

Cisco DSL Remote Access to Multiprotocol Label Switching Virtual Private Network Solution

Executive Summary

Cisco Remote Access to Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) solutions enable service providers to connect remote access users with DSL, dial, or cable connections to an MPLS VPN and to deliver bundled value-added services. The Cisco DSL Remote Access to MPLS VPN solution integrates the MPLS-based VPN with multiple access architectures: PPPoX to SSG, PPPoX, Layer 2 Tunneling Protocol (L2TP), RFC 1483 Routed, and RFC 1483 Routed Bridge Encapsulation (RBE). For all architectures, key solution features include:

- Efficient address management
 - Overlapping address pool
 - On-demand address pool (ODAP)
 - Virtual Route Forwarding (VRF)-aware Dynamic Host Configuration Protocol (DHCP) Option 82
 - VRF-aware framed route with customer premises equipment (CPE) subnet assignment
- Flexible authentication, authorization, and accounting (AAA) options
 - Proxy AAA
 - Per-VRF AAA
 - Broadcast accounting
- Network management
 - Fault management
 - Configuration management

- Accounting management
- Performance management
- Security management

This solution overview describes the solution features, lists the functional components, and then describes each service architecture.

MPLS VPN Background

MPLS is an Internet Engineering Task Force (IETF) protocol introduced by Cisco Systems as tag switching. The key differentiator of MPLS is that packets and cells are forwarded based on labels or label values instead of IP header information, regardless of the network type. Labels indicate routes as well as service attributes. At the ingress edge, incoming packets are processed and labels are selected and applied. The MPLS core merely reads labels, applies appropriate services, and forwards packets based on the label. Processor-intensive analysis, classification, and filtering occur only once, at the ingress edge. At the egress edge, labels are stripped and packets are forwarded to their final destinations.

Cisco MPLS VPN is an IP network infrastructure that delivers private network services over a public infrastructure using a Layer 3 infrastructure with the following attributes:

- Provides traffic separation between customers



- Scales easily, simplifying provisioning
- Provides controlled access and quality of service
- Is easily configurable for customers
- Supports global as well as nonunique private address space
- Enables very large-scale VPN implementation
- Enables service provider mechanisms to support a wide range of service requirements from VPN customers

Solution Features

Efficient Address Management

The Cisco DSL Access Solution for MPLS VPNs is designed for efficient address management—specifically, efficient utilization of address space, maximized route summarization, and avoidance of Border Gateway Protocol (BGP) route propagation delays. Three solution components—the virtual home gateway (VHG) or provider edge, Remote Access Dial-In User Service (RADIUS) server, and DHCP server—cooperate to achieve these goals, as shown in Table 1.

VHG or Provider Edge	RADIUS Server (Cisco Access Registrar®)	DHCP Server (Cisco Network Registrar®)
<ul style="list-style-type: none"> • Groups address pools per VPN • Supports overlapping addresses • Dynamically assigns address space from RADIUS server via ODAPs • Allows efficient route summarization 	<ul style="list-style-type: none"> • Is VPN aware • Assigns adjacent addresses to requests from the same VHG-VPN pair • Relies on Accounting Stop records for release 	<ul style="list-style-type: none"> • Is VPN aware • Supports overlapping addresses

Overlapping Address Pool

In the standard implementation of Internet Protocol Control Protocol (IPCP) IP pool processing, all IP addresses belong to a single IP address space, also called a global pool. The same IP address cannot be assigned multiple times from this global address pool. Hence, implementation requires verifying that no overlap occurs in the IP address ranges of the global pool.

The Cisco DSL Remote Access to MPLS VPN solution takes advantage of IP address space segmentation. That is, each customer is assigned his or her own address group on the VHG or provider edge and Cisco Access Registrar, and each address group can include multiple private address pools. The private address pools of different customers can contain overlapping addresses, meaning that the same IP addresses can be used in different customers' private IP address spaces.

