark (?) for a list of complete command names, semantics, and command mode command syntax. Use arrow keys at command prompts to scroll through previous mode-specific commands for display.

Note Cycle through mode specific commands at a mode specific prompt.

- For a list of available commands, enter a question mark.

```
AS5800> ?
```

- To complete a command, enter known characters followed by a question mark (no space).

```
AS5800> s?
```

- For a list of command variables, enter the command followed by a space and a question mark.

```
AS5800> show ?
```

Refer to the chapter "Configuring the User Interface" in the *Configuration Fundamentals Configuration Guide* for more information about working with the user interface in the Cisco IOS software.

Note You can press **Ctrl-Z** in any mode to immediately return to enable mode (AS5800#), instead of entering **exit**, which returns you to the previous mode.

Saving Configurations

To prevent losing the Cisco AS5800 configuration, save it to NVRAM using the following steps:

Step 1 Enter the **enable** command and password. You are in privileged EXEC mode when the prompt changes to AS5800#.

```
AS5800> enable
Password: password
AS5800#
```

Note Press **Ctrl-Z** to return to privileged EXEC mode. Any subsequent system response message is normal and does not indicate an error.

Step 2 Execute the **copy running-config startup-config** command to save configuration changes to nonvolatile random-access memory (NVRAM) so configuration data will not be lost during a system reload, power cycle or outage.

```
AS5800# copy running-config startup-config
Building configuration...
```

The following message and prompt appears after a successful configuration copy.

```
[OK]
AS5800#
```

Undoing a Command

To undo a command or disable a feature, enter the keyword **no** before the command; for example, **no ip routing**.

Passwords

Several passwords are used when configuring your Cisco IOS software. Passwords are used to identify user authorization and permission rights, virtual terminal configuration, and network management software initialization. Most passwords can use the same notation.

You need the following types of passwords when configuring Cisco IOS software:

- Enable password—A nonencrypted and, therefore, less secure password.
- Enable secret password—A very secure, encrypted password that is used in place of the enable password. Because many privileged-level EXEC commands are used to set operating parameters, we recommend that you use the enable secret password to prevent unauthorized use.

Note The enable password and enable secret password should be different. In both cases, you cannot use a number cannot be the first character. Spaces are also valid password characters, but only when following valid characters; lead spaces are ignored.

- Virtual console password—A password that enables terminal emulation.

CHAPTER 2

Overview of Dial Access to MPLS VPN Integration

This chapter gives a brief overview of Cisco dial access to Multiprotocol Label Switching (MPLS) virtual private network (VPN) integration. It also offers overviews of each of the methods of dial access. It covers the following subjects:

- Overview of Dial Access, page 2-1
- Dial-in access methods:
  - Overview of L2TP Dial-in Remote Access, page 2-2
  - Overview of Direct ISDN PE Dial-in Remote Access, page 2-5
  - Overview of Dial Backup, page 2-7
- Dial-out access methods:
  - Overview of Dial-out Access, page 2-9, describing both L2TP dial-out access and direct ISDN PE dial-out access

Each section provides:

- An overview of the topology
- A description of the associated components and features

The chapter also describes:

- Common Components and Features, page 2-11
- Optional features that can be used with dial access:
  - Multilink PPP, page 2-18
  - Multichassis Multilink PPP, page 2-18

Procedures for provisioning dial access are described in Chapter 3, "Provisioning Dial Access to MPLS VPN Integration".

Overview of Dial Access

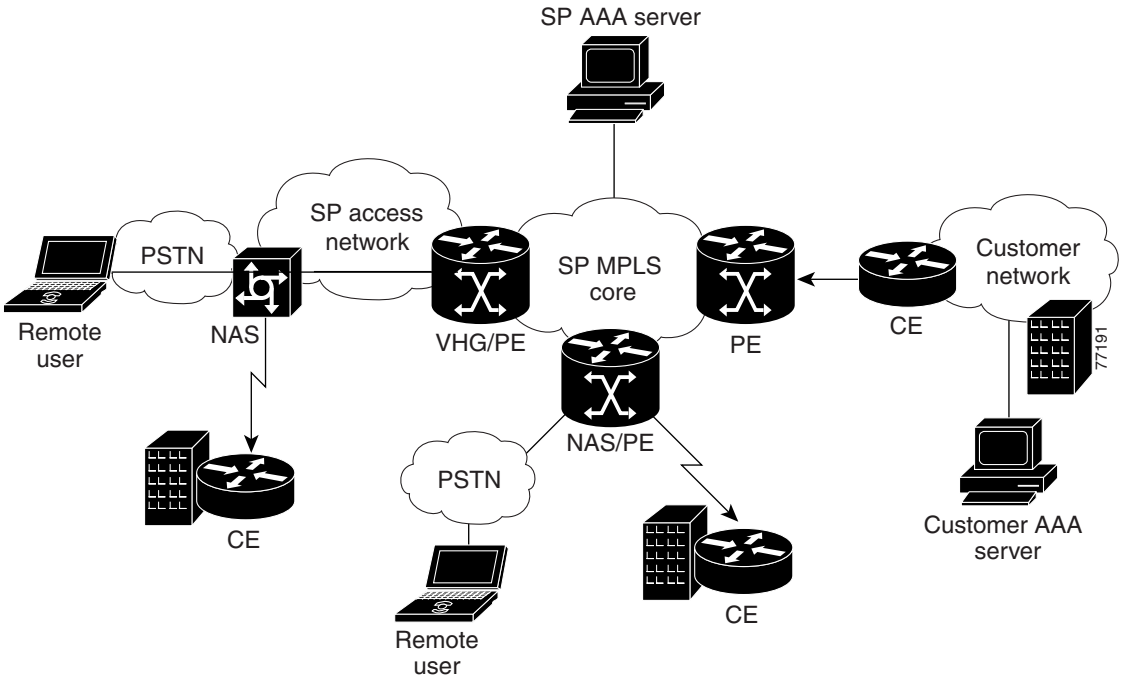
With MPLS VPN, a service provider can create scalable, efficient, and feature-rich customer VPNs across the core of a network. Adding remote dial access integration provides the remote customer edge router (CE) to provider edge router (PE) link that integrates dial users into their MPLS VPNs.

Cisco remote dial access integration covers the following scenarios:

- Individuals dialing in over ISDN or the analog public switched telephone network (PSTN) to a PE from their laptop computers, or users at a remote office dialing in to a PE through a CE. This is dial-in access.
- A CE dialing in to a PE, creating a backup link for use when a primary, direct remote connection, such as cable or digital subscriber line (DSL), has failed. This is dial backup access.
- A PE dialing out to a remote CE, with the call triggered by traffic coming from the MPLS VPN. For example, a central database system might connect to vending machines at night to collect daily sales data and check inventories. This is dial-out access.

Figure 2-1 shows a service provider network with several kinds of remote dial access. In this example, the customer is outsourcing all remote access operations to the service provider, but the service provider operates an MPLS VPN that interconnects all customer sites.

Figure 2-1 Overview of Remote Dial Access to MPLS VPN



Note Cisco remote access to MPLS VPN integration is based on the assumption that the MPLS core network is in place and the PE-to-PE and PE-to-provider core router links are configured.

Overview of L2TP Dial-in Remote Access

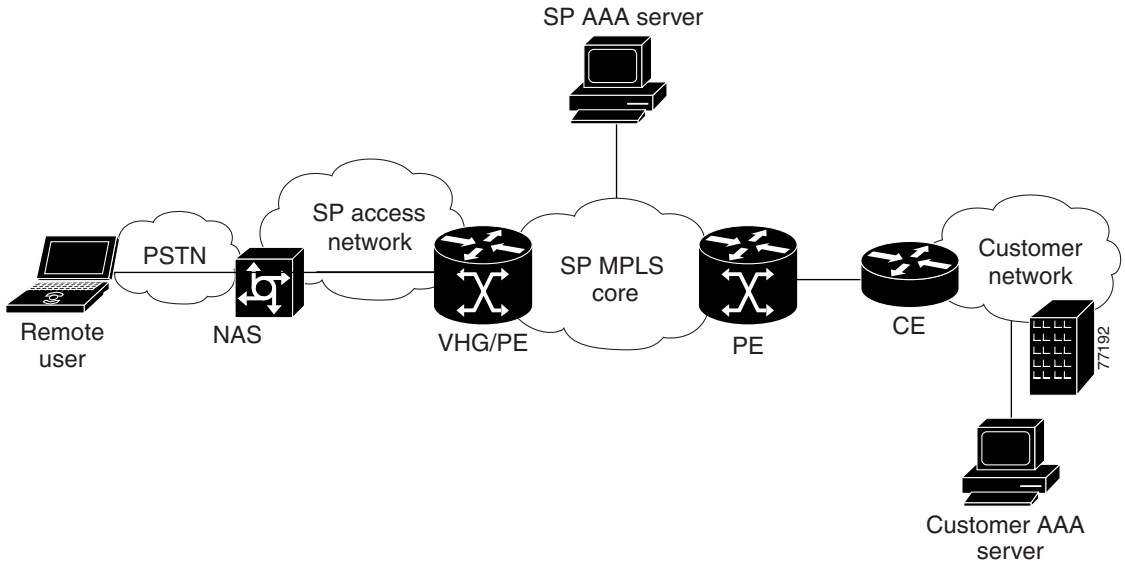
Layer 2 Tunnel Protocol (L2TP) dial-in access is designed for service providers who want to offer wholesale dial service to their customers. The service provider (or a large Internet service provider) maintains geographically dispersed points of presence (POPs). A customer of the service provider dials in to a network access server (NAS) at a local POP, and the NAS creates a virtual private dial network (VPDN) tunnel to the customer's network.

L2TP dial-in can also include these features:

- Multilink PPP (MLP)—A Point-to-Point Protocol (PPP) that is split across multiple data links. See "Multilink PPP" section on page 2-18.
- Multichassis MLP (MMP)—MLP with redundant stacked NAS/PEs. A stack group bidding process is used to manage the allocation of PPP sessions among the members of the stack. See "Multichassis Multilink PPP" section on page 2-18.
- Address management (1) through overlapping local pools configured on the NAS/PE or overlapping address pools on the SP AAA server, or (2) through the use of a Dynamic Host Configuration Protocol (DHCP) server. See "Address Management" section on page 2-13.

Figure 2-2 shows an example of L2TP dial-in topology.

Figure 2-2 Topology of L2TP Dial-in Access to MPLS VPN



These are the main events in the call flow that corresponds to the topology shown in the figure:

1. The remote user initiates a PPP connection to a network access server (NAS) using either analog service or ISDN. If MLP is enabled, the session is identified as potentially a part of an MLP bundle.
2. The NAS accepts the connection and a PPP or MLP link is established.
3. The NAS partially authenticates the user with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). The domain name or dialed number identification service (DNIS) is used to determine whether the user is a VPN client. If the user is not a VPN client (the service provider is also the user's ISP), authentication continues on the NAS. If the user is a VPN client, as in the L2TP dial-in scenario, the AAA server returns the address of a virtual home gateway/provider edge router (VHG/PE).
4. If an L2TP tunnel does not exist, the NAS initiates a tunnel to the VHG/PE. The NAS and the VHG/PE authenticate each other before any sessions are attempted within a tunnel.

Note A VHG/PE can also accept tunnel creation without the NAS providing tunnel authentication.

5. Once the tunnel exists, a session within the tunnel is created for the remote user, and the PPP connection is extended to terminate on the VHG/PE.

6. The NAS propagates all available PPP information (the LCP negotiated options and the partially authenticated CHAP/PAP information) to the VHG/PE.
7. The VHG/PE associates the remote user with a specific customer MPLS VPN. The VPN's virtual routing/forwarding instance (VRF) has been instantiated on the VHG/PE. (The VRF is information associated with a specific VPN.)
8. The VHG/PE completes the remote user's authentication.
9. The VHG/PE obtains an IP address for the remote user.
10. The remote user becomes part of the customer VPN. Packets flow from and to the remote user.
11. If MLP is enabled, the remote user initiates a second PPP link of the MLP bundle. The above steps are repeated, except that an IP address is not obtained; the existing IP address is used. The remote user can use both PPP sessions. Packets are fragmented across links and defragmented on the VHG/PE, with both MLP bundles being put into the same VRF. The VRF includes routing information for a specific customer VPN site.

Note In the context of L2TP dial methods, the NAS functions as an L2TP access concentrator, and the VHG/PE functions as an L2TP network server. In diagrams and descriptions, we show this simply as "NAS" and "VHG/PE".

L2TP Dial-in Components

This section describes the major components of the L2TP dial-in architecture shown in Figure 2-2. It also describes the role each component plays and the specific platforms and software supported. Table 2-5 describes additional components common to this and other dial access methods.

Dial L2TP Service Provider Access Network

The service provider access network could be a high-speed LAN or an ATM network. The service provider needs to place a NAS and VHG/PE in each access network POP.

Network Access Servers

Functioning as a LAC, the NAS receives an incoming PPP session over an analog or ISDN connection, places the session into a VPDN tunnel, and forwards it to the VHG/PE. Table 2-1 lists the platforms supported for the NAS.

Table 2-1 Supported Network Access Servers, IOS Release, and Documentation Location

Platform Supported	IOS Release	Documentation Location
Cisco 36x0 series router: • For the Cisco 3640 series router, 60 ISDN ports or 48 POTS ports • For the Cisco 3660 series router, 120 ISDN ports or 96 POTS ports	12.2(6)	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:3600
Cisco AS5300 universal access server: up to 8 T1/E1/ISDN PRI interfaces (up to 192/240 ports)	12.2(6)	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:AS5300

Table 2-1 Supported Network Access Servers, IOS Release, and Documentation Location

Platform Supported	IOS Release	Documentation Location
Cisco AS5400 universal access server	12.2(6)	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:AS5400
Cisco AS5800 universal access server: up to 48 T1/E1/ISDN PRI interfaces (up to 1152/1440 ports) or up to two T3 interfaces (up to 1344 ports)	12.2(6)	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:AS5800

VHG/PE Routers

The VHG/PE router terminates the L2TP-tunneled session and places it in the correct customer VRF, passing it on to the MPLS core network. Table 2-2 lists the platforms supported for the VHG/PE.

Table 2-2 Supported VHG/PE Routers, IOS Release, and Documentation Location

Component	IOS Release	Documentation Location
Cisco 7200 NPE300/NPE400 series routers	12.2(8)T or higher	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7200
Cisco 7500 RSP4 and RSP8 series routers	12.2(8)T or higher	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7500
Cisco 6400 NRP1/NRP2 universal access concentrator	12.2(2)B3 or higher	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:6400

Overview of Direct ISDN PE Dial-in Remote Access

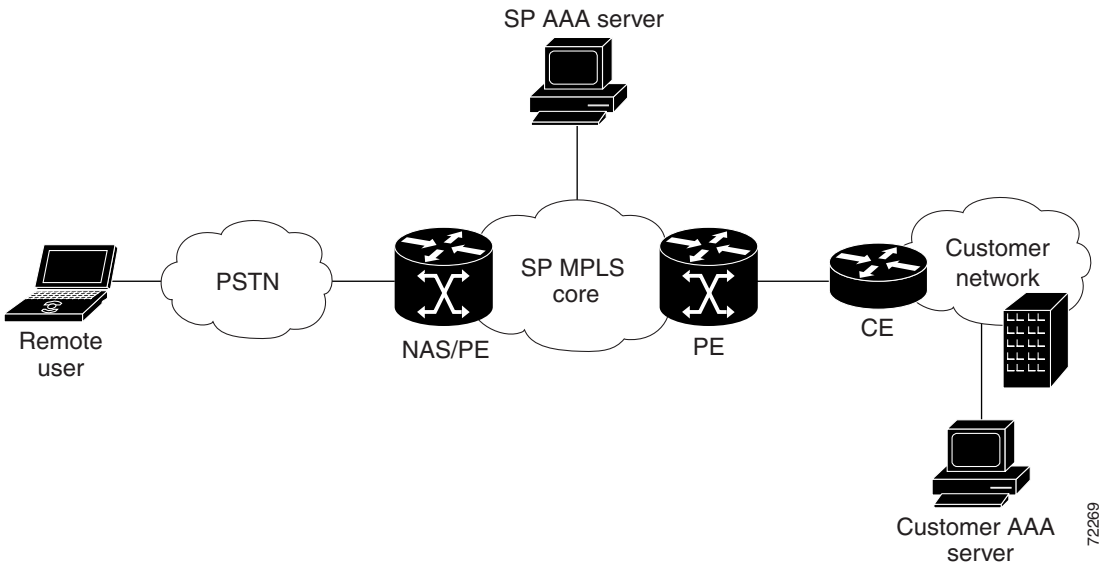
In direct ISDN PE dial-in access to an MPLS VPN, a NAS functions as both NAS and PE. (For that reason, the NAS is referred to here as a NAS/PE.) In contrast to an L2TP dial-in access session, the PPP session is placed directly in the appropriate VRF for the MPLS VPN, rather than being forwarded to a network concentrator by a tunneling protocol. Direct dial-in is implemented only with pure ISDN calls, not analog calls.

Direct dial-in can also include these features:

- Multilink PPP (MLP)—A Point-to-Point Protocol (PPP) that is split across multiple data links. See "Multilink PPP" section on page 2-18.
- Multichassis MLP (MMP)—MLP with redundant stacked NAS/PEs. A stack group bidding process is used to manage the allocation of PPP sessions among the members of the stack. See "Multichassis Multilink PPP" section on page 2-18.
- Address management (1) through overlapping local pools configured on the NAS/PE or overlapping address pools on the SP AAA server, or (2) through the use of a Dynamic Host Configuration Protocol (DHCP) server. See "Address Management" section on page 2-13.

Figure 2-3 shows an example of direct dial-in topology.

Figure 2-3 Topology of Direct Dial-in Access to MPLS VPN



These are the main events in the call flow that corresponds to the topology shown in Figure 2-3:

1. The remote user initiates a PPP or MLP connection to the NAS/PE using ISDN.
2. The NAS/PE accepts the connection, and a PPP or MLP link is established.
3. The NAS/PE authorizes the call with the service provider AAA server. Authorization is based on the domain name or DNIS.
4. The service provider AAA server associates the remote user with a specific VPN and returns the corresponding VPN routing/forwarding instance (VRF) name to the NAS/PE, along with an IP address pool name.
5. The NAS/PE creates a virtual access interface to terminate the user's PPP sessions. Part of the virtual interface's configuration will have been retrieved from the service provider AAA server as part of the authorization. The remainder comes from a locally configured virtual template.
6. CHAP continues and completes. An IP address is allocated to the remote user. You can use any of several different methods for address assignment.
7. The remote user is now part of the customer VPN. Packets can flow from and to the remote user.

Direct ISDN PE Dial-in Components

This section describes the major components of the direct dial-in architecture shown in Figure 2-3. It also describes the role each component plays and the specific platforms and software this architecture supports. Table 2-5 describes additional components common to dial access methods.

Network Access Servers/Provider Edge Routers

Each NAS performs both NAS and PE functions:

1. It receives incoming PPP sessions over ISDN.
2. It terminates the PPP session in an MLP virtual access bundle.
3. It inserts the bundle into the specific customer VRF domain.

4. It removes PPP encapsulation.
5. It forwards the IP header and data to the MPLS VPN network through tag switching.

Table 2-3 lists the platforms that direct ISDN PE dial-in supports.

Table 2-3 Supported NAS/PEs, IOS Release, and Documentation Location

Platform Supported	IOS Release	Documentation Location
Cisco 36x0 series router: • For the Cisco 3640 series router, 60 ISDN ports or 48 POTS ports • For the Cisco 3660 series router, 120 ISDN ports or 96 POTS ports	12.2(8)T	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:3600
Cisco 7200 NPE300/NPE400 series routers	12.2(8)T	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7200

Overview of Dial Backup

You can use dial backup to provide a fallback link for a primary, direct connection such as cable or DSL. If you use L2TP dial-in architecture, dial backup provides connectivity from the customer's remote office to the customer's VPN when the primary link becomes unavailable.

You typically configure the primary link and the backup link on the same CE router at the remote site.

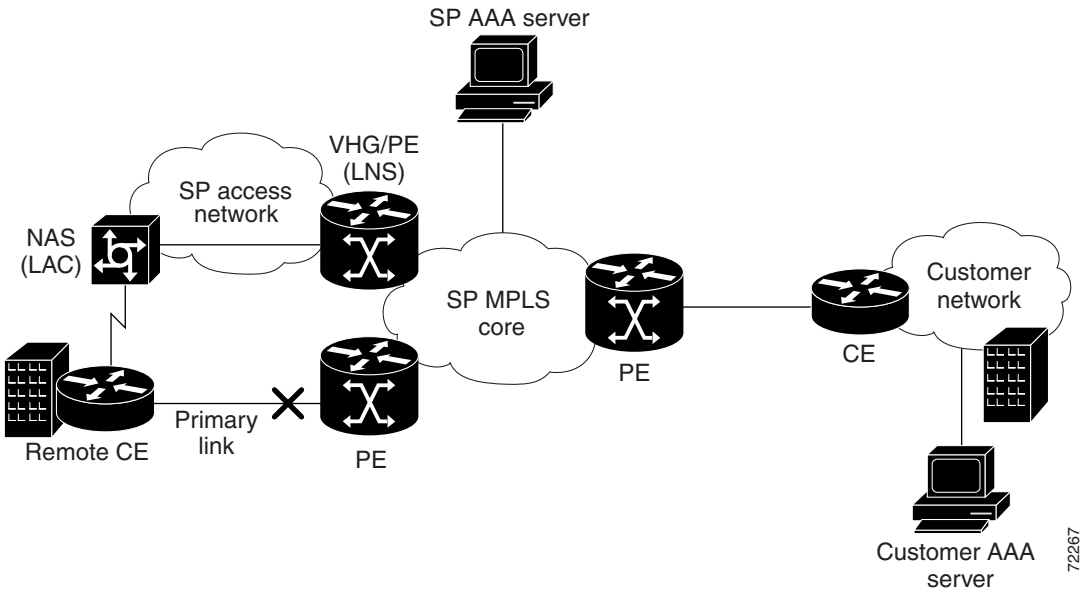
Call flow in dial backup is identical to that in L2TP dial-in access, except that the call is initiated by a backup interface when connectivity to the primary interface is lost, instead of by a remote user. A dialer interface is configured to dial in to the service provider's NAS using a dial backup phone number. The phone number indicates that dial backup is being initiated instead of a typical L2TP dial-in.

Using L2TP, the NAS tunnels the PPP session to the VHG/PE, which then maps the incoming session into the appropriate VRF. The VRF routing tables on all remote PEs must converge; updates come from the VHG/PE.

When the primary link is restored, the primary route is also restored, the remote user terminates the backup connection, and the VHG/PE deletes the backup route.

Figure 2-4 shows an example of topology for dial backup.

Figure 2-4 Topology for Dial Backup



Dial Backup Components and Features

Like L2TP dial-in, dial backup requires a NAS and a VHG/PE. The following sections describe the ways in which dial backup differs from L2TP dial-in.

No Address Assignment

Because dial backup is used primarily to connect remote sites (not remote users) to a customer VPN, address assignment is not needed.

MLP Typically Used

Backup links are typically MLP links, and you can configure an IGP routing protocol on the backup link.

Static or Dynamic Routing Must Be Provisioned

If routing is not enabled on the links between the CE and the VHG/PE, you must provision static VRF routes on the VHG/PE. For the primary link, provisioning is straightforward. The primary static route is withdrawn when the primary link goes down, due to lack of connectivity. For the backup PPP session, you can download the static route from the RADIUS AAA server as part of the virtual profile (framed-route attribute). The route is then inserted into the appropriate VRF when the backup virtual interface is brought up.

When the primary link is restored, the primary static VRF route is also restored, and the CE terminates the backup connection. The PE then deletes the backup static VRF route.

Alternatively, you can configure dynamic routing on both the primary and the backup CE-PE link.

Note Typically, static routing is used when remote networks rarely change their IP addresses, or when the connecting network is a stub network, and there is only one path to the remote destination. Dynamic routing is more suitable when network routing might be reconfigured or when there are multiple paths to the remote destination.

Authentication by Service Provider AAA server

With dial backup, authentication of the remote CE is similar to remote user authentication in L2TP dial-in. If there is a managed CE, the service provider AAA server can authenticate the remote CE; proxy authentication is not needed.

Accounting

The service provider AAA server or RADIUS proxy on the VHG/PE maintains accounting records, including MLP information, for the duration of the backup session.

Overview of Dial-out Access

In dial-out remote access, instead of a remote user or CE initiating a call into the MPLS VPN, the connection is established by traffic coming *from* the MPLS VPN and triggering a call from the dial-out router to the remote CE. Dial-out access can use either L2TP or direct ISDN architecture.

Dial-out is often used for automated functions. For example, a central database system might dial out nightly to remote vending machines to collect daily sales data and check inventories.

In this release of Cisco Remote Access to MPLS VPN integration, the dialer interface used is a *dialer profile*. With a dialer profile, each physical interface becomes a member of a dialer pool. The VHG/PE (in L2TP dial-out) or the NAS/PE (in direct dial-out) triggers a call when it receives interesting traffic from a remote peer in the customer VPN. (“Interesting traffic” is traffic identified as destined for this particular dial-out network.)

Based on the dialer interface configuration, the VHG/PE or NAS/PE borrows a physical interface from the dialer pool for the duration of the call. Once the call is complete, the router returns the physical interface to the dialer pool. Because of this dynamic binding, different dialer interfaces can be configured for different customer VPNs, each with its own VRF, IP address, and dialer string.

Unlike dial-in remote access, dial-out access does not require the querying of an AAA server or the use of two-way authentication, because user information is directly implemented on the dialer profile interface configured on the dial-out router.

Figure 2-5 shows an example of the topology for L2TP dial-out access, and Figure 2-6 shows an example of the topology for direct ISDN dial-out access.

Figure 2-5 Topology of L2TP Dial-out Remote Access

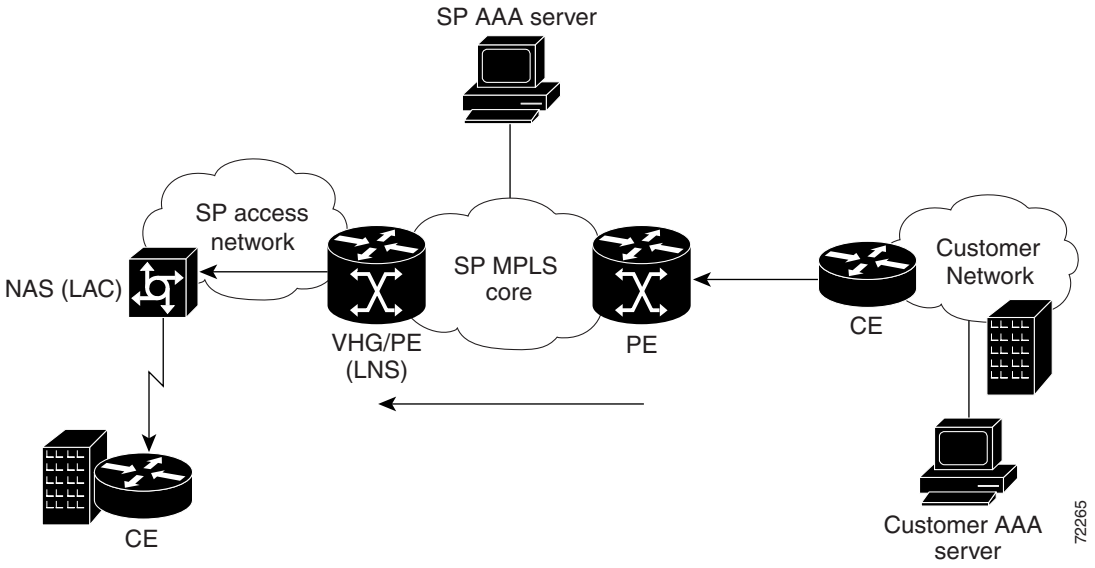
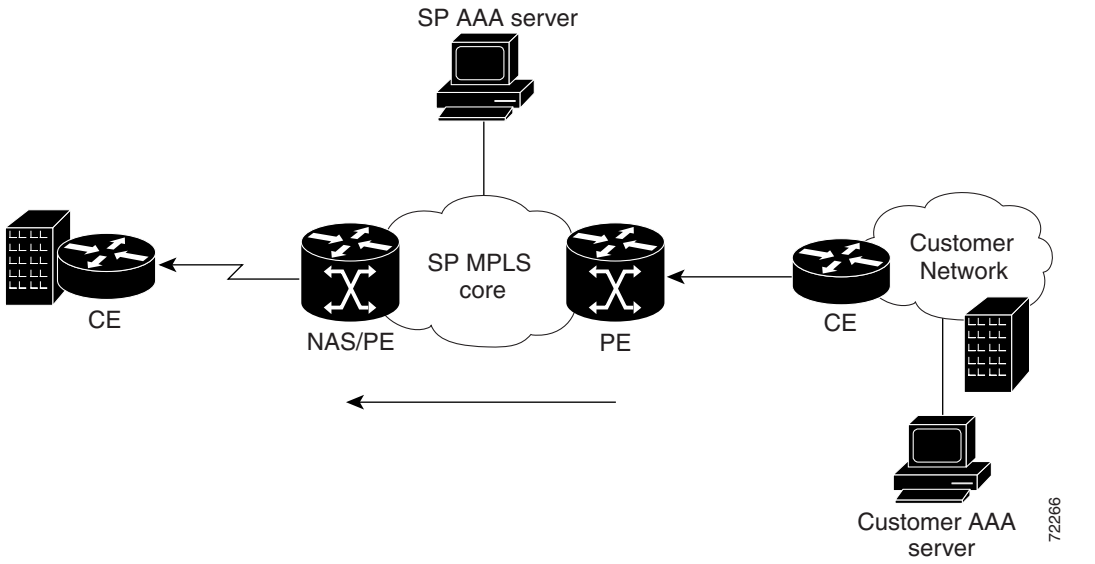


Figure 2-6 Topology of Direct ISDN Dial-out Remote Access



These are the main events in the dial-out call flow:

1. Traffic from a specific customer VPN, destined for a specific dial-out network (identified through static routes in the customer VRF) is directed to the appropriate VHG/PE or NAS/PE.
2. Upon receiving the traffic, either the VHG/PE or the NAS/PE responds:
   - In L2TP dial-out, the VHG/PE brings up an L2TP tunnel and negotiates an outgoing PPP session with the NAS. The dial-out PPP session is triggered using dialer profiles. The NAS then dials out to the CE using dial-out information received in the L2TP session negotiation.

– In direct dial-out, the NAS/PE dials out directly to the CE. The dial-out PPP session is triggered using dialer profiles.

Platforms Supported for Dial-Out Remote Access

Table 2-4 lists platforms supported for L2TP dial-out remote access, and Table 2-5 lists platforms supported for direct ISDN dial-out.

Table 2-4 Supported NAS and VHG/PE Platforms for L2TP Dial-Out

Platform Supported	IOS Release	Documentation Location
NAS		
Cisco 36x0 series router: • For the Cisco 3640 series router, 60 ISDN ports or 48 POTS ports • For the Cisco 3660 series router, 120 ISDN ports or 96 POTS ports	12.2(6)	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:3600
VHG/PE		
Cisco 7200 NPE300/NPE400 series routers	12.2(8)T or higher	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7200
Cisco 7500 RSP4 and RSP8 series routers	12.2(8)T or higher	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7500
Cisco 6400 NRP2 universal access concentrator	12.2(2)B3 or higher	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:6400

Table 2-5 Supported NAS/PE Platforms for Direct ISDN Dial-Out

Platform Supported	IOS Release	Documentation Location
Cisco 36x0 series router: • For the Cisco 3640 series router, 60 ISDN ports or 48 POTS ports • For the Cisco 3660 series router, 120 ISDN ports or 96 POTS ports	12.2(8)T	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:3600
Cisco 7200 NPE300/NPE400 series routers	12.2(8)T	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7200

Common Components and Features

This section describes components and features that are common to more than one dial architecture. An understanding of these features and the alternative ways in which they can be implemented can help you plan the configuration you will use in Chapter 3, "Provisioning Dial Access to MPLS VPN Integration".

The section covers the following features:

Virtual Access Interface

The interface on the VHG/PE or NAS/PE to an MPLS VPN must be VRF-aware and must support Cisco Express Forwarding (CEF) switching. PPP sessions are terminated at the VHG/PE or the NAS/PE on a virtual access interface. The virtual access interface is an instance of either a virtual template or a virtual profile.

Because a virtual template is configured for a specific VRF, and there is a maximum of 25 virtual templates per system, the use of virtual templates limits a system to supporting no more than 25 VPNs.

By contrast, a virtual profile is more scalable and flexible. It defines and applies per-user configuration information, which can come from a virtual interface template, per-user configuration information stored on an AAA server, or both, depending on how the router and AAA server are configured.

Framed-Route VRF Aware

You can use the Framed-Route VRF Aware feature to apply static IP routes to a particular VRF table rather than the global routing table. The feature makes RADIUS Attribute 22 (Framed-Route) and a combination of Attribute 8 (Framed-IP-Address) and Attribute 9 (Framed-IP-Netmask) VRF aware.

You can configure a per-user static route using the framed-route attribute in any of three ways.

- Use the cisco VSA route command
- Use the framed-route attribute. When it receives a framed-route from the RADIUS server, the VHG/PE checks whether the user is a VPN customer. If so, then the static route is implemented in the routing table of the VRF to which the user belongs.
- Use the framed-ip-address /framed-netmask, which has the same function as framed route.

Per-VRF AAA

The Per-VRF AAA feature allows a service provider to partition AAA services based on VRF which eliminates the need for proxy AAA. The virtual home gateway (VHG) or provider edge (PE) router is able to communicate directly with an AAA RADIUS server associated with the user's VPN. The Per-VRF AAA feature includes support for both static configuration of per-VRF data (local authorization) and downloading of the per-VRF data from a AAA RADIUS server (remote authorization).

