



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

Executive Summary

This document provides a technical perspective of the Cisco Remote Access to Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) solution implemented over a shared infrastructure. This solution integrates various access services with MPLS in the service provider's core and lets the service provider offer bundled end-to-end VPN services. The Cisco Remote Access to MPLS VPN solution has been thoroughly tested, and is a proven and stable solution for any service provider considering applying it to an MPLS infrastructure. With Cisco MPLS VPNs, many service providers can offer scalable, efficient, and feature-rich VPN services to their enterprise and small-to-midsize business customers. Access VPNs interconnect individual remote users to their corporate site. Users include telecommuters, mobile workers, day extenders, and remote offices that need to connect to their corporate intranets. Connectivity is deployed through dial, ISDN, DSL, and cable technologies.

MPLS VPN Summary

MPLS is an Internet Engineering Task Force (IETF) protocol standard, pioneered by Cisco Systems 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 merely reads labels, applies appropriate services, and forwards packets based on the label. Processor-intensive analysis, classification, and filtering happen only once, at the ingress edge. At the egress edge, labels are stripped, and packets are forwarded to their final destinations.

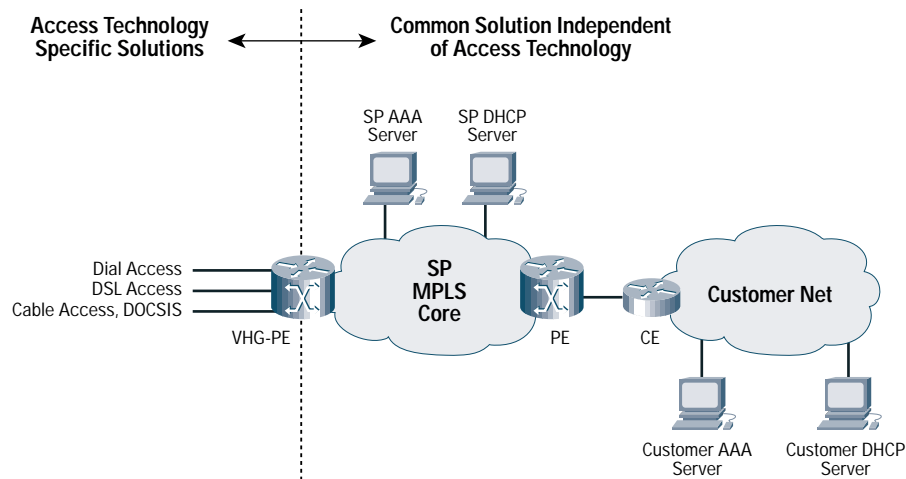
Cisco MPLS VPN is an IP network infrastructure delivering private network services over a public infrastructure using a Layer 3 infrastructure with the following attributes:

- Provides traffic separation between customers
- Is scalable, for easy provisioning
- Provides controlled access and quality of service
- Is easily configurable for customers
- Supports global as well as non-unique private address space
- Enables very-large-scale VPN implementation
- Enables service providers mechanisms to support a wide range of service requirements from VPN customers

Assumptions

The scenarios described in this document are based on the assumption that the service provider has an existing MPLS core network. It also assumes that the service provider currently provides basic dial connectivity to its existing subscribers. Figure 1 illustrates the topology included in a VPN-capable MPLS backbone operated by the service provider. The end-user customer has outsourced all remote access operations to its service provider. In addition, but not explicitly shown, the service provider operates an MPLS VPN that connects teleworkers and mobile workers to the network. This solution overview document will review all the unique dial access methods that are relevant to the Cisco Remote Access to MPLS VPN solution.

