



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

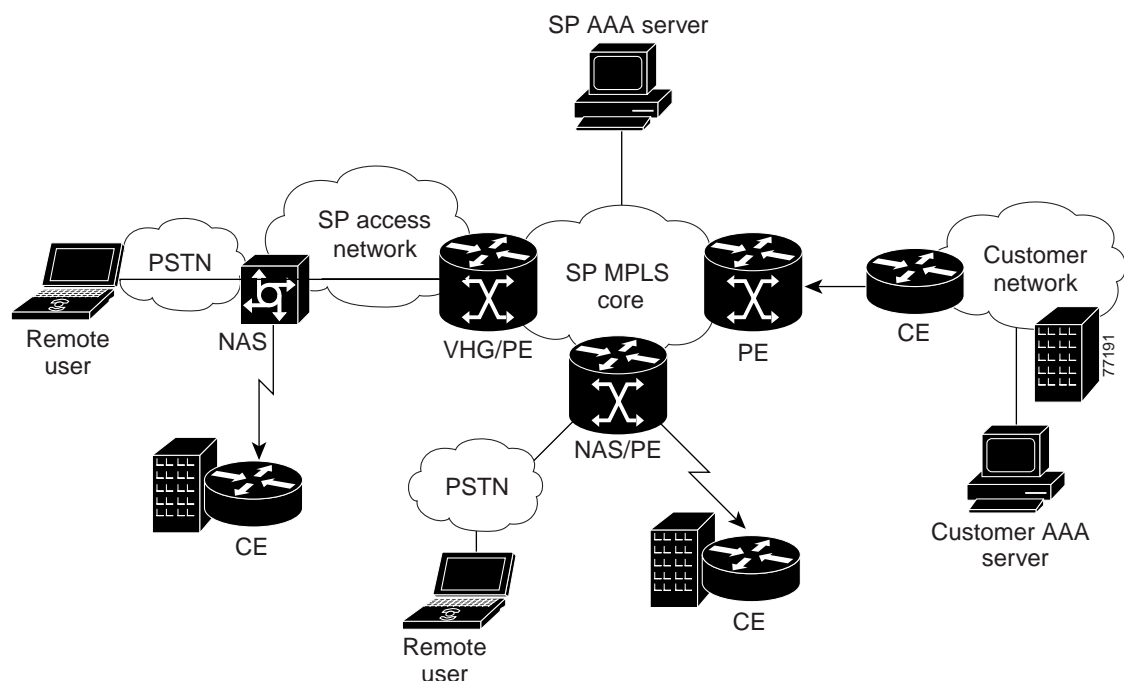
With MPLS VPN, a service provider can create scalable, efficient, and feature-rich customer VPNs across the core of a network. Adding remote dial access integration provides the remote customer edge router (CE) to provider edge router (PE) link that integrates dial users into their MPLS VPNs.

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

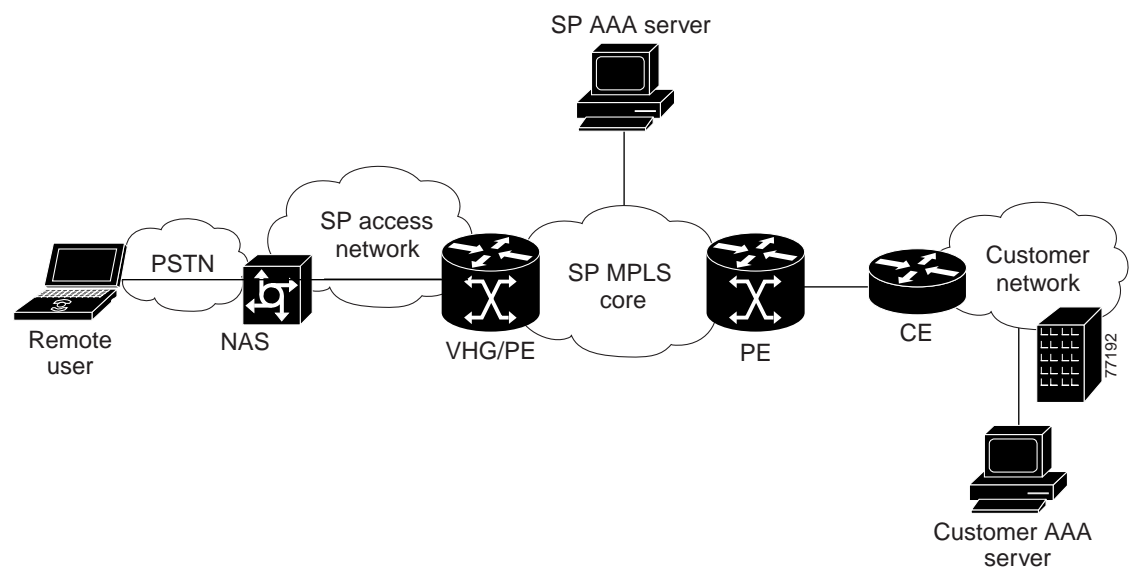
Layer 2 Tunnel Protocol (L2TP) dial-in access is designed for service providers who want to offer wholesale dial service to their customers. The service provider (or a large Internet service provider) maintains geographically dispersed points of presence (POPs). A customer of the service provider dials 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: <ul style="list-style-type: none"> • 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/cgi-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/cgi-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/cgi-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/cgi-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/cgi-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/cgi-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/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:6400

