VPDN Technology Overview

Virtual private dial-up networks (VPDNs) securely carry private data over a public network, allowing remote users to access a private network over a shared infrastructure such as the Internet. VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for point-to-point connections between remote users and a central network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About VPDNs

Overview of VPDN Technology

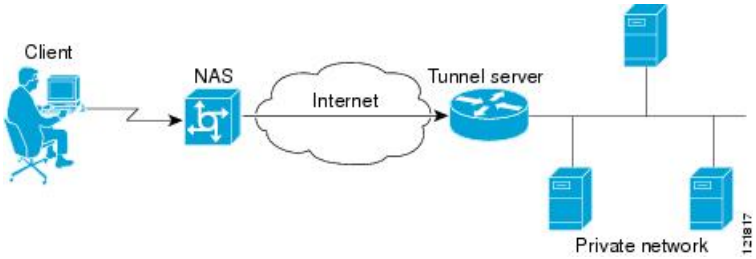
VPDNs extend private network dial-in services to remote users. VPDNs use Layer 2 tunneling technologies to create virtual point-to-point connections between remote clients and a private network. VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for point-to-point connections between remote users and a central network.

Instead of connecting directly to the remote private network, VPDN users connect to a nearby access server, which is often located at an Internet service provider (ISP) local point of presence (POP). Data is securely forwarded from the access server to the private network over the Internet, providing a cost-effective method of communication between remote clients and the private network.

A benefit of VPDNs is the way they delegate responsibilities for the network. The customer can outsource responsibility for the information technology (IT) infrastructure to an ISP that maintains the modems that the remote users dial in to, the access servers, and the internetworking expertise. The customer is then responsible only for authenticating users and maintaining the private network.

The figure below shows a basic VPDN network deployment.

Figure 1: Basic VPDN Network Deployment



A PPP client dials in to an ISP access server, called the Network Access Server (NAS). The NAS determines whether it should forward that PPP session on to the router or access server that serves as the point of contact for the private network, the tunnel server. The tunnel server authenticates the user and initiates PPP negotiations. Once PPP setup is complete, all frames that are sent between the client and the tunnel server pass through the NAS.

VPDNs can use these tunneling protocols to tunnel link-level frames:

- Layer 2 Tunneling Protocol (L2TP)
- Layer 2 Tunneling Protocol Version 3 (L2TPv3)
- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)

Note PPTP is not supported on the Cisco ASR 1000 Series routers.

Using one of these protocols, a tunnel is established between the NAS or client and the tunnel server, providing secure data transport over a shared infrastructure such as the Internet.

Note VPDNs on the Cisco ASR 1000 Series Aggregation Services Routers can use only the Layer 2 Tunneling Protocol (L2TP) or the Layer 2 Tunneling Protocol Version 3 (L2TPv3) to tunnel link-level frames.

VPDN Terminology

VPDN Hardware Devices

Generally three devices are involved in VPDN tunneling. Two of these devices function as tunnel endpoints--one device initiates the VPDN tunnel, and the other device terminates the VPDN tunnel. Depending on the tunneling architecture, different types of devices can act as the local tunnel endpoint.

As new tunneling protocols have been developed for VPDNs, protocol-specific terminology has been created to describe some of the devices that participate in VPDN tunneling. However, these devices perform the same basic functions no matter what tunneling protocol is being used. For the sake of clarity we will use this generic terminology to refer to VPDN devices throughout this documentation:

- Client--The client device can be the PC of a dial-in user, or a router attached to a local network. In client-initiated VPDN tunneling scenarios, the client device acts as a tunnel endpoint.
- NAS--The network access server (NAS) is typically a device maintained by an ISP that provides VPDN services for its customers. The NAS is the local point of contact for the client device. Establishing a connection between the NAS and the client will referred to as *receiving a calll* or *placing a calll*, depending on whether a dial-in or dial-out scenario is being discussed. Depending on the tunneling architecture, the NAS functions as follows:
  - For NAS-initiated VPDN tunneling scenarios and dial-out VPDN tunneling scenarios, the NAS functions as a tunnel endpoint. The NAS initiates dial-in VPDN tunnels and terminates dial-out VPDN tunnels. The Cisco ASR 1000 Series Aggregation Services Routers support dial-in only.
  - For client-initiated VPDN tunneling scenarios, the NAS does not function as a a tunnel endpoint; it simply provides Internet connectivity.
- Tunnel server--The tunnel server is typically maintained by the customer and is the contact point for the remote private network. The tunnel server terminates dial-in VPDN tunnels and initiates dial-out VPDN tunnels.
- Tunnel server--The tunnel server is typically maintained by the customer and is the contact point for the remote private network. The tunnel server terminates dial-in VPDN tunnels and initiates dial-out VPDN tunnels.
- Tunnel switch--A tunnel switch is a device configured to perform multihop VPDN tunneling. A tunnel switch acts as both a NAS and a tunnel server. The tunnel switch terminates incoming VPDN tunnels and initiates the outgoing VPDN tunnels that will carry data on to the next hop.

Although technically a tunnel switch is a tunnel endpoint for both the incoming tunnel and the outgoing tunnel, for the sake of simplicity the tunnel endpoints in a multihop deployment are considered to be the device that initiates the first tunnel and the device that terminates the final tunnel of the multihop path.

The table below lists the generic terms and the corresponding technology-specific terms that are sometimes used to describe the NAS and the tunnel server.

Table 1: VPDN Hardware Terminology

Generic Term	L2F Term	L2TP Term	PPTP Term
NAS	NAS	L2TP access concentrator (LAC)	PPTP access concentrator (PAC)
Tunnel server	Home gateway	L2TP network server (LNS)	PPTP network server (PNS)

Note The Cisco ASR 1000 Series Aggregation Services Routers support only L2TP.

VPDN Tunnels

A VPDN tunnel exists between the two tunnel endpoints. The tunnel consists of a control connection and zero or more Layer 2 sessions. The tunnel carries encapsulated PPP datagrams and control messages between the tunnel endpoints. Multiple VPDN sessions can use the same VPDN tunnel.

VPDN Sessions

A VPDN session is created between the tunnel endpoints when an end-to-end PPP connection is established between a client and the tunnel server. Datagrams related to the PPP connection are sent over the tunnel. There is a one-to-one relationship between an established session and the associated call. Multiple VPDN sessions can use the same VPDN tunnel.

VPDN Architectures

Client-Initiated Dial-In VPDN Tunneling

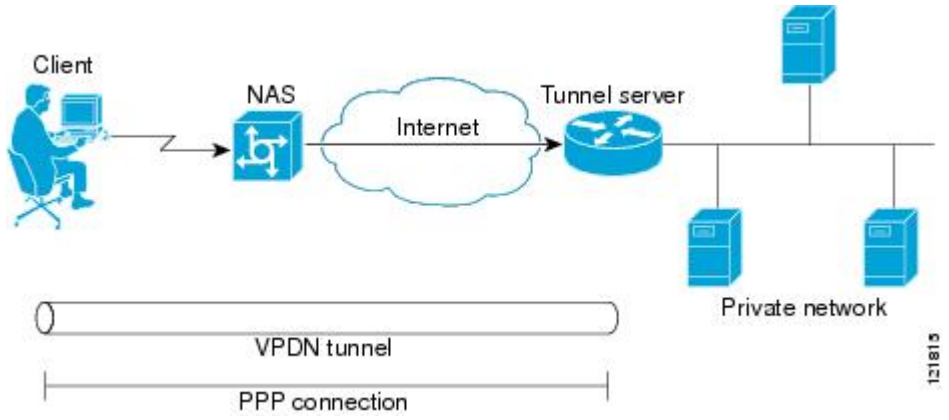
Client-initiated dial-in VPDN tunneling is also known as voluntary tunneling. In a client-initiated dial-in VPDN tunneling scenario, the client device initiates a Layer 2 tunnel to the tunnel server, and the NAS does not participate in tunnel negotiation or establishment. In this scenario, the NAS is not a tunnel endpoint; it simply provides Internet connectivity. The client device must be configured to initiate the tunnel.