Figure 1
Remote Access to MPLS VPN



Overview of Dial Remote Access

This section describes three unique methods of dial access scenarios of this fully tested Remote Access to MPLS VPN solution:

- Dial-in access—Individuals dialing in over ISDN or the analog Public Switched Telephone Network (PSTN) to a service provider edge router from their computers, or users at a remote office dialing in to a service provider edge router via a customer edge router. Two specific dial-in scenarios exist:
 - L2TP dial-in
 - Direct ISDN provider edge dial-in
- Dial backup—A customer edge router dialing in to a provider edge router, creating a backup link for use when a primary, direct connection such as Frame Relay circuit has failed
- Dial-out access —A provider edge router dialing out to a remote customer edge router, with the call triggered by traffic from the enterprise customer. For example, an enterprise customer central database system needs to contact vending machines at night to collect daily sales data and check inventory. Two specific dial-out scenarios exist:
 - L2TP dial-out
 - Direct ISDN provider edge dial-out

Dial-In Remote Access Scenarios

L2TP Dial-In Remote Access

The L2TP dial-in access solution is designed for service providers that want to offer managed and wholesale dial service to their customers. The service provider (or a large Internet service provider [ISP]) maintains geographically dispersed points of presence (POPs). To gain VPN remote access, a customer of the service provider dials in to a network access server at a local POP, which

enables the dial traffic to be placed into the customer's VPN. To gain VPN remote access, a customer of the service provider dials in to a network access server at a local POP, which enables the dial traffic to be placed into the customer's VPN. L2TP dial-in can include these features:

- Multilink PPP (MLP)—Point-to-Point Protocol (PPP) split across multiple data links
- Multichassis MLP (MMP)—MLP with redundant stacked network access servers and provider edge routers; a stack group bidding process is used to manage the allocation of PPP sessions among the members of the stack
- Address management—Through overlapping local pools configured on the network access servers and provider edge routers and through the use of a Dynamic Host Configuration Protocol (DHCP) server

Figure 2
Topology of L2TP Dial-In Remote Access

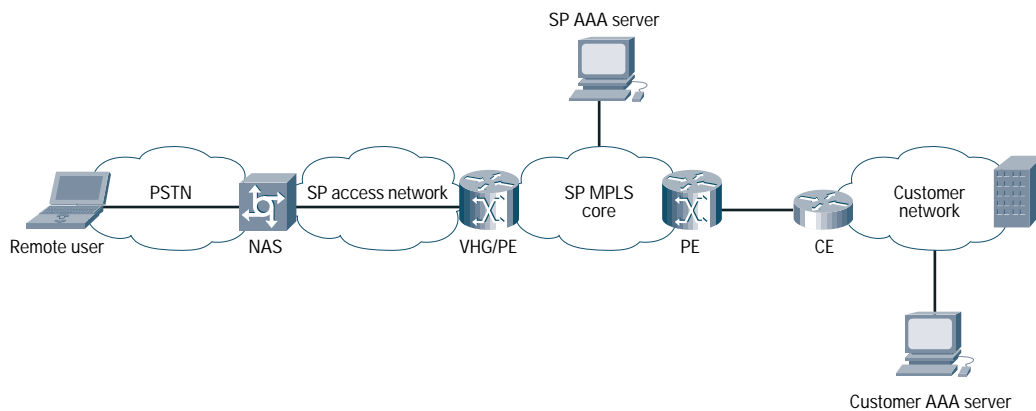


Figure 2 illustrates the call flow in a L2TP dial-in access scenario. The remote user initiates a PPP connection to a network access server using either analog service or ISDN. If MLP is enabled, the session is identified as potentially a part of an MLP bundle. The network access server accepts the connection, and a PPP or MLP link is established between the customer PC or customer edge router and the VHG or provider edge router. The network access server 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 network access server. If the user is a VPN client then, as in the L2TP dial-in scenario, the authentication, authorization, and accounting (AAA) server returns the address of a VHG or provider edge router. If an L2TP tunnel does not exist, the network access server initiates a tunnel to the VHG or provider edge.

