

Multihop VPDN

Feature Summary

Multihop Virtual Private Dialup Network (VPDN) solves two problems for users. They are described below.

- It enables Multichassis Multilink PPP in multiple home gateways. It allows packets generated by the same remote host and received by two different home gateways in a multichassis stack group to be recombined successfully on the initial home gateway contacted.

Multihop VPDN solves the problem of multilink packets generated from the same remote host being unable to recombine once they arrive at the target home gateway in the corporate network. To arrive at the proper router, packets can traverse two tunnels en route to the first router contacted, generally called the bundle owner. Hopping over two tunnels is ordinarily not allowed, but with Multihop VPDN, multiple-tunnel hops are possible. For a detailed breakdown of the Multihop VPDN process, see the example in the “Functional Description” section.

- Multihop VPDN also enables wholesale dial service by allowing an ISP to use the equipment of a service provider to provide coverage of the corporate user.

Benefits

With Multihop VPDN, packets generated from a remote host can traverse more than one tunnel. Ordinarily, packets cannot hop through more than one tunnels. Packets received by different home gateways in a multiple home gateway stack must be recombined and resequenced on the bundle owner. Some instances require packets to be rerouted to the bundle owner in another home gateway, traversing more than two tunnels. Before even reaching the corporate network, the packets have already crossed a tunnel created by the VPDN, connecting the Network Access Server (NAS) to the corporate network. Once they arrive at the corporate network, the packets may have to traverse more than another tunnel, crossing home gateways to arrive at the bundle owner. This number of tunnel crossings would violate the multiple-tunnel rule, preventing the packets from successfully arriving at the bundle owner.

Multihop VPDN allows packets to pass through multiple tunnels using both L2F and L2TP protocols in a VPDN environment.

List of Terms

The following terms are useful in understanding Multihop VPDN functionality.

Basic Rate Interface (BRI). An ISDN interface that contains two B links and one D link of circuit switched communication of voice, video, and data.

bundle owner—Typically, the device that terminates the PPP connection of the call from the remote client. Once this device has terminated the connection, then it owns all connections generated by the client. As soon as the client hangs up, the terminating device is no longer the bundle owner.

Challenge Handshake Authentication Protocol (CHAP)—Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

hop—Term describing the passage of a packet between two network nodes (for example, two routers).

home gateway—A router which terminates an L2F/L2TP tunnel originating from a network access server.

L2F—A tunneling protocol that allows an Internet service provider (ISP) or other access service to create a virtual tunnel to link a customer's remote site or remote users with corporate home networks.

L2TP—An extension to PPP merges features of two tunneling protocols: Layer 2 Forwarding (L2F) from Cisco Systems and Point-to-Point Tunneling (PPTP) from Microsoft. L2TP is an Internet Engineering Task Force (IETF) emerging standard, currently under codevelopment and endorsed by Cisco Systems, and other networking industry leaders.

L2TP Access Concentrator (LAC)—A device attached to a switched network fabric (such as, PSTN or ISDN) or colocated with a PPP end system capable of handling the L2TP protocol. A LAC device implements the media, over which L2TP passes traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. LAC is the initiator of incoming calls and the receiver of outgoing calls. LAC is also known as NAS in Layer 2 Forwarding (L2F) terminology.

L2TP Network Server (LNS)—A device operating on any platform capable of PPP termination that handles the server side of the L2TP protocol. Since L2TP relies on the single media over which L2TP tunnels arrive, an LNS may have only a single LAN or WAN interface, yet still be able to terminate calls arriving at any of the LACs' full range of PPP interfaces. LNS is the initiator of outgoing calls and the receiver of incoming calls.

Multilink PPP—A protocol that provides the capability of fragmenting and reassembling packets to a single end-system across a logical pipe (also called a bundle) formed by multiple links. Multilink PPP provides bandwidth on demand.

Multichassis Multilink PPP—Multilink PPP with the additional capability for links to terminate at multiple routers with different remote addresses. This protocol is intended for situations with large pools of dial-in users, where a single chassis cannot provide enough dial-in ports.

Network Access Server (NAS)—A communications processor that connects asynchronous devices to a LAN or WAN through network and terminal emulation software. Performs both synchronous and asynchronous routing of supported protocols.

Password Authentication Protocol (PAP)—Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines.

Primary Rate Interface (PRI)—An ISDN interface that contains 23 B links and one D link of circuit switched communication of voice, video, and data. Also, it can be an E1 interface with 30 data channels.

stack group—A group of peer routers comprising a home gateway stack.

Stack Group Bidding Protocol (SGBP)—A protocol that determines the proper bundle owner for a packet after the packet is received from another home gateway.

stack group peer—Any router in a given home gateway stack. Stack groups do not need a lead router.

tunneling—Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

Virtual Private Dialup Network (VPDN)—A network that allows separate and autonomous protocol domains to share common access infrastructure, including modems, access servers, and ISDN routers. A VPDN enables users to configure secure networks that take advantage of ISPs that tunnel the company's remote access traffic through the ISP cloud.

