



PPP and Multilink PPP Configuration



Note PPP and Multilink PPP Configuration is *not* supported on the Cisco ASR 900 RSP3 module.

This module describes how to configure PPP and Multilink PPP (MLP) features on any interface. Multilink PPP provides a method for spreading traffic across multiple physical WAN links.

- [Limitations, on page 1](#)
- [PPP and Multilink PPP, on page 2](#)
- [IP Address Pooling, on page 3](#)
- [How to Configure PPP, on page 5](#)
- [Monitoring and Maintaining PPP and MLP Interfaces, on page 24](#)

Limitations

The following limitations apply when using MLPPP on the Cisco ASR 903 Router:

- All links in an MLPPP bundle must be on the same interface module.
- All links in an MLPPP bundle must be of the same bandwidth.
- The router supports a maximum of 16 links per bundle and a minimum of 2 links per bundle. Maximum number of bundles supported per interface module is 168.
- To change the MLPPP bundle fragmentation mode between enabled and disabled, perform a **shutdown/no shutdown** on the bundle.
- LFI is not supported. However, PPP Multilink fragmentation is supported by default. To disable fragmentation, see [Disabling PPP Multilink Fragmentation](#).
- Multicast MLP is not supported.
- PPP compression is not supported.
- PPP half bridging is not supported.
- IPv6 is not supported for this feature.
- To enable an ACFC or PFC configuration, issue a shut **shutdown/no shutdown** on the serial interface.

- Channelization is not supported
- Also that only 1 channel-group can be created per controller with complete timeslots.
- PPP and MLPPP are supported on synchronous serial interfaces; Asynchronous serial interfaces, high-speed serial interfaces (HSSI), and ISDN interfaces are not supported.
- If you configure interfaces on each end of an MLPPP connection with different MTU values, the link drops traffic at high traffic rates. We recommend that you configure the same MTU values across all nodes in an MLPPP connection.

PPP and Multilink PPP

To configure the Media-Independent PPP and Multilink PPP, you should understand the following concepts:

Point-to-Point Protocol

Point-to-Point Protocol (PPP), described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on synchronous serial interfaces.

Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), or Password Authentication Protocol (PAP)

Magic Number support is available on all serial interfaces. PPP always attempts to negotiate for Magic Numbers, which are used to detect looped-back lines. Depending on how the **down-when-looped** command is configured, the router might shut down a link if it detects a loop.

CHAP or PPP Authentication

PPP with CHAP or PAP authentication is often used to inform the central site about which remote routers are connected to it.

With this authentication information, if the router or access server receives another packet for a destination to which it is already connected, it does not place an additional call. However, if the router or access server is using rotaries, it sends the packet out the correct port.

CHAP and PAP were originally specified in RFC 1334, and CHAP was updated in RFC 1994. These protocols are supported on synchronous and asynchronous serial interfaces. When using CHAP or PAP authentication, each router or access server identifies itself by a name. This identification process prevents a router from placing another call to a router to which it is already connected, and also prevents unauthorized access.

Access control using CHAP or PAP is available on all serial interfaces that use PPP encapsulation. The authentication feature reduces the risk of security violations on your router or access server. You can configure either CHAP or PAP for the interface.



Note To use CHAP or PAP, you must be running PPP encapsulation.

When CHAP is enabled on an interface and a remote device attempts to connect to it, the local router or access server sends a CHAP packet to the remote device. The CHAP packet requests or “challenges” the remote

device to respond. The challenge packet consists of an ID, a random number, and the hostname of the local router.

The required response has two parts:

- An encrypted version of the ID, a secret password, and the random number
- Either the hostname of the remote device or the name of the user on the remote device

When the local router or access server receives the response, it verifies the secret password by performing the same encryption operation as indicated in the response and looking up the required hostname or username. The secret passwords must be identical on the remote device and the local router.

Because this response is sent, the password is never sent in clear text, preventing other devices from stealing it and gaining illegal access to the system. Without the proper response, the remote device cannot connect to the local router.

CHAP transactions occur only when a link is established. The local router or access server does not request a password during the rest of the call. (The local device can, however, respond to such requests from other devices during a call.)

When PAP is enabled, the remote router attempting to connect to the local router or access server is required to send an authentication request. The username and password specified in the authentication request are accepted, and the Cisco IOS software sends an authentication acknowledgment.