The network access server and the VHG/provider edge router authenticate each other before any sessions are attempted within a tunnel. A VHG/provider edge router can also accept tunnel creation without the network access server providing tunnel authentication. Once the tunnel is established, a session within the tunnel is created for the remote user, and the PPP connection is extended to terminate on the VHG/provider edge router. The network access server propagates all available PPP information (the Link Control Protocol-negotiated options and the partially authenticated CHAP/PAP information) to the VHG/provider edge router. The VHG/provider edge router associates the remote user with a specific customer VPN. The VPN's virtual routing/forwarding (VRF) instance has already been instantiated on the VHG/provider edge router. (VRF is information associated with a specific VPN.) The VHG/provider edge router completes the remote user's authentication. The VHG/provider edge router obtains an IP address for the remote user. The remote user's session becomes part of the customer VPN. Packets flow from and to the remote user.

If MLP is enabled, the remote user initiates a second PPP link of the MLP bundle. The previously described scenario would be 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/provider edge router, with both MLP bundles being put into the

same VRF. The VRF includes routing information for a specific customer VPN site. In the context of L2TP dial methods, the network access server functions as an L2TP access concentrator, and the VHG/provider edge router functions as an L2TP network server.

L2TP Dial-In Components

Figure 2 shows the major components of the L2TP dial-in architecture. Listed below are the components and the specific platforms and software supported:

- Dial L2TP service provider access network—The service provider access network could be a high-speed network. The service provider can place a network access server and VHG/provider edge router in each access network POP.
- Network access servers—Functioning as an L2TP access concentrator (LAC), the network access server receives an incoming PPP session over an analog or ISDN connection, places the session into a virtual-private-dialup-network (VPDN) tunnel, and forwards it to the VHG/provider edge router.
- Platforms supported:
 - Cisco 3640 Router, 60 ISDN ports, or 48 basic telephone service ports
 - Cisco 3660 Router, 120 ISDN ports, or 96 basic telephone service ports
 - Cisco AS5300 Universal Access Server, up to 8 T1/E1/ISDN Primary Rate Interfaces (PRIs) (up to 192/240 ports)
 - Cisco AS5400 Universal Access Server
 - Cisco AS5800 Universal Access Server, with up to 48 T1/E1/ISDN PRIs (up to 1152/1440 ports) or up to two T3 interfaces (up to 1344 ports)
- VHG/provider edge routers—The VHG/provider edge router terminates the L2TP-tunneled session by placing in the applicable customer VRF and then passing it on to the MPLS core network. Supported VHG/provider edge routers include:
 - Cisco 7200 Network Processing Engine (NPE) 300 and NPE 400 Series routers
 - Cisco 7500 Route Switch Processor (RSP) 4 and RSP 8 Series routers
 - Cisco 6400 Node Route Processor (NRP) 1 and NRP 2 Universal Access
- Network management software—Cisco VPN Solution Center v2.1

Direct ISDN Provider Edge Router Dial-In Remote Access

In direct ISDN provider edge router dial-in access to an MPLS VPN, a network access server functions as both network access server and provider edge router. (For that reason, the network access server is referred to here as a network access server/provider edge router). 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 MLP, Multichassis MLP (MMP) or address management, as previously described in the L2TP Dial-In Remote Access section.

