Configuring Media-Independent PPP and Multilink PPP

Last Updated: October 7, 2011

This module describes how to configure the PPP and Multilink PPP (MLP) features that can be configured on any interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Media-Independent PPP and Multilink PPP

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

PPP Encapsulation Overview

PPP, described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on the following types of physical interfaces:

- Asynchronous serial
- High-Speed Serial Interface (HSSI)
- Synchronous serial

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.

Multilink PPP

The Multilink PPP feature provides load balancing functionality over multiple WAN links while providing multivendor interoperability, packet fragmentation, 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 types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

Multilink PPP Minimum Links Mandatory

Multilink PPP allows multiple PPP links to be established in parallel to the same destination. Multilink PPP is often used to increase the amount of bandwidth between points. The Multilink PPP Minimum Links Mandatory feature enables you to configure the minimum number of links in a Multilink PPP (MLP) bundle required to keep that bundle active.

The Multilink PPP Minimum Links Mandatory feature causes all Network Control Protocols (NCPs) for an MLP bundle to be disabled until the MLP bundle has the required minimum number of links. When a new link is added to the MLP bundle that brings the number of links up to the required minimum number of links, the NCPs are activated for the MLP bundle. When a link is removed from an MLP bundle, and the number of links falls below the required minimum number of links for that MLP bundle, the NCPs are disabled for that MLP bundle.

CHAP or PAP 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 is 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 host name 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 host name 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 host name 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. If the username and password specified in the authentication request are accepted, the Cisco IOS or Cisco IOS XE 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.

Microsoft Point-to-Point Compression

Microsoft Point-to-Point Compression (MPPC) is a scheme used to compress PPP packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ)-based algorithm with a continuous history buffer called a dictionary.

The Compression Control Protocol (CCP) configuration option for MPPC is 18.

Exactly one MPPC datagram is encapsulated in the PPP information field. The PPP protocol field indicates the hexadecimal type of 00FD for all compressed datagrams. The maximum length of the MPPC datagram sent over PPP is the same as the MTU of the PPP interface; however, this length cannot be greater than

8192 bytes because the history buffer is limited to 8192 bytes. If compressing the data results in data expansion, the original data is sent as an uncompressed MPPC packet.

The history buffers between compressor and decompressor are synchronized by maintaining a 12-bit coherency count. If the decompressor detects that the coherency count is out of sequence, the following error recovery process is performed:

1. Reset Request (RR) packet is sent from the decompressor.
2. The compressor then flushes the history buffer and sets the flushed bit in the next packet it sends.
3. Upon receiving the flushed bit set packet, the decompressor flushes the history buffer.

Synchronization is achieved without CCP using the Reset Acknowledge (RA) packet, which can consume additional time.

Compression negotiation between a router and a Windows 95 client occurs through the following process:

1. Windows 95 sends a request for both STAC (option 17) and MPPC (option 18) compression.
2. The router sends a negative acknowledgment (NAK) requesting only MPPC.
3. Windows 95 resends the request for MPPC.
4. The router sends an acknowledgment (ACK) confirming MPPC compression negotiation.

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.

See the chapter "Configuring Asynchronous SLIP and PPP" in this publication for additional information about address pooling on asynchronous interfaces and about the Serial Line Internet Protocol (SLIP).

Peer Address Allocation

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

- 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--The **peer default ip address** command and the **member peer default ip address** command can be used to define default peer IP addresses.
- 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.

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. Configured address from the **peer default ip address** command or address from the protocol **translate** command
4. Peer provided address from IPCP negotiation (not accepted unless no other address exists)

Interfaces Affected

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

PPP Half-Bridging

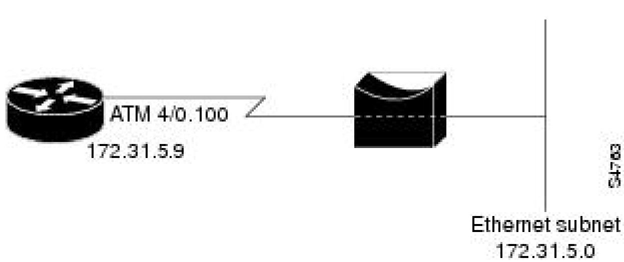
For situations in which a routed network needs connectivity to a remote bridged Ethernet network, a serial interface can be configured to function as a PPP half-bridge. The line to the remote bridge functions as a virtual Ethernet interface, and the serial interface on the router functions as a node on the same Ethernet subnetwork as the remote network.