After you have enabled CHAP or PAP, the local router or access server requires authentication from remote devices. If the remote device does not support the enabled protocol, no traffic will be passed to that device.

To use CHAP or PAP, you must perform the following tasks:

- Enable PPP encapsulation.
- Enable CHAP or PAP on the interface.

For CHAP, configure hostname authentication and the secret password for each remote system with which authentication is required.

IP Address Pooling

A point-to-point interface must be able to provide a remote node with its IP address through the IP Control Protocol (IPCP) address negotiation process. The IP address can be obtained from a variety of sources. The address can be configured through the command line, entered with an EXEC-level command, provided by TACACS+ or the Dynamic Host Configuration Protocol (DHCP), or from a locally administered pool.

IP address pooling uses a pool of IP addresses from which an incoming interface can provide an IP address to a remote node through IPCP address negotiation process. IP address pooling also enhances configuration flexibility by allowing multiple types of pooling to be active simultaneously.

The IP address pooling feature allows configuration of a global default address pooling mechanism, per-interface configuration of the address pooling mechanism, and per-interface configuration of a specific address or pool name.

Peer Address Allocation

A peer IP address can be allocated to an interface through several methods:

- Dialer map lookup—This method is used only if the peer requests an IP address, no other peer IP address has been assigned, and the interface is a member of a dialer group.
- PPP EXEC command—An asynchronous dialup user can enter a peer IP address or hostname when PPP is invoked from the command line. The address is used for the current session and then discarded.
- IPCP negotiation—If the peer presents a peer IP address during IPCP address negotiation and no other peer address is assigned, the presented address is acknowledged and used in the current session.
- Default IP address.
- TACACS+ assigned IP address—During the authorization phase of IPCP address negotiation, TACACS+ can return an IP address that the user being authenticated on a dialup interface can use. This address overrides any default IP address and prevents pooling from taking place.
- DHCP retrieved IP address—If configured, the routers acts as a proxy client for the dialup user and retrieves an IP address from a DHCP server. That address is returned to the DHCP server when the timer expires or when the interface goes down.
- Local address pool—The local address pool contains a set of contiguous IP addresses (a maximum of 1024 addresses) stored in two queues. The free queue contains addresses available to be assigned and the used queue contains addresses that are in use. Addresses are stored to the free queue in first-in, first-out (FIFO) order to minimize the chance the address will be reused, and to allow a peer to reconnect using the same address that it used in the last connection. If the address is available, it is assigned; if not, another address from the free queue is assigned.
- Chat script (asynchronous serial interfaces only)—The IP address in the **dialer map** command entry that started the script is assigned to the interface and overrides any previously assigned peer IP address.
- Virtual terminal/protocol translation—The translate command can define the peer IP address for a virtual terminal (pseudo asynchronous interface).
- The pool configured for the interface is used, unless TACACS+ returns a pool name as part of authentication, authorization, and accounting (AAA). If no pool is associated with a given interface, the global pool named default is used.

Precedence Rules

The following precedence rules of peer IP address support determine which address is used. Precedence is listed from most likely to least likely:

1. AAA/TACACS+ provided address or addresses from the pool named by AAA/TACACS+
2. An address from a local IP address pool or DHCP (typically not allocated unless no other address exists)
3. Dialer map lookup address (not done unless no other address exists)
4. Address from an EXEC-level PPP command, or from a chat script
5. Configured address from the **peer default ip address** command or address from the protocol **translate** command
6. Peer-provided address from IPCP negotiation (not accepted unless no other address exists)

MLP on Synchronous Serial Interfaces

Address pooling is available on all synchronous serial interfaces that are running PPP and PPPoX sessions.

MLP provides characteristics are most similar to hardware inverse multiplexers, with good manageability and Layer 3 services support. Figure below shows a typical inverse multiplexing application using two Cisco routers and Multilink PPP over four T1 lines.

How to Configure PPP

The sections below describe how to configure PPP.

Enabling PPP Encapsulation

The `encapsulation ppp` command enables PPP on serial lines to encapsulate IP and other network protocol datagrams.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface serial <i>slot/subslot/port:channel</i> Example: Router(config)# interface serial 0/0/0:0	Enters interface configuration mode.
Step 4	encapsulation ppp Example: Router(config-if) # encapsulation ppp	Enables PPP encapsulation. Note PPP echo requests are used as keepalives to minimize disruptions to the end users of your network. Use the no keepalive command to disable echo requests.
Step 5	end Example:	Exits interface configuration mode.