Figure 3

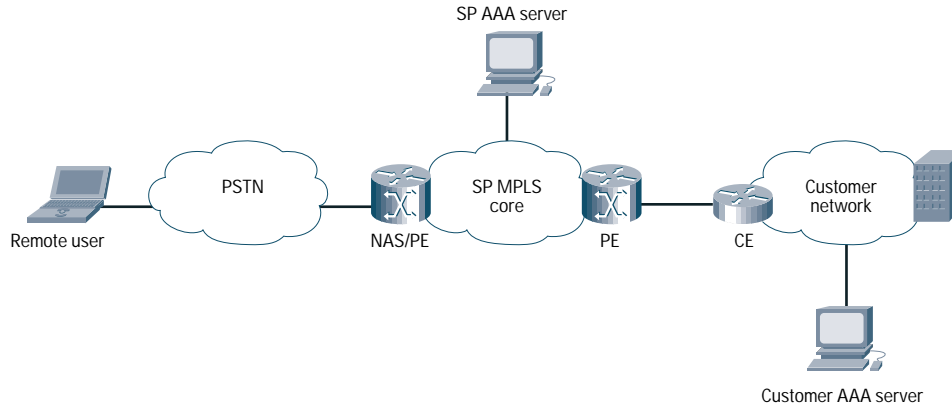


Figure 3 illustrates the call flow in a direct dial-in access scenario. The remote user initiates a PPP or MLP connection to the network access server/provider edge router using ISDN. The network access server/provider edge router accepts the connection, and a PPP or MLP link is established. The network access server/provider edge router authorizes the call with the service provider AAA server, and authorization is based on the domain name or DNIS. The service provider AAA server associates the remote user with a specific VPN and returns the corresponding VRF instance name to the network access server/provider edge router, along with an IP address pool name.

The network access server/provider edge router creates a virtual access interface to terminate the user's PPP sessions, and 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. CHAP continues and completes. An IP address is allocated to the remote user. Any of several different methods can be used for address assignment. The remote user is now part of the customer VPN, and packets can flow from and to the remote user.

Direct ISDN Provider Edge Router Dial-In Components

The major components of the direct dial-in architecture shown in Figure 3 are listed here along with a description of the role each component plays and the specific platforms this architecture supports.

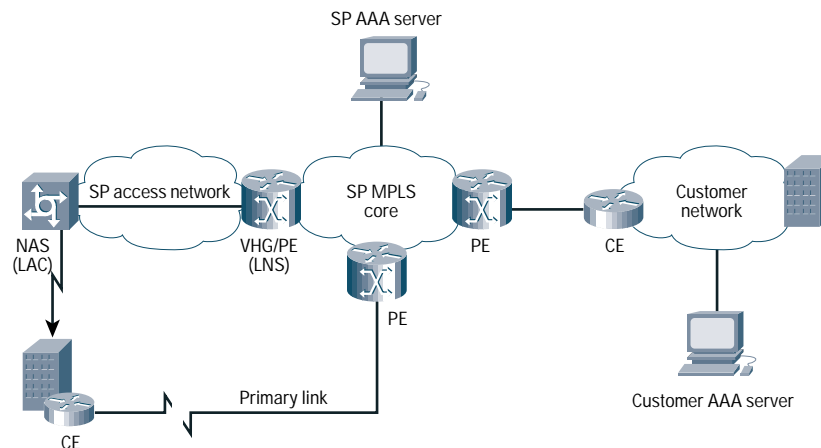
- Network access server/provider edge routers—These network access server/provider edge routers receive incoming PPP sessions over ISDN and terminate the PPP session in an MLP virtual access bundle, if appropriate. The network access server inserts the bundle into the specific customer's VRF domain, removes PPP encapsulation, and forwards the IP header and data to the MPLS VPN network through tag switching.
- Platforms for ISDN provider edge router dial-in:
 - Cisco 3640 Router, 60 ISDN ports, or 48 basic telephone service ports
 - Cisco 3660 Router, 120 ISDN ports, or 96 basic telephone service ports
 - Cisco 7200 NPE 300 or NPE 400 Series routers
- Network management software
 - Cisco VPN Solution Center Version v2.1

Dial Backup Remote Access Scenario

Dial backup can be used to provide a fallback link for a primary, direct connection such as Frame Relay. If L2TP dial-in architecture is used, dial backup provides connectivity from the customer's remote office to the customer's VPN when the primary link becomes unavailable. The primary and backup links are both configured on the same customer edge router at the remote site. The call flow in dial backup is identical to that in L2TP dial-in access, except that the call is initiated by a backup interface—instead of by a remote user—when connectivity to the primary interface is lost.

