Configuring Multihop VPDN

Multihop virtual private dialup networking (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 deployment, the VPDN tunnel is terminated after each hop and a new tunnel is initiated to the next hop destination.

Multihop VPDN deployments are required when the remote private network uses Multichassis Multilink PPP (MMP) with multiple tunnel servers in a stack group.

Multihop VPDN deployments can also be used to configure a device as a tunnel switch. A tunnel switch acts as both a network access server (NAS) and a tunnel server, 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 Internet service providers (ISPs) to provide wholesale VPDN services.

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 at the end of this module.

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.

Prerequisites for Multihop VPDN

Before you configure multihop VPDN, a VPDN deployment must be configured. For more information about VPDN deployments that are compatible with multihop VPDN scenarios, see the Configuring an MMP Stack Group for Multihop VPDN, on page 6 or the Configuring a Multihop Tunnel Switch, on page 14.

Information About Multihop VPDN

Using Multihop VPDN with an MMP Stack Group

Multihop VPDN is required when a VPDN tunnel delivers Multilink PPP (MLP) data to a private network that uses an MMP stack group.

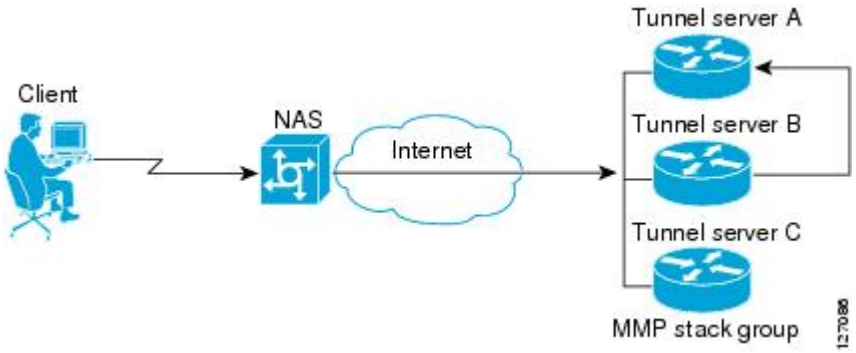
MLP provides the capability of splitting and recombining packets to a single end system across a logical pipe (also called a bundle) formed by multiple links.

MMP deployments link multiple tunnel servers in a stack group. Different members of a stack group can terminate MLP links from the same source. Stack group tunnel servers must establish Layer 2 tunnels between each other so that MLP packets from a single host can be properly recombined. If the incoming MLP data is delivered to the stack group over a VPDN tunnel, multihop VPDN is required for the stack group to function.

MMP using multihop VPDN can use only the Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) protocol on the NAS and the stack group members.

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

Figure 1: MMP Using Multihop VPDN



Data from the client is tunneled from the NAS to a stack group member using either L2TP or L2F. If the client is using MLP, multiple data links can terminate on different stack members. Stack group bidding protocol (SGBP) is used to determine which stack member is the MLP bundle owner. Tunnel servers that receive calls belonging to a bundle owned by a different stack group member will forward those calls to the owner using an L2TP or L2F tunnel. Because the data must traverse two VPDN tunnels in this scenario, multihop VPDN must be enabled.

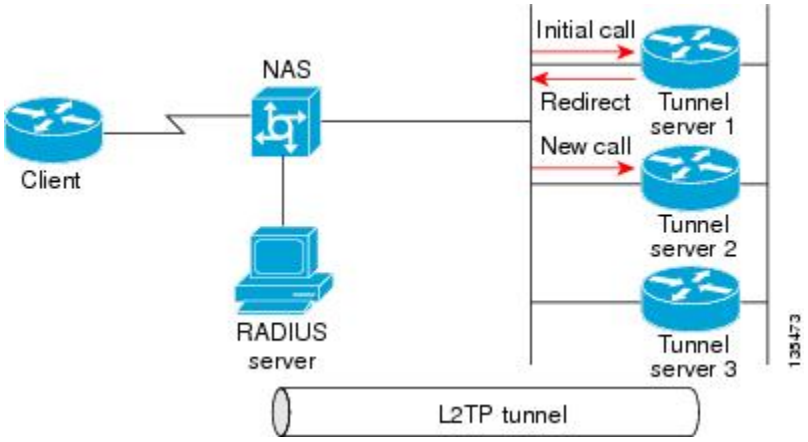
L2TP Redirect for MMP Multihop Deployments

In a traditional MMP deployment, the stack group tunnel servers use L2TP or L2F tunnels to deliver MLP links to the bundle owner. This architecture does not easily scale beyond a few routers per tunnel server stack, and inherently adds hops and latency variations between links in a bundle.

