Chapter 7

# Configuring Point-to-Point Protocol

This chapter describes how to configure a Point-to-Point Protocol (PPP) interface on E-series routers.

This chapter contains the following sections:



## Overview

PPP provides a standard method for transporting multiprotocol datagrams over a point-to-point link. PPP uses the High-Speed Data Link Control (HDLC) protocol for its physical interface and provides a packet-oriented interface for the network-layer protocols.

Internet Protocol Control Protocol (IPCP) (which negotiates for transport of IP version 4 datagrams), IPv6CP (which negotiates for transport of IP version 6 datagrams), the OSI Network Layer Control Protocols (OSINLCPs), and Multiprotocol Label Switching (MPLS) run within PPP.

The router supports dynamic PPP interfaces. For details, see *Chapter 15, Configuring Dynamic Interfaces*.

### Framing

The software restricts the use of the general HDLC protocol (RFC 1662) to unnumbered mode:

- HDLC address field is 0xFF (all stations)
- HDLC control field is 0x03 (to indicate unnumbered mode)

The router does not support the following framing features:

- Numbered mode (RFC 1663)
- Autodetection of encapsulation

### Error Frames

The router relies on higher-layer protocols to recover from PPP data loss. All unrecognized protocol data units (PDUs) are discarded; however, statistics are maintained for packets dropped.

### Link Control Protocol

PPP's Link Control Protocol (LCP) establishes a PPP link by negotiating with the PPP peer at the other end of a proposed connection. When two routers initialize a PPP dialogue, each router sends control packets to the peer. The control packets contain a list of LCP options and corresponding values that the sending peer uses to define its end of the link, such as the maximum receive unit (MRU).

LCP negotiations continue until the peers either converge (that is, reach an agreement about values for connection parameters) or abandon attempts to establish a connection.

If you configure a PPP interface without an IP interface or profile, the router negotiates LCP, but then terminates LCP after 2 to 3 minutes. Previously, the behavior in such a circumstance was to negotiate LCP and then leave LCP open.

For static PPP interfaces, whenever LCP achieves a stopped state because of termination, negotiation failure, or some other cause, it goes into passive mode and waits for the other side of the connection to restart the negotiation process. Once in passive mode, the router periodically attempts to negotiate with the other side according to an exponential timeout algorithm.

For static PPP interfaces, the router waits 15 seconds, attempts negotiation, waits 30 seconds if it fails, attempts negotiation, waits 60 seconds if it fails, and so on. The timeout periods are 15 seconds, 30 seconds, 60 seconds, 2 minutes, 4 minutes, 8 minutes, and 15 minutes. Once it reaches the 15-minute timeout, the router attempts negotiation every 15 minutes until successful. When LCP reaches the open state, the timer resets to 15 seconds.

Dynamic PPP interfaces are always torn down when LCP achieves a stopped state. For more information, see *Chapter 15, Configuring Dynamic Interfaces*.

### LCP Negotiation Parameters

LCP can negotiate many PPP options, as follows:

- MRU size—Maximum receive unit size (always accepted).
- Magic number—Randomly generated number used to identify one end of a point-to-point connection. Each side negotiates its magic number, taking note of each other's magic number. If both sides discover that the magic numbers they are negotiating are the same, each side attempts to change its magic number. If they are not successful, and the magic numbers remain the same, the session terminates because of the loopback that is detected. Magic numbers are always accepted.

  By default, the router always attempts to negotiate a local magic number. The peer can also determine whether to negotiate its magic number—the peer magic number. The router always accepts a peer's attempt to negotiate its magic number.

  If the peer does not attempt to negotiate its magic number, you can configure the router to ignore a mismatch of the peer magic number and retain the PPP connection. For details, see *Validation of LCP Peer Magic Number* on page 224.
- Authentication—Requested if configured.
- Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (ACFC)—Accepted, but never requested.
- Multilink PPP—Additional options can be negotiated when Multilink PPP is configured. See *Chapter 8, Configuring Multilink PPP*.
- Async-Control-Character-Map (ACCM—Supported by PPP when used with an L2TP Network Server (LNS). ACCM allows PPP to indirectly support asynchronous PPP connections tunneled via a third-party L2TP Access Concentrator (LAC). PPP on the router uses the ACCM configuration data as supplied by the LAC via proxy LCP. The router does not directly support asynchronous PPP connections and will not negotiate an ACCM option unless directed to do so by a third-party LAC.