A dialer interface is configured to dial in to the service provider's network access server 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 network access server tunnels the PPP session to the VHG/provider edge router, which then maps the incoming session into the appropriate VRF. The VRF routing tables on all remote provider edge routers must converge; updates come from the VHG/provider edge router. When the primary link is restored, the primary route is also restored, the remote user terminates the backup connection, and the VHG/provider edge router deletes the backup route.

Figure 4
Topology for Dial Backup



Like L2TP dial-in, dial backup requires a network access server and a VHG/provider edge router. The following points describe the ways in which dial backup differs from L2TP dial-in. Figure 4 shows the call flow that occurs in a direct dial-in access scenario. No address assignment is required as dial backup is used primarily to connect remote sites (not remote users) to a customer VPN. MLP is typically used across the data links. Backup links are typically MLP links, and an Interior Gateway Protocol (IGP) routing protocol can be configured on the backup link. Static addresses or Routing Information Protocol (RIP) can be supported if dynamic routing updates are desired.

If routing is not enabled on the links between the customer edge router and the VHG/provider edge router, static VRF routes on the VHG/provider edge router must be provisioned. For the primary link, provisioning is straightforward. Because of a lack of connectivity, the primary static route is withdrawn when the primary link goes down. For the backup PPP session, the static route can be downloaded from the Remote Access Dial-In User Service (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 customer edge router terminates the backup connection. The provider edge router then deletes the backup static VRF route.

Alternatively, dynamic routing can be configured on both the primary and the backup customer edge-provider edge link. Typically, static routing is used when remote networks rarely change their IP addresses or when the connecting network is a stub network and only one path is available to the remote destination. Dynamic routing is more suitable when network routing might be reconfigured or when multiple paths to the remote destination exist.

With dial backup, authentication of the remote customer edge router is similar to remote user authentication in L2TP dial-in. If a managed customer edge router is used, the service provider's AAA server can authenticate the remote customer edge router; proxy authentication is not needed. The service provider's AAA server or RADIUS proxy on the VHG/provider edge router maintains accounting records, including MLP information, for the duration of the backup session.

Dial Backup Components

The major components of the dial backup architecture shown in Figure 4 are listed here along with a description of the role each component plays and the specific platforms this architecture supports.

- Network access servers/provider edge routers—These network access server/provider edge routers receive incoming PPP sessions over ISDN and terminate the PPP session in an MLP virtual access bundle, if appropriate. The network access server inserts the bundle into the specific customer VRF domain, removes PPP encapsulation, and forwards the IP header and data to the MPLS VPN network through tag switching.

- Platforms for ISDN provider edge router dial-in:
 - Cisco 3640 Router, 60 ISDN ports, or 48 basic telephone service ports
 - Cisco 3660 Router, 120 ISDN ports, or 96 basic telephone service ports
 - Cisco 7200 NPE 300 or NPE 400 Series routers
- Network management software
 - Cisco VPN Solution Center v2.1

Dial Out Remote Access Scenarios

L2TP Dial-Out Remote Access

In dial-out remote access, instead of a remote user or customer edge router 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 customer edge router. Dial-out access can use either L2TP or direct ISDN architecture.

