PPP Commands

This module provides command line interface (CLI) commands for configuring Point-to-Point Protocol (PPP) on the Cisco CRS Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

Point-to-Point Protocol (PPP) is an encapsulation scheme that can be used on Packet-over-SONET (POS) and serial interfaces. PPP is a standard protocol used to send data over synchronous serial links. PPP also provides a Link Control Protocol (LCP) for negotiating properties of the link. LCP uses echo requests and responses to monitor the continuing availability of the link.

PPP provides the following Network Control Protocols (NCPs) for negotiating properties of data protocols that will run on the link:

- Cisco Discovery Protocol Control Protocol (CDPCP) to negotiate CDP properties
- IP Control Protocol (IPCP) to negotiate IP properties
- IP Version 6 Control Protocol (IPv6CP) to negotiate IPv6 properties
- Multiprotocol Label Switching Control Protocol (MPLSCP) to negotiate MPLS properties
- Open System Interconnection Control Protocol (OSICP) to negotiate OSI properties

clear ppp sso state

To clear the replicated Inter-Chassis Stateful Switchover (ICSSO) states for the specified standby interface or for all interfaces on the specified node, use the **clear ppp sso state** command in EXEC mode.

clear ppp sso state {**interface** *interface-path-id* | **all**} **location** *node-id*

Syntax Description

interface *interface-path-id*	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module*.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command sets the PPP sessions in the Standby-Up state to the Standby-Down state. All replicated data received from the peer is purged, and SSRP Request messages are re-sent to the peer.

Task ID

Task ID	Operations
ppp	execute

Examples

The following example shows how to clear the replicated ICSSO states for the specified standby interface:

```
RP/0/RP0/CPU0:router# clear ppp sso state interface 0/1/0/1
```

The following example shows how to clear the replicated Inter-Chassis Stateful Switchover (ICSSO) states for all interfaces on the specified node:

```
RP/0/RP0/CPU0:router# clear ppp sso state all location 1/0/1
```

clear ppp statistics

To clear all Point-to-Point Protocol (PPP) statistics for a PPP interface, use the **clear ppp statistics** command in EXEC mode.

clear ppp statistics interface *interface-path-id*

Syntax Description

interface *interface-path-id*	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	execute

Examples

The following example shows how to clear PPP statistics for a PPP interface:

```
RP/0/RP0/CPU0:router# clear ppp statistics interface 0/1/0/1
```

encapsulation ppp

To enable encapsulation for communication with routers or bridges using the Point-to-Point Protocol (PPP), use the **encapsulation ppp** command in interface configuration mode. To disable PPP encapsulation, use the **no** form of this command.

encapsulation ppp

Syntax Description

This command has no keywords or arguments.

Command Default

PPP encapsulation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

Use the **encapsulation ppp** command to enable PPP encapsulation on an interface.

Task ID

Task ID	Operations
ppp	read, write
interface	read, write

Examples

The following example shows how to set up PPP encapsulation on interface POS 0/1/0/1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
```

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# interface serial 0/0/1/2/4:3
RP/0/RP0/CPU0:router# encapsulation ppp
```

Related Commands

Command	Description
show ppp interfaces (BNG), on page 40	Displays PPP state information for an interface.

group

To create a Session State Redundancy Protocol (SSRP) group and associate it with a profile, use the **group** command in Global Configuration mode. To remove this group, use the no form of this command.

group *group-id* **profile** *profile_name* [**default**]

Syntax Description

group-id	SSRP group identifier. The range is 1 to 65535.
profile *profile_name*	Profile to associate with this group.
default	Associates the group to the default profile.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Any interfaces on this card can be configured to use this group. The group number must be unique across the router.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to create an SSRP group:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp location 0/1/cpu0
RP/0/RP0/CPU0:router(config-ssrp-node)# group 1 profile default
```

Related Commands

Command	Description
ssrp location, on page 52	specify the node on which to create a SSRP group and enter the SSRP node configuration mode.

multi-router aps

To configure Multi-Router Automatic Protection Switching (MR-APS) and enter APS redundancy configuration mode, use the **multi-router aps** command in redundancy configuration mode. To deactivate Multi-Router Automatic Protection Switching (MR-APS), use the no form of this command.

multi-router aps

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Redundancy configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# redundancy
RP/0/RP0/CPU0:router(config-redundancy)# multi-router aps
RP/0/RP0/CPU0:router(config-redundancy-aps)
```

Related Commands

Command	Description
redundancy, on page 38	Enters the redundancy configuration mode to configure MR-APS.

peer ipv4 address

To configure the IPv4 address for a Session State Redundancy Protocol (SSRP) peer, use the **peer ipv4 address** command in SSRP configuration mode. To remove the address, use the no form of this command.

peer ipv4 address *ip-address*

Syntax Description

ip-address	IP address of the peer interface whose states will be replicated by SSRP.