Enabling L2TP redirect allows a stack group member to send a redirect message to the NAS if it receives a link that is owned by another stack group member. L2TP redirect increases the scalability of MMP deployments, load balances sessions across the stack group tunnel servers, and smooths traffic as all links in a multilink bundle experience the same delay and latency.

The figure below shows a network scenario using L2TP redirect for an MMP deployment.

Figure 2: L2TP Redirect Scenario



When tunnel server 1 answers the initial call, SGBP bidding is performed by all stack group members to determine which device owns the call. If the call is owned by a different tunnel server, such as tunnel server 2, the call must be passed from tunnel server 1 to the owner.

In a traditional multihop SGBP deployment, tunnel server 1 would establish an L2F or L2TP tunnel to to tunnel server 2 and forward the call over that tunnel.

With L2TP redirect enabled, instead of establishing a new tunnel to tunnel server 2, tunnel server 1 sends a redirect message to the NAS informing it that tunnel server 2 actually owns the call. The NAS then tears down the initial connection to tunnel server 1 and establishes a new L2TP tunnel directly to tunnel server 2.

How L2TP Redirect Works

In a traditional SGBP multihop VPDN deployment, if a stack group member receives a call that belongs to a different stack group member, it forwards the call to the bundle owner over an L2TP or L2F tunnel. When L2TP redirect is configured, instead of forwarding the call to the bundle owner the stack group member will send a redirect message to the NAS. The redirect message includes the IP address or redirect identifier of the bundle owner. The NAS will terminate the initial connection, and initiate a new connection directly to the bundle owner.

For L2TP redirect to function, it must be enabled on both the NAS and the stack group tunnel servers. If the NAS is not configured for L2TP redirect, the tunnel server will forward the call to the bundle owner using

traditional multihop technology. This maintains interoperability with non-Cisco devices and Cisco devices running older versions of Cisco IOS software.

In order to redirect the call, the NAS must perform redirect authorization for the bundle owner. If a redirect identifier has been configured on the bundle owner, the NAS uses that identifier to get redirect authorization information. Otherwise, the IP address of the bundle owner must be configured on the NAS.

Number of Redirect Attempts on the NAS

In some cases, a stack group member other than the device that answers the first call from a particular MLP bundle might win the SGBP bid for that call. The call will be redirected to the winning device, but because the call is again the first call from that MLP bundle, another SGBP bid will be triggered. In some rare instances this behavior might result in the initial call being passed from one stack group member to another as different devices win the bid each time.

By default, the NAS will redirect a particular call only three times, preventing excessive redirects. The number of redirect attempts the NAS will make can be configured to meet the needs of a particular network deployment. Once the NAS has redirected a call the configured number of times it will refuse further redirection requests, and traditional multihop forwarding will occur on the stack group.

Load Balancing Calls Using L2TP Redirect

Enabling L2TP redirect allows load balancing of calls to be performed by the stack group rather than the NAS. The stack group tunnel servers bid for each link that comes in, and those tunnel servers with the lightest load will win the bid and become the bundle owner. The managing of bids in this manner results in an even load distribution of sessions among a stack of tunnel servers.

L2TP redirect can also be used to load balance all L2TP PPP calls (not just MLP calls) across a stack group. All the NASs for a particular domain can point to a primary contact tunnel server. This primary tunnel server must have SGBP and the **sgbp ppp-forward** command configured to force it to issue a mastership query to the stack group for every PPP link. As when performing MLP load balancing, the stack group tunnel servers bid for each link that comes in, and those tunnel servers with the lightest load will win the bids. The primary tunnel server might not actually terminate any sessions; it might simply issue the mastership query, collects the bids, choose the highest one, and redirect the originating NAS to that tunnel server.

Redirect Identifier

The redirect identifier is an optional configuration that simplifies the task of configuring NASs to perform L2TP redirects. If the redirect identifier is not configured, the IP address of every tunnel server in the stack group must be configured with the **initiate-to** command on each NAS.

The redirect identifier allows new stack group members to be added without the need to update the NAS configuration with their IP addresses. With the redirect identifier configured, a new stack group member can be added and given the same redirect identifier as the rest of the stack group. If stack group members have different authorization information, unique redirect identifiers must be configured.

The redirect identifier can also be configured on a remote RADIUS server, rather than directly on the NAS. The RADIUS server can update multiple NASs with the redirect identifier information, avoiding the requirement to configure the redirect identifier on each NAS.