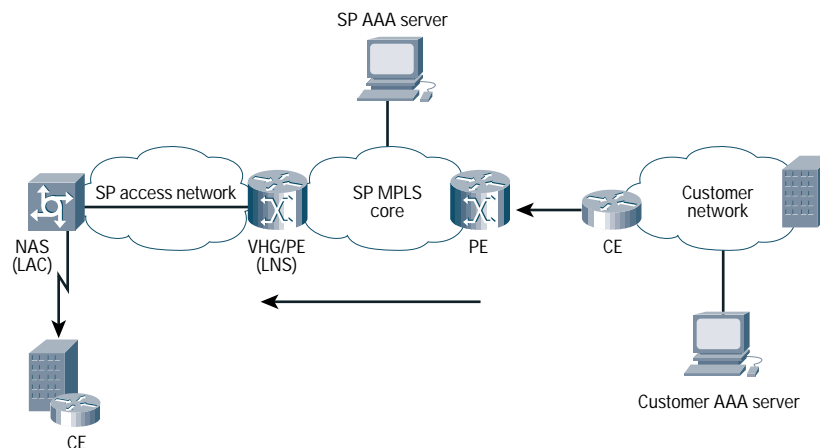
Dial-out is often used for automated functions. For example, a central database system might dial out nightly to remote vending machines to collect daily sales data and to check inventories. In this release of Cisco Remote Access to MPLS VPN Integration, the dialer interface used is a dialer profile. With a dialer profile, each physical interface becomes a member of a dialer pool. The VHG/provider edge router (in L2TP dial-out) or the network access server/provider edge router (in direct dial-out) triggers a call when it receives interesting traffic from a remote peer in the customer VPN. (“Interesting traffic” is traffic destined for this particular dial-out network.)

Based on the dialer interface configuration, the VHG/provider edge router or network access server/provider edge router 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 remote 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 5 shows the topology for L2TP dial-out access, and Figure 6 shows the topology for direct ISDN dial-out access.

Figure 5
Topology of L2TP Dial-Out Remote Access

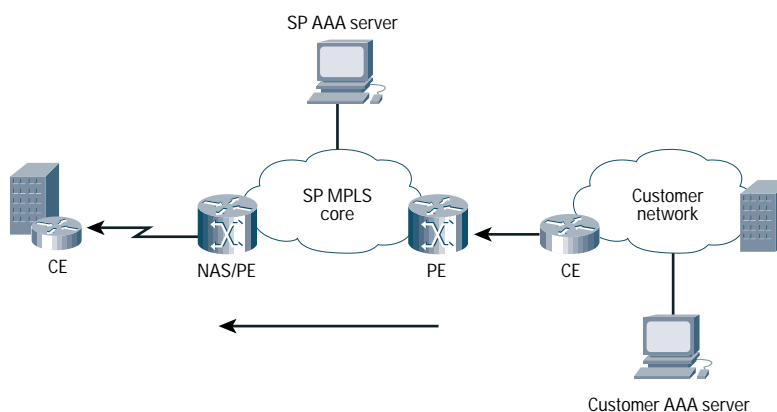


In the dial-out scenario, traffic from a specific customer VPN that is destined for a specific dial-out network (identified through static routes in the customer VRF) is directed to the appropriate VHG/provider edge router or network access server/provider edge router. Upon receiving the traffic, either the VHG/provider edge router or the network access server/provider edge router responds. In the case of L2TP dial-out (Figure 5), the VHG/provider edge router brings up an L2TP tunnel and negotiates an outgoing PPP session with the network access server. The dial-out PPP session is triggered using dialer profiles, and the network access server then dials out to the customer edge router using dial-out information received in the L2TP session negotiation.

Direct ISDN Dial-Out Remote Access

In the case of direct ISDN dial-out (Figure 6), the network access server/provider edge router dials out directly to the customer edge router and the dial-out PPP session is triggered using dialer profiles.

Figure 6
Topology of Direct ISDN Dial-Out Remote Access



L2TP Dial-Out Components

The major components of the dial-out architecture shown in Figures 5 and 6 are listed here along with a description of the role each component plays and the specific platforms these architectures supports.

