L2TP Redirect

The L2TP Redirect feature allows an L2TP network server (LNS) participating in Stack Group Bidding Protocol (SGBP) to send a redirect message to the L2TP access concentrator (LAC) if another LNS wins the bid. The LAC will then reinitiate the call to the newly redirected LNS. The feature provides two purposes:

- Allows the user to have more evenly load-balanced sessions among a stack of LNSs
- For multilink calls over Layer 2 Tunneling Protocol (L2TP), eliminates the need for multiple hops

Feature Specifications for L2TP Redirect

Feature History	
Release	**Modification**
12.2(13)T	This feature was introduced.
12.2(15)B	This feature was integrated into Cisco IOS Release 12.2(15)BT.
Supported Platforms	
This feature is supported on all platforms, including the Cisco 800 series, Cisco 1400 series, Cisco 1600 series, Cisco 1600R series, Cisco 1700 series, Cisco 2400 series, Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, Cisco 7400 series, Cisco 7500 series, Cisco AS5300, Cisco AS5400, Cisco AS5800, Cisco IGX 8400 series, Cisco MC3810, Cisco uBR7200 series.	

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

Contents

Prerequisites for L2TP Redirect

The LAC and the LNS must be Cisco equipment.

Restrictions for L2TP Redirect

The L2TP Redirect feature does not extend redirect capability to regular non-SGBP multihop cases.

This feature can redirect only L2TP calls.

Information About L2TP Redirect

To configure the L2TP Redirect feature, you must to understand the following concepts:

Benefits of L2TP Redirect

The L2TP Redirect feature is an enhancement to L2TP. L2TP is an extension of PPP, which is an important component of Virtual Private Networks (VPNs).

When a network is running Multilink PPP (MLP), subsequent calls to add bandwidth could come in to an LNS that is different from the LNS that terminates the first link (that is, the bundle master). The LNS routers in the stack group use the SGBP to deliver all the links to a single box.

This Multichassis Multilink PPP (MMP) architecture does not scale beyond a few routers per LNS stack and inherently adds hop and latency variations between bonded channels.

Benefits of this feature include the following:

- Increased scalability because the need for multiple hops is eliminated and sessions between the LNSs are effectively load-balanced
- Increased number of calls that can be entered in to a stack group because the LNSs need not act as virtual private dialup network (VPDN) multihop nodes and perform multihop tasks
- Smoother traffic with increased throughput because the L2TP Redirect feature eliminates the need for multiple hops and therefore allows links in a multilink bundle to have the same delay and latency

The L2TP Redirect feature can also be used to distribute sessions in a stack of LNSs (load balancing). You can have a primary contact LNS that all the LACs point to for a particular domain. This primary contact LNS would have SGBP configured and the **sgbp ppp-forward** command configured to force it to issue a mastership query to the SGBP group for every PPP link. The rest of the LNSs would bid for each link that came in, and the number of bids of each LNS would decrease for every session that was added to the LNS. The managing of bids in this manner would result in a perfectly even load distribution of sessions among a stack of LNSs. The primary contact LNS may not actually terminate any sessions; it may simply issue the mastership query, collects the bids, choose the highest one, and redirect the originating LAC to that LNS.

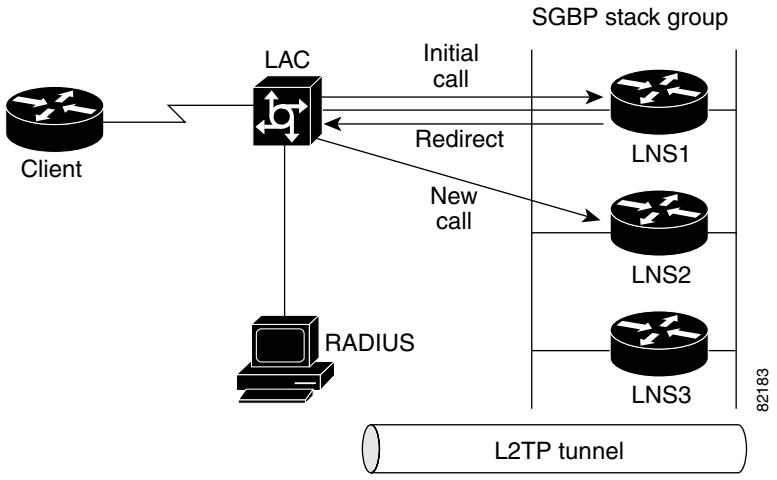
If you are not familiar with the protocols mentioned in this section, see the "Additional References" section on page 20 for more information.