As of Release FA03, attribute filtering for remote authorization is also supported on a per-domain basis. Attribute filtering for remote authorization is supported with a AAA attribute as part of the template downloaded from the AAA RADIUS server. In addition, framed routes downloaded with an AAA template are VRF-aware.

VPDN Multihop with VRF Support

The VPDN Multihop feature allows packets to pass through multiple tunnels using both L2F and L2TP protocols in a VPDN environment with VRF awareness.

The VPDN Multihop with VRF Support feature enables an L2TP tunnel to start outside the MPLS VPN, and to terminate (or multihop) somewhere within the MPLS VPN. Before the introduction of this feature, the IP addresses used by the VPDN tunnel could not overlap across VPNs because VPDN only uses global IP addresses. With the VPDN Multihop with VRF Support feature support is possible for L2TP tunnels that terminate with the VRF and have overlapping IP addresses.

AAA Servers

You can use one or more AAA servers for address management and for authorization, authentication, and accounting. The AAA server runs Cisco Access Registrar (AR) or similar server software and uses Remote Authentication Dial-In User Service (RADIUS) as the protocol for communication with the NAS, VHG/PE, or NAS/PE. The server is sometimes referred to as a RADIUS server or an AR server.

Depending on the alternatives you choose for each of those features, you might have one of the following:

- Local AAA servers in each access network
- Shared AAA servers in the core MPLS network
- A mix of local AAA servers in each access network and shared AAA servers in the core MPLS network

Performing authentication and authorization only, a single AAA server running AR can process up to 800 calls per second (one request per call) without losses. Performing address management, authentication, authorization, and accounting, a single AAA server running AR can process up to 300 calls per second (three requests per call).

The following feature descriptions indicate how the AAA server functions:

- Address Management, page 2-13
- Authorization and Authentication, page 2-14
- Accounting, page 2-15

Address Management

You can handle address management using one of the following methods:

- Overlapping address pools—With overlapping address pools, you configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces. Pools can be implemented in one of two ways:
  - Locally—The VHG/PE or NAS/PE maintains the overlapping address pools.

  - Remotely—An AAA server maintains the overlapping address pools, and the VHG/PE or NAS/PE requests an address from the AAA server. If you use overlapping address pools on an AAA server, you must configure authentication and accounting on the same server. The recommended server is the Cisco AR.

- DHCP address management—With DHCP address management, a DHCP server maintains a common address pool for the service provider (not for each customer VPN) and dynamically assigns IP addresses in response to requests from the VHG/PE or NAS/PE. The recommended DHCP server is the Cisco Network Registrar.
- On-demand address pools (ODAP)—In on-demand address pools (ODAP), a central SP RADIUS server manages a block of addresses for each customer. Each pool is divided into subnets of various sizes, and the server assigns subnets to the VHG/PE or NAS/PE on request.

  The VHG/PE or NAS/PE acts as a DHCP server. On the VHG/PE or NAS/PE, one on-demand pool is configured for each customer VPN supported by that router. Upon configuration, the VHG/PE or NAS/PE's pool manager requests an initial subnet from the server.

  Address management is on demand because address pool subnets are allocated or released based on a threshold. If use exceeds a defined ceiling threshold, the pool manager requests an additional subnet from the server and adds it to the on-demand pool. If use falls below a floor threshold, the pool manager attempts to free one, or more then one, of the on-demand pool's subnets to return it to the server. The VRF routing table on the VHG/PE or NAS/PE is updated with the subnet route whenever a range of addresses is requested from the AR.

  ODAP's benefits include efficient management of address space and dynamic address summarization on the VRF table. ODAP has two main drawbacks:

  - An allocated subnet is not released so long as a single dial-in client in a given VRF is connected (using an IP address)
  - BGP route summarization is not possible with ODAP, because multiple PEs have subnets of a major Class C or Class B subnet, there is no way to summarize on the Class C or Class B subnet. Using ODAP thus causes an increase in the BGP routing table.

  Consider using ODAP, then, if subnet management is more important than route summarization.

  ODAP requires Access Registrar 1.7 or 1.7R1.

  ODAP can be used with the following dial architectures:

  - Dial-in L2TP and Direct ISDN
  - Dial-out L2TP and Direct ISDN

Authorization and Authentication

You can handle user authorization and authentication in one of the following ways:

- (For L2TP only.) The VHG/PE does user authorization and authentication locally.
- (For either L2TP or direct dial access.) The service provider AAA server handles all user authorization and authentication.
- (For L2TP only.) The service provider AAA server uses *proxy authentication*, passing the authentication request on to a customer AAA server, where all user-specific data is stored. When the VHG/PE or NAS/PE receives an incoming PPP session, it sends an access-request to the service provider AAA server, which then sends the proxy request to the customer AAA server. The customer

AAA server authorizes the PPP session based on the remote user's domain name or DNIS, and associates the PPP session with a specific VPN. The VPN information is returned to the VHG/PE as configuration commands that are applied to the virtual interface being created for that PPP session.

Accounting

You can handle accounting in one of the following ways:

- Maintain user accounting records on the service provider AAA server. If you are using an AAA server for address management, you must also use it for accounting.
- Configure the VHG/PE or NAS/PE to handle accounting records based on proxy accounting. Proxy accounting involves sending the records to your AAA server, which then passes them on to the customer AAA server.

On the VHG/PE or NAS/PE, you can use NetFlow for per-flow usage accounting. The NetFlow Collector provides usage data collection. You can use the data for performance reporting, capacity planning, and usage-based billing. The VPN Solutions Center (VPNSC), running on a separate management workstation, can collect usage records from the NetFlow Collector and correlate them with VPN service layer information to provide per-VPN statistics.

Core MPLS Network

Dial access to MPLS VPN supports two core network types, IP MPLS and ATM MPLS.

Management Tools

The VPN Solutions Center (VPNSC) is the primary tool used to provision a management VPN for all managed sites. The management VPN is required for applications that need access to a customer's VPN. In dial access to MPLS VPN, those applications are VPNSC, Cisco IP Manager (CIPM), and SP Access Registrar, if you are using authentication proxy to a customer AAA server.

The configuration of the VPN management for the VPNSC and CIPM applications is generic to all managed MPLS VPN solutions. For example, because of the way the management VPN is configured by VPNSC, only applications on the management VPN can access the managed PE and CE routers.

For RADIUS AAA proxy authentication, you need the following configuration:

- Each VPN's AAA server must have a unique address.
- The SP's AAA server must be in a Management VPN.
- Routes to each of the VPN AAA servers must be distributed to the management VPN, and the route to the SP AAA server must be distributed to each of the other VPNs.

Network Management Components for Dial Access

Network management components for dial access are as follows:

- Element managers:
  - Service Connection Manager (SCM) for the Cisco 6400-NRP1/NRP2. SCM requires a Sun Ultra 60 workstation with 512 MB of RAM, 2 GB of swap space, and 2.2 GB of disk space, Solaris 2.6.

  - CIPM for the Cisco 7200-NPE300/NPE400/7500.
  - Cisco Access Manager (CAM) for the access servers. CAM requires a Sun workstation, whose exact specifications depend on the number of ports to be managed. CAM also requires Solaris 2.5.1 and Oracle Enterprise Server 7.3.4 with 4 GB of available disk space. (The database server is local or remote.)
- VPNSC—For VPN service provisioning, auditing, SLA monitoring, and accounting. VPNSC also uses CIPM for configuration downloads/uploads. For details, see the VPNSC 2.1 documentation set at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/2_1/index.htm
- Cisco AR—For AAA functionality. AR Release 1.5 is used. It runs on a Sun SPARCstation with Solaris 2.6 or 2.7, 128 MB of RAM, and 80 MB of disk space.
- Cisco Network Registrar—For IP address allocation; Release 3.5 or 4.0 is appropriate. Release 3.5(1) runs on Windows NT 4.0, Windows 2000, Solaris 2.5.1, Solaris 2.6, and Solaris 7. Network Registrar's Release 3.5(1) GUI also runs on Windows 95 and Windows 98.
- NetFlow—For usage accounting of non-PPP connections. Only NetFlow Collector is needed. NetFlow Collector 3.0 runs on either Sun Ultra 1 or higher with at least 128 MB of RAM, 512 MB of swap space, and 4 GB of disk space. It also requires Solaris Version 2.5.1 or 2.6, or HP Class C or higher with at least 128 MB of RAM, 512 MB of swap space, and 4 GB of disk space. Finally, it requires UX Version 11.0 (32-bit and 64-bit are supported).
- Cisco Info Center (CIC)—For VPN fault monitoring. CIC Release 1.2 requires Sun Ultra-II or higher running Solaris 2.5.1 or 2.6 and Java 1.1. CIC also requires 256 MB of main memory, 200 MB of hard disk space, and 23 MB available in /var/tmp.
- Concord Network Health—For VPN performance reporting. Network Health is integrated with VPNSC.

Fault Monitoring

Fault monitoring is performed at the device and service levels. VPNSC monitors the PE-CE connections.

At the device level, fault monitoring is performed by the element managers. (CEMF has an event manager component, accessed through VPNSC.) CAM provides fault monitoring for each dial port.

CIC, accessed through VPNSC, is used at the service level to provide event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems. CIC is an OEM product from Micromuse's NetCool. CIC's Release 2.0 provides event management at the IP VPN service level through integration with VPNSC.

SLA Reporting

Service level agreements can include uptime as well as guaranteed performance levels. SLA reporting is performed by the Service Assurance Agent (SAA) integrated with VPNSC.

Overview of Optional Features Used with Dial Access

This section describes the optional features that you can use with various dial access methods:

- L2TP Large-Scale Dial-Out per-User Attribute via AAA, page 2-17
- L2TP Dial-Out Load Balancing and Redundancy, page 2-17

- Multilink PPP, page 2-18
- Multichassis Multilink PPP, page 2-18

L2TP Large-Scale Dial-Out per-User Attribute via AAA

The L2TP Large-Scale Dial-Out per-User Attribute via AAA feature makes it possible for IP and other per-user attributes to be applied to an L2TP dial-out session from an LNS. Before this feature was released, IP per-user configurations from authentication, authorization, and accounting (AAA) servers were not supported; the IP configuration would come from the dialer interface defined on the router.

The L2TP Large-Scale Dial-Out per-User Attribute via AAA feature works in a way similar to virtual profiles and L2TP dial-in. The L2TP virtual access interface is first cloned from the virtual template, which means that configurations from the virtual template interface will be applied to the L2TP virtual access interface. After authentication, the AAA per-user configuration is applied to the virtual access interface. Because AAA per-user attributes are applied only after the user has been authenticated, the LNS must be configured to authenticate the dial-out user (configuration authentication is needed for this feature).

With the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature, all software components can now use the configuration present on the virtual access interface rather than what is present on the dialer interface. For example, IP Control Protocol (IPCP) address negotiation uses the local address of the virtual access interface as the router address while negotiating with the peer.

Because per-user attributes are contained within the dialin AAA profile and are not supplied withing the LSDO profile, you must enable bidirectional CHAP authentication with this feature.

You must enable bidirectional CHAP authentication to use this feature because per-user attributes are contained within the dialin AAA profile and thes per-user attributes are not supplied within the LSDO profile.

For more information about this feature, refer to the *L2TP Large-Scale Dial-Out per-User Attribute via AAA* document.

L2TP Dial-Out Load Balancing and Redundancy

It is recommended that you use Cisco IOS Release 12.2(2)BX or Cisco IOS Release 12.2(11)T or later releases on the LAC to ensure proper dial-out bidding with this feature.

This feature enables an LNS to dial out to multiple L2TP access concentrators (LACs). When the LAC with the highest priority goes down, it is possible for the LNS to failover to another lower priority LAC. The LNS can also load balance the sessions between multiple LACs that have the same priority settings.

Dial-Out and Multiple LACs on the LNS

In Cisco IOS software prior to Release 12.2(15)T, L2TP large-scale dial-out using the Stacked Group Bidding Protocol (SGBP) for dial-out connection bidding required configuring a primary and secondary LAC. Dial-out used the secondary LAC only when ports were not available on the primary LAC, or when more ports were available on the secondary LAC. However, the LNS could use the ports only on the primary LAC. Because the **initiate-to** VPDN group configuration command used to specify the IP address for the tunnel did not support multiple statements on an LNS, only the IP address of the primary LAC could be configured. Therefore, the LNS could not contact any other LACs when the primary LAC went down, and failover was not supported for dial-out calls by the LNS.

The L2TP Dial-Out Load Balancing and Redundancy feature introduced in Cisco IOS Release 12.2(15)T enables an LNS to dial out to multiple LACs (multiple **initiate-to** VPDN group configuration commands, and therefore multiple IP addresses, are supported).

Load Balancing and Redundancy

The L2TP Dial-Out Load Balancing and Redundancy feature supports load balancing between multiple LACs that have the same priority settings in the **initiate-to** VPDN group configuration commands. You can also set redundancy and failover by configuring differing priority values in the **initiate-to** VPDN group configuration commands. When the LAC with the highest priority goes down, the LNS will failover to another lower priority LAC.

For more information about this feature, refer to the *L2TP Dial-Out Load Balancing and Redundancy* document.

Multilink PPP

With Multilink PPP (MLP), you can use additional bandwidth that might be available between two network devices. If MLP is used, a single user session is split over two PPP links, and the same IP address is assigned to both. The multilink bundles are reassembled on the VHG/PE or NAS/PE. From the user's point of view, there appears to be a single link, but because packets can be transferred on both links, the connection operates more efficiently than a single link would and carries an equivalent amount of traffic.

The multilink bundle is always associated with a virtual access interface.

Requirements for MLP Support

The VHG/PE or the NAS/PE requires Cisco IOS Release 12.2(8)T for MLP support.

Multichassis Multilink PPP

Multichassis Multilink PPP (MMP) is an extension of Multilink PPP and enables MLP links to terminate at multiple stacked VHG/PEs (in L2TP dial) or NAS/PEs (in direct ISDN PE dial). You configure the routers as members of a stack group, so that they operate as a single, large dialup pool using a single dialup telephone number. MMP enhances a network's scalability; an organization can add new routers to its dialup pool as needed.

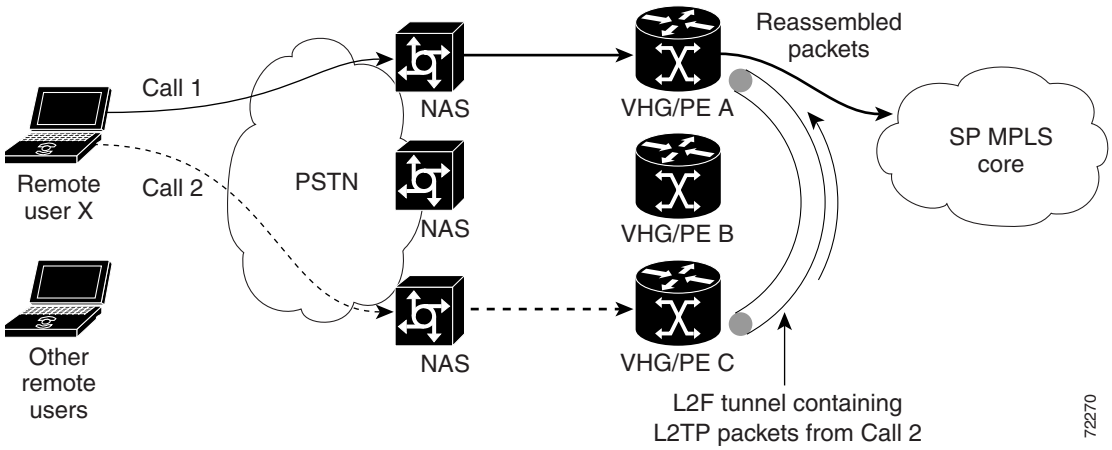
To set up MMP, you use the Stack Group Bidding Protocol (SGBP), which assigns ownership of a call to a master VHG/PE or NAS/PE in the stack group through a process of bidding. The call flow follows this general sequence (shown in Figure 2-7):

1. User X makes MLP Call 1. NAS A answers the call and tunnels the session to VHG/PE A.
2. VHG/PE A informs its stack group peer network access servers that it has accepted a call from user X on CE router X.
3. All members of the stack group bid for the ownership ("bundle mastership") of the call.
4. In this example, SGBP bidding is configured so that the VHG/PE that receives the first call "wins." VHG/PE A, therefore, becomes the bundle master for the MLP session and receives the call. As bundle master, VHG/PE A owns all connections with user X.

5. When user X needs more bandwidth (based on the dialer threshold configured for MLP), a second MLP call (Call 2) is triggered. In this example, NAS C accepts the call and tunnels the session to VHG/PE C, which informs its stack group peers of the call.
6. As in Step 3, the stack group members bid for ownership of this call.
7. VHG/PE A wins the bidding, because it already has an MLP session from user X. VHG/PE C forwards the raw PPP data to VHG/PE A (tunneling via L2F), which reassembles and resequences the call packets.
8. The bundle master, VHG/PE A, performs final authentication.
9. The reassembled packets are passed on to the MPLS VPN, just as if they had all come through one physical link.

L2F performs standard PPP operations up to authentication.

Figure 2-7 Topology in Multichassis Multilink PPP



Requirements for MMP Support

As with MLP, the VHG/PE or the NAS/PE requires Cisco IOS Release 12.2(8)T for MMP support. Multiple NAS and VHG/PE routers are required, and the VHG/PEs are configured with SGBP.

CHAPTER 3

Provisioning Dial Access to MPLS VPN Integration

This chapter describes how to provision each of the methods of dial access to MPLS (Multiprotocol Label Switching) VPN (virtual private network) integration. It covers the following subjects:

- Provisioning Dial-In Access, page 3-1
  - Provisioning L2TP dial-in
  - Provisioning direct ISDN PE dial-in

Note Because many of the configuration tasks for these two methods are the same, they are described in a single section, with differences noted where a task applies to only one of the access methods.

  - Provisioning L2TP Dial Backup, page 3-18
- Provisioning Dial-out Access, page 3-20
  - Provisioning L2TP dial-out
  - Provisioning direct ISDN dial-out

The chapter also includes a section on Sample Configurations, page 3-24.

Descriptive overviews of the dial access methods and related features are covered in Chapter 2, "Overview of Dial Access to MPLS VPN Integration".

Provisioning Dial-In Access

Before You Begin

The procedures provided here are specific to provisioning remote access to an MPLS VPN and are based on two assumptions:

1. That the following setup and configuration tasks have already been carried out:
   - Setup of the MPLS core network
   - Setup of the customer VPN
   - Configuration of the links between the provider edge router (PE) and the customer edge router (CE)

2. That you have a good understanding of the architecture and features you are using and that you have selected the means you will use for implementing those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

See Chapter 2, "Overview of Dial Access to MPLS VPN Integration" for information that will help you understand the dial architectures and decide on your implementation approach.

Dial-In Provisioning Checklist

Table 3-2 lists provisioning tasks for L2TP dial-in and for direct ISDN PE dial-in. Procedures for completing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 3-1 Checklist of Tasks for Dial-in Provisioning

	Task	L2TP Dial-In	Direct ISDN PE Dial-In
	Before you begin, read the Cisco Remote Access to MPLS VPN Integration 2.0 Release Notes at http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/rampls2/relnote/index.htm		
Do initial, one-time setup			
	Task 1. Configure the PE Routers for MPLS.	On the VHG/PE	On the NAS/PE
	Task 2. Configure the SP AAA RADIUS Server with Client Information.	On the SP AAA server: • NAS/LAC client information • VHG/PE client information	On the SP AAA server: NAS/PE client information
	Task 3. Configure RADIUS AAA on the Querying Device.	On the NAS/LAC On the VHG/PE	On the NAS/PE
Add new customer groups as needed			
	Task 1. Configure L2TP Information for New Customers (L2TP only).	On the NAS/LAC or the SP AAA RADIUS server	—
	Task 2. Configure VRF Information for the Customer Group.	On the VHG/PE	On the NAS/PE
	Task 3. Configure VPDN Information for the Customer Group (L2TP only).	On the VHG/PE	—
	Task 4. Configure Authentication and Authorization.	On one of the following, depending on how you are handling authentication and authorization: • VHG/PE • SP AAA RADIUS server • (Proxy) SP AAA RADIUS server and customer AAA RADIUS server	On the SP AAA server

Table 3-1 Checklist of Tasks for Dial-in Provisioning (continued)

	Task	L2TP Dial-In	Direct ISDN PE Dial-In
	Task 5. Configure Accounting Between the VHG/PE or NAS/PE and the Access Registrar.	On VHG/PE	On NAS/PE
	Task 6. Configure Address Management.	On VHG/PE or On SP AAA server	On NAS/PE or On SP AAA server
	Task 7. (If You Are Using MLP) Configure LCP Renegotiation and Enable MLP for Users in the Group.	On VHG/PE	On NAS/PE
	Task 8. (If You Are Using MMP) Configure SGBP on Each Stack Group Member.	On each VHG/PE in the stack group	On each NAS/PE in the stack group

Miscellaneous Component Configurations

For miscellaneous component configuration details, refer to the documentation listed in Table 3-2.

Table 3-2 Miscellaneous component configurations

Component	Documentation Location
Cisco Access Registrar	http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm
Cisco Network Registrar	http://www/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/index.htm
MPLS VPN PE (IOS Release 12.2x)	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagc.htm
MPLS VPNSC 2.1	http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/2_1/index.htm

Initial, One-Time Setup Tasks

These tasks are done once and are not specific to a particular customer or VPN.

Task 1. Configure the PE Routers for MPLS

In L2TP dial-in, configure the VHG/PE routers. In direct ISDN PE dial-in, configure the NAS/PE routers. Perform the following steps:

Step 1 Configure the loopback interface:

Router (config)# **interface loopback** [*number*]

Step 2 Configure IGP (OSPF or IS-IS).

Note For details on configuring OSPF, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfospf.htm.

For details on configuring IS-IS, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfisis.htm

Step 3 On the interface connected to the MPLS core, use the following commands to configure CEF and label switching:

a. Router (config)# **ip cef**

b. Router (config-if)# **tag-switching ip**

Step 4 Use the following commands to configure a BGP peer from the VHG/PE or the NAS/PE to loop back on the remote PEs:

a. Router (config)# **router bgp** [*autonomous system number of sp*]

b. Router (config-router)# **neighbor** [*ip address of the first remote pe*] **remote-as** [*same autonomous number*]

c. Router (config-router)# **neighbor** [*ip address of first remote pe*] **update-source Loopback0**

d. Repeat (b) and (c) for each remote PE.

Step 5 Use the following commands to configure the BGP session to exchange VPN-IPV4 route prefixes for each remote PE:

a. Router (config-router)# **address-family vpnv4**

b. Router (config-router-af)# **neighbor** [*ip address of first remote pe*] **activate**

c. Router (config-router-af)# **neighbor** [*ip address of first remote pe*] **send-community extended**

d. Repeat (b) and (c) for each remote PE.

Table 3-3 provides links to relevant Cisco router configuration documentation.

Table 3-3 PE Routers and Configuration Documentation

Platform	Documentation Location
Cisco 7200-NPE300/NPE400 series routers	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Hardware:7200&s=Hardware_Info#Hardware_Installation_%26_Configuration
Cisco 7500 series routers	http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/cicg7500/cicg75bc.htm
Cisco 6400-NRP1/NRP2 series routers	http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/sw_setup/ss_nrp.htm

Task 2. Configure the SP AAA RADIUS Server with Client Information

You must perform this task if you are using a AAA RADIUS server in your network to provide address management or user authentication, authorization, and accounting.

On the AAA RADIUS server, perform the steps in the following section to configure the Cisco Access Registrar (AR) application with information for either of the following dial-in situations:

- L2TP dial-in, where the SP AAA RADIUS server can be queried for user information by the VHG/PE, or for L2TP information by the NAS/LAC, or both.
- Direct ISDN PE dial-in, where the AAA SP RADIUS server is queried by the NAS/PE.

Configure the SP AAA RADIUS Server for L2TP Dial-In

Step 1 Use the following commands to configure the NAS/LAC client information:

a. Enter CLI configuration mode of AR:

admin@sun-ar% aregcmd -s

b. Change to the client directory:

--> **cd /radius/clients**

c. Add the NAS/LAC router name to the client directory:

--> **add [***name of NAS/LAC***]**

d. Define the IP address and shared key of the NAS/LAC:

--> **cd** to the new directory

--> **set ipaddress [***ip address***]**

--> **set sharedsecret [***sharedsecret***]**

Step 2 Repeat Step 1 to configure VHG/PE client information.

Configure the SP AAA RADIUS Server for Direct ISDN PE Dial-In

Use the following commands to configure the NAS/PE client:

Step 1 Enter CLI configuration mode of AR:

admin@sun-ar% aregcmd -s

Step 2 Change to the client directory:

--> **cd /radius/clients**

Step 3 Add the NAS/PE router name to the client directory:

--> **add [***name of NAS/PE***]**

Step 4 Define the IP address and shared key of the NAS/PE :

--> **cd** to the new directory

--> **set ipaddress [***ip address***]**

--> **set sharedsecret [***sharedsecret***]**

For AR configuration details, refer to
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

Task 3. Configure RADIUS AAA on the Querying Device

This task is required if you are using an AAA RADIUS server in your network to provide address management or user authentication, authorization, and accounting.

Perform the following steps on whichever device queries the SP AAA RADIUS server—the NAS/LAC or VHG/PE (in L2TP dial-in) or the NAS/PE (in direct ISDN PE dial-in):

Step 1 Enable the device to use the RADIUS protocol for authorization and authentication:

a. Router (config)# **aaa new-model**

b. Router (config)# **aaa authentication ppp default local group radius**

c. Router (config)# **aaa authorization network default local group radius**

Step 2 Use the following command to configure the RADIUS server on the device:

Router (config)# **radius-server host [***ip address of radius server***] key [***sharedscret***]**

Note The sharedsecret must match the sharedsecret defined in Step 1d of "Task 2. Configure the SP AAA RADIUS Server with Client Information" on page 3-4.

Task 4. On the RADIUS AAA Server, Configure a Per-user Static Route Using the Framed-route Attribute

To use the cisco VSA route command, enter:

```
cisco-avpair "ip:route = vrf vrf-name 10.10.100.0 255.255.255.0 [next hop ip address(opt)]"
```

To use the framed route attribute, enter:

```
framed-route = 10.10.100.0 255.255.255.0 [next hop ip address(opt)]
```

To use the framed-ip-address /framed-netmask (same function as framed route above), enter:

```
framed-route = 10.10.100.0/24 [next hop ip address(opt)]
```

Example 3-1 Example of RADIUS Access Registrar Configuration

```
[ //localhost/Radius/Profiles/827-fr/Attributes ]
    cisco-avpair = "lcp:interface-config#1= ip vrf forwarding FRtest.com"
    cisco-avpair = "lcp:interface-config#2= ip unnumbered FastEthernet0/0"
    cisco-avpair = "lcp:interface-config#3= encapsulation ppp"
    Framed-IP-Address = 10.10.8.1
    Framed-IP-Netmask = 255.255.255.224
    Framed-Protocol = ppp
    Framed-Routing = None
    Service-Type = Framed
```

Adding New Customer Groups

Perform the tasks described in the following sections for each new customer group.

Task 1. Configure L2TP Information for New Customers (L2TP only)

To configure L2TP information for new customers, do one of the following. The option you select depends on where the L2TP information is stored, on the NAS/LAC or on the AAA server.

- Option 1. Configure L2TP Information Locally on the NAS/LAC
- Option 2. Configure L2TP Information on the AAA Server

Option 1. Configure L2TP Information Locally on the NAS/LAC

Perform the following steps to configure local L2TP information on the NAS/LAC:

Step 1 Enable VPDN on the access server:

Router (config)# **vpdn enable**

Step 2 Enable the search order to look up L2TP tunnels:

Router (config)# **vpdn search-order domain dnis**

Step 3 Define a new VPDN group for each user:

a. Router (config)# **vpdn-group** [*number*]

b. Router (config-vpdn)# **request-dialin**

c. Router (config-vpdn-req-in)# **protocol l2tp**

d. Router (config-vpdn-req-in)# **domain** [*domain name*]

Note Use the domain name syntax for VPDN customers and the **dnis** [*number*] syntax for DNIS customers.

e. Router (config-vpdn-req-in)# **exit**

f. Router (config-vpdn)# **initiate-to ip** [*ip address of VHG*]

Step 4 Define a local username and password for tunnel authentication:

Router (config)# **username** [*hostname*] **password** [*tunnel password*]

Note By default, the host name used in the L2TP tunnel authentication is the host name of the router. You can change this by adding the following command to the VPDN group:
Router (config-vpdn)# **local name** [*hostname*]

Option 2. Configure L2TP Information on the AAA Server

Perform the following steps to configure L2TP information on the AAA server:

Step 1 On the NAS/LAC, enable VPDN:

Router (config)# **vpdn enable**

Step 2 Enable the search order to look up L2TP tunnels:

Router (config)# **vpdn search-order domain dnis**

Step 3 On the AAA server, enable AAA to look up L2TP information. For details, see "Task 3. Configure RADIUS AAA on the Querying Device" on page 3-6.

Step 4 On the AAA server, configure the AR to receive L2TP information:

a. Add a service to the AR:

--> **add /Radius/Services/[***service name***] [***service name description***] local "" "" RejectAll "" [***userlist name***]**

--> **set /Radius/DefaultAuthenticationService [***service name***]**

--> **set /Radius/DefaultAuthorizationService [***service name***]**

Note You can also select the authentication and authorization service with scripting. For Access Registrar (AR) configuration details, refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm.

b. Add a user list to the AR:

--> **add /Radius/Userlists/[***userlist name***]**

Note The user list name must match the user list name defined in Step a. Add a service to the AR:

c. Add tunnel names to user lists:

--> **add /Radius/UserLists/[***userlist name***]/[***domain name***] [***domain name description***] cisco TRUE "" [***attributes list***]**

Note The userlist name must match the userlist name defined in Step a, "Add a service to the AR:".

Note All user records inside the AR database containing tunnel information must have **cisco** entered in the password field.

The command for adding a DNIS user is:

--> **add /Radius/UserLists/[***userlist name***]/dnis:[***dnis number***] [***dnis description***] cisco TRUE "" [***attributes list***]**

d. Add tunnel attributes:

--> **add /Radius/Profiles/[***attributes list***]**

--> **cd /Radius/Profiles/[***attributes list***]/Attributes**

--> **set tunnel-medium-type_tag1 1**

--> **set tunnel-password_tag1 [***tunnel password***]**

--> **set tunnel-server-endpoint_tag1 [***vhg ip address***]**

--> **set tunnel-type_tag1 3**

Note If you are using AR 1.6 Revision 1 or higher, the syntax for the following commands changes from what is given above:
--> **set tunnel-medium-type_tag1 ipv4**
--> **set tunnel-type_tag1 l2tp**

Task 2. Configure VRF Information for the Customer Group

To configure the customer virtual routing/forwarding instance (VRF), which is information associated with a specific VPN, perform the following steps on the VHG/PE or NAS/PE.

Note Before you begin, make sure you have performed the initial BGP configuration in "Task 1. Configure the PE Routers for MPLS" on page 3-3.

Step 1 Define the VRF:

a. Router (config)# **ip vrf** [*vpn name*]

b. Router (config-vrf)# **rd** [*route descriptor value*]

c. Router (config-vrf)# **route-target import** [*route target value*]

d. Router (config-vrf)# **route-target export** [*route target value*]

Step 2 Configure the loopback interface:

a. Router (config)# **interface loopback** [*number*]

b. Router (config-if)# **ip vrf forwarding** [*vpn name*]

Note The vpn name must match that defined in Step 1a above.

c. Router (config-if)# **ip address** [*ip address*] [*netmask*]

Step 3 Configure the BGP session to transport VRF information:

a. Router (config)# **router bgp** [*autonomous system number*]

Note The autonomous system number must match that defined in Step 4a of "Task 1. Configure the PE Routers for MPLS" on page 3-3.

b. Router (config-router)# **address-family ipv4 vrf** [*vpn name*]

c. Router (config-router-af)# **redistribute connected metric 1**

Task 3. Configure VPDN Information for the Customer Group (L2TP only)

To configure VPDN information for the customer group, perform the following steps:

Step 1 Enable VPDN on the VHG/PE:

Router (config)# **vpdn enable**

Step 2 Define a new VPDN group for each user:

Note VPDN on a home gateway is stored locally on the VHG/PE.

a. Router (config)# **vpdn-group** [*number*]
b. Router (config-vpdn)# **accept-dialin**
c. Router (config-vpdn-acc-in)# **protocol l2tp**
d. Router (config-vpdn-acc-in)# **virtual-template** [*virtual template number*]
e. Router (config-vpdn-acc-in)# **exit**
f. Router (config-vpdn)# **terminate-from hostname** [*hostname*]

Note The host name must match the host name defined in Step 4 of "Task 1. Configure L2TP Information for New Customers (L2TP only)" on page 3-7.

Step 3 Define a local username and password for tunnel authentication:

Router (config)# **username** [*hostname*] **password** [*tunnel password*]

Task 4. Configure Authentication and Authorization

To configure components where user authentication and authorization take place, use one of the following options. (The choice you make depends on your strategy for authentication and authorization.)

- Option 1. Configure Local Authentication on the VHG/PE (L2TP Only).
- Option 2. Configure Authorization and Authentication on the SP AAA RADIUS Server.
- Option 3. Configure Proxy AAA (L2TP Only). Here the SP AAA RADIUS server queries the customer AAA RADIUS server.
- Task 4. On the RADIUS AAA Server, Configure a Per-user Static Route Using the Framed-route Attribute.

Option 1. Configure Local Authentication on the VHG/PE (L2TP Only)

Note Local authentication is not used with direct ISDN PE dial-in.