On-Demand Address Pool

The ODAP feature allows a central server—either the RADIUS server (Cisco Access Registrar) or the DHCP server (Cisco Network Registrar)—to manage a block of addresses on a per-customer basis. Each pool is divided into subnets of various sizes, and the server assigns these subnets to the VHG or provider edge routers upon request. The VHG or provider edge router has at least one on-demand pool configured for each VPN supported by that VHG or



provider edge. Upon configuration of an on-demand pool, the VHG or provider edge pool manager requests an initial subnet for that pool from the server and monitors the utilization of the on-demand pool. If the utilization of the pool exceeds a certain threshold, the pool manager requests an additional subnet from the server and adds it to the on-demand pool. Similarly, if the utilization of the on-demand pool decreases below another threshold, the pool manager attempts to free one or more of the subnets of the on-demand pool to return it to the server. When the subnets are downloaded from the server, the VHG or provider edge installs a corresponding summarized route into the VRF table. For Point-to-Point Protocol (PPP) sessions, individual address allocation from an ODAP follows a first leased subnet first (FLF) policy. FLF searches for a free address beginning on the first leased subnet, followed by a search on the second leased subnet if no free address is available in the first subnet, and so on. This policy groups the leased addresses over time to a set of subnets, allowing an efficient subnet release and route summarization.

VRF-Aware Framed Route and CPE Subnet Assignment

In the Cisco DSL Remote Access to MPLS VPN solution, a remote CPE can behave like a DHCP server for the local LAN. The CPE requests a subnet from the VHG or provider edge during the IPCP phase of the PPP negotiation process. The VHG or provider edge requests a subnet from the RADIUS server, which returns a framed IP address and netmask that are handed off to the CPE. The CPE can use the IP address subnet to initialize its DHCP server process and thus respond to DHCP requests generated on the LAN segment.

VPN-Aware DHCP Option 82

With VPN-aware DHCP, the DHCP server can reside on a VPN that is not directly accessible from the client, providing greater network design flexibility. This feature also allows the DHCP server to assign VPN-specific overlapping addresses. The DHCP relay agent (VHG or provider edge) appends the VPN-ID into Option 82, along with the originating client's Layer 2 interface information in the DHCP request. The Cisco IOS[®] Software and Cisco Network Registrar, used as the DHCP server in this solution, can read the VPN-ID field to determine the VPN from which server to allocate the address.

Flexible AAA Options

Any of the following methods can be deployed for PPP-based architectures. For non-PPP based architectures, Cisco IOS NetFlow can be used to collect accounting details.

Per-VRF AAA

Using the Per-VRF AAA feature, Internet service providers (ISPs) can partition AAA services based on VRF. This permits the VHG to communicate directly with the customer RADIUS server associated with the customer VPN without having to go through a RADIUS proxy. Hence, ISPs can scale their VPN offerings more efficiently because they do not need to proxy AAA to provide their customers with the flexibility they demand.

To support Per-VRF AAA, the AAA server must be VRF aware. ISPs must define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and secure the parameters to the VRF partitions.



Proxy AAA

Cisco Access Registrar supports RADIUS proxy. That is, rather than directly authenticating and authorizing users against a directory, the server selectively proxies the AAA request to another RADIUS server belonging to another service provider or a customer. That RADIUS server, in turn, authenticates and authorizes users against another directory or database.

Broadcast Accounting

The Broadcast Accounting feature allows accounting information to be broadcast to multiple AAA RADIUS servers at the same time. Using this function, service providers can send accounting information both to their own private RADIUS servers and to the RADIUS servers of their end customers. It also provides redundant billing information for voice applications.

Service providers and their end customers can independently specify their backup servers for failover. Information is sent first to the first server in a server group. If the first server is unavailable, the information is sent to the next server in the server group. This process continues until the information is successfully sent to one of the servers within the server group or until all servers have been tried.

For voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

Network Management

The Cisco DSL Remote Access for MPLS VPN solution provides full fault, configuration, accounting, performance, and security (FCAPS) element management. Functionality at the network level includes:

- *Fault management*—Network fault event correlation and filtering, network fault isolation, circuit testing, and trouble-ticket administration
- *Configuration management*—Network connection management and network installation management
- *Accounting management*—Network usage correlation and usage data storage
- *Performance management*—Traffic management, network capacity analysis, network performance characterization, network data aggregation, and trending
- *Security management*—Traffic pattern analysis, network security alarm, and network security breach detection and discovery

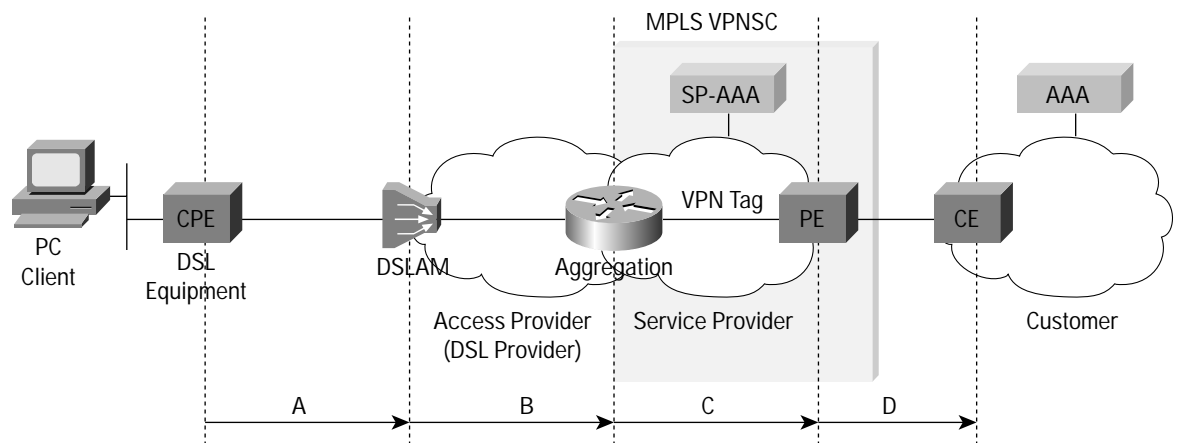
Solution Components

Figure 1 illustrates a simplified view of the components used in a DSL remote access session. The session is initiated by an end user through a DSL CPE and then transmitted to a DSL access multiplexer (DSLAM) in the access provider network cloud where the DSL connection is terminated. The session is forwarded to an aggregation (VHG) or provider edge router. Depending on the type of architecture being used, the session can be directly forwarded on an aggregated ATM connection or tunneled via L2TP across the access provider to the service provider. The PPP session



is terminated on the VHG or provider edge and IP traffic is subsequently placed in the corresponding VRF. When the user IP address is redistributed to the other provider edges in the same VPN, the user has end-to-end connectivity to the VPN. The MPLS VPN provisioning can be managed via the Cisco VPN Solution Center (VPNSC). Various RADIUS-based AAA methods are available (discussed previously) for authentication and authorization of the incoming PPP sessions.