Overview of Direct ISDN PE Dial-in Remote Access

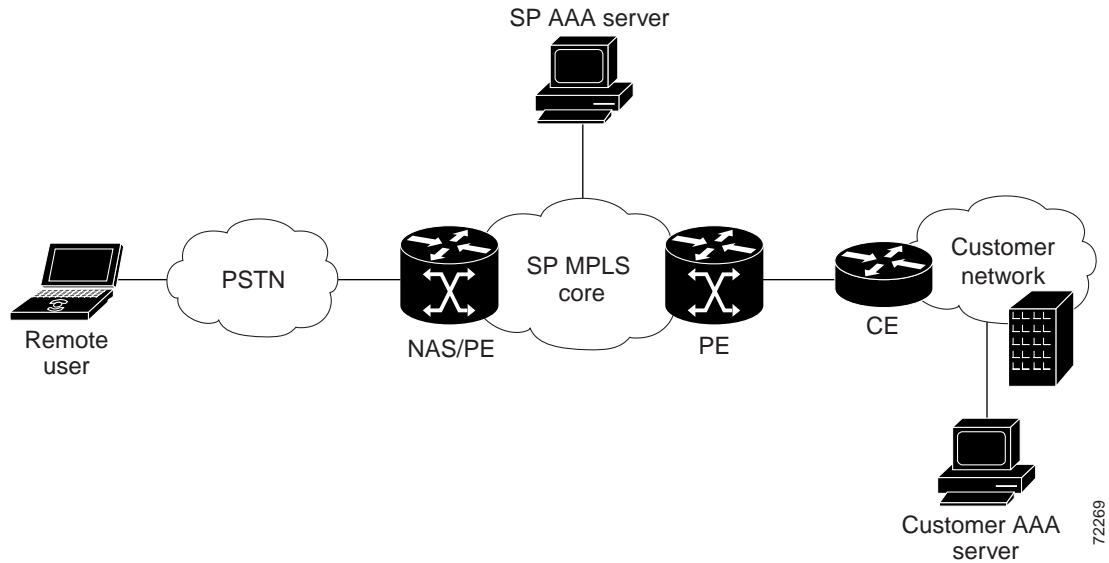
In direct ISDN PE dial-in access to an MPLS VPN, a NAS functions as both NAS and PE. (For that reason, the NAS is referred to here as a NAS/PE.) In contrast to an L2TP dial-in access session, the PPP session is placed directly in the appropriate VRF for the MPLS VPN, rather than being forwarded to a 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: <ul style="list-style-type: none"> • 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/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:3600
Cisco 7200 NPE300/NPE400 series routers	12.2(8)T	http://www.cisco.com/cgi-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.