To configure user authentication and authorization on the VHG/PE, perform the following steps:

Step 1 Create a virtual template:

a. Router (config)# **interface virtual-template** [*number*]

Note The virtual template number must match the virtual template number defined in Step 2d of "Task 2. Configure VRF Information for the Customer Group" on page 3-9.

b. Router (config-if)# **ip vrf forwarding** [*vpn name*]

Note The vpn name must match the vpn name in Step 1a of "Task 2. Configure VRF Information for the Customer Group" on page 3-9.

c. Router (config-if)# **ip unnumbered loopback** [*loopback number*]

Note The loopback number must match the loopback number in Step 2a of "Task 2. Configure VRF Information for the Customer Group" on page 3-9.

d. Router (config-if)# **ppp authentication chap callin**

Step 2 For each user in the customer group, use the following command to configure a username and password:

Router (config)# **username** [*username@domain*] **password** [*user password*]

Option 2. Configure Authorization and Authentication on the SP AAA RADIUS Server

To configure user authentication and authorization on the SP AAA RADIUS server, perform the following steps:

Step 1 Configure the VHG/PE or NAS/PE with information on the MPLS group:

a. Router (config)# **aaa new-model**

b. Router (config)# **aaa authentication ppp default local group radius**

c. Router (config)# **aaa authorization ppp default local group radius**

d. Router (config)# **virtual-profile aaa**

e. Router (config)# **interface virtual-template** [*number*]

Note The virtual template number must match the virtual template number in Step 2d of "Task 2. Configure VRF Information for the Customer Group" on page 3-9.

f. Router (config-if)# **ppp authentication chap callin**

g. Router (config-if)# **exit**

h. Router (config)# **radius-server host** [*radius server ip address*] **key** [*sharedsecret*]

Step 2 Configure the AR with VHG/PE or NAS/PE client information:

a. Add the VHG/PE or NAS/PE as a client:

--> **add /Radius/Clients/**[*vhg name*] [*vhg description*] [*vhg ip address*] [*sharedsecret*] **NAS ""** [*script*]

Note The script indicates which service needs to be selected for VPDN user authorization and authentication.

b. Add the service:

--> **add /Radius/Services/[***vpdn name***] {***vpdn description***] local "" "" RejectAll "" [***vpdn userlist name***]**

Note The VPDN name is derived from the username that is sent by the VHG within the RADIUS access request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm.

c. Add the user list:

--> **add /Radius/Userlists/[***vpdn userlist name***]**

d. Add individual VPDN users for the user list:

--> **add /Radius/UserLists/[***vpdn userlist name***]/[***vpdn username***] [***vpdn user description***] [***vpdn user password***] TRUE "" [***vpdn user attributes***]**

e. Define attributes for selecting the VPN service:

--> **add /Radius/Profiles/[***vpdn user attrbutes***]**

--> **cd /Radius/Profiles/[***vpdn user attrbutes***]/Attributes**

--> **set service-type framed**

--> **set framed-protocol ppp**

--> **set cisco-avpair "lcp:interface-config=ip vrf forwarding [***vpn name***]\\n ip unnumbered Loopback [***number***]**

Note If you are configuring dial backup, see "Option 1. Configure Static Routing" on page 3-18.

Note The vpn name must match the vpn name in Step 1a of "Task 2. Configure VRF Information for the Customer Group" on page 3-9.

Note The loopback number must match the loopback number in Step 2a of "Task 2. Configure VRF Information for the Customer Group" on page 3-9.

Option 3. Configure Proxy AAA (L2TP Only)

To configure proxy AAA, perform the following steps:

Step 1 Configure the VHG/PE:

a. Router (config)# **aaa new-model**

b. Router (config)# **aaa authentication ppp default local group radius**

c. Router (config)# **aaa authorization ppp default local group radius**

d. Router (config)# **virtual-profile aaa**

e. Router (config)# **interface virtual-template** [*number*]

Note The virtual template number must match the virtual template number defined in Step 2d of "Task 2. Configure VRF Information for the Customer Group" on page 3-9.

f. Router (config-if)# **ppp authentication chap callin**

g. Router (config-if)# **exit**

h. Router (config)# **radius-server host** [*radius server ip address*] **key** [*sharedsecret*]

Step 2 Configure the SP AAA RADIUS server:

a. Add the VHG as a client:

--> **add /Radius/Clients/**[*vhg name*] [*vhg description*] [*vhg ip address*] [*sharedsecret*] **NAS ""** [*script*]

Note The script indicates which service needs to be selected for VPDN user authorization and authentication.

b. Add remote AA servers to which you proxy AA information:

--> **add /Radius/RemoteServers/**[*remote server host name*] [*remote server description*] **radius** [*remote server ip address*] **1645 300000** [*sharedsecret*]

Note The remote server IP address cannot be reached from the SP AAA server because the MPLS service provider cloud does not have VPN customer routing information. To provide the SP AAA server with routing information, use route leaking or a management VPN. For information on VPN management refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/index.htm.

c. Add a service:

--> **add /Radius/Services/**[*vpdn name*] [*vpdn description*] **radius**

--> **cd /Radius/Services/**[*vpdn name*]**/RemoteServers**

--> **set 1** [*remote server host name*]

Note The VPDN name is derived from the username that is sent by the VHG/PE in the RADIUS access request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm.

Task 5. Configure Accounting Between the VHG/PE or NAS/PE and the Access Registrar

To configure accounting between the VHG/PE or NAS/PE and the AR, perform the following steps:

Note Make sure you have performed the configuration of the user authentication and authorization on your AAA server, described in "Task 4. Configure Authentication and Authorization" on page 3-10.

Step 1 Configure the VHG/PE.

a. Router (config)# **aaa accounting network default start-stop group radius**

Step 2 Configure the AR.

--> **add /radius/services/[** *accounting service name*]

--> **cd /radius/services/[** *accounting service name*]

--> **set type file**

Note The accounting service name is derived from the username that is sent by the VHG/PE in the RADIUS accounting request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm.

Task 6. Configure Address Management

Configure address management using one of the following procedures. The procedure you select depends on the address management strategy you are using.

- Option 1. Configure Local Overlapping Address Pools on the VHG/PE or NAS/PE
- Option 2. Configure Address Management on the SP AAA RADIUS Server
- Option 3. Configure ODAP on the VHG/PE or NAS/PE
- Option 4. Configure the RADIUS AR for ODAP

Option 1. Configure Local Overlapping Address Pools on the VHG/PE or NAS/PE

To configure address management using local overlapping address pools, perform the following steps on the VHG/PE or NAS/PE:

Step 1 Create an address pool on the VHG/PE:

Router (config)# **ip local pool [***vpn customer address pool***] [***start ip address***] [***end ip address***]**

Step 2 Perform one of the following steps. The step you select depends on how you configured user authentication and authorization in "Task 4. Configure Authentication and Authorization" on page 3-10.

- If you configured user authentication and authorization on the VHG/PE, add the following command to the virtual template configuration:

  Router (config-if)# **peer default ip address pool [***vpn customer address pool***]**

- If you configured user authentication and authorization on the AAA server, add the following command to the attributes for selecting VPN service:

  --> **set cisco-avpair "lcp:interface-config=ip vrf forwarding [***vpn name***]\\n ip unnumbered Loopback[***number***]\\n peer default ip address pool [***vpn customer address pool***]"**

Option 2. Configure Address Management on the SP AAA RADIUS Server

To configure address management on the SP AAA RADIUS server, perform the following steps.

Note Make sure you have performed the accounting configuration in "Task 5. Configure Accounting Between the VHG/PE or NAS/PE and the Access Registrar" on page 3-13. Accounting is mandatory for address management on a RADIUS server.

Step 1 Define the resource manager:

a. --> **add /Radius/ResourceManagers/[***resource manager for vpn customer***]**

b. --> **cd /Radius/ResourceManagers/[***resource manager for vpn customer***]**

c. --> **set type ip-dynamic**

d. --> **set netmask 255.255.255.255**

e. --> **cd IPaddresses**

f. --> **add [***ip address range for address pool***]**

Step 2 Define the session manager:

a. --> **add /Radius/SessionManagers/[***session manager name* **]**

b. --> **cd /Radius/SessionManagers/[***session manager name***]/ResourceManagers**

c. --> **add 1 [***resource manager for vpn customer***]**

Note The session manager name is derived from the domain name that is sent by the VHG/PE in the RADIUS access request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm.

Option 3. Configure ODAP on the VHG/PE or NAS/PE

If you are implementing ODAP, perform the following steps on VHG/PE or NAS/PE.

Step 1 Configure a DHCP address pool on a Cisco IOS DHCP server.

Router(config)# **ip dhcp pool** *address pool name*

Step 2 Tie the pool to a particular VPN.

a. Router(config-dhcp)# **vpn type 1** *vrf name*

b. Router(config-dhcp)# **origin aaa autogrow** *size*

Step 3 Configure the network access server to recognize and use vendor-specific attributes.

a. Router(config)# **radius-server host** *ip address*

b. Router(config)# **radius-server key** *string*

c. Router(config)# **radius-server vsa send accounting**

d. Router(config)# **radius-server vsa send authentication**

Step 4 Enable an address pooling mechanism used to supply IP addresses.

Router(config)# **ip address-pool dhcp-pool**

Step 5 Create a virtual template interface.

Router(config)# **interface virtual-template** *number*

Step 6 Specify an address from the DHCP mechanism to be returned to a remote peer connecting to this virtual-template interface.

Router(config-if)# **peer default ip address dhcp-pool**

Note Since the user name might be the same as the VPDN domain name, either use scripts on the RADIUS AR to differentiate between requests for subnets and VPDN information, or make the VRF name different from the domain name.

Example 3-2 ODAP Configuration Example

```
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius (to release subnets accounting
   needed)
ip dhcp pool odap-test  vrf <vrf-name> (part of access-request username)
origin aaa subnet size initial /27 autogrow /27
radius-server host 10.10.100.3 radius-server key wwradius-server vsa send accounting (VSA
attributes in accounting packet)
radius-server vsa send authentication (VSA attributes in access-request packet)
ip address-pool dhcp-pool (global command – use local DHCP VRF pools)
int virtual-template X
peer default ip address dhcp-pool
```

Option 4. Configure the RADIUS AR for ODAP

To configure the RADIUS AR for ODAP, use a script that accomplishes the following:

- Selects a service with its name ***<vrf name>-odap*** and a session manager with the same name as the service
- Configures the resource manager for ODAP

Cisco AR 1.7 R1 has been enhanced to make ODAP functionality more accessible and to enable ODAP requests and normal user authentication to occur on the same Cisco AR server. To achieve this functionality, a new Cisco vendor script **CiscoWithODAPIncomingScript** was written to direct ODAP requests to particular services and session managers. **CiscoWithODAPIncomingScript** also provides the same functionality as the previous **CiscoIncomingScript**.

Additionally, Cisco AR 1.7 R1 has a new vendor type, **CiscoWithODAP** which references **CiscoWithODAPIncomingScript** as its IncomingScript and references the existing script, **CiscoOutgoingScript,** as its Outgoing Script.

For Cisco AR configuration details, see http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/users/odap.htm#xtocid1.

Task 7. (If You Are Using MLP) Configure LCP Renegotiation and Enable MLP for Users in the Group

If you are implementing MLP, perform the following steps on the VHG/PE or NAS/PE:

Step 1 (L2TP only) On the VHG/PE, configure LCP renegotiation so that requests from the LAC are not rejected. For each customer group, enter these commands on the VPDN group:

a. Router (config)# **vpdn-group** [*number*]

Note The vpdn-group number is the number defined for this group in "Task 3. Configure VPDN Information for the Customer Group (L2TP only)" on page 3-9.

b. Router (config)# **lcp renegotiation always**

Note Without LCP renegotiation, the NAS/LAC might reject MLP requests during initial LCP negotiation between the dial-in user and the NAS/LAC.

Step 2 Use the following command on the virtual template (in L2TP dial-in) or the physical interface or rotary dialer group (in direct ISDN PE dial-in) to enable MLP for users in the group:

Router (config)# **enable mlppp**

Note Enabling MLP is exactly the same in this context as in a non-MPLS environment. For more information, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt9/dcdppp.htm.

Task 8. (If You Are Using MMP) Configure SGBP on Each Stack Group Member

Note To use MMP, you must also implement MLP. See Task 7. (If You Are Using MLP) Configure LCP Renegotiation and Enable MLP for Users in the Group, page 3-16.

If you are implementing MMP, perform the following steps to configure SGBP on each stack group member (VHG/PE or NAS/PE). Do not define more than one stack group on the same router. In this example, you are configuring stack group member C.

Step 1 Define a stack group:

Router (config)# **sgbp group** <*stack-group-name*>

Where <*stack-group-name*> is the name of the stack group. A stack group name is a unique name used for all members of the group.

Step 2 Define the username and the password for stack group member authentication between members of the group:

Router (config)# **user** <*stack-group-name*> **password** <*password*>

Note The username and password must be the same for all members of the group.

Step 3 Specify the host name and IP address of each stack group peer of this router. For each peer (but not for the local system), enter the following command:

Router (config)# **sgbp member** <*peer-name*> <*peer-ip-address*>

Provisioning L2TP Dial Backup

You provision L2TP dial backup in the same way as L2TP dial-in (see "Dial-In Provisioning Checklist" on page 2), with the following differences:

- The same remote CE is used for the primary and the backup link.
- Because dial backup ordinarily connects remote sites, not remote users, to a customer VPN, address assignment is not needed.
- Backup links are typically MLP links, and an IGP routing protocol can be configured on the backup link.
- Static or dynamic routing must be provisioned. Authentication of the remote CE is similar to remote user authentication in L2TP dial-in. If you are managing the CE, the SP AAA server can authenticate the remote CE; proxy authentication is not needed.
- Accounting records, including MLP information, are maintained for the duration of the backup session. As with L2TP dial-in, accounting can be implemented through use of the SP AAA server or AAA proxy.

For more information on dial backup technology, refer to "Dial Backup Configuration" in the *Cisco IOS Dial Technologies Configuration Guide, Release 12.2* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt6/dcdbakdp.htm.

Configuring Routing on a Backup CE-PE Link

In dial backup, either static or dynamic routing can be used, depending on whether dynamic routing is enabled on the primary link.

If dynamic routing is not enabled on the primary link between the CE and the VHG/PE, you must configure static VRF routes for the backup link on the VHG/PE. When the primary link goes down because of lack of connectivity, the primary static route is withdrawn.

For the backup PPP session, the static route is downloaded from the RADIUS AAA server as part of the virtual profile, and the route is inserted into the appropriate VRF when the backup virtual interface is brought up. When the primary link is restored, the primary static VRF route is also restored, and the CE terminates the backup connection. The PE then deletes the backup static VRF route.

If dynamic routing is enabled on the primary CE-PE link, you should configure dynamic routing for the backup link also.

Option 1. Configure Static Routing

Where static routing is used for the backup link, the static route is configured on the SP RADIUS AAA server as part of the virtual profile and downloaded to the VHG/PE. The route is inserted into the appropriate VRF when the backup virtual interface is brought up.

To configure static routing, perform the following steps:

Step 1 On the AAA RADIUS server, modify the Cisco vendor-specific attribute route command. Change:

--> **cisco-avpair "ip:route =** <*nexthop IP address netmask*>*"* (the next hop IP address is optional)

to

--> **cisco-avpair "ip:route = vrf** [vrf-name] <*nexthop IP address netmask*>

Defining the next hop IP address configures static routing. When the CE requests an IP address for the PPP link, the next hop will be set to this address. (If the next hop is not defined, routing is dynamic.)

Step 2 Download the above information to the VHG/PE.

Option 2. Configure Dynamic Routing

Where you have configured dynamic routing on the primary CE-PE link, also configure dynamic routing on the backup VHG/PE.

To configure dynamic routing, perform the following steps on the VHG/PE:

Step 1 Configure a loopback interface to forward traffic to the appropriate VRF:

a. Router (config-if)# **interface loopback 1**

b. Router (config-if)# **ip vrf forwarding [vrf-name]**

Step 2 Assign an address in a.b.c.d format (an IP address on the VHG/PE) to the loopback interface:

Router (config-if)# **ip address** [a.b.c.d] **255.255.255.255**

Step 3 Configure the IGP instance (such as RIP, in this example) for this VRF:

a. Router (config-if)# **router rip**

b. Router (config-if)# **address-family ipv4 vrf [vrf-name]**

Step 4 Make network a.b.c.d part of the IGP:

Router (config-router-at)# **network a.0.0.0**

For example, if the IP address in Step 2 is 10.10.33.241, enter **network 10.0.0.0**.

Step 5 Use a virtual template to download virtual access interface-specific settings from the SP AAA RADIUS server.

a. Add the service:

--> **add /Radius/Services/[***vpdn name***] {***vpdn description***] local "" "" RejectAll "" [***vpdn userlist name***]**

Note The VPDN name is derived from the PPP session username that is sent by the VHG/PE in the RADIUS access request packet. This information is provided by the script in Task 4, Configure Authentication and Authorization, Option 2. Configure Authorization and Authentication on the SP AAA RADIUS Server. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm.

b. Add the user list:

--> **add /Radius/Userlists/[***vpdn userlist name***]**

c. Add individual VPDN users for the user list:

--> **add /Radius/UserLists/[***vpdn userlist name***]/[***vpdn username***] [***vpdn user description***] [***vpdn user password***] TRUE "" [***vpdn user attrbutes***]**

d. Define attributes for selecting the VPN service:

--> **add /Radius/Profiles/[***vpdn user attrbutes***]**

--> **cd /Radius/Profiles/[***vpdn user attrbutes***]/Attributes**

--> **set service-type framed**

--> **set framed-protocol ppp**

--> **set cisco-avpair "lcp:interface-config=ip vrf forwarding [***vpn name***]\\n ip unnumbered Loopback [***number***]**

Note The vpn name must match the vpn name in Step 1a of "Task 2. Configure VRF Information for the Customer Group" on page 3-9. The loopback number must match the loopback number in Step 2a of "Task 2. Configure VRF Information for the Customer Group" on page 3-9. The virtual interface should be unnumbered to the loopback interface.

Note If you are using a third-party RADIUS server, use the PPP session username to select the RADIUS record. The RADIUS record should contain the attributes in the **set cisco-avpair** command above.

Provisioning Dial-out Access

Provisioning dial-out access is similar to provisioning dial-in access, with these exceptions:

- For users to be able to place dial-out calls, you must configure dialer profiles on the VHG/PE (in L2TP dial-out) or on the NAS/PE (in direct ISDN PE dial-out).
- No AAA RADIUS configuration is needed, because user information is directly implemented on the dialer profile interface configured on the dial-out router.

Before You Begin

The procedures provided here are specific to provisioning remote access to an MPLS VPN and are based on two assumptions:

1. That the following setup and configuration tasks have already been carried out:
   - Setup of the MPLS core network
   - Setup of the customer VPN
   - Configuration of the links between the PE and the CE

2. That you have a good understanding of the architecture and features you are using and that you have selected the means you will use for implementing those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

See Chapter 2, "Overview of Dial Access to MPLS VPN Integration" for information that will help you understand the dial architectures and decide on your implementation approach.

Dial-Out Provisioning Checklist

Table 3-4 lists tasks for dial-out provisioning. Procedures for completing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 3-4 Checklist of Tasks for Dial-out Provisioning

	Task	L2TP Dial-Out	Direct ISDN PE Dial-Out
	Before you begin, read the Cisco Remote Access to MPLS VPN Integration 2.0 Release Notes at http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/rampls2/relnote/index.htm		
	Task 1. Configure the Dialer Profile.	On the VHG/PE	On the NAS/PE
	Task 2. Configure the VPDN Group (L2TP Only).	On the VHG/PE	—
	Task 3. Configure a Static Route in the Customer VRF.	On the VHG/PE and On the NAS	On the NAS/PE
	Task 4. Configure VPDN on the NAS (L2TP only).	On the NAS	—

Miscellaneous Component Configurations

For miscellaneous component configuration details, see Table 3-2.

Task 1. Configure the Dialer Profile

In this task, you configure a dialer profile (on the VHG/PE or NAS/PE) to be part of the customer VRF. In L2TP dial-out, you also configure the dialer profile to use a VPDN group.

Step 1 On the VHG/PE or NAS/PE, include the following command in the dialer profile:

Router (config-if)# **ip vrf forwarding** [*vpn name*]

Step 2 (L2TP only) On the VHG/PE, include the **dialer vpdn** command in the dialer profile to configure the dialer profile for L2TP:

Router (config-if)# **dialer vpdn**

In Example 3-3, the commands listed above are in bold. The dialer profile defined is Dialer50. The vpn name is V1.17.com. The dialer pool number, 4, is referenced in the configuration of the VPDN group in Task 2.

Example 3-3 VHG/PE Dialer Profile Configuration (L2TP dial-out)

```
interface Dialer50
 ip vrf forwarding V1.17.com
 ip unnumbered Loopback172
 encapsulation ppp
 no keepalive
 dialer pool 4
 dialer remote-name U0001N1P4V1.17@V1.17.com
 dialer idle-timeout 200000
 dialer string 11710
 dialer load-threshold 5 either
 dialer vpdn
 dialer-group 1
 peer default ip address 42.1.17.10
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname dialout
 ppp chap password 7 071836
 ppp multilink
 multilink load-threshold 5 outbound
end
```

Note The **dialer-group** command specifies which dialer list to use. In the example, dialer-group 1 is linked to **dialer-list 1 protocol ip permit**, a global command that, like an access list, tells the router which traffic (in this case, all IP traffic) will trigger the dialer profile and thus the call. Alternatively, you can use an access list to filter out routing updates or allow only HTTP traffic (URL requests) to trigger a call.

For more information on configuring dialer profiles, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt5/dcdiprof.htm.

Task 2. Configure the VPDN Group (L2TP Only)

This task applies to L2TP dial-out only. In this task, you configure the VPDN group as a pool member of the dialer pool defined in the dialer profile in Task 1.

On the VHG/PE, use the following command to configure the VPDN group as a pool member:

Router (config-vpdn-group)# **pool-member** [*pool number*]

In Example 3-4, the pool-member corresponds to the pool number in the dialer profile configured in Task 1.

Example 3-4 VHG/PE VPDN Group Configuration

```
vpdn-group V1.17
    request-dialout
        protocol l2tp
        pool-member 4
    initiate-to ip 10.10.104.36
    local name c72d2-2-V1.17
    source-ip 10.10.104.12
    l2tp tunnel password <password>
```

The **l2tp tunnel password** command overrides the default password in the local user database. You can also define a username for the local name in the global configuration. To do so, use this command: Router (config)# **username c72d2-2-V1.17 password <password>**

Task 3. Configure a Static Route in the Customer VRF

In this task, you configure the customer VRF (on the VHG/PE or NAS/PE) with a static route for this dial-out user. This will attract traffic to the appropriate remote CE.

On the VHG/PE, in the customer VRF use this command to configure a static route for this dial-out user:

Router (vrf)# **ip route vrf [vpnname][CE ip address] 255.255.255.255 Dialer50 permanent**

Task 4. Configure VPDN on the NAS (L2TP only)

Perform the following steps to configure VPDN for dial-out on the NAS. See Example 3-5 for a configuration example.

Step 1 Enable VPDN:

Router (config)# **vpdn enable**

Step 2 Configure the VPDN group to accept dial-out (when the VHG/PE requests a tunnel and attempts to trigger a session):

a. Router (config)# **vpdn-group** [*number*]

b. Router (config-vpdn)# **accept-dialout**

c. Router (config-vpdn-acc-out)# **protocol l2tp**

Router (config-vpdn-group-acc-out)# **dialer 1**

Note dialer 1 specifies the dialer that is used to dial out to the client.

d. Router (config-vpdn-acc-out)# **exit**

e. Router (config-vpdn)# **terminate-from hostname** [*hostname*]

Note L2TP tunnels that have this hostname will be accepted.

Step 3 Configure the tunnel secret to be used for VPN tunnel authentication for this VPDN group:

Router (config)# **l2tp tunnel password** [*tunnel password*]

Note The secret must match that used in the VPDN group on the VHG/PE or the entry in the local user password database.

Step 4 On the dialer interface, enable dial-on-demand routing:

Router (config-if)# **dialer aaa**

Note This enables the dialer to use the AAA server to locate the profiles to use for dialing information. When the VHG/PE sends dialer string attributes, the rotary group will trigger the call.

Step 5 On the physical dialer interface, use this command to reference the rotary group dialer 1:

Router (config)# **interface serial** [*physical dialer interface*]

Router (config-ip)# **dialer rotary-group 1**

Example 3-5 NAS VPDN Group Configuration

```
vpdn enable

vpdn-group V1.17
    accept-dialout
    protocol l2tp
    dialer 1

/*Specifies the dialer that is used to dial out to the client. */

terminate-from hostname c72d9-1-V1.4

/*Accepts L2TP tunnels that have this host name configured as a local name. */

l2tp tunnel password 7 <password>

/*Configures the tunnel secret that will be used for VPN tunnel authentication for this
VPN group. This password must match that configured in Task 2 in the VPDN group on the
VHG/PE or the entry in the local user password database.*/

source-ip 10.10.104.22
!
interface Dialer1
 ip unnumbered Loopback0
 encapsulation ppp
 no keepalive
 dialer in-band

/*Enables DDR on Dialer */

 dialer aaa

/* Enables the dialer to use the AAA server to locate profiles for dialing information. */

 dialer-group 1
 no cdp enable
 ppp authentication chap callin
!
```

Sample Configurations

This section includes sample configurations. The examples are presented as illustrations only; your configuration specifics depend on how you are implementing remote access to MPLS VPN and will vary from what is presented here. The relevant commands for remote access to MPLS VPN are in bold and are described in italicized comments.

Sample Configurations for L2TP Dial-In

Sample NAS Configuration

On the NAS, you configure the VPDN group that will bring up the L2TP tunnel to the VHG/PE.

Note All MPLS VPN-relevant commands are configured on the VHG/PE, not the NAS.

Example 3-6 NAS Sample Configuration

```
Router# show run
version 12.2
no service pad
service tcp-keepalives-in
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname c54d2-1
!
enable secret <password>.
enable password <password>
!
username c54d2-1-V1.1 password 0 ww
resource-pool disable
call rsvp-sync
dial-tdm-clock priority 1 6/0
!
!
! - VPDN configuration:
vpdn enable
vpdn search-order domain dnis
! - Look up VPDN by domain and then by DNIS
!
! - Configuration for a VPDN group (in this example, V1.1):
vpdn-group V1.1
  request-dialin
    protocol l2tp
    domain V1.1.com
initiate-to ip 10.10.104.12
local name c54d2-1-V1.1
! - Name used on this NAS, used on VHG in terminate-from hostname c54d2-1-V1.1
source-ip 10.10.104.36
! - Loopback interface
!
controller E1 6/0
pri-group timeslots 1-31
!
interface Loopback0
ip address 10.10.104.36 255.255.255.255
!
interface FastEthernet0/0
ip address 10.10.145.3 255.255.255.0
!
interface Serial6/0:15
no ip address
encapsulation ppp
dialer rotary-group 1
isdn switch-type primary-net5
ppp authentication chap callin
!
interface Dialer1
ip unnumbered Loopback0
encapsulation ppp
no ip route-cache
no ip mroute-cache
```

```
dialer in-band
ppp authentication chap callin
!
router ospf 100
log-adjacency-changes
network 10.10.0.0 0.0.255.255 area 0
!
ip classless
no ip http server
ip pim bidir-enable
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
logging synchronous
line vty 0 4
exec-timeout 0 0
login
!
end
```

Sample VHG/PE Configuration

In this example, the VHG/PE is configured to terminate L2TP sessions received from the NAS and query the RADIUS server for dial options authorized for a given dial-in user.

Example 3-7 VHG/PE Sample Configuration

```
Router# sh run
version 12.2
service tcp-keepalives-in
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
hostname c72d2-2
! - RADIUS request:
aaa new-model
aaa authentication login default none
aaa authentication ppp default local group radius
! - Look for user name in local database, if not found, look on RADIUS
aaa authorization network default local group radius
! - Similarly for network authorization
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa session-id common
enable secret <password>
enable password <password>
!
! - Authenticate user and L2TP tunnel locally:
username c72d2-2 password 0 ww
( since no local name defined on vpdn group in this example the VHG/PE will use its
hostname as the username in the L2TP authentication process for the tunnel)
ip subnet-zero
!
!
ip vrf V1.1.com
rd 1:1
route-target export 1:1
```

```
route-target import 1:1
!
vpdn enable
vpdn search-order domain dnis
!
! - Bind the user coming from NAS c54d2-1-V1.1 to this profile (V1.1.) and use virtual
template 1:
vpdn-group V1.1
   accept-dialin
      protocol l2tp
      virtual-template 1
terminate-from hostname c54d2-1-V1.1
lcp renegotiation always
source-ip 10.10.104.12
! - Note that the VHG/PE clones a virtual access interface (a set of generic IOS commands)
from the specified virtual template. If per-user configuration is also used (through the
virtual-profile aaa command), the VHG/PE queries the RADIUS server to authenticate the PPP
user with a username and password.
!
tag-switching tdp router-id Loopback0
!
interface Loopback0
ip address 10.10.104.12 255.255.255.255
!
interface Loopback1
ip vrf forwarding V1.1.com
ip address 42.1.1.241 255.255.255.255
!
interface FastEthernet0/0
ip address 10.10.145.1 255.255.255.0
!
interface POS5/0
ip address 10.10.103.33 255.255.255.252
tag-switching ip
!
! - Configuration from the template; multilink is enabled
interface Virtual-Template1
no peer default ip address
ppp authentication chap callin
ppp multilink
!
router ospf 100
log-adjacency-changes
network 10.10.0.0 0.0.255.255 area 0
!
router bgp 100
no synchronization
bgp log-neighbor-changes
neighbor 10.10.104.31 remote-as 100
neighbor 10.10.104.31 update-source Loopback0
neighbor 10.10.104.31 soft-reconfiguration inbound
neighbor 10.10.104.35 remote-as 100
neighbor 10.10.104.35 update-source Loopback0
no auto-summary
!
address-family ipv4 vrf V1.1.com
redistribute connected metric 1
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.10.104.31 activate
neighbor 10.10.104.31 send-community extended
```

```
neighbor 10.10.104.35 activate
neighbor 10.10.104.35 send-community extended
no auto-summary
exit-address-family
!
ip local pool V1.1-pool 42.1.1.10 42.1.1.19 group V1.1-group

ip classless
!
ip radius source-interface Loopback0
! - The IP source is changed to the loopback interface
!
radius-server host 10.10.100.6 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key ww
call rsvp-sync
mgcp profile default
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
!
end
```

Sample SP AAA Server Configuration

In this example, the SP AAA server is configured to:

- Add the VHG/PE as a RADIUS client
- Add a RADIUS service specifying that the list of users is found in a local database
- Add a user list and users to populate the database
- Add attributes for those users, to be provided (in the access-accept packet) upon request from the VHG/PE. Attributes can also come from the customer AAA server

In the example, you are assumed to be logged in to the RADIUS host and to have accessed the Access Registrar application.

Note Be sure that you save and reload after changing the Access Registrar configuration.

Example 3-8 SP AAA Sample Configuration

```
--> cd     c72d2-2
[ //localhost/Radius/Clients/c72d2-2 ]
    Name = c72d2-2
    Description = c72d2-2
    IPAddress = 10.10.104.12
    SharedSecret = ww
    Type = NAS
    Vendor =
    IncomingScript~ = ParseAAARealm
    OutgoingScript~ =
    UseDNIS = FALSE
    DeviceName =
    DevicePassword =
```

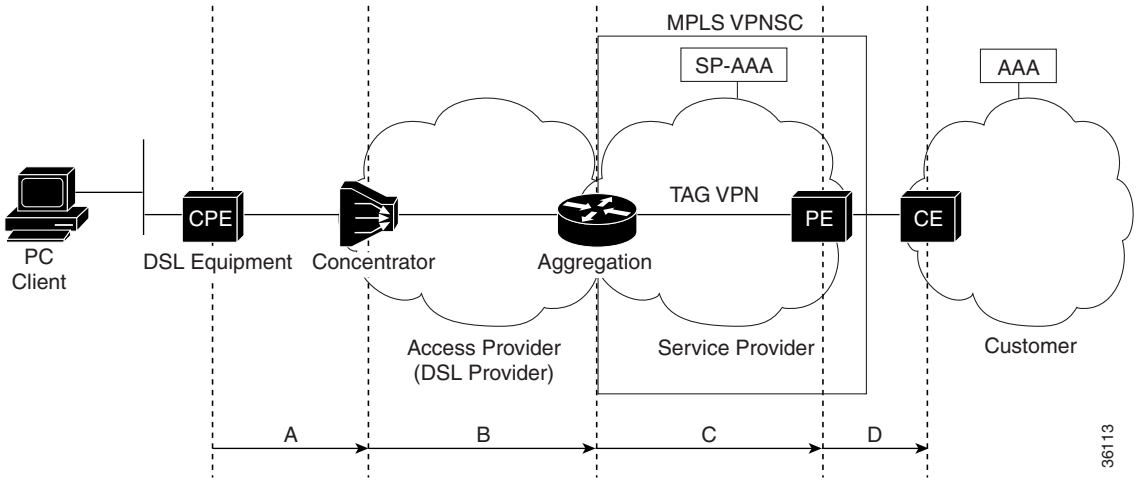
```
--> cd /radius/scripts/ParseAAARealm

[ //localhost/Radius/Scripts/ParseAAARealm ]
    Name = ParseAAARealm
    Description = "Parse out the @<realm> from the User-Name and use it as the name of the
    AAA Service that should handle this request"
    Language = Rex
    Filename = librexscript.so
    EntryPoint = ParseAAARealm
    InitEntryPoint =
    InitEntryPointArgs =

--> cd /radius/services/V1.1.com

[ //localhost/Radius/Services/V1.1.com ]
    Name = V1.1.com
    Description = V1.1.com
    Type = local
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    UserList = V1.1.com

--> cd /radius/userlists/V1.1.com

[ //localhost/Radius/UserLists/V1.1.com ]
    Entries 1 to 4 from 4 total entries
    Current filter: <all>

    Name = V1.1.com
    Description =
    U0001N1P4V1.1/

--> cd U0001N1P4V1.1

[ //localhost/Radius/UserLists/V1.1.com/U0001N1P4V1.1 ]
    Name = U0001N1P4V1.1
    Description = U0001N1PV1.1@V1.1.com
    Password = <encrypted>
    AllowNullPassword = FALSE
    Enabled = TRUE
    Group~ =
    BaseProfile~ = V1.1.com-attrib
    AuthenticationScript~ =
    AuthorizationScript~ =
    UserDefined1 =

--> cd /radius/profiles/V1.1.com-attrib

[ //localhost/Radius/Profiles/V1.1.com-attrib ]
    Name = V1.1.com-attrib
    Description =
    Attributes/

--> cd attributes

[ //localhost/Radius/Profiles/V1.1.com-attrib/Attributes ]
    cisco-avpair = "lcp:interface-config=ip vrf forwarding V1.1.com \n ip unnumbered
Loopback1 \n peer default ip address pool V1.1-pool"
    framed-protocol = ppp
    service-type = framed
```

DSL Access to MPLS VPN Integration

In a DSL solution, a session initiated by a client, through DSL equipment (CPE), as depicted in Figure 4-1 is:

1. Transmitted to a digital subscriber line access multiplexer (DSLAM) in the access provider network cloud
2. Distributed to an aggregation router within the same access provider network cloud where the PPP session is terminated and IP traffic is subsequently placed on one of the many tunnels that starts at the provider edge (PE) equipment in the service provider cloud
3. Tunneled through the access provider network cloud
4. Redistributed or delivered to the customer edge (CE) equipment as the final destination in the customer network cloud

Figure 4-1 DSL Access to MPLS VPN



DSL Access Methods

Methods of DSL access (network environment architectures) covered in this Cisco VPN Dial Access to MPLS solution include:

- RFC 1483 Routing Integration, page 4-2
- RFC 1483 Routed Bridge Encapsulation to MPLS VPN Integration, page 4-8
- PPPoX Remote Access SSG to MPLS VPN Integration, page 4-19
- PPPoX Remote Access to MPLS VPN Integration, page 4-30
- DSL L2TP to MPLS VPN Integration, page 4-40

These access methods are described in the following sections. Each section includes an overview of the architecture, a description of the solution components, and procedures for configuring the solution. Some configuration tasks can be expedited by using VPN Solution Center 2.1 templates. For details, see Using Templates for Configuration, page 4-61.