Figure 1
DSL Remote Access to MPLS VPN Session Flow



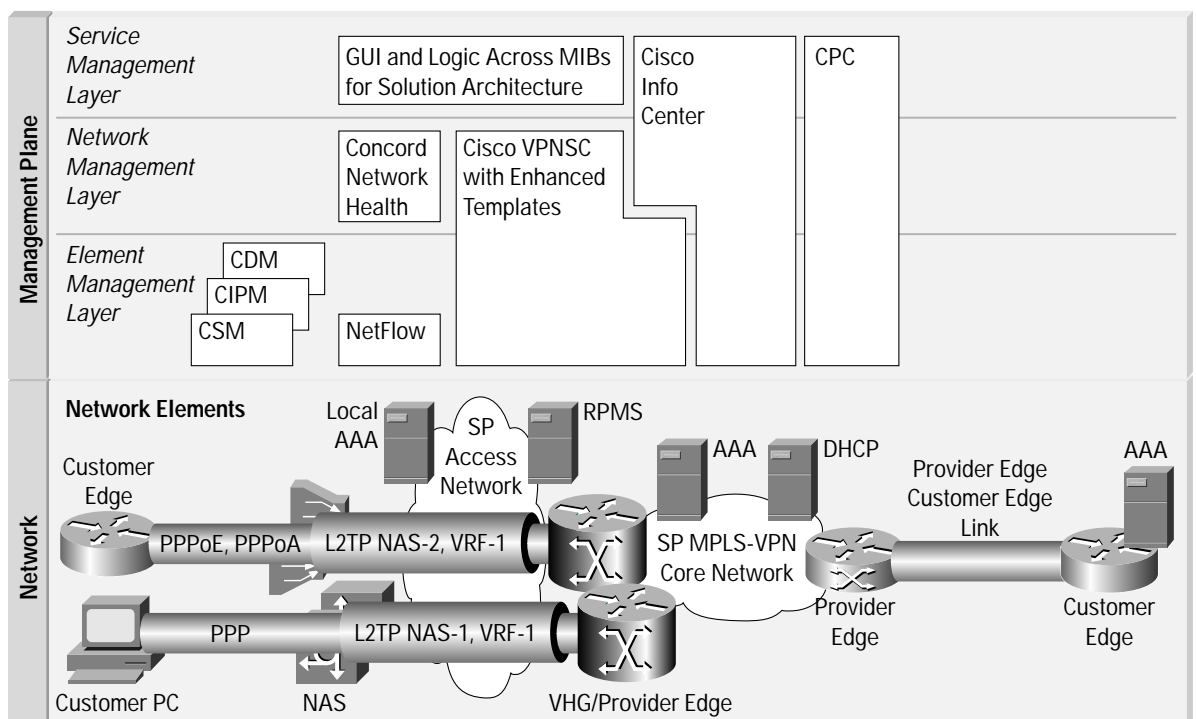
Solution components include:

- *CPE*
 - Cisco 820 Series DSL routers
 - Cisco 1700 Series and Cisco 2600 Series access routers with WAN interface cards (WICs)
- *DSL access network*—The DSL access network is not a direct part of the solution. DSL connectivity is provided by the service provider's DSLAM. DSLAMs available from Cisco Systems include:
 - Cisco 6015 IP DSL Switch
 - Cisco 6160 IP DSL Switch
 - Cisco 6260 IP DSL Switch
- *IP termination and provider edge router*—For the PPPoX SSG access architecture, separate IP termination and provider edge devices are used. For all other access architectures—PPPoX, L2TP, RFC 1483 Routed, and RFC 1483 RBE—IP termination and provider edge are combined on a VHG or provider edge device. Supported VHG and provider edge devices include:
 - Cisco 6400 Broadband Aggregator with node router processor (NRP)1 and NRP2 memory
 - Cisco 7200 Series Router
 - Cisco 7500 Series Router with Route Switch Processor 8 (RSP8)
 - Cisco Route Processor Module (RPM) for Cisco 8850 Series



- **RADIUS server**—Cisco Access Registrar (1.7) acts as the AAA server. It processes up to 300 calls per second for AAA and address management. Cisco Access Registrar is VPN aware; service providers can configure it for on-demand or overlapping address pools.
- **DHCP server**—Cisco Network Registrar (5.5) acts as the DHCP server. It supports up to 1800 new lease requests per second. Like Cisco Access Registrar, Cisco Network Registrar is VPN aware and supports overlapping address pools.
- **Service-selection-dashboard (SSD) server**—The SSD Web server allows users to view, log on, and disconnect from various services.
- **Network management system**—The Cisco DSL Remote Access to MPLS VPN Solution can include the following network management tools, illustrated in Figure 2.
- Cisco Service Connection Manager (SCM) is an element management application that manages the Cisco 6400 DSL Access Concentrator and DSL routers at the customer premises.
- Cisco VPNSC is used for VPN service provisioning, auditing, and SLA monitoring and accounting. Cisco VPNSC also uses Cisco IP Manager (IPM) for configuration downloads and uploads.
- Cisco IOS NetFlow is used for usage accounting of non-PPP connections.
- Cisco Info is used for VPN fault monitoring. Cisco Info Center also provides event correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems.
- Concord Network Health is used for VPN performance reporting.
- Service Assurance Agent in Cisco IOS Software is used for service-level agreement (SLA) reporting.