Command Default

No default behavior or values

Command Modes

SSRP configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to configure the IPv4 address for a Session State Redundancy Protocol (SSRP) peer:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RP0/CPU0:router(config-ssrp)# peer ipv4 address 10.10.10.10
```

Related Commands

Command	Description
ssrp profile, on page 53	Configures a SSRP profile and enters the SSRP configuration mode.

ppp authentication (BNG)

To enable Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, or Password Authentication Protocol (PAP), and to specify the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface, use the **ppp authentication** command in an appropriate configuration mode. To disable PPP authentication, use the **no** form of this command.

ppp authentication *protocol* [*protocol* [*protocol*]] {*list-name* | **default**}

Syntax Description

protocol	Name of the authentication protocol used for PPP authentication. See Table 1: PPP Authentication Protocols for Negotiation, on page 10 for the appropriate keyword. You may select one, two, or all three protocols, in any order.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Specifies the name of the list of methods created with the **aaa authentication ppp** command.

Command Default

PPP authentication is not enabled.

Command Modes

Interface configuration

Dynamic template configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	This command was corrected to include the possibility of specifying three protocols simultaneously.

Usage Guidelines

When you enable CHAP or PAP authentication (or both), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a response message. The local router attempts to match the remote device's name with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

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.

To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

Note If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, then authentication does not complete successfully and the line does not come up.

Table 1: PPP Authentication Protocols for Negotiation, on page 10 lists the protocols used to negotiate PPP authentication.

Table 1: PPP Authentication Protocols for Negotiation

Protocol	Description
chap	Enables CHAP on an interface.
ms-chap	Enables Microsoft's version of CHAP (MS-CHAP) on an interface.
pap	Enables PAP on an interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication. In this case, authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

Enabling or disabling PPP authentication does not affect the local router authenticating itself to the remote device.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In this example, CHAP is enabled on POS 0/4/0/1 and uses the authentication list MIS-access:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/4/0/1
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap MIS-access
```

This is an example of configuring the **ppp authentication** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp authentication chap ms-chap pap
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
encapsulation	Sets the encapsulation method used by the interface.
username	Configures a new user with a username, establishes a password, and grants permissions for the user.

ppp chap password

To enable a router calling a collection of routers to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password, use the **ppp chap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp chap password [{**clear** | **encrypted**}] *password*

Syntax Description

clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **ppp chap password** command is sent in CHAP responses and is used by the peer to authenticate the local router. This does not affect local authentication of the peer. This command is useful for routers that do not support this command (such as routers running older Cisco IOS XR images).

The CHAP secret password is used by the routers in response to challenges from an unknown peer.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In this example, a password (xxxx) is entered as a cleartext password:

```
RP/0/RP0/CPU0:router(config-if)# ppp chap password xxxx
```

When the password is displayed (as shown in the following example, using the **show running-config** command), the password xxxx appears as 030752180500:

```
RP/0/RP0/CPU0:router(config)# show running-config interface POS 1/0/1/0

interface POS0/1/4/2
```

```
description Connected to P1 POS 0/1/4/3
ipv4 address 10.12.32.2 255.255.255.0
encapsulation ppp
ppp authentication chap pap
ppp chap password encrypted 030752180500
```

On subsequent logins, entering any of the three following commands would have the same effect of making xxxx the password for remote CHAP authentication:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 1/0/1/0
RP/0/RP0/CPU0:router(config-if)# ppp chap password xxxx
RP/0/RP0/CPU0:router(config-if)# ppp chap password clear xxxx
RP/0/RP0/CPU0:router(config-if)# ppp chap password encrypted 1514190900
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication (BNG), on page 9	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp chap refuse, on page 14	Refuses CHAP authentication from peers requesting it.
ppp max-bad-auth (BNG), on page 19	Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

ppp chap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **ppp chap refuse** command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP are refused.

If outbound Password Authentication Protocol (PAP) has been configured (using the **ppp authentication** command), PAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to specify POS interface 0/3/0/1 and disable CHAP authentication from occurring if a peer calls in requesting CHAP authentication. The method of encapsulation on the interface is PPP.

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.