	Command or Action	Purpose
	Router(config-if)# end	

Enabling CHAP or PAP Authentication

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface serial <i>number</i> Example: Router(config)# interface serial 0/0/0	Enters Interface Configuration mode.
Step 4	ppp authentication {chap chap pap pap chap pap} [if-needed] [list-name default] [callin] Example: Router(config-if)# ppp authentication chap	Defines the authentication methods supported and the order in which they are used. <p>Note</p> <ul style="list-style-type: none"> • Use the ppp authentication chap command only with TACACS or extended TACACS. • With AAA configured on the router and list names defined for AAA, the <i>list-name</i> optional argument can be used with AAA/TACACS+. Use the ppp use-tacacs command with TACACS and Extended TACACS. Use the aaa authentication ppp command with AAA/TACACS+.
Step 5	ppp use-tacacs [single-line] or aaa authentication ppp Example:	Configure TACACS on a specific interface as an alternative to global host authentication.

	Command or Action	Purpose
	<pre>Router(config-if)# ppp use-tacacs single-line Router(config-if)# aaa authentication ppp</pre>	
Step 6	<p>exit</p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.
Step 7	<p>username name [user-maxlinks link-number] password secret</p> <p>Example:</p> <pre>Router(config)# username name user-maxlinks 1 password password1</pre>	<p>Configures identification.</p> <ul style="list-style-type: none"> • Optionally, you can specify the maximum number of connections a user can establish. • To use the user-maxlinks keyword, you must also use the aaa authorization network default local command and PPP encapsulation and name authentication on all the interfaces the user will be accessing.
Step 8	<p>end</p> <p>Example:</p> <pre>Router(config)# end</pre>	<p>Exits global configuration mode and enters privileged EXEC mode.</p> <p>Caution If you use a list name that has not been configured with the aaa authentication ppp command, you disable PPP on the line.</p>

Example

```
Router# configure terminal
Router(config)# interface serial 0/0/0
Router(config-if)# ppp authentication chap
Router(config-if)# aaa authentication ppp
Router(config-if)# exit
Router(config)# username name user-maxlinks 1 password password1
Router(config)# end
```

Configuring IP Address Pooling

You can define the type of IP address pooling mechanism used on router interfaces in one or both of the ways described in the following sections:



Note For more information about address pooling, see the [IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S](#)

Global Default Address Pooling Mechanism

The global default mechanism applies to all point-to-point interfaces that support PPP encapsulation and that have not otherwise been configured for IP address pooling. You can define the global default mechanism to be either DHCP or local address pooling.

To configure the global default mechanism for IP address pooling, perform the tasks in the following sections:

- [Defining DHCP as the Global Default Mechanism](#)
- [Defining Local Address Pooling as the Global Default Mechanism](#)

After you have defined a global default mechanism, you can disable it on a specific interface by configuring the interface for some other pooling mechanism. You can define a local pool other than the default pool for the interface or you can configure the interface with a specific IP address to be used for dial-in peers.

You can also control the DHCP network discovery mechanism; see the following section for more information:

- [Controlling DHCP Network Discovery](#)

Defining DHCP as the Global Default Mechanism

DHCP specifies the following components:

- A DHCP server—A host-based DHCP server configured to accept and process requests for temporary IP addresses.
- A DHCP proxy client—A Cisco access server configured to arbitrate DHCP calls between the DHCP server and the DHCP client. The DHCP client-proxy feature manages a pool of IP addresses available to dial-in clients without a known IP address.

Perform this task to enable DHCP as the global default mechanism.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	ip address-pool dhcp-proxy-client Example: <pre>Router(config)# ip address-pool dhcp-proxy-client</pre>	Specifies the DHCP client-proxy feature as the global default mechanism. <ul style="list-style-type: none"> • The peer default ip address command and the member peer default ip address command can be used to define default peer IP addresses.