Redirect Source

The redirect source is an optional configuration that allows a stack group member to advertise a public IP address for L2TP redirection, rather than the IP address used for SGBP bidding. Often a stack group will use private IP addresses for stack group bidding, and these IP addresses will not be reachable by the NAS. Configuring a public IP address as the redirect source allows a stack group member to inform the NAS of the reachable IP address of another stack group member in the redirect request.

Tunnel Switching Using Multihop VPDN

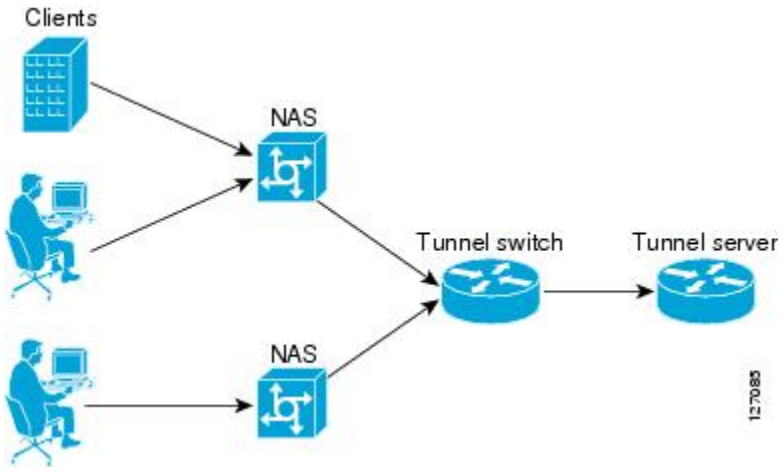
Multihop VPDN can be used to configure a device as a tunnel switch. A tunnel switch acts as both a NAS and a tunnel server, receiving packets from an incoming VPDN tunnel and sending them out over an outgoing VPDN tunnel. Tunnel switch configurations can be used between ISPs to provide wholesale VPDN services. A VPDN tunnel switch can forward L2TP, L2F, or Point-to-Point Tunneling Protocol (PPTP) sessions.

In an L2TP or L2F tunnel switching deployment, the tunnel endpoints are considered the originating NAS and the terminating tunnel server. The tunnel switch is not considered a tunnel endpoint.

In a PPTP tunnel switching deployment, the tunnel endpoints are considered the originating client device and the terminating tunnel server. The tunnel switch is not considered a tunnel endpoint.

The figure below shows a network scenario using a basic L2TP tunnel switching deployment.

Figure 3: Tunnel Switching Using Multihop VPDN



The tunnel switch can be configured to terminate incoming VPDN tunnels from multiple devices, and to initiate outgoing VPDN tunnels to one or more tunnel servers.

The Subscriber Service Switch (SSS) framework is supported for VPDN tunnel switching. SSS supports additional Layer 2 protocols, including PPP over Ethernet (PPPoE), PPP over ATM (PPPoA), and generic routing encapsulation (GRE). Configuring SSS for VPDN tunnel switching is optional. SSS profiles increase the scalability of tunnel switching configurations, particularly in multiprotocol environments.

How to Configure Multihop VPDN

Configuring an MMP Stack Group for Multihop VPDN

Multihop VPDN is required when a VPDN tunnel delivers MLP data to a private network that uses a MMP stack group.

Perform this task on each of the stack group tunnel servers to enable multihop VPDN.

Before You Begin

- MMP must be enabled, and a stack group must be configured.
- The NAS must be configured to initiate L2TP or L2F VPDN tunnels. For information on configuring the NAS to initiate L2TP or L2F VPDN tunnels, see the Configuring NAS-Initiated Dial-In Tunneling module.
- The stack group tunnel servers must be configured to accept incoming L2TP or L2F VPDN tunnels. For information on configuring the stack group tunnel servers to accept incoming L2TP or L2F VPDN tunnels, see the Configuring NAS-Initiated Dial-In Tunneling module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn multihop**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn multihop** **Example:** `Router(config)# vpdn multihop`	Enables VPDN multihop.

Configuring L2TP Redirect for MMP VPDNs

Enabling L2TP redirect allows a tunnel server in a stack group to send a redirect message to the NAS if it receives a link that belongs to another tunnel server in the stack group. L2TP redirect increases the scalability of MMP deployments. Because all links in a multilink bundle will travel directly to the bundle master after redirection they will experience the same delays and latency, resulting in smoother traffic.