Command	Description
ppp authentication (BNG), on page 9	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp max-bad-auth (BNG), on page 19	Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
ppp pap sent-username password, on page 33	Enables remote PAP support for an interface, and includes the **sent-username** and **password** commands in the PAP authentication request packet to the peer.

ppp ipcp dns

To configure the primary and secondary Domain Name System (DNS) IP addresses for the Internet Protocol Control Protocol (IPCP), use the **ppp ipcp dns** command in interface configuration mode. To remove the addresses, use the no form of this command.

ppp ipcp dns *primary-ip-address* [*sec-ip-address*]

Syntax Description

primary-ip-address	Primary DNS IP address, in the format A.B.C.D.
sec-ip-address	Secondary DNS IP address, in the format W.X.Y.Z.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to configure the primary and secondary DNS IP addresses for Internet Protocol Control Protocol (IPCP):

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ipcp dns 10.10.10.10 10.10.10.11
```

ppp ipcp neighbor-route disable

To disable installation of a route to the peer address negotiated by Internet Protocol Control Protocol (IPCP), use the **ppp ipcp neighbor-route disable** command in interface configuration mode. To re-enable installation of a route to the peer address negotiated by IPCP, use the no form of this command.

ppp ipcp neighbor-route disable

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to disable installation of a route to the peer address negotiated by IPCP:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ipcp neighbor-route disable
```

ppp ipcp peer-address default

To specify the default IPv4 address that is assigned to the peer by the Internet Protocol Control Protocol (IPCP), use the **ppp ipcp peer-address default** command in interface configuration mode. To remove the address, use the no form of this command.

ppp ipcp peer-address default *ip-address*

Syntax Description

ip-address	Specifies the IP address for the peer node.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to specify the default IPv4 address that is assigned to the peer by IPCP.

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ipcp peer-address default 10.10.10.10
```

ppp max-bad-auth (BNG)

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

ppp max-bad-auth *retries*

Syntax Description

retries	Number of retries after which the interface is to reset itself. Range is from 0 to 10. Default is 0 retries.

Command Default

retries: 0

Command Modes

Interface configuration

Dynamic template configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **ppp max-bad-auth** command applies to any interface on which PPP encapsulation is enabled.

To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In this example, POS interface 0/3/0/1 is set 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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap
RP/0/RP0/CPU0:router(config-if)# ppp max-bad-auth 3
```

This example shows how to allow two additional retries after an initial authentication failure in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp max-configure 5
```

ppp max-configure (BNG)

To specify the maximum number of configure requests to attempt (without response) before stopping the requests, use the **ppp max-configure** command in an appropriate configuration mode. To disable the maximum number of configure requests and return to the default, use the **no** form of this command.

ppp max-configure *retries*

Syntax Description

retries	Maximum number of retries. Range is 4 through 20. Default is 10.

Command Default

retries: 10

Command Modes

Interface configuration

Dynamic template configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

Use the **ppp max-configure** command to specify how many times an attempt is made to establish a Link Control Protocol (LCP) session between two peers for a particular interface. If a configure request message receives a reply before the maximum number of configure requests are sent, further configure requests are abandoned.

To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This example shows a limit of four configure requests:

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-configure 4
```

This example shows how a limit of four configure requests is specified in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp ipcp
```

Related Commands

Command	Description
ppp max-failure (BNG), on page 22	Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.

ppp max-failure (BNG)

To configure the maximum number of consecutive Configure Negative Acknowledgments (CONFNAKs) to permit before terminating a negotiation, use the **ppp max-failure** command in an appropriate configuration mode. To disable the maximum number of CONFNAKs and return to the default, use the **no** form of this command.

ppp max-failure *retries*

Syntax Description

retries	Maximum number of CONFNAKs to permit before terminating a negotiation. Range is from 2 to 10. Default is 5.

Command Default

retries: 5

Command Modes

Interface configuration

Dynamic template configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To enter the dynamic template configuration mode, run **dynamic-template** command in the

Global Configuration mode.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The **ppp max-failure** command specifies that no more than three CONFNAKs are permitted before terminating the negotiation:

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-failure 3
```

This example shows how no more than three CONFNAKs are permitted before terminating the negotiation in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ppp max-failure 4
```

Related Commands

Command	Description
ppp max-configure (BNG), on page 20	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.

ppp max-terminate

To configure the maximum number of terminate requests (TermReqs) to send without reply before closing down the Link Control Protocol (LCP) or Network Control Protocol (NCP), use the **ppp max-terminate** command in interface configuration mode. To disable the maximum number of TermReqs and return to the default, use the **no** form of this command.

ppp max-terminate *number*

Syntax Description

number	Maximum number of TermReqs to send without reply before closing down the LCP or NCP. Range is from 2 to 10. Default is 2.

Command Default

number: 2

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

In the following example, a maximum of five TermReqs are specified to be sent before terminating and closing LCP or NCP:

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp max-terminate 5
```

Related Commands

Command	Description
ppp max-configure (BNG), on page 20	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.
ppp max-failure (BNG), on page 22	Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.

ppp ms-chap hostname

To configure the hostname for MS-CHAP authentication on an interface, use the **ppp ms-chap hostname** command in interface configuration mode. To remove the hostname, use the no form of this command.