Platforms

This feature is supported on the following routers and access servers:

- Cisco 7500 series
- Cisco 7000 series
- Cisco 7200 series
- Cisco 4000 series
- Cisco 3800 series
- Cisco 3600 series
- Cisco 2600 series
- Cisco 2500 series
- Cisco 1600 series
- Cisco 2500 series access servers
- Cisco AS5100 access server
- Cisco AS5200 universal access server

Prerequisites

To use the VPDN Multihop feature, you need to configure the following entities on your network:

- A remote client
- An ISDN or asynchronous lines connection
- A stack of home gateways in a corporate network
- A computer with a PPP stack and dial-out access
- An L2F/L2TP-capable network access server
- An L2F/L2TP-capable home gateway

Supported MIBs and RFCs

There are no new MIBs or RFCs supported for this feature.

Functional Description

Multihop VPDN is useful in enabling packets to traverse up to four tunnels. Packet traversal of more than one tunnel is not permitted without the Multihop VPDN feature. Two scenarios are common where four tunnels need to be traversed by file packets.

- A packet needs to make five hops across four home gateways (that is, from home gateway 1 to home gateway 2 to home gateway 3 to home gateway 4 to home gateway 5).
- A packet needs to traverse a service provider link from a phone call made to a corporate network and then make hops between four separate home gateways, thus creating four tunnel traversals

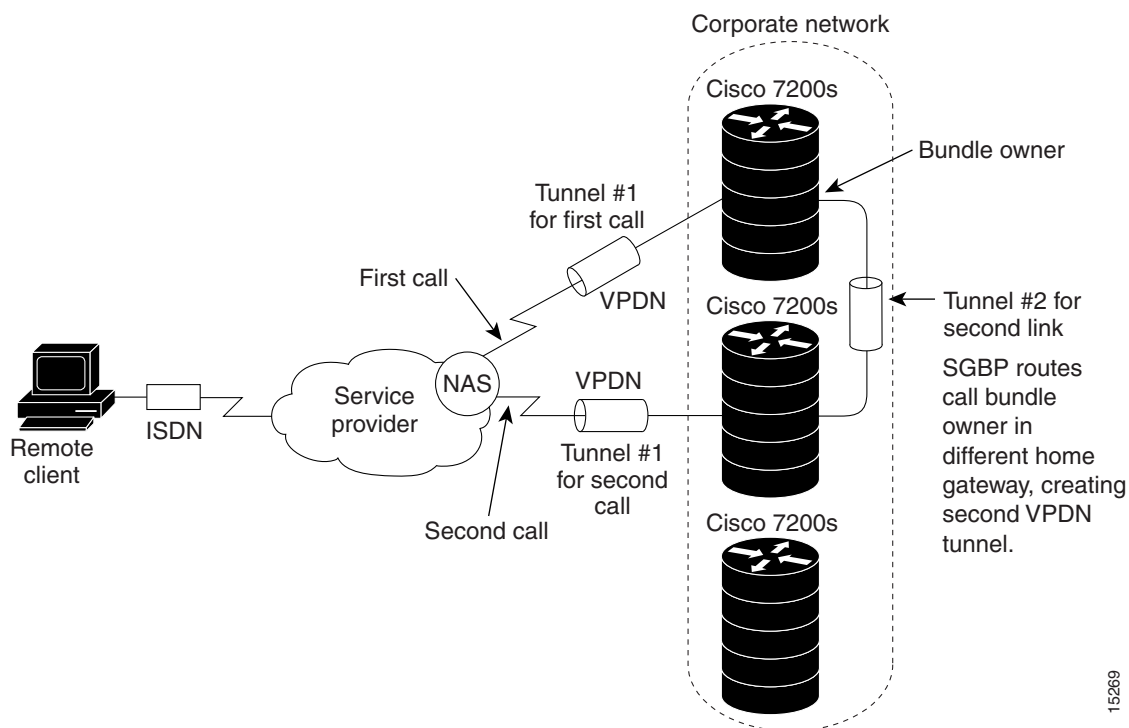
The following process describes a common Multihop VPDN scenario where packets need to traverse multiple home gateways at a corporate network:

- 1 When the home gateways are set up, they are configured with Multihop VPDN enabled.
- 2 As a remote user, you contact your corporate network by dialing up a stack of home gateways, each containing a bank of devices that will receive a call, for example, Cisco 7200 routers. The call is made through a Network Access Server (NAS) created by a service provider. The connection between the NAS and the corporate network is created through a VPDN tunnel. Typically, the connection comprises the following entities:
 - Your PC is connected to an ISDN line or multiple asynchronous lines containing a Basic Rate Interface (BRI). BRIs contain two B links and one D link.
 - One of the B links on the BRI line is connected to a NAS at a service provider (for example, a telephone company) with a VPDN.
 - The service provider NAS is connected to an ISDN line or multiple asynchronous lines that contain a Primary Rate Interface (PRI). PRIs contain 23 B channels and one D channel. This connection is made through a VPDN.
 - One of the B links on the PRI is connected to a corporate network comprised of a stack group of home gateways each containing a bank of devices set up to receive a call, for example, Cisco 7200 routers. Each of these home gateways is connected to each other with a VPDN.
- 3 Using a round-robin technique, members of the stack group contend to field the dialup session from the call.
- 4 One of the stack group members in a home gateway fields the dialup connection and becomes the receiver or *bundle owner* for the session and the session is established.
- 5 Because you are sending a large file (for example, an elaborate graphic) performance is a concern. To enhance performance, the Multilink PPP technique is deployed on the connection line, splitting each packet into fragments, each of which will flow through both the two B channels on the BRI and the 23 B channels on the PRI. This creates bandwidth on demand and reduces transmission latency across WAN links.
- 6 The packet fragments arrive at the corporate network and are reassembled.
- 7 Sometimes, multiple calls are established in cases when the file is too large to be handled by one call. This calls made after the first call may not initially be received by the bundle owner or even by a router in the home gateway where the bundle owner resides.

- 8 Using Stack Group Bidding Protocol (SGBP), the packets are identified as belonging to the proper bundle owner in the correct home gateway.
- 9 If the router that receives the packets from the second call resides on a different home gateway, it establishes a *tunnel* and forwards all packets belonging to the call to the router that owns the call in its proper home gateway. This technique is called Multichassis Multilink PPP because more than one home gateway is deployed in the receipt of packets. Note that this bundle owner packet forwarding session creates a second tunnel and that only one tunnel is allowed per session. By issuing the **vpdn multihop** command when the network administrator has initially set up your home gateway, you have enabled two tunnels to occur.
- 10 After arriving at the bundle owner in the proper home gateway, the packets are reassembled.

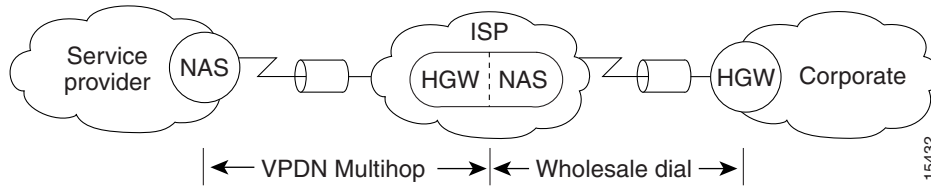
Figure 1 illustrates the Multihop VPDN process for traversing multiple home gateways. Figure 2 illustrates the Multihop VPDN process for traversing two consecutive home gateways (wholesale dial service).

Figure 1 Multihop VPDN Enabling Traversal of Two Tunnels in Multiple Home Gateways



15269

Figure 2 Multihop VPDN Enabling Traversal of Two Consecutive Home Gateways



Configuration Tasks

Connect your remote host to a service provider via either an ISDN line or pair of asynchronous lines. Make sure the service provider connects you to the destination network you are interested in reaching.

Use the following commands in Interface Configuration Mode:

Command	Purpose
vpdn incoming <i>remote-name local-name</i> virtual-template <i>number</i>	Specify the local name to use for authenticating and the virtual template to use for building interfaces for incoming connections when an L2F or L2TP tunnel connection is required from a remote host.
vpdn multihop	Enable the Multihop VPDN feature so that packets can be recombined at the target router.

Configuration Examples

The following example shows the scenario detailed in the “Functional Description” section and shown in Figure 1 where a packet traverses a VPDN tunnel over a service provider link and then a second tunnel by traversing a hop between home gateways on the corporate network. The bundle owner is Home-Gateway1 and the stack group peer, Home-Gateway2, is specified as a peer (1.1.1.2).

```
vpdn multihop
username stack password hellothere
multilink virtual-template 1

sgbp group stack
sgbp member Home-Gateway2 1.1.1.2

interface virtual-template 1
ip unnum e0
ppp multilink
ppp auth chap
```

Stack Group Bidding Protocol (SGBP) is initiated using the SGBP commands. SGBP identifies the proper bundle owner of the packets from a second call. Challenge Handshake Authentication Protocol (CHAP) is initiated using the command line `ppp auth chap`. CHAP is an authentication protocol that validates receipt of packets and ensures they are reassembled correctly upon receipt at a corporate network.

The following example shows code that specifies the home gateway as the next hop to another home gateway as shown in Figure 2:

```
vpdn incoming isp hp-gw virtual-template 1
vpdn outgoing hp.com hp-gw ip 1.1.1.4
```

Command Reference

This section documents the new **vpdn multihop** command.

vpdn multihop

To enable Multihop VPDN, use the **vpdn multihop** interface configuration command.

vpdn multihop

Syntax Description

This command has no arguments or keywords.

Default

Multihop is not enabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)T.

Before using the **vpdn multihop** command, refer to the *Dial Solutions Configuration Guide* to learn more about Multilink PPP and Multichassis Multilink PPP.

Example

The following example enables Multihop VPDN:

```
vpdn multihop
```

What to Do Next

For more information, see sections on Multilink PPP and Multichassis Multilink PPP in the *Dial Solutions Configuration Guide*.