Figure 2
Network Management System





Service Architectures

Service providers can choose from several service architectures. Table 1 lists the primary benefits of each.

Service Architecture	Benefits
PPPoX to Cisco SSG to MPLS VPN	<ul style="list-style-type: none"> • Allows service providers to allow customers to select desired services, each offered over a separate MPLS VPN • Allows service provider to offer managed security access (AAA) on a per-service basis • Allows service provider to offer VPN services for users with nonregistered IP addresses, preserving IP addressing space in backbone
PPPoX to MPLS VPN	<ul style="list-style-type: none"> • Enables service provider to offer open and managed access • Allows service selection to be based on domain name • Allows each session to be mapped to a different VPN • Allows service provider to offer VPN services for users with nonregistered IP addresses, or to save scarce IP addressing space in backbone
L2TP to MPLS VPN	<ul style="list-style-type: none"> • Provides a better aggregation for service provider than the single-card PPPoX solution • Eliminates the need for virtual private dialup network (VPDN) so tunnels are not required in backbone; achieves optimal routing • Scales well • Eliminates need for a customer home gateway; the service provider can offer managed home gateway service (virtual home gateway)
RFC 1483 Routed to MPLS VPN	<ul style="list-style-type: none"> • Supports managed CPE service offering • Provides routing capabilities to branch offices
RBE to MPLS VPN	<ul style="list-style-type: none"> • Simplifies implementation and reduces overhead • Is useful in deployments with low-cost, bridged CPE

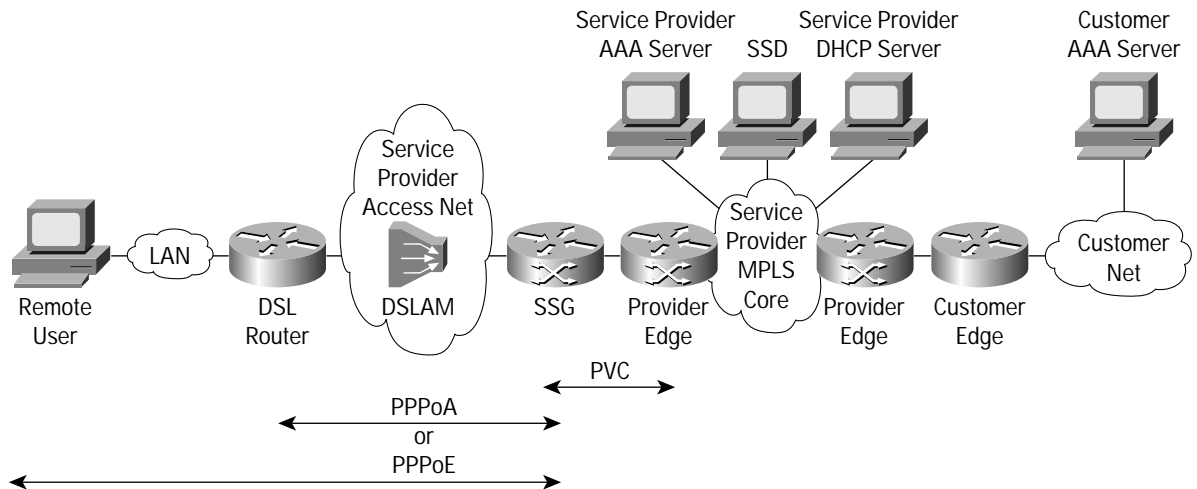
PPPoX Remote Access SSG to MPLS VPN Integration

Figure 3 shows DSL access integrated into an MPLS VPN via a SSG. This solution permits a remote user to select desired services, such as an ISP, enterprise VPN, a gaming network, and so on. Each service is provided through a separate MPLS VPN in the core. A remote user can switch between services dynamically and can even be logged on to multiple services at the same time. The user selects desired services from the SSD Web page.