L2TP redirect can be used to load balance both MLP and PPP calls across a stack group.

Perform these tasks to configure L2TP redirect:

Prerequisites for Configuring L2TP Redirect

- The NAS and tunnel servers must be Cisco equipment.
- MMP must be enabled, and a stack group must be configured.
- The NAS and the stack group tunnel servers must be configured for L2TP VPDN tunneling. For configuration information, see the Configuring NAS-Initiated Dial-In VPDN Tunneling module.
- Multihop VPDN must be enabled on the stack group members. To enable multihop VPDN on the stack group, perform the task in the Configuring an MMP Stack Group for Multihop VPDN section.

Restrictions for Configuring L2TP Redirect

- Only the L2TP tunneling protocol is supported.
- L2TP redirect capability is supported only for stack group deployments.

Enabling L2TP Redirect

For the redirection of calls to occur, L2TP redirect must be enabled on the NAS and on each participating tunnel server.

Perform this task to enable L2TP redirect on all participating devices and to optionally set the number of allowed redirect attempts on the NAS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn redirect**
4. **vpdn redirect attempts** *number-of-attempts*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn redirect** **Example:** `Router(config)# vpdn redirect`	Enables L2TP redirect functionality on a NAS or tunnel server.
Step 4	**vpdn redirect attempts** *number-of-attempts* **Example:** `Router(config)# vpdn redirect attempts 5`	(Optional) Restricts the number of redirect attempts possible for a given L2TP call on the NAS. • *number-of-attempts* --The number of redirect attempts. Valid values range from 1 to 20. The default value is 3. • If you do not issue this command, the default value for *number-of-attempts* will be applied. **Note** This command is used only on the NAS.

What to Do Next

You must perform the task in the Enabling Multihop VPDN on the NAS section.

Enabling Multihop VPDN on the NAS

Because redirected packets will pass through multiple VPDN tunnels, multihop must be enabled on the NAS for L2TP redirect to function.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn multihop**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn multihop** **Example:** `Router(config)# vpdn multihop`	Enables VPDN multihop on the NAS.

Configuring the Redirect Identifier on the NAS

The L2TP redirect identifier is an optional configuration that simplifies the task of configuring the NAS for L2TP redirect. The redirect identifier can be configured directly on the NAS, or on the remote RADIUS server. Configuring the redirect identifier on the remote RADIUS server allows it to be propagated to multiple NASs without having to configure each NAS directly.

Perform this task to configure the redirect identifier directly on the NAS.

To configure the redirect identifier on the RADIUS server, perform the task in the Configuring the Redirect Identifier on the RADIUS Server, on page 10 instead.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **redirect identifier** *identifier-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and to enters VPDN group configuration mode.
Step 4	**redirect identifier** *identifier-name* **Example:** `Router(config-vpdn)# redirect identifier stack1`	Configures a VPDN redirect identifier to use for L2TP call redirection on a NAS. **Note** The redirect identifier configured on the NAS must match the redirect identifier configured on the stack group tunnel servers. **Note** If stack group members have different authorization information, unique redirect identifiers must be configured for each.

What to Do Next

You must perform the task in the Configuring the Redirect Identifier on the Stack Group Tunnel Servers, on page 11.

Configuring the Redirect Identifier on the RADIUS Server

The L2TP redirect identifier is an optional configuration that simplifies the task of configuring the NAS for L2TP redirect. The redirect identifier can be configured directly on the NAS, or on the remote RADIUS server. Configuring the redirect identifier on the remote RADIUS server allows it to be propagated to multiple NASs without having to configure each one.

Perform this task to configure the redirect identifier in the RADIUS server profile.

To configure the redirect identifier directly on a NAS, perform the task in the"Configuring the Redirect Identifier on the NAS, on page 9 instead.

SUMMARY STEPS

1. **:0:" vpdn:vpdn-redirect-id =** *identifier-name* **"**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**:0:" vpdn:vpdn-redirect-id =** *identifier-name* **"** **Example:** `:0:"vpdn:vpdn-redirect-id = stack1"`	Configures the redirect identifier in the RADIUS profile. • To avoid having to configure multiple NASs, update the RADIUS profile so that the RADIUS server automatically updates the configurations of the multiple NASs. • Refer to your vendor-specific RADIUS configuration documentation for specific instructions on updating the RADIUS profile. **Note** The redirect identifier configured in the RADIUS profile must match the redirect identifier configured on the stack group tunnel servers. **Note** If stack group members have different authorization information, unique redirect identifiers must be configured for each.