	Command or Action	Purpose
		<p>Note You can provide as few as one or as many as ten DHCP servers for the proxy client (the Cisco router or access server) to use. The DHCP servers provide temporary IP addresses.</p>
Step 4	<p>ip dhcp-server [<i>ip-address</i> <i>name</i>]</p> <p>Example:</p> <pre>Router(config)# ip dhcp-server 209.165.201.1</pre>	(Optional) Specifies the IP address of a DHCP server for the proxy client to use.
Step 5	<p>end</p> <p>Example:</p> <pre>Router(config)# end</pre>	Exits global configuration mode.

Defining Local Address Pooling as the Global Default Mechanism

Perform this task to define local address pooling as the global default mechanism.



Note If no other pool is defined, a local pool called “default” is used. Optionally, you can associate an address pool with a named pool group.

Procedure

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>ip address-pool local</p> <p>Example:</p> <pre>Router(config)# ip address-pool local</pre>	Specifies local address pooling as the global default mechanism.

	Command or Action	Purpose
Step 4	<p>ip local pool {<i>named-address-pool</i> default} <i>first-IP-address</i> [<i>last-IP-address</i>] [group <i>group-name</i>] [cache-size <i>size</i>]</p> <p>Example:</p> <pre>Router(config)# ip local pool default 192.0.2.1</pre>	Creates one or more local IP address pools.

Controlling DHCP Network Discovery

Perform the steps in this section to allow peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IPCP extensions.

The **ip dhcp-client network-discovery** global configuration command provides a way to control the DHCP network discovery mechanism. The number of DHCP Inform or Discovery messages can be set to 1 or 2, which determines how many times the system sends the DHCP Inform or Discover messages before stopping network discovery. You can set a timeout period from 3 to 15 seconds, or leave the default timeout period at 15 seconds. The default for the **informs** and **discovers** keywords is 0, which disables the transmission of these messages.



Note For more information about DHCP, see the [IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S](#)

Procedure

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>ip dhcp-client network-discovery <i>informs</i> <i>number-of-messages</i> discovers <i>number-of-messages</i> period <i>seconds</i></p> <p>Example:</p> <pre>Router(config)# ip dhcp-client network-discovery informs 2 discovers 2 period 2</pre>	Provides control of the DHCP network discovery mechanism by allowing the number of DHCP Inform and Discover messages to be sent, and a timeout period for retransmission, to be configured.

Configuring IP Address Assignment

Perform this task to configure IP address alignment.

After you have defined a global default mechanism for assigning IP addresses to dial-in peers, you can configure the few interfaces for which it is important to have a nondefault configuration. You can do any of the following;

- Define a nondefault address pool for use by a specific interface.
- Define DHCP on an interface even if you have defined local pooling as the global default mechanism.
- Specify one IP address to be assigned to all dial-in peers on an interface.
- Make temporary IP addresses available on a per-interface basis to asynchronous clients using PPP.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip local pool { <i>named-address-pool</i> default } { <i>first-IP-address</i> [<i>last-IP-address</i>]} [group <i>group-name</i>] [cache-size <i>size</i>] Example: Router(config)# ip local pool default 192.0.2.0	Creates one or more local IP address pools.
Step 4	interface <i>type number</i> Example: Router(config)# interface ethernet 2/0	Specifies the interface and enters interface configuration mode.
Step 5	peer default ip address pool <i>pool-name-list</i> Example: Router(config-if)# peer default ip address pool 2	Specifies the pool or pools for the interface to use.
Step 6	peer default ip address pool dhcp Example:	Specifies DHCP as the IP address mechanism on this interface.

	Command or Action	Purpose
	Router(config-if)# peer default ip address pool dhcp	
Step 7	peer default ip address ip-address Example: Router(config-if)# peer default ip address 192.0.2.2	Specifies the IP address to assign to all dial-in peers on an interface.

Disabling or Reenabling Peer Neighbor Routes

The Cisco IOS software automatically creates neighbor routes by default; that is, it automatically sets up a route to the peer address on a point-to-point interface when the PPP IPCP negotiation is completed.

To disable this default behavior or to reenale it once it has been disabled, perform the following task:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Enters global configuration mode.	
Step 3	interface type number Example: Router(config)# interface ethernet 0/1	Specifies the interface and enters interface configuration mode.
Step 4	no peer neighbor-route Example: Router(config-if)# no peer neighbor-route	Disables creation of neighbor routes.
Step 5	peer neighbor-route Example: Router(config-if)# peer neighbor-route	Reenables creation of neighbor routes. Note If entered on a dialer or asynchronous group interface, this command affects all member interfaces.