The SSG can offer many VPN services; each VPN service the SSG offers maps to a corresponding MPLS VPN. The SSG can also offer services, such as standard Internet access, that might not require a VPN. For each VPN service the SSG supports, an RFC 1483 permanent virtual circuit (PVC) or Inter-Switch Link (ISL) virtual LAN (VLAN) is configured between the SSG and the provider edge router. The PVC or VLAN terminates at the provider edge router and is statically mapped to a VRF.

Figure 3
Cisco VPN DSL Access PPPoX to SSG MPLS



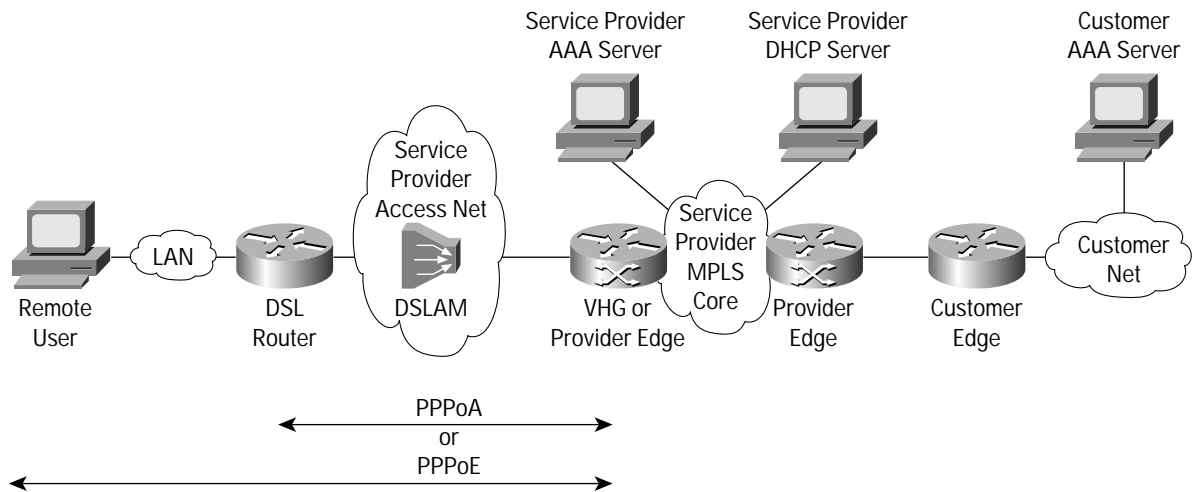
PPPoX Remote Access to MPLS VPN

Figure 4 shows an integrated DSL PPPoX remote access to MPLS VPN solution. The VHG or provider edge terminates an incoming PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) session and maps the remote user to the corresponding VRF. The following events occur when the remote user creates a PPPoA or PPPoE session over DSL in an attempt to access its corporate network or ISP:

1. The remote user initiates a PPPoE session or the DSL router initiates a PPPoA session over the DSL access network.
2. The VHG or provider edge accepts and terminates the PPPoA or PPPoE session.
3. The VHG or provider edge queries the RADIUS server to associate the remote user with a specific customer MPLS VPN. The VPN VRF (routing table and other information associated with a specific VPN) must have been preinstantiated on the VHG or provider edge.
4. The VHG or provider edge completes the remote user's authentication through the RADIUS server.
5. The VHG or provider edge obtains an IP address for the remote user.
6. The remote user is now part of the customer VPN. Packets can flow from and to the remote user.