What to Do Next

You must perform the task in the Configuring the Redirect Identifier on the Stack Group Tunnel Servers, on page 11.

Configuring the Redirect Identifier on the Stack Group Tunnel Servers

The redirect identifier is an optional configuration that simplifies the task of configuring the NAS for L2TP redirect. The redirect identifier must be configured on each member of the stack group.

Perform this task on each stack group tunnel server to configure the redirect identifier.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn redirect identifier** *identifier-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn redirect identifier** *identifier-name* **Example:** `Router(config)# vpdn redirect identifier stack1`	Configures a VPDN redirect identifier to use for L2TP call redirection on a stack group tunnel server. **Note** The redirect identifier configured on the stack group members must match the redirect identifier configured on the NAS or in the RADIUS profile. **Note** If stack group members have different authorization information, unique redirect identifiers must be configured for each.

Configuring the Redirect Source on the Stack Group Tunnel Servers

The redirect source is an optional configuration that allows a stack group member to advertise a public IP address for L2TP redirect, rather than the default IP address. The default IP address is that used for SGBP bidding. If your stack group uses private IP addresses for SGBP bidding, you must configure the redirect source for each tunnel server in the stack. Otherwise the NAS will be redirected to the default IP address, which will be unreachable.

Perform this task on each stack group tunnel server to configure the redirect source.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn redirect source** *redirect-ip-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**vpdn redirect source** *redirect-ip-address* **Example:** `Router(config)# vpdn redirect source 10.1.1.1`	Configures the public redirect IP address of a tunnel server.

Monitoring L2TP Redirect Configurations

The number of L2TP sessions that were redirected or forwarded using traditional multihop technology can be monitored. Statistics are maintained on both the NAS and the tunnel servers.

Perform this task on the NAS or a tunnel server to examine L2TP redirect statistics.

SUMMARY STEPS

1. **enable**
2. **show vpdn redirect**
3. **clear vpdn redirect**

DETAILED STEPS

Step 1 **enable**
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

Example:

```
Router> enable
```

Step 2 **show vpdn redirect**
Enter this command to display statistics for all L2TP call redirects and forwards. The display shown in this example is from a tunnel server that redirected four calls using L2TP redirect, and forwarded two calls using traditional multihop VPDN.

Example:

```
Router# show vpdn redirect
‘vpdn redirection enabled’
‘sessions redirected as access concentrator: 4’
‘sessions redirected as network server: 0’
‘sessions forwarded: 2’
```

Step 3 **clear vpdn redirect**
Enter this command to clear the counters for the **show vpdn redirect** command.

Example:

```
Router# clear vpdn redirect
```

Configuring a Multihop Tunnel Switch

Multihop VPDN can be used to configure a device as a tunnel switch. A tunnel switch acts as both a NAS and a tunnel server, and must be configured with both a NAS VPDN group and a tunnel server VPDN group.

Tunnel switching using the SSS infrastructure is supported. SSS allows L2TP, L2F, PPTP, PPPoE, PPPoA, GRE, and general packet radio service (GPRS) sessions to be switched over virtual links using a tunnel switch. SSS configurations are not required for tunnel switching data over L2TP, L2F, or PPTP tunnels, but SSS increases the scalability of tunnel switching deployments .

A multihop VPDN tunnel switch can be configured to forward L2TP, L2F, or PPTP tunnels.

Perform these tasks to configure a device as a multihop VPDN tunnel switch:

Prerequisites for Configuring a Multihop Tunnel Switch

- The tunnel endpoints must be configured for VPDN tunneling as described in the Configuring Client-Initiated Dial-In VPDN Tunneling or in the Configuring NAS-Initiated Dial-IN VPDN Tunneling module.
- If you want to perform VPDN tunnel authorization searches based on the multihop hostname, you must configure the search to use the multihop hostname as described in the Configuring the VPDN Tunnel Authorization Search Order section of the Configuring AAA for VPDNs module.

Restrictions for Configuring a Multihop Tunnel Switch

Tunnel switching based on dialed number identification service (DNIS) numbers or multihop hostnames is supported only in Cisco IOS Release 12.2(13)T and later releases.

Enabling Multihop VPDN on the Tunnel Switch

In tunnel switching deployments, packets must traverse multiple tunnels. Multihop VPDN must be enabled on the tunnel switch for the deployment to function.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn multihop**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn multihop** **Example:** `Router(config)# vpdn multihop`	Enables VPDN multihop.