- Network access servers:
 - Cisco 3640 Router, 60 ISDN ports, or 48 basic telephone service ports
 - Cisco 3660 Router, 120 ISDN ports, or 96 basic telephone service ports
- VHG/provider edge routers:
 - Cisco 7200 NPE 300 or NPE 400 Series routers
 - Cisco 7500 RSP 4 or RSP 8 Series routers
 - Cisco 6400 NRP 2 Universal Access Concentrator
- Network management software
 - Cisco VPN Solution Center v2.1

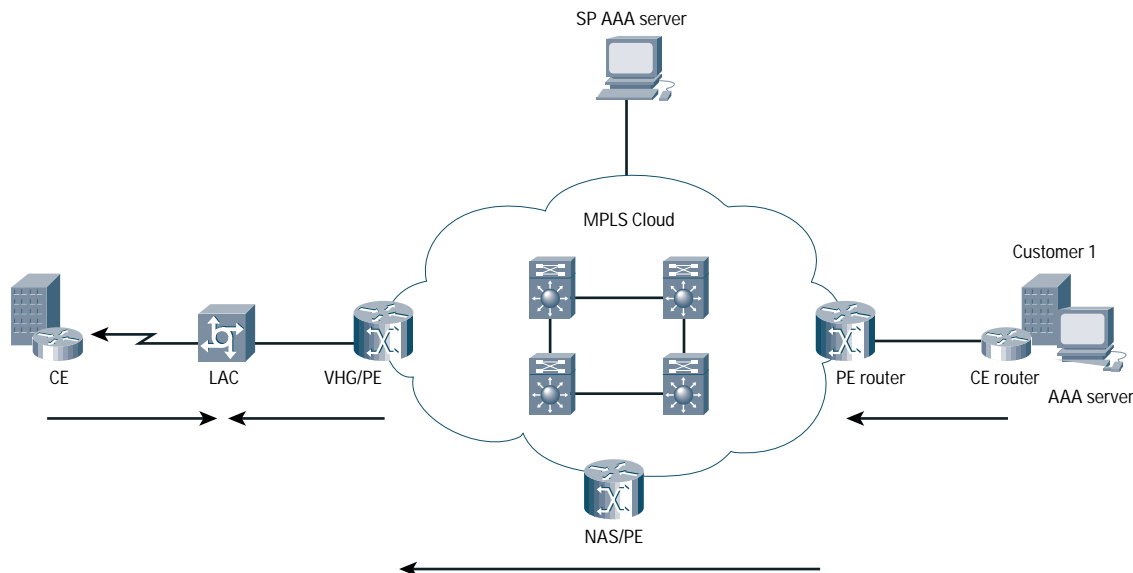
Direct ISDN Dial-Out Components

- Network access servers:
 - Cisco 3640 Router, 60 ISDN ports, or 48 basic telephone service ports
 - Cisco 3660 Router, 120 ISDN ports, or 96 basic telephone service ports
 - Cisco 7200 NPE 300 or NPE 400 Series routers
- Customer premises equipment (CPE)
 - Any Cisco CPE supporting dial/ISDN functionality

Large-Scale Dial-Out Remote Access

Large-scale dial-out eliminates the need to configure dialer maps on every network access server for every destination. Instead, you can create remote site profiles containing outgoing call attributes (telephone number, service type, and so on) on the AAA server (Figure 7). The network access server downloads this profile when an interesting packet requires that a call be placed to a remote site. Additionally, large-scale dial-out addresses congestion management by seeking a non-congested, alternative network access server within the same POP when the designated primary network access server experiences port congestion.

Figure 7
Topology of Large-Scale Dial-Out



Large-Scale Dial-Out Components

- Network access servers:
 - Cisco 3640 Router, 60 ISDN ports, or 48 basic telephone service ports
 - Cisco 3660 Router, 120 ISDN ports, or 96 basic telephone service ports
- Virtual home gateway/provider edge:



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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

- Cisco 7200 NPE 300 or NPE 400 Series routers
- Cisco 7500 RSP 4 or RSP 8 Series routers
- Cisco 6400 NRP 2 Universal Access Concentrator
- Network management software
 - Cisco VPN Solution Center v2.1
- Customer Premise Equipment (CPE)
 - Any Cisco CPE supporting dial/ISDN functionality

For More Information

For more information about the Cisco Remote Access to MPLS VPN Solution, go to the following URL:

Cisco VPN solutions: <http://www.cisco.com/go/vpnsolutions>