The bridge sends bridge packets to the PPP half-bridge, which converts them to routed packets and forwards them to other router processes. Likewise, the PPP half-bridge converts routed packets to Ethernet bridge packets and sends them to the bridge on the same Ethernet subnetwork.

Note An interface cannot function as both a half-bridge and a bridge.

The figure below shows a router with an interface configured as a PPP half-bridge. The interface functions as a node on the Ethernet subnetwork with the bridge. Note that the interface has an IP address on the same Ethernet subnetwork as the bridge.

Figure 1 Router Interface Configured as a Half-Bridge



Note The Cisco IOS XE software supports no more than one PPP half-bridge per Ethernet subnetwork.

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.

MLP Interleaving and Queueing

Interleaving on MLP allows large packets to be multilink encapsulated and fragmented into a small enough size to satisfy the delay requirements of real-time traffic; small real-time packets are not multilink encapsulated and are sent between fragments of the large packets. The interleaving feature also provides a special transmit queue for the smaller, delay-sensitive packets, enabling them to be sent earlier than other flows.

Weighted fair queueing on MLP works on the packet level, not at the level of multilink fragments. Thus, if a small real-time packet gets queued behind a larger best-effort packet and no special queue has been reserved for real-time packets, the small packet will be scheduled for transmission only after all the fragments of the larger packet are scheduled for transmission.

Weighted fair queueing is supported on all interfaces that support Multilink PPP, including MLP virtual access interfaces and virtual interface templates. Weighted fair-queueing is enabled by default.

Interleaving applies only to interfaces that can configure a multilink bundle interface.

Multilink and fair queueing are not supported when a multilink bundle is off-loaded to a different system using Multichassis Multilink PPP (MMP). Thus, interleaving is not supported in MMP networking designs.

How to Configure Media-Independent PPP and Multilink PPP

Enabling PPP Encapsulation

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface fastethernet** *number*
4. **encapsulation ppp**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface fastethernet** *number* **Example:** `Router(config)# interface fastethernet 0/0`	Enters interface configuration mode.

	Command or Action	Purpose

Step 4	**encapsulation ppp**
	
	Example:
	
	`Router`
	`(config-if)`
	` # encapsulation ppp`
		Enables PPP encapsulation.

Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Enabling CHAP or PAP Authentication

To enable CHAP or PAP authentication, perform the steps mentioned in this section.

Caution

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

For an example of CHAP, see the section CHAP with an Encrypted Password Examples, page 41". CHAP is specified in RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)* .

For information about MS-CHAP, see MS-CHAP Support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface fastethernet** *number*
4. **ppp authentication** {**chap** | **chap pap** | **pap chap** | **pap**} [**if-needed**] [*list-name* | **default**] [**callin**]
5. Do one of the following:
   - **ppp use-tacacs** [**single-line**]
   -
   - **aaa authentication ppp**
6. **exit**
7. **username** *name* [**user-maxlinks** *link-number*] **password** *secret*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface fastethernet** *number* **Example:** `Router(config)# interface fastethernet 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.
		
		Note Use the **ppp authentication chap** command only with TACACS or extended TACACS.
		
		Note With AAA configured on the router and list names defined for AAA, the *list-name* 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+.

	Command or Action	Purpose

Step 5	Do one of the following:
	• **ppp use-tacacs** [**single-line**]
	•
	• **aaa authentication ppp**
	
	Example:
	`Router(config-if)# ppp use-tacacs single-line`
	
	Example:
	
	Example:
	`Router(config-if)# aaa authentication ppp`
		Configure TACACS on a specific interface as an alternative to global host authentication.

Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	**username** *name* [**user-maxlinks** *link-number*] **password** *secret* **Example:** `Router(config)# username name user-maxlinks 1 password password1`	Configures identification. • 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	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Enabling Link Quality Monitoring

Link Quality Monitoring (LQM) is available on all serial interfaces running PPP. LQM will monitor the link quality, and if the quality drops below a configured percentage, the router will shut down the link. The percentages are calculated for both the incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent with 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 with the total number of packets and bytes sent by the destination peer.