The main advantage of client-initiated VPDN tunneling is that it secures the connection between the client and the ISP NAS. However, client-initiated VPDNs are not as scalable and are more complex than NAS-initiated VPDNs.

Client-initiated VPDN tunneling can use the L2TP protocol or the L2TPv3 protocol if the client device is a router. If the client device is a PC, only the PPTP protocol is supported.

The figure below shows a client-initiated VPDN tunneling scenario.

Figure 2: Client-Initiated Dial-In VPDN Scenario



For further information about client-initiated tunneling deployments, see the “Configuring Client-Initiated Dial-In VPDN Tunneling” module.

Before configuring a client-initiated dial-in VPDN tunneling deployment, you must complete the required tasks in the “Configuring AAA for VPDNs” module.

NAS-Initiated Dial-In VPDN Tunneling

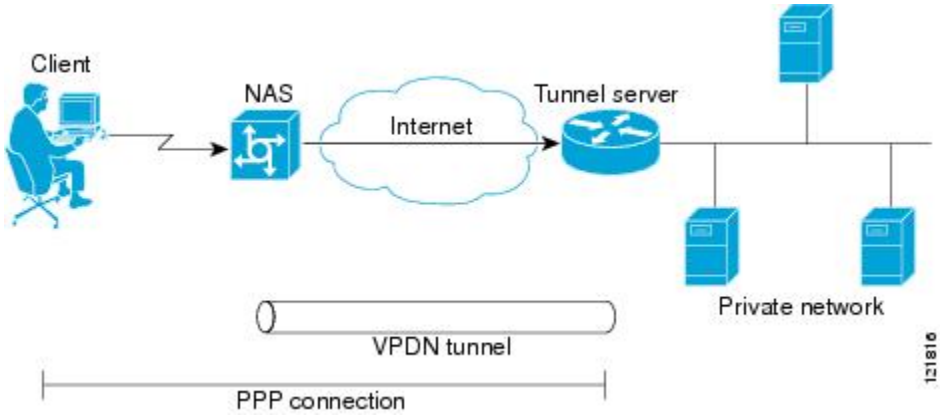
NAS-initiated dial-in VPDN tunneling is also known as compulsory tunneling. In a NAS-initiated dial-in VPDN tunneling scenario, the client dials in to the NAS through a medium that supports PPP. If the connection from the client to the ISP NAS is over a medium that is considered secure, such as digital subscriber line (DSL), ISDN, or the public switched telephone network (PSTN), the client can choose not to provide additional security. The PPP session is securely tunneled from the NAS to the tunnel server without any special knowledge or interaction required from the client.

NAS-initiated VPDN tunneling can be configured with the L2TP or L2F protocol.

Note The Cisco ASR 1000 Series Aggregation Services Routers support only L2TP.

The figure below shows a NAS-initiated dial-in tunneling scenario.

Figure 3: NAS-Initiated Dial-In VPDN Scenario



For further information about NAS-initiated tunneling deployments, see the Configuring NAS-Initiated Dial-In VPDN Tunneling module.

Before configuring a NAS-initiated dial-in VPDN tunneling deployment, you must complete the required tasks in the Configuring AAA for VPDNs module.

Multihop VPDN Tunneling

Multihop VPDN is a specialized VPDN configuration that allows packets to pass through multiple tunnels. Ordinarily, packets are not allowed to pass through more than one tunnel. In a multihop tunneling deployment, the VPDN tunnel is terminated after each hop and a new tunnel is initiated to the next hop destination. A maximum of four hops is supported.

