

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

Executive Summary

This document provides a technical perspective of the Cisco Cable Remote Access to Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) solution implemented over a shared infrastructure. This solution enables a cable operator's MPLS-based core network to offer customers bundled end-to-end remote access VPN services.

The Cisco Cable Remote Access to MPLS VPN solution is a proven and stable solution for any cable operator that considers incorporating it to an existing MPLS infrastructure. With Cisco MPLS VPNs, many cable operators can now offer much more scalable, efficient, and feature-rich VPN services to their enterprise and small-to-midsize business customers. Access VPNs enable interconnection between individual remote users and a corporate site. Users include telecommuters, mobile workers, and remote offices that need to connect to their corporate intranets.

MPLS VPN Summary

MPLS is a suite of Request for Comments (RFCs) developed by the Internet Engineering Task Force (IETF) MPLS working group (<http://www.ietf.org/html.charters/mpls-charter.html>), and was pioneered by Cisco Systems initially as tag switching. The key differentiation of MPLS is that packet/cell forwarding is performed using 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 reads labels, applies appropriate services, and forwards packets based on the label. Processor-intensive packet analysis, classification, and filtering are all performed only once, at the ingress edge. When the packets reach the egress edge, labels are removed and packets are forwarded to their final destinations. In a VPN enabled MPLS network, service provider edge routers have multiple routing and forwarding tables called VPN Routing/Forwarding (VRF) and routing information of a VPN remains inside a VRF. Labels are assigned based on VPN information received by routing protocols, thus isolating traffic to that VPN. MPLS VPNs enables all service providers, including cable operators, to deliver advanced VPN transport services over existing network infrastructure and can be implemented over multiple network architectures, including IP, ATM, Frame Relay, and hybrid networks. Cisco MPLS VPNs have the following attributes:

- Maintain traffic separation between customers
- Are scalable for easy provisioning
- Provide controlled access and quality of service
- Are easily configurable for customers



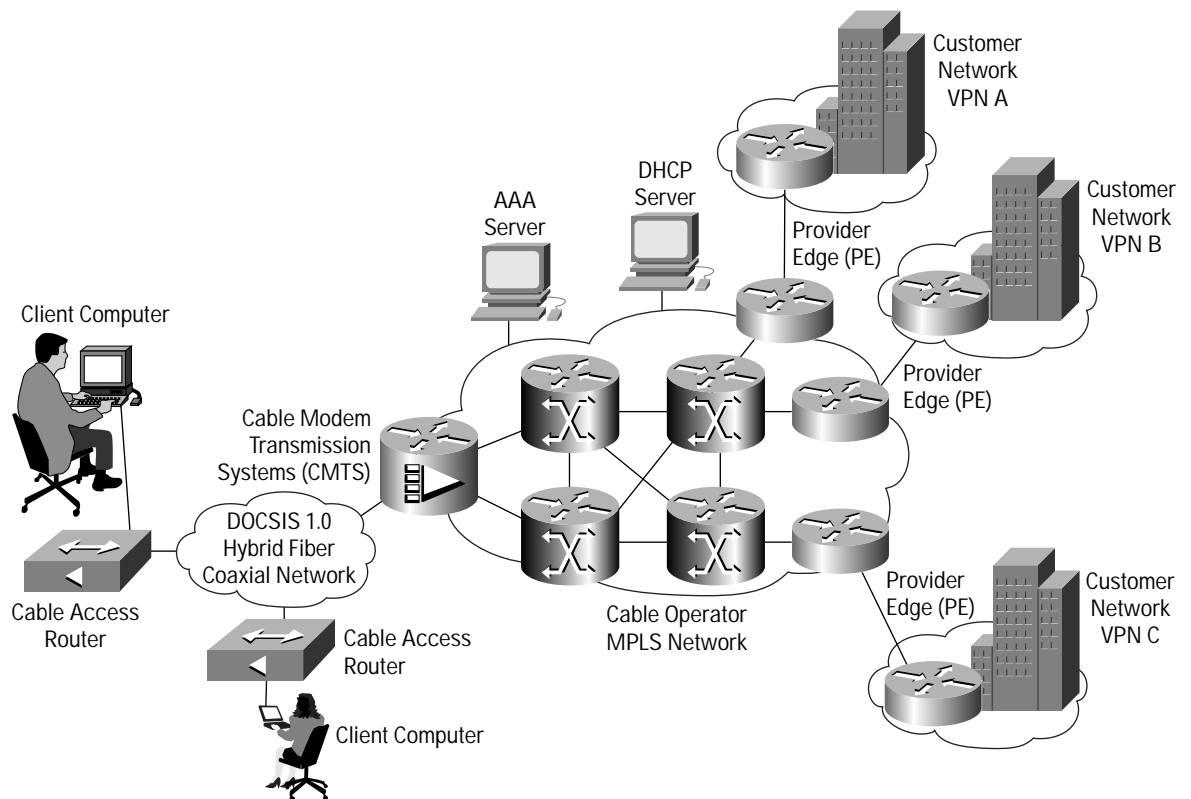
- Support global as well as non-unique private address space
- Enable very-large-scale VPN implementations
- Enable cable operators to support a wide range of service requirements from VPN customers, for example, quality of service (QoS), service-level agreement (SLA)

Assumptions

The scenarios described in this document assume that the cable operator has an existing MPLS core network and provides basic cable connectivity to its existing subscribers.