ppp ms-chap hostname *hostname*

Syntax Description

hostname	Specifies the hostname for MS-CHAP authentication.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to configure the hostname for MS-CHAP authentication on an interface:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap hostname Host_1
```

ppp ms-chap password

To configure a common Microsoft Challenge Handshake Authentication (MS-CHAP) secret password, use the **ppp ms-chap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp ms-chap password [{**clear** | **encrypted**}] *password*

Syntax Description

clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

The password is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **ppp ms-chap password** command is sent in CHAP responses and is used by the peer to authenticate the local router. This does not affect local authentication of the peer. The **ppp ms-chap password** command is useful for routers that do not support this command (such as routers running older software images).

The MS-CHAP secret password is used by the routers in response to challenges from an unknown peer.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to enter a password (xxxx) as a cleartext password:

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap password clear xxxx
```

ppp ms-chap refuse

To refuse Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication from peers requesting it, use the **ppp ms-chap refuse** command in interface configuration mode. To allow MS-CHAP authentication, use the **no** form of this command.

ppp ms-chap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

MS-CHAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **ppp ms-chap refuse** command specifies that MS-CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using MS-CHAP are refused.

If outbound Password Authentication Protocol (PAP) has been configured (using the **ppp authentication** command), PAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write

Examples

This example shows how to specify POS interface 0/3/0/1 and disable MS-CHAP authentication from occurring if a peer calls in requesting MS-CHAP authentication. The method of encapsulation on the interface is PPP.

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap refuse
```

Related Commands

Command	Description
ppp authentication (BNG), on page 9	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.

ppp multilink multiclass

To enable multiclass multilink PPP, use the **ppp multilink multiclass** command in interface configuration mode. To disable multiclass multilink PPP, use the no form of this command.

ppp multilink multiclass

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to enable multiclass multilink PPP:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ppp multilink multiclass
```

ppp multilink multiclass local

To configure the initial number and maximum number of Multiclass Multilink PPP (MCMP) receive classes in a Conf-Request sent from a local host to its peer, use the **ppp multilink multiclass local** command in interface configuration mode. To remove these settings, use the no form of this command.

ppp multilink multiclass local initial *init-number* **maximum** *max-number*

Syntax Description

initial *init-number*	Specifies the initial number of receive classes in the Conf-Request. The range is 1 to 16.
maximum *max-number*	Specifies the maximum number of receive classes in the Conf-Request. The range is 1 to 16.

Command Default

When MCMP is enabled, the default **initial** value is 2 and the default **maximum** value is 4.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The maximum number of receive classes configures the number of transmission classes on the local host.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to configure the initial number and maximum number of Multiclass Multilink PPP (MCMP) receive classes in a Conf-Request sent from a local host to its peer:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ppp multilink multiclass local initial 1 maximum 16
```

ppp multilink multiclass remote apply

To configure the minimum number of Multiclass Multilink PPP (MCMP) receive classes that a local host will accept from its peer in a Conf-Request, use the **ppp multilink multiclass** command in interface configuration mode. To remove this setting, use the no form of this command.

ppp multilink multiclass remote apply *min-number*

Syntax Description

min-number	Specifies the minimum number of receive classes in the Conf-Request. The range is 1 to 16.

Command Default

The default is 2 if MCMP is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command is used to coerce the peer to accept a minimum number of MCMP classes. If the peer does not accept the minimum number of MCMP classes specified by this command, the local router will not bring up the PPP link.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to use the **ppp multilink multicast remove** apply command.

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ppp multilink multiclass remote apply 16
```

Related Commands

Command	Description
ppp ipcp dns, on page 16	Configures the primary and secondary DNS IP addresses for the IPCP.
ppp ipcp neighbor-route disable, on page 17	Disables installation of a route to the peer address negotiated by IPCP.
ppp ipcp peer-address default, on page 18	Specifies the default IPv4 address that is assigned to the peer by the IPCP.
ppp ms-chap hostname, on page 25	Configures the hostname for MS-CHAP authentication on an interface.

ppp pap refuse

To refuse Password Authentication Protocol (PAP) authentication from peers requesting it, use the **ppp pap refuse** command in interface configuration mode. To allow PAP authentication, use the **no** form of this command.

ppp pap refuse

Syntax Description

This command has no keywords or arguments.

Command Default

PAP authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **ppp pap refuse** command specifies that PAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using PAP are refused.

If outbound Challenge Handshake Authentication Protocol (CHAP) has been configured (using the **ppp authentication** command), CHAP is suggested as the authentication method in the refusal packet.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

The following example shows how to specify POS 0/3/0/1 using PPP encapsulation on the interface. This example shows PAP authentication being specified as disabled if a peer calls in requesting PAP authentication.

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp pap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.