What to Do Next

You must perform the task in the Configuring the Multihop Tunnel Switch to Terminate Incoming VPDN Tunnels, on page 15.

Configuring the Multihop Tunnel Switch to Terminate Incoming VPDN Tunnels

A tunnel switch must be configured as a tunnel server, allowing it to terminate incoming VPDN tunnels. You can configure a tunnel switch to terminate tunnels from multiple devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **description** *string*
5. **accept-dialin**
6. **protocol** {**any** | **l2f** | **l2tp** | **pptp**}
7. **virtual-template** *number*
8. **exit**
9. **terminate-from hostname** *host-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and to enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.
Step 5	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures a tunnel switch to accept requests from a NAS to establish a tunnel, creates an accept-dialin VPDN subgroup, and enters VPDN accept dial-in subgroup configuration mode.
Step 6	**protocol** {**any** | **l2f** | **l2tp** | **pptp**} **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the Layer 2 protocol that the VPDN group will use. • The **any** keyword can be used to specify that L2TP, L2F, and PPTP tunnels can be switched.
Step 7	**virtual-template** *number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1`	(Optional) Specifies which virtual template will be used to clone virtual access interfaces. This step is not required if the virtual access interface is not going to be cloned when a user connects.
Step 8	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits to VPDN group configuration mode.

	Command or Action	Purpose
Step 9	**terminate-from hostname** *host-name* **Example:** `Router(config-vpdn)# terminate-from hostname NAS12`	Specifies the hostname of the remote NAS that will be required when accepting a VPDN tunnel.

What to Do Next

You must perform the task in the Configuring the Multihop Tunnel Switch to Initiate Outgoing VPDN Tunnels, on page 17.

Configuring the Multihop Tunnel Switch to Initiate Outgoing VPDN Tunnels

A tunnel switch must be configured as a NAS, allowing it to initiate outgoing VPDN tunnels. You can configure a tunnel switch to initiate tunnels to multiple devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **description** *string*
5. **request-dialin**
6. **protocol** {**any** | **l2f** | **l2tp** | **pptp**}
7. Do one of the following:
   - **domain** *domain-name*
   - **dnis** {*dnis-number* | *dnis-group-name*}
   - **multihop-hostname** *ingress-tunnel-name*
8. **exit**
9. **initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.
Step 5	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	Configures a tunnel switch to request the establishment of a tunnel to a tunnel server, creates a request-dialin VPDN subgroup, and enters VPDN request dial-in subgroup configuration mode.
Step 6	**protocol** {**any** | **l2f** | **l2tp** | **pptp**} **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 protocol that the VPDN group will use. • The **any** keyword can be used to specify that L2TP, L2F, and PPTP tunnels can be switched.
Step 7	Do one of the following: • **domain** *domain-name* • **dnis** {*dnis-number* | *dnis-group-name*} • **multihop-hostname** *ingress-tunnel-name* **Example:** `Router(config-vpdn-req-in)# domain company.com`	Requests that PPP calls from a specific domain name be tunneled. or Requests that PPP calls from a specific DNIS number or DNIS group be tunneled. or Enables the tunnel switch to initiate a tunnel based on the NAS host name or the ingress tunnel ID. **Note** If you use the **multihop-hostname** command to configure your tunnel switch, you must configure **vpdn search-order** command with the **multihop-hostname** keyword. For more information on configuring the VPDN tunnel authorization search order, see the "Configuring AAA for VPDNs" module.

	Command or Action	Purpose

	Example:
	`Router(config-vpdn-req-in)# dnis 5687`
	Example:
	`Router(config-vpdn-req-in)# multihop-hostname nas1`	

Step 8	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits to VPDN group configuration mode.
Step 9	**initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*] **Example:** `Router(config-vpdn)# initiate-to ip 10.1.1.1 limit 12`	Specifies an IP address that will be used for Layer 2 tunneling. • These options are available for this command: • **limit**--Maximum number of connections that can be made to this IP address. • **priority**--Priority for this IP address. **Note** The **priority** keyword is typically not configured on a tunnel switch. Information used for load balancing and failover is configured on a remote authentication, authorization, and accounting (AAA) server instead. For configuration information, see the "Configuring L2TP Tunnel Server Load Balancing and Failover on the NAS Remote RADIUS AAA Server" section in the "Configuring AAA for VPDNs" module. • Multiple tunnel servers can be configured on the tunnel switch by configuring multiple **initiate-to** commands.