Feature Design of L2TP Redirect

Figure 1 shows how the L2TP Redirect feature redirects a multilink call that comes in to LNS1 from the LAC. The LAC has been configured for redirecting and includes the vendor-specific attribute-value pair (AVP) in the L2TP Incoming-Call-Request (ICRQ) control message. This AVP will inform LNS1 that the LAC is configured for the L2TP Redirect feature and can redirect the call. Only the presence of this AVP will allow LNS1 to drop and redirect the call. If this AVP is missing, then LNS1 will not drop the call and will instead do SGBP forwarding using multihop technology as usual. In this manner, interoperability with non-Cisco equipment is maintained. LNS1 initiates SGBP bidding. LNS2 wins the bid because it owns the master bundle. LNS1 and LNS2 are both configured for redirecting, so LNS1 sends an L2TP Call-Disconnect-Notify (CDN) message to the LAC, telling it to disconnect and redirect the call. This CDN message also includes the redirect IP address of LNS2. The LAC brings down the call to LNS1 and initiates a new call to LNS2. LNS2 realizes that it is the bundle master and therefore terminates the call.

With redirection enabled, load balancing is now being done by the SGBP stack group LNSs instead of the LAC, resulting in a perfectly even load distribution of sessions among the stack of LNSs.

Figure 1 L2TP Redirect



RADIUS Server Configuration for L2TP Redirect

The user has the option to configure the L2TP Redirect feature on a RADIUS server, so that if there are multiple LACs, the RADIUS server automatically updates the configurations of the LACs. The user will be offered the choice of configuring the RADIUS server where applicable in this feature.

How to Configure L2TP Redirect

This section contains the configuration procedures described inthe following sections. Each procedure is identified as either required or optional. Where procedures are documented for the LNS, they will need to be performed for each LNS in the SGBP stack group, unless otherwise noted.

Note The user has the option to configure the L2TP Redirect feature on a RADIUS server, so that if there are multiple LACs, the RADIUS server automatically updates the configurations of the LACs. The user will be offered the choice of configuring the RADIUS server where applicable in this feature.

- Configure L2TP on the LAC and LNS, page 4 (required)
- Configure SGBP on LNS1 and LNS2, page 10 (required)
- Enable and Verify L2TP Redirect on the LAC and LNS, page 11 (required)
- Configure Additional L2TP Redirect Functions, page 14 (optional)

Configure L2TP on the LAC and LNS

To configure L2TP on the LAC and the LNS, perform the tasks described in the following sections:

- Configure L2TP on the LAC, page 5 (required)

- Configure L2TP on the RADIUS Server as an Alternative to Configuring Multiple LACs, page 6 (required)
- Configure L2TP on the LNS, page 7 (required)
- Verify that L2TP Is Running, page 8 (required)

Configure L2TP on the LAC

This section provides the steps necessary to configure L2TP on the LAC.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **vpdn enable**
4. **vpdn-group** *name*
5. **request-dialin**
6. **protocol** {**l2f** | **l2tp** | **pppoe** | **any**}
7. **exit**
8. **domain** *domain-name*
9. **initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables a VPDN and enters VPDN group configuration mode.
Step 4	**vpdn-group** *name* **Example:** `Router(config-vpdn)# vpdn-group 1`	Associates a VPDN group to a customer or VPDN profile.

	Command or Action	Purpose
Step 5	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	Configures a LAC to request Layer 2 Forwarding (L2F) or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or dialed number identification service (DNIS), and enters VPDN request-dialin group configuration mode.
Step 6	**protocol** {**l2f** | **l2tp** | **pppoe** | **any**} **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the L2TP that the VPDN subgroup will use. • Configures L2TP as the tunnel protocol.
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Returns to VPDN group configuration mode.
Step 8	**domain** *domain-name* **Example:** `Router#(config-vpdn)# domain l2tp.com`	Requests that PPP calls from a specific domain name be tunneled, and supports additional domain names for a specific VPDN group.
Step 9	**initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*] **Example:** `Router(config-vpdn)# initiate-to ip 10.1.1.2`	Specifies the IP address that will be tunneled to.
Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits any configuration mode or closes an active terminal session.

