



## Configuring PPP

This module describes the configuration of Point-to-Point Protocol (PPP) on POS and serial interfaces on the Cisco CRS-1 Router.

### Feature History for Configuring PPP Interfaces

Release	Modification
Release 2.0	PPP authentication was introduced on the Cisco CRS-1 Router.

- [Prerequisites for Configuring PPP, on page 1](#)
- [Information About PPP, on page 2](#)
- [How to Configure PPP, on page 4](#)
- [Configuration Examples for PPP, on page 18](#)

## Prerequisites for Configuring PPP

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before you can configure PPP authentication on a POS or serial interface, be sure that the following tasks and conditions are met:

- Your hardware must support POS or serial interfaces.
- You have enabled PPP encapsulation on your interface with the **encap ppp** command, as described in the appropriate module:
  - To enable PPP encapsulation on a POS interface, see the [Configuring POS Interfaces](#) module in this manual.
  - To enable PPP encapsulation on a serial interface, see the [Configuring Serial Interfaces](#) module in this manual.

# Information About PPP

To configure PPP and related features, you should understand the information in this section:

## PPP Authentication

When PPP authentication is configured on an interface, a host requires that the other host uniquely identify itself with a secure password before establishing a PPP connection. The password is unique and is known to both hosts.

PPP supports the following authentication protocols:

- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft extension to the CHAP protocol (MS-CHAP)
- Password Authentication Protocol (PAP).

When you first enable PPP on a POS or serial interface, no authentication is enabled on the interface until you configure a CHAP, MS-CHAP, or PAP secret password under that interface. Keep the following information in mind when configuring PPP on an interface:

- CHAP, MS-CHAP, and PAP can be configured on a single interface; however, only one authentication method is used at any one time. The order in which the authentication protocols are used is determined by the peer during the LCP negotiations. The first authentication method used is the one that is also supported by the peer.
- PAP is the least secure authentication protocol available on POS and serial interfaces. To ensure higher security for information that is sent over POS and serial interfaces, we recommend configuring CHAP or MS-CHAP authentication in addition to PAP authentication.
- Enabling or disabling PPP authentication does not effect the local router's willingness to authenticate itself to the remote device.
- The **ppp authentication** command is also used to specify the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface. You can enable CHAP, MS-CHAP, or PAP in any order. If you enable all three methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the remote device's ability to correctly negotiate the appropriate method and on the level of data line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.



---

**Caution**

If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, your interface cannot authenticate the peer. For details on implementing the **aaa authentication** command with the **ppp** keyword, see the *Authentication, Authorization, and Accounting Commands on Cisco IOS XR Software* module of *Cisco IOS XR System Security Command Reference* and *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

---

## PAP Authentication

PAP provides a simple method for a remote node to establish its identity using a two-way handshake. After a PPP link is established between two hosts, a username and password pair is repeatedly sent by the remote node across the link (in clear text) until authentication is acknowledged, or until the connection is terminated.

PAP is not a secure authentication protocol. Passwords are sent across the link in clear text and there is no protection from playback or trial-and-error attacks. The remote node is in control of the frequency and timing of the login attempts.

## CHAP Authentication

CHAP is defined in RFC 1994, and it verifies the identity of the peer by means of a three-way handshake. The steps that follow provide a general overview of the CHAP process:

### SUMMARY STEPS

1. The CHAP authenticator sends a challenge message to the peer.
2. The peer responds with a value calculated through a one-way hash function.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, then the authentication is successful. If the values do not match, then the connection is terminated.

### DETAILED STEPS

- |               |  |
|---------------|--|
| <b>Step 1</b> | The CHAP authenticator sends a challenge message to the peer.  |
| <b>Step 2</b> | The peer responds with a value calculated through a one-way hash function.   |
| <b>Step 3</b> | The authenticator checks the response against its own calculation of the expected hash value. If the values match, then the authentication is successful. If the values do not match, then the connection is terminated. |

This authentication method depends on a CHAP password known only to the authenticator and the peer. The CHAP password is not sent over the link. Although the authentication is only one-way, you can negotiate CHAP in both directions, with the help of the same CHAP password set for mutual authentication.