RFC 1483 Routing Integration

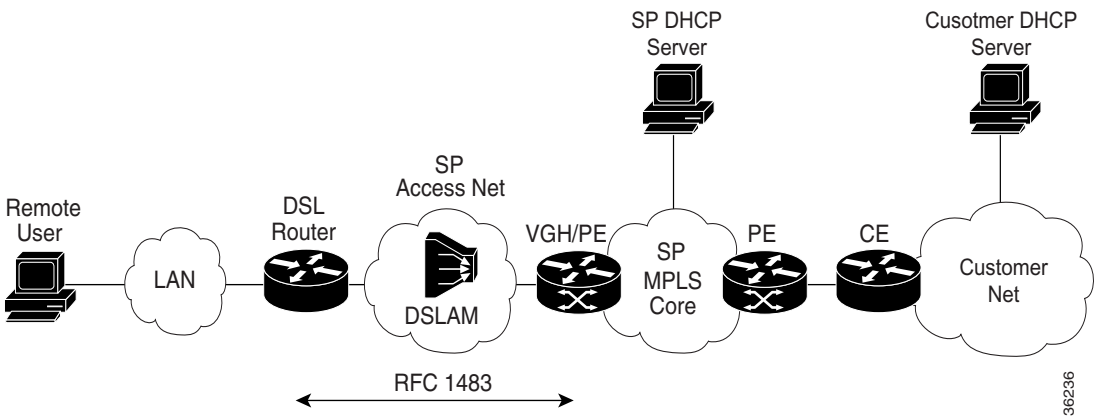
RFC 1483 DSL remote access routing provides connectivity between the Digital Subscriber Line (DSL) router and the Virtual Home Gateway/Provider Edge (VHG/PE). At the VHG/PE, the RFC 1483 interface is statically configured with a specific VRF (see Figure 4-2). Multiple IP subnets can be configured at the customer site and dynamic IP routing protocols can run between the DSL Router and the VHG/PE.

A Cisco DSL router is attached to a LAN connecting to a remote site's host PCs, and used as the customer premise equipment (CPE) to connect the remote access network to the SP DSL access network. The supported DSL routers are the Cisco 82x series, 14xx series, or SOHO77.

There is no remote user authorization and authentication with this RFC 1483 routing solution. Factors such as address assignment being DHCP-based, and accounting being Netflow-based make RFC 1483 routing more suitable for remote office, rather than residential user, connectivity to a MPLS VPN. See RFC 1483 Core Network, page 4-4 for additional considerations.

IP routing protocols can be configured over the RFC 1483 PVC (permanent virtual circuit) which is useful when connecting remote offices with multiple subnets to the VPN.

Figure 4-2 Cisco VPN RFC 1483 DSL access to MPLS.



RFC 1483 VHG/PE Routers

The following VHG/PE platforms are used in Cisco VPN RFC 1483 remote access to MPLS.

- Cisco 6400 NRP1 and NRP2.
- Cisco 7200 NPE-300 and NPE-400
- Cisco MGX 8850 with route processor module (RPM-PR)

The service provider access network is DSL with Cisco 6xx0 DSLAMs. RFC 1483 routing supports IP MPLS and ATM MPLS core networks.

RFC 1483 DHCP Server

DHCP (dynamic host configuration protocol) is used for address assignment through a Cisco Network Registrar (CNR) DHCP server for Cisco VPN RFC 1483 DSL access to MPLS.

Address Management

The DHCP server assigns public and private addresses from a common service provider's address pool to all remote users regardless of the VPN they belong to. The DSL router and the VHG/PE interfaces must have IP addresses. Private addresses can be assigned from the service provider's private pool, if interfaces are reachable from other PE routers connected to the same VPN.

Note The service provider DHCP server does not support overlapping addresses and is not VPN aware.

The DHCP server can dynamically assigning addresses, to enable route summarization by assigning contiguous addresses to requests coming from the same DSL or VHG/PE router.

The following options exist for CPE address management.

- CPEs can have statically assigned addresses.
- A CPE can request an IP address using DHCP.
- The DHCP server can be local. In many cases the DSL router is configured as a DHCP server.
- The DSL Router can relay the request to a DHCP server in the VPN. The VPN DHCP router must be configured for remote user address assignment, for route summarization.

  Note The DSL router cannot relay the DHCP request to the DHCP server. It relays the request to the next hop, the VHG/PE routers, which relays it again to the DHCP server.

- The VHG/PE router relays the DHCP request to a service provider DHCP server, or a VPN DHCP server.

Accounting

Netflow is used for Cisco VPN RFC 1483 access to MPLS accounting. On the PE routers, Netflow is used to provide per flow usage accounting. The Netflow Collector provides Netflow usage data collection statistics such as time of first packets, time of last packet, number of packets, and number of octets used for performance reporting, capacity planning, and usage based billing. VPNSC collects the usage records from the Netflow Collector(s) and correlates them with the VPN service layer information.

A flow is identified by source address, source port, destination address, destination port, and more. When configured for Netflow accounting, the VHG/PE collects per flow accounting data and exports it to a Netflow Collector workstation, which stores it in flat files. A Netflow Analyzer is then used for analyzing the collected data.

RFC 1483 Core Network

Network management, fault monitoring, and SLA reporting are management functions performed in the core network.

Network Management

Network management components for RFC 1483 consist of the following:

- **Element managers:** Service Connection Manager (SCM) for the 6400 and CDM (with CPE management extensions) for the DSLAMS and the DSL routers at the CPE.
- **VPNSC:** for VPN service provisioning, auditing, SLA monitoring and accounting. VPNSC also uses Cisco IP Manager (CIPM) for configuration downloads/uploads.
- **Netflow:** for usage accounting of non-PPP connections.
- **Cisco Info Center (CIC):** for VPN fault monitoring.
- **Concord Network Health:** for VPN performance reporting.

Fault Monitoring

Fault monitoring is performed at the device, and service levels.

At the device level, fault monitoring is performed by the element managers (CEMF has an event manager component). CAM provides fault monitoring per dial port.

CIC is user at the service level to provide event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems. CIC is an OEM product from Micromuse's NetCool. CIC's release 2.0 provides eventing at the IP VPN service level through integration with VPNSC.

SLA Reporting

SLA reporting is performed using the Service Assurance Agent (SA Agent) in IOS. At conventional MPLS VPN customer sites, VPNSC configures the SA Agent probes on managed CE routers, or shadow CE routers. At remote access sites, there is no real CE router so the SA Agent probes are configured on the PE routers at the PoPs. It is not possible to configure them on the NASs, because a NAS is not connected to a specific VPN so the probes are not routed using the VRFs. VPNSC collects statistics from the SA Agent MIB, and provides reports on a per VPN basis. For PPP users, performance numbers are derived from AR. For RFC 1483, the SA Agent probes are configured on the DSL routers at the CPE.

Performance and SLA reporting can be provided at a VPN service level through integration with VPNSC. RPMS is used to provide SLA information regarding incoming call rates per VPN customer.

RFC 1483 Provisioning

Provisioning Cisco VPN RFC 1483 DSL access to MPLS entails:

1. Initial non-VPN services configurations performed through router pre-staging using config Xpress, an element manager (for example, SCM), CIPM templates, or any combination of these tools that include:
   a. configuring the VHG/PE
   b. configuring the DSLAMS using CDM
2. Customer and service configurations that include:
   a. configuring the CNR servers
   b. configuring the RFC 1483 PVCs on PE routers, using VPNSC 2
   c. configuring the PE router for a new service by adding the required VRF configuration and DHCP helper addresses, using VPNSC 2

Note The DCHP helper address is only required for DHCP relay from the CPE device.

3. VPN service configurations that include:
   a. actual service activation performed by VPNSC where a VPN is created and CE sites and remote access sites are added to it.

Note For VPNSC configuration, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Configuring the VHG/PE

Perform the following steps to configure the VHG/PE.

Note On the Cisco 6400, you can use SCM to perform configuration.

Step 1 Define loopbacks.

a. Router (config)# **interface loopback [***number***]**

b. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Commands in a and b create a general loopback interface used for reachability to the router and are used as a source IP address for sessions (IBGP, TDP, etc.).

c. Router (config-if)# **interface loopback** [*number*]

d. Router (config-if)# **ip vrf forwarding** [*vpn name*]

e. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Commands c, d, and e create a loopback interface in a VRF necessary only if you use ip unnumbered interfaces to the CE device when you would ip unnumber the interface to this loopback. These steps are repeated for each customer VRF you ip unnumber interfaces to.

Step 2 Define PVCs.

a. Router (config)# **interface ATM**[*interface]***/**[*interface]***/**[*interface]***.[***number***] point-to-point** (for the Cisco 6400). For example, **interface ATM0/0/0.1 point-to-point**
Router (config)# **interface ATM[***slot***]/**[*port*]**.[***number***] point-to-point** (for the Cisco 7200). For example, **interface ATM0/0.1 point-to-point**
Router (config)# **interface Switch [***switchnumber***].[***number***] point-to-point** (for the Cisco MGX 8850 RPM-PR). For example, **interface Switch 1.1 point-to-point**

b. Router (config-if)# **ip unnumbered Loopback [***number***]**

c. Router (config-if)# **pvc [***vpi/vci number***]**

d. Router (config-if-pvc)# **encapsulation aal5snap**

Step 3 Use the following global command to configure label switching on the interface connected to the MPLS cloud:

a. Router (config)# **ip cef**

For connecting to a MPLS cloud using MPLS ATM tagging, use the following commands:

a. Router (config-if)# **interface ATM0/0/0.**[*number*] **mpls**

b. Router (config-if)# **ip address** [*ip address*]

c. Router (config-if)# **tag-switching atm vp-tunnel** [*number*]

d. Router (config-if)# **tag-switching ip**

For frame-based tagging, the equivalent commands would be:

a. Router (config-if)# **interface ATM0/0/0.**[*number*]

b. Router (config-if)# **ip address** [*ip address*]

c. Router (config-if)# **tag-switching ip**

Step 4 Configure the VRF for each VPN.

a. Router (config)# **ip vrf [***vpn name***]**

b. Router (config-vrf)# **rd [***route descriptor***]**

c. Router (config-vrf)# **route-target export [***route target communities***]**

d. Router (config-vrf)# **route-target import [***route target communities***]**

Note You need two route descriptors, for send and receive.

Step 5 Configure a dedicated PVC for each VPN (PTA-MD).

a. Router (config)# **interface ATM0/0/0.[***number***] point-to-point**

b. Router (config-if)# **ip vrf forwarding [v***pn name***]**

c. Router (config-if)# **ip address [i***p address***]**

d. Router (config-if)# **pvc [***vpi/vci numbers***]**

e. Router (config-if-pvc)# **encapsulation aal5snap**

Step 6 Configure BGP to advertise the networks for each VPN.

a. Router (config)# **router bgp [***autonomous system number of sp***]**

b. Router (config-router)# **neighbor [***ip address of remote pe***] remote-as [***same autonomous number***]**

c. Router (config-router)# **neighbor [***ip address of remote pe***] update-source Loopback0**

d. Router (config-router)# **address-family vpnv4**

e. Router (config-router-af)# **neighbor [***ip address of remote pe***] activate**

f. Router (config-router-af)# **neighbor [***ip address of remote pe***] send-community extended**

Step 7 If using static routes, define them and redistribute them into BGP.

Configuring the DSLAM using CDM

Perform the following step to configure the DSLAMS using CDM.

Step 1 Create subscriber properties, including VPI/VCI pairs.

For Cisco DSL Manager (CDM) configuration details, refer to

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cdm/cdm33/index.htm

Configuring CNR Network Server

A Cisco 82x series, 14xx series, or SOHO77 router is configured to forward DHCP requests unaltered to the VHG/PE for DHCP relay. If the VHG/PE interface is a numbered interface with the ip-helper command configured, the GIADDR field of the DHCP discover packet is set to the IP address of the VHG/PE interface. This allows the DHCP scope to be provisioned on the CNR server accordingly.

If the VHG/PE interface is unnumbered to a loopback interface, the GIADDR field of the DHCP discover packet is set to the IP address of the loopback interface. If several interfaces are unnumbered to the same loopback interface, the CNR server relies on the client MAC address to determine the correct IP address to supply. This entails configuring client class processing on the CNR server.

For Cisco Network Registrar (CNR) configuration details, refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/nr3-5/index.htm

Configuring the RFC 1483 PVCs on PE routers

For VPNSC configuration details, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Configuring the PE Router for a New Service

For VPNSC configuration details, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

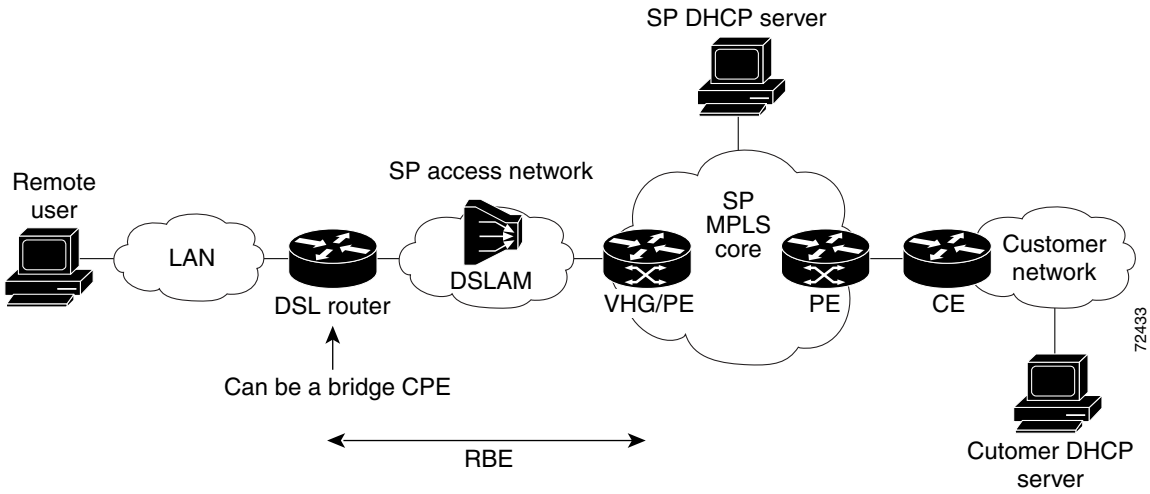
RFC 1483 Routed Bridge Encapsulation to MPLS VPN Integration

ATM routed bridge encapsulation (RBE) routes IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN. Bridged IP packets received on an ATM interface configured in routed-bridge mode are routed via an IP header. The interface takes advantage of the characteristics of a stub LAN topology commonly used for DSL access and offers increased performance and flexibility over integrated routing and bridging (IRB).

In Figure 4-3, RBE is configured between the DSL router and the VHG/PE. The DSL router can be set up as a pure bridge or can be set up for IRB, where multiple LAN interfaces are bridged through the bridge group virtual interface (BVI). Each of the DSL routers terminates on a separate point-to-point subinterface on the VHG/PE which is statically configured with a specific VRF. Remote user authentication or authorization is available with Option 82 for DSL routed bridge encapsulation remote access.

RBE treats the VHG/PE subinterface as if it were connected to an Ethernet LAN, but avoids the disadvantages of pure bridging such as broadcast storms, IP hijacking, and ARP spoofing issues. Address management options include static and VRF-aware DHCP servers. Since this architecture is not PPP based, RADIUS accounting cannot be used. Netflow is used for accounting.

Figure 4-3 Cisco VPN DSL RBE to MPLS Integration



RBE References

For a description of RBE architecture, refer to:
http://www.cisco.com/warp/public/794/routed_bridged_encap.html.

For RBE IOS commands, refer to
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122csum/csum2/122cswan/wsfbrda.htm#1051874

For platform-specific overview and configuration information, refer to:

ATM Routed Bridge Encapsulation Feature Overview - Cisco 6400 series:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc5/atm_rb.htm

ATM Routed Bridge Encapsulation Feature Overview - Cisco 7200 series:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtatmrbe.htm

RBE VHG/PE Routers

The following VHG/PE platforms are used in Cisco RFC 1483 RBE remote access to MPLS.

- Cisco 6400 NRP1 and NRP2.
- Cisco 7200 NPE-300 and NPE-400

The service provider access network is DSL with Cisco 6xx0 DSLAMs. RFC 1483 RBE supports ATM MPLS core networks.

RBE DHCP Server

DHCP (dynamic host configuration protocol) is used for address assignment through a Cisco Network Registrar (CNR) DHCP server.

Address Management

The DHCP server assigns public and private addresses from a common service provider's address pool to all remote users regardless of the VPN they belong to. The DSL router and the VHG/PE interfaces must have IP addresses. Private addresses can be assigned from the service provider's private pool, if interfaces are reachable from other PE routers connected to the same VPN.

Note The service provider DHCP server does not support overlapping addresses and is not VPN aware.

The DHCP server can dynamically assigning addresses, to enable route summarization by assigning contiguous addresses to requests coming from the same DSL or VHG/PE router.

The following options exist for CPE address management.

- CPEs can have statically assigned addresses.
- A CPE can request an IP address using DHCP.
- The DHCP server can be local. In many cases the DSL router is configured as a DHCP server.
- The DSL router can relay the request to a DHCP server in the VPN. The VPN DHCP router must be configured for remote user address assignment, for route summarization.

  Note The DSL router cannot relay the DHCP request to the DHCP server. It relays the request to the next hop, the VHG/PE routers, which relays it again to the DHCP server.

- The VHG/PE router relays the DHCP request to a service provider DHCP server, or a VPN DHCP server.

Authorization and Authentication

DHCP is used primarily to assign IP addresses to one or more customer premise hosts for public Internet access. The DHCP Relay Agent Information Option resides at the end of a DHCP message. As it relays a DHCP message, the PE can append a VPN-ID into Option 82 of the relayed message so that the VPN context can be presented to the DHCP server. The VPN enhanced DHCP server then receives this request, and uses the VPN-ID that is contained in the Option 82 field to determine from which VPN to allocate an address. Then, the DHCP server responds to the DHCP Relay Agent (the PE).

The DHCP Option 82 Support for Routed Bridge Encapsulation feature provides support for the DHCP relay agent information option when routed bridge encapsulation (RBE) is used. Figure 4-4 shows a typical network topology in which RBE and DHCP are used. The router that is using RBE is also serving as the DHCP relay agent.

Figure 4-4 Network Topology Using RBE and DHCP

The PE router also adds an Option 82 to the request being relayed. Option 82 is used to indicate:

- whether the request came from a host PC or a cable modem (suboption 1)
- carry the MAC address of the BBFW interface of the PE (suboption 1)
- if the request is from a host PC, the MAC address of the BBFW modem/router is included in suboption 2.

Figure 4-5 shows the format of the agent remote ID suboption.

Figure 4-5 Format of the Agent Remote ID Suboption

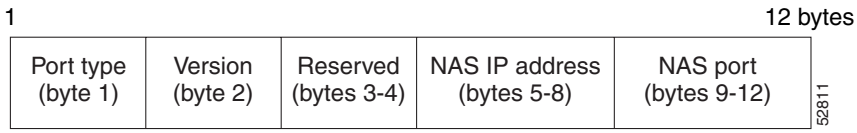


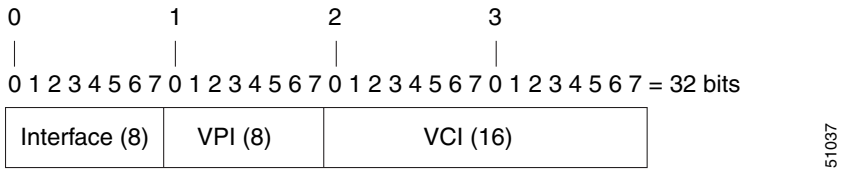
Table 4-1 describes the agent remote ID suboption fields displayed in Figure 4-5.

Table 4-1 Agent Remote ID Suboption Field Descriptions

Field	Description
Port Type	Port type. The value 0x01 indicates RBE. (1 byte)
Version	Option 82 version. The value 0x01 specifies the RBE version of Option 82. (1 byte)
Reserved	Reserved. (2 bytes)
NAS IP Address	Identifies the relay agent/LAC from which this DHCP request is coming in. On the Cisco 6400 platform, this IP address is the management IP address of NSP. On non Cisco 6400 platforms, this is the IP address of the interface pointed by the **rbe nasip** command.(4 bytes)
NAS Port	Identifies the RBE-enabled virtual circuit through which this DHCP request has come in. See Figure 4-6 for the format of this field. (4 bytes)

Figure 4-6 shows the format of the network access server (NAS) port field in the agent remote ID suboption.

Figure 4-6 Format of the NAS Port Field



Use the Cisco IOS **ip dhcp relay information option** global configuration command to activate the Option-82 feature.

Accounting

Netflow is used for accounting. On the PE routers, Netflow is used to provide per flow usage accounting. The Netflow Collector provides Netflow usage data collection statistics such as time of first packets, time of last packet, number of packets, and number of octets used for performance reporting, capacity planning, and usage based billing. VPNSC collects the usage records from the Netflow Collector(s) and correlates them with the VPN service layer information.

A flow is identified by source address, source port, destination address, destination port, and more. When configured for Netflow accounting, the VHG/PE collects per flow accounting data and exports it to a Netflow Collector workstation, which stores it in flat files. A Netflow Analyzer is then used for analyzing the collected data.

RBE Core Network

Network management, fault monitoring, and SLA reporting are management functions performed in the core ATM network.

Network Management

Network management components for RBE remote access consist of the following:

- **Element managers:** Service Connection Manager (SCM) for the 6400 and CDM (with CPE management extensions) for the DSLAMS and the DSL routers at the CPE.
- **VPNSC:** for VPN service provisioning, auditing, SLA monitoring and accounting. VPNSC also uses Cisco IP Manager (CIPM) for configuration downloads/uploads.
- **Netflow:** for usage accounting of non-PPP connections.
- **Cisco Info Center (CIC):** for VPN fault monitoring.
- **Concord Network Health:** for VPN performance reporting.

Fault Monitoring

Fault monitoring is performed at the device, and service levels.

At the device level, fault monitoring is performed by the element managers (CEMF has an event manager component). CAM provides fault monitoring per dial port.

CIC is user at the service level to provide event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems. CIC is an OEM product from Micromuse's NetCool. CIC's release 2.0 provides eventing at the IP VPN service level through integration with VPNSC.

SLA Reporting

SLA reporting is performed using the Service Assurance Agent (SA Agent) in IOS. At conventional MPLS VPN customer sites, VPNSC configures the SA Agent probes on managed CE routers, or shadow CE routers. At remote access sites, there is no real CE router so the SA Agent probes are configured on the PE routers at the PoPs. It is not possible to configure them on the NASs, because a NAS is not connected to a specific VPN so the probes are not routed using the VRFs. VPNSC collects statistics from the SA Agent MIB, and provides reports on a per VPN basis. For PPP users, performance numbers are derived from AR. The SA Agent probes are configured on the DSL routers at the CPE.

Performance and SLA reporting can be provided at a VPN service level through integration with VPNSC. RPMS is used to provide SLA information regarding incoming call rates per VPN customer.

RBE Provisioning

Configuration of RBE to MPLS VPN integration is very similar to configuration of RFC 1483 remote access integration, except that the PVC is configured to RBE.

Configuring the VHG/PE

Perform the following steps to configure the VHG/PE.

Step 1 Define loopbacks.

a. Router (config)# **interface loopback [***number***]**

b. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Commands in a and b create a general loopback interface used for reachability to the router and are used as a source IP address for sessions (IBGP, TDP, etc.).

c. Router (config-if)# **interface loopback** [*number*]

d. Router (config-if)# **ip vrf forwarding** [*vpn name*]

e. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Commands c, d, and e create a loopback interface in a VRF necessary only if you use ip unnumbered interfaces to the CE device when you would ip unnumber the interface to this loopback. These steps are repeated for each customer VRF you ip unnumber interfaces to.

Step 2 Define PVCs.

a. Router (config)# **interface ATM0/0/0.[***number***] point-to-point** (for the Cisco 6400). For example, **interface ATM0/0/0.1 point-to-point**
Router (config)# **interface ATM[***slot***]/[***port***].[***number***] point-to-point** (for the Cisco 7200). For example, **interface ATM4/0.1 point-to-point**

b. Router (config-if)# **ip vrf forwarding [***vpn name***]**

c. Router (config-if)# **ip unnumbered Loopback [***number***]**

Note If you are configuring an interface as unnumbered to a loopback interface, the loopback interface needs to be in the same VRF.

d. Router (config-if)# **pvc [***vpi/vci number***]**

e. Router (config-if-pvc)# **encapsulation aal5snap**

f. Router (config-if-pvc)# **no protocol ip inarp**

Step 3 Configure label switching on the interface connected to the MPLS cloud.

a. Router (config)# **ip cef**

Note The **tag-switching ip** command is on by default.

For connecting to a MPLS cloud using MPLS ATM tagging, perform the following commands:

a. Router (config-if)# **interface ATM0/0/0.**[*number*] **tag-switching**

Note Use the command above for the Cisco 6400. For the Cisco 7200, use **interface ATM[***slot***]/[***port***].[***number***]**.

b. Router (config-if)# **ip address** [*ip address*]

c. Router (config-if)# **tag-switching atm vp-tunnel** [*number*]

d. Router (config-if)# **tag-switching ip**

For frame-based tagging, the equivalent commands would be:

a. Router (config-if)# **interface ATM0/0/0.**[*number*]

Note Use the command above for the Cisco 6400. For the Cisco 7200, use **interface ATM[***slot***]/[***port***].[***number***]**.

b. Router (config-if)# **ip address** [*ip address*]

c. Router (config-if)# **tag-switching ip**

Note For NSP configuration details refer to Configuring Multiprotocol Label Switching on the Cisco 6400 UAC at
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/softnote/mpls_cfg.htm

Step 4 Configure the VRF for each VPN.

a. Router (config)# **ip vrf [***vpn name***]**

b. Router (config-vrf)# **rd [***route descriptor***]**

c. Router (config-vrf)# **route-target export [***route target communities***]**

d. Router (config-vrf)# **route-target import [***route target communities***]**

Note You need two route descriptors, for send and receive.

Step 5 Configure a dedicated PVC for each VPN (PTA-MD).

a. Router (config)# **interface ATM0/0/0.[***number***] point-to-point**

Note Use the command above for the Cisco 6400. For the Cisco 7200, use **interface ATM[***slot***]/0.[***number***]**.

b. Router (config-if)# **ip vrf forwarding [v***pn name***]**

c. Router (config-if)# **ip address [i***p address***]**

d. Router (config-if)# **pvc [***vpi/vci numbers***]**

e. Router (config-if-pvc)# **encapsulation aal5snap**

Step 6 Configure BGP to advertise the networks for each VPN.

a. Router (config)# **router bgp [***autonomous system number of sp***]**

b. Router (config-router)# **neighbor [***ip address of remote pe***] remote-as [***same autonomous number***]**

c. Router (config-router)# **neighbor [***ip address of remote pe***] update-source Loopback0**

d. Router (config-router)# **address-family vpnv4**

e. Router (config-router-af)# **neighbor [***ip address of remote pe***] activate**

f. Router (config-router-af)# **neighbor [***ip address of remote pe***] send-community extended**

Step 7 If using static routes, define them and redistribute them into BGP.

Step 8 Enable RBE on the interface:

a. Router (config)# **interface ATM0/0/0.[***number***] point-to-point**

Note Use the command above for the Cisco 6400. For the Cisco 7200, use **interface ATM[***slot***]/0.[***number***]**.

b. Router (config-subif)# **atm route-bridged ip**

Configuring DHCP Option 82 for RBE

Perform the following steps to configure DHCP Option 82 support for RBE.

Step 1 Enable the system to insert the DHCP relay agent information option in VPN suboptions.

a. Router (config)# **ip dhcp relay information option vpn**

Step 2 If you are on a non Cisco 6400 platform, specify the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the Agent Remote ID suboption.

a. Router (config) # **rbe nasip** *source_interface*

Step 3 Specify the ip helper address on the DSL interface:

a. Router (config-subif)# **ip helper-address vrf vpn [***ip address dhcp server***]**

Configuring the DSLAM using CDM

Perform the following step to configure the DSLAMS using CDM.

Step 1 Create subscriber properties, including VPI/VCI pairs.

For Cisco DSL Manager (CDM) configuration details, refer to

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cdm/cdm33/index.htm

Configuring CNR Network Server

The modem is configured to forward DHCP requests unaltered to the VHG/PE for DHCP relay. If the VHG/PE interface is a numbered interface with the ip-helper command configured, the GIADDR field of the DHCP discover packet is set to the IP address of the VHG/PE interface. This allows the DHCP scope to be provisioned on the CNR server accordingly.

If the VHG/PE interface is unnumbered to a loopback interface, the GIADDR field of the DHCP discover packet is set to the IP address of the loopback interface. If several interfaces are unnumbered to the same loopback interface, the CNR server relies on the client MAC address to determine the correct IP address to supply. This entails configuring client class processing on the CNR server.

For Cisco Network Registrar (CNR) configuration details, refer to
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/nr3-5/index.htm

Configuring the PVCs on PE routers

For VPNSC configuration details, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Configuring the PE Router for a New Service

For VPNSC configuration details, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

RBE Configuration Example

Example 4-1 shows an example of an RBE configuration, with the interface unnumbered.

Example 4-1 RBE Configuration Example

```
! Enable CEF Globally
!
ip cef
!
! VRF Definition
ip vrf <vrf-name>
 rd [VPN Route Distinguisher]:nn
 route-target export [VPN Route Distinguisher]:nn
 route-target import [VPN Route Distinguisher]:nn
!
interface Loopback0
 ip address 25.0.13.29 255.255.255.255
 no ip mroute-cache
!
! Connection to MPLS Network
!
interface ATM2/0
 no ip address
 no ip mroute-cache
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 30.0.3.106 255.255.255.252
 no ip mroute-cache
 pvc 5/2
  encapsulation aal5snap
 !
 tag-switching ip
!
! Connection to DSL Network using RBE
!
interface ATM4/0
 no ip address
 no ip mroute-cache
 no atm ilmi-keepalive

interface ATM4/0.1 point-to-point
 ip vrf forwarding <vrf-name>
 ip unnumbered Loopback0
 no ip mroute-cache
 atm route-bridged ip
 pvc 1/100
  encapsulation aal5snap
 !
 !
 ! IGP within the ISP core for routing to BGP peer(s)
!
router ospf 1
log-adjacency-changes
network <ip address> <wildcard mask> area <number>
!
!
! BGP Router Definition to Pass VPN Labels
!
router bgp <Autonomous System number>
 no synchronization
```

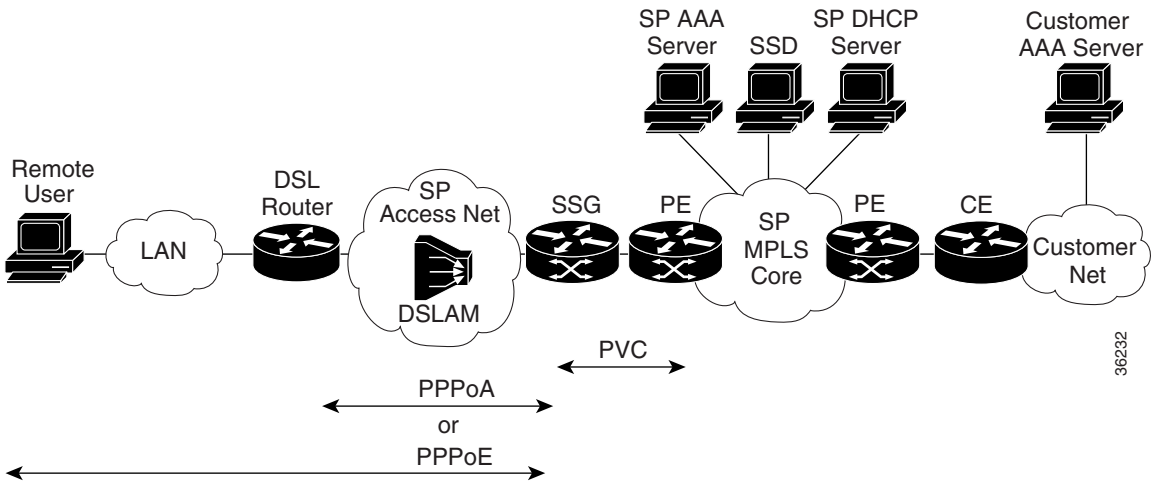
```
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor <peer-ip address> remote-as <number.
 neighbor <peer-ip address> update-source Loopback0
 no auto-summary
 !
 address-family ipv4 vrf <vrf-name>
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
!
address-family vpnv4
 neighbor 25.0.13.23 activate
 neighbor 25.0.13.23 send-community extended
 no auto-summary
 exit-address-family
!
```

PPPoX Remote Access SSG to MPLS VPN Integration

The topology of an integrated DSL remote access PPPoX with SSG to MPLS VPN solution is illustrated in Figure 4-7. PPPoX to SSG permits a remote user to select a desired service (ISP, enterprise VPN, etc.) provided through a separate MPLS VPN in the core. A remote user can switch between services dynamically and be logged on to multiple services simultaneously. The Service Selection Gateway (SSG), the Service Selection Dashboard (SSD), and the Radius server interact with each other to provide the service selection functionality.