Configuring Multilink PPP

The Multilink PPP feature provides load balancing functionality over multiple WAN links, while providing multivendor interoperability, packet fragmentation and proper sequencing, and load calculation on both inbound and outbound traffic. The Cisco implementation of MLP supports the fragmentation and packet sequencing specifications in RFC 1990. Additionally, you can change the default endpoint discriminator value that is supplied as part of user authentication. Refer to RFC 1990 for more information about the endpoint discriminator.

MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address. The multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound traffic, outbound traffic, or on either, as needed for the traffic between the specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP is designed to work over synchronous and asynchronous serial and BRI and PRI types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

Perform the tasks in the following sections, as required for your network, to configure MLP:

Configuring MLP on Synchronous Interfaces

To configure Multilink PPP on synchronous interfaces, you configure the synchronous interfaces to support PPP encapsulation and Multilink PPP.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface serial <i>number</i> Example: Router(config)# interface serial 0/0/1	Specifies an asynchronous interface and enters interface configuration mode.
Step 4	no ip address Example: Router(config-if)# no ip address	Specifies no IP address for the interface.
Step 5	encapsulation ppp Example:	Enables PPP encapsulation.

	Command or Action	Purpose
	<code>Router(config-if)# encapsulation ppp</code>	
Step 6	ppp multilink Example: <code>Router(config-if)# ppp multilink</code>	Enables Multilink PPP.
Step 7	pulse-time <i>seconds</i> Example: <code>Router(config-if)# pulse-time 60</code>	Enables pulsing data terminal ready (DTR) signal intervals on an interface. Note Repeat these steps for additional synchronous interfaces, as needed.

Configuring a Multilink Group

A multilink group allows you to assign multiple interfaces to a multilink bundle. When the **ppp multilink group** command is configured on an interface, the interface is restricted from joining any interface but the designated multilink group interface. If a peer at the other end of the interface tries to join a different multilink group, the connection is severed. This restriction applies when Multilink PPP (MLP) is negotiated between the local end and the peer system. The interface can still come up as a regular PPP interface.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	interface multilink <i>group-number</i> Example: <code>Router(config)# interface multilink 2</code>	Creates a multilink bundle and enters interface configuration mode to configure the bundle.
Step 4	ip address <i>address mask</i> Example: <code>Router(config-if)# ip address 192.0.2.1 255.255.255.224</code>	Sets a primary IP address for an interface.
Step 5	encapsulation ppp Example:	Enables PPP encapsulation.

	Command or Action	Purpose
	<code>Router(config-if)# encapsulation ppp</code>	
Step 6	ppp chap hostname <i>hostname</i> Example: <code>Router(config-if)# ppp chap hostname host1</code>	Specifies the hostname on the interface.
Step 7	exit Example: <code>Router(config-if)# exit</code>	Exits interface configuration mode.
Step 8	interface <i>type number</i> Example: <code>Router(config)# interface serial 0/0/1</code>	Enters interface configuration mode.
Step 9	ppp multilink group <i>group-number</i> Example: <code>Router(config-if)# ppp multilink group 2</code>	Restricts a physical link to joining only a designated multilink group interface.
Step 10	exit Example: <code>Router(config-if)# exit</code>	Exits interface configuration mode.

Configuring PFC and ACFC

Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (ACFC) are PPP compression methods defined in RFCs 1661 and 1662. PFC allows for compression of the PPP Protocol field; ACFC allows for compression of the PPP Data Link Layer Address and Control fields.

Configuring ACFC

Follow these steps to configure ACFC handling during PPP negotiation

Procedure

	Command or Action	Purpose
Step 1	enable Example: <code>Router> enable</code>	

	Command or Action	Purpose
	Enables privileged EXEC mode. Enter your password if prompted.	
Step 2	configure terminal Example: <pre>Router# configure terminal</pre> Enters global configuration mode.	
Step 3	interface multilink <i>number</i> Example: <pre>Router(config)# interface multilink 2</pre>	Select a multilink interface.
Step 4	ppp acfc local {request forbid} Example: <pre>Router(config-if)# ppp acfc local request</pre>	Configure how the router handles ACFC in its outbound configuration requests where: <ul style="list-style-type: none"> • request—The ACFC option is included in outbound configuration requests. • forbid—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.
Step 5	ppp acfc remote {apply reject ignore} Example: <pre>Router(config-if)# ppp acfc remote apply</pre>	Configure how the router handles the ACFC option in configuration requests received from a remote peer where: <ul style="list-style-type: none"> • apply—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer. • reject—ACFC options are explicitly ignored. • ignore—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.
Step 6	exit Example: <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.