**Note** For CHAP authentication to be valid, the CHAP password must be identical on both hosts.

## MS-CHAP Authentication

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension to RFC 1994. MS-CHAP follows the same authentication process used by CHAP. In this case, however, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).



**Note** For MS-CHAP authentication to be valid, the MS-CHAP password must be identical on both hosts.

# How to Configure PPP

This section includes the following procedures:

## Modifying the Default PPP Configuration

When you first enable PPP on an interface, the following default configuration applies:

- The interface resets itself immediately after an authentication failure.
- The maximum number of configuration requests without response permitted before all requests are stopped is 10.
- The maximum number of consecutive Configure Negative Acknowledgments (CONFNAKs) permitted before terminating a negotiation is 5.
- The maximum number of terminate requests (TermReqs) without response permitted before the Link Control Protocol (LCP) or Network Control Protocol (NCP) is closed is 2.
- Maximum time to wait for a response to an authentication packet is 10 seconds.
- Maximum time to wait for a response during PPP negotiation is 3 seconds.

This task explains how to modify the basic PPP configuration on serial and POS interfaces that have PPP encapsulation enabled. The commands in this task apply to all authentication types supported by PPP (CHAP, MS-CHAP, and PAP).

### Before you begin

You must enable PPP encapsulation on the interface with the **encapsulation ppp** command.

- To enable PPP encapsulation on a POS interface, see the [Configuring POS Interfaces](#) module in this manual.
- To enable PPP encapsulation on an interface, see the [Configuring Serial Interfaces](#) module in this manual.

### SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp max-bad-auth** *retries*
4. **ppp max-configure** *retries*
5. **ppp max-failure** *retries*
6. **ppp max-terminate** *number*
7. **ppp timeout authentication** *seconds*
8. **ppp timeout retry** *seconds*
9. **end** or **commit**
10. **show ppp interfaces** *{type interface-path-id | all | brief {type interface-path-id | all | location node-id} | detail {type interface-path-id | all | location node-id} | location node-id}*

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface type interface-path-id</b> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1	Enters interface configuration mode.
<b>Step 3</b>	<b>ppp max-bad-auth retries</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp max-bad-auth 3	(Optional) Configures the number of authentication retries allowed on an interface after a PPP authentication failure. <ul style="list-style-type: none"> <li>• If you do not specify the number of authentication retries allowed, the router resets itself immediately after an authentication failure.</li> <li>• Replace the <i>retries</i> argument with number of retries after which the interface is to reset itself, in the range from 0 through 10.</li> <li>• The default is 0 retries.</li> <li>• The <b>ppp max-bad-auth</b> command applies to any interface on which PPP encapsulation is enabled.</li> </ul>
<b>Step 4</b>	<b>ppp max-configure retries</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp max-configure 4	(Optional) Specifies the maximum number of configure requests to attempt (without response) before the requests are stopped. <ul style="list-style-type: none"> <li>• Replace the <i>retries</i> argument with the maximum number of configure requests retries, in the range from 4 through 20.</li> <li>• The default maximum number of configure requests is 10.</li> <li>• If a configure request message receives a reply before the maximum number of configure requests are sent, further configure requests are abandoned.</li> </ul>
<b>Step 5</b>	<b>ppp max-failure retries</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp max-failure 3	(Optional) Configures the maximum number of consecutive Configure Negative Acknowledgments (CONFNAKs) permitted before a negotiation is terminated. <ul style="list-style-type: none"> <li>• Replace the <i>retries</i> argument with the maximum number of CONFNAKs to permit before terminating a negotiation, in the range from 2 through 10.</li> <li>• The default maximum number of CONFNAKs is 5.</li> </ul>