Note LQM is not compatible with Multilink PPP.

When LQM is enabled, Link Quality Reports (LQRs) are sent, in place of keepalives, every keepalive period. All incoming keepalives are responded to properly. If LQM is not configured, keepalives are sent every keepalive period and all incoming LQRs are responded to with an LQR.

LQR is specified in RFC 1989, *PPP Link Quality Monitoring* .

To enable LQM on the interface, use the following command in interface configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface fastethernet** *number*
4. **ppp quality** *percentage*
5. **exit**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface fastethernet** *number* **Example:** `Router(config)# interface fastethernet 0/0`	Enters Interface Configuration mode.

	Command or Action	Purpose
Step 4	**ppp quality** *percentage* **Example:** `Router(config-if)# ppp quality 10`	Enables LQM on the interface. • *percentage* --Specifies the link quality threshold. The percentage must be maintained, or the link is deemed to be of poor quality and is taken down.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 6	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring Compression of PPP Data

You can configure point-to-point software compression on serial interfaces that use PPP encapsulation. Compression reduces the size of a PPP frame via lossless data compression. PPP encapsulations support both predictor and Stacker compression algorithms.

If most of your traffic is already compressed files, do not use compression.

To configure software compression, perform the following task:

Software compression is available in all router platforms. Software compression is performed by the main processor in the router.

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

To configure compression over PPP, use the following commands in interface configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface fastethernet** *number*
4. **encapsulation ppp**
5. **compress** [**predictor** | **stac**| **mppc**[**ignore-pfc**]]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface fastethernet** *number* **Example:** `Router(config)# interface fastethernet 0/0`	Enters interface configuration mode.
Step 4	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Enables encapsulation of a single protocol on the serial line.
Step 5	**compress** [**predictor** | **stac**| **mppc**[**ignore-pfc**]] **Example:** `Router(config-if)# compress predictor`	Enables compression.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Configuring Microsoft Point-to-Point Compression

Perform this task to configure MPCC. This will help you set MPPC once PPP encapsulation is configured on the router.

Ensure that PPP encapsulation is enabled before you configure MPPC.

Note

The following restrictions apply to the MPPC feature:

- MPPC is supported only with PPP encapsulation.
- Compression can be processor intensive because it requires a reserved block of memory to maintain the history buffer. Do not enable modem or hardware compression because it may cause performance degradation, compression failure, or data expansion.
- Both ends of the point-to-point link must be using the same compression method (STAC, Predictor, or MPPC, for example).

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial** *number*
4. **compress** [**mppc**[**ignore-pfc**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface serial** *number* **Example:** `Router(config)# interface serial 2/0`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**compress** [**mppc**[**ignore-pfc**]] **Example:** `Router(config-if)# compress mppc`	Enables encapsulation of a single protocol on the serial line. • The **ignore-pfc** keyword instructs the router to ignore the protocol field compression flag negotiated by Link Control Protocol (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 that use an uncompressed protocol field (0x0021), even though the protocol field compression is negotiated between peers.

Example

Following is sample **debug ppp negotiation** command output showing protocol reject:

```
PPP Async2: protocol reject received for protocol = 0x2145
PPP Async2: protocol reject received for protocol = 0x2145
PPP Async2: protocol reject received for protocol = 0x2145
```

Configuring IP Address Pooling

Choosing the IP Address Assignment Method

The IP address pooling feature now 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.

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:

Defining the 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.

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.

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.

To enable DHCP as the global default mechanism, use the following commands in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip address-pool dhcp-proxy-client**
4. **ip dhcp-server** [*ip-address* | *name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip address-pool dhcp-proxy-client** **Example:** `Router(config)# ip address-pool dhcp-proxy-client`	Specifies the DHCP client-proxy feature as the global default mechanism. • The **peer default ip address** command and the **member peer default ip address** command can be used to define default peer IP addresses. **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.

	Command or Action	Purpose
Step 4	**ip dhcp-server** [*ip-address* | *name*] **Example:** `Router(config)# ip dhcp-server 209.165.201.1`	(Optional) Specifies the IP address of a DHCP server for the proxy client to use.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Defining 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.