Each service an SSG supports corresponds to an MPLS VPN. For each service supported on the SSG, a RFC 1483 PVC is configured between the SSG and the PE router. The PVC terminates at the PE router and is statically mapped to a VRF.

Figure 4-7 Cisco VPN DSL access PPPoX to SSG MPLS



PPPoX with SSG CPE Equipment

A DSL router is used to connect the remote access users to the SP DSL access network. In remote access PPPoX with SSG, the supported DSL routers are the Cisco 82x series, 14xx series, or SOHO77. At the residential side, the DSL router is attached to a LAN connecting to the remote users' host PCs.

PPPoX with SSG Access Network

The SP access network is a DSL access network with Cisco 6xx0 DSLAMs.

PPPoX with SSG

The Service Selection Gateway (SSG) is a software feature that runs on the 6400 NRP. The SSG permits remote users to use a single PPP session to log on to multiple services simultaneously. The set of services offered by a particular SSG must be known in advance. For each service an RFC 1483 PVC must be provisioned between the SSG NRP and the PE router to carry that service's traffic.

PPPoX with SSG SP Radius Server

The Access Registrar (AR) is the Radius server used for this solution. The AR stores two types of records: user profiles and service profiles. The vendor-specific attributes used by the SSG must be supported by the AR.

The Access Registrar Release 1.5 is used and runs on a Sun Sparc workstation with Solaris 2.6 or 2.7, 128 MB of RAM, 80 MB disk space.

A single AR safely processes up to 800 calls per second (one request per call), without losses, in case of performing authentication and authorization only, and can process up to 300 calls per second (three requests per call) in case of performing authentication, authorization, accounting, and address management.

Address Management

The following address management alternatives are available to a PPPoX user when it first logs on to the SSG:

- The virtual template configured on the SSG NRP specifies which address pools to use for address allocation.
- The user profile obtained from the SP Radius server specifies the name of the local address pool to use for address allocation.
- The SP Radius server allocates an address for that user. The Access Registrar is capable of address management and will claim the address back when it receives a Stop Accounting record for that user from the SSG.

If the address assigned when the user first logs on to the SSG is valid across all services this user selects afterwards, then there will be no need for assigning a new IP address for each service that user selects. This is a configurable option.

If the SSG service is not configured to reauthenticate the user, the user can be added to the service directly without proxying other servers. However, if the SSG service is configured to reauthenticate the user prior to joining the service, SSG queries that VPN's Radius server to authenticate the user.

- The VPN Radius server may return the name of the local pool to use for address assignment in its response to the SSG.
- The VPN Radius server may allocate an address to that user and return it to the SSG. The problem with this approach is that it makes address summarization at the PE difficult.

Authorization

When the remote user first logs on to the SSG, the SSG authenticates the user with the SP Radius server. The response from SP Radius includes a list of services this user is authorized to access. The SSG creates a host object and stores the list of authorized services.

When the remote user attempts to log on to a service it is authorized to use, the SSG queries the SP Radius server for more detailed authorization information for the service. The SP Radius server responds with that service's service profile, which includes among others: the service type, the address of the remote Radius server (VPN Radius server), and the address of the remote DNS server (VPN Radius server).

Authentication

- Logging on to the SSG: The SSG queries the SP Radius server to authenticate the remote user.
- Logging onto a service: The SSG queries the service's (=VPN's) Radius server to authenticate the remote user. The SSG must be made reachable from that service's VPN, in order for the response from the service's Radius server to make it back to the SSG.

Accounting

The SSG can be configured for PPP users and connections to perform the following accounting actions:

- Send accounting records to the SP Radius server when a remote user logs on to the SSG and when it logs off the SSG.
- Send accounting records to the SP Radius server when a remote user logs on to a service and when it logs off of a service.
- Send accounting records to the service's (=VPN's) Radius server when a remote user logs on to that service and when it logs off of that service.

On the PE routers, Netflow is used to provide per flow usage accounting (since Netflow needs to be enabled on the PE, the PE needs to support Netflow to support accounting). The Netflow Collector provides Netflow usage data collection used for performance reporting, capacity planning, and usage based billing. VPNSC collects the usage records from the Netflow Collector(s) and compares them with VPN service layer information.

PPPoX with SSG SSD

The Service Selection Dashboard (SSD) is a specialized web server that allows a user to its web browser for service selection. Once the user selects a service, the SSD forwards relevant information: user name, user password (if required), and service name to the SSG for authentication and service connectivity.

Each SSG must have its own SSD, i.e., 1:1 mapping.

The SSD may run on either:

- a SPARCStation running Solaris 2.4 or later with a minimum of 64 MB of RAM, or
- a Windows NT server with a minimum of 64 MB of RAM.

The following SSD software release is to be used: Altair-Dashboard, Version Number: 2.2s(1.12) Build 012.

The RFC 1483 PVCs connecting the SSGs to a PE router must be provisioned. Each PVC is statically mapped to a VRF on that PE router. Each PE router supports up to 400 VRFs.

The PE router terminates up to 2000 PVCs. On the MPLS VPN side, a PE can maintain 400 VRFs. This is within all three platform limits, since the maximum number of PVC sessions. The maximum number of VRFs is limited by the maximum number of interfaces.

More than one PE router in the same PoP can be configured with the same VRF.

The exact IOS release depends on the release schedule for the "overlapping local pools" feature.

PPPoX with SSG Core Network

DSL PPPoX to SSG supports two types of core networks, IP MPLS, and ATM MPLS.

Network Management

The network management components relevant for this solution are:

- **Element managers:** Service Connection Manager (SCM) for the 6400 (both the SSG NRPs and the PE NRPs), CIPM for the 7200 PE routers, and CDM for the DSLAMS. CDM extensions for CPE management are required for managing the DSL routers at the CPE.
  - CDM requires a Sun Ultra 60 with 256 MB of RAM and 10GB of disk space and solaris 2.6.
- **VPNSC:** for VPN service provisioning, auditing, SLA monitoring and accounting. VPNSC also uses Cisco IP Manager (CIPM) for configuration downloads/uploads.
- **AR:** for AAA functionality.
- **Netflow:** for usage accounting of non-PPP connections.
- **Cisco Info Center (CIC):** for VPN fault monitoring.
- **Concord Network Health:** for VPN performance reporting.
- **SSG/SSD**

Fault Monitoring

Fault monitoring is performed at the device, and service levels.

At the device level, fault monitoring is performed by the element managers (CEMF has an event manager component). CAM provides fault monitoring per dial port.

CIC is user at the service level to provide event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems. CIC is an OEM product from Micromuse's NetCool. CIC's release 2.0 provides eventing at the IP VPN service level through integration with VPNSC.

SLA Reporting

SLA reporting is performed using the Service Assurance Agent (SA Agent) in IOS. In conventional MPLS VPN customer sites, VPNSC configures SA Agent probes on managed CE routers or shadow CE routers. However, in remote access sites, there are no real CE router. The SA Agent probes is configured on the PE routers at the PoPs. It is not possible to configure them on the NASs, because a NAS is not connected to any particular VPN so the probes are not routed using the VRFs. VPNSC collects statistics from the SA Agent MIB and provides reports on a per VPN basis. For PPP users, performance numbers is derived from AR.

Concord's Net Health provides performance and SLA reporting at a VPN service level through integration with VPNSC.

RPMS is used to provide SLA information on such measures as incoming call rates for each VPN customers.

The SA Agent probes are configured on the DSL routers at the CPE for reporting on PPPoA connections, but not for the PPPoE connections which are initiated by the host PCs behind the DSL routers. Configure multiple SA probes on the DSL router, one for each of VPN service accessed through that router.

PPPoX with SSG Event Sequences

Perform the following two log on event sequences before provisioning the DSL PPPoX Integration.

Logging On To SSG

Perform the following steps to log on to the SSG:

Step 1 Either the DSL router creates a PPPoA session to the SSG or a host PC located behind the DSL router creates a PPPoE session to the SSG.

Step 2 The SSG receives the remote user's user id and password and queries the SP Radius server to authenticate the remote user.

Step 3 The SP Radius server responds to the SSG with the remote user's User Profile (the user profile includes the list of services this user is allowed to access).

Step 4 The SSG accepts the PPP session.

Step 5 An IP address is allocated to the remote user either by the SP Radius server, or from a local pool on the SSG. This address could be either a private or a public IP address.

Step 6 The assigned address is propagated back to the user using IPCP.

Step 7 The SSG creates a host object for the remote user, and the user gets access to the default service only. The default service includes access to the SSD.

Logging On To a Service

Perform the following steps to log on to a service:

Step 1 The remote user, a host PC in this case, accesses the SSD using a web client over the existing PPPoX connection and selects a service it is authorized to use (a service listed in its user profile).

Step 2 The SSD initiates a request to the SSG with user name, password, and service name.

Step 3 The SSG queries the SP Radius server and receives the service profile in response. The service profile includes, among others, the service type and the address of the service's (=VPN's) Radius server. The SSG creates a service object for that service.

Step 4 If the service type is “passthrough”, no authentication is required. If the service type is “proxy”, the SSG queries the VPN's Radius server to authenticate the remote user. The query is routed over the appropriate RFC 1483 PVC to the PE router then forwarded to that VPN's VRF. Note: A route back to the SSG must be redistributed into the VRF in order for the reply from the VPN's Radius server to be successfully routed back to the SSG (part of provisioning).

Step 5 The SSG assigns an address to the remote user. The address may come from:

- A local address pool. In this case SP Radius returns a pool name as part of the service profile.
- SP Radius server. Not a good idea, poor address management.
- VPN Radius server. Works but will result in poor route summarization.

Step 6 The SSG creates a connection object linking the remote user's host object to the service object. The SSG currently can not propagate a route to the remote host to the PE router in order to inject injects it into the VRF. Routes corresponding to the entire address pool corresponding to a service must currently be provisioned into that service's VRF.

Step 7 The SSG can not propagate the address assigned to the remote user back to the user, because the remote user may access multiple services (VPNs) simultaneously over the same PPPoX session. The user will always use the address it received in Step 5 as its source address. The SSG will differentiate between packets from the same user to different VPNs based on the destination address. This implies that a single remote host can not be logged on the two VPNs using overlapping address spaces simultaneously. The SSG must apply NAT to the source address of packets from the remote host to the VPN and it must apply NAT to the destination address of packets from the VPN to the remote host. An exception to this is when the user IP address assigned in Step 5 is valid and unique across all services the user is logged on to. In this case NAT need not be applied, and the user does not even have to be allocated a different IP address for each service. The IP address of Step 5 is sufficient in this case.

PPPoX with SSG Provisioning

Provisioning Cisco DSL PPPoX with SSG to MPLS VPN entails:

1. Initial Configuration through pre-staging of the routers, using config Xpress, using an element manager (for example, SCM), using CIPM templates, or any combination of the above. This configuration is not tied to VPN services per se. It includes:
   a. configuration of the PE routers
   b. configuration of the SSG NRP
   c. configuration of the customer's DSL routers
2. Although this is tied to customer provisioning, it is different from the VPN service provisioning (for example,, add a site to VPN). An example would be a customer with an existing VPN requests access for dial-up users. It includes:
   a. configuration of the different network servers: AR, CNR
   b. configuring the SSG NRP for a service: adding the RFC 1483 PVCs connecting to the PE router. This can be done using the SCM.
   c. configuring the PE router for a service: adding the required VRF configuration and the RFC 1483 PVCs connecting to the SSG. This is performed using VPNSC 2.
3. VPN service configurations are critically repetitive tasks to automate that include:
   a. actual service activation, performed by VPNSC, where a VPN is created, and CE sites and remote access sites are added to it.

Note For VPNSC configuration, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Configuring the PE Routers

Perform the following steps to configure the PE routers.

Step 1 Define loopbacks.

a. Router (config)# **interface loopback [***number***]**

b. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Command in a and b create a general loopback interface used for reachability to the router and are also used as a source IP address for sessions (IBGP, TDP, etc.).

c. Router (config-if)# **interface loopback** [*number*]

d. Router (config-if)# **ip vrf forwarding** [*vpn name*]

e. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Commands c, d, and e create a loopback interface in a VRF necessary only if you use ip unnumbered interfaces to the CE device when you would ip unnumber the interface to this loopback. These steps are repeated for each customer VRF you ip unnumber interfaces to.

Step 2 Configure the VRF for each VPN.

a. Router (config)# **ip vrf [***vpn name***]**

b. Router (config-vrf)# **rd [***route descriptor***]**

c. Router (config-vrf)# **route-target export [***route target communities***]**

d. Router (config-vrf)# **route-target import [***route target communities***]**

Note You need two route descriptors, for send and receive.

Step 3 Configure label switching on the interface connected to the MPLS cloud.

a. Router (config)# **ip cef**

Note The **tag-switching ip** command is on by default.

For connecting to a MPLS cloud using MPLS ATM tagging, perform the following commands:

a. Router (config-if)# **interface ATM0/0/0.**[*number*] **tag-switching**

b. Router (config-if)# **ip address** [*ip address*]

c. Router (config-if)# **tag-switching atm vp-tunnel** [*number*]

d. Router (config-if)# **tag-switching ip**

For frame-based tagging, the equivalent commands would be:

a. Router (config-if)# **interface ATM0/0/0** [*number*]

b. Router (config-if)# **ip address** [*ip address*]

c. Router (config-if)# **tag-switching ip**

Note For NSP configuration details refer to Configuring Multiprotocol Label Switching on the Cisco 6400 UAC at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/softnote/mpls_cfg.htm

Step 4 Configure a dedicated PVC for each VPN (PTA-MD).

a. Router (config)# **interface ATM0/0/0.[***number***] point-to-point**

b. Router (config-if)# **ip vrf forwarding [v***pn name***]**

c. Router (config-if)# **ip address [***ip address***]**

d. Router (config-if)# **pvc [***vpi/vci numbers***]**

e. Router (config-if-pvc)# **encapsulation aal5snap**

Step 5 Configure BGP to advertise the networks for each VPN.

a. Router (config)# **router bgp [***autonomous system number of sp***]**

b. Router (config-router)# **neighbor [***ip address of remote pe***] remote-as [***same autonomous number***]**

c. Router (config-router)# **neighbor [***ip address of remote pe***] update-source Loopback0**

d. Router (config-router)# **address-family vpnv4**

e. Router (config-router-af)# **neighbor [***ip address of remote pe***] activate**

f. Router (config-router-af)# **neighbor [***ip address of remote pe***] send-community extended**

Step 6 If using static routes, define them and redistribute them into BGP.

For configuration details of the Cisco 6400, refer to the 6400 documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/index.htm

Configuring the SSG NRP

Perform the following steps to configure the SSG NRP.

- For steps 1, 2, 4, and 5, refer to sections 6.4, 6.5, 6.3, and 6.8, respectively, in the following URL for configuration details: http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/con_r2/nrp_con.htm
- For step 3, refer to the following URL for configuration details: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc3/ssgfm.htm
  - For configuration enhancements to Steps 3, refer to the following for details: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc7/ssgl2tp.htm

---

Step 1 Merge user-specific information with RADIUS configuration information through a generic virtual-template using the following command:

a. Router (config)# **virtual-profile aaa**

Step 2 If using PPPoE, define a VPDN group that accepts PPPoE and specifies a virtual template to use.

a. Router (config)# **vpdn enable**

b. Router (config)# **vpdn-group <***group number***>**

c. Router (config-vpdn)# **accept-dialin**

d. Router (config-vpdn-acc-in)# **protocol pppoe**

e. Router (config-vpdn-acc-in)# **virtual-template <***virtual template number***>**

f. Router (config-vpdn-acc-in)# **pppoe limit per-vc 10**

Step 3 Configure the Subscriber PPP/ATM termination. (See section 6.4 of the URL)

a. Router (config)# **interface ATM0/0/0.[***number***] point-to-point**

b. Router (config-if)# **ip unnumbered Loopback0**

c. Router (config-if)# **pvc [***vpi/vci numbers***]**

d. Router (config-if)# **protocol pppoe**

Note For PPPoA, the encapsulation command is
Router (config-i-pvc)# **encapsulation aal5mux ppp Virtual-Template1**

Step 4 Configure the AAA server information. (See section 6.5 of the URL)

Step 5 Configure the SSG information.

a. Router (config)# **ssg enable**

b. Router (config)# **ssg default-network [***ssd ip address***]**

c. Router (config)# **ssg service-password [***password***]**

d. Router (config)# **ssg radius-helper auth-port 1645 acct-port 1646**

e. Router (config)# **ssg radius-helper key [***password***]**

f. Router (config)# **ssg bind service [***vpn name***] [***next-hop-interface***]**

Step 6 Configure the PTA-MD. (See section 6.3 of the URL)

Step 7 Configure Routing information. (See section 6.8 of the URL)

Configuring the Customer DSL Routers

Perform the following steps to configure the customer DSL routers.

Step 1 Configure the WAN interface of the router.

a. cbos# **set int wan0-0 close**

b. cbos# **set int wan0-0 vpi 1**

c. cbos# **set int wan0-0 vci 1**

d. cbos# **set int wan0-0 open**

e. cbos# **set dhcp server enabled (optional)**

f. cbos# **set nat enabled (optional)**

Step 2 Configure the PPP information.

For PPPoA, configure the router to bridge as follows.

a. cbos# **set ppp wan0-0 login [***user name***]**

b. cbos# **set ppp wan0-0 password [***password***]**

c. cbos# **set ppp wan0-0 ipcp 0.0.0.0**

For PPPoE

a. cbos# **set bridging RFC1483 enable**

For DSL router configuration details, refer to
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c600s/index.htm

Configuring the AR Network Server

Perform the following steps to configure the AR network server.

Step 1 Define the SSG and SSD as clients.

a. Enter CLI configuration mode of AR.

admin@sun-ar% aregcmd -s

b. Change to client directory

--> **cd /radius/clients**

c. Add SSG or SSD to client directory

--> **add [***name of SSG or SSD***]**

d. Define IP address and shared key of SSG or SSD.

--> **set ipaddress [***ip address***]**

--> **set sharedsecret [***sharedsecret***]**

Step 2 Define the users in the Userlists database.

--> **add /Radius/Userlists/[***userlist name***]**

--> **cd /Radius/Userlists/[***userlist name***]**

--> **set password [***password***]**

--> **set baseprofile [***profile name***]**

Step 3 Define a profile for each user in the database.

--> **cd /Radius/Profile**

--> **add [***profile name***]**

--> **cd [***profile name***]/attributes**

--> **set framed-ip-addres** [*ip address*]

--> **set framed-mtu** [*mtu size*]

--> **set framed-protocol ppp**

--> **set account-info "**[*vpn1*] [*vpn2*] [*vpnn*]**"**

Step 4 Define services (vpn) in the Userlists database.

--> **add /Radius/Userlists/[***service name***]**

--> **cd /Radius/Userlists/[***service name***]**

--> **set password [***password***]**

--> **set baseprofile [***profile name***]**

Step 5 Define a profile for each service.

--> **cd /Radius/Profile**

--> **add [***profile name***]**

--> **cd [***profile name***]/attributes**

--> **set service-info "**[*Iservice-name Tservice-type Mservice-mode Rservice-routing ...*]**"**

For Access Registrar (AR) configuration details, refer to
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

Configuring CNR Network Server

The 67X modem is configured to forward DHCP requests unaltered to the 6400. If the 6400 interface is a numbered interface with the ip-helper command configured, the GIADDR field of the DHCP discover packet is set to the IP address of the 6400 interface. This allows the DHCP scope to be provisioned on the CNR server accordingly.

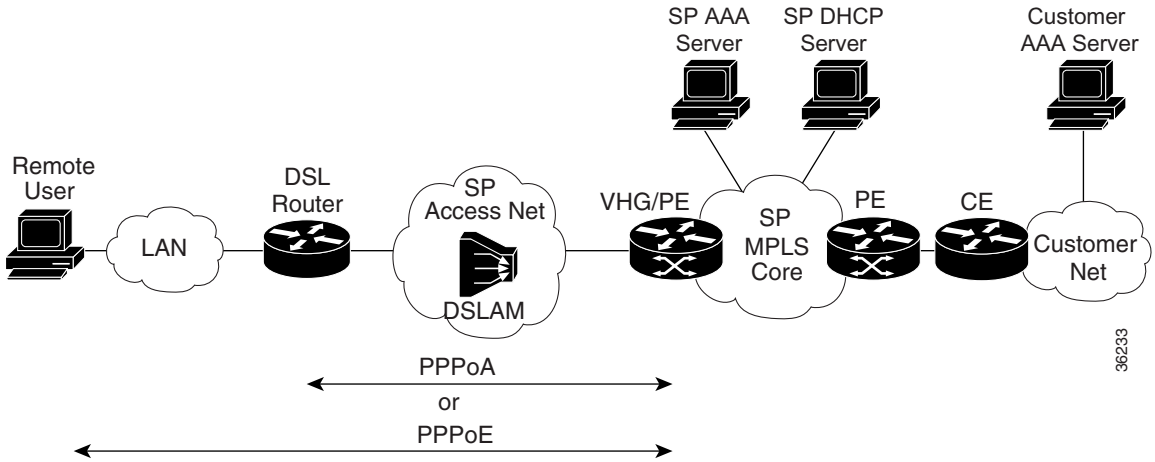
If the 6400 interface is unnumbered to a loopback interface, the GIADDR field of the DHCP discover packet is set to the IP address of the loopback interface. If several interfaces are unnumbered to the same loopback interface, the CNR server relies on the client MAC address to determine the correct IP address to supply. This entails configuring client class processing on the CNR server.

For Cisco Network Registrar (CNR) configuration details, refer to
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/nr3-5/index.htm

PPPoX Remote Access to MPLS VPN Integration

The topology of an integrated DSL remote access PPPoX to MPLS VPN solution is illustrated in Figure 4-8 using a VPN capable service provider's MPLS backbone. In PPPoX remote access, the VHG/PE terminates an incoming PPPoX session and maps the remote user to the corresponding VRF.

Figure 4-8 PPPoX DSL remote access to MPLS VPN



PPPoX CPE Equipment

A DSL router is used to connect the remote access users to the SP DSL access network. In PPPoX remote access, the supported DSL routers are the Cisco 82x series, 14xx series, or SOHO77. At the residential side, the DSL router is attached to a LAN connecting to the remote users' host PCs.

PPPoX Access Network

The SP access network is a DSL access network with Cisco 6xx0 DSLAMs.

PPPoX VHG/PE Routers

The following VHG/PE platforms are used in Cisco PPPoX remote access to MPLS.

- Cisco 6400 NRP1 and NRP2
- Cisco 7200 NPE-300 and NPE-400

Each VHG/PE accepts up to 300 L2TP tunnels carrying a total of 2000 PPP sessions. On the MPLS VPN side, a PE can maintain 400 VRFs. This is within all three platform limits, since the maximum number of PPP sessions. The maximum number of VRFs is limited by the maximum number of interfaces.

Since each 7x00/NRP router can terminate only 2048/3000 PPP sessions, about 33/50 7x00/NRP routers are configured as VHG/PEs per PoP. More than one PE router in the same PoP can be configured with the same VRF.

Each VHG/PE router must be configured with appropriate VRFs. Each VRF must be enabled on the VHG/PE router by creating a loopback interface and configuring it to forward all packets to the VRF. 400 IDBs is consumed to enable 400 VRFs on VHG/PE.

PPPoX Radius Servers

The Access Registrar (AR) is the Radius server used in this solution. There may need to be multiple Radius servers in the network, depending on:

- the size of the solution, and
- the ability of the AR to provide different responses to the same request based on the identity of the requestor. For example, a NAS sending an Access-Request for cisco.com expects to receive the L2TP tunnel configuration in response, while a VHG/PE sending an Access-Request for cisco.com expects to receive a VRF information in response. AR is capable of performing this function.

In large solutions, where a single PoP has 100,000 ports, it may be economical to allocate a Local SP Radius server for the NASs in each PoP. The VHG/PEs sends the requests to Radius servers to a separate set of SP Radius servers, the one residing in the core.

The NASs and VHG/PEs only query the SP's Radius servers. An SP Radius server must be capable of proxying authentication and accounting requests to the relevant VPN Radius servers. The AR has this capability. However, the VPN Radius server can be using private addresses and may be unreachable through the global routing table. For the SP Radius server to communicate with the VPN Radius servers it must be made part of a management VPN.

See Appendix A, “AAA Radius Access to MPLS VPN Integration” for details on using Radius for AAA and address management.

The solution supports the following alternatives:

- Only local Radius servers in each PoP.
- Only shared Radius servers in the core.
- A mix of local Radius servers in each PoP and shared Radius servers in the core.

A single AR can safely process up to 800 calls per second (one request per call), without losses, in case of performing authentication and authorization only, and it can process up to 300calls per second (three requests per call) in case of performing authentication, authorization, accounting, and address management.

Address Management

A PE assigns addresses to remote users through:

- **Local Address Pools.** The VHG/PE associates a local pool with a specific VRF by overlapping local address pools.
- **SP's Radius Server**. The AR maintains overlapping address pools. It has a separate pool per (VPN, VHG/PE) pair. The AR identifies the VPN as part of the authorization. The VHG/PE is identified by the NAS-IP-Address attribute or the NAS-Identifier attribute in the Access-Request. AR relies on Stop accounting messages to reclaim unused addresses after a remote user disconnects. It is necessary to configure authentication and accounting to the same AR for address assignment to function properly.

- **SP's DHCP Serve**. If the VHG/PE requests an IP address from the SP DHCP server, it does not provide sufficient information to the VPN server the address is used for. The DHCP server assigns addresses from a common pool SP's address pool to all remote users regardless of the VPN each belongs to.

Note VPN DHCP (Cisco Network Registrar, CNR) is not available in this Release.

Authorization and Authentication

The following functions are provided:

- Authorization by the SP Radius server,
- Proxy authentication
- Authentication by the SP Radius server
- Return virtual interface configuration to the VHG/PE

Upon receipt of an incoming PPP session, the VHG/PE sends an Access-Request to the SP Radius server. The SP Radius server authorizes the PPP session based on the remote user's domain name or DNIS, and associates the PPP session with a specific VPN. The VPN is returned to the interface as configuration commands to be applied to the virtual interface being created for that PPP session.

Based on the domain name or DNIS, the SP Radius server proxies the request to the appropriate VPN Radius server for authenticating the remote user. Alternately, the SP Radius server can complete the authentication itself. See Appendix A, "AAA Radius Access to MPLS VPN Integration" for details.

Accounting

Accounting is provided by the AAA records in AR for the PPP users and is required if the SP Radius server is used for address management.

The VHG/PE is configured to send accounting records to the SP Radius server. The accounting mode is start-stop or stop-only. SP Radius server, and Proxy accounting functions are provided.

The SSG can be configured for PPP users and connections to perform the following accounting actions:

- Send accounting records to the SP Radius server when a remote user logs on to the SSG and when it logs off the SSG.
- Send accounting records to the SP Radius server when a remote user logs on to a service and when it logs off of a service.
- Send accounting records to the service's (=VPN's) Radius server when a remote user logs on to that service and when it logs off of that service.

On the PE routers, Netflow is used to provide per flow usage accounting (since Netflow needs to be enabled on the PE, the 6400 needs to support Netflow for this feature to be supported, which is not the case yet). The Netflow Collector provides collection of Netflow usage data that can be used for performance reporting, capacity planning and usage based billing. VPNSC collects the usage records from the Netflow Collector(s) and correlates them with the VPN service layer information.

PPPoX Core Network

DSL Single-Card PPPoX supports two core network types, IP MPLS and ATM MPLS.

VPN Management

The VPN Solutions Center (VPNSC) is the primary tool used to provision a management VPN for all managed sites. The management VPN is required for applications that need access to a customer's VPN.

In Single-Card PPPoX MPLS VPN those applications are VPNSC, CIPM, and SP Access Registrar (where it proxies to a customer AAA server).

The configuration of the management VPN for the VPNSC and CIPM applications is generic to all managed MPLS VPN solutions described in other documents. For example. the way the management VPN is configured by VPNSC, it only allows applications on the management VPN to access the managed PE and CE routers.

In case of Radius proxy, the following configuration is required:

- Each VPN's Radius server must have a unique address.
- The SP's Radius server must be in a Management VPN.
- Routes to each of the VPN Radius servers must be distributed to the Management VPN, and the route to the SP Radius server needs to be distributed into each of the other VPNs.

Network Management

The network management components relevant for this solution are:

- **Element Managers**: mainly Service Connection Manager (SCM) for the 6400, and CDM for the DSLAMS. CDM extension for CPE management are required in order to manage the DSL routers at the CPEs. The availability date for these extensions is not known yet.
- **VPNSC**: for VPN service provisioning, auditing, SLA monitoring and accounting. VPNSC also uses Cisco IP Manager (CIPM) for configuration downloads/uploads.
- **AR**: for AAA functionality.
- **CNR**: for IP address allocation.
- **Netflow**: for usage accounting of non-PPP connections.
- **Cisco Info Center (CIC)**: for VPN fault monitoring.
- **Concord Network Health**: for VPN performance reporting.

Fault Monitoring

Fault monitoring is performed at the device, and service levels.

At the device level, fault monitoring is performed by the element managers (CEMF has an event manager component). CAM provides fault monitoring per dial port.

CIC is user at the service level to provide event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems. CIC is an OEM product from Micromuse's NetCool. CIC's release 2.0 provides eventing at the IP VPN service level through integration with VPNSC.

SLA Reporting

SLA reporting is performed using the Service Assurance Agent (SA Agent) in IOS. In conventional MPLS VPN customer sites, VPNSC configures SA Agent probes on managed CE routers or shadow CE routers. However, in remote access sites, there are no real CE router. The SA Agent probes is configured on the PE routers at the PoPs. It is not possible to configure them on the NASs, because a NAS is not connected to any particular VPN so the probes are not routed using the VRFs. VPNSC collects statistics from the SA Agent MIB and provides reports on a per VPN basis. For PPP users, performance numbers is derived from AR.

Concord's Net Health provides performance and SLA reporting at a VPN service level through integration with VPNSC.

RPMS is used to provide SLA information on such measures as incoming call rates for each VPN customer.

The SA Agent probes are configured on the DSL routers at the CPE for reporting on PPPoA connections, but not for the PPPoE connections which are initiated by the host PCs behind the DSL routers. Configure multiple SA probes on the DSL router, one for each of VPN service accessed through that router.

PPPoX Event Sequence

Perform the following steps for creating a PPPoX session over DSL to access its corporate network or ISP as a remote user, the customer network in Figure 4-8.

Step 1 The remote user initiates a PPPoE session, or the DSL router initiates a PPPoA session, over the DSL access network.

Step 2 The VHG/PE accepts and terminates the PPPoX session.

Step 3 The VHG/PE queries Radius to associate the remote user with a specific customer MPLS VPN. The VPN's VRF (routing table and other information associated with a specific VPN) must have been pre-instantiated on the VHG/PE. See

Step 4 The VHG/PE completes the remote user's authentication through Radius.

Step 5 The VHG/PE obtains an IP address for the remote user.

Step 6 The remote user is now part of the customer VPN. Packets can flow from/to the remote user.

PPPoX Provisioning

Provisioning Cisco VPN DSL PPPoX remote access to MPLS entails:

1. Initial configuration through router pre-staging, using config Xpress, using an element manager (for example, SCM), using CIPM templates, or any combination of the above. This configuration is not necessarily tied to VPN services and includes:
   a. configuration of the VHG/PE routers
   b. configuring the AR and CNR servers on the VHG/PE
2. Although this is tied to customer provisioning, it is different from the VPN service provisioning (for example,, add a site to VPN). An example would be a customer with an existing VPN requests access for dial-up users. It includes:
   a. configuration of the different network servers: AR, CNR
   b. configuring the VHG/PE for a new customer by adding the required VRF configuration, address pools, and virtual templates through VPNSC 2 using templates from IP Manager (CIPM).
   c. configuring the customer DSL routers.
3. VPN service configurations are critically repetitive tasks to automate that include:
   a. actual service activation, performed by VPNSC, where a VPN is created, and CE sites and remote access sites are added to it.

Note For VPNSC configuration, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Configuring the VHG/PE Routers

Perform the following steps to configure the VHG/PE router.