Command	Description
ppp authentication (BNG), on page 9	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp max-bad-auth (BNG), on page 19	Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
ppp pap sent-username password, on page 33	Enables remote PAP support for an interface, and includes the **sent-username** and **password** commands in the PAP authentication request packet to the peer.

ppp pap sent-username password

To enable remote Password Authentication Protocol (PAP) support for an interface, and to use the values specified for username and password in the PAP authentication request, use the **ppp pap sent-username password** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** [{**clear** | **encrypted**}] *password*

Syntax Description

username	Username sent in the PAP authentication request.
clear	(Optional) Specifies the cleartext encryption parameter for the password.
encrypted	(Optional) Indicates that the password is already encrypted.
password	Cleartext or already-encrypted password.

Command Default

Remote PAP support is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

Use the **ppp pap sent-username password** command to enable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

You must configure the **ppp pap sent-username password** command for each interface.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

In the following example, a password is entered as a cleartext password, xxxx:

```
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
```

When the password is displayed (as shown in the following example, using the **show running-config** command), the password notified appears as 05080F1C2243:

```
RP/0/RP0/CPU0:router(config-if)# show running-config
```

```
interface POS0/1/0/0
description Connected to P1 POS 0/1/4/2
 ipv4 address 10.12.32.2 255.255.255.0
 encapsulation ppp
 ppp pap sent-username P2 password encrypted 05080F1C2243
```

On subsequent logins, entering any of the three following commands would have the same effect of making xxxx the password for remote PAP authentication:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password clear notified
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx encrypted 1514190900
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication (BNG), on page 9	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.
ppp multilink multiclass, on page 28	Refuses PAP authentication from peers requesting it
ppp timeout authentication, on page 35	Sets PPP authentication timeout parameters.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ppp timeout authentication

To set PPP authentication timeout parameters, use the **ppp timeout authentication** command in interface configuration mode. To reset the default value, use the **no** form of this command.

ppp timeout authentication *seconds*

Syntax Description

seconds	Maximum time, in seconds, to wait for a response to an authentication packet. Range is from 3 to 30 seconds. Default is 10 seconds.

Command Default

seconds: 10

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

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 **ppp timeout authentication** command to lower the timeout period to improve connection times in the event that an authentication response is lost.

Note The timeout affects connection times only if packets are lost.

Note Although lowering the authentication timeout is beneficial if packets are lost, sending authentication requests faster than the peer can handle them results in churn and a slower connection time.

Task ID

Task ID	Operations
ppp	read, write

Examples

In the following example, PPP timeout authentication is set to 20 seconds:

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp timeout authentication 20
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.
ppp authentication (BNG), on page 9	Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.

ppp timeout retry

To set PPP timeout retry parameters, use the **ppp timeout retry** command in interface configuration mode. To reset the time value, use the **no** form of this command.

ppp timeout retry *seconds*

Syntax Description

seconds	Maximum time, in seconds, to wait for a response during PPP negotiation. Range is from 1 to 10 seconds. Default is 3 seconds.

Command Default

seconds: 3

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

The **ppp timeout retry** command is useful for setting a maximum amount of time PPP should wait for a response to any control packet it sends.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows the retry timer being set to 8 seconds:

```
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)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# ppp timeout retry 8
```

redundancy

To enter the redundancy configuration mode to configure Multi-Router Automatic Protection Switching (MR-APS), use the **redundancy** command in Global Configuration mode.

redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to enter the redundancy configuration mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# redundancy
RP/0/RP0/CPU0:router(config-redundancy)#
```

security ttl

To specify that the time-to-live (TTL) value in the IP header of the packet is used to validate that a packet is from the expected source, use the **security ttl** command in SSRP configuration mode. To remove the TTL requirement, use the no form of this command.

security ttl max-hops *number*

Syntax Description

max-hops *number*	Maximum number of hops between the peer routers.

Command Default

The **max-hops** default is 255.

Command Modes

SSRP configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

If **max-hops** is not specified, the TTL value must be 255 for a packet to be accepted.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to specify that the time-to-live (TTL) value in the IP header of a packet is used to validate that the packet is from the expected source:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RP0/CPU0:router(config-ssrp)# peer ipv4 address 10.10.10.10
RP/0/RP0/CPU0:router(config-ssrp)# security ttl max-hops number 50
```

show ppp interfaces (BNG)

To display PPP state information for an interface, use the **show ppp interfaces** command in EXEC mode.

show ppp interfaces [{**brief** | **detail**}] {**all** | *type interface-path-id* | **location** *node-id*}

Syntax Description

brief	(Optional) Displays brief output for all interfaces on the router, for a specific POS interface instance, or for all interfaces on a specific node.
detail	(Optional) Displays detailed output for all interfaces on the router, for a specific interface instance, or for all interfaces on a specific node.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	(Optional) Displays detailed PPP information for all nodes.
location *node-id*	(Optional) Displays detailed PPP information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.9.0	For ICSSO, when SSRP is configured, the **show ppp interfaces** command displays the SSO-State for LCP, IPCP, and authentication layers.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.
Release 5.3.2	The command was modified to include a new output display field, **SRG-state**, as part of geo redundancy support for PPPoE sessions in BNG router.

