



Media-Independent PPP and Multilink PPP Commands

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

For information about configuring PPP on Cisco routers, see the “Configuring Media-Independent PPP and Multilink PPP” chapter in the *Dial Solutions Configuration Guide*.

For information about configuring PPP on asynchronous links, refer to the “Configuring SLIP and PPP” chapter in the *Dial Solutions Configuration Guide*. For PPP commands for asynchronous links, refer to the “SLIP and PPP Commands” chapter in the *Dial Solutions Command Reference*.

For more information about PPP, see RFC 1661. For more information about MLP, see RFC 1717. For more information about PAP, see RFC 1334. For more information about CHAP, see RFC 1994.

compress

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

```
compress [predictor | stac | mppc [ignore-pfc]]  
no compress [predictor | stac | mppc [ignore-pfc]]
```

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.
mppc	(Optional) Specifies that the MPPC compression algorithm will be used.
ignore-pfc	(Optional) Specifies that the protocol field compression flag negotiated through LCP will be ignored.

Default

PPP compression is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

The **mppc** and **ignore-pfc** options first appeared in Cisco IOS Release 11.3 T.

End-point devices must be configured to use the same compression method (predictor, Stacker or MPPC).

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.

MPPC Compression

The **compress** command using the **mppc** and **ignore-pfc** options support compression between Cisco routers and access servers and Microsoft clients, such as Windows 95 and Windows NT. MPPC implements an LZ based compression algorithm that uses a compression dictionary to compress PPP packets. The **ignore-pfc** keyword instructs the router to ignore the protocol field compression flag negotiated by LCP. For example, the uncompressed standard protocol field value for IP is 0x0021 and 0x21 when compression is enabled. When the **ignore-pfc** option is enabled, the router will continue to use the uncompressed value (0x0021). Using the **ignore-pfc** option is helpful for some asynchronous driver devices which use an uncompressed protocol field (0x0021), even though the pfc is negotiated between peers. If protocol rejects are displayed when the **debug ppp negotiation** command is enabled, setting the **ignore-pfc** option may remedy the problem.

System performance

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.

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
 compress predictor
```

The following example configures BRI interface 0 to perform MPPC:

```
interface BRI0
 ip unnumbered ethernet0
 encapsulation ppp
 isdn spid1 5551234
 dialer map ip 172.21.71.74 5551234
 dialer-group 1
 compress mppc
```

The following example configures asynchronous interface 1 to implement MPPC and ignore the protocol field compression flag negotiated by LCP:

```
interface async1
 ip unnumbered ethernet0
 encapsulation ppp
 async default routing
 async dynamic routing
 async mode interactive
 peer default ip address 172.21.71.74
 compress mppc ignore-pfc
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

encapsulation ppp
show compress

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. Use the **no** form of this command to disable PPP encapsulation.

encapsulation ppp
no encapsulation ppp

Syntax Description

This command has no arguments or keywords.

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

You can use the master indexes or search online to find documentation of related commands.

keepalive
ppp
ppp authentication

ip address-pool

To enable an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces, use the **ip address-pool** global configuration command. To disable IP address pooling globally on all interfaces with the default configuration, use the **no** form of the command.

```
ip address-pool { dhcp-proxy-client | local }  
no ip address-pool
```

Syntax Description

dhcp-proxy-client	Uses the router as the proxy-client between a third-party Dynamic Host Configuration Protocol (DHCP) server and peers connecting to the router.
local	Uses the local address pool named <i>default</i> .

Default

IP address pooling is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

The global default IP address pooling mechanism applies to all interfaces that have been left in the default setting of the **peer default ip address** command.

If any **peer default ip address** command other than **peer default ip address pool** (the default) is configured, the interface uses that mechanism and not the global default mechanism. Thus all interfaces can be independently configured, or left unconfigured so that the global default configuration applies. This flexibility minimizes the configuration effort on the part of the administrator.

