



# PPP Commands for Wide-Area Networking

---

This chapter describes the commands available to configure the Point-to-Point Protocol (PPP) for wide-area networking on your router.

For information about configuring PPP for wide-area networking, see the *Wide-Area Networking Configuration Guide*.

For PPP configuration on an access server, refer to the “Configuring SLIP and PPP” chapter in the *Access Services Configuration Guide*. For PPP commands for access servers, refer to the “SLIP and PPP Commands” chapter in the *Access Services Command Reference*.

For hardware technical descriptions, and for information about installing the router interfaces, refer to the hardware installation and maintenance publication for your particular product.

## autodetect encapsulation

To enable automatic detection of the encapsulation types in operation over a point-to-point link to a specified serial or ISDN interface, use the **autodetect encapsulation** interface configuration command. To disable automatic, dynamic detection of the encapsulation types in operation on a link, use the **no** form of this command.

**autodetect encapsulation** *encapsulation-type*  
**no autodetect encapsulation**

### Syntax Description

*encapsulation-type*                      One or more of the encapsulation keywords **v120** and **ppp**.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

At least one encapsulation type is required in the command, but you can specify additional encapsulation types.

Use this command to enable the specified serial or ISDN interface to accept calls and dynamically change the encapsulation in effect on the interface when the remote device does not signal the call type. For example, if an ISDN call does not identify the call type in the Lower Layer Compatibility fields and is using an encapsulation that is different from the one configured on the interface, the interface can change its encapsulation type on the fly.

This command enables interoperability with ISDN terminal adapters that use V.120 encapsulation but do not signal V.120 in the call setup message. An ISDN interface that by default answers a call as synchronous serial with PPP encapsulation can change its encapsulation and answer such calls.

Automatic detection is attempted for the first 10 seconds after the link is established or the first five packets exchanged over the link, whichever is first.

### Related Commands

**encapsulation**

## clear vpdn tunnel

To shut down a specified tunnel and all the MIDs within it, use the **clear vpdn tunnel EXEC** command.

**clear vpdn tunnel** *network-access-server gateway-name*

### Syntax Description

<i>network-access-server</i>	Name of the network access server at the far end of the tunnel, probably the point of presence of the public data network or the Internet Service Provider's.
<i>gateway-name</i>	Host name of Home Gateway at the local end of the tunnel.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command is used primarily for troubleshooting. You can use the command to force the tunnel to come down without unconfiguring it (the tunnel could be restarted immediately by a user logging in).

### Example

The following example clears a tunnel between a network access server called orion and a home gateway called sampson:

```
clear vpdn tunnel orion sampson
```

## dialer callback-secure

To enable callback security, use the **dialer callback-secure** interface configuration command.

**dialer callback-secure**

### Syntax Description

This command has no arguments or keywords.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command ensures that the initial call is always disconnected at the receiving end and that the return call is made only if the username is configured for callback. If the username (*hostname* in the **dialer map** command) is not configured for callback, the initial call stays up and no return call is made.

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**dialer callback-server**

**dialer map** †

**map-class** †

**ppp callback accept**

## dialer callback-server

To enable an interface to make return calls when callback is successfully negotiated, use the **dialer callback-server** interface configuration command.

**dialer callback-server [username dialstring]**

### Syntax Description

<b>username</b>	(Optional) Identifies the return call by looking up the authenticated host name in a <b>dialer map</b> command. This is the default.
<b>dialstring</b>	(Optional) Identifies the return call during callback negotiation.

### Default

Disabled. The default keyword is **username**.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**dialer callback-secure**  
**dialer enable-timeout** †  
**dialer hold-queue** †  
**dialer map** †  
**map-class** †  
**ppp callback**

## encapsulation ppp

To set the Point-to-Point Protocol (PPP) as the encapsulation method used by a serial or ISDN interface, use the **encapsulation ppp** interface configuration command.

### **encapsulation ppp**

#### Syntax Description

This command has no keywords or arguments.

#### Default

HDLC on synchronous serial interfaces

#### Command Mode

Interface configuration

#### Usage Guidelines

This command first appeared in a release prior to Cisco IOS Release 10.0.