Usage Guidelines

There are seven possible PPP states applicable for either the Link Control Protocol (LCP) or the Network Control Protocol (NCP).

The command output displays a summary of the interface as it is in the PPP Interface Descriptor Block (IDB). The output includes the following information (where applicable):

- Interface state
- Line protocol state
- Link Control Protocol (LCP) state
- Network Control Protocol (NCP) state
- Multilink PPP state
- Multilink PPP configuration
- Keepalive configuration
- Authentication configuration
- Negotiated MRUs
- Negotiated IP addresses

This command can display information for a single interface, all interfaces on a specified node, or all interfaces on the router.

Task ID

Task ID	Operations
ppp	read

Examples

This example shows how to display PPP state information for a POS interface:

```
RP/0/RP0/CPU0:router# show ppp interface POS 0/2/0/3

    POS0/2/0/3 is up, line protocol is up
      LCP: Open
         Keepalives enabled (10 sec)
         Local MRU: 4470 bytes
         Peer  MRU: 4470 bytes
      Authentication
         Of Us:    CHAP (Completed as 'test-user')
         Of Peer:  PAP (Completed as 'peer-user')
      CDPCP: Listen
      IPCP: Open
         Local IPv4 address: 55.0.0.1
         Peer IPv4 address:  55.0.0.2
         Peer DNS Primary:   55.0.0.254
         Peer DNS Secondary: 155.0.0.254
      IPV6CP: Open
         Local IPv6 address: fe80::3531:35ff:fe55:5747/128
         Peer IPv6 address:  fe80::3531:35ff:fe55:4213/128
      MPLSCP: Stopped
```

This example shows how to display PPP state information for a POS interface that is running as a Layer 2 attachment circuit:

```
RP/0/0/CPU0:# show ppp interface POS0/2/0/2

    POS0/2/0/2 is up, line protocol is up
```

```
      LCP: Open
         Running as L2 AC
```

This example shows how to display PPP state information for a multilink interface:

```
RP/0/RP0/CPU0:router:# show ppp interface Multilink 0/3/0/0/100

    Multilink0/3/0/0/100 is up, line protocol is down
      LCP: Open
         SSO-State: Standby-Up
         Keepalives disabled
      IPCP: Open
         SSO-State: Standby-Up
         Local IPv4 address: 100.0.0.1
         Peer IPv4 address:  100.0.0.2
      IPV6CP: Open
         Local IPv6 address: fe80::3531:35ff:fe55:4600/128
         Peer IPv6 address:  fe80::3531:35ff:fe55:3215/128
      Multilink
         Local MRRU: 1500 bytes
         Peer MRRU:  1500 bytes
         Local Endpoint Discriminator: 1234567812345678
         Peer Endpoint Discriminator:  1111222233334444
         MCMP classes: Local 4, Remote 2
         Member links: 2 active, 6 inactive (min-active 2)
           - Serial0/3/1/3/1  ACTIVE
           - Serial0/3/1/3/2  ACTIVE
           - Serial0/3/1/3/3  INACTIVE : LCP not negotiated
           - Serial0/3/1/3/4  INACTIVE : Mismatching peer endpoint
           - Serial0/3/1/3/5  INACTIVE : Mismatching peer auth name
           - Serial0/3/1/3/6  INACTIVE : MRRU option rejected by Peer
           - Serial0/3/1/3/7  INACTIVE : Mismatching local MCMP classes
           - Serial0/3/1/3/8  INACTIVE : MCMP option rejected by peer
```

This example shows how to display PPP state information for a serial interface:

```
RP/0/RP0/CPU0:router# show ppp interface Serial 0/3/1/3/1

    Serial0/3/1/3/1 is down, line protocol is down
      LCP: Open
         SSO-State: Standby-Up
         Keepalives enabled (10 sec)
         Local MRU: 1500 bytes
         Peer MRU:  1500 bytes
         Local Bundle MRRU: 1500 bytes
         Peer Bundle MRRU:  1500 bytes
         Local Endpoint Discriminator: 1234567812345678
         Peer Endpoint Discriminator:  1111222233334444
         Local MCMP Classes:  Not negotiated
         Remote MCMP Classes: Not negotiated
      Authentication
         Of Us:    CHAP (Completed as 'test-user')
         Of Peer:  PAP (Completed as 'peer-user')
      Multilink
         Multilink group id: 100
         Member status: ACTIVE
```