To specify that the global default mechanism to use is local pooling, use the following commands in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip address-pool local**
4. **ip local pool** {*named-address-pool* | **default**} *first-IP-address* [*last-IP-address*] [*group group-name*] [**cache-size** *size*]

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip address-pool local** **Example:** `Router(config)# ip address-pool local`	Specifies local address pooling as the global default mechanism.
Step 4	**ip local pool** {*named-address-pool* | **default**} *first-IP-address* [*last-IP-address*] [*group group-name*] [**cache-size** *size*] **Example:** `Router(config)# ip local pool default 192.0.2.1`	Creates one or more local IP address pools.

Controlling DHCP Network Discovery

To allow peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IP Control Protocol (IPCP) extensions, use the following command in global configuration mode:

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp-client network-discovery informs** *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp-client network-discovery informs** *number-of-messages* **discovers** *number-of-messages* **period** *seconds* **Example:** `Router(config)# ip dhcp-client network-discovery informs 2 discovers 2 period 2`	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

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 SLIP or PPP.

To define a nondefault address pool for use on an interface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip local pool** {*named-address-pool* | **default**} {*first-IP-address* [*last-IP-address*]} [**group** *group-name*] [**cache-size** *size*]}
4. **interface** *type number*
5. **peer default ip address pool** *pool-name-list*
6. **peer default ip address pool dhcp**
7. **peer default ip address** *ip-address*

DETAILED STEPS

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

Configuring PPP Reliable Link

PPP reliable link is Cisco's implementation of RFC 1663, *PPP Reliable Transmission* , which defines a method of negotiating and using Numbered Mode Link Access Procedure, Balanced (LAPB) to provide a reliable serial link. Numbered Mode LAPB provides retransmission of error packets across the serial link.

Although LAPB protocol overhead consumes some bandwidth, you can offset that consumption by the use of PPP compression over the reliable link. PPP compression is separately configurable and is not required for use of a reliable link.

Note PPP reliable link is available only on synchronous serial interfaces. PPP reliable link cannot be used over V.120, and does not work with Multilink PPP.

To configure PPP reliable link on a specified interface, use the following command in interface configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ppp reliable-link**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 2/0`	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ppp reliable-link** **Example:** `Router(config-if)# peer default ip address pool 2`	Enables PPP reliable link. **Note** Having reliable links enabled 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.

- Troubleshooting PPP, page 22

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 LAPB has been established on a connection by using the **show interface** command.

Disabling or Reenabling Peer Neighbor Routes

Cisco IOS XE 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 reenable it once it has been disabled, use the following commands in interface configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no peer neighbor-route**
5. **peer neighbor-route**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**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 PPP Half-Bridging

To configure a serial interface to function as a half-bridge, use the following commands beginning in global configuration mode as appropriate for your network:

or

appletalk address *network.node*

or

appletalk cable-range *cable-range network.node*

or

ipx network *network*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ppp bridge appletalk**
   -
   - **ppp bridge ip**
   -
   - **ppp bridge ipx** [**novell-ether** | **arpa** | **sap** | **snap**]
5. Do one of the following:
   - **ip address** *n.n.n.n*
   -
   - **appletalk address** *network.node*
   -
   - **appletalk cable-range** *cable-range network.node*
   -
   - **ipx network** *network*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/1`	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose

Step 4	Do one of the following:
	• **ppp bridge appletalk**
	•
	• **ppp bridge ip**
	•
	• **ppp bridge ipx** [**novell-ether** | **arpa** | **sap** | **snap**]
	
	Example:
	`Router(config-if)`
	` ppp bridge ipx novell-ether`
		Enables PPP half-bridging for one or more routed protocols: AppleTalk, IP, or Internet Protocol Exchange (IPX).
		Note You must enter the **ppp bridge** command either when the interface is shut down or before you provide a protocol address for the interface.

Step 5	Do one of the following:
	• **ip address** *n.n.n.n*
	•
	• **appletalk address** *network.node*
	•
	• **appletalk cable-range** *cable-range network.node*
	•
	• **ipx network** *network*
	
	Example:
	`Router(config-if)`
	` ipx network abc`
		Provides a protocol address on the same subnetwork as the remote network.