Configure L2TP on the RADIUS Server as an Alternative to Configuring Multiple LACs

If your network configuration has multiple LACS, you can configure the RADIUS server rather than configure each LAC separately. To configure L2TP on the RADIUS server, update the RADIUS user profile as shown in Step 1.

SUMMARY STEPS

1. Update the RADIUS profile.

DETAILED STEPS

	Command or Action	Purpose

Step 1	Update the RADIUS profile.
	
	Example:
	`l2tp.com Password = "cisco"`
	`Tunnel-Type = :0:L2TP,`
	`Tunnel-Medium-Type = :0:IP,`
	`Tunnel-Server-Endpoint = :0:"10.0.0.54",`
	`Tunnel-Type = :1:L2TP,`
	`Tunnel-Medium-Type = :1:IP,`
	`Tunnel-Server-Endpoint = :1:"10.9.9.9",`
		Enables L2TP on the RADIUS profile.
		• To avoid having to configure multiple LACs, update the RADIUS profile so that the RADIUS server automatically updates the configurations of the multiple LACs.
		• Refer to your vendor-specific RADIUS configuration documentation for specific instructions on updating the RADIUS profile.

Configure L2TP on the LNS

This section provides the steps necessary to configure L2TP on the LNS.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **vpdn enable**
4. **vpdn multihop**
5. **vpdn-group** *name*
6. **accept-dialin**
7. **protocol** {**l2f** | **l2tp** | **pppoe** | **any**}
8. **virtual-template** *template-number*
9. **exit**
10. **terminate-from hostname** *host-name*
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables a VPDN and enters VPDN group configuration mode.
Step 4	**vpdn multihop** **Example:** `Router# vpdn multihop`	Enables a multihop VPDN.
Step 5	**vpdn-group** *name* **Example:** `Router(config-vpdn)# vpdn-group 1`	Associates a VPDN group to a customer or VPDN profile.
Step 6	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures an LNS to accept tunneled PPP connections from a LAC, creates an accept-dialin VPDN subgroup, and enters VPDN accept-dialin group configuration mode.
Step 7	**protocol** {**l2f** | **l2tp** | **pppoe** | **any**} **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the L2TP that the VPDN subgroup will use. • Configures L2TP as the tunnel protocol.
Step 8	**virtual-template** *template-number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 9	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Returns to VPDN group configuration mode.
Step 10	**terminate-from hostname** *host-name* **Example:** `Router(config-vpdn)# terminate-from hostname dk7200`	Establishes a username-based authentication system, such as PPP Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
Step 11	**exit** **Example:** `Router(config-vpdn)# exit`	Exits any configuration mode or closes an active terminal session.

Verify that L2TP Is Running

This section provides the steps necessary to verify that L2TP is running.

SUMMARY STEPS

1. Attempt to bring up an L2TP call.

2. **enable**
3. **show vpdn**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Attempt to bring up an L2TP call.	—
Step 2	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 3	**show vpdn** **Example:** `Router# show vpdn`	Displays information about active L2F protocol tunnel and L2F message identifiers in a VPDN. • To verify that L2TP is configured on the LAC, use this command on both the LAC and the LNS.

In the following example, the **show vpdn** command was entered after an MLP call was made from the client. The command output displays L2TP tunnel and session information.

```
userid03# show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID   RemID   Remote Name   State   Remote Address   Port   Sessions   VPDN Group
39204   32587   userid02    est     172.18.184.230   1701   1          1
LocID   RemID   TunID   Intf   Username             State   Last Chg   Uniq ID
2       13      39204   Vi3    userid01@l2tp.com  est     00:00:14   1
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
```

Table 1 describes the significant fields shown in the display.

Table 1 show vpdn Field Descriptions

Field	Description
LocID	Local tunnel and session ID.
RemID	Remote tunnel and session ID.
Remote Name	Name of the remote L2TP peer.
State	State of the tunnel and session.
Remote Address	IP address of the remote L2TP peer.
Port	User Datagram Protocol (UDP) port number used for L2TP.
Sessions	Number of sessions in the tunnel.
VPDN Group	The VPDN group used for the specified tunnel.
LocID	Local tunnel and session ID.
RemID	Remote tunnel and session ID.
TunID	Local tunnel ID to which the specified session belongs.