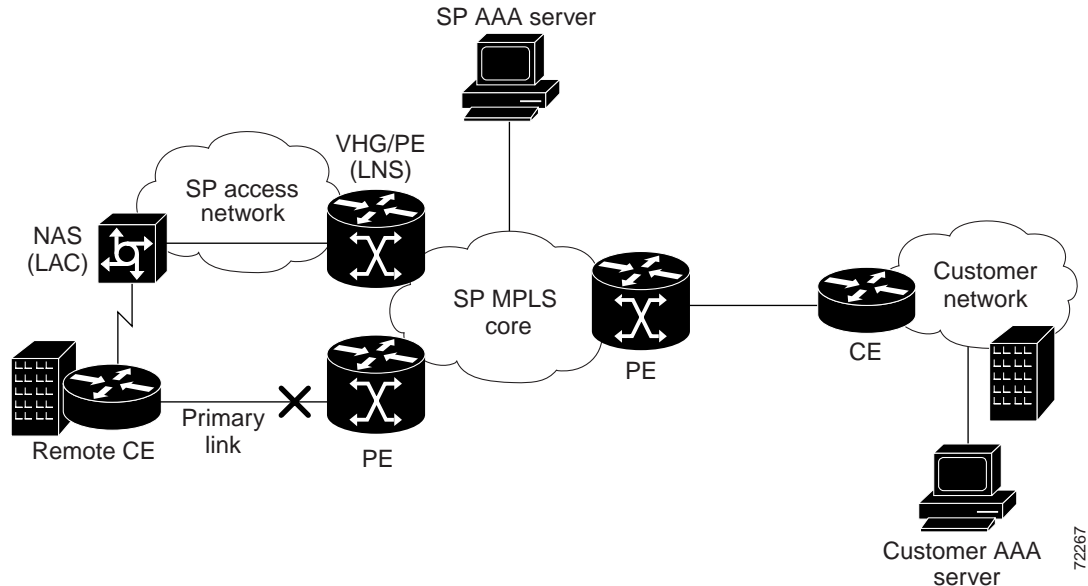
Call flow in dial backup is identical to that in L2TP dial-in access, except that the call is initiated by a backup interface when connectivity to the primary interface is lost, instead of by a remote user. A dialer interface is configured to dial in to the service provider's NAS using a dial backup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

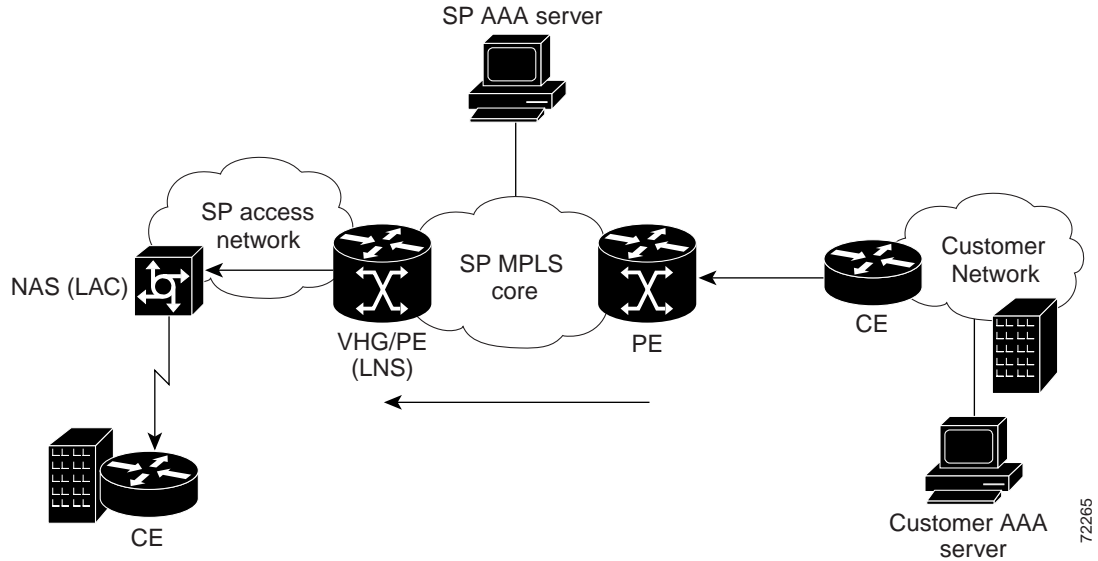
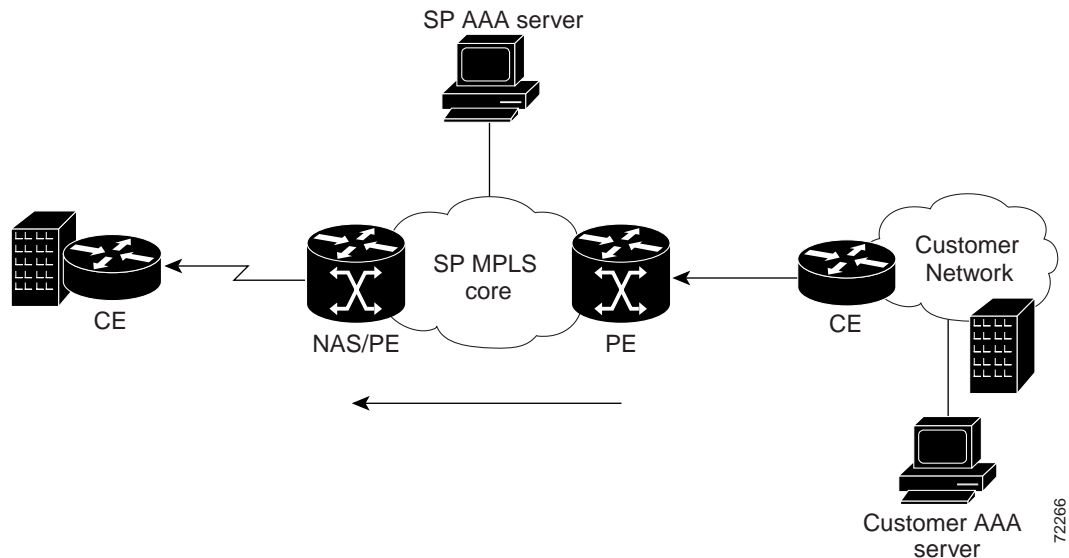