Table 2: show ppp interfaces Field Descriptions

Field	Description
Ack-Rcvd	Configuration acknowledgemt was received; waiting for peer to send configuration request.
Ack-Sent	Configuration acknowledgemt was sent; waiting for peer to respond to configuration request.
Authentication	Type of user authentication configured on the local equipment and on the peer equipment. Possible PPP authentication protocols are Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, and Password Authentication Protocol (PAP).
Closed	Lower layer is up, but this layer is not required.
Closing	Shutting down due to local change.
Initial	Connection is idle.
IPCP	IP Control Protocol (IPCP) state. The seven possible states that may be displayed are as follows: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— IPCP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a IPCP-Ack has not yet been received. Req-Sent. • ACKsent—IPCP has received a request and has replied to it. • ACKrcvd—IPCP has received a reply to a request it sent. • Open—IPCP is functioning properly.
Keepalive	Keepalive setting and interval in seconds for echo request packets.

Field	Description
LCP	Indicates the current state of LCP. The state of the LCP will report the following states: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— LCP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent. • ACKsent—LCP has received a request and has replied to it. • ACKrcvd—LCP has received a reply to a request it sent. • Open—LCP is functioning properly
Local IPv4 address	IPv4 address for the local interface.
Local MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the local equipment.
Open	Connection open.

Field	Description
OSICP	Open System Interconnection Control Protocol (OSICP) state. The possible states that may be displayed are as follows: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— OSICP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent. • ACKsent—OSICP has received a request and has replied to it. • ACKrcvd—OSICP has received a reply to a request it sent. • Open—OSICP is functioning properly.
Peer IPv4 address	IPv4 address for the peer equipment.
Peer MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the peer equipment.
Req-Sent	Configuration request was sent; waiting for peer to respond.
Starting	This layer is required, but lower layer is down.
Stopped	Listening for a configuration request.
Stopping	Shutting down as a result of interactions with peer.

show ppp sso alerts

To display all Inter-Chassis Stateful Switchover (ICSSO) alerts that have occurred, use the **show ppp sso alerts** command in EXEC mode.

show ppp sso alerts location *node-id*

Syntax Description

location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module*.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command displays the following information for alerts that have prevented a standby session from being brought to the Standby-Up state using replicated data.

- The interfaces on which the alerts have occurred
- The layer in which the error has occurred
- A short description of the error

Note Only one error is reported for each layer for each interface. The error displayed is the most recent error that has occurred.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to display all ICSSO alerts that have occurred:

```
RP/0/RP0/CPU0:router# show ppp sso errors location 0/3/cpu0

 Intf              Layer          SSO
 Name              with error     Error
 ------------------------------------------------------------------------------
 Mu0/3/0/0/100     IPCP           Unsupported IPCP option 0x07
 Se0/3/1/3/1:0     LCP            Unacceptable value for LCP MRU option
 Se0/3/1/3/2:0     of-us-auth     Incorrect Authentication protocol, CHAP
 Se0/3/1/3/3:0     of-peer-auth   Invalid CHAP Authentication options
 Se0/3/1/3/4:0     LCP            Inconsistent LCP MRRU options
```

show ppp sso state

To display the Inter-Chassis Stateful Switchover (ICSSO) states of a Point-to-Point Protocol (PPP) session running under a particular Multi-Router Automatic Protection Switching (MR-APS) group, use the **show ppp sso state** command in EXEC mode.

show ppp sso state group *group-id* **location** *node-id*

Syntax Description

group *group-id*	Specifies the redundancy group number. The range is 1 to 32.
location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module*.

Command Default

If group is not specified, states are displayed for all redundancy groups.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command shows the states of these session layers:

- LCP
- of-us authentication
- of-peer authentication
- IPCP

Note When an interface is in Standby mode, it is ready to forward traffic immediately after a switchover, if all the session layers, including IPCP, are in the S-Negd state.

Task ID

Task ID	Operations
ppp	read

Examples

The following example shows how to display the ICSSO states for PPP running under a redundancy group:

```
RP/0/RP0/CPU0:router# show ppp sso state location 0/3/cpu0

 Not-Ready : The session is not yet ready to run as Active or Standby
 S-UnNegd  : In Standby mode, no replication state received yet
 A-Down    : In Active mode, lower layer not yet up
 Deact'ing : Session was Active, now going Standby
 A-UnNegd  : In Active mode, not fully negotiated yet
```

```
S-Negd    : In Standby mode, replication state received and pre-programmed
Act'ing   : Session was Standby and pre-programmed, now going Active
A-Negd    : In Active mode, fully negotiated and up
-         : This layer not running

SSO-Group 1                     |            of-us     of-peer
Sess-ID    Ifname               |  LCP       auth      auth      IPCP
--------------------------------+-------------------------------------------
1          Multilink0/3/0/0/100 :  S-Negd    S-Negd    S-Negd    S-Negd

2          Multilink0/3/0/0/101 :  S-UnNegd  S-UnNegd  S-UnNegd  Not-Ready
3          Serial0/3/1/3/1      :  S-Negd    S-Negd    S-Negd    -
4          Serial0/3/1/3/2      :  A-Negd    A-Negd    A-Negd    A-UnNegd
5          Serial0/3/1/3/3      :  A-Down    Not-Ready Not-Ready -
6          Serial0/3/1/3/4      :  A-Up      A-Up      A-Up      A-Up

SSO-Group 1                     |            of-us     of-peer
Sess-ID    Ifname               |  LCP       auth      auth      IPCP
--------------------------------+-------------------------------------------
1          Multilink0/3/0/0/102 :  S-Negd    S-Negd    S-Negd    S-Negd

2          Serial0/3/1/3/5      :  S-Negd    S-Negd    S-Negd    -
3          Serial0/3/1/3/6      :  A-Negd    A-Negd    A-Negd    A-UnNegd
```