Configuration Examples for Multihop VPDN

Example Configuring Multihop VPDN on an MMP Stack Group

The following example configures a stack group and a NAS for dial-in L2F VPDN tunneling with multihop VPDN enabled:

Tunnel Server A Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop VPDN
vpdn multihop
!
!Configure the tunnel server to accept L2F tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2f
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelserverb 10.1.1.2
sgbp member tunnelserverc 10.1.1.3
```

Tunnel Server B Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop VPDN
vpdn multihop
!
!Configure the tunnel server to accept L2F tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2f
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelservera 10.1.1.1
sgbp member tunnelserverc 10.1.1.3
```

Tunnel Server C Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop VPDN
vpdn multihop
!
!Configure the tunnel server to accept L2F tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2f
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelservera 10.1.1.1
sgbp member tunnelserverb 10.1.1.2
```

NAS Configuration

```
!Enable VPDN
vpdn enable
!
!Configure the NAS to initiate L2TP tunnels
vpdn-group group1
 request-dialin
  protocol l2tp
  domain cisco.com
!
!Configure the NAS with the IP address of each tunnel server in the stack group
 initiate-to ip 10.1.1.1
 initiate-to ip 10.1.1.2
 initiate-to ip 10.1.1.3
```

Example Configuring L2TP Redirect

The following example configures a stack group and a NAS for dial-in L2TP VPDN tunneling and enables basic L2TP redirect:

Tunnel Server A Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop to ensure interoperability with devices that are not capable of !performing
 L2TP redirect.
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the tunnel server to accept L2TP tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2tp
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelserverb 10.1.1.2
sgbp member tunnelserverc 10.1.1.3
```

Tunnel Server B Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop to ensure interoperability with devices that are not capable of !performing
 L2TP redirect.
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the tunnel server to accept L2TP tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2tp
  virtual-template 1
  exit
```

```
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelservera 10.1.1.1
sgbp member tunnelserverc 10.1.1.3
```

Tunnel Server C Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop to ensure interoperability with devices that are not capable of !performing
 L2TP redirect.
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the tunnel server to accept L2TP tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2tp
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelservera 10.1.1.1
sgbp member tunnelserverb 10.1.1.2
```

NAS Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop VPDN
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the NAS to initiate L2TP tunnels
vpdn-group group1
 request-dialin
  protocol l2tp
  domain cisco.com
!
!Configure the NAS with the IP address of each tunnel server in the stack group
 initiate-to ip 10.1.1.1
 initiate-to ip 10.1.1.2
 initiate-to ip 10.1.1.3
```

Example Configuring L2TP Redirect with a Redirect Identifier

The following example configures the NAS and stack group tunnel servers for L2TP redirect using a redirect identifier:

Tunnel Server A Configuration

```
!Enable VPDN
```

```
vpdn enable
!
!Enable multihop to ensure interoperability with devices that are not capable of !performing
 L2TP redirect.
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the tunnel server to accept L2TP tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2tp
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelserverb 10.1.1.2
sgbp member tunnelserverc 10.1.1.3
!
!Configure the redirect identifier
vpdn redirect identifier stack1
```

Tunnel Server B Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop to ensure interoperability with devices that are not capable of !performing
 L2TP redirect.
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the tunnel server to accept L2TP tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2tp
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelservera 10.1.1.1
sgbp member tunnelserverc 10.1.1.3
!
!Configure the redirect identifier
vpdn redirect identifier stack1
```

Tunnel Server C Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop to ensure interoperability with devices that are not capable of !performing
 L2TP redirect.
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the tunnel server to accept L2TP tunnels from the NAS
vpdn-group group1
```

```
 accept-dialin
  protocol l2tp
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelservera 10.1.1.1
sgbp member tunnelserverb 10.1.1.2
!
!Configure the redirect identifier
vpdn redirect identifier stack1
```

NAS Configuration

```
!Enable VPDN
vpdn enable
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the NAS to initiate L2TP tunnels
vpdn-group group1
 request-dialin
  protocol l2tp
  domain cisco.com
!
!Configure the NAS with the redirect identifier
 redirect identifier stack1
```

Example Configuring Redirect Identifiers on the RADIUS Server

The following example shows the RADIUS server profile configured with three unique redirect identifiers for stack group members with unique authentication requirements. Each stack group member must be configured with the corresponding unique redirect identifier. When the NAS receives a redirect request containing the redirect identifier of the owner of the call, it can look up the proper authentication information in the RADIUS profile associated with that redirect identifier.