Figure 4
PPPoX Remote Access to MPLS VPN



The VHG or provider edge can assign addresses to remote users using one of the following methods:

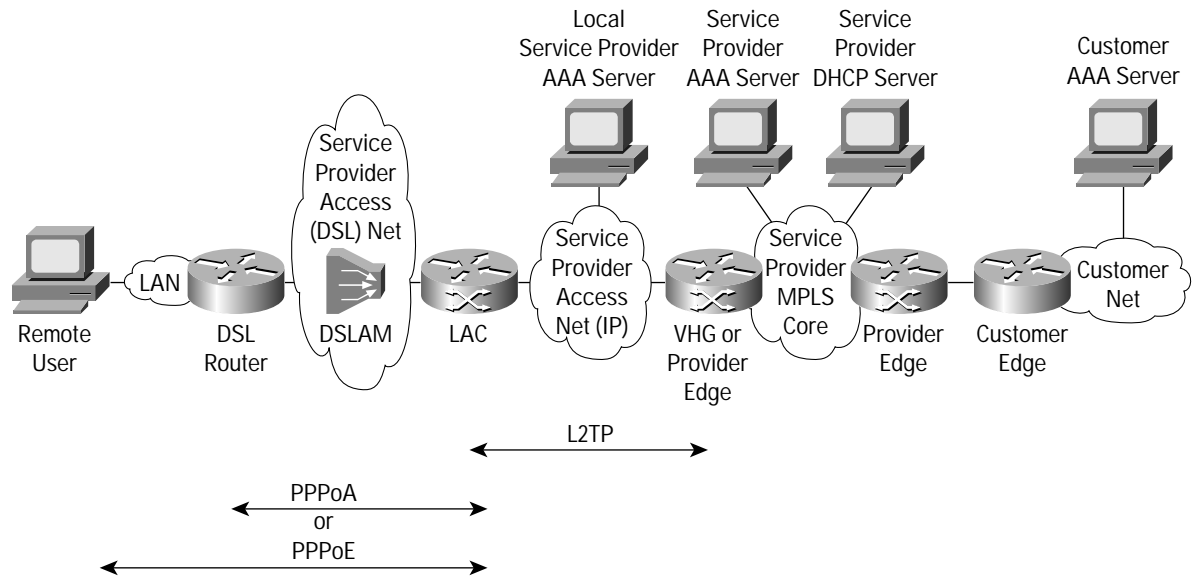
- Local address pools
- Service provider's RADIUS server
- Service provider's DHCP server

DSL L2TP to MPLS VPN Integration

With DSL L2TP to MPLS VPN integration, incoming PPPoX sessions that arrive at the L2TP access concentrator (LAC) are L2TP tunneled to the VHG or provider edge router, which maps the session to the corresponding VRF (refer to Figure 5). This solution provides enhanced aggregation and route summarization at the edge of the MPLS VPN core.