Step 1 Define loopbacks.

a. Router (config)# **interface loopback [***number***]**

b. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Commands in a and b create a general loopback interface used for reachability to the router and are used as a source IP address for sessions (IBGP, TDP, etc.).

c. Router (config-if)# **interface loopback** [*number*]

d. Router (config-if)# **ip vrf forwarding** [*vpn name*]

e. Router (config-if)# **ip address** [*address*] [*netmask*]

Note Commands c, d, and e create a loopback interface in a VRF necessary only if you use ip unnumbered interfaces to the CE device when you would ip unnumber the interface to this loopback. These steps are repeated for each customer VRF you ip unnumber interfaces to.

Step 2 Configure the VRF for each VPN.

a. Router (config)# **ip vrf [***vpn name***]**

b. Router (config-vrf)# **rd [***route descriptor***]**

c. Router (config-vrf)# **route-target export [***route target communities***]**

d. Router (config-vrf)# **route-target import [***route target communities***]**

Note You need two route descriptors, for send and receive.

Step 3 Configure the virtual template.

a. Router (config)# **interface virtual-template[***number***]**

b. Router (config-if)# **ip unnumbered loopback[***number***]**

c. Router (config-if)# **ip ppp authenication chap**

Step 4 Configure BGP to advertise the networks for each VPN.

a. Router (config)# **router bgp [***autonomous system number of sp***]**

b. Router (config-router)# **neighbor [***ip address of remote pe***] remote-as [***same autonomous number***]**

c. Router (config-router)# **neighbor [***ip address of remote pe***] update-source Loopback0**

d. Router (config-router)# **address-family vpnv4**

e. Router (config-router-af)# **neighbor [***ip address of remote pe***] activate**

f. Router (config-router-af)# **neighbor [***ip address of remote pe***] send-community extended**

Step 5 If using static routes, define them and redistribute them into BGP.

Refer to Table 4-2 for Cisco PE router product URLs:

Table 4-2 PE Router URLs

Component	URL
Cisco 7200 series routers	http://www.cisco.com/univercd/cc/td/doc/product/core/index.htm
Cisco 6400 doc suite	http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/index.htm

Configuring the AR and CNR Network Servers on the VHG/PE

Perform the following steps to configure the AR and CNR network servers on the VHG/PE.

Note Configuring CNRnetwork servers is optional since it only needs to be performed for assigning IP addresses to users with a DHCP server, or to do DHCP relays.

Step 1 Merge user-specific information with RADIUS configuration information through a generic virtual-template using the following command:

a. Router (config)# **virtual-profile aaa**

Step 2 If using PPPoE, define a VPDN group that accepts PPPoE and specifies a virtual template to use.

a. Router (config)# **vpdn enable**

b. Router (config)# **vpdn-group <***group number***>**

c. Router (config-vpdn)# **accept-dialin**

d. Router (config-vpdn-acc-in)# **protocol pppoe**

e. Router (config-vpdn-acc-in)# **virtual-template <***virtual template number***>**

f. Router (config-vpdn-acc-in)# **pppoe limit per-vc 10**

Step 3 Define authentication and accounting on the VHG/PE to point to the appropriate AR server(s).

Step 4 Enable the VHG/PE to use the Radius protocol for authorization and authentication.

a. Router (config)# **aaa new-model**

b. Router (config)# **aaa authentication ppp default local group radius**

c. Router (config)# **aaa authorization network default local group radius**

Step 5 Define necessary share secrets to properly communicate with the Radius server on the VHG/PE.

a. Router (config)# **radius-server host [***ip address of radius server***] key [***sharedscret***]**

Note The sharedsecret has to be the same as the sharedsecret defined in Step 1d of “Configuring the AR Network Server” on page 38.

Step 6 Define local pools if using local pool addressing.

Configuring the AR Network Server

Perform the following steps to configure the AR network server.

Step 1 Define DNIS or domains for the customer group.

Step 2 Define VPN users for each customer group.

Step 3 Define profile containing the necessary attributes.

One required attribute for single card PPPoA or PPPoE is to pass a Cisco attribute value pair (AV-Pair) to configure the interface into a VRF. Exemplified as follows:

```
[//localhost/Radius/Profiles/1cardpppoa1_profile/Attributes]
        cisco-avpair = "lcp:interface-config#1 = ip vrf forwarding vpn200"
        cisco-avpair = "lcp:interface-config#2 = ip unnumbered Loopback200"
        cisco-avpair = "lcp:interface-config#3 = peer default ip address pool 1cardpppoa_pool_vpn200"
        Framed-mtu = 1500
        Framed-Protocol = PPP
        Service-Type = Framed
```

Note This assumes the user is attached to vpn200, that I used lo200 as my interface address, and that I have an address pool defined on the PE router called 1cardpppoa_pool_vpn200.

For Access Registrar (AR) configuration details, refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

Configuring CNR Network Server

The 67X modem is configured to forward DHCP requests unaltered to the 6400. If the 6400 interface is a numbered interface with the ip-helper command configured, the GIADDR field of the DHCP discover packet is set to the IP address of the 6400 interface. This allows the DHCP scope to be provisioned on the CNR server accordingly.

If the 6400 interface is unnumbered to a loopback interface, the GIADDR field of the DHCP discover packet is set to the IP address of the loopback interface. If several interfaces are unnumbered to the same loopback interface, the CNR server relies on the client MAC address to determine the correct IP address to supply. This entails configuring client class processing on the CNR server.

For Cisco Network Registrar (CNR) configuration details, refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/nr3-5/index.htm

Configuring the VHG/PE for a New Customer

Perform the following steps to configure the VHG/PE for a new customer. Refer to “Configuring the VHG/PE Routers” on page 36.

Step 1 Define a new PVC end to end to the customer's CPE device.

a. Router (config)# **interface ATM0/0/0.233 point-to-point**

b. Router (config-subif)# **pvc 20/33**

Step 2 Attach a generic virtual template to the PVC.

a. Router (config-if-atm-vc)# **encapsulation aal5mux ppp virtual-template 1**

A final configuration would look like the following:

```
interface ATM0/0/0.233 point-to-point
   pvc 20/33
    encapsulation aal5mux ppp Virtual-Template1
interface Virtual-Template1
```

Note This assumes you have a virtual template configured that will be combined with user specific information passed from the AAA server.

```
   ip unnumbered Loopback1
   ip mroute-cache
   ppp authentication chap callin
```

Configuring the Customer DSL Routers

Perform the following steps to configure a customer DSL routers.

Step 1 Configure the WAN interface of the router.

Step 2 If using PPPoA, configure necessary PPP information on the DSL router such as username and password. Other information is optional depending on user requirements.

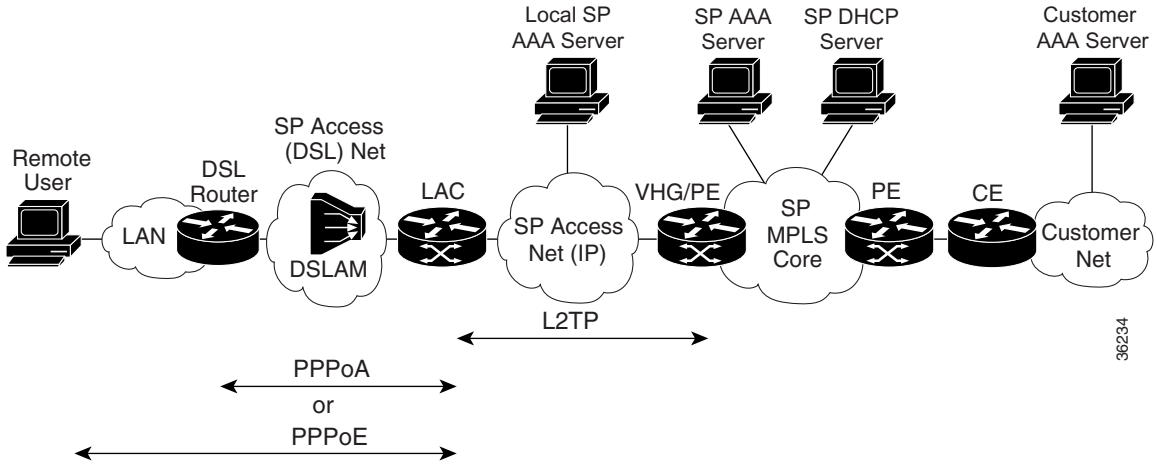
Step 3 If using PPPoE, configure the DSL router to bridge the ethernet frames into the WAN ATM interface.

For DSL router configuration details, refer to
http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c600s/index.htm

DSL L2TP to MPLS VPN Integration

Figure 4-9, depicts the topology of an integrated DSL L2TP to MPLS VPN access solution. It shows a topology with a VPN capable service provider's MPLS backbone. In Figure 4-9, the customer is outsourcing all remote access operations to its service provider. The service provider operates an MPLS VPN that interconnects all customer sites. Incoming PPPoX sessions, arriving at the LAC, are L2TP-tunneled to the VHG/PE that maps it to the corresponding VRF. This solution provide enhanced aggregation and route summarization at the edge of the MPLS VPN core. This solution is similar to the dial in L2TP to MPLS VPN solution discussed in Chapter 2.

Figure 4-9 PPPoX/L2TP DSL remote access - MPLS VPN, solution.



DSL L2TP CPE Equipment

A DSL router is used to connect the remote access users to the SP DSL access network. In DSL L2TP remote access, the supported DSL routers are the Cisco 82x series, 14xx series, or SOHO77. At the residential side, the DSL router is attached to a LAN connecting to the remote users' host PCs. Specify PPPoE software for the PCs.

DSL L2TP Access Network

The SP access network consists of two components:

- The DSL access network, which connects the remote users to the SP's PoP.
- The IP access network , which connects various network elements present at a PoP. It may be a high-speed LAN or an ATM network. In addition to the LACs and VHG/PEs, a Radius server may have to be placed in each IP access Network.

The access network could be a high-speed LAN or an ATM network. Like the NASs and VHG/PEs, a Radius server may need to be placed in each Access Network (PoP).

DSL L2TP VHG/PE Routers

The following VHG/PE platforms are used in Cisco DSL L2TP remote access to MPLS.

- Cisco 6400 NRP1 and NRP2
- Cisco 7200 NPE-300 and NPE-400

Each VHG/PE is capable of accepting up to 300 L2TP tunnels carrying a total of 2000 PPP sessions. On the MPLS VPN side, a PE is capable of maintaining 400 VRFs. These numbers are within the limits of all three platforms, since the maximum number of PPP sessions, and also the maximum number of VRFs, is limited by the maximum number of interfaces.

Since each 6400/7x00/NRP router can terminate only 2048/3000 PPP session, about 50/33 7x00/NRP routers are configured as VHG/PEs per PoP. More than one PE router in the same PoP can be configured with the same VRF.

Each VHG/PE router must be configured with appropriate VRFs. Each VRF must be pre-instantiated on the VHG/PE router. This is performed by creating a loopback interface and configuring it to forward all packets to the VRF. 400 IDBs is consumed to pre-instantiate 400 VRFs on VHG/PE.

DSL L2TP LACs

The LAC platform is the 6400 NRP. It receives incoming PPPoX sessions and L2TP-tunnels them to the VHG/PE.

When configured as a LAC the 6400 NRP processes up to 2000 PPPoX sessions and 50 L2TP tunnels (one tunnel to each VHG/PE in the same access network).

DSL L2TP Radius Servers

The Access Registrar (AR) is the Radius server used for this solution. There may need to be multiple Radius servers in the network, depending on:

- the size of the solution, and
- the ability of the AR to provide different responses to the same request based on the identity of the requestor. For example, a NAS sending an Access-Request for cisco.com expects to receive the L2TP tunnel configuration in response, while a VHG/PE sending an Access-Request for cisco.com expects to receive a VRF information in response. AR is capable of performing this function.

In large solutions, where a single PoP has 100,000 ports, it may be economical to allocate a Local SP Radius server for the NASs in each PoP. The VHG/PEs sends the requests to Radius servers to a separate set of SP Radius servers, the one residing in the core.

The NASs and VHG/PEs only query the SP's Radius servers. A SP Radius server must be capable of proxying authentication and accounting requests to the relevant VPN Radius servers. The AR has this capability. However, the VPN Radius server can be using private addresses and may be unreachable through the global routing table. For the SP Radius server to communicate with the VPN Radius servers it must be made part of a management VPN.

The AR when queried by the NASs provides for tunnel authorization only, and when queried by the VHGs provide AAA and optionally address management functions. In case of small-scale solutions, the same AR may be used by both the NAS and the VHG/PE. The AR must be configured to differentiate between the a request from a NAS and a request from a VHG/PE. A NAS's request has

service-type=Outbound-User while a VHG/PE's request has a service-type=Framed-User. In larger solutions the NASs can be configured with different AAA servers than those configured on the VHG/PEs.

See Appendix A, "AAA Radius Access to MPLS VPN Integration" for details on using Radius for AAA and address management.

The solution supports the following alternatives:

- Only local Radius servers in each PoP.
- Only shared Radius servers in the core.
- A mix of local Radius servers in each PoP and shared Radius servers in the core.

A single AR can safely process up to 800 calls per second (one request per call), without losses, in case of performing authentication and authorization only, and it can process up to 300calls per second (three requests per call) in case of performing authentication, authorization, accounting, and address management.

Address Management

A PE assigns addresses to remote users through:

- **Local Address Pools.** The VHG/PE associates a local pool with a specific VRF by overlapping local address pools.
- **SP's Radius Server**. The AR maintains overlapping address pools. It has a separate pool per (VPN, VHG/PE) pair. The AR identifies the VPN as part of the authorization. The VHG/PE is identified by the NAS-IP-Address attribute or the NAS-Identifier attribute in the Access-Request. AR relies on Stop accounting messages to reclaim unused addresses after a remote user disconnects. It is necessary to configure authentication and accounting to the same AR for address assignment to function properly.
- **SP's DHCP Serve**. If the VHG/PE requests an IP address from the SP DHCP server, it does not provide sufficient information to the VPN server the address is used for. The DHCP server assigns addresses from a common pool SP's address pool to all remote users regardless of the VPN each belongs to.

Note VPN DHCP is not available in this Release.

The DHCP server is Cisco Network Registrar (CNR).

Accounting

Accounting is provided by the AAA records in AR for the PPP users and is required if the SP Radius server is used for address management.

The VHG/PE is configured to send accounting records to the SP Radius server. The accounting mode is start-stop or stop-only. SP Radius server, and Proxy accounting functions are provided

On the PE routers, Netflow provides per flow usage accounting. The Netflow Collector provides of Netflow usage data collection used for performance reporting, capacity planning, and usage based billing. VPNSC collects the usage records from the Netflow Collector(s) and correlates them with VPN service layer information.

DSL L2TP Core Network

The DSL L2TP to MPLS VPN Integration solution supports two types of core networks, IP MPLS and ATM MPLS.

VPN Management

The VPN Solutions Center (VPNSC) is the primary tool used to provision a management VPN for all managed sites. The management VPN is required for applications that need access to a customer's VPN.

In dial L2TP MPLS VPN those applications are VPNSC, CIPM, and SP Access Registrar (where it proxies to a customer AAA server).

The configuration of the management VPN for the VPNSC and CIPM applications is generic to all managed MPLS VPN solutions described in other documents. For example. the way the management VPN is configured by VPNSC, it only allows applications on the management VPN to access the managed PE and CE routers.

In case of Radius proxy, the following configuration is required:

- Each VPN's Radius server needs to have a unique address.
- The SP's Radius server needs to be in a Management VPN.
- Routes to each of the VPN Radius servers need to be distributed to the Management VPN, and the route to the SP Radius server needs to be distributed into each of the other VPNs.

Network Management

Network management considerations for DSL L2TP opposed to Dial L2TP are:

- The NASs are replaced by the 6400 LACs. SCM is used to provision and manage the LAC.
- The DSL routers at the CPE and the DSLAMs are managed by CDM (if CPE management extensions are available).
- The SA Agent probes are configured on the DSL routers at the CPE.

Network management components for DSL L2TP are:

- **Element managers:**
  - Service Connection Manager (SCM) for the 6400. It requires Sun Ultra 60 workstation with 512 MB of RAM, 2 GB Swap, and 2.2 GB of disk space, Solaris 2.6.
  - CIPM for the 7200, see below for requirements.
  - Cisco Access Manager (CAM) for the Access Servers . It requires a Sun workstation, its exact specification depend on the number of ports to be managed. Solaris 2.5.1 and Oracle Enterprise Server 7.3.4 with 4 GB of available disk space (the database server is local or remote)
- **VPNSC:** for VPN service provisioning, auditing, SLA monitoring and accounting. VPNSC also uses Cisco IP Manager (CIPM) for configuration downloads/uploads. VPNSC 2 requires Sun workstations and Solaris 2.6. The exact hardware requirements depend on the the size of the VPN networks to be managed. CIPM 2.0 runs on separate hardware. It requires a minimum of Sun Ultra 60 (1 processor) workstation, 512 MB RAM with 500 MB of swap space, 10 GB of disk space, and Solaris 2.6. Oracle 8.0.5 Enterprise database must be installed.
- **AR:** for AAA functionality. The Access Registrar Release 1.5 is used. It runs on a Sun Sparc workstation with Solaris 2.6 or 2.7, 128 MB of RAM, 80 MB disk space.

- **CNR:** for IP address allocation. CNR 3.5 or 4.0 are appropriate. CNR 3.5(1) runs on Windows NT 4.0, Windows 2000, Solaris 2.5.1, Solaris 2.6, and Solaris 7. Network Registrar's 3.5(1) GUI also runs on Windows 95 and Windows 98.
- **Netflow:** for usage accounting of non-PPP connections. Only Netflow Collector is needed. Netflow Collector 3.0 runs on either Sun Ultra 1 or higher with at least 128 MB RAM, 512 MB of swap space, and 4 GB of disk space, Solaris version 2.5.1 or 2.6, or HP Class C or higher with at least 128 MB RAM, 512 MB of swap space, and 4 GB of disk space., UX version 11.0 (32-bit and 64-bit are supported).
- **Cisco Info Center (CIC):** for VPN fault monitoring. CIC Release 1.2 requires Sun Ultra-II or higher running Solaris 2.5.1 or 2.6 and Java 1.1, 256 Mbytes of main memory, 200 Mbytes of hard disk space, and 23 Mbytes available in /var/tmp.
- **Concord Network Health:** for VPN performance reporting. Integration of Network Health with the VPNSC is targeted for this summer.
- **RPMS:** for managing the Access Server resources. The RPMS requires a Sun Ultra 60 workstation running Solaris 2.6 or higher, and Oracle v7.3.4 or v8.04. Detailed software and hardware requirements are provided in the RPMS documentation.

Tunnels

The LAC retrieves the L2TP tunnel (VPDN) information from a Radius server, or local configuration.

Both methods allow load balancing among multiple VHG/PEs, but using Radius is more scalable. For load balancing, the Radius server returns a list of VHG addresses, and the LAC filters through that list in a specific order providing failover.

Both the AR and IOS support IETF standard tunnel attributes for passing tunnel information from the Radius to the NAS. These standard attributes are used instead of vendor-specific cisco-avpairs.

The VHG/PE is configured with a default VPDN to accept L2TP tunnels from any LAC or remote entity, or with VPDNs to only accept calls from LACs with given names (tunnels ids).

Other L2TP tunnels issues include:

- Tunnel authentication is optional and only local authentication is possible. Radius is not used for that purpose.
- Complete user authentication at the NAS is not performed.
- No requirement for multiple tunnels between the same (LAC,VHG/PE) pair.
- The number of sessions per L2TP tunnel is not limited.

VHG Farms

In some scenarios, the number of remote users, belonging to the same VPN customer, expected to log on to certain PoP is so small, such that enabling a VRF on one of the VHG/PE routers at that PoP won't be economical. In such a case when the remote user dials into a LAC at that PoP, its PPP session is L2TP tunneled over the MPLS core to a VHG/PE router having the remote user's VRF pre-instantiated on it. This VHG/PE router can be located at a nearby PoP or, alternatively, multiple VHGs can be clustered together at a central location, a VHG farm. Each VHG still functions as a PE routers as well.

The L2TP tunnel from LAC to VHG is routed using the global routing table, and a single L2TP tunnel can carry PPP sessions of different VPN customers.

The following functions are provided:

- Authorization by the SP Radius server
- Proxy authentication
- Authentication by the SP Radius server
- Return virtual interface configuration to the VHG/PE

Upon receipt of an incoming PPP session, the VHG/PE sends an Access-Request to the SP Radius server. The SP Radius server authorizes the PPP session based on the remote user's domain name or DNIS, and associates the PPP session with a specific VPN. The VPN is returned to the interface as configuration commands to be applied to the virtual interface being created for that PPP session.

Based on the domain name or DNIS, the SP Radius server proxies the request to the appropriate VPN Radius server for authenticating the remote user. Alternately, the SP Radius server can complete the authentication itself. See Appendix A, “AAA Radius Access to MPLS VPN Integration”.

Fault Monitoring

Fault monitoring is performed at the device, and service levels.

At the device level, fault monitoring is performed by the element managers (CEMF has an event manager component). CAM provides fault monitoring per dial port.

CIC is user at the service level to provide event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems. CIC is an OEM product from Micromuse's NetCool. CIC's release 2.0 provides eventing at the IP VPN service level through integration with VPNSC.

SLA Reporting

SLA reporting is performed using the Service Assurance Agent (SA Agent) in IOS. In conventional MPLS VPN customer sites, VPNSC configures SA Agent probes on managed CE routers or shadow CE routers. However, in remote access sites, there are no real CE router. The SA Agent probes is configured on the PE routers at the PoPs. It is not possible to configure them on the LACs, because a LAC is not connected to any particular VPN so the probes are not routed using the VRFs. VPNSC collects statistics from the SA Agent MIB and provides reports on a per VPN basis. For PPP users, performance numbers is derived from AR.

Concord's Net Health provides performance and SLA reporting at a VPN service level through integration with VPNSC.

RPMS is used to provide SLA information on measures such as incoming call rates for each VPN customer.

DSL L2TP Event Sequence

The following events occur when the remote user creates a PPPoX session over DSL to access its corporate network or ISP (i.e. customer network of Figure 4-9):

Step 1 The remote user initiates a PPPoE session, or the DSL router initiates a PPPoA session, over the DSL access network.

Step 2 The LAC accepts the PPPoX session.

Step 3 The LAC partially authenticates the remote user with CHAP or PAP. The domain name is used to determine whether the user is a VPN client. The LAC queries a AAA server to determine if the user is a VPN client. If the user is not a VPN client (it is using the DSL service provider also as his ISP), authentication continues on the LAC. If the user is a VPN client, the AAA server will return the address of a VHG/PE and other L2TP tunnel information to the LAC.

Step 4 If an L2TP tunnel does not already exist, the LAC initiates a tunnel to the VHG/PE (LNS). The NAS and the VHG/PE authenticate each other before any sessions are attempted within a tunnel. It is also possible for a VHG/PE to accept tunnel creation without any tunnel authentication of the NAS.

Step 5 Once the tunnel exists, a session within the tunnel is created for the remote user and the PPP session is extended to terminate on the VHG/PE.

Step 6 The LAC propagates all available PPP information (the LCP negotiated options and the partially authenticated CHAP/PAP information) to the VHG/PE.

Step 7 The VHG/PE associates the remote user with a specific customer MPLS VPN. The VPN's VRF (routing table and other information associated with a specific VPN) has been already instantiated on the VHG/PE.

Step 8 The VHG/PE completes the remote user's authentication.

Step 9 The VHG/PE obtains an IP address for the remote user.

Step 10 The remote user is now part of the customer VPN. Packets can flow from/to the remote user.

DSL L2TP Provisioning

Provisioning Dial L2TP access to MPLS VPN entails:

1. Initial configuration through router pre-staging, using config Xpress, using an element manager (for example, SCM), using CIPM templates, or any combination of the above. This configuration is not necessarily tied to VPN services and includes:
   a. configuration of the PE routers
   b. configuration of the AAA network servers using AR
   c. configuration of the AR and CNR servers on the VHG/PE

Note In this solution the Cisco IOS Command Line Interface (CLI) is used for configuring routers and Access Registrar (see "Cisco IOS Software Fundamentals" on page 1-9), and a Graphical User Interface (GUI) for CNR.

2. Although this is tied to customer provisioning, it is different from the VPN service provisioning (for example, add a site to VPN). An example would be a customer with an existing VPN requests access for dsl users. It includes:
   a. configuring access servers for new customers in one of the following methods
   - L2TP information Local on LAC
   - L2TP information on AAA server

   b. configuring the VHG/PE for a new customer
   - VRF configuration
   - L2TP information

   c. configuring components where user authentication & authorization takes place
   - on VHG/PE
   - on AR inside SP domain
   - proxy AA

   d. configuring accounting on AR
   e. configuring components where address management takes place
   - on VHG/PE (overlapping pools)
   - on AR
   - on CNR (DHCP)

Note Customer and service configurations differ from VPN service configurations of adding a VPN site for a customer with an existing VPN who might request access for dsl users.

3. VPN service configurations are critically repetitive tasks to automate, that include:
   a. actual service activation, performed by VPNSC, where a VPN is created, and CE sites and remote access sites are added to it.

Note You cannot use VPNSC on the VHG/PEs.

Note For VPNSC configuration, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Miscellaneous Component Configurations

For miscellaneous component configuration details, refer to the following corresponding URLs:

Table 4-3 DSL L2TP miscellaneous component configurations

Component	URL
AR	http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm
CNR	http://www/univercd/cc/td/doc/product/rtrmgmt/cnr/index.htm

Configuring the PE Routers

Perform the following steps to configure the PE routers.

Step 1 Configure the loopback interface.

a. Router (config)# **interface loopback [***number***]**

Step 2 Configure the IGP on the PE (OSPF, ISIS).

Step 3 Configure label switching on the interface connected to the MPLS cloud.

a. Router (config)# **ip cef**

b. Router (config-if)# **tag-switching ip**

Step 4 Configure BGP peer from VHG to loopback on the remote PEs.

a. Router (config)# **router bgp [***autonomous system number of sp***]**

b. Router (config-router)# **neighbor [***ip address of remote pe***] remote-as [***same autonomous number***]**

c. Router (config-router)# **neighbor [***ip address of remote pe***] update-source Loopback0**

Step 5 Configure BGP session to exchange VPN-IPV4 prefixes.

a. Router (config-router)# **address-family vpnv4**

b. Router (config-router-af)# **neighbor [***ip address of remote pe***] activate**

c. Router (config-router-af)# **neighbor [***ip address of remote pe***] send-community extended**

Step 6 Define a VPDN group that accepts L2TP and specifies a virtual template to use.

a. Router (config)# **vpdn enable**

b. Router (config)# **vpdn-group <***group number***>**

c. Router (config-vpdn)# **accept-dialin**

d. Router (config-vpdn-acc-in)# **protocol l2tp**

e. Router (config-vpdn-acc-in)# **virtual-template <***virtual template number***>**

Step 7 Configure virtual profile and virtual interface.

Configuring the AAA Network Server using AR

Perform the following steps to configure the AR application with a new NAS or VHG when using the Radius protocol on the NAS or VHG.

Step 1 Configure the LAC client on the AR.

a. Enter CLI configuration mode of AR.

admin@sun-ar% aregcmd -s

b. Change to client directory

--> **cd /radius/clients**

c. Add NAS or VHG to client directory

--> **add [***name of NAS or VHG***]**

d. Define IP address and shared key of NAS or VHG.

--> **set ipaddress [***ip address***]**

--> **set sharedsecret [***sharedsecret***]**

For Access Registrar (AR) configuration details, refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

Configuring the AR and CNR Servers on the LAC or VHG/PE

Perform the following steps to configure the LAC or VHG/PE, or both, with an AAA server.

Step 1 Enable the LAC or VHG/PE to use the Radius protocol for authorization and authentication.

a. Router (config)# Router (config)# **aaa new-model**

b. Router (config)# **aaa authentication ppp default local group radius**

c. Router (config)# **aaa authorization network default local group radius**

Step 2 Configure the Radius server on the VHG/PE or LAC.

a. Router (config)# **radius-server host [***ip address of radius server***] key [***sharedscret***]**

Note The sharedsecret has to be the same as the sharedsecret defined in Step 1d of "Configuring the AAA Network Server using AR" on page 48.

Configuring Access Servers for New Customers

To configure access servers for new customers perform **only one** the following procedures.

- L2TP information Local on LAC
- L2TP information on AAA server

When L2TP information is stored locally on LAC, perform the following steps:

Step 1 Enable VPN on the access server.

a. Router (config)# **vpdn enable**

Step 2 Enable the search order to look up L2TP tunnels.

a. Router (config)# **vpdn search-order domain**

Step 3 Define a new VPDN group for each user.

a. Router (config)# **vpdn-group [***number***]**

b. Router (config-vpdn)# **request-dialin**

c. Router (config-vpdn-req-in)# **protocol l2tp**

d. Router (config-vpdn-req-in)# **domain [***domain name***]**

e. Router (config-vpdn-req-in)# **exit**

f. Router (config-vpdn)# **initiate-to ip [***ip address of VHG***]**

Step 4 Define local username and password for tunnel authentication.

a. Router (config)# **username [***hostname***] password [***tunnel password***]**

Note The hostname used in the L2TP tunnel authentication is the hostname of the router by default and can be changed by using the following command under the VPDN group: Router (config-vpdn)# **local name [***hostname***]**

When L2TP information is stored on a AAA server, perform the following steps:

Step 1 Enable VPN on the access server.

a. Router (config)# **vpdn enable**

Step 2 Enable the search order to look up L2TP tunnels.

a. Router (config)# **vpdn search-order domain**

Step 3 Enable AAA to lookup L2TP information on the RADIUS server. Refer to "Configuring the AR and CNR Servers on the LAC or VHG/PE" on page 49.

Step 4 Configure the AR.

a. Configure the LAC as a client. Refer to "Configuring the AAA Network Server using AR" on page 48

b. Add a service to the AR.

--> **add /Radius/Services/[***service name***] [***service name description***] local "" "" RejectAll "" [***userlist name***]**

--> **set /Radius/DefaultAuthenticationService [***service name***]**

--> **set /Radius/DefaultAuthorizationService [***service name***]**

Note The authentication and authorization service can also be selected by scripting. For Access Registrar (AR) configuration details, refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

c. Add a userlist to the AR.

--> **add /Radius/Userlists/[***userlist name***]**

Note The userlist name must be the same as the userlist defined in b. Add a service to the AR.

d. Add tunnel names to userlists.

--> **add /Radius/UserLists/[***userlist name***]/[***domain name***] [***domain name description***] cisco TRUE "" [***attributes list***]**

Note The userlist name must be the same as the userlist defined in b. Add a service to the AR.

Note All user records inside the AR database containing tunnel information must have the password field set to cisco.

The command for adding a DNIS user is:

--> **add /Radius/UserLists/[***userlist name***]/dnis:[***dnis number***] [***dnis description***] cisco TRUE "" [***attributes list***]**

e. Add tunnel attributes.

--> **add /Radius/Profiles/[***attributes list***]**

--> **cd /Radius/Profiles/[***attributes list***]/Attributes**

--> **set tunnel-medium-type_tag1 1**

--> **set tunnel-password_tag1 [***tunnel password***]**

--> **set tunnel-server-endpoint_tag1 [***vhg ip address***]**

--> **set tunnel-type_tag1 3**

Note If you are using AR 1.6 revision 1 or higher, syntax changes for the following commands
--> **set tunnel-medium-type_tag1 ipv4**
--> **set tunnel-type_tag1 l2tp**

For configuring L2TP information on RPMS, refer to the Cisco Resource Pool Manager Server Configuration Guide at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/rpmsconf/index.htm

Configuring VHG/PE for a New Customer

To configure the VRF, perform the following steps:

Note Make sure you performed the initial BGP configuration in "Configuring the PE Routers" on page 4-48 before proceeding.

Step 1 Define the VRF.

a. Router (config)# **ip vrf [***vpn name***]**

b. Router (config-vrf)# **rd** [*route descriptor value*]

c. Router (config-vrf)# **route-target import** [*route target value*]

d. Router (config-vrf)# **route-target export** [*route target value*]

Step 2 Configure the loopback.

a. Router (config)# **interface loopback [***number***]**

b. Router (config-if)# **ip vrf forwarding [***vpn name***]**

Note The vpn name must be the same as defined in Step 1a above.

c. Router (config-if)# **ip address [***ip address***] [***netmask***]**

Step 3 Configure the BGP session to transport VRF information.

a. Router (config)# **router bgp [***autonomous system number***]**

Note The autonomous system number must be the same as defined in Step 4a of "Configuring the PE Routers" on page 48.

b. Router (config-router)# **address-family ipv4 vrf [***vpn name***]**

c. Router (config-router-af)# **redistribute connected metric 1**

To configure the L2TP information, perform the following steps:

Step 1 Enable VPDN on the VHG.

a. Router (config)# **vpdn enable**

Step 2 Define a new VPDN group for each user.

Note VPDN on a home gateway can only be stored locally on the router.

a. Router (config)# **vpdn-group [***number***]**

b. Router (config-vpdn)# **accept-dialin**

c. Router (config-vpdn-acc-in)# **protocol l2tp**

d. Router (config-vpdn-acc-in)# **virtual-template [***virtual template number***]**

e. Router (config-vpdn-acc-in)# **exit**

f. Router (config-vpdn)# **terminate-from hostname [***hostname***]**

Note The hostname must be the same as the hostname defined in Step 4 of "Configuring Access Servers for New Customers" on page 49.

Step 3 Define local username and password for tunnel authentication.

a. Router (config)# **username [***hostname***] password [***tunnel password***]**

Configuring Authentication & Authorization Components

To configure components where user authentication & authorization takes place, perform **only one** of the following procedures.