Multihop VPDN is required for the scenarios described in these sections:

VPDN Tunneling to an MMP Stack Group

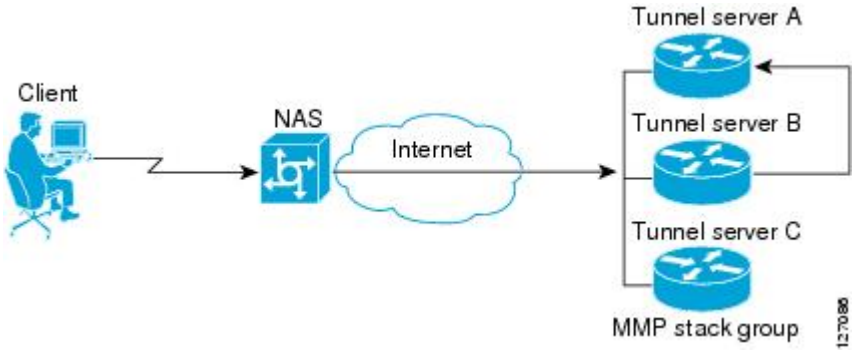
Multihop VPDN is required when the private network uses Mutlichassis Multilink PPP (MMP) with multiple tunnel servers in a stack group. Stack group configurations require the ability to establish Layer 2 tunnels between participating hardware devices. If the incoming data is delivered to the stack group over a VPDN tunnel, multihop VPDN is required for the stack group to function.

Multihop VPDN tunneling with MMP can be configured using the L2TP or L2F protocol.

Note The Cisco ASR 1000 Aggregation Services Routers support only L2TP.

The figure below shows a network scenario using a multihop VPDN with an MMP deployment.

Figure 4: MMP Using Multihop VPDN



For further information about configuring multihop VPDN for MMP deployments, see the Configuring Multihop VPDN module.

Before configuring a multihop VPDN for MMP deployment, you must configure MMP and you must complete the required tasks in the Configuring AAA for VPDNs module.

Tunnel Switching VPDNs

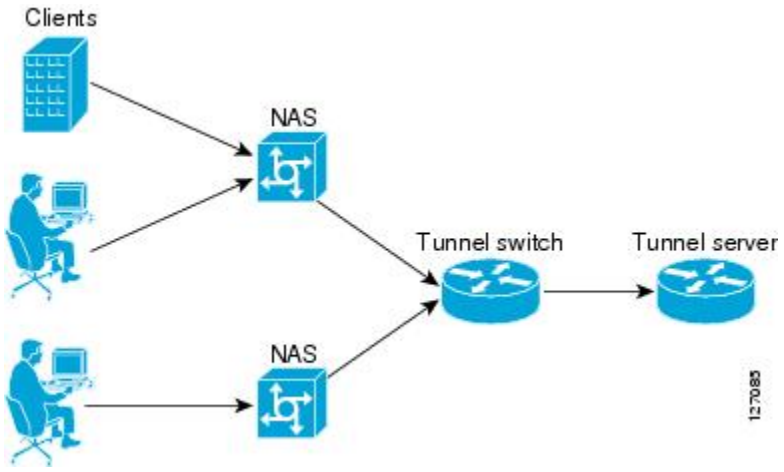
Multihop VPDN can be used to configure a router as a tunnel switch. A tunnel switch is a device that is configured as both a NAS and a tunnel server. A tunnel switch is able to receive packets from an incoming VPDN tunnel and send them out over an outgoing VPDN tunnel. Tunnel switch configurations can be used between ISPs to provide wholesale VPDN services.

Multihop tunnel switching can be configured using the L2TP, L2F, or PPTP protocol.

Note The Cisco ASR 1000 Aggregation Services Routers support only L2TP.

The figure below shows a network scenario using a tunnel switching deployment.

Figure 5: Tunnel Switching Using Multihop VPDN



For further information about multihop tunnel switching deployments, see the Configuring Multihop VPDN module.

Before configuring a multihop tunnel switching deployment, you must complete the required tasks in the Configuring AAA for VPDNs module.