Configuring Multilink PPP

Configuring MLP on Synchronous Interfaces

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

To configure a synchronous interface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial** *number*
4. **no ip address**
5. **encapsulation ppp**
6. **ppp multilink**
7. **pulse-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface serial** *number* **Example:** `Router(config)# interface serial 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:
	
	`Router(config-if)#`
	`encapsulation ppp`
		Enables PPP encapsulation.

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

Creating a Multilink Bundle

To create a multilink bundle, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multilink** *group-number*
4. **ip address** *address mask*
5. **encapsulation ppp**
6. **ppp multilink**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 10`	Assigns a multilink group number and enters interface configuration mode.

Step 4	**ip address** *address mask*
	
	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 MLPP lease line. This can be disabled using the **no ppp peer-neighbor-route** command under the MLPPP bundle interface.

Perform this task to assign an interface to a multilink bundle.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multilink** *group-number*
4. **no ip address**
5. **keepalive**
6. **encapsulation ppp**
7. **ppp multilink group** *group-number*
8. **ppp multilink**
9. **ppp authentication chap**
10. **pulse-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *group-number* **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.

	Command or Action	Purpose
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** *group-number* **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** *seconds* **Example:** `Router(config-if)# pulse-time 10`	(Optional) Configures DTR signal pulsing.

Configuring MLP Using Multilink Group Interfaces

MLP can be configured by assigning a multilink group to a virtual template configuration. Virtual templates allow a virtual access interface to dynamically clone interface parameters from the specified virtual template. If a multilink group is assigned to a virtual template, and then the virtual template is assigned to a physical interface, all links that pass through the physical interface will belong to the same multilink bundle.

Note If a multilink group interface has one member link, the amount of bandwidth available will not change when a multilink interface is shut down. Therefore, you can shut down the multilink interface by removing its link.

A multilink group interface configuration will override a global multilink virtual template configured with the **multilink virtual template** command.

Multilink group interfaces can be used with ATM, PPP over Frame Relay, and serial interfaces.

To configure MLP using a multilink group interface, perform the following tasks:

- Configure the multilink group.
- Assign the multilink group to a virtual template.
- Configure the physical interface to use the virtual template.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multilink** *group-number*
4. **ip address** *address mask*
5. **encapsulation ppp**
6. **exit**
7. **interface virtual template** *number*
8. **ppp multilink group** *group-number*
9. **exit**
10. **interface atm** *interface-number.subinterface-number* **point-to-point**
11. **pvc** *vpi* / *vci*
12. **protocol ppp virtual-template** *name*
13. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 2`	Creates a multilink bundle and enters interface configuration mode to configure the bundle.

Step 4	**ip address** *address mask*
	
	Example:
	
	`R`
	`outer(config-if)#`
	` ip address 192.0.2.1 255.255.255.224`
		Sets a primary IP address for an interface.

Step 5	**encapsulation ppp**
	
	Example:
	
	`R`
	`outer(config-if)#`
	` encapsulation ppp`
		Enables PPP encapsulation.

Step 6	**exit**
	
	Example:
	
	`R`
	`outer(config-if)#`
	` exit`
		Exits interface configuration mode.

Step 7	**interface virtual template** *number* **Example:** `Router(config)# interface virtual template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, and enters interface configuration mode.

	Command or Action	Purpose

Step 8	**ppp multilink group** *group-number*
	
	Example:
	
	`R`
	`outer(config-if)#`
	` ppp multilink group 2`
		Restricts a physical link to joining only a designated multilink group interface.

Step 9	**exit**
	
	Example:
	
	`R`
	`outer(config-if)#`
	` exit`
		Exits interface configuration mode.

Step 10	**interface atm** *interface-number.subinterface-number* **point-to-point** **Example:** `Router(config)# interface atm 1.2 point-to-point`	Configures an ATM interface and enters interface configuration mode.

Step 11	**pvc** *vpi* / *vci*
	
	Example:
	
	`R`
	`outer(config-if)#`
	` pvc 1/100`
		Creates or assigns a name to an ATM permanent virtual circuit (PVC), specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode.