Examples

The following example specifies the DHCP proxy client mechanism as the global default mechanism for assigning peer IP addresses:

```
ip address-pool dhcp-proxy-client
```

The following example specifies a local IP address pool called *default* as the global default mechanism for all interfaces that have been left in their default setting:

```
ip address-pool local
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

peer default ip address

ip dhcp-server

To specify which Dynamic Host Configuration Protocol (DHCP) servers to use on your network, specify the IP address of one or more DHCP servers available on the network, use the **ip dhcp-server** global configuration command. Use the **no** form of the command to remove a DHCP server's IP address.

```
ip dhcp-server [ip-address | name]  
no ip dhcp-server [ip-address | name]
```

Syntax Description

<i>ip-address</i>	(Optional) IP address of a DHCP server.
<i>name</i>	(Optional) Name of a DHCP server.

Default

The IP limited broadcast address of 255.255.255.255 is used for transactions if no DHCP server is specified. This allows automatic detection of DHCP servers.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

A DHCP server temporarily allocates network addresses to clients through the access server on an as-needed basis. While the client is active, the address is automatically renewed in a minimum of 20-minute increments. When the user terminates the session, the interface connection is terminated so that network resources can be quickly reused. You can specify up to ten servers on the network.

In normal situations, if a user's SLIP/PPP session fails (for example if a modem line disconnects), the allocated address will be reserved temporarily to preserve the same IP address for the client when dialed back into the server. This way, the session that was accidentally terminated can often be resumed.

To use the DHCP proxy-client feature, enable your access server to be a proxy-client on asynchronous interfaces by using the **ip address-pool dhcp-proxy-client** command. If you wish to specify which DHCP servers are used on your network, use the **ip dhcp-server** command to define up to ten specific DHCP servers.

Note To facilitate transmission, configure intermediary routers (or access servers with router functionality) to use an IP helper address whenever the DHCP server is not on the local LAN and the access server is using broadcasts to interact with the DHCP server. See "Configuring IP Addressing" in the *Network Protocols Configuration Guide, Part 1*.

The **ip address-pool dhcp-proxy-client** command initializes proxy-client status to all interfaces defined as asynchronous on the access server. To selectively disable proxy-client status on a single asynchronous interface, use the **no peer default ip address** interface command.

Example

The following command specifies a DHCP server with the IP address of 129.12.13.81:

```
ip dhcp-server 129.12.13.81
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip address-pool dhcp-proxy-client

ip helper address

peer default ip address pool

show dhcp

ip local pool

To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, or to add a range of addresses to an existing pool, use the **ip local pool** global configuration command. To remove an address pool, or a range of addresses from a pool, use the appropriate **no** form of this command.

```
ip local pool { default | pool-name } low-ip-address [high-ip-address]
no ip local pool { default | pool-name }
no ip local pool { default | pool-name } low-ip-address [high-ip-address]
```

Note There are two ways to use the **ip local pool** command and its **no** forms; see the usage guidelines and examples for more explanation of use.

Syntax Description

default	Default local address pool that is used if no other pool is named.
<i>pool-name</i>	Name of a specific local address pool. (Always use the <i>pool-name</i> argument consistently.)
<i>low-ip-address</i>	Lowest IP address in the pool.
<i>high-ip-address</i>	(Optional) Highest IP address in the pool. If this value is omitted only the <i>low-ip-address</i> IP address is included in the local pool.

Default

No address pools are configured.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0. Enhancements to the command were made in Releases 11.3AA and 12.0, to support multiple address ranges.

Use the **ip local pool** command to create one or more local address pools from which IP addresses are assigned when a peer connects. The **default** address pool is then used on all point-to-point interfaces after the **ip address-pool local** global configuration command is issued. To use a specific, named address pool on an interface, use the **peer default ip address pool** interface configuration command.

Use the shorter **no** form of the command to remove the entire address pool (default or specific). Use the longer **no** form of the command with appropriate keywords and arguments to remove a range of addresses from a pool.

These pools can also be used with the **translate** commands for one-step vty-async connections and in certain AAA/TACACS+ authorization functions. Refer to the “Configuring Protocol Translation and Virtual Asynchronous Devices” chapter in the *Dial Solutions Configuration Guide* and the “System Management” part of the *Configuration Fundamentals Configuration Guide* for more information. Pools can be displayed with the **show ip local pool** command.