	Command or Action	Purpose
<b>Step 6</b>	<b>ppp max-terminate</b> <i>number</i> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp max-terminate 5	(Optional) Configures the maximum number of terminate requests (TermReqs) to send without reply before the Link Control Protocol (LCP) or Network Control Protocol (NCP) is closed. <ul style="list-style-type: none"> <li>• Replace the <i>number</i> argument with the maximum number of TermReqs to send without reply before closing down the LCP or NCP. Range is from 2 to 10.</li> <li>• The default maximum number of TermReqs is 2.</li> </ul>
<b>Step 7</b>	<b>ppp timeout authentication</b> <i>seconds</i> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp timeout authentication 20	(Optional) Sets PPP authentication timeout parameters. <ul style="list-style-type: none"> <li>• Replace the <i>seconds</i> argument with the maximum time, in seconds, to wait for a response to an authentication packet. Range is from 3 to 30 seconds.</li> <li>• The default authentication time is 10 seconds, which should allow time for a remote router to authenticate and authorize the connection and provide a response. However, it is also possible that it will take much less time than 10 seconds. In such cases, use the <b>ppp timeout authentication</b> command to lower the timeout period to improve connection times in the event that an authentication response is lost.</li> </ul>
<b>Step 8</b>	<b>ppp timeout retry</b> <i>seconds</i> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp timeout retry 8	(Optional) Sets PPP timeout retry parameters. <ul style="list-style-type: none"> <li>• Replace the <i>seconds</i> argument with the maximum time, in seconds, to wait for a response during PPP negotiation. Range is from 1 to 10 seconds.</li> <li>• The default is 3 seconds.</li> </ul>
<b>Step 9</b>	<b>end</b> or <b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# end or RP/0/RP0/CPU0:router(config-if)# commit	Saves configuration changes. <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes:   Uncommitted changes found, commit them before exiting(yes/no/cancel)?  [cancel]:  - Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.  - Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>- Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 10</b>	<b>show ppp interfaces</b> <i>{type interface-path-id   all   brief {type interface-path-id   all   location node-id}   detail {type interface-path-id   all   location node-id}   location node-id}</i>  <b>Example:</b>  RP/0/RP0/CPU0:router# show ppp interfaces serial 0/2/0/0	Verifies the PPP configuration for an interface or for all interfaces that have PPP encapsulation enabled.

## Configuring PPP Authentication

This section contains the following procedures:

### Enabling PAP, CHAP, and MS-CHAP Authentication

This task explains how to enable PAP, CHAP, and MS-CHAP authentication on a serial or POS interface.

#### Before you begin

You must enable PPP encapsulation on the interface with the **encapsulation ppp** command, as described in the following modules:

- To enable PPP encapsulation on a POS interface, see the [Configuring POS Interfaces](#) module in this manual.
- To enable PPP encapsulation on an interface, see the [Configuring Serial Interfaces](#) module in this manual.

#### SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp authentication** *protocol [protocol [protocol]] [list-name | default]*
4. **end** or **commit**
5. **show ppp interfaces** *{type interface-path-id | all | brief {type interface-path-id | all | location node-id} | detail {type interface-path-id | all | location node-id} | location node-id}*

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router# configure</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>interface type interface-path-id</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1</pre>	Enters interface configuration mode.
<b>Step 3</b>	<b>ppp authentication protocol [protocol [protocol]] [list-name   default]</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-if)# ppp authentication chap pap MIS-access</pre>	<p>Enables CHAP, MS-CHAP, or PAP on an interface, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.</p> <ul style="list-style-type: none"> <li>• Replace the <i>protocol</i> argument with <b>pap</b>, <b>chap</b>, or <b>ms-chap</b>.</li> <li>• Replace the <i>list name</i> argument with the name of a list of methods of authentication to use. To create a list, use the <b>aaa authentication ppp</b> command, as described in the <i>Authentication, Authorization, and Accounting Commands on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Command Reference</i>.</li> <li>• If no list name is specified, the system uses the default. The default list is designated with the <b>aaa authentication ppp</b> command, as described in the <i>Authentication, Authorization, and Accounting Commands on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Command Reference</i>.</li> </ul>
<b>Step 4</b>	<b>end or commit</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-if)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-if)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes:</li> </ul> <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> <li>- Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>- Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> </ul>