Figure 5
PPPoX or L2TP DSL Remote Access to MPLS VPN Solution



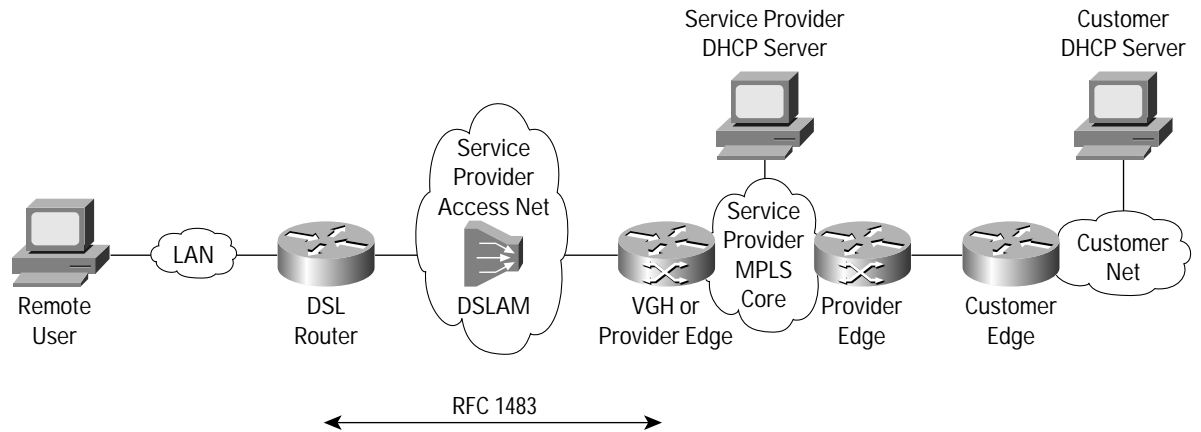
RFC 1483 Routed to MPLS VPN

RFC 1483 DSL remote access routing provides connectivity between the Cisco DSL router at the customer site and the VHG or provider edge (refer to Figure 6). At the VHG or provider edge, the service provider configures the RFC 1483 interface with a static VRF. At the customer site, the service provider can configure multiple IP subnets at the customer site using dynamic IP routing protocols between the DSL router and the VHG or provider edge.

Note that the RFC 1483 routing solution does not support remote user authorization and authentication. This solution is most suitable for remote offices rather than residential users because address assignment is based on DHCP and accounting is based on Cisco IOS NetFlow. The architecture is especially useful for connecting remote offices with multiple subnets to the VPN because IP routing protocols can be configured over the RFC 1483 PVC.



Figure 6
Cisco VPN RFC 1483 DSL Access to MPLS



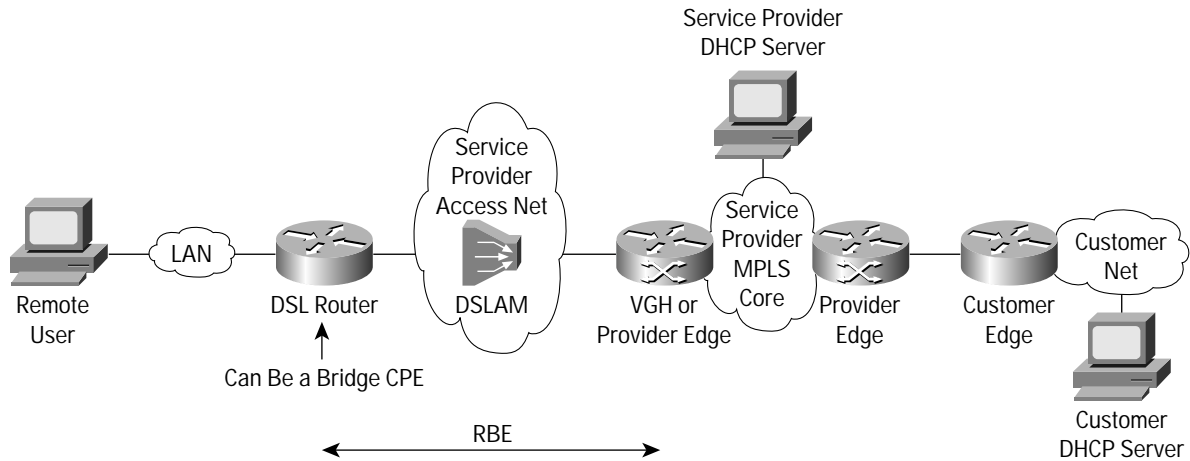
RFC 1483 Routed Bridge Encapsulation to MPLS VPN

ATM 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 7, RBE is configured between the DSL router and the VHG or provider edge. The DSL router can be set up as a pure bridge or for IRB. In the latter case, 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 or provider edge, which is statically configured with a specific VRF. Remote user authentication or authorization is available with Option 82 for DSL RBE remote access. RBE treats the VHG or provider edge subinterface as if it were connected to an Ethernet LAN, but avoids bridging issues such as broadcast storms, IP hijacking, and Address Resolution Protocol (ARP) spoofing. Address management options include static and VRF-aware DHCP servers. Because this architecture is not Point-to-Point Protocol (PPP) based, RADIUS accounting cannot be used; Cisco IOS NetFlow can be used instead.

Figure 7

Cisco VPN RFC 1483 RBE Access to MPLS



For more information about the Cisco Remote Access to MPLS VPN solution, visit:

<http://www.cisco.com/go/vpnsolutions>.



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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

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

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

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, Network Registrar, and Registrar are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R) SP/LW3726 12/02