Figure 2-6 Topology of Direct ISDN Dial-out Remote Access



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: <ul style="list-style-type: none"> • 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/cgi-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/cgi-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/cgi-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/cgi-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: <ul style="list-style-type: none"> • 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/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:3600
Cisco 7200 NPE300/NPE400 series routers	12.2(8)T	http://www.cisco.com/cgi-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, page 2-12](#)
- [Framed-Route VRF Aware, page 2-12](#)

- [Per-VRF AAA, page 2-12](#)
- [VPDN Multihop with VRF Support, page 2-13](#)
- [AAA Servers, page 2-13](#)
- [Address Management, page 2-13](#)
- [Authorization and Authentication, page 2-14](#)
- [Accounting, page 2-15](#)
- [Core MPLS Network, page 2-15](#)
- [Management Tools, page 2-15](#)
- [Network Management Components for Dial Access, page 2-15](#)

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 than 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/vpns/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 within 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 the 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.

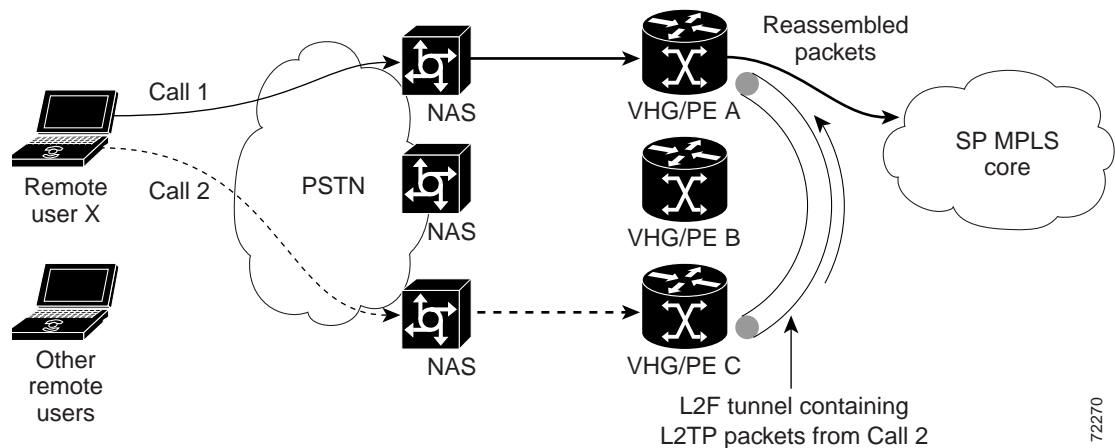
To set up MMP, you use the Stack Group Bidding Protocol (SGBP), which assigns ownership of a call to a master VHG/PE or NAS/PE in the stack group through a process of bidding. The call flow follows this general sequence (shown in [Figure 2-7](#)):

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.