Step 12	**protocol ppp virtual-template** *name*
	
	Example:
	
	`Router(config-if-atm-vc)# protocol ppp virtual-`
	`template 2`
		Configures VC multiplexed encapsulation on a PVC.

Step 13	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM virtual circuit configuration mode.

Configuring Multilink PPP Minimum Links Mandatory

Perform this task to configure the minimum number of links in an MLP bundle required to keep that bundle active.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ppp multilink**
4. **ppp multilink min-links** *links* **mandatory**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables MLP.
Step 4	**ppp multilink min-links** *links* **mandatory** **Example:** `Router(config-if)# ppp multilink min-links 5 mandatory`	Specifies the required minimum number of links in a Multilink PPP (MLP) bundle. • If the minimum number of links in the MLP bundle falls below the number specified by the *links* argument, the MLP bundle is disabled. • *links* --Minimum number of links, in the range from 0 to 255.

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 host name (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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual template** *number*
4. **ppp multilink endpoint** {**hostname** | **ip** *ipaddress* | **mac** *LAN-interface* | **none** | **phone** *telephone-number* | **string** *char-string*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual template** *number* **Example:** `Router(config)# interface virtual template 1`	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:** `Router(config-if)# ppp multilink endpoint ip 192.0.2.0`	Overrides or changes the default endpoint discriminator the system uses when negotiating the use of MLP with the peer.

Configuring MLP Interleaving and Queueing

MLP support for interleaving can be configured on virtual templates. To configure interleaving, complete the following tasks:

- Configure the virtual template.
- Configure MLP and interleaving on the interface or template.

Note Fair queueing, which is enabled by default, must remain enabled on the interface.

- Configuring MLP Interleaving, page 36
- Disabling PPP Multilink Fragmentation, page 38

Configuring MLP Interleaving

Note Interleaving statistics can be displayed by using the **show interfaces** command, specifying the particular interface on which interleaving is enabled. Interleaving data is displayed only if there are interleaves. For example, the following line shows interleaves: Output queue: 315/64/164974/31191 (size/threshold/drops/interleaves)

Perform this task to configure MLP Interleaving.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual template** *number*
4. **ppp multilink**
5. **ppp multilink interleave**
6. **ppp multilink fragment delay** *milliseconds*
7. **ip rtp reserve** *lowest-udp-port range-of-ports* [*maximum-bandwidth*]
8. **exit**
9. **multilink virtual-template** *virtual-template-number*

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface virtual template** *number* **Example:** `Router(config)# interface virtual template 1`	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**
	
	Example:
	
	`Router(config-if)#`
	` ppp multilink`
		Enables Multilink PPP.

Step 5	**ppp multilink interleave**
	
	Example:
	
	`Router(config-if)#`
	` configure terminal`
		Enables interleaving of packets among the fragments of larger packets on an MLP bundle.

Step 6	**ppp multilink fragment delay** *milliseconds*
	
	Example:
	
	`Router(config-if)#`
	` ppp multilink fragment delay 50`
		Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.

Step 7	**ip rtp reserve** *lowest-udp-port range-of-ports* [*maximum-bandwidth*]
	
	Example:
	
	`Router(config-if)#`
	` ip rtp reserve 1 2`
		Reserves a special queue for real-time packet flows to specified destination UDP ports, allowing real-time traffic to have higher priority than other flows.

Step 8	**exit**
	
	Example:
	
	`Router(config-if)#`
	` exit`
		Exits interface configuration mode.

Step 9	**multilink virtual-template** *virtual-template-number* **Example:** `Router(config)# multilink virtual-template 1`	For virtual templates only, applies the virtual template to the multilink bundle. **Note** This step is not used for ISDN or dialer interfaces.

Disabling PPP Multilink Fragmentation

Perform the following task to disable PPP multilink fragmentation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multilink** *group-number*
4. **ppp multilink fragment disable**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 10`	Assigns a multilink group number and enters interface configuration mode.

Step 4	**ppp multilink fragment disable**
	
	Example:
	
	`Router(config-if)#`
	` ppp multilink fragment disable`
		(Optional) Disables PPP multilink fragmentation.

Step 5	**exit**
	
	Example:
	
	`Router(config-if)#`
	` exit`
		Exits privileged EXEC mode.