- on VHG/PE
- on AR inside SP domain
- proxy AA

To configure user authentication & authorization on the VHG/PE, perform the following steps:

Step 1 Create a virtual template.

a. Router (config)# **interface virtual-template [***number***]**

Note The virtual template number has to be the same as the virtual template number in Step 2d of "Configuring VHG/PE for a New Customer" on page 51.

b. Router (config-if)# **ip vrf forwarding [***vpn name***]**

Note The vpn name has to be the same as the vpn name in Step 1a of "Configuring VHG/PE for a New Customer" on page 51.

c. Router (config-if)# **ip unnumbered loopback [***loopback number***]**

Note The loopback number has to be the same as the loopback number in Step 2a of "Configuring VHG/PE for a New Customer" on page 51.

d. Router (config-if)# **ppp authentication chap callin**

Step 2 Configure username and password for all VPDN users belonging to the new customer.

e. Router (config)# **username [***username@domain***] password [***user password***]**

Note For each new customer you need to define a new virtual template when using the local AA methods on the VHG. IOS is limited to 25 virtual templates maximum.

To configure user authentication & authorization on the AR inside the SP domain, perform the following:

Step 1 Configure the VHG.

a. Router (config)# **aaa new-model**

b. Router (config)# **aaa authentication ppp default local group radius**

c. Router (config)# **aaa authorization ppp default local group radius**

d. Router (config)# **virtual-profile aaa**

e. Router (config)# **interface virtual-template [***number***]**

Note The virtual template number has to be the same as the virtual template number in Step 2d of "Configuring VHG/PE for a New Customer" on page 51.

f. Router (config-if)# **ppp authentication chap callin**

g. Router (config-if)# **exit**

h. Router (config)# **radius-server host [***radius server ip address***] key [***sharedsecret***]**

Step 2 Configure the AR.

a. Adding the VHG as a client.

--> **add /Radius/Clients/[***vhg name***] [***vhg description***] [***vhg ip address***] [***sharedsecret***] NAS "" [***script* **]**

Note The script tells which service needs to be selected for VPDN user authorization and authentication.

b. Adding the service.

--> **add /Radius/Services/[***vpdn name***] {***vpdn description***] local "" "" RejectAll "" [***vpdn userlist name***]**

Note The VPDN name is derived from the username that is sent by the VHG within the RADIUS access request packet. This is provided by the script in 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

c. Adding the userlist.

--> **add /Radius/Userlists/[***vpdn userlist name***]**

d. Adding VPDN users for the userlist.

--> **add /Radius/UserLists/[***vpdn userlist name***]/[***vpdn username***] [***vpdn user description***] [***vpdn user password***] TRUE "" [***vpdn user attrbutes***]**

e. Defining attributes for selecting VPN service.

--> **add /Radius/Profiles/[***vpdn user attrbutes***]**

--> **cd /Radius/Profiles/[***vpdn user attrbutes***]/Attributes**

--> **set service-type framed**

--> **set framed-protocol ppp**

--> **set cisco-avpair "lcp:interface-config=ip vrf forwarding [***vpn name***]\\n ip unnumbered Loopback [***number***]**

Note The vpn name has to be the same as the vpn name in Step 1a of "Configuring VHG/PE for a New Customer" on page 51.

Note The loopback number has to be the same as the loopback number in Step 2a of "Configuring VHG/PE for a New Customer" on page 51.

To configure proxy AA on the SP AR server, perform the following steps:

Step 1 Configure the VHG.

a. Router (config)# **aaa new-model**

b. Router (config)# **aaa authentication ppp default local group radius**

c. Router (config)# **aaa authorization ppp default local group radius**

d. Router (config)# **virtual-profile aaa**

e. Router (config)# **interface virtual-template [***number***]**

Note The virtual template number has to be the same as the virtual template number in Step 2d of "Configuring VHG/PE for a New Customer" on page 51.

f. Router (config-if)# **ppp authentication chap callin**

g. Router (config-if)# **exit**

h. Router (config)# **radius-server host [***radius server ip address***] key [***sharedsecret***]**

Step 2 Configure the SP AR.

a. Adding the VHG as a client.

--> **add /Radius/Clients/[***vhg name***] [***vhg description***] [***vhg ip address***] [***sharedsecret***] NAS "" [***script* **]**

Note The script tells which service needs to be selected for VPDN user authorization and authentication.

b. Adding remote AA servers to which you proxy AA information.

--> **add /Radius/RemoteServers/[***remote server host name***] [***remote server description***] radius [***remote server ip address***] 1645 300000 [***sharedsecret***]**

Note The remote server IP address is not reachable from the SP AA server because the MPLS service provider cloud does not have VPN customers routing information. Due to this we have to use route leaking or a management VPN to provide the SP AA server with routing information to go to the remote server defined here. For more information on VPN management refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/index.htm

c. Adding a service.

--> **add /Radius/Services/[***vpdn name***] [***vpdn description***] radius**

--> **cd /Radius/Services/[***vpdn name***]/RemoteServers**

--> **set 1 [***remote server host name***]**

Note The VPDN name is derived from the username that is sent by the VHG within the RADIUS access request packet. This is provided by the script in 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

Configuring Accounting Between the VHG and AR

To configure accounting between the VHG and AR, perform the following steps:

Note Make sure you performed the configuration of the user authentication & authorization, on the AR inside the SP domain, in "Configuring Authentication & Authorization Components" on page 4-52 before proceeding.

Step 1 Configure the VHG.

a. Router (config)# **aaa accounting network default start-stop group radius**

Step 2 Configure the AR.

--> **add /radius/services/[** *accounting service name*]

--> **cd /radius/services/[** *accounting service name*]

--> **set type file**

Note The accounting service name is derived from the username that is sent by the VHG within the RADIUS accounting request packet. This is provided by the script in 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

Configuring Address Management Components

To configure components where address management takes place, perform the only one of the following procedures.

- on VHG/PE (overlapping pools)
- on AR
- on CNR (DHCP)

To configure address management on the VHG/PE, perform the following steps:

Step 1 Create an address pool on the VHG.

a. Router (config)# **ip local pool [***vpn customer address pool***] [***start ip address***] [***end ip address***]**

Step 2 If you configured user authentication and authorization on the VHG/PE, in "Configuring Authentication & Authorization Components" on page 52, you need to add the following command to the virtual template configuration.

Router (config-if)# **peer default ip address pool [***vpn customer address pool***]**

If you configured user authentication and authorization on the AR inside the AP domain, in "Configuring Authentication & Authorization Components" on page 52, you need to add the following command to the attributes for selecting VPN service.

--> **set cisco-avpair "lcp:interface-config=ip vrf forwarding [***vpn name***]\\n ip unnumbered Loopback[***number***]\\n peer default ip address pool [***vpn customer address pool***]"**

To configure address management on the AR, perform the following steps:

Note Make sure you performed the accounting configuration in "Configuring Accounting Between the VHG and AR" on page 4-55 before proceeding.

Tip Accounting is mandatory for address management on an AR.

Step 1 Define the resource manager on the AR.

a. --> **add /Radius/ResourceManagers/[***resource manager for vpn customer***]**
b. --> **cd /Radius/ResourceManagers/[***resource manager for vpn customer***]**
c. --> **set type ip-dynamic**
d. --> **set netmask 255.255.255.255**
e. --> **cd IPaddresses**
f. --> **add [***ip address range for address pool***]**

Step 2 Define the session manager.

a. --> **add /Radius/SessionManagers/[***session manager name* **]**
b. --> **cd /Radius/SessionManagers/[***session manager name***]/ResourceManagers**
c. --> **add 1 [***resource manager for vpn customer***]**

Note The session manager name is derived from the username that is sent by the VHG within the RADIUS access request packet. This is provided by the script in 2a. For scripting procedures, refer to http://www/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm.

To configure address management on the on CNR (DHCP), perform the following steps:

Step 1 Configure the VHG.

If you configured user authentication and authorization on the VHG/PE, in "Configuring Authentication & Authorization Components" on page 52, you need to add the following command to the virtual template configuration.

Router (config-if)# **peer default ip address dhcp**

If you configured user authentication and authorization on the AR inside the AP domain, in "Configuring Authentication & Authorization Components" on page 52, you need to add the following command to the attributes for selecting VPN service.

--> **set cisco-avpair "lcp:interface-config=ip vrf forwarding [***vpn name***]\\n ip unnumbered Loopback[***number***]\\n peer default ip address dhcp"**

Configure the DHCP server.

Router (config)# **ip helper-address [***ip address dhcp server***]**

Note The IP address of the loopback referenced on the virtual template, or AA user specific settings, needs to be in the global routing table of the SP cloud.

Step 2 Configure the CNR.

a. Router (config-if)# **peer default ip address dhcp**

nrcmd> **scope [***primary scope***] create [***ip address range primary scope 1***] [***primary netmask***]**

Note The IP address of the primary scope should contain the IP address of the loopback number referenced in the virtual template configuration.

nrcmd> **scope [***secondary scope***] create [***ip address range secondary scope 1***] [***netmask***]**

nrcmd> **scope [***secondary scope***] addRange [***start ip address secondary scope 1***] [***end ip address secondary scope 1***]**

nrcmd> **scope [***secondary scope***] set primary-scope [***primary scope***]**

nrcmd> **scope [***secondary scope***] set primary-addr [***ip address range primary scope 1***]**

nrcmd> **scope [***secondary scope***] set primary-mask** [*primary netmask*]

Common Components and Features

This section describes components and features that are common to more than one DSL architecture. An understanding of these features and the alternative ways in which they can be implemented can help you plan your DSL configuration.

Framed-Route VRF Aware Feature

You can use the Framed-Route VRF Aware feature to apply static IP routes to a particular VRF table rather than the global routing table. The feature makes RADIUS Attribute 22 (Framed-Route) and a combination of Attribute 8 (Framed-IP-Address) and Attribute 9 (Framed-IP-Netmask) VRF aware.

You can configure a per-user static route using the framed-route attribute in any of three ways.

- Use the cisco VSA route command
- Use the framed-route attribute. When it receives a framed-route from the RADIUS server, the VHG/PE checks whether the user is a VPN customer. If so, then the static route is implemented in the routing table of the VRF to which the user belongs.
- Use the framed-ip-address /framed-netmask, which has the same function as framed route.

This feature applies to PPPox, PPPox SSG, and L2TP.

Configure a Per-user Static Route Using the Framed-route Attribute on the RADIUS AAA Server,

To use the cisco VSA route command, enter:

```
cisco-avpair "ip:route = vrf vrf-name 10.10.100.0 255.255.255.0 [next hop ip address(opt)]"
```

To use the framed route attribute, enter:

```
framed-route = 10.10.100.0 255.255.255.0 [next hop ip address(opt)]
```

To use the framed-ip-address /framed-netmask (same function as framed route above), enter:

```
framed-route = 10.10.100.0/24 [next hop ip address(opt)]
```

Example 4-2 Example of RADIUS Access Registrar Configuration

```
[ //localhost/Radius/Profiles/827-fr/Attributes ]
    cisco-avpair = "lcp:interface-config#1= ip vrf forwarding FRtest.com"
    cisco-avpair = "lcp:interface-config#2= ip unnumbered FastEthernet0/0"
    cisco-avpair = "lcp:interface-config#3= encapsulation ppp"
    Framed-IP-Address = 10.10.8.1
    Framed-IP-Netmask = 255.255.255.224
    Framed-Protocol = ppp
    Framed-Routing = None
    Service-Type = Framed
```

On-demand Address Pools (ODAP)

In on-demand address pools (ODAP), a central SP RADIUS server manages a block of addresses for each customer. Each pool is divided into subnets of various sizes, and the server assigns subnets to the VHG/PE or NAS/PE on request.

The VHG/PE or NAS/PE acts as a DHCP server. On the VHG/PE or NAS/PE, one on-demand pool is configured for each customer VPN supported by that router. Upon configuration, the VHG/PE or NAS/PE's pool manager requests an initial subnet from the server.

Address management is on demand because address pool subnets are allocated or released based on a threshold. If use exceeds a defined ceiling threshold, the pool manager requests an additional subnet from the server and adds it to the on-demand pool. If use falls below a floor threshold, the pool manager attempts to free one, or more then one, of the on-demand pool's subnets to return it to the server. The VRF routing table on the VHG/PE or NAS/PE is updated with the subnet route whenever a range of addresses is requested from the AR.

ODAP's benefits include efficient management of address space and dynamic address summarization on the VRF table. ODAP has two main drawbacks:

- An allocated subnet is not released so long as a single dial-in client in a given VRF is connected (using an IP address)
- BGP route summarization is not possible with ODAP, because multiple PEs have subnets of a major Class C or Class B subnet, there is no way to summarize on the Class C or Class B subnet. Using ODAP thus causes an increase in the BGP routing table.

Consider using ODAP, then, if subnet management is more important than route summarization.

ODAP requires Access Registrar 1.7 or 1.7R1.

ODAP can be used with the following DSL architectures:

- PPPoX
- PPPoX SSG
- DSL L2TP
- RFC 1483
- RFC 1483 RBE

Configuring ODAP on the VHG/PE or NAS/PE

If you are implementing ODAP, perform the following steps on VHG/PE or NAS/PE.

Step 1 Configure a DHCP address pool on a Cisco IOS DHCP server.

Router(config)# **ip dhcp pool** *address pool name*

Step 2 Tie the pool to a particular VPN.

a. Router(config-dhcp)# **vpn type 1** *vrf name*

b. Router(config-dhcp)# **origin aaa autogrow** *size*

Step 3 Configure the network access server to recognize and use vendor-specific attributes.

a. Router(config)# **radius-server host** *ip address*

b. Router(config)# **radius-server key** *string*

c. Router(config)# **radius-server vsa send accounting**

d. Router(config)# **radius-server vsa send authentication**

Step 4 Enable an address pooling mechanism used to supply IP addresses.

Router(config)# **ip address-pool dhcp-pool**

Step 5 Create a virtual template interface.

Router(config)# **interface virtual-template** *number*

Step 6 Specify an address from the DHCP mechanism to be returned to a remote peer connecting to this virtual-template interface.

Router(config-if)# **peer default ip address dhcp-pool**

Note Since the user name might be the same as the VPDN domain name, either use scripts on the RADIUS AR to differentiate between requests for subnets and VPDN information, or make the VRF name different from the domain name.

Example 4-3 ODAP Configuration Example

```
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius (to release subnets accounting
   needed)
ip dhcp pool odap-test  vrf <vrf-name> (part of access-request username)
origin aaa subnet size initial /27 autogrow /27
radius-server host 10.10.100.3 radius-server key wwradius-server vsa send accounting (VSA
attributes in accounting packet)
radius-server vsa send authentication (VSA attributes in access-request packet)
ip address-pool dhcp-pool (global command – use local DHCP VRF pools)
int virtual-template X
peer default ip address dhcp-pool
```

Configuring the RADIUS AR for ODAP

To configure the RADIUS AR for ODAP, use a script that accomplishes the following:

- Selects a service with its name ***<vrf name>-odap*** and a session manager with the same name as the service

- Configures the resource manager for ODAP

Cisco AR 1.7 R1 has been enhanced to make ODAP functionality more accessible and to enable ODAP requests and normal user authentication to occur on the same Cisco AR server. To achieve this functionality, a new Cisco vendor script **CiscoWithODAPIncomingScript** was written to direct ODAP requests to particular services and session managers. **CiscoWithODAPIncomingScript** also provides the same functionality as the previous **CiscoIncomingScript**.

Additionally, Cisco AR 1.7 R1 has a new vendor type, **CiscoWithODAP** which references **CiscoWithODAPIncomingScript** as its IncomingScript and references the existing script, **CiscoOutgoingScript,** as its Outgoing Script.

For Cisco AR configuration details, see

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/users/odap.htm#xtocid1.

Using Templates for Configuration

You can use VPN SC 2.1 to expedite many provisioning tasks by creating templates to generate Cisco IOS configuration files. The VPNSC Template Manager can be used to provide initial configuration for any service provider core device or edge device. The Template Manager can be used as a stand-alone tool to generate complete configuration files that you can download to any VPN Solutions Center target. You can download a VPNSC service request and an Cisco IOS configuration file through the console in one download operation. This edge device staging method creates a template and applies the service request in one step.

VPNSC creates an initial VPNSC configlet. Through the Template Manager, you create a template configuration file. You then associate this file with a service request, which effectively merges the VPNSC configlet and the template configuration file. You can then download this merged VPNSC configlet to the target routers.

Before you can integrate templates with service requests, you must edit the csm.properties file and change the following property from its default setting of false to true, then restart VPNSC.

```
netsys.vpn.serviceRequest.showTemplates=true
```

Creating Templates and Configuration Files

Following are the main steps to create templates and configuration files. For more information, refer to the VPN Solution Center documentation at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/2_1/index.htm

Step 1 From the VPN Console, select the Template Console under Tools. Create a new Template folder under Template Home.

Step 2 Select the newly created template and enter the desired IOS configuration commands in the Template Body.

Step 3 After entering the IOS commands, you can create Variables and assign Attributes to these Variables.

Step 4 Create a Template Data File under an appropriate Data Folder. A template data file is a text file that stores the variable values necessary to generate a template file. A valid template data file contains a name-value pair for each variable defined in a template.

Step 5 After selecting the values or range of values for the variables, create the configuration file by selecting the template and the associated data file.

The generated configuration can then be downloaded directly into the target router(s).

Template Examples

Following are examples of templates used for common provisioning tasks.

Example 4-4 Sample template for provisioning a virtual template

```
interface Virtual-Template $Virtual-Template
ip vrf forwarding $vrf_name
ip unnumbered $loopback_int
peer default ip address pool $pool+$pool_number
```

Example 4-5 Sample template for provisioning ATM interfaces

```
interface $ATM_intf
pvc $vpi+$slash+$vci
encapsulation aal5mux ppp virtual-template $Virtual-Template
```

Example 4-6 Sample template for provisioning one virtual template and many sub-interfaces

```
interface Virtual-Template $Virtual-Template
ip vrf forwarding $vrf_name
ip unnumbered $loopback_int
peer default ip address pool $pool+$pool_number

#repeat($vci,$i)
{
interface $ATM_intf
pvc $vpi+$slash+$vci[$i]
encapsulation aal5mux ppp virtual-template $Virtual-Template
}
```

Example 4-7 Sample configlet generated by the VPNSC

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! Generated by Cisco Template Provision System
!!
!! template = /Naiad/VT-PPPOA
!! datafile = /Data0
!!
!! Thu Sep 20 17:13:50 EDT 2001
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 interface Virtual-Template 1
 ip vrf forwarding V1:VPN1
 ip unnumbered loopback1
 peer default ip address pool pool1

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! Generated by Cisco Template Provision System
!!
!! template = /Naiad/ATM-PPPOA
!! datafile = /Data0
```

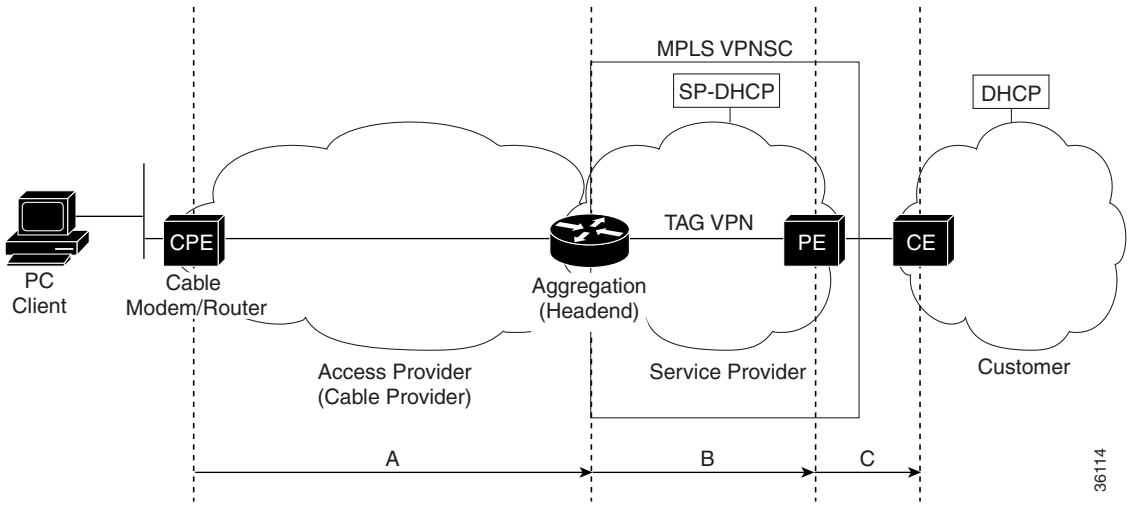
```
!! Thu Sep 20 17:13:50 EDT 2001
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Cable Access to MPLS VPN Integration

When accessing the Cisco MPLS VPN solution over a DOCSIS 1.0-compliant hybrid fiber-coaxial (HFC) network, the PC client obtains a DHCP address from the secondary IP address range configured on the cable subinterface attached to its cable access router. A session initiated by a client as depicted in Figure 5-1:

1. Transmits through the cable access router attached to the VPN subinterface determined by its DHCP assigned IP address
2. Routes packets to and from the PC across the MPLS VPN cloud
3. Distributes customer network packets through C back to the TAG VPN to the user

Figure 5-1 Cable Access to MPLS VPN



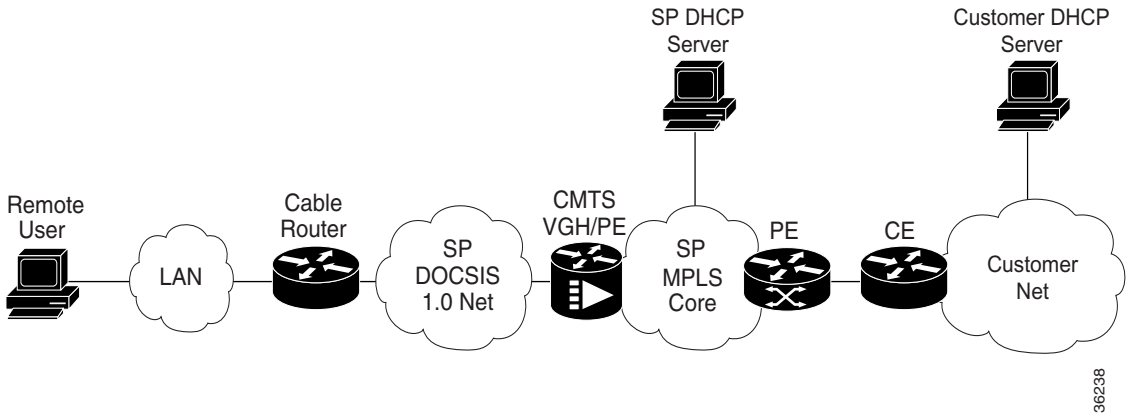
Cable DOCSIS 1.0 SID to MPLS VPN Integration

In a DOCSIS 1.0-compliant HFC network, all traffic from a given cable access router is identified by the same Service ID (SID). On the VHG/PE, all traffic with the same SID value terminates on the same subinterface. At the VHG/PE, the subinterface is statically configured to map all traffic to a specific

VRF. As a result, traffic from all CPEs behind a given cable access router is mapped to the same VPN. There is no remote user authorization and authentication necessary in this solution. Address assignment is DHCP-based. Accounting is based on Netflow.

The VPN to which a remote cable access router is attached is determined by the IP address assigned by a DHCP server. Cisco Network Registrar (CNR) is the DHCP server used in this solution. Client class processing is used on CNR to determine which subnet and subsequent VPN the cable access router attaches to, and is based on the cable access router MAC address.

Figure 5-2 Cisco VPN Cable Access DOCSIS 1.0 SID MPLS Integration



Note Whenever a service provider (SP) is mentioned in this section, it refers to the multiple service operator (MSO) in cable terminology.

CPE Equipment

Cisco uBR924 cable access routers are used to connect the remote access users to the SP DOCSIS 1.0-compliant HFC network. At the residential side, the cable access router is attached to a LAN connecting to the remote users' host PCs.

Note The Cisco uBR924 router is EOL. Please refer to the EOL page for further information http://www.cisco.com/univercd/cc/td/doc/pcat/elhw__g1.htm#xtocid0 and/or the Cisco Product page http://www.cisco.com/public/products_prod.shtml.

VHG/PE Routers

The following VHG/PE platforms are used:

- Cisco uBR7223 has up to two cable modem cards
- Cisco uBR7246 has up to four cable modem cards

Note The Cisco uBR7223 and Cisco uBR7246 routers are EOL. Please refer to the EOL page for further information http://www.cisco.com/univercd/cc/td/doc/pcat/elhw__g1.htm#xtocid0 and/or the Cisco Product page http://www.cisco.com/public/products_prod.shtml.

HFC Network

The SP access network is a DOCSIS 1.0-compliant HFC network. Cable access routers connect over the HFC network to a Cisco uBR7223 or Cisco uBR7246. At the headend, the Cisco uBR7223 or Cisco uBR7246 routes packets between the HFC network and the MPLS VPN backbone. In this case, the Cisco uBR7223 or Cisco uBR7246 functions as the PE router.

Note The Cisco uBR7223 and Cisco uBR7246 routers are EOL. Please refer to the EOL page for further information http://www.cisco.com/univercd/cc/td/doc/pcat/elhw__g1.htm#xtocid0 and/or the Cisco Product page http://www.cisco.com/public/products_prod.shtml.

DHCP Server

Cisco Network Registrar (CNR) serves as the DHCP server for this solution. CNR 3.5 or 4.0 are appropriate. CNR 3.5(1) runs on Windows NT 4.0, Windows 2000, Solaris 2.5.1, Solaris 2.6, and Solaris 7.

Note CNR 3.5, CNR 3.5.1, and CNR 4.0 are EOL. Please refer to the EOL page for further information http://www.cisco.com/univercd/cc/td/doc/pcat/elhw__g1.htm#xtocid0 and/or the Cisco Product page http://www.cisco.com/public/products_prod.shtml.

Cisco Network Registrar's 3.5(1) GUI also runs on Windows 95 and Windows 98.

Address Management

DHCP is used for address assignment in DOCSIS 1.0 SID to MPLS VPN integration. DHCP requests are handled by one or a combination of the following methods:

- The SP DHCP server assigns addresses to cable access routers based on the MAC address and whether or not the GIADDR parameter has been included in the request. The DHCP server can also provide IP addresses to host PCs within a VPN. This implies that the VPN customer assigns blocks of addresses from its address space to the SP, and that the SP manages these addresses and assigns them to the VPN customers.
- The customer DHCP server is used to allocate IP addresses to hosts within its VPN.

Note The term "customer DHCP server" refers to either an enterprise customer or an open-access ISP.

Both the cable access router and the corresponding VHG/PE interface must have IP addresses. The address for the subinterface must be provisioned. The cable access router requests an address from DHCP when it boots up. The request is relayed by the VHG/PE to the appropriate DHCP server. It could

be a SP DHCP server or the VPN DHCP server. The DHCP server assigns an address to the cable access router based on its MAC address and the GIADDR of the VHG/PE that forwarded the request. The cable access router's MAC address is provisioned at the DHCP server and is bound to a specific service/VPN.

Note Each subinterface and each VRF must be configured with a primary and secondary IP address. Cable access routers get their IP addresses from a primary IP address space, whereas PCs on the LAN behind the cable access router get their IP addresses from a secondary address space.

The addresses assigned to the cable access router and the VHG/PE's subinterface may be private addresses (assigned from the service provider's private pool) on the condition that these interfaces must be reachable from other PE routers connected to the same VPN.

When host PC located on the cable access router's LAN boots up, it initiates a similar series of steps in that it sends a DHCP discover request, which the cable access router passes on to the VHG/PE router. The VHG/PE relays the request to the appropriate DHCP server. The DHCP server assigns an address to the PC from the VPN's address pool, that is, from the ISP's address pool.

Accounting

Netflow is used for accounting in DOCSIS 1.0 SID to MPLS VPN integration. Netflow collects per-flow statistics such as time of first packet, time of last packet, number of packets, and number of octets. A flow is identified by source address, source port, destination address, and destination port. When configured for Netflow accounting, the VHG/PE collects per-flow accounting data and exports it to a Netflow Collector workstation, which stores it in flat files. A Netflow Analyzer is then used for analyzing the collected data.

Core Network

The DOCSIS 1.0 SID to MPLS VPN integration supports two types of core networks, IP MPLS and ATM MPLS.

Network Management

The network management components relevant for this solution are:

- Element managers—Cisco Cable Manager (CCM) for configuring the Cisco uBR7223 and Cisco uBR7246 VHG/PEs, and the Cisco uBR924 cable access routers.

  Note The Cisco uBR7223, Cisco uBR7246, and Cisco uBR924 routers are EOL. Please refer to the EOL page for further information http://www.cisco.com/univercd/cc/td/doc/pcat/elhw__g1.htm#xtocid0 and/or the Cisco Product page http://www.cisco.com/public/products_prod.shtml.

  CCM Release 2.2 requires a Sun Ultra 60 workstation for small deployments (up to 20,000 cable modems) or a Sun Enterprise 250 workstation for large deployments (over 20,000 cable modems) with dual processors, Solaris 2.6 OS, 9 GB of available disk space, and 2 GB of RAM.

- VPNSC—For VPN service provisioning, auditing, SLA monitoring and accounting. VPNSC also uses Cisco IP Manager (CIPM) for configuration downloads/uploads.

- CNR—For IP address allocation.
- Netflow—For usage accounting.
- Cisco Info Center (CIC)—For VPN fault monitoring.
- Concord Network Health—For VPN performance reporting.

Fault Monitoring

Fault monitoring is performed at the device and service levels.

At the device level, fault monitoring is performed by the element managers. (CEMF has an event manager component.) CCM provides fault monitoring per dial port.

CIC is used at the service level to provide event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems. CIC is an OEM product from Micromuse's NetCool. CIC's release 2.0 provides eventing at the IP VPN service level through integration with VPNSC.

SLA Reporting

SLA reporting is performed using the Service Assurance Agent (SA Agent) in IOS. In conventional MPLS VPN customer sites, VPNSC configures SA Agent probes on managed CE routers or shadow CE routers. However, in remote access sites, there is no real CE router. The SA Agent probes are configured on the PE routers at the POPs and are not configured on the NAS, because a NAS is not connected to a particular VPN prohibiting probes being routed using VRFs. VPNSC collects statistics from the SA Agent MIB and provides reports on a per-VPN basis. For PPP users, performance numbers are derived from AR.

Concord's Net Health provides performance and SLA reporting at a VPN service level through integration with VPNSC.

RPMS is used to provide SLA information regarding incoming call rates per VPN customers, and so on.

The SA Agent probes are configured on the cable access routers at the CPE.

DOCSIS Provisioning

Provisioning Cable DOCSIS 1.0 SID to MPLS VPN integration entails:

1. Initial configuration through router pre-staging, using config Xpress, using an element manager (e.g., SCM), using CIPM templates, or any combination of the above. This configuration is not necessarily tied to VPN services and includes:
   a. Configuring the Cisco uBR7200 VHG/PE routers and cable access routers at the CPE using SCM.
   b. Configuring the SP CNR server.
   c. Configuring the VPN/ISP DHCP server.

Note In this solution the Cisco IOS command line interface (CLI) is used for configuring routers and Access Registrar (see the "Cisco IOS Software Fundamentals" section on page 1-9) and a graphical user interface (GUI) for RPMS and CNR.

2. Although this is tied to customer provisioning, it is different from the VPN service provisioning (for example, adding a site, adding a Cisco uBR7223 or Cisco uBR7246, or adding a VPN). An example would be a customer with an existing VPN requesting access for cable users. This includes:
   a. Configuring the VHG/PE for a new customer by adding the required VRF configuration.

Note VPNSC 1.2 supports the provisioning of SID to VRF mapping and the relevant configuration on both VHG/PE and CPE routers. Refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

   b. Configuring the customer cable access router.
3. VPN service configurations are repetitive tasks that are critical to automate, including:
   c. Actual service activation, performed by VPNSC, where a VPN is created and CE sites and remote access sites are added to it.

Note For VPNSC configuration, refer to the MPLS VPNSC documentation suite at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Configuring Cisco uBR7200 VHG/PE Routers

Perform the following steps to configure the Cisco uBR7200 VHG/PE routers and cable access routers at the CPE using SCM.

Note This example is just one way of performing this configuration task.

Step 1 Create a management VPN where three VPNs are established with “management” serving as the management VPN by entering the following IOS command lines:

a. `Router (config)# ip vrf management`
b. `Router (config-vrf)# rd 100:1`
c. `Router (config-vrf)# route-target export 100:1`
d. `Router (config-vrf)# route-target import 100:1`
e. `Router (config-vrf)# route-target import 1000:1000`
f. `Router (config)# ip vrf vpn2`
g. `Router (config-vrf)# rd 200:1`
h. `Router (config-vrf)# route-target export 200:200`
i. `Router (config-vrf)# route-target export 1000:1000`
j. `Router (config-vrf)# route-target import 200:200`
k. `Router (config-vrf)# route-target import 100:1`
l. `Router (config)# ip vrf vpn3`
m. `Router (config-vrf)# rd 300:1`
n. `Router (config-vrf)# route-target export 300:300`
o. `Router (config-vrf)# route-target export 1000:1000`
p. `Router (config-vrf)# route-target import 300:300`
q. `Router (config-vrf)# route-target import 100:1`

The management VPN learns the routes from the other VRFs from the import statement. The other two VPNs (referred to as "vpn2" and "vpn3") export their routes to the management VPN and import the management VPN's routes. Refer to the "Sample VHG/PE Configuration File" section on page 5-8 for a complete sample Cisco uBR7246 configuration file featuring this type of VPN configuration.

Note The management VPN exports and imports routes to and from each of the other VPNs. Nonmanagement VPNs do not exchange information with one another, however, thus preserving isolation between nonmanagement VPNs.

Step 2 Configure the cable subinterfaces on the VHG/PE by entering the following IOS command lines.