```
cisco.com Password = "cisco"
       Tunnel-Type = :0:L2TP,
       Tunnel-Medium-Type = :0:IP,
       Tunnel-Server-Endpoint = :0:"10.1.1.1",
       Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=ts1",
       Tunnel-Type = :1:L2TP,
       Tunnel-Medium-Type = :1:IP,
       Tunnel-Server-Endpoint = :1:"10.1.1.2",
       Cisco:Cisco-Avpair = :1:"vpdn:vpdn-redirect-id=ts2"
       Tunnel-Type = :2:L2TP,
       Tunnel-Medium-Type = :1:IP,
       Tunnel-Server-Endpoint = :1:"10.1.1.3",
       Cisco:Cisco-Avpair = :1:"vpdn:vpdn-redirect-id=ts3"
```

Example Configuring the Redirect Source on a Stack Group Tunnel Server

The following example configures one member of a stack group to accept dial-in L2TP VPDN tunnels and enables L2TP redirect using a redirect source IP address:

```
!Enable VPDN
vpdn enable
```

```
!
!Enable multihop to ensure interoperability with devices that are not capable of !performing
 L2TP redirect.
vpdn multihop
!
!Enable L2TP redirect
vpdn redirect
!
!Configure the tunnel server to accept L2TP tunnels
vpdn-group group1
 accept-dialin
  protocol l2tp
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group stack1
sgbp member tunnelserverb 10.1.1.2
sgbp member tunnelserverc 10.1.1.3
!
!Configure the redirect source
vpdn redirect source 172.23.1.1
```

Example Configuring Multihop VPDN Tunnel Switching

The following example configures a NAS, tunnel switch, and tunnel server to establish a multihop VPDN tunnel using L2TP:

NAS Configuration

```
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel switch
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
!
 initiate-to ip 172.22.66.25
 local name ISP-NAS
```

Tunnel Switch Configuration

```
!Enable VPDN
vpdn enable
!
!Enable multihop
vpdn multihop

!

! Configure the tunnel switch to use the multihop hostname in the authentication search.

 vpdn search-order multihop-hostname domain dnis

!

! Configure the tunnel switch to accept dial-in sessions from the NAS
vpdn-group tunnelin
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-NAS
 local name ISP-Sw
!
```

```
! Configure the tunnel switch to initiate VPDN dial-in sessions to the tunnel server
vpdn-group tunnelout
 request-dialin
  protocol l2tp
  multihop-hostname ISP-NAS
!
 initiate-to ip 10.2.2.2
 local name ISP-Sw
```

Tunnel Server Configuration

```
! Configure the tunnel server to accept dial-in sessions from the NAS
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-Sw
 local name ENT-TS
```

Where to Go Next

You can perform any of the relevant optional tasks in the Configuring Additional VPDN Features and in the VPDN Tunnel Management modules.

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*
VPDN technology overview	VPDN Technology Overview module
Information about Multichassis Multilink PPP	Implementing Multichassis Multilink PPP module
Information about virtual templates	Configuring Virtual Template Interfaces module
Dial Technologies commands	*Cisco IOS Dial Technologies Command Reference*
Information about SSS	Configuring a Cisco Subscriber Service Switch Policy module
Broadband access aggregation and DSL command: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	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 2341	Cisco Layer Two Forwarding (Protocol) L2F
RFC 2661	*Layer Two Tunneling Protocol L2TP*

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 Multihop VPDN

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 . An account on Cisco.com is not required.

Table 1: Feature Information for Multihop VPDN

Feature Name	Software Releases	Feature Configuration Information
L2TP Redirect	12.2(13)T	This feature allows a tunnel server participating in SGBP to send a redirect message to the NAS if another stack group member wins the SGBP bid. The NAS will then reinitiate the call to the newly redirected tunnel server. The following commands were introduced by this feature: **clear vpdn redirect**, **show vpdn redirect**, **vpdn redirect**, **vpdn redirect attempts**, **vpdn redirect identifier**, **vpdn redirect source**.
Subscriber Service Switch	12.2(13)T	This feature provides flexibility on where and how many subscribers are connected to available services and how those services are defined. The primary focus of SSS is to direct PPP from one point to another using a Layer 2 subscriber policy. The policy will manage tunneling of PPP in a policy-based bridging fashion. The following VPDN commands were introduced or modified by this feature: **multihop-hostname**, **vpdn search-order**.
VPDN Multihop by DNIS	12.2(13)T	This feature allows DNIS-based multihop capability for VPDNs. The following commands were introduced or modified by this feature: **vpdn multihop**, **vpdn search-order**.