Table 1 show vpdn Field Descriptions (continued)

Field	Description
Intf	Interface on which the specified session is terminated.
Username	Name of the incoming user.
State	State of the tunnel and session.
Last Chg	Time (in hours:minutes:seconds) since the specified session has been in the current state.

Configure SGBP on LNS1 and LNS2

This section provides the steps necessary to configure SGBP on LNS1 and LNS2.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **sgbp group** *name*
4. **sgbp member** *peer-name* [*peer-ip-address*]
5. **sgbp ppp-forward**
6. **show sgbp**

Note Repeat these steps for LNS2.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enters higher privilege levels, such as privileged EXEC mode.
	Example: `Router> enable`	Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**}	Enters global configuration mode.
	Example: `Router# configure terminal`	
Step 3	**sgbp group** *name*	Defines a named stack group and makes this router a member of that stack group.
	Example: `Router(config)# sgbp group group1`	
Step 4	**sgbp member** *peer-name* [*peer-ip-address*]	Specifies the host name and IP address of a router or access server that is a peer member of a stack group.
	Example: `Router(config)# sgbp member dk3640 10.1.1.3`	

	Command or Action	Purpose
Step 5	**sgbp ppp-forward** **Example:** `Router(config)# sgbp ppp-forward`	Enables forwarding of PPP calls—in addition to MLP calls—to the winner of the SGBP bid.
Step 6	**show sgbp** **Example:** `Router# show sgbp`	Displays the status of the stack group members.

Enable and Verify L2TP Redirect on the LAC and LNS

To enable and verify the L2TP Redirect feature on the LAC and the LNS, perform the tasks described in the following sections:

- Enable the L2TP Redirect Feature on the LAC, page 11 (required)
- Enable the L2TP Redirect Feature on the LNS, page 12 (required)
- Set the SGBP Seed Bid on LNS2, page 12 (required)
- Verify the L2TP Redirect Feature, page 13 (required)

Enable the L2TP Redirect Feature on the LAC

This section provides the steps necessary to enable the L2TP Redirect feature on the LAC.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **vpdn redirect**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn redirect** **Example:** `Router(config)# vpdn redirect`	Enables L2TP redirect functionality. • Enables L2TP redirect functionality on the LAC.

Enable the L2TP Redirect Feature on the LNS

This section provides the steps necessary to enable the L2TP Redirect feature on the LNS.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **vpdn redirect**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn redirect** **Example:** `Router(config)# vpdn redirect`	Enables L2TP redirect functionality. • Enables L2TP redirect functionality on the LNS.

Set the SGBP Seed Bid on LNS2

This section provides the steps necessary to set the SGBP seed-big on LNS2.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **sgpb seed-bid** {**default** | **offload** | **forward-only** | **bid**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sgbp seed-bid** {**default** | **offload** | **forward-only** | **bid**} **Example:** `Router(config)# sgbp seed-bid offload`	Sets the bidding level that a stack group member can be used to bid for a bundle. • Sets the seed-bid on LNS2 so that it wins the bid and receives the redirected call.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits any configuration mode or closes an active terminal session.

Verify the L2TP Redirect Feature

This section provides the steps necessary to verify the L2TP Redirect feature.

SUMMARY STEPS

1. Make a call from the client.
2. **enable**
3. **show vpdn**
4. **show vpdn redirect**
5. **clear vpdn redirect**

DETAILED STEPS

	Command or Action	Purpose
Step 1	`Make a call from the client.`	Verifies if the call terminates on LNS2 and therefore if the L2TP Redirect feature is enabled.
Step 2	**`enable`** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 3	**`show vpdn`** **Example:** `Router# show vpdn`	Displays information about active L2F protocol tunnel and L2F message identifiers in a VPDN. • Verifies if the LAC redirected the L2TP call.
Step 4	**`show vpdn redirect`** **Example:** `Router# show vpdn redirect`	Displays statistics for L2TP call redirects and forwards. • Verifies that LNS1 shows a “Redirected” call notification.
Step 5	**`clear vpdn redirect`** **Example:** `Router# clear vpdn redirect`	(Optional) Clears the counters for the **vpdn show** commands.