	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>- Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<p><b>show ppp interfaces</b> {<i>type interface-path-id</i>   <b>all</b>   <b>brief</b> {<i>type interface-path-id</i>   <b>all</b>   <b>location node-id</b>}   <b>detail</b> {<i>type interface-path-id</i>   <b>all</b>   <b>location node-id</b>}   <b>location node-id</b>}</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router# show ppp interfaces serial 0/2/0/0</pre>	<p>Displays PPP state information for an interface.</p> <ul style="list-style-type: none"> <li>• Enter the <i>type interface-path-id</i> argument to display PPP information for a specific interface.</li> <li>• Enter the <b>brief</b> keyword to display brief output for all interfaces on the router, for a specific interface instance, or for all interfaces on a specific node.</li> <li>• Enter the <b>all</b> keyword to display detailed PPP information for all nodes installed in the router.</li> <li>• Enter the <b>location node-id</b> keyword argument to display detailed PPP information for the designated node.</li> </ul> <p>There are seven possible PPP states applicable for either the Link Control Protocol (LCP) or the Network Control Protocol (NCP).</p>

### What to do next

Configure a PAP, CHAP, or MS-CHAP authentication password, as described in the appropriate section:

- If you enabled PAP on an interface, configure a PAP authentication username and password, as described in the “Configuring a PAP Authentication Password” section on page 641.
- If you enabled CHAP on an interface, configure a CHAP authentication password, as described in the “Configuring a CHAP Authentication Password” section on page 643
- If you enabled MS-CHAP on an interface, configure an MS-CHAP authentication password, as described in the “Configuring an MS-CHAP Authentication Password” section on page 645

## Configuring a PAP Authentication Password

This task explains how to enable and configure PAP authentication on a serial or POS interface.



### Note

PAP is the least secure authentication protocol available on POS and interfaces. To ensure higher security for information that is sent over POS and interfaces, we recommend configuring CHAP or MS-CHAP authentication in addition to PAP authentication.

**Before you begin**

You must enable PAP authentication on the interface with the **ppp authentication** command, as described in the [Enabling PAP, CHAP, and MS-CHAP Authentication](#).

**SUMMARY STEPS**

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp pap sent-username** *username* **password** [**clear** | **encrypted**] *password*
4. **end** or **commit**
5. **show running-config**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# <b>configure</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# <b>interface</b> serial 0/4/0/1	Enters interface configuration mode.
<b>Step 3</b>	<b>ppp pap sent-username</b> <i>username</i> <b>password</b> [ <b>clear</b>   <b>encrypted</b> ] <i>password</i> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# <b>ppp pap sent-username</b> xxxx <b>password</b> notified	<p>Enables remote Password Authentication Protocol (PAP) support for an interface, and includes the <b>sent-username</b> and <b>password</b> commands in the PAP authentication request packet to the peer.</p> <ul style="list-style-type: none"> <li>• Replace the <i>username</i> argument with the username sent in the PAP authentication request.</li> <li>• Enter <b>password clear</b> to select cleartext encryption for the password, or enter <b>password encrypted</b> if the password is already encrypted.</li> <li>• The <b>ppp pap sent-username</b> command allows you to replace several username and password configuration commands with a single copy of this command on interfaces.</li> <li>• You must configure the <b>ppp pap sent-username</b> command for each interface.</li> <li>• Remote PAP support is disabled by default.</li> </ul>
<b>Step 4</b>	<b>end</b> or <b>commit</b> <b>Example:</b>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes:</li> </ul>

	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router(config-if)# end</pre> <p>OR</p> <pre>RP/0/RP0/CPU0:router(config-if)# commit</pre>	<p>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</p> <ul style="list-style-type: none"> <li>- Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>- Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>- Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul> <ul style="list-style-type: none"> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router# show running-config</pre>	Verifies PPP authentication information for interfaces that have PPP encapsulation enabled.