Figure 1 illustrates a generic topology of a VPN-enabled MPLS backbone operated by the cable operator. The enterprise customer has outsourced some of its end users' remote access operations that lie within the cable operator's service area. In addition, but not explicitly shown, the cable operator is providing the connection between telecommuters, mobile workers, and the customer network through MPLS VPNs.

Figure 1
Remote Access to MPLS VPN Topology

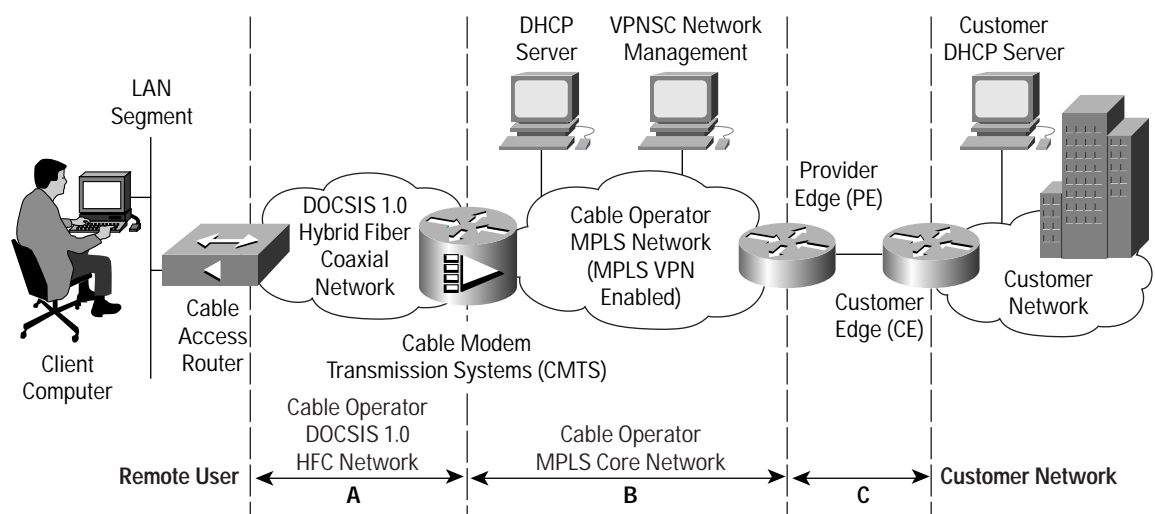




Deployment Model

By deploying the Cisco Cable Remote Access to MPLS VPN solution, a cable operator can create scalable and efficient virtual private networks with access to the MPLS core for its customers. In Figure 2, a cable operator is providing remote access VPN over a DOCSIS 1.0-compliant hybrid fiber-coaxial (HFC) network to a client computer attached to cable access router.

Figure 2
Cable Remote Access to MPLS VPN



Client computer address assignment and packet flow between the client computer and customer network take place in the following order:

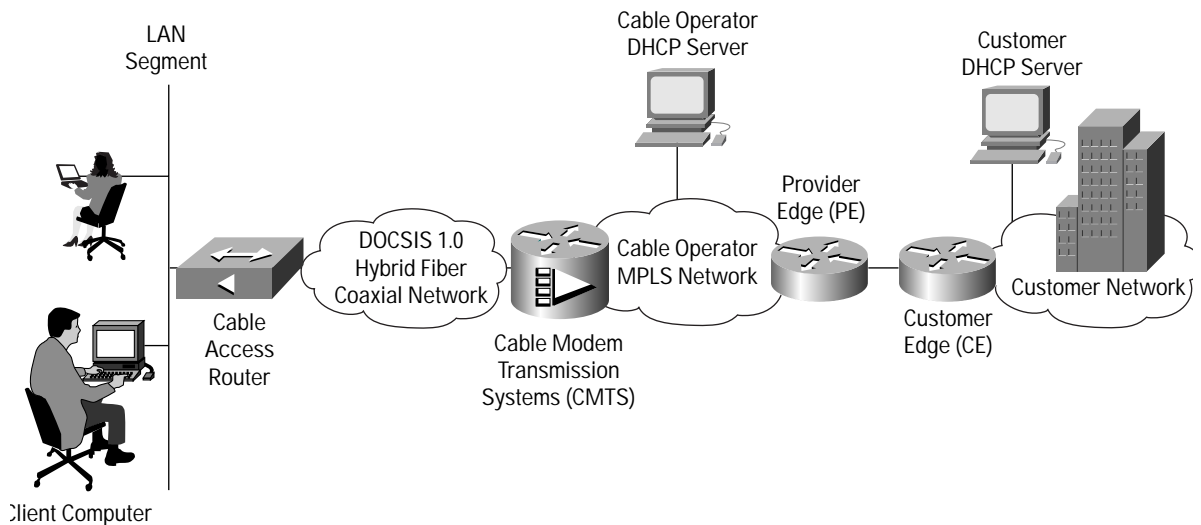
- When a client computer is powered up or rebooted, an IP address is assigned to the client computer by a Dynamic Host Configuration Protocol (DHCP) server from the secondary IP address range.
- Transmission occurs through the cable access router attached to the VPN subinterface.
- Packets are routed to and from the client's computer across the associated MPLS VPN.
- Customer network packets are forwarded to the remote user across the associated MPLS VPN and the HFC network.