PPP can also detect a loopback that occurs after LCP is negotiated, provided that:

- No loopback occurs during LCP negotiations.
- A loopback is introduced after LCP negotiation without forcing LCP renegotiation. (LCP is renegotiated if the lower layer goes down or if an LCP confReq is received from the other end.)

### Validation of LCP Peer Magic Number

If the peer has not negotiated an LCP magic number, you can configure the router to ignore a mismatch of the LCP peer magic number and retain the PPP connection.

Previously, the router terminated a PPP connection with a non-conforming peer when it received LCP echo request packets or LCP echo reply packets from the peer with a magic number that did not match the LCP peer magic number on the router. This is still the current default behavior if you do not explicitly configure the router to ignore the LCP peer magic number mismatch if the peer has not negotiated the magic number and retain the PPP connection.

Configuring the router to ignore the peer magic number mismatch and retain the PPP connection is useful if your network includes peers that send a non-null or invalid magic number in the LCP echo request and reply packets despite having not negotiated the magic number. In this situation, the router expects to receive a null magic number from the peer, and terminates the PPP connection unless you configure it to ignore the peer magic number mismatch and retain the connection.

To configure the router to ignore the LCP peer magic number mismatch and retain the PPP connection, use the **ppp magic-number ignore-mismatch** command from Interface Configuration mode or Subinterface Configuration mode. For more information, see **ppp magic-number ignore-mismatch** on page 237.

To verify configuration of LCP peer magic number validation on the router, you can use the **show ppp interface** command. For more information, see **show ppp interface** on page 243.

Keep the following points in mind when configuring the router to ignore the peer magic number mismatch and retain the PPP connection:

- If the peer negotiates the magic number but sends the router an LCP echo request or reply packet that contains a null or invalid magic number, the router strictly terminates the PPP connection. The router can ignore a mismatch of the LCP peer magic number only when the peer has not negotiated the magic number.

- Using the **ppp magic-number disable** command to disable negotiation of the magic number on the router does not affect validation of the peer magic number. When you issue the **ppp magic-number disable** command, the router sets only the local magic number to null, but does not change or validate the peer magic number. (For more information, see **ppp magic-number disable** on page 236.)

You can also configure validation of the LCP peer magic number for static MLPPP interfaces, dynamic PPP interfaces, and dynamic MLPPP interfaces. For more information about configuring static MLPPP interfaces, see *Chapter 8, Configuring Multilink PPP*. For more information about using profiles to configure dynamic PPP and dynamic MLPPP interfaces, see *Configuring a Dynamic Interface from a Profile* in *Chapter 15, Configuring Dynamic Interfaces*.

### B-RAS Support

Broadband Remote Access Server (B-RAS) is an application that aggregates the output from digital subscriber line access multiplexers (DSLAMs). B-RAS provides user PPP sessions and PPP session termination and routes traffic onto the backbone. See *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access* for details on B-RAS.

The router provides an enhanced version of PPP to accommodate B-RAS with the following features:

- Internet Protocol Control Protocol (IPCP) extensions for Windows Internet Name Service (WINS) and Domain Name System (DNS) name server addresses
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Keepalive timeout
- Session timeout
- Inactivity timeout
- Accounting

### Authentication

The router acts as an authenticator. It demands authentication from a remote PPP peer but refuses to authenticate itself.

### Rate Limiting for PPP Control Packets

The router implements rate limiting for PPP control packets to protect the corresponding PPP interface from denial-of-service (DoS) attacks. The interface discards control packets when the rate of control packets received exceeds the rate limit for PPP interfaces.