## Configuring a CHAP Authentication Password

This task explains how to enable CHAP authentication and configure a CHAP password on a serial or POS interface.

### Before you begin

You must enable CHAP authentication on the interface with the **ppp authentication** command, as described in the [Enabling PAP, CHAP, and MS-CHAP Authentication](#).

### Restrictions

The same CHAP password must be configured on both host endpoints.

### SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp chap password** [clear | encrypted] *password*
4. **end** or **commit**
5. **show running-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1	Enters interface configuration mode.
<b>Step 3</b>	<b>ppp chap password</b> [clear   encrypted] <i>password</i> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp chap password clear xxxx	<p>Enables CHAP authentication on the specified interface, and defines an interface-specific CHAP password.</p> <ul style="list-style-type: none"> <li>• Enter <b>clear</b> to select cleartext encryption, or <b>encrypted</b> if the password is already encrypted.</li> <li>• Replace the <i>password</i> argument with a cleartext or already-encrypted password. This password is used to authenticate secure communications among a collection of routers.</li> <li>• The <b>ppp chap password</b> command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not effect local CHAP authentication. This command is useful when you are trying to authenticate a peer that does not support this command (such as a router running an older Cisco IOS XR software image).</li> <li>• The CHAP secret password is used by the routers in response to challenges from an unknown peer.</li> </ul>
<b>Step 4</b>	<b>end</b> or <b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# end or RP/0/RP0/CPU0:router(config-if)# commit	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes:  <pre>Uncommitted changes found, commit them before   exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> <li>- Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>- Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> </ul> </li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>- Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b>  RP/0/RP0/CPU0:router# show running-config	Verifies PPP authentication information for interfaces that have PPP encapsulation enabled.

## Configuring an MS-CHAP Authentication Password

This task explains how to enable MS-CHAP authentication and configure an MS-CHAP password on a serial or POS interface.

### Before you begin

You must enable MS-CHAP authentication on the interface with the **ppp authentication** command, as described in the [Enabling PAP, CHAP, and MS-CHAP Authentication](#).

### Restrictions

The same MS-CHAP password must be configured on both host endpoints.

## SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp ms-chap password** [clear | encrypted] *password*
4. **end** or **commit**
5. **show running-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b>  RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type interface-path-id</i> <b>Example:</b>  RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1	Enters interface configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>ppp ms-chap password [clear   encrypted] password</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-if)# ppp ms-chap password clear xxxx</pre>	<p>Enables a router calling a collection of routers to configure a common Microsoft Challenge Handshake Authentication (MS-CHAP) secret password.</p> <p>The MS-CHAP secret password is used by the routers in response to challenges from an unknown peer.</p>
<b>Step 4</b>	<b>end or commit</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router(config-if)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-if)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>When you issue the <b>end</b> command, the system prompts you to commit changes:   <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul> </li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b> <pre>RP/0/RP0/CPU0:router# show running-config</pre>	Verifies PPP authentication information for interfaces that have PPP encapsulation enabled.

## Disabling an Authentication Protocol

This section contains the following procedures:

### Disabling PAP Authentication on an Interface

This task explains how to disable PAP authentication on a serial or POS interface.

#### SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp pap refuse**
4. **end or commit**

## 5. show running-config

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1	Enters interface configuration mode.
<b>Step 3</b>	<b>ppp pap refuse</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp pap refuse	Refuses Password Authentication Protocol (PAP) authentication from peers requesting it. <ul style="list-style-type: none"> <li>• If outbound Challenge Handshake Authentication Protocol (CHAP) has been configured (using the <b>ppp authentication</b> command), CHAP will be suggested as the authentication method in the refusal packet.</li> <li>• PAP authentication is disabled by default.</li> </ul>
<b>Step 4</b>	<b>end</b> or <b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# end or RP/0/RP0/CPU0:router(config-if)# commit	Saves configuration changes. <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes:   Uncommitted changes found, commit them before exiting(yes/no/cancel)?  [cancel]:  - Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.  - Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.  - Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b>	Verifies PPP authentication information for interfaces that have PPP encapsulation enabled.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router# show running-config	

## Disabling CHAP Authentication on an Interface

This task explains how to disable CHAP authentication on a serial or POS interface.

### SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp chap refuse**
4. **end** or **commit**
5. **show running-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1	Enters interface configuration mode.
<b>Step 3</b>	<b>ppp chap refuse</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# ppp chap refuse	Refuses CHAP authentication from peers requesting it. After you enter the <b>ppp chap refuse</b> command under the specified interface, all attempts by the peer to force the user to authenticate with the help of CHAP are refused. <ul style="list-style-type: none"> <li>• CHAP authentication is disabled by default.</li> <li>• If outbound Password Authentication Protocol (PAP) has been configured (using the <b>ppp authentication</b> command), PAP will be suggested as the authentication method in the refusal packet.</li> </ul>
<b>Step 4</b>	<b>end</b> or <b>commit</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-if)# end or RP/0/RP0/CPU0:router(config-if)# commit	Saves configuration changes. <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes:   Uncommitted changes found, commit them before exiting(yes/no/cancel)?  [cancel]: </li> </ul>



	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>- Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>- Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>- Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b> RP/0/RP0/CPU0:router# show running-config	Verifies PPP authentication information for interfaces that have PPP encapsulation enabled.

## Disabling MS-CHAP Authentication on an Interface

This task explains how to disable MS-CHAP authentication on a serial or POS interface.

### SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp ms-chap refuse**
4. **end** or **commit**
5. **show running-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b> <b>Example:</b> RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type interface-path-id</i> <b>Example:</b> RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1	Enters interface configuration mode.
<b>Step 3</b>	<b>ppp ms-chap refuse</b> <b>Example:</b>	Refuses MS-CHAP authentication from peers requesting it. After you enter the <b>ppp ms-chap refuse</b> command under

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config-if)# ppp ms-chap refuse	<p>the specified interface, all attempts by the peer to force the user to authenticate with the help of MS-CHAP are refused.</p> <ul style="list-style-type: none"> <li>MS-CHAP authentication is disabled by default.</li> <li>If outbound Password Authentication Protocol (PAP) has been configured (using the <b>ppp authentication</b> command), PAP will be suggested as the authentication method in the refusal packet.</li> </ul>
<b>Step 4</b>	<p><b>end or commit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-if)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-if)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>When you issue the <b>end</b> command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul> </li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
<b>Step 5</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router# show running-config</pre>	Verifies PPP authentication information for interfaces that have PPP encapsulation enabled.

## Configuration Examples for PPP

This section provides the following configuration examples:

### Configuring a POS Interface with PPP Encapsulation: Example

The following example shows how to create and configure a POS interface with PPP encapsulation:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/0
```

```
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username P1_TEST-8 password xxxx
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap pap MIS-access
RP/0/RP0/CPU0:router(config-if)# ppp chap password encrypted xxxx
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
```

The following example shows how to configure POS interface 0/3/0/1 to allow two additional retries after an initial authentication failure (for a total of three failed authentication attempts):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# ppp max-bad-auth 3
```

## Configuring a Serial Interface with PPP Encapsulation: Example

The following example shows how to create and configure a serial interface with PPP MS-CHAP encapsulation:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface serial 0/3/0/0/0:0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# ppp authentication ms-chap MIS-access
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap password encrypted xxxx
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
```