To use PPP encapsulation, the router must be configured with an IP routing protocol.

#### Example

The following example enables PPP encapsulation on serial interface 0:

```
interface serial 0
encapsulation ppp
```

#### Related Commands

The dagger (†) indicates that the command is documented outside this chapter.

**keepalive** †

**ppp** †

**ppp authentication**





## peer neighbor-route

To reenoble the creation of peer neighbor routes on an interface once this default behavior has been disabled, use the **peer neighbor-route** interface configuration command. To disable the default behavior of creating a neighbor route for the peer on a point-to-point interface, use the **no** form of this command.

**peer neighbor-route**  
**no peer neighbor-route**

### Syntax Description

This command has no keywords and arguments.

### Default

Creation of a route to the peer address on any point-to-point interface when the PPP IPCP negotiation is completed.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Use the **no** form of this command only if the default behavior creates problems in your network environment.

If if you enter this command on a dialer interface or a async-group interface, it affects all member interfaces.

### Example

The following examples reenables the default behavior on an interface.

```
peer neighbor-route
```

## ppp authentication

To specify the order in which the CHAP or PAP protocols are requested on the interface, use the **ppp authentication** interface configuration command. Use the **no** form of the command to disable this authentication.

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed] [list-name | default]  
[callin]  
no ppp authentication
```

### Syntax Description

<b>chap</b>	Enables CHAP on a serial interface.
<b>pap</b>	Enables PAP on a serial interface.
<b>chap pap</b>	Enables both CHAP and PAP, and performs CHAP authentication before PAP.
<b>pap chap</b>	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
<b>if-needed</b>	(Optional) Used with TACACS and XTACACS. Do not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
<i>list-name</i>	(Optional) Used with AAA/TACACS+. Specifies the name of a list of TACACS+ methods of authentication to use. If no list name is specified, the system uses the default. Lists are created with the <b>aaa authentication ppp</b> command.
<b>default</b>	(Optional) Used with AAA/TACACS+. Created with the <b>aaa authentication ppp</b> command.
<b>callin</b>	Specifies authentication on incoming (received) calls only.

### Default

PPP authentication is not enabled.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in a release prior to Cisco IOS Release 11.1.

Once you have enabled CHAP or PAP authentication or both, the local router requires the remote device to prove its identity before allowing data traffic to flow.

- PAP authentication requires the remote device to send a name and password to be checked against a matching entry in the local username database or in the remote TACACS/TACACS+ database.

- CHAP authentication sends a challenge to the remote device. The remote device must encrypt the challenge value with a shared secret and return the encrypted value and its name to the local router in a response message. The local router uses the remote device's name to look up the appropriate secret in the local username or remote TACACS/TACACS+ database. It uses the looked-up secret to encrypt the original challenge and verify that the encrypted values match.

You may enable PAP or CHAP or both, in either order. If both methods are enabled, then the first method specified will be requested during link negotiation. If the peer suggests using the second method or simply refuses the first method, then the second method will be tried. Some remote devices support CHAP only and some PAP only. The order in which you specify the methods will be based on your concerns about the remote device's ability to correctly negotiate the appropriate method as well as your concern about data line security. PAP usernames and passwords are sent as "clear-text" strings and can be intercepted and reused. CHAP has eliminated most of the known security holes.

Enabling or disabling PPP authentication does not affect the local router's willingness to authenticate itself to the remote device.



**Caution** If you use a *list-name* that has not been configured with the **aaa authentication ppp** command, you disable PPP on this line.

### Example

The following example enables CHAP on asynchronous interface 4, and uses the authentication list *MIS-access*:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**aaa authentication ppp** †  
**aaa new-model** †  
**autoselect** †  
**dialer map** †  
**encapsulation ppp**  
**ppp use-tacacs** †  
**username password**

## ppp bridge appletalk

To enable half-bridging of AppleTalk packets across a serial interface, use the **ppp bridge appletalk** interface configuration command.

### **ppp bridge appletalk**

#### Syntax Description

This command has no keywords or arguments.

#### Default

Disabled

#### Command Mode

Interface configuration

#### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

When you configure a serial or ISDN interface for half bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial or ISDN interface converts bridge packets to routed packets and forwards them, as needed.

The serial interface must be configured with an AppleTalk address for communication on the Ethernet subnetwork, and the AppleTalk address must have the same AppleTalk cable range as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging.

No more than one half-bridge should be on any subnetwork.

#### Example

The following example configures serial interface 0 for half-bridging of AppleTalk. The remote bridge and other Ethernet nodes must be on the same network.