Example

The following command creates a local IP address pool by the name of quark, which contains all local IP addresses from 172.16.23.0 to 172.16.23.255:

```
ip local pool quark 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
2511(config)#no ip local pool default
2511(config)#ip local pool default 1.1.1.0 1.1.4.255
2511(config)#^Z
2511#show ip local pool
Pool      Begin      End          Free InUse
default  1.1.1.0    1.1.4.255   1024  0
```

The following example configures multiple ranges of IP addresses into one pool:

```
7206-9(config)#no ip local pool default
7206-9(config)#ip local pool default 9.1.1.0 9.1.9.255
7206-9(config)#ip local pool default 9.2.1.0 9.2.9.255
7206-9(config)#^Z

7206-9#show ip local pool
Pool      Begin      End          Free  In use  Cache Size
default  9.1.1.0    9.1.9.255   2304  0       20
         9.2.1.0    9.2.9.255   2304  0
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- ip address-pool**
- show ip local pool**

ip rtp reserve

To reserve a special queue for a set of Real-time Transport Protocol (RTP) packet flows belonging to a range of UDP destination ports, use the **ip rtp reserve** interface configuration command. To disable the special queue for real-time traffic, use the **no** form of the command.

```
ip rtp reserve lowest-udp-port range-of-ports [maximum-bandwidth]  
no rtp reserve
```

Syntax Description

<i>lowest-udp-port</i>	Lowest UDP port number to which the packets are sent.
<i>range-of-ports</i>	Number, which added to the lowest-UDP-port value, yields the highest UDP port value.
<i>maximum-bandwidth</i>	(Optional) Bandwidth, in kilobits per second, reserved for the RTP packets to be sent to the specified UDP ports.

Default

This function is disabled by default. No default values are provided for the arguments.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Release 11.3.

If the bandwidth needed for RTP packet flows exceeds the maximum bandwidth specified, the reserved queue will degrade to a best-effort queue.

This command helps in improving the delay bounds of voice streams by giving them a higher priority.

Example

The following example reserves a unique queue for traffic to destination UDP ports in the range 32768 to 32788 and reserves 1,000 kbps bandwidth for that traffic:

```
ip rtp reserve 32768 20 1000
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ppp multilink  
ppp multilink fragment-delay  
ppp multilink interleave
```


peer default ip address

Use the **peer default ip address** interface configuration command to specify an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface. Use the **no** form of the command to disable a prior peer IP address pooling configuration on an interface.

```
peer default ip address { ip-address | dhcp | pool [pool-name] }
no peer default ip address
```

Syntax Description

<i>ip-address</i>	Specific IP address to be assigned to a remote peer dialing in to the interface. To prevent duplicate IP addresses from being assigned on more than one interface, this command argument cannot be applied to a dialer rotary group nor to an ISDN interface.
dhcp	Retrieve an IP address from the DHCP server.
pool	Use the global default mechanism as defined by the ip address-pool command unless the optional <i>pool-name</i> argument is supplied. This is the default.
<i>pool-name</i>	(Optional) Name of a local address pool created using the ip local pool command. Retrieve an address from this pool regardless of the global default mechanism setting.

Default

pool

Command Mode

Interface configuration

Usage Guidelines

This command applies to point-to-point interfaces that support the PPP or SLIP encapsulation.

This command allows an administrator to configure all possible address pooling mechanisms on a interface-by-interface basis.

The **peer default ip address** command can override the global default mechanism defined by the **ip address-pool** command on an interface-by-interface basis.

- For all interfaces not configured with a peer default IP address mechanism (equivalent to selecting the **peer default ip address pool** command), the router uses the global default mechanism that is defined by the **ip address-pool** command.
- If you select the **peer default ip address pool** *pool-name* form of this command, then the router uses the locally configured pool on this interface and does not follow the global default mechanism.

- If you select the **peer default ip address *ip-address*** form of this command, the specified IP address is assigned to any peer connecting to this interface and any global default mechanism is overridden for this interface.
- If you select the **peer default ip address dhcp** form of this command, the DHCP proxy-client mechanism is used by default on this interface and any global default mechanism is overridden for this interface.

Examples

The following command specifies that this interface will use a local IP address pool called pool3:

```
peer default ip address pool pool3
```

The following command specifies that this interface will use the IP address 172.140.34.21:

```
peer default ip address 172.140.34.21
```

The following command reenables the global default mechanism to be used on this interface:

```
peer default ip address pool
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

encapsulation ppp

encapsulation slip

ip address-pool

ip dhcp-server

ip local pool

ppp

slip

show dhcp

peer neighbor-route

To reenables 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 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

chap	Enables CHAP on a serial interface.
pap	Enables PAP on a serial interface.
chap pap	Enables both CHAP and PAP, and performs CHAP authentication before PAP.
pap chap	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
if-needed	(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 aaa authentication ppp command.
default	(Optional) Used with AAA/TACACS+. Created with the aaa authentication ppp command.
callin	(Optional) 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

You can use the master indexes or search online to find documentation of related commands.

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. Use the **no** form of this command to disable AppleTalk packet half-bridging.

ppp bridge appletalk
no ppp bridge appletalk

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 11.2.

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

You can use the master indexes or search online to find documentation of related commands.

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. Use the **no** form of this command to disable IP packet half-bridging.

```
ppp bridge ip  
no ppp bridge ip
```

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 11.2.

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

You can use the master indexes or search online to find documentation of related commands.

```
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. Use the **no** form of this command to return to Novell Ethernet encapsulation.

```
ppp bridge ipx [novell-ether | arpa | sap | snap]  
no ppp bridge ipx
```

Syntax Description

novell-ether	(Optional) Use Novell's Ethernet_802.3 encapsulation. This is the default.
arpa	(Optional) Use Novell's Ethernet_II encapsulation.
sap	(Optional) Use Novell's Ethernet_802.2 encapsulation.
snap	(Optional) 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

You can use the master indexes or search online to find documentation of related commands.

ipx network
ppp bridge appletalk
ppp bridge ip

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 hostname ISPCorp
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

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

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 1234567891 is decrypted and used to create a CHAP response value.

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

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

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

<i>number</i>	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 Commands

You can use the master indexes or search online to find documentation of related commands.

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.

Multilink PPP is designed to work over single or multiple interfaces that are configured to support both dial-on-demand rotary groups and PPP encapsulation. This command applies asynchronous serial interfaces, ISDN Basic Rate Interfaces (BRIs), and ISDN Primary Rate Interfaces (PRIs).

PPP compression is allowed with MLP.

Multilink PPP and PPP reliable link do not work together.

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.

Example

The following partial example configures a dialer for Multilink PPP; it does not show the configuration of the physical interfaces.

```
interface Dialer0  
  ip address 99.0.0.2 255.0.0.0  
  encapsulation ppp  
  dialer in-band  
  dialer idle-timeout 500  
  dialer map ip 99.0.0.1 name atlanta broadcast 81012345678901  
  dialer load-threshold 30 either  
  dialer-group 1  
  ppp authentication chap  
  ppp multilink
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

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

ppp multilink fragment-delay

To configure a maximum delay allowed for transmission of a packet fragment on a Multilink PPP bundle, use the **ppp multilink fragment-delay** interface configuration command. To reset the maximum delay to the default value, use the **no** form of the command.

```
ppp multilink fragment-delay milliseconds  
no ppp multilink fragment-delay
```

Syntax Description

<i>milliseconds</i>	Maximum delay, in milliseconds, allowed for any packet fragment. Default is 30 milliseconds.
---------------------	--

Default

This command is disabled by default.
Default delay is 30 milliseconds.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

The **ppp multilink fragment-delay** command applies only to interfaces that can configure a bundle interface. These include virtual-templates, dialer interfaces, and ISDN BRI or PRI interfaces.

Multilink PPP chooses a fragment size based on the maximum delay allowed. If real-time traffic requires a certain maximum bound on delay, using this command to set that maximum delay can ensure that a real-time packet will get interleaved within the fragments of a large packet.