A PPP interface has a rate limit control that is non-configurable and always in effect; the rate limit is the same for all PPP interfaces. In addition, each interface instance maintains its own state and statistics counters for tracking the rate. The rate limit for PPP control packets is approximately 10 packets per second.

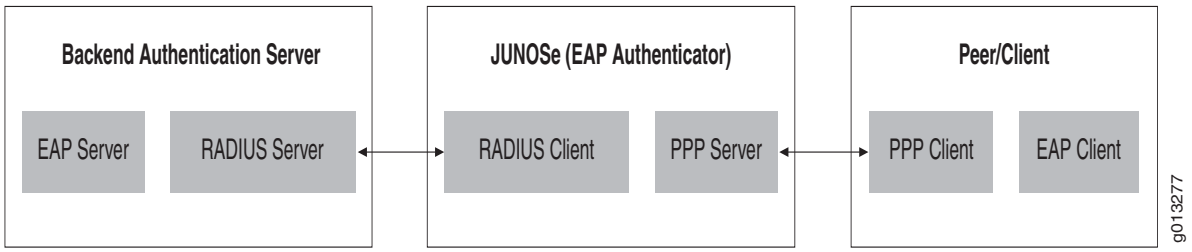
For a PPP interface, the router increments the discards counter in the **show ppp interface** command display to track the number of PPP control packets discarded on receipt (in) or discarded before they were transmitted (out) on this interface.

For examples of the **show ppp interface** command display, see **show ppp interface** on page 243.

### *Extensible Authentication Protocol*

The JUNOSe software supports Extensible Authentication Protocol (EAP) for authenticating a peer before allowing network layer protocols to transmit over the link. EAP supports multiple authentication methods, including EAP-TLS and EAP-MD5-Challenge. The EAP server and the peer negotiate the specific authentication method to be used. Figure 30 illustrates the three components required for EAP: an EAP authenticator, an EAP server, and an EAP client.

**Figure 30: Authentication with EAP**




After LCP negotiation, JUNOSe starts the EAP negotiation process by initiating an identity exchange with the EAP client on the peer. The router sends an EAP identity request packet to the peer, which replies with an EAP identity response packet. After this exchange, the E-series router acts only as a pass-through device, enabling the EAP server residing on the backend authentication server to select and negotiate the particular EAP authentication method directly with the EAP client on the peer.

The JUNOSe software forwards or discards packets received from the backend authentication router and the peer depending on the identifying code contained in the packet.

The E-series router forwards:

- Packets received from the peer with a Response code
- Packets received from the backend authentication server with a Request, Success, or Failure code

The E-series router discards:

- Packets received from the peer with a Request, Success, or Failure code
- Packets received from the backend authentication server with a Response code

The JUNOSe software determines the outcome of the authentication based only on the Accept or Reject indication sent by the RADIUS server

## EAP Types

The JUNOSe software has been qualified to work with the EAP authentication methods—known as EAP types—described in Table 12. Other EAP authentication methods have not been qualified with the JUNOSe software.

**Table 12: Supported EAP Types**

| EAP Type | Behavior |
|---|---|
| 1—Identity | When LCP negotiation completes, PPP sends an initial EAP identity request packet to the peer. The EAP identity response packet received from the peer is forwarded to AAA. AAA forwards the response as an Access-Request to the RADIUS server hosted on the backend authentication server. |
| 2—Notification | The JUNOSe software forwards Notification requests from the backend authentication server to the peer and Notification responses from the peer to the server. The JUNOSe software does not initiate any Notification requests or responses. |
| 3—NAK | The JUNOSe software forwards the NAKs received from the peer to the backend authentication server. |
| 4—MD5-Challenge | The JUNOSe software acts as a pass-through for the EAP-MD5-Challenge negotiated between the peer and backend authentication server. |
| 13—TLS | The JUNOSe software acts as a pass-through for the EAP-TLS negotiated between the peer and backend authentication server. |

## EAP Packet Retransmission

PPP retransmits the EAP request packets to the peer. The RADIUS client retransmits the EAP response packets to the RADIUS Server. The request packets to the peer are governed by nonconfigurable values for retransmission attempts and interval. The configuration of the RADIUS client determines retransmission values for response packets to the RADIUS server. The retransmission values are as follows:

- PPP makes five attempts to retransmit an EAP request before the authentication attempt is terminated. You cannot configure the number of retransmission attempts.
- When an EAP request is transmitted, a timer is started with a nonconfigurable retransmission interval value of 3 seconds. When the timer expires, the EAP request is retransmitted.