```
interface serial 0
ppp bridge appletalk
appletalk cable-range 301-301
appletalk zone remote-lan
```

#### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**appletalk cable-range** †

**appletalk zone** †

**ppp bridge ip**

**ppp bridge ipx**

## ppp bridge ip

To enable half-bridging of IP packets across a serial interface, use the **ppp bridge ip** interface configuration command.

### **ppp bridge ip**

#### Syntax Description

This command has no keywords or arguments.

#### Default

Disabled

#### Command Mode

Interface configuration

#### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

When you configure a serial or ISDN interface for half-bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial interface converts bridge packets to routed packets and forwards them, as needed.

The interface must be configured with an IP address for communication on the Ethernet subnetwork, and the IP address must be on the same subnetwork as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging.

No more than one half-bridge should be on any subnetwork.

#### Example

The following example configures serial interface 0 for half-bridging of IP. The remote bridge and other Ethernet nodes must be on the same subnetwork.

```
interface serial 0
ip address 172.69.5.8
ppp bridge ip
```

#### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**ip address** †

**ppp bridge appletalk**

**ppp bridge ipx**

## ppp bridge ipx

To enable half-bridging of IPX packets across a serial interface, use the **ppp bridge ipx** interface configuration command.

**ppp bridge ipx** [**novell-ether** | **arpa** | **sap** | **snap**]

### Syntax Description

<b>novell-ether</b>	Use Novell's Ethernet_802.3 encapsulation. This is the default.
<b>arpa</b>	Use Novell's Ethernet_II encapsulation.
<b>sap</b>	Use Novell's Ethernet_802.2 encapsulation.
<b>snap</b>	Use Novell Ethernet_Snap encapsulation.

### Default

Default encapsulation is **novell-ether**.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

When you configure a serial interface for half bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial interface converts bridge packets to routed packets and forwards them, as needed.

The serial interface must be configured with an IPX address for communication on the Ethernet subnetwork, and the IPX address must be on the same subnetwork as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging.

No more than one half-bridge should be on any subnetwork.

### Example

The following example configures serial interface 0 for half-bridging of IPX. The remote bridge and other Ethernet nodes must be on the same subnetwork.

```
interface serial 0
  ppp bridge ipx
  ipx network 1800
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

```
ipx network †  
ppp bridge appletalk  
ppp bridge ip
```

## ppp callback

To enable a dialer interface that is not a data terminal ready (DTR) interface to function either as a callback client that requests callback or as a callback server that accepts callback requests, use the **ppp callback** interface configuration command.

```
ppp callback {accept | request}
```

### Syntax Description

<b>accept</b>	Enables this dialer interface to accept PPP callback requests (and function as the PPP callback server).
<b>request</b>	Enables this dialer interface to request PPP callback (and function as the PPP callback client).

### Default

Callback requests are neither accepted nor requested.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

An interface can request PPP callback only if the interface is configured for PPP authentication with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).

### Example

The following example configures a previously defined dialer interface to accept PPP callback requests:

```
ppp callback accept
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**dialer callback-secure**

**map-class dialer** †

## ppp chap hostname

Use the **ppp chap hostname** interface configuration command to create a pool of dialup routers that all appear to be the same host when authenticating with CHAP. To disable this function, use the **no** form of the command.