Cisco Cable DOCSIS 1.0 Service ID to MPLS VPN Integration

In Figure 3, all traffic originated from a specific cable access router is identified by a unique Service ID (SID) in a DOCSIS 1.0-compliant HFC network. Based on the SID, traffic from a specific cable access router is terminated on the same sub-interface at the CMTS/PE located at the edge of the cable provider's MPLS network. At the CMTS/PE, each subinterface is provisioned to map all traffic to a specific VPN Routing/Forwarding (VRF). As a result, traffic from all devices connected to a given cable access router is associated with the same VPN and forwarded to a specific customer network. No remote user authorization or authentication is necessary in this solution. Address assignment is DHCP-based and accounting is based on Netflow.

Figure 3
Cisco Cable DOCSIS 1.0 SID to MPLS Integration



Each remote cable access router is associated with a specific VPN based on the IP address assigned by a DHCP server. Cisco Network Registrar[®] is the DHCP server used in this solution. Client-class processing is used on Cisco Network Registrar to determine which subnet and subsequent VPN the cable access router attaches to, based on the MAC address.

Cable Access Solution Components

CPE Equipment

At the user side, Cisco uBR900 Series (or a DOCSIS 1.0 compliant) cable access routers are used to connect remote access users to the cable operator's DOCSIS 1.0-compliant HFC network. Clients' computers are typically connected to the Cisco uBR900 Series cable access router through the integrated 4-port hub.

Cable Modem Termination Systems (CMTS)

The CMTS that supports this solution include the following two platforms:

- Cisco uBR7223 Universal Broadband Router with up to two cable RF Line Cards
- Cisco uBR7246 Universal Broadband Router with up to four cable RF Line Cards



Hybrid Fiber-Coaxial (HFC) Network

The cable operator access network is a DOCSIS 1.0-compliant HFC network. Cable access routers are connected to a Cisco uBR7223 or Cisco uBR7246 across the HFC network. 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 provider edge router.

DHCP Server

Cisco Network Registrar functions as the DHCP server for this solution. Cisco Network Registrar 3.5 (and higher versions) will support this MPLS VPN solution. Cisco Network Registrar runs on Windows NT 4.0, Windows 2000, and Solaris 2.5.1 (and higher versions).

Address Management

DHCP is used for address assignment in the Cisco Cable VPN access DOCSIS 1.0 SID to MPLS VPN integration. DHCP requests occur by one or more of the following methods:

- A. The cable operator DHCP server assigns addresses to cable access routers based on the MAC address, whether or not the gateway IP address (GIADDR) parameter has been included in the request. The DHCP server can also provide IP addresses to client computers within a VPN. Hence it is possible that as a service option, a VPN customer can designate blocks of addresses from its address space to the cable operator, and that the cable operator manages these addresses and assigns them to the authorized remote users on behalf of the VPN customer.
- B. The customer DHCP server is used to allocate IP addresses directly to end users within its VPN.

Both the cable access router and the corresponding CMTS interface must have an assigned IP addresses. The address for the subinterface must be provisioned. When the cable access router is powered up, it immediately requests an address assignment from the DHCP server. The request is relayed by the CMTS to the appropriate DHCP server, which could either be a cable operator DHCP server or the customer's DHCP server. The DHCP server assigns an address to the cable access router based on its MAC address and the GIADDR of the CMTS that forwarded the request. The cable access router's MAC address is provisioned at the DHCP server and is associated with a specific service or VPN.

The addresses assigned to both the cable access router and the CMTS subinterface can use private addresses (assigned from the cable operator's private pool) on the condition that these interfaces must be reachable from other provider edge routers associated to the same VPN for a multi-site customer network implementation.

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 CMTS 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 solution can be implemented in two types of MPLS core network architectures: IP-based and ATM-based.

Network Management

The network management components used in this solution are:

- Cisco Cable Manager—For configuring the Cisco uBR7223 and Cisco uBR7246 Universal Broadband Routers and the Cisco uBR900 series cable access routers.
- Cisco VPN Solution Center (VPNSC)—For VPN service provisioning, auditing, service-level agreement (SLA) monitoring and accounting. Cisco VPNSC also uses Cisco IP Manager for configuration downloads and uploads.

- Cisco Network Registrar—For IP address allocation.
- NetFlow—For usage accounting.
- Cisco Info Center—For VPN fault monitoring.
- Concord Network Health—For VPN performance reporting.

For More Information

For more information about the Cisco Cable Remote Access to MPLS VPN solution, go to: Cisco VPN solutions:

<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 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco 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 © 1992–2003 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. (0301R) SP/LW4084 01/03