In some cases, you might want a longer retransmission interval. For example, you might need to accommodate the additional time required by a user to enter information or scan a fingerprint or retina. RADIUS can instruct the JUNOSe software to wait longer by passing an appropriate Session-Timeout attribute in the RADIUS Access-Challenge packet. This retransmission interval value applies only to the EAP request packet present in the RADIUS Access-Challenge packet.

The Session-Timeout attribute value overrides the default retransmission interval value, up to a maximum of 30 seconds. If RADIUS recommends a greater value, then PPP resets it back to 30 seconds in order to avoid longer or infinite delays.

## EAP Behavior in an L2TP Environment

EAP behavior in an L2TP environment varies depending on whether the router acts as a LAC or an LNS,

### *When the E-series Router Acts as a LAC*

When PPP forwards an EAP identity response packet to AAA, AAA might be configured to return a tunnel response upon successful validation of the packet. You can use AAA domain maps, a AAA profile, or both to force such tunneling.

On an LAC, PPP forwards the PPP EAP authentication information to the LNS during the establishment of the L2TP session. This authentication information consists of the EAP type, the data appropriate to the type (such as a username) contained in the EAP identity response packet, and the identifier of the EAP identity response packet. If the LNS trusts the LAC, then the LNS uses this authentication information to resume the EAP negotiation where the LAC left off.

L2TP on an LAC forwards the PPP EAP authentication information in the Proxy Authen AVPs as described in L2TP Proxy Authenticate Extensions for EAP—draft-ietf-l2tpext-proxy-authen-ext-eap-01.txt (December 2006 expiration).

### *When the E-series Router Acts as an LNS*

PPP on an LNS resumes the EAP negotiation operation by detecting the presence of EAP information in the proxy authentication data supplied by L2TP. PPP reconstructs the EAP identity response packet from the proxy authentication data and forwards it to AAA.

L2TP on an LNS processes the received Proxy Authen AVPs as described in L2TP Proxy Authenticate Extensions for EAP—draft-ietf-l2tpext-proxy-authen-ext-eap-01.txt (December 2006 expiration).

## Limitations

EAP is subject to internal limits. When the E-series router acts as a pass-through between the backend authentication server and the peer, EAP packets traverse the controllers within the router. The size of EAP packets and fragments tends to be larger than the buffer exchange limit—1450 bytes—between the controllers. This intercontroller buffer exchange limit is tuned for the optimal system performance and scalability; also, when stacked over L2TP on LNS, it prevents PPP control packets from causing IP fragmentation and reassembly on the Ethernet downlink. Hence, if EAP is configured as a PPP authentication protocol, then EAP packet or fragment size is affected by the intercontroller buffer exchange limit as follows:

- The MRU value advertised by JUNOSe in the LCP request packet takes the lowest of the following values:
  - the lower layer MRU minus the PPP overhead
  - the configured MRU
  - 1450 bytes
- The MTU value is initialized by JUNOSe to the lowest of the following values:

- the lower layer MTU minus the PPP overhead
- the peer MRU
- 1450 bytes

The MTU value is passed to RADIUS in an Access-Request packet by means of the Framed-Mtu attribute.

### Performance

When EAP is configured on the router, it affects the performance and scalability of PPP in terms of round-trip packet exchanges, negotiations, EAP server requirements, and EAP client requirements. For information on the number of PPP interfaces supported with EAP, see the *Link Layer Maximums* tables in *Appendix A, System Maximums*, of the current *JUNOSe Release Notes*.