Example

The following example requires a voice to have a maximum bound on delay of 20 milliseconds:

```
ppp multilink fragment-delay 20
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ip rtp reserve  
ppp multilink  
ppp multilink interleave
```

ppp multilink interleave

To enable interleaving of Real-Time Transport Protocol (RTP) packets among the fragments of larger packets on a Multilink PPP bundle, use the **ppp multilink interleave** interface configuration command. To disable interleaving, use the **no** form of the command.

ppp multilink interleave
no ppp multilink interleave

Syntax Description

This command has no arguments and keywords.

Default

This function is disabled by default.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Release 11.3.

The **ppp multilink interleave** command applies only to interfaces that can configure a bundle interface. These include virtual-templates, dialer interfaces, and ISDN BRI or PRI interfaces.

Example

The following example defines a virtual interface template that enables Multilink PPP interleaving and a maximum real-time traffic delay of 20 milliseconds, and then applies that virtual template to the Multilink PPP bundle:

```
interface virtual-template 1
 ip unnumbered ethernet 0
 ppp multilink
 ppp multilink interleave
 ppp multilink fragment-delay 20
 !
 multilink virtual-template 1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip rtp reserve
ppp multilink
ppp multilink fragment-delay

ppp pap sent-username

To enable remote PAP support for an interface and use the **sent-username** and **password** elements 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 pap sent-username
```

Syntax Description

<i>username</i>	Username sent in the PAP authentication request.
password	Password sent in the PAP authentication request.
<i>password</i>	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters; cannot contain spaces or underscores.

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. *ISPCorp* 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 ISPCorp  
  ppp pap sent username ISPCorp password 7 fjhfeu  
  ppp pap sent-username ISPCorp password 7 1123659238
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- aaa authentication ppp**
- ppp authentication**
- ppp chap hostname**
- ppp chap password**
- ppp use-tacacs**

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

You can use the master indexes or search online to find documentation of related commands.

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 does not work with Multilink PPP.

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

You can use the master indexes or search online to find documentation of related commands.

debug lapb
debug ppp
compress
show interface

show dhcp

To display the current DHCP settings on point-to-point interfaces, use the **show dhcp** privileged EXEC command.

```
show dhcp {server | lease [interface async [number]]}
```

Syntax Description

server	Show known DHCP servers.
lease	Show DHCP addresses leased from a server.
interface async [number]	(Optional) Specify asynchronous interfaces and, optionally, a specific interface number.

Command Mode

Privileged EXEC

Usage Guidelines

If you omit the optional argument, the **show dhcp** command displays information about all interfaces.

You can use this command on any point-to-point type of interface (for example, serial, ISDN, and asynchronous) that uses DHCP for temporary IP address allocation.

Sample Display

The following is sample output from the **show dhcp server** command:

```
Router# show dhcp server

IP address pooling for Point to Point clients is: DHCP Proxy Client
DHCP Proxy Client Status:
  DHCP server: ANY (255.255.255.255)
  Leases:      0
  Offers:      0      Requests: 0      Acks: 0      Naks: 0
  Declines:    0      Releases: 0      Bad: 0
```

Table 110 describes the fields shown in the display.

Table 110 Show DHCP Field Descriptions

Field	Description
Leases	Number of current leased IP addresses.
Offers	Number of offers for an IP address sent to a proxy-client from the server.
Requests	Number of requests for an IP address to the server.
Acks	Number of 'acknowledge' messages sent by the server to the proxy-client.
Naks	Number of 'not acknowledge' messages sent by the server to the proxy-client.
Declines	Number of offers from the server that are declined by the proxy-client.

Table 110 **Show DHCP Field Descriptions (continued)**

Field	Description
Releases	Number of times IP addresses have been relinquished gracefully by the client.
Bad	Number of bad packets received from wrong length, wrong field type, etc.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip address-pool

ip dhcp-server

peer default ip address

show ip local pool

To display statistics for any defined IP address pools, use the **show ip local pool** command.

show ip local pool [*name*]

Syntax Description

name (Optional) Name of a specific IP address pool.

Command Mode

Privileged EXEC

Usage Guidelines

If you omit the variable *name*, the software will display a generic list of all defined address pools and the IP addresses that belong to them. If you specify a name, the software displays more detailed information for that pool.