VPDN Tunneling Protocols

VPDNs use Layer 2 protocols to tunnel the link layer of high-level protocols (for example, PPP frames or asynchronous High-Level Data Link Control (HDLC). ISPs configure their NAS to receive calls from users and to forward the calls to the customer tunnel server.

Usually, the ISP maintains only information about the customer tunnel server. The customer maintains the users' IP addresses, routing, and other user database functions. Administration between the ISP and the tunnel server is reduced to IP connectivity.

This section contains information on L2TP and L2TPv3, which are the only protocols that can be used for VPDN tunneling on the Cisco ASR 1000 Series Routers.

L2TP

L2TP is an Internet Engineering Task Force (IETF) standard that combines the best features of the two older tunneling protocols: Cisco L2F and Microsoft PPTP.

L2TP offers the same full-range spectrum of features as L2F, but offers additional functionality. An L2TP-capable tunnel server will work with an existing L2F NAS and will concurrently support upgraded components running L2TP. Tunnel servers do not require reconfiguration each time an individual NAS is upgraded from L2F to L2TP. The table below compares L2F and L2TP feature components.

Table 2: L2F and L2TP Feature Comparison

Function	L2F	L2TP
Flow Control	No	Yes
Attribute-value (AV) pair hiding	No	Yes

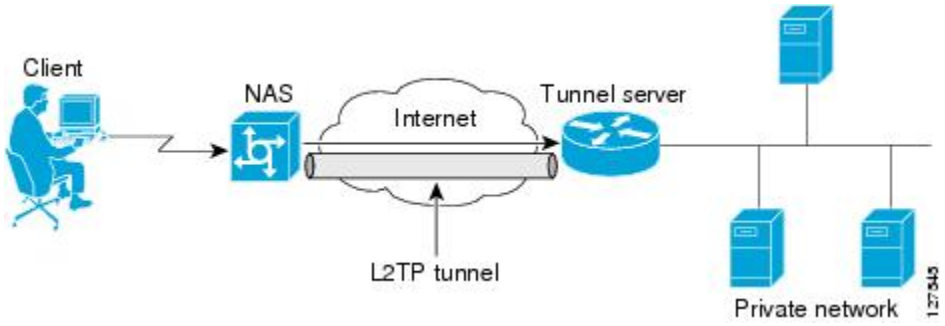
Function	L2F	L2TP
Tunnel server load sharing	Yes	Yes
Tunnel server stacking/multihop support	Yes	Yes
Tunnel server primary and secondary backup	Yes	Yes
Domain Name System (DNS) name support	Yes	Yes
Domain name flexibility	Yes	Yes
Idle and absolute timeout	Yes	Yes
Multilink PPP support	Yes	Yes
Multichassis Multilink PPP support	Yes	Yes

Security	• All security benefits of PPP, including multiple per-user authentication options:
	  • Challenge Handshake Authentication Protocol (CHAP)
	  • Microsoft CHAP (MS-CHAP)
	  • Password Authentication Protocol (PAP)
	• Tunnel authentication mandatory
		• All security benefits of PPP, including multiple per-user authentication options:
		  • CHAP
		  • MS-CHAP
		  • PAP
		• Tunnel authentication optional

Traditional dialup networking services support only registered IP addresses, which limits the types of applications that are implemented over VPDNs. L2TP supports multiple protocols and unregistered and privately administered IP addresses. This allows the existing access infrastructure--such as the Internet, modems, access servers, and ISDN terminal adapters (TAs)--to be used. It also allows customers to outsource dial-out support, thus reducing overhead for hardware maintenance costs and 800 number fees, and allows them to concentrate corporate gateway resources.

The figure below shows the basic L2TP architecture in a typical dial-in environment.