Monitoring and Maintaining PPP and MLP Interfaces

Perform this task to display MLP and MMP bundle information.

SUMMARY STEPS

1. **enable**
2. **show ppp multilink**
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ppp multilink** **Example:** `Router# show ppp multilink`	Displays MLP and MMP bundle information.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Configuration Examples for PPP and MLP

Multilink PPP with Traffic Shaping Example

The following example shows the configuration of multilink PPP with traffic shaping and QoS. In this example two bundles, with four links in each bundle, are configured between two devices. The **ppp chap**

hostname command entries are required for originating and terminating multiple bundles on a single pair of devices.

```
controller T3 0/3/1
 framing c-bit
 cablelength 224
 t1 1 channel-group 0 timeslots 1-24
 t1 2 channel-group 0 timeslots 1-24
 t1 3 channel-group 0 timeslots 1-24
 t1 4 channel-group 0 timeslots 1-24
 t1 5 channel-group 0 timeslots 1-24
 t1 6 channel-group 0 timeslots 1-24
 t1 7 channel-group 0 timeslots 1-24
 t1 8 channel-group 0 timeslots 1-24
!
class-map match-all DETERMINISTICOUT
  match ip precedence 3
class-map match-all VOICEVIDEOCONTROLOUT
  match ip precedence 2
class-map match-all VOICEOUT
  match ip precedence 1
class-map match-all ROUTINGPROTOCOLS
  match ip precedence 5
class-map match-all CONTROLLEDLOADOUT
  match ip precedence 4
!
policy-map QOS304QCHILD
 class VOICEOUT
    priority level 1
    police cir percent 30
 class VOICEVIDEOCONTROLOUT
    priority level 2
    police cir percent 5
 class DETERMINISTICOUT
    bandwidth remaining ratio 20
 class CONTROLLEDLOADOUT
    bandwidth remaining ratio 18
 class ROUTINGPROTOCOLS
    bandwidth remaining ratio 4
 class class-default
    bandwidth remaining ratio 22
policy-map ASRMLPPP6MBPARENT
 class class-default
    shape average percent 98
   service-policy QOS304QCHILD
!
interface Multilink1
 ip address 192.168.1.1 255.255.255.0
 ppp chap hostname multilink_name-1
 ppp multilink
 ppp multilink group 1
 service-policy output ASRMLPPP6MBPARENT
!
interface Multilink2
 ip address 192.168.2.1 255.255.255.0
 ppp chap hostname multilink_name-2
 ppp multilink
 ppp multilink group 2
 service-policy output ASRMLPPP6MBPARENT
!
interface Serial0/3/1/1:0
 no ip address
 encapsulation ppp
 no keepalive
 ppp chap hostname multilink_name-1
 ppp multilink
 ppp multilink group 1
!
interface Serial0/3/1/2:0
 no ip address
 encapsulation ppp
 no keepalive
```

```
 ppp chap hostname multilink_name-1
 ppp multilink
 ppp multilink group 1
!
interface Serial0/3/1/3:0
 no ip address
 encapsulation ppp
 no keepalive
 ppp chap hostname multilink_name-1
 ppp multilink
 ppp multilink group 1
!
interface Serial0/3/1/4:0
 no ip address
 encapsulation ppp
 no keepalive
 ppp chap hostname multilink_name-1
 ppp multilink
 ppp multilink group 1
!
interface Serial0/3/1/5:0
 no ip address
 encapsulation ppp
 no keepalive
 ppp chap hostname multilink_name-2
 ppp multilink
 ppp multilink group 2
!
interface Serial0/3/1/6:0
 no ip address
 encapsulation ppp
 no keepalive
 ppp chap hostname multilink_name-2
 ppp multilink
 ppp multilink group 2
!
interface Serial0/3/1/7:0
 no ip address
 encapsulation ppp
 no keepalive
 ppp chap hostname multilink_name-2
 ppp multilink
 ppp multilink group 2
!
interface Serial0/3/1/8:0
 no ip address
 encapsulation ppp
 no keepalive
 ppp chap hostname multilink_name-2
 ppp multilink
 ppp multilink group 2
!
```

CHAP with an Encrypted Password Examples

The following examples show how to enable CHAP on serial interface 0 of three devices:

Configuration of Router yyy

```
hostname yyy
interface serial 0/0/0
 encapsulation ppp
 ppp authentication chap
username xxx password secretxy
username zzz password secretzy
```

Configuration of Router xxx

```
hostname xxx
```

```
interface serial 0/0/0
 encapsulation ppp
 ppp authentication chap
username yyy password secretxy
username zzz password secretxz
```

Configuration of Router zzz

```
hostname zzz
interface serial 0/0/0
 encapsulation ppp
 ppp authentication chap
username xxx password secretxz
username yyy password secretzy
```

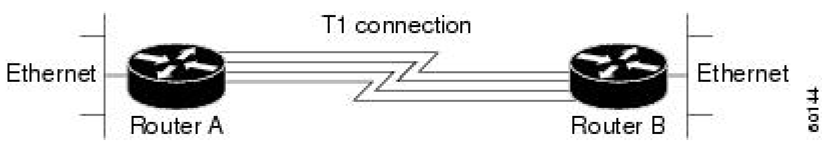
When you look at the configuration file, the passwords will be encrypted and the display will look similar to the following:

```
hostname xxx
interface serial 0/0/0
 encapsulation ppp
 ppp authentication chap
username yyy password 7 121F0A18
username zzz password 7 1329A055
```

MLP on Synchronous Serial Interfaces Example

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

Figure 2 Inverse Multiplexing Application Using Multilink PPP



The following example shows the configuration commands used to create the inverse multiplexing application:

Router A Configuration

```
hostname RouterA
!
!
username RouterB password your_password
ip subnet-zero
multilink virtual-template 1
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 ppp authentication chap
 ppp multilink
!
interface Serial0
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
```

```
!
interface Serial1
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
!
interface Serial2
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
!
interface Serial3
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
!
interface GigabitEthernet0/0/0
 ip address 10.17.1.254 255.255.255.0
!
router rip
network 10.0.0.0
!
end
```

Router B Configuration

```
hostname RouterB
!
!
username RouterB password your_password
ip subnet-zero
multilink virtual-template 1
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 ppp authentication chap
 ppp multilink
!
interface Serial0
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
!
interface Serial1
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
!
interface Serial2
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
!
interface Serial3
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 pulse-time 3
!
```

```
interface Ethernet0
 ip address 10.17.2.254 255.255.255.0
!
router rip
network 10.0.0.0
!
end
```

MLP Using Multilink Group Interfaces over ATM Example

The following example configures MLP over an ATM PVC using a multilink group:

```
interface multilink 1
 ip address 10.200.83.106 255.255.255.252
 ip tcp header-compression iphc-format delay 20000
 service policy output xyz
 encapsulation ppp
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink interleave
 ppp timeout multilink link remove 10
 ip rtp header-compression iphc-format
interface virtual-template 3
 bandwidth 128
 ppp multilink group 1
interface atm 4/0.1 point-to-point
 pvc 0/32
 abr 100 80
 protocol ppp virtual-template 3
.
```

MLP Interleaving and Queueing for Real-Time Traffic Example

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

```
interface virtual-template 1
 ip unnumbered ethernet 0
 ppp multilink
 ppp multilink interleave
 ppp multilink fragment delay 20
 ip rtp interleave 32768 20 1000
multilink virtual-template 1
```

Additional References

Related Documents

Related Topic	Document Title
PPP commands	*Cisco IOS Dial Technologies Command Reference*

MIBs

MIB	MIBs Link
• No MIBs were introduced or modified for this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Media-Independent PPP and Multilink PPP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Media-Independent PPP and Multilink PPP

Feature Name	Releases	Feature Information
Media-Independent PPP and Multilink PPP	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Feature Name	Releases	Feature Information
Multilink PPP Minimum Links Mandatory	Cisco IOS XE Release 2.1	The Multilink PPP Minimum Links Mandatory feature enables you to configure the minimum number of links in a MLP bundle required to keep that bundle active. The following commands were introduced or modified: **multilink min-links**, **ppp multilink links minimum**.
DHCP Proxy Client	Cisco IOS XE Release 2.3	The DHCP proxy client feature allows you to manage a pool of IP addresses available to PPP or SLIP dial-in clients without a known IP address.