Sample Display

The following is sample output from the **show ip local pool** command:

```
Router# show ip local pool

Scope   Begin           End             Free InUse
Dialin  172.30.228.11  172.30.228.26  16    0
Available addresses:
 172.30.228.12
 172.30.228.13
 172.30.228.14
 172.30.228.15
 172.30.228.16
 172.30.228.17
 172.30.228.18
 172.30.228.19
 172.30.228.20
 172.30.228.21
 172.30.228.22
 172.30.228.23
 172.30.228.24
 172.30.228.25
 172.30.228.26
 172.30.228.11           Async5

Inuse addresses:
None
```

Table 111 describes the fields shown in the display.

Table 111 Show IP Local Pool Field Descriptions

Field	Description
Scope	The type of access.
Begin	The first IP address in the defined range of addresses in this pool.

Table 111 Show IP Local Pool Field Descriptions (continued)

Field	Description
End	The last IP address in the defined range of addresses in this pool.
Free	The number of addresses currently available.
InUse	The number of addresses currently in use.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip address-pool

ip local pool

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 arguments or keywords.

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# show 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 queuing virtual-access

To display information about interleaving, use the **show queuing virtual-access EXEC** command.

show queuing virtual-access *number*

Syntax Description

number Virtual access interface number.

Command Mode

EXEC

Sample Display

This command was first added in Cisco Release 11.3.

The following is sample output of the **show queuing virtual-access** command:

```
Router# show queuing virtual-access 1

Input queue: 0/75/0 (size/max/drops); Total output drops: 164974
Queueing strategy: weighted fair
Output queue: 315/64/164974/31191 (size/threshold/drops/interleaves)
  Conversations 5/8 (active/max active)
  Reserved Conversations 2/2 (allocated/max allocated)

(depth/weight/discard/interleaves) 64/4096/38669/0
Conversation 36, linktype: ip, length: 52
source: 140.3.3.201, destination: 225.1.2.3, id: 0x0001, ttl: 254,
TOS: 0 prot: 17, source port 6789, destination port 2345

(depth/weight/discard/interleaves) 64/4096/0/0
Conversation 2, linktype: ip, length: 52
source: 140.3.3.201, destination: 225.1.2.4, id: 0x0001, ttl: 254,
TOS: 0 prot: 17, source port 5432, destination port 9870
```

Table 112 describes significant fields in the **show queuing virtual-access** command output.

Table 112 Show Queuing Virtual-Access Command Output

Field	Description
Input queue: size, max, drops	Input queue used for virtual access interface 1, with the current size, the maximum size, and the number of dropped packets.
Total output drops	Number of output packets dropped.
Output queue: size/threshold/drops/interleaves	Output queue counters. Maximum number of packets allowed in the queue, number in the queue, the number of packets dropped due to a full queue, and the number of real-time packets interleaved among fragments of larger packets.
Conversations (active/max active)	Fair queue conversation statistics: number of conversations currently active and the maximum that have been active.

Table 112 Show Queuing Virtual-Access Command Output (continued)

Field	Description
Reserved conversations (allocated, max allocated)	Reserved conversations in the weighted fair queue. (current/maximum number allocated). Reserved conversations get the highest priority.
(depth/weight/discards/interleaves) 64/4096/38669/0	Depth of the queue, weight assigned to each packet in the queue, number of packets discarded in the queue so far, and the number of interleaves.
Conversation 36, linktype: ip, length: 52	Conversation identifier, protocol used on the link (IP), and the number of bytes.
source: 140.3.3.201, destination: 225.1.2.3,	Source IP address and destination IP address.
id: 0x0001	Protocol ID, identifying IP.
ttl: 254	Time to live, in seconds.
TOS: 0	Type of service.
prot: 17	Protocol field in IP. The value 17 indicates UDP.
source port 5432	Source TCP/UDP port.
destination port 9870	Destination TCP/UDP port.

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** global configuration command.

```
username name password secret
```

Syntax Description

<i>name</i>	Host name, server name, user ID, or command name.
password	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 password can consist of any string of up to 11 printable ASCII characters, but cannot include spaces or underscores. 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 serial interface 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 Commands

You can use the master indexes or search online to find documentation of related commands.

hostname