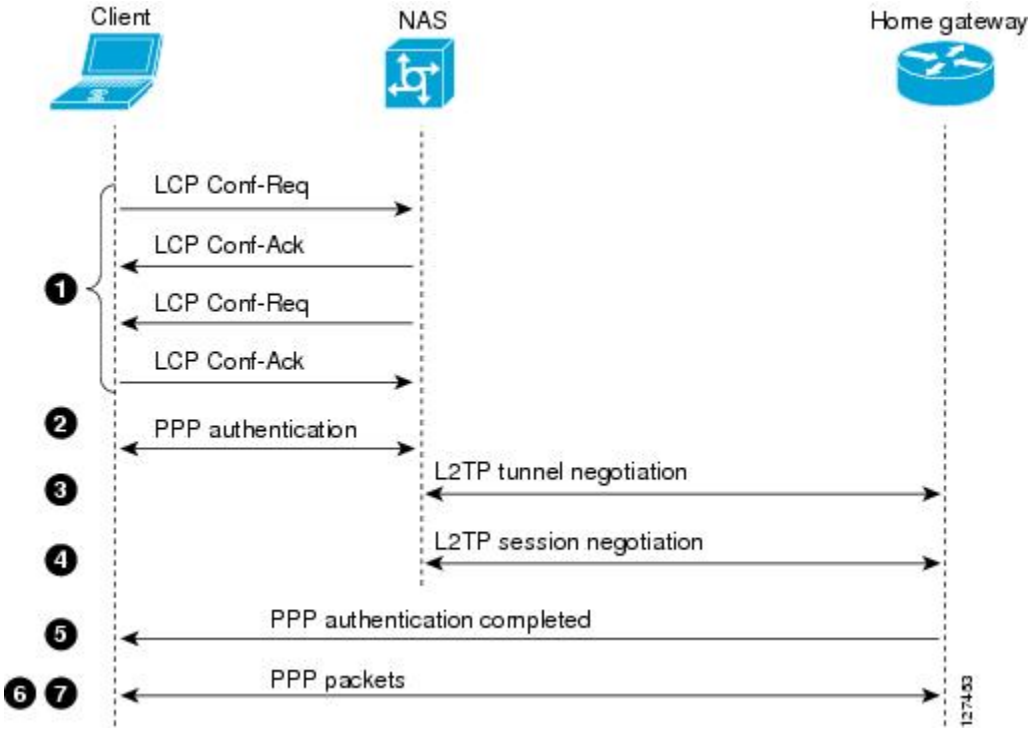
Figure 6: L2TP Architecture



Using L2TP tunneling, an ISP or other access service can create a virtual tunnel to link remote sites or remote users with corporate home networks. The NAS located at the POP of the ISP exchanges PPP messages with remote users and communicates by way of L2TP requests and responses with the private network tunnel server to set up tunnels. L2TP passes protocol-level packets through the virtual tunnel between endpoints of a point-to-point connection. Frames from remote users are accepted by the ISP NAS, stripped of any linked framing or transparency bytes, encapsulated in L2TP, and forwarded over the appropriate tunnel. The private network tunnel server accepts these L2TP frames, strips the L2TP encapsulation, and processes the incoming frames for the appropriate interface.

The figure below depicts the events that occur during establishment of a NAS-initiated dial-in L2TP connection.

Figure 7: L2TP Protocol Negotiation Events



The following describes the sequence of events shown in the figure above and is keyed to the figure:

1. The remote user initiates a PPP connection to the ISP NAS using a medium that supports PPP such as the analog telephone system. The NAS accepts the connection, the PPP link is established, and Link Control Protocol (LCP) is negotiated.
2. After the end user and NAS negotiate LCP, the NAS partially authenticates the end user with CHAP or PAP. The username, domain name, or Dialed Number Information Service (DNIS) is used to determine whether the user is a VPDN client. If the user is not a VPDN client, authentication continues, and the client will access the Internet or other contacted service. If the username is a VPDN client, the mapping will name a specific endpoint (the tunnel server).
3. The tunnel endpoints, the NAS and the tunnel server, authenticate each other before any tunnel or session establishment is attempted. Alternatively, the tunnel server can accept tunnel creation without any tunnel authentication of the NAS. The NAS and the tunnel server exchange control messages to negotiate tunnel establishment.
4. Once the tunnel exists, an L2TP session is created for the end user. The NAS and the tunnel server exchange call messages to negotiate session establishment.
5. The NAS will propagate the negotiated LCP options and the partially authenticated CHAP or PAP information to the tunnel server. The tunnel server will funnel the negotiated options and authentication information directly to the virtual access interface, allowing authentication to be completed. If the options configured in the virtual template interface do not match the options negotiated with the NAS, the connection will fail and a disconnect notification will be sent to the NAS.
6. PPP packets are exchanged between the dial-in client and the remote tunnel server as if no intermediary device (the NAS) is involved.

Subsequent PPP incoming sessions (designated for the same tunnel server) do not repeat the L2TP tunnel negotiation because the L2TP tunnel is already open.

L2TPv3

L2TPv3 is an enhanced version of L2TP with the capability to tunnel any Layer 2 payload. L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 Virtual Private Networks (VPNs).

In VPDN deployments, L2TPv3 can be used to establish a client-initiated tunnel from a local router to the remote customer network over an emulated circuit known as a pseudowire. There is one pseudowire associated with each L2TPv3 session.

Rather than using a VPDN group configuration, L2TPv3 uses an L2TP class configuration that is associated with the pseudowire. L2TPv3 pseudowires can also be used to establish L2TP tunnels by configuring an L2TP class on the local device and an accept-dialin VPDN group on the customer network.

For detailed information about the L2TPv3 protocol, see the Additional References section.

VPDN Group Configuration Modes

Many VPDN configuration tasks are performed within a VPDN group. A VPDN group can be configured to function either as a NAS VPDN group or as a tunnel server VPDN group, but not as both. However, an individual router can be configured with both a NAS VPDN group and a tunnel server VPDN group.

You can configure a VPDN group as a specific type of VPDN group by issuing at least one of the commands listed in the table below:

Table 3: VPDN Subgroup Configuration Modes

VPDN Group Type	Command	Command Mode	Command Mode Prompt
tunnel server	**accept-dialin**	VPDN accept-dialin configuration	Router(config-vpdn-acc-in)#
NAS	**request-dialin**	VPDN request-dialin configuration	Router(config-vpdn-req-in)#

Many of the commands required to properly configure VPDN tunneling are issued in one of the VPDN subgroup configuration modes shown in the table below. Removing the VPDN subgroup command configuration will remove all subordinate VPDN subgroup configuration commands as well.

Where to Go Next

Once you have identified the VPDN architecture that you want to configure and the tunneling protocol that you will use, you should perform the required tasks in the Configuring AAA for VPDNs module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
VPDN commands	*Cisco IOS VPDN Command Reference*
Technical support documentation for L2TP	Layer 2 Tunnel Protocol (L2TP)
Technical support documentation for VPDNs	Virtual Private Dial-Up Network (VPDN)
Information on L2TPv3	L2TPv3: Layer 2 Tunnel Protocol Version 3 module

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2661	*Layer Two Tunneling Protocol L2TP*
RFC 3931	*Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VPDN Technology Overview

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for VPDN Technology Overview

Feature Name	Releases	Feature Information
L2TP Layer 2 Tunneling Protocol	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3S	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. VPDNs use Layer 2 protocols to tunnel the link layer of high-level protocols (for example, PPP frames or asynchronous HDLC). L2TP is an IETF standard that combines the best features of the two older tunneling protocols: Cisco L2F and Microsoft PPTP. No commands were introduced or modified by this feature.

Feature Name	Releases	Feature Information
Virtual Private Dial-up Network (VPDN)	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. VPDNs securely carry private data over a public network, allowing remote users to access a private network over a shared infrastructure such as the Internet. VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for point-to-point connections between remote users and a central network. No commands were introduced or modified by this feature.