show ppp sso summary

To display the number of sessions in each Inter-Chassis Stateful Switchover (ICSSO) state for each session layer, use the **show ppp sso summary** command in EXEC mode.

show ppp sso summary location *node-id*

Syntax Description

location *node-id*	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module*.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

This command displays information for these session layers:

- LCP
- of-us
- of-peer authentication
- IPCP

Note Only sessions with Session State Redundancy Protocol (SSRP) configured are displayed.

Task ID

Task ID	Operations
ppp	read

Examples

This example shows how to display the number of sessions in each ICSSO state for each session layer.

```
RP/0/RP0/CPU0:router# show ppp sso summary location 0/3/cpu0

Not-Ready    : The session is not yet ready to run as Active or Standby
Stby-UnNegd  : In Standby mode, no replication state received yet
Act-Down     : In Active mode, lower layer not yet up
Deactivating : Session was Active, now going Standby
Act-UnNegd   : In Active mode, not fully negotiated yet
Stby-Negd    : In Standby mode, replication state received and pre-programmed
Activating   : Session was Standby and pre-programmed, now going Active
Act-Negd     : In Active mode, fully negotiated and up
-            : This layer not running
```

```
                      Not-   Stby-  Act- Deactiv- Act-   Stby-  Activ- Act
Layer         | Total  Ready  UnNegd Down   ating  UnNegd Negd   ating  Negd
--------------+------- ------ ------ ------ ------ ------ ------ ------ -----
LCP           |     20      2      5      0      0      3      6      0     4
of-us-auth    |     20     10      2      0      0      1      4      0     3
of-peer-auth  |     20     10      3      0      0      2      3      0     2
IPCP          |     10      1      2      1      0      3      2      0     1
```

ssrp group

To attach an Session State Redundancy Protocol (SSRP) group on an interface, use the **ssrp group** command in interface configuration mode. To remove the SSRP group from the interface, use the **no** form of this command.

ssrp group *group-number* **id** *id-number* **ppp**

Syntax Description

group-number	SSRP group number. The range is 1 to 65535.
id *id-number*	SSRP identifier number. The range is 1 to 4294967295.
ppp	Specifies point-to-point protocol.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The group must be configured first on a specific location (linecard) and then assigned to the interface. The redundancy ID must be unique within the group. This command specifies a list the protocols that the group can replicate. Currently only PPP is supported.

Task ID

Task ID	Operations
ppp	read, write

Examples

The following example shows how to

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RP0/CPU0:router(config-if)# ssrp group 1 id 1 ppp
```

ssrp location

To specify the node on which to create a Session State Redundancy Protocol (SSRP) group and enter the SSRP node configuration mode, use the **ssrp location** command in Global Configuration mode.

ssrp location *node_id*

Syntax Description

node_id	Specifies the full qualified path of a specific node in the format *rack*/*slot*/*module*.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

The location specifies the card on which an SSRP group is created.

Task ID

Task ID	Operations
ppp	read, write

Examples

This example shows how to create an SSRP group on a specified node for use by any interface on the card:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp location 0/1/cpu0
RP/0/RP0/CPU0:router(config-ssrp-node)#
```

ssrp profile

To configure a Session State Redundancy Protocol (SSRP) profile and enter the SSRP configuration mode, use the **ssrp profile** command in Global Configuration mode. To remove the profile, use the **no** form of this command.

ssrp profile *profile-name*

Syntax Description

profile-name	Name of this SSRP profile.

Command Default

No default behavior or values

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

A Session State Redundancy Protocol (SSRP) profile allows the same SSRP configuration to be shared across multiple groups. The same profile can be attached to multiple groups across the router. The group must be configured before the interface that uses the group can be configured. The group number is used in the TCP port number so, the group number must be unique across the router.

Task ID

Task ID	Operations
ppp	read, write

Examples

This example shows how to configure an SSRP profile:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RP0/CPU0:router(config-ssrp)#
```