Configure Additional L2TP Redirect Functions

Two optional configuration tasks are described in the following sections:

- Configure the Redirect Identifier, page 14 (optional)
- Configure Redirect Source, page 18 (optional)

Configure the Redirect Identifier

To configure a redirect identifier, perform the tasks described in the following sections:

- Configure the Redirect Identifier on the LAC, page 14 (optional)
- Configure the Redirect Identifier on the RADIUS Server as an Alternative to Configuring Multiple LACs, page 16 (optional)
- Configure the Redirect Identifier on the LNS, page 17 (optional)

Note You are not required to configure a redirect identifier in order to do redirects. If the redirect identifier is not configured, the LAC uses the new received redirect IP address in order to get authorization information to redirect the call. In this instance of the use of the IP address for authorization, the IP address of the new redirected LNS must be present in the vpdn-group, initiate-to configuration.

Configure the Redirect Identifier on the LAC

This section provides the steps necessary to configure the redirect identifier on the LAC.

Note To configure the redirect identifier on the LAC, you must enter the **redirect identifier** command within the VPDN group configuration of the LAC.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **vpdn enable**
4. **vpdn-group** *name*
5. **redirect identifier** *identifier-name*
6. **request-dialin**
7. **protocol** {**l2f** | **l2tp** | **pppoe** | **any**}
8. **exit**
9. **domain** *domain-name*
10. **initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables a VPDN.
Step 4	**vpdn-group** *name* **Example:** `Router(config-vpdn)# vpdn-group 1`	Associates a VPDN group to a customer or VPDN profile.
Step 5	**redirect identifier** *identifier-name* **Example:** `Router(config)# redirect identifier stack1`	Indicates the name of the redirect identifier to use for L2TP call redirection. • If a user adds LNSs, the LAC need not be updated each time. The redirect identifier can be configured locally or via RADIUS.

	Command or Action	Purpose
Step 6	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	Configures a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, and specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or DNIS.
Step 7	**protocol** {**l2f** | **l2tp** | **pppoe** | **any**} **Example:** `Router(config-vpdn-subgroup)# protocol l2tp`	Specifies the L2TP that the VPDN subgroup will use. • Configures L2TP as the tunnel protocol.
Step 8	**exit** **Example:** `Router(config-vpdn-subgroup)# exit`	Returns to VPDN group configuration mode.
Step 9	**domain** *domain-name* **Example:** `Router(config-vpdn)# domain l2tp.com`	Requests that PPP calls from a specific domain name be tunneled, and supports additional domain names for a specific VPDN group.
Step 10	**initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*] **Example:** `Router(config-vpdn)# initiate-to ip 10.1.1.2`	Specifies the IP address that will be tunneled to.
Step 11	**exit** **Example:** `Router(config-vpdn)# exit`	Exits any configuration mode or closes an active terminal session.

Configure the Redirect Identifier on the RADIUS Server as an Alternative to Configuring Multiple LACs

This section provides the steps to configure the redirect identifier on the RADIUS server, using a Cisco-specific tagged attribute.

SUMMARY STEPS

1. Update the RADIUS profile.

DETAILED STEPS

	Command or Action	Purpose

Step 1	Update the RADIUS profile.
	
	Example:
	`l2tp.com Password = "cisco"`
	`Tunnel-Type = :0:L2TP,`
	`Tunnel-Medium-Type = :0:IP,`
	`Tunnel-Server-Endpoint = :0:"10.0.0.54",`
	`! Cisco:Cisco-Avpair =`
	`:0:"vpdn:vpdn-redirect-id=idforLNS1",`
		Configures the redirect identifier on the RADIUS profile.
		• To avoid having to configure multiple LACs, update the RADIUS profile so that the RADIUS server automatically updates the configurations of the multiple LACs.
		• Refer to your vendor-specific RADIUS configuration documentation for specific instructions on updating the RADIUS profile.

Configure the Redirect Identifier on the LNS

This section provides the steps necessary to configure the redirect identifier on the LNS.

Note To configure the redirect identifier on the LNS, you must enter the **vpdn redirect identifier** command for each LNS on the stack group.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **vpdn redirect identifier** *identifier-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn redirect identifier** *identifier-name* **Example:** `Router(config)# vpdn redirect identifier idname`	Indicates the name of the redirect identifier to use for L2TP call redirection. • If a user adds LNSs, the LAC need not be updated each time. The redirect identifier can be configured locally or via RADIUS.

Configure Redirect Source

This section provides the steps necessary to configure the redirect source on the LNS.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **vpdn redirect source** *redirect-ip-address-of-LNS*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn redirect source** *redirect-ip-address-of-LNS* **Example:** `Router(config)# vpdn redirect source 10.1.1.2`	Allows a user to specify an IP address on the LNS that is reachable from the LAC. • Bidding could be a private IP address. If the LNS has multiple IP addresses, the user can select a public one that is reachable by the LAC. For instance, SGBP bidding can be on a private site, and the LAC can only reach a public address. **Note** If the **vpdn redirect source** command is not configured, the IP address used for SGBP bidding will be used as the redirect address. **Note** On the LAC, this command will have no significance.

Configuration Examples for L2TP Redirect

Configure L2TP Redirect on the LAC and SGBP Stack Group LNSs Example

The following example shows the L2TP Redirect feature configuration on the LAC and on LNS1 and LNS2 of the SGBP stack group:

LAC: (dk7200)

```
vpdn enable
vpdn redirect
!
!
vpdn-group 1
 request-dialin
 protocol l2tp
 domain l2tp.com
 initiate-to ip 10.1.1.2
!
!
```

LNS1: (dk7200_2)

```
username teststack password 0 lab
!
sgbp group teststack
sgbp member dk3640 10.1.1.3
sgbp ppp-forward
vpdn enable
vpdn multihop
vpdn redirect
!
vpdn-group 1
 accept-dialin
 protocol any
 virtual-template 1
 terminate-from hostname dk7200
!
```

LNS2: (dk3640)

```
!
username teststack password 0 lab
!
sgbp group teststack
sgbp seed-bid 9000
sgbp member dk7200_2 10.1.1.2
sgbp ppp-forward
vpdn enable
vpdn multihop
vpdn redirect
!
vpdn-group 1
 accept-dialin
 protocol any
 virtual-template 1
 terminate-from hostname dk7200
```

Configure L2TP Redirect via RADIUS on the LAC Example

The following example shows the RADIUS server profile configured for the L2TP Redirect feature:

```
l2tp.com Password = "cisco"
       Tunnel-Type = :0:L2TP,
       Tunnel-Medium-Type = :0:IP,
       Tunnel-Server-Endpoint = :0:"10.0.0.54",
       Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=idforLNS1",
Tunnel-Type = :1:L2TP,
       Tunnel-Medium-Type = :1:IP,
       Tunnel-Server-Endpoint = :1:"10.9.9.9",
       Cisco:Cisco-Avpair = :1:"vpdn:vpdn-redirect-id=idforLNS2"
```

Additional References

For additional information related to L2TP Redirect, refer to the following references:

Related Documents

Related Topic	Document Title
L2TP	*Layer 2 Tunnel Protocol Technology Brief* http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm
Configuring PPP, MLP, MMP, and SGBP	"PPP Configuration" chapter in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.
PPP commands: complete syntax, command mode, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*, Release 12.2.
RADIUS configuration tasks	"Configuring RADIUS" chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2.
RADIUS configuration commands: complete syntax, command mode, usage guidelines, and examples	*Cisco IOS Security Command Reference*, Release 12.2.

Standards

Standards	Title
None	—

MIBs

MIBs[1]	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **clear vpdn redirect**
- **show vpdn redirect**
- **vpdn redirect**
- **vpdn redirect attempts**
- **vpdn redirect identifier**
- **vpdn redirect source**

clear vpdn redirect

To clear the redirect counters shown in the **show vpdn redirect** command output, use the **clear vpdn redirect** command in privileged EXEC mode.

clear vpdn redirect

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Clear the previous display statistics regarding redirects and forwards before entering the **show vpdn redirect** command again.

Examples

The following example clears the redirect counters from a previously entered **show vpdn redirect** command:

```
Router# clear vpdn redirect
```

Related Commands

Command	Description
show vpdn redirect	Displays statistics for L2TP call redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the LAC.
vpdn redirect identifier	Indicates the name of the VPDN redirect identifier to use for L2TP call redirection.
vpdn redirect source	Configures the public redirect IP address of an LNS.

show vpdn redirect

To display statistics for redirects and forwards, use the **show vpdn redirect** command in privileged EXEC mode.

show vpdn redirect

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Statistics about the number of Layer 2 Tunneling Protocol (L2TP) forwards and redirects that were done by the L2TP network server (LNS) are maintained and displayed when you enter the **show vpdn redirect** command. To clear the redirect counters of the statistics, use the **clear vpdn redirect** command.

Examples

The following example displays statistics for redirects and forwards for a LAC:

```
Router# show vpdn redirect

'vpdn redirection enabled'
'sessions redirected as access concentrator: 2'
'sessions redirected as network server: 0'
'sessions forwarded: 2'
```

Table 2 describes the significant fields shown in the display.

Table 2 show vpdn redirect Field Descriptions

Field	Description
vpdn redirection enabled	Verifies that the L2TP Redirect feature is enabled.
sessions redirected as access concentrator	Displays the number of sessions that the L2TP access concentrator (LAC) has redirected.
sessions redirected as network server	Displays the number of sessions that the LNS has redirected.
sessions forwarded	Displays the total number of sessions that have been forwarded.

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the LAC.
vpdn redirect identifier	Indicates the name of the VPDN redirect identifier to use for L2TP call redirection.
vpdn redirect source	Configures the public redirect IP address of an LNS.

vpdn redirect

To enable Layer 2 Tunneling Protocol (L2TP) redirect functionality, use the **vpdn redirect** command in global configuration mode. To disable L2TP redirect functionality, use the **no** form of this command.

vpdn redirect

no vpdn redirect

Syntax Description

This command has no arguments or keywords.

Defaults

L2TP redirect functionality is disabled so that current multihop forwarding behavior is preserved.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Configuring this command on the L2TP access concentrator (LAC) enables the LAC to perform the L2TP redirect by sending a new vendor-specific vendor-specific attribute-value pair (AVP) to the L2TP network server (LNS). Configuring this command on the LNS allows the LNS to redirect a call by disconnecting it and requesting the LAC to redirect it. The Stack Group Bidding Protocol (SGBP) stack group LNSs must have this command enabled in order to receive redirected calls, or else they will receive calls only through the usual multihop forwarding from the LNS that first took the call.

Examples

The following example enables the L2TP Redirect feature on the LAC:

```
Router(config)# vpdn redirect
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP call redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the LAC.
vpdn redirect identifier	Indicates the name of the VPDN redirect identifier to use for L2TP call redirection.

vpdn redirect attempts

To restrict the number of redirect attempts possible for a given Layer 2 Tunneling Protocol (L2TP) call on the L2TP access concentrator (LAC), use the **vpdn redirect attempts** command in global configuration mode. To revert to the default of three redirect attempts, use the **no** form of this command.

vpdn redirect attempts *number-of-attempts*

no vpdn redirect attempts *number-of-attempts*

Syntax Description

number-of-attempts	Number of redirect attempts in a range from 1 to 20.

Defaults

Three redirect attempts

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Note that the number of redirect attempts is by default always restricted to three, even if this command is not explicitly configured. The only use of this command is to configure a redirect attempts value other than the default (which is always in effect).

Examples

The following example configures four redirect attempts:

```
Router(config)# vpdn redirect attempts 4
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP call redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect identifier	Indicates the name of the VPDN redirect identifier to use for L2TP call redirection.
vpdn redirect source	Configures the public redirect IP address of an LNS.

vpdn redirect identifier

To indicate the name of the virtual private dialup network (VPDN) redirect identifier to use for Layer 2 Tunneling Protocol (L2TP) call redirection, use the **vpdn redirect identifier** command in global configuration mode. To remove the name of the redirect identifier from the L2TP network server (LNS) of the stack group, use the **no** form of this command.

vpdn redirect identifier *identifier-name*

no vpdn redirect identifier *identifier-name*

Syntax Description

identifier-name	Name of the redirect identifier to use for call redirection.

Defaults

No identifier name is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The **vpdn redirect identifier** command is configured on the L2TP access concentrator (LAC) and the stack group LNSs. The LAC compares this identifier with the one received from the stack group LNS to determine authorization information to redirect the call.

Note that configuring the redirect identifiers is not necessary in order to do redirects. If not configured, the LAC uses the new received redirect IP address in order to get authorization information to redirect the call. In that case, the IP address of the new redirected LNS must be present in the vpdn-group, initiate-to <addresses> configuration of the LAC.

The redirect identifier allows new stack group members to be added without the need to update the LAC configuration with their IP addresses (which would be needed for redirect authorization). Now, you can add a new stack group member and give it the same redirect identifier as the rest of the stack group. The LAC configuration then need not be updated. Note that if the authorization information for getting to the new redirected LNS is different, then you will need to configure the authorization information via RADIUS using tagged attributes Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=<identifier name>". Then the LAC will choose the correct tagged parameters to get authorization information for the new redirected LNS by first trying to match the redirect identifier (if present) or else by matching the Tunnel-Server-Endpoint IP address.

Examples

The following example configures the redirect identifier for LNS1:

```
Router(config)# vpdn redirect identifier LNS1
```

The following example configures the RADIUS server with the redirect identifier for LNS1:

```
Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=idforLNS1"
```

The following example configures the redirect identifier on the LAC:

```
Router(config-vpdn)# vpdn-group 1
.
.
.
redirect identifier lns1
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP call redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the LAC.
vpdn redirect source	Configures the public redirect IP address of an LNS.

vpdn redirect source

To configure the public redirect IP address of an L2TP network server (LNS), use the **vpdn redirect source** command in global configuration mode. To remove the public redirect IP address of an LNS, use the **no** form of this command.

vpdn redirect source *redirect-ip-address*

no vpdn redirect source *redirect-ip-address*

Syntax Description

redirect-IP-address	Public redirect IP address for an LNS.

Defaults

If the **vpdn redirect source** command is not configured, then the IP address used for Stack Group Bidding Protocol (SGBP) bidding itself will be used as the redirect address (the public redirect address is then omitted in the bid response).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

On the LAC, this command will have no significance.

Examples

The following example configures a public IP address as a redirect source:

```
Router(config)# vpdn redirect source 255.255.1.1
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP call redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the LAC.
vpdn redirect identifier	Indicates the name of the VPDN redirect identifier to use for L2TP call redirection.

Glossary

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.

AVP—attribute-value pairs (AVPs). Each AVP consists of a type identifier associated with one or more assignable values. AVPs specified in user and group profiles define the authentication and authorization characteristics for their respective users and groups. TACACS+ and RADIUS implement an array of AVPs, each with separate type definitions and characteristics.

CDN—Call-Disconnect-Notify message

CHAP—Challenge Handshake Authentication Protocol

DNIS—dialed number identification service. Feature of trunk lines where the called number is identified; this called number information is used to route the call to the appropriate service. DNIS is a service used with toll-free dedicated services whereby calls placed to specific toll-free numbers are routed to the appropriate area within a company to be answered.

ICRQ—Incoming-Call-Request message. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.

LAC—L2TP access concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with L2TP as defined in this document. The connection from the LAC to the remote system is either local or a PPP link.

LNS—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. Analogous to the Layer 2 Forwarding (L2F) home gateway (HGW).

MMP—Multichassis Multilink PPP. Extends MLP support across multiple routers and access servers. MMP enables multiple routers and access servers to operate as a single, large dialup pool, with a single network address and an ISDN access number. MMP correctly handles packet fragmenting and reassembly when a user connection is split between two physical access devices.

PAP—Password Authentication Protocol. 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 the 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 whether that user is allowed access. PAP is supported only on PPP lines.

SCCRQ—Start-Control-Connection-Request message

SGBP—Stack Group Bidding Protocol (SGBP). Routers or access servers are configured to belong to groups of peers called stack groups. All members of the stack group are peers; stack groups do not need a permanent lead router.

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.

VPDN—virtual private dialup network. Also known as a virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network

connection from a remote user across an ISP network to a private network. VPDNs are a cost-effective method of establishing a long distance, point-to-point connection between remote dial users and a private network.