For provisioning and management:

a. `Router (config)# interface Cable3/0.1`

b. `Router (config-if)# ip vrf forwarding management`

c. `Router (config-if)# cable dhcp-giaddr policy`

d. `Router (config-if)# cable helper-address 24.25.1.18`

For VPN cable access router and VPN users subnets

a. `Router (config)# interface Cable3/0.2`

b. `Router (config-if)# ip vrf forwarding vpn2`

c. `Router (config-if)# ip address 24.25.12.1 255.255.255.0 secondary`

d. `Router (config-if)# ip address 24.25.13.1 255.255.255.0`

e. `Router (config-if)# cable dhcp-giaddr policy`

f. `Router (config-if)# cable helper-address 24.25.1.18 cable-modem`

g. `Router (config-if)# cable helper-address 10.15.20.1 host`

For non-VPN cable and users subnets

a. `Router (config)# interface Cable3/0.3`

b. `Router (config-if)# ip address 24.25.15.1 255.255.255.0 secondary`

c. `Router (config-if)# ip address 24.25.14.1 255.255.255.0`

d. `Router (config-if)# cable dhcp-giaddr policy`

e. `Router (config-if)# cable helper-address 24.25.1.18 cable-modem`

f. `Router (config-if)# cable helper-address 10.19.15.1 host`

The first subinterface is placed in the management VPN. It is configured with a cable helper-address that forwards all DHCP requests to a Cisco Network Register DHCP server. The CNR DHCP server is connected to a router interface within the management VPN, either on this router or on a remote router. Create cable subinterfaces for each VPN and for non-VPN users, if required. Create a primary and a secondary IP address for each subinterface. The primary IP address subnet is used by the cable access routers and the secondary IP address subnet is used by the hosts connected to the cable access router. The cable DHCP-GIADDR policy command instructs the VHG/PE to differentiate DHCP requests from a cable access router and a host behind the cable access router. If different IP addresses are listed by the cable helper-address for hosts and cable access routers, the request is sent to different DHCP servers.

The DHCP-GIADDR command also causes the VHG/PE to set the GIADDR field of PC DHCP requests to that of the secondary interfaces IP address. This enhances the network administrators ability to define DHCP scopes on the Cisco Network Register (CNR) server.

In this configuration, VPN users are connected to cable interface 3/0.2, and non-VPN users attach to 3/0.3.

Both non-VPN and VPN cable access routers receive IP addresses from the same DHCP server. The VPN hosts obtains IP addresses from a DHCP server within the VPN. The non-VPN hosts obtain IP addresses from a server reachable from the global routing table.

The sharing of routes between the management VPN and user VPN allows the user VPN cable access routers to obtain and renew their IP addresses. The non-VPN hosts need additional routing configuration commands to obtain and renew their IP addresses.

Since the DHCP request from the non-VPN user cable access router enters the network on a non-VPN interface and the DHCP server is connected to the management VPN, the global routing table requires a route to the DHCP server. The easiest way to achieve this is to configure a static route on the router connected to the DHCP server, and redistribute the static route into the global routing table. The DHCP server's router interface is in the management VPN, which must have a route back to the user's subnet. A simple way to achieve this is to place a static route within the management VPN pointing at a P router's interface. The P router uses the global routing table to reach the user's subnet.

The keyword global should be used with the static route. For example, if the DHCP server were connected to a router that is remote to the VHG/PE, the static route could be "ip route vrf vpn1 24.25.17.0 255.255.255.0 195.10.20.1" global, where 195.10.20.1 is a P router's interface.

Sample VHG/PE Configuration File

```
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 7246-I1905
!
no logging console
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
ip subnet-zero
ip cef
!
!This configuration causes all management routes to be exported
!to all VRF's and all VRF routes to be present in the management VRF.
ip vrf management
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 1000:1000
!
ip vrf vpn2
 rd 200:1
 route-target export 200:200
 route-target export 1000:1000
 route-target import 200:200
 route-target import 100:1
!
ip vrf vpn3
 rd 300:1
 route-target export 300:300
 route-target export 1000:1000
 route-target import 300:300
 route-target import 100:1
!
```

```
!
!
interface Loopback0
 ip address 24.25.11.4 255.255.255.255
!
interface FastEthernet0/0
 ip address 24.25.30.1 255.255.255.0
 half-duplex
!
interface POS2/0
 ip address 24.25.1.14 255.255.255.252
 tag-switching ip
 clock source internal
!
interface Cable3/0
 no ip address
 load-interval 30
 no keepalive
 cable downstream rate-limit token-bucket shaping
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 583000000
 cable upstream 0 frequency 37008000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 frequency 40016000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 cable upstream 2 frequency 34016000
 cable upstream 2 power-level 0
 no cable upstream 2 shutdown
 cable upstream 3 frequency 31008000
 cable upstream 3 power-level 0
 no cable upstream 3 shutdown

!The cable dhcp-giaddr policy command causes the GIADDR field of dhcp requests
!to be set to the interface primary ip address for cable modem dhcp requests
!and the secondary ip address for host requests.

cable dhcp-giaddr policy


interface Cable3/0.1
 ip vrf forwarding management
 cable dhcp-giaddr policy
 cable helper-address 24.25.1.18
!
!All cable modems get their IP addresses from the same DHCP server which is
!connected to an interface in the management VRF. The hosts get their IP addresses
!from DHCP servers that are in the respective VRFs

interface Cable3/0.2
 ip vrf forwarding vpn2
 ip address 24.25.12.1 255.255.255.0 secondary
 ip address 24.25.13.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 24.25.1.18 cable-modem
 cable helper-address 10.15.20.1 host
!
interface Cable3/0.3
 ip vrf forwarding vpn3
 ip address 24.25.15.1 255.255.255.0 secondary
 ip address 24.25.14.1 255.255.255.0
```

```
 cable dhcp-giaddr policy
 cable helper-address 24.25.1.18 cable-modem
 cable helper-address 10.19.15.1 host
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 200
 neighbor 24.25.10.4 remote-as 200
 neighbor 24.25.10.4 update-source Loopback0
 !
 address-family ipv4 vrf vpn3
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf management
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
no ip http server
!
tftp-server slot0:running-config
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Configuring the SP CNR Network Server

CNR uses client class processing and secondary scopes to assign the correct IP address to the VPN and non-VPN cable access routers. The VPN cable access routers have their MAC addresses listed in a client class. The client class is tied to a scope selection tag. When a DHCP request is received from a cable access router that matches a client listed in a client class, the DHCP scope selected must have the included selection tag attached. Because VPN cable access routers use client class processing, it is a good idea to use it for non-VPN cable access routers, as well. The client class “default” is used to avoid listing each MAC address for the non-VPN cable access routers. This client class matches all MAC addresses that are not contained in another client class. Its scope selection tag selects a non-VPN cable access router scope. Scopes that provide IP addresses for hosts do not need to use client class processing, or selection tags. The DHCP discover packet from a host carries the GIADDR of the host subnet. CNR uses this field to select the correct scope.

CNR currently has a limit of 30 tags. If more than 30 scopes must be created, the use of the include and exclude tag scope selection feature must be employed. A client class can specify which scope is to be selected by both include tag and exclude tag statements. In this manner the tags can be used in a binary

fashion. A scope can have multiple tags attached to it. For example, if 11 tags are defined, a scope could have three of them attached to it. The client class for this scope would specify inclusion of these three tags and exclusion of the other eight. The requested scope would be unique in that it had the three included tags attached to it and no others tags.

When any cable access router boots for the first time, the VHG/PE forwards its DHCP discover packet as if it is connected to the first logical subinterface on the VHG/PE. It sets the GIADDR field of the DHCP DISCOVER packet equal to the IP address of the first logical subinterface. CNR uses the GIADDR field to determine from which scope the IP address is to be assigned. In the following scenario, CNR uses the GIADDR field of the DHCP discover packet to determine which scope should be used to provide the requested IP address. It does this before performing client class processing. Because the initial DHCP discover packet from every cable modem has its GIADDR field set to the IP address of the first logical cable subinterface, the scope that matches this GIADDR is selected. If a single IP address is contained within this scope and it is reserved to a dummy MAC address, CNR determines that there are no more IP addresses available within that scope. CNR then examines any scopes that are secondary to this scope and then uses client class processing to determine the correct scope. For this reason, all of the scopes used to provide cable modem IP addresses must be secondary scopes to the scope whose address range contains the IP address of the first logical cable subinterface.

Cisco recommends that you do not assign IP addresses from the address space of the first logical subinterface in this solution. Instead, configure the scope for the logical subinterface's IP address range to contain only a single IP address, and reserve that IP address to a nonexistent MAC address.

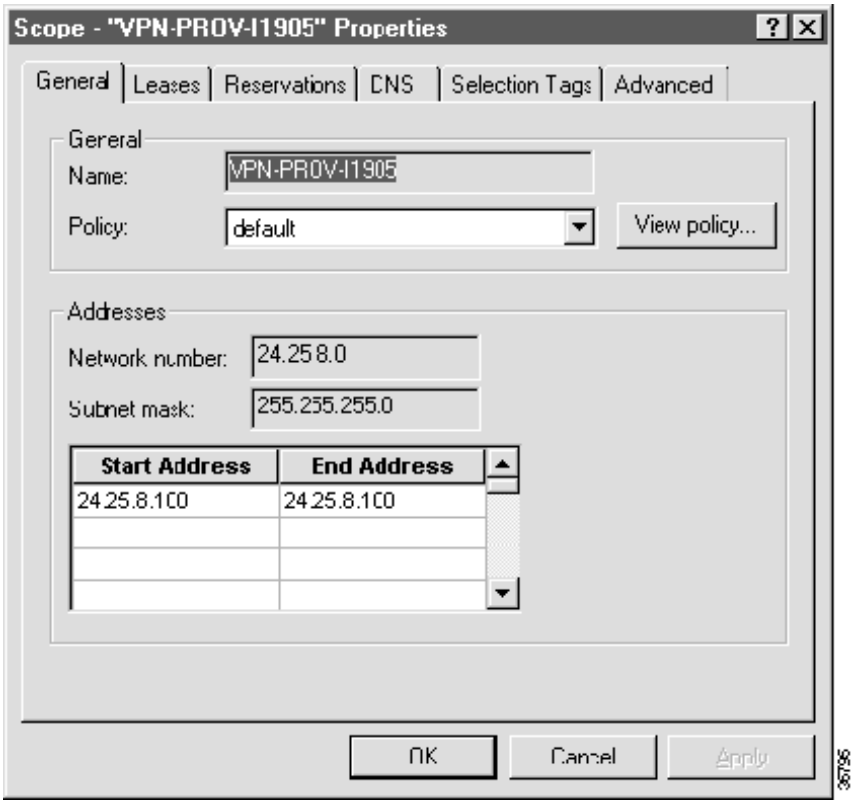
If interface bundling is not used on the VHG/PE, there must be a separate group of primary and secondary scopes for each cable interface. This is because the VHG/PE sets the GIADDR field of the cable access router's initial DHCP DISCOVER packet equal to the IP address of the first logical interface subinterface on every physical interface. Likewise, if there are multiple VHG/PE routers in the network, there must be separate primary and secondary scope combinations for each router.

In this example, the scope that covers the IP address range of the first logical cable subinterface is displayed on the CNR GUI in Figure 5-3.

Note For Cisco Network Registrar (CNR) configuration details, refer to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/nr3-5/index.htm and http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/mplscabl.htm.

Step 1 Define the primary scope of the first logical cable subinterface IP address range.

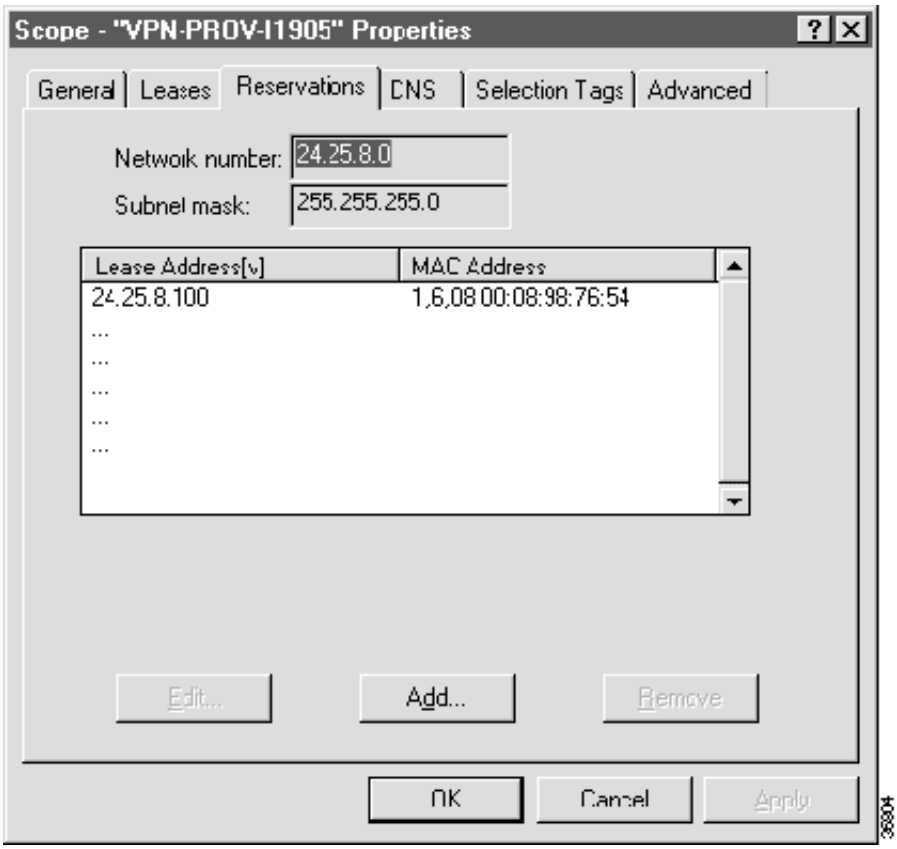
Figure 5-3 Scope of First Logical Cable Subinterface IP Address Range



Step 2 Reserve a dummy MAC address.

Its only IP address is reserved to a dummy MAC address (Figure 5-4), so no IP addresses are assigned from this scope on the CNR GUI Reservations tab.

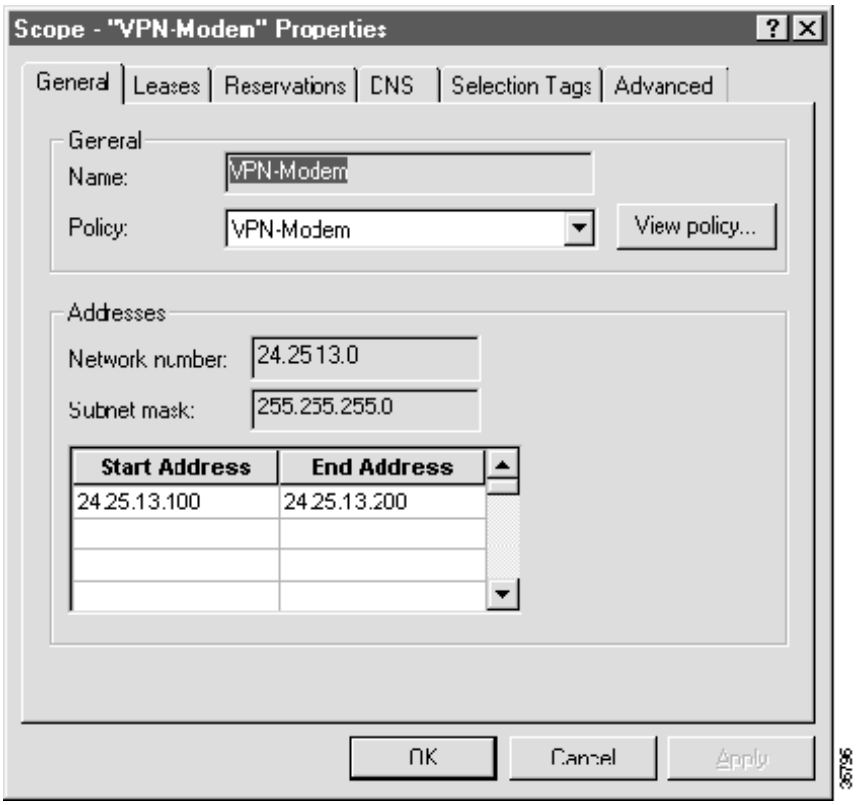
Figure 5-4 Reserved Dummy MAC Address



Step 3 Assign the scope for VPN cable access router IP addresses.

The scope provides IP addresses for VPN cable access routers on the CNR GUI General tab in Figure 5-5.

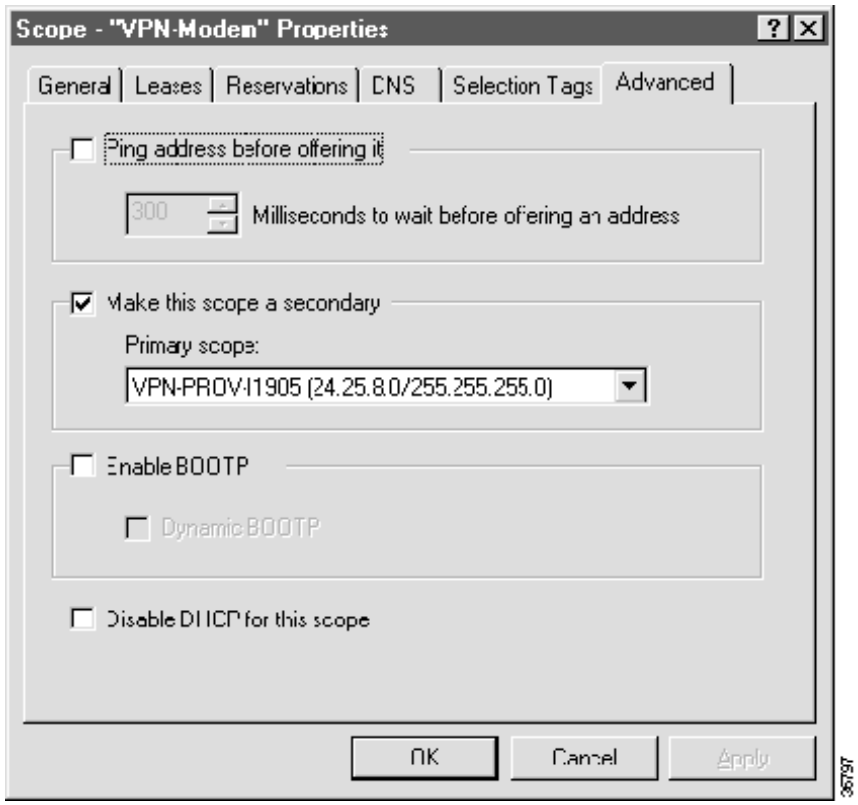
Figure 5-5 VPN Cable Access Router IP Addresses



Step 4 Configure a secondary scope.

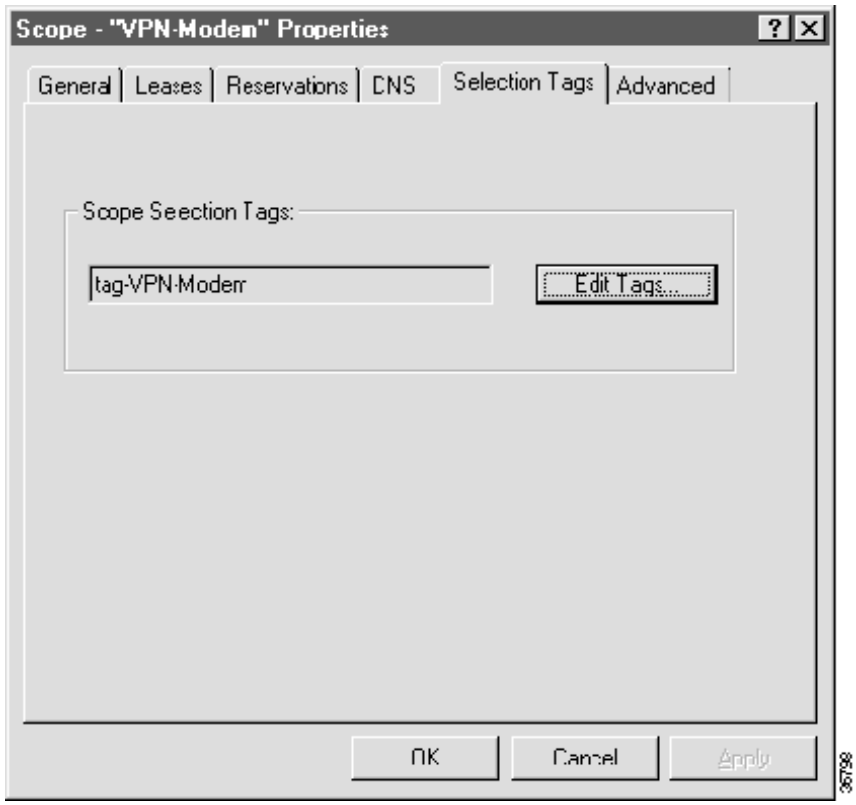
Figure 5-6 shows a secondary scope to the logical first interfaces scope on the CNR GUI Advanced tab.

Figure 5-6 Secondary Scope to Logical First Interface Scope



Step 5 Attach a scope selection tag of tag-VPN-cable access router to this scope.

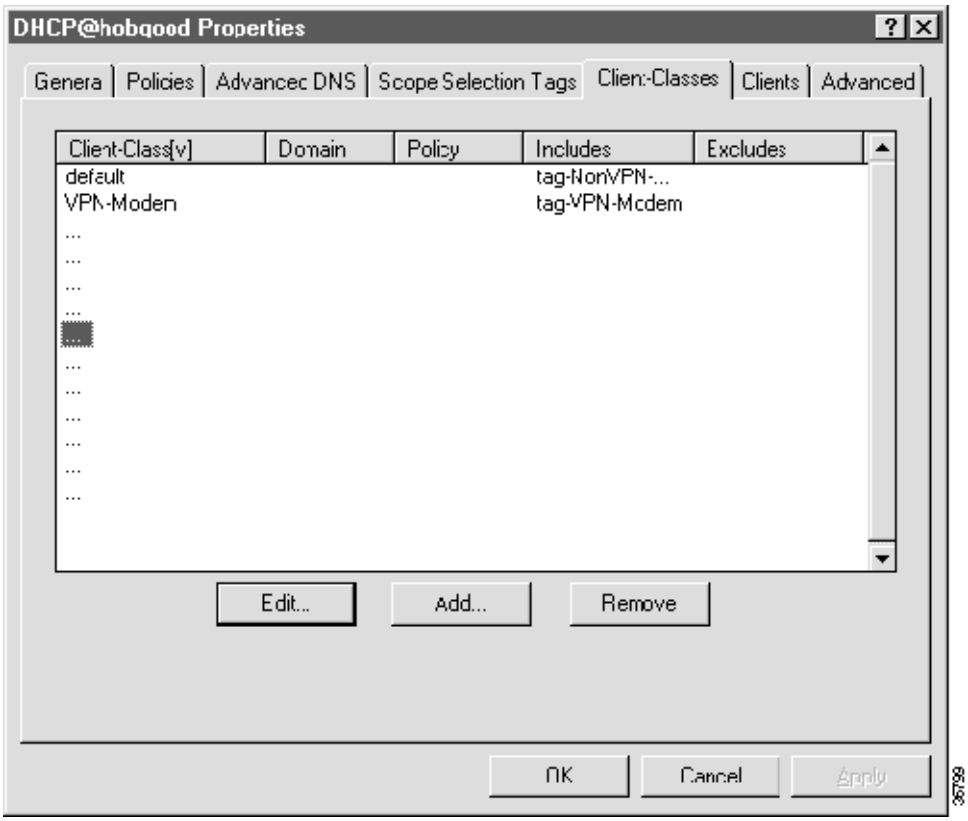
Figure 5-7 Scope Selection Tags Attached



Step 6 Create two client classes and attach “Includes” scope selection tags.

The client class VPN-Modem requires that any scope, provided for devices with MAC addresses listed within it, have a selection tag of “tag-VPN-Modem” attached to it (Figure 5-8). A client class can have multiple “Includes” tags attached.

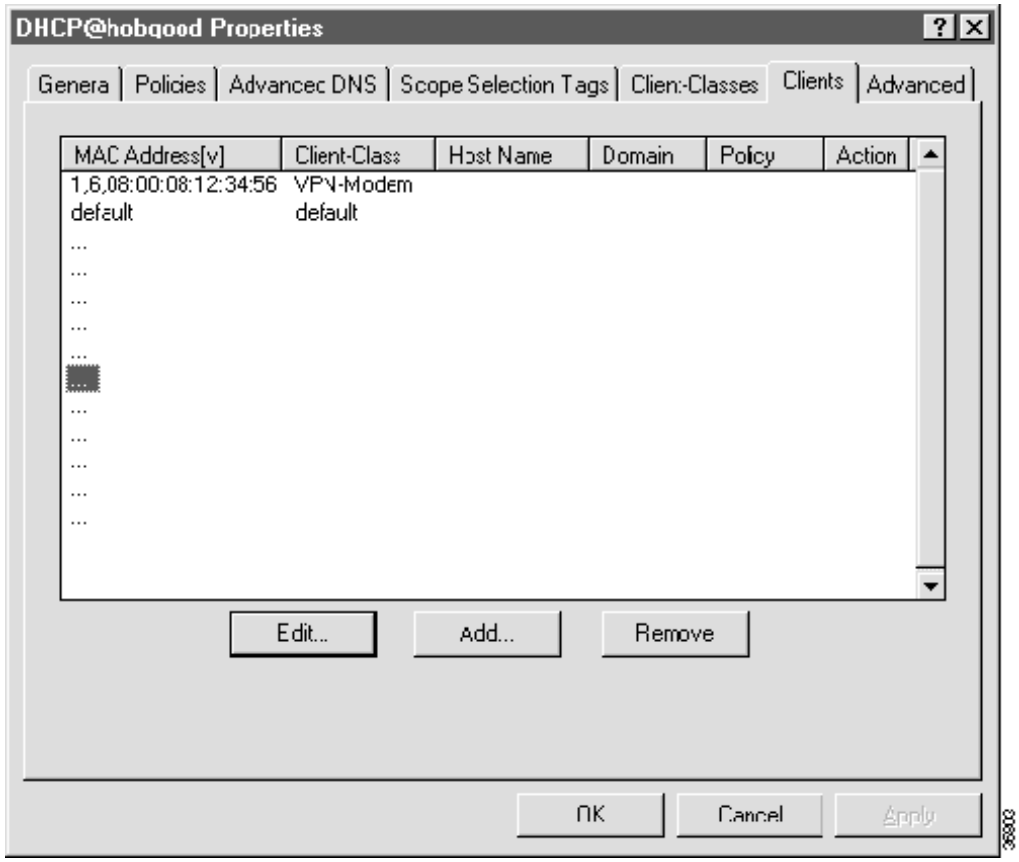
Figure 5-8 VPN Cable Access Router MAC Addresses



Step 7 Place the MAC address for the VPN cable access routers in the client-class VPN-Modem.

The MAC addresses for the VPN cable access routers are matched by “default” on the CNR GUI Client tab, shown in Figure 5-9.

Figure 5-9 Matching MAC Addresses



Configuring VPN/ISP DHCP Server

Perform the following steps to configure the VPN/ISP DHCP server.

Step 1 Configure a scope for each cable subinterface within the VPN. See Figure 5-5.

Note The GIADDR of the DHCP request is set to the secondary IP address of the respective cable subinterface.

Configuring the Customer Cable Access Router

Perform the following steps to configure a new customer's cable access router.

Step 1 Apply the default cable access router configuration.

Note A TFTP server providing DOCSIS 1.0 cable access router configuration files, and time-of-day server, must be configured in the network.

AAA Radius Access to MPLS VPN Integration

This appendix details remote access to MPLS VPN integration AAA and Radius requirements for authorization, authentication, accounting, and address management. Direct and proxy authentication are discussed.

AAA Radius Requirements

The Dial L2TP solution (see Provisioning Dial-In Access, page 3-1) is used in this Radius AAA example, but the requirements apply to all RA to MPLS VPN solution environments.

AAA Radius Event Sequence

The following steps are indicative of a AAA and Radius centric call flow.

Step 1 Remote user dials in. A PPP session is created between the remote user and the NAS.

Step 2 The NAS uses the SP Radius server to determine the address of the VHG/PE the session should be tunneled toward. The SP Radius server determines the appropriate VHG based on the remote user's domain name or the DNIS.

Step 3 The NAS creates an L2TP tunnel to VHG. The NAS and the VHG authenticate each other.

Step 4 The remote users PPP session is tunneled to the VHG.

Step 5 The VHG uses the SP Radius server to authenticate the incoming PPP session.

Step 6 The SP Radius server:

- authorizes remote users (associates user with the correct VPN, and corresponding VRF on VHG/PE)
- proxies the request to the user's VPN Radius server for authentication
- could assign an address to the remote user

Step 7 Call setup is complete where packets can flow in both directions.

Step 8 The VHG sends accounting records to the SP Radius servers. The SP Radius server saves a copy of the accounting records, and also proxies the record to the relevant VPN Radius server.

Note If the AR Radius server is used for address assignment, accounting is necessary.

Authorization at the NAS

For a scalable solution with multiple VHG/PEs in a POP, the NAS can not be configured with VPDN information to each PE. It has to retrieve information from the SP Radius Server.

When a remote user calls in, the NAS sends an Access-Request to the SP Radius server that includes the following attributes:

- The NAS IP address and/or the NAS Identifier
- The user name. This attribute contains the remote user's domain name, e.g., cisco.com or the DNIS.
- The user password. In this case, it is a standard password, e.g., cisco.

The SP Radius server must be configured with the following record. Assume the remote user's domain name is being used to associate it for retrieving the appropriate VHG to tunnel to:

```
cisco.com  Password="cisco"
    Service-Type=Outbound-User
    Framed-Protocol = PPP,
    Tunnel-Type = :1:L2TP,
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Server-Endpoint = :1:172.21.9.13, ? Address of the VHG.
    Tunnel-Password = :1:"welcome",
    Tunnel-Assignment-ID = :1:"nas"
```

All communication between the NAS and the SP Radius server should be carried over the management VPN, if the NAS and the SP Radius server do not reside in the same POP.

Based on the NAS's IP address and/or Identifier, the SP Radius Server recognizes the POP in which this NAS is located. The SP returns the address of a VHG/PE router which is located in that POP, and has a VRF pre-enabled for the cisco.com VPN.

There are multiple VHG/PEs in the POP that have cisco.com VRF enabled. The SP Radius server load balances amongst them. Random load balancing is acceptable, however, if the SP Radius server monitors the utilization of the various VHG/PEs via accounting records, it can load balance more intelligently.

The NAS also load balances among multiple VHGs as well as failover if one VHG is not available. In this case, the Radius server returns a list of VHG addresses to the NAS and the NAS load balances among these VHGs.

The Tunnel-Assignment-ID and Tunnel-Password are the local name and the local password used by the NAS for L2TP tunnel setup. If these commands are left out, the NAS uses its hostname and default password. The attributes that must be returned are the tunnel type (l2tp) and the IP address of VHG/PE.

Tunnel Authentication

When establishing an L2TP tunnel, the LAC (NAS) and the LNS (VHG) first authenticate each other. This is optional and can be disabled. For L2TP tunnel authentication, the LAC and LNS must use the same password. Currently tunnel authentication is possible via local authentication, not via Radius.

Authorization, Authentication, and Address Assignment at the VHG using SP Radius Server

The VHG sends an Access-Request to the SP Radius server. The request includes the following information:

- The VHG IP address and/or identifier (filled into the NAS IP address or NAS-Identifier attributes)
- The user name must be in the form remote-user@domain-name if the DNIS is not supplied. If the DNIS is provided no domain-name is provided.
- The remote user “real” password, not a standard password like "cisco."
- The DNIS, optional.

The SP Radius server strips of the user-name, and looks up a record for the domain name to associate it with the appropriate VRF on the VHG/PE. The domain name's record could be, for example:

```
cisco.com    Password = "cisco"
                User-Service-Type = Framed-User,
                Framed-Protocol = PPP,
cisco-avpair = "lcp:interface-config=ip vrf forwarding vpn1\nip unnumbered
                           loop1\npeer default ip address pool vpn1-pool"
```

These cisco-avpairs include VPN specific information and configs, but nothing user specific. The last command in the "lcp:interface-config" specifies the local pool. It may change when the “overlapping address pools” feature is implemented. Or the SP Radius server may not include this command, and include an IP address itself in the Framed-IP-Address attribute.

Based on the domain name or DNIS, the SP Radius server, associates the user with a VPN and proxies the Access-Request to that VPN's Radius server.

The VPN Radius server authenticates the remote user, and returns an Access-Accept or Access-Reject message to the SP Radius server. The Access-Accept message includes user specific information and configs. The SP Radius server merges this user-specific information with the VPN specific information in the Access-Accept message it returns to the VHG/PE.

Note An alternative to this proxy authentication mechanism is for the SP Radius server to do both the authorization and remote user authentication itself. The customer must provide the SP with complete, up-to-date records for all users with remote access privileges.

The SP provider needs to keep distinct records for the same domain name: one to respond to the NAS's request in Step 2 and the other one to respond to the VHG's request in Step 6. The AR can do this. In large networks, there can be a local Radius server in each POP and other Radius servers in the core of the network. The local Radius servers is configured with tunneling information specific to that POP, addresses of VHGs, etc. The NASs query the local Radius server to obtain tunneling information. The Radius server(s) in the core respond to queries from the VHGs for authorization, authentication, address management, and accounting.

If the SP Radius server is responsible for address assignment it maintains a separate address pools per (VHG,VPN) pair to prevent address fragmentation. The other requirement is for the Radius server to maintain overlapping address pools. The AR can fulfill both requirements. The AR can reclaim unused addresses by monitoring the accounting messages sent for each remote user.

Access Registrar Scripts

- Ability to differentiate between a request from a NAS and a request from a VHG/PE.
- Load balancing among multiple VHGs (low priority can be done by the NAS itself).
- When receiving an Access-Request from a VHG, the SP AR will perform the following:

- Authorize based on domain name or DNIS.
- Then proxy request to VPN Radius server for actual authentication.
- If proxy authentication succeeds, the relevant virtual interface configuration.
- Assign an IP address to the remote user. The AR maintains a separate address pool for each (VHG,VPN) pair.
- Reply to the VHG with an Access-Accept.

Symbols

A

B

C

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W