```
ppp chap hostname hostname  
no ppp chap hostname hostname
```

### Syntax Description

*hostname*                      Name to be sent in the CHAP challenge.

### Default

Disabled. The router name is sent in any CHAP challenges.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Currently, a router dialing a pool of access routers requires a username entry for each possible router in the pool because each router challenges with its hostname. If a router is added to the dialup rotary pool, all connecting routers must be updated. The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when authenticating to the peer), but it will also be used for remote CHAP authentication.

### Example

The commands in the following example identify the dialer interface 0 as the dialer rotary group leader and specifies ppp as the method of encapsulation used by all member interfaces. Authentication is by CHAP on received calls only. The username *ISPCorp* will be sent in all CHAP challenges and responses.

```
interface dialer 0  
  encapsulation ppp  
  ppp authentication chap callin  
  ppp chap hostnmae ISPCorp
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

```
ppp authentication  
aaa authentication ppp †  
ppp pap †  
ppp chap password
```

## ppp chap password

To configure a common CHAP secret to be used in responses to challenges from an unknown remote peer in a collection of routers that do not support this command (such as routers running older Cisco IOS software images), use the **ppp chap password** interface configuration command. To disable this function, use the **no** form of this command.

```
ppp chap password secret  
no ppp chap password secret
```

### Syntax Description

<i>secret</i>	Secret used to compute the response value for any CHAP challenge from an unknown peer.
---------------	--

### Default

Disabled.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when authenticating to the peer) and does not affect local CHAP authentication.

### Example

The following example configures interface BRI 0 for PPP encapsulation. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri0  
  encapsulation ppp  
  ppp chap password 7 1234567891
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

```
ppp authentication  
aaa authentication ppp †  
ppp pap †  
ppp chap hostname
```

## ppp compress

To configure software compression for Point-to-Point Protocol (PPP) encapsulation, use the **ppp compress** interface configuration command. To disable compression, use the **no** form of this command.

```
ppp compress [predictor | stac]  
no ppp compress [predictor | stac]
```

### Syntax Description

**predictor** (Optional) Specifies that a predictor compression algorithm will be used.

**stac** (Optional) Specifies that a Stacker (LZS) compression algorithm will be used.

### Default

PPP compression is disabled.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Compression reduces the size of frames via lossless data compression. The compression algorithm used is a predictor algorithm (the RAND compression algorithm), which uses a compression dictionary to predict what the next character in the frame will be.

PPP encapsulation supports both predictor and Stacker compression algorithms.

Compression is performed in software and may significantly affect system performance. We recommend that you disable compression if CPU load exceeds 65 percent. To display the CPU load, use the **show process cpu EXEC** command.

Compression requires that both ends of the point-to-point link be configured to use compression. You should never enable compression for connections to a public data network.

If the majority of your traffic is already compressed files, we recommend that you not use compression. If the files are already compressed, the additional processing time spent in attempting unsuccessfully to compress them again will slow system performance.

### Examples

The following example enables predictor compression on serial interface 0:

```
interface serial 0  
  encapsulation ppp  
  ppp compress predictor
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

encapsulation ppp  
show compress

## ppp pap sent-username

To enable remote PAP support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** interface configuration command. Use the **no** form of this command to disable remote PAP support.

```
ppp pap sent-username username password password  
no ppp sent-username
```

### Syntax Description

<i>username</i>	Username sent in the PAP authentication request
<b>password</b>	Password sent in the PAP authentication request
<i>password</i>	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters

### Default

Remote PAP support disabled.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Use this command to enable remote PAP support (for example to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP Authentication Request.

### Example

The following example configures dialer interface 0 as the dialer rotary group leader and enables PPP encapsulation on the interface. Authentication is by CHAP or PAP on received calls only. *ISPCor* is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0  
encapsulation ppp  
ppp authentication chap pap callin  
ppp chap hostname ISPCor  
ppp pap sent username ISPCorp password 7 fjhfeu  
ppp pap sent-username ISPCorp password 7 1123659238
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

```
ppp authentication
aaa authentication ppp †
ppp chap hostname
ppp chap password
ppp use-tacacs †
```

## ppp max-bad-auth

To configure a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries, use the **ppp max-bad-auth** interface configuration command. To reset to the default of immediate reset, use the **no** form of this command.