- Performance depends on the number of packets exchanged during the negotiation. When the number of packets exchanged increases—that is, when the number of round-trips increases—it takes longer to finish the interface negotiation. System resources are locked for a longer duration. As a result it takes longer to bring up all the interfaces.

  The number of round-trip message exchanges varies with the EAP authentication method. When no retransmission of packets takes place and there is no fragmentation, PAP and CHAP require one round-trip, EAP-MD5-Challenge requires two round-trips, and EAP-TLS requires four round-trips.

  Retransmission increases the number of round-trips. When the negotiated EAP authentication method requires fragmentation, such as for the exchange of large certificate chains, then the number of round-trips increases.

- The number of simultaneous EAP negotiations is limited to 50 because of resource limitations. Consequently, the time required to bring up interfaces when you configure EAP authentication is longer than when you specify PAP or CHAP authentication.

- EAP authentication methods fragment packets when the EAP packet size is greater than the link MTU. The EAP server must fragment the EAP packet to the size of the Framed-Mtu attribute contained in the RADIUS Access-Request packet.

  If the server fragments the packet to a larger size than specified by the attribute, then JUNOSe drops the packet, because the E-series router acts as a pass-through device and is not involved in the authentication method's fragmentation and reassembly mechanisms.

  On the other hand, if the EAP server fragments the EAP packet to a smaller size than specified by the attribute, then performance decreases because of the increased number of smaller packets that must be exchanged.

- The EAP client on the peer must fragment the EAP packets to the size of the link MTU on the E-series router. When it does not do so, performance can be affected.

## Platform Considerations

You can configure PPP interfaces on the following E-series routers:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

### *Module Requirements*

For information about the modules that support PPP interfaces on ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support PPP.

For information about the modules that support PPP interfaces on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support PPP.

### *Interface Specifiers*

Some of the configuration task examples in this chapter use the *slot*/*port*[.*subinterface* ] format to specify the physical interface on which you want to configure PPP. However, the interface specifier format that you use depends on the router that you are using.

For ERX-7xx models, ERX-14xx models, and ERX-310 routers, use the *slot*/*port*[.*subinterface* ] format. For example, the following command specifies ATM 1483 subinterface 10 on slot 0, port 1 of an ERX-7xx model, ERX-14xx model, or ERX-310 router. n

```
host1(config)#interface atm 0/1.10
```

For E120 and E320 routers, use the *slot*/*adapter*/*port*[.*subinterface* ] format, which includes an identifier for the bay in which the I/O adapter (IOA) resides. In the software, adapter 0 identifies the right IOA bay (E120 router) and the upper IOA bay (E320 router); adapter 1 identifies the left IOA bay (E120 router) and the lower IOA bay (E320 router). For example, the following command specifies ATM 1483 subinterface 20 on slot 5, adapter 0, port 0 of an E320 router.

```
host1(config)#interface atm 5/0/0.20
```

For more information about supported interface types and specifiers on E-series routers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

## References

For more information about the PPP protocol, consult the following resources:

- L2TP Proxy Authenticate Extensions for EAP—draft-ietf-l2tpext-proxy-authen-ext-eap-01.txt (December 2006 expiration)
- RFC 1332—The PPP Internet Protocol Control Protocol (IPCP) (May 1992)
- RFC 1661—The Point-to-Point Protocol (PPP) (July 1994)
- RFC 1662—PPP in HDLC-like Framing (July 1994)
- RFC 1877—PPP Internet Protocol Control Protocol Extensions for Name Server Addresses (December 1995)
- RFC 1994—PPP Challenge Handshake Authentication Protocol (CHAP) (August 1996)
- RFC 2153—PPP Vendor Extensions (May 1997)
- RFC 2246—The TLS Protocol Version 1.0 (January 1999)
- RFC 2615—PPP over SONET/SDH (June 1999)
- RFC 2716—PPP EAP TLS Authentication Protocol (October 1999)
- RFC 3032—MPLS Label Stack Encoding (January 