Configuring PFC

Follow these steps to configure PFC handling during PPP negotiation:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre> Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. 	
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface multilink <i>number</i> Example: <pre>Router(config)# interface multilink 2</pre>	Select a multilink interface.
Step 4	ppp pfc local {request forbid} Router(config-if)# ppp pfc local request	Configure how the router handles PFC in its outbound configuration requests where: <ul style="list-style-type: none"> • request—The PFC option is included in outbound configuration requests. • forbid—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.
Step 5	ppp pfc remote {apply reject ignore} Example: <pre>Router(config-if)# ppp pfc remote apply</pre>	Configure a method for the router to use to manage the PFC option in configuration requests received from a remote peer where: <ul style="list-style-type: none"> • apply—PFC options are accepted and PFC may be performed on frames sent to the remote peer. • reject—PFC options are explicitly ignored. • ignore—PFC options are accepted, but PFC is not performed on frames sent to the remote peer.
Step 6	exit Example: <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.

Changing the Default Endpoint Discriminator

By default, when the system negotiates use of MLP with the peer, the value that is supplied for the endpoint discriminator is the same as the username used for authentication. That username is configured for the interface by the Cisco IOS **ppp chap hostname** or **ppp pap sent-username** command, or defaults to the globally configured hostname (or stack group name, if this interface is a Stack Group Bidding Protocol, or SGBP, group member).

Perform this task to override or change the default endpoint discriminator.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface virtual template <i>number</i> Example: <pre>Router(config)# interface virtual template 1</pre>	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode.
Step 4	ppp multilink endpoint {hostname ip ipaddress mac LAN-interface none phone telephone-number string char-string} Example: <pre>Router(config-if)# ppp multilink endpoint ip 192.0.2.0</pre>	Overrides or changes the default endpoint discriminator the system uses when negotiating the use of MLP with the peer.

Creating a Multilink Bundle

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface multilink <i>group-number</i> Example: Router(config)# interface multilink 10	Assigns a multilink group number and enters interface configuration mode.
Step 4	ip address <i>address mask</i> Example: Router(config-if)# ip address 192.0.2.9 255.255.255.224	Assigns an IP address to the multilink interface.
Step 5	encapsulation ppp Example: Router(config-if)# encapsulation ppp	Enables PPP encapsulation.
Step 6	ppp multilink Example: Router(config-if)# ppp multilink	Enables Multilink PPP.

Assigning an Interface to a Multilink Bundle



Caution Do not install a router to the peer address while configuring an MLP lease line. This installation can be disabled when **no ppp peer-neighbor-route** command is used under the MLPPP bundle interface.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface multilink <i>group-number</i> Example: Router(config)# interface multilink 10	Assigns a multilink group number and enters interface configuration mode.
Step 4	no ip address Example: Router(config-if)# no ip address	Removes any specified IP address.
Step 5	keepalive Example: Router(config-if)# keepalive	Sets the frequency of keepalive packets.
Step 6	encapsulation ppp Example: Router(config-if)# encapsulation ppp	Enables PPP encapsulation.
Step 7	ppp multilink group <i>group-number</i> Example: Router(config-if)# ppp multilink 12	Restricts a physical link to joining only the designated multilink-group interface.
Step 8	ppp multilink Example: Router(config-if)# ppp multilink	Enables Multilink PPP.
Step 9	ppp authentication chap Example: Router(config-if)# ppp authentication chap	(Optional) Enables CHAP authentication.
Step 10	pulse-time <i>seconds</i> Example: Router(config-if)# pulse-time 10	(Optional) Configures DTR signal pulsing.