```
ppp max-bad-auth number  
no ppp max-bad-auth
```

### Syntax Description

*number* Number of retries after which the interface is to reset itself.  
Default is 0.

### Default

0

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command applies to any serial interface (asynchronous serial, synchronous serial, or ISDN) on which PPP encapsulation is enabled.

### Example

The following example sets BRI interface 0 to allow two additional retries after an initial authentication failure (for a total of three failed authentication attempts):

```
interface bri 0  
encapsulation ppp  
ppp authentication chap  
ppp max-bad-auth 3
```

### Related Command

**encapsulation ppp**

## ppp multilink

To enable Multilink PPP on an interface, use the **ppp multilink** interface configuration command. To disable Multilink PPP, use the **no** form of this command.

**ppp multilink**  
**no ppp multilink**

### Syntax Description

This command has no arguments or keywords.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command applies only to interfaces that use PPP encapsulation.

PPP compression is allowed with MLP.

The **dialer load-threshold** command is used to enable a rotary group to bring up additional links and to add them to a multilink bundle.

When multilink PPP is configured, **dialer-load threshold 1** command no longer keeps a multilink bundle of  $n$  links connected indefinitely and the **dialer-load threshold 2** command no longer keeps a multilink bundle of 2 links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**dialer-group** †  
**dialer idle-timeout** †  
**dialer load-threshold** †  
**encapsulation ppp**  
**ppp authentication**  
**ppp compress**

## ppp quality

To enable Link Quality Monitoring (LQM) on a serial interface, use the **ppp quality** interface configuration command. Use the **no** form of this command to disable LQM.

**ppp quality** *percentage*  
**no ppp quality**

### Syntax Description

*percentage* Specifies the link quality threshold. Range is 1 to 100.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in a release prior to Cisco IOS Release 10.0.

The percentages are calculated for both incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent to the total number of packets and bytes received by the destination node. The incoming quality is calculated by comparing the total number of packets and bytes received to the total number of packets and bytes sent by the destination node.

If the link quality percentage is not maintained, the link is deemed to be of poor quality and is taken down. LQM implements a time lag so that the link does not bounce up and down.

### Example

The following example enables LQM on serial interface 2:

```
interface serial 2
 encapsulation ppp
 ppp quality 80
```

### Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

**encapsulation ppp**  
**keepalive** †

## ppp reliable-link

To enable LAPB Numbered Mode negotiation for a reliable serial link, use the **ppp reliable-link** interface configuration command. To disable negotiation for a PPP reliable link on a specified interface, use the **no** form of the command.

**ppp reliable-link**  
**no ppp reliable-link**

### Syntax Description

This command has no arguments and keywords.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Enabling LAPB Numbered Mode negotiation as a means of providing a reliable link does not guarantee that all connections through the specified interface will in fact use reliable link. It only guarantees that the router will attempt to negotiate reliable link on this interface.

PPP reliable link can be used with PPP compression over the link, but it does not require PPP compression.

PPP reliable link and Multilink PPP do not work together.

You can use the **show interface** command to determine whether LAPB has been established on the link. You can troubleshoot PPP reliable link by using the **debug lapb** command and the **debug ppp negotiations**, **debug ppp errors**, and **debug ppp packets** commands.

### Example

The following example enables PPP reliable link and predictor compression on interface BRI 0:

```
interface bri 0
  description Enables predictor compression on BRI 0
  ip address 170.1.1.1 255.255.255.0
  encapsulation ppp
  dialer map ip 170.1.1.2 name starbuck 14195291357
  compress predictor
  ppp authentication chap
  dialer-group 1
  ppp reliable-link
```

Related Commands

**debug lapb**

**debug ppp**

**compress**

**show interface**

## sgbp group

To define a named stack group and make the system a member of that stack group, use the **sgbp group** global configuration command.

**sgbp group** *name*

### Syntax Description

*name* Name of the stack group the system belongs to.

### Default

Disabled. No stack group name is provided.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Define the same stack group name across all the stack members.

### Example

In the following example, this system is made a member of the stack group named *stackq*:

```
sgbp stackq
```

### Related Commands

**sgbp member**  
sgbp seed-bid

## sgbp member

To specify the host name and IP address of a router or access server to be a peer member of a stack group, use the **sgbp member** global configuration command.

```
sgbp member peer-name [peer-ip-address]
```

### Syntax Description

<i>peer-name</i>	Host name of the peer member.
<i>peer-ip-address</i>	(Optional) IP address of the peer member. If the domain name system (DNS) can perform a lookup on the <i>peer-name</i> value, the IP address is not required. Otherwise, it must be specified.

### Default

Disabled. Peer names and peer IP addresses are not provided.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Use this command to specify the names of peer hosts in the specified stack group after you have entered the **sgbp group** command.

### Example

The following example configures the three routers (*yoda*, *han*, and *darth*) to be peer members of the *starfleet* stack group:

```
sgbp group starfleet
sgbp member yoda 10.69.5.2
sgbp member han 172.16.6.3
sgbp member darth 192.165.15.4
```

### Related Commands

**sgbp group**  
**sgbp seed-bid**

## sgbp seed-bid

To set the bidding level that a stack group member can bid with for a bundle, use the **sgbp seed-bid** global configuration command.

```
sgbp seed-bid { default | offload | bid }
```

### Syntax Description

<b>default</b>	If set across all members of a stack group, indicates that the member which receives the first call for a certain user always wins the bid and hosts the master bundle interface. All subsequent calls to the same user received by another stack group member will <i>project</i> to this stackgroup member. This is the default.
<b>offload</b>	Indicates that this router is a relatively higher powered stack group member, is to function as an offload server, and host the master bundle interface.
<i>bid</i>	Bid level, an integer in the range 0 through 9999.

### Default

The **default** keyword; no bid-level integer value is set.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

In the case of equivalent stack group members stacked to receive calls in a rotary group across multiple PRIs, use **sgbp seed-bid default** *across all stack members*. The stack member that receives the first call for a certain user always wins the bid and hosts the master bundle interface. All subsequent calls to the same user received by another stack member will project to this stack member. If the multiple calls come in concurrently over multiple stack members, the SGBP tie-breaking mechanism will break the tie.

To leverage the relative higher power of one stack member over another, you can set the designated stack member (of higher CPU power) as offload server with **sgbp seed-bid offload**. The bid that is sent is the precalibrated per-platform bid approximating the CPU power, minus the *bundle load*. In this case, the offload server hosts the master bundle. All calls from other stack members get projected to this stack member. One or more offload servers can be defined—if the bids are equal, the SGBP tie-breaking mechanism will break the tie.

The interfaces that received the calls are projected to the master bundle interface and are considered children of the master bundle interface for the call. See the output of the **show ppp multilink** for an example of master bundle interface (shown as “Master link”) and the children of it.

You can also manually designate bid values with the **sgbp seed-bid** command. This value overrides the **default** or **offload** setting.

To check the bid value currently assigned on the system, use the **show sgbp queries** command.

Related Commands

**sgbp group**

**sgbp member**

**show sgbp queries**

## show ppp multilink

To display bundle information for the Multilink PPP bundles, use the **show ppp multilink EXEC** command.

### show ppp multilink

#### Syntax Description

This command has no keywords or arguments.

#### Command Mode

EXEC

#### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

#### Sample Display

The following is the output when no bundles are on a system.

```
impulse#sh ppp multilink
No active bundles
```

The following is sample output when a single Multilink PPP bundle (named rudder) is on a system:

```
systema# show ppp multilink

Bundle rudder, 3 members, first link is BRI0: B-channel 1
0 lost fragments, 8 reordered, 0 unassigned, sequence 0x1E/0x1E rcvd/sent
```

The following is sample output when two active bundles are on a system. Subsequent bundles would be displayed below the previous bundle.

```
impulse# show ppp multilink

Bundle rudder, 3 members, first link is BRI0: B-Channel 1
0 lost fragments, 8 reordered, 0 unassigned, sequence 0x1E/0x1E rcvd/sent
Bundle dallas, 4 members, first link is BRI2: B-Channel 1
0 lost fragments, 28 reordered, 0 unassigned, sequence 0x12E/0x12E rcvd/sent
```

The following example shows output when a stack group has been created. On stack group member *systema* on stackgroup *stackq*, Multilink PPP bundle *hansolo* has bundle interface *Virtual-Access4*. Two child interfaces are joined to this bundle interface. The first is a local PRI channel (serial 0:4), and the second is an interface from stack group member *systemb*.

```
systema# show ppp multilink

Bundle hansolo 2 members, Master link is Virtual-Access4
0 lost fragments, 0 reordered, 0 unassigned, 100/255 load
0 discarded, 0 lost received, sequence 40/66 rcvd/sent
members 2
Serial0:4
systemb:Virtual-Access6 (1.1.1.1)
```

## show sgbp

To display the status of the stack group members, use the **show sgbp** EXEC command.

```
show sgbp
```

### Syntax Description

This command has no keywords or arguments.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

### Sample Output

The following is sample output from the **show sgbp** command:

```
systema#show sgbp

Group Name: stack State: 0 Ref: 0xC07B060
Member Name: systemb State: ACTIVE Id: 1
Ref: 0xC14256F
Address: 1.1.1.1 Tcb: 0x60B34538

Member Name: systemc State: ACTIVE Id: 2
Ref: 0xA24256D
Address: 1.1.1.2 Tcb: 0x60B34439

Member Name: systemd State: IDLE Id: 3
Ref: 0x0
Address: 1.1.1.3 Tcb: 0x0
```

## show sgbp queries

To display the current seed bid value, use the **show sgbp queries** EXEC command.

```
show sgbp queries
```

### Syntax Description

This command has no keywords or arguments.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

### Sample Display

The following example shows a bid of 50 from this system. Peers queried the system for the bid, the bid was accepted, and a connection was opened from a peer in the stack group:

```
systema# show sgbp queries

Seed bid: default, 50

Bundle: foo      State: Query_from_peers OurBid: 50
1.1.1.2         State: Open_from_peer   Bid: 050 Retry: 0
```

## show vpdn

To display information about active Level 2 Forwarding (L2F) protocol tunnel and Level 2 Forwarding (L2F) message identifiers in a virtual private dialup network, use the **show vpdn** EXEC command.

### show vpdn

### Syntax Description

This command has no keywords or arguments.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

### Sample Display

The following is sample output of the **show vpdn** command:

```
Router#show vpdn

Active L2F tunnels
NAS Name      Gateway Name  NAS CLID  Gateway CLID  State
nas           gateway       4         2             open

L2F MIDs
Name          NAS Name     Interface  MID           State
phil@cisco.com  nas         As7       1             open
sam@cisco.com  nas         As8       2             open
```

Table 41 describes the fields in this sample display.

**Table 41 Show Vpdn Field Descriptions**

Field	Description
<b>Active L2F tunnels</b>	
NAS Name	Host name of the network access server, which is the remote termination point of the tunnel.
Gateway Name	Host name of the home gateway, which is local termination point of the tunnel.
NAS CLID	A number uniquely identifying the VPDN tunnel on the network access server.
Gateway CLID	A number uniquely identifying the VPDN tunnel on the gateway
State	Indicates whether the tunnel is open, opening, closing, or closed.
<b>L2F MIDs</b>	
Name	Username of the person from whom a protocol message was forwarded over the tunnel.
NAS Name	Host name of the network access server.

**Table 41 Show Vpdn Field Descriptions (Continued)**

<b>Field</b>	<b>Description</b>
Interface	Interface from which the protocol message was sent.
MID	A number uniquely identifying this user in this tunnel.
State	Indicates status for the individual user in the tunnel. The states are: opening, open, closed, closing, and waiting_for_tunnel.  The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.

Related Commands

- vpdn enable**
- vpdn incoming**
- vpdn outgoing**

## vpdn enable

To enable virtual private dial-up networking on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** global configuration command.

**vpdn enable**

### Syntax Description

This command has no keywords or arguments.

### Default

Disabled

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

### Example

The following example enables virtual private dial-up networking on the router:

```
vpdn enable
```

### Related Commands

**vpdn incoming**

**vpdn outgoing**

## vpdn force-local-chap

To cause the home gateway to issue its own CHAP challenge even if one has already been issued from the network access server, use the **vpdn force-local-chap** global configuration command. To disable the home gateway's issuing its own CHAP challenge, use the **no** form of this command.

**vpdn force-local-chap**  
**no vpdn force-local-chap**

### Syntax Description

This command has no keywords or arguments.

### Default

The home gateway does not issue its own CHAP challenge.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

## vpdn incoming

To specify the local name to use for authenticating and the virtual template to use for building interfaces for incoming connections when a Level 2 Forwarding (tunnel) connection is requested from a certain remote host, use the **vpdn incoming** global configuration command.

```
vpdn incoming remote-name local-name virtual-template number
```

### Syntax Description

<i>remote-name</i>	Case-sensitive name of the remote host requesting the connection.
<i>local-name</i>	Case-sensitive local name to use when authenticating back to the remote host.
<b>virtual-template</b> <i>number</i>	Virtual template to use for building interfaces for incoming calls.

### Default

Disabled. No host name, IP address, or local name for authentication are provided.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

The *remote-name* and *local-name* arguments are case sensitive.

This command is usually used on a home gateway, not on the network access server in the ISP or public data network.

### Example

```
vpdn incoming dallas_wan go_blue virtual-template 6
```

## vpdn outgoing

To specify the name and IP address of a remote host and the name to use when authenticating a tunnel for forwarding traffic to the remote host on a virtual private dialup network, use the **vpdn outgoing** global configuration command.

**vpdn outgoing** *domain-name local-name ip ip-address*

### Syntax Description

<i>domain-name</i>	Case-sensitive name of the domain to forward traffic to.
<i>local-name</i>	Case-sensitive local name to use when authenticating the tunnel to the remote host.
<i>ip-address</i>	IP address of the remote host.

### Default

Disabled. No remote names and local names are defined.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

The *domain-name* and *local-name* arguments are case sensitive.

This command is usually used on a network access server, not on a home gateway.

The domain name can be used to choose a tunnel destination. For example, if people dial in as "joe@company-a.com," then we can match on "company-a.com," and based on that, choose a tunnel destination.

### Example

```
vpdn outgoing chicago-main go-blue ip 172.17.33.125
```

### Related Commands

**vpdn enable**  
**vpdn incoming**

## username

To specify the password to be used in the PPP Challenge Handshake Authentication Protocol (CHAP) caller identification and Password Authentication Protocol (PAP), use the **username** command.

```
username name password secret
```

### Syntax Description

<i>name</i>	Host name, server name, user ID, or command name.
<b>password</b>	An encrypted password for this username.
<i>secret</i>	For CHAP authentication: specifies the secret password for the local router or access server or the remote device. The secret is encrypted when it is stored on the local router or access server. This prevents the secret from being stolen. The secret can consist of any string of up to 11 printable ASCII characters. There is no limit to the number of username-password combinations that can be specified, allowing any number of remote devices to be authenticated.

### Default

No password is predefined.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in a release prior to Cisco IOS Release 11.1.

Add a *name* entry for each remote system that the local router or access server requires authentication from.

The **username** command is required as part of the configuration for authentication protocols, such as CHAP and PAP. For each remote system that the local router or access server communicates with from which it requires authentication, you add a **username** entry.

---

**Note** To enable the local router or access server to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** *name* entry that has already been assigned to your device.

---

If no secret is specified and **debug serial-interface** is enabled, an error is displayed when a link is established and the authentication protocol challenge is not implemented. Debugging information about authentication protocols is available via the **debug serial-interface** and **debug serial-packet** commands. See the *Debug Command Reference* publication for more information.

### Example

The following example configuration enables CHAP on interface serial 0. It also defines a password for local server *Adam* and remote server *Eve*.

```
hostname Adam
interface serial 0
encapsulation ppp
ppp authentication chap
username Eve password theirsystem
```

When you look at your configuration file, the passwords will be encrypted and the display will look similar to the following:

```
hostname Adam
interface serial 0
encapsulation ppp
ppp authentication chap
username Eve password 7 121F0A18
```

### Related Command

A dagger (†) indicates that the command is documented outside this chapter.

**hostname** †