Configuring PPP/MLP MRRU Negotiation Configuration on Multilink Groups

In this task, you configure MRRU negotiation on the multilink interface. The bundle interface is static, that is, always available.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface multilink <i>number</i> Example: <pre>Router(config)# interface multilink 10</pre>	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: <pre>Router(config-if)# ip address 10.13.1.1 255.255.255.0</pre>	Sets the IP address for the interface.
Step 5	ppp multilink mrru [local remote] <i>mrru-value</i> Example: <pre>Router(config-if)# ppp multilink mrru local 1600</pre>	Configures the MRRU value negotiated on a multilink bundle when MLP is used. <ul style="list-style-type: none"> • local—(Optional) Configures the local MRRU value. The default values for the local MRRU are the value of the multilink group interface MTU for multilink group members, and 1524 bytes for all other interfaces. • remote—(Optional) Configures the minimum value that the software will accept from the peer when it advertises its MRRU. By default, the software accepts any peer MRRU value of 128 or higher. You can specify a higher minimum acceptable MRRU value in a range from 128 to 16384 bytes.
Step 6	mtu bytes Example: <pre>Router(config-if)# mtu 1600</pre>	(Optional) Adjusts the maximum packet size or MTU size. <ul style="list-style-type: none"> • Once you configure the MRRU on the bundle interface, you enable the router to receive large reconstructed MLP frames. You may want to configure the bundle MTU so the router can transmit large

	Command or Action	Purpose
		<p>MLP frames, although it is not strictly necessary.</p> <ul style="list-style-type: none"> The maximum recommended value for the bundle MTU is the value of the peer's MRRU. The default MTU for serial interfaces is 1500. The software will automatically reduce the bundle interface MTU if necessary, to avoid violating the peer's MRRU.
Step 7	<p>exit</p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.
Step 8	<p>interface serial <i>slot/port</i></p> <p>Example:</p> <pre>Router(config)# interface serial 0/0</pre>	Selects a serial interface to configure and enters interface configuration mode.
Step 9	<p>ppp multilink</p> <p>Example:</p> <pre>Router(config-if)# ppp multilink</pre>	Enables MLP on the interface.
Step 10	<p>ppp multilink group <i>group-number</i></p> <p>Example:</p> <pre>Router(config-if)# ppp multilink group 1</pre>	Restricts a physical link to joining only a designated multilink-group interface.
Step 11	<p>mtu <i>bytes</i></p> <p>Example:</p> <pre>Router(config-if)# mtu 1600</pre>	<p>(Optional) Adjusts the maximum packet size or MTU size.</p> <ul style="list-style-type: none"> The default MTU for serial interfaces is 1500. When the bundle interface MTU is tuned to a higher number, then depending upon the fragmentation configuration, the link interface may be given larger frames to transmit. You must ensure that fragmentation is performed such that fragments are sized less than the link interface MTU (refer to command pages for the ppp multilink fragmentation and ppp multilink fragment-delay commands for more

	Command or Action	Purpose
		information about packet fragments), or configure the MTUs of the link interfaces such that they can transmit the larger frames.
Step 12	exit Example: <pre>Router(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.

Disabling PPP Multilink Fragmentation

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface multilink <i>group-number</i> Example: <pre>Router(config)# interface multilink 10</pre>	Assigns a multilink group number and enters interface configuration mode.
Step 4	ppp multilink fragment disable Example: <pre>Router(config-if)# ppp multilink fragment disable</pre>	(Optional) Disables PPP multilink fragmentation.
Step 5	exit Example: <pre>Router(config-if)# exit</pre>	Exits privileged EXEC mode.

Troubleshooting Tips

Use the **debug ppp negotiation** command to verify and troubleshoot MRRU negotiation on multilink groups. Use the **show interface** command to verify MRRU negotiation on the interfaces.

For more information about configuring MRRU and MTU values, see the [Wide-Area Networking Configuration Guide: Multilink PPP, Cisco IOS XE Release 3S](#).

Troubleshooting PPP

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. You can determine whether Link Access Procedure, Balanced (LAPB) has been established on a connection by using the **show interface** command.

Monitoring and Maintaining PPP and MLP Interfaces

You can use the **show ppp multilink** command to display MLP bundle information.

For more information about configuring MLPPP interfaces, see the [Wide-Area Networking Configuration Guide: Multilink PPP, Cisco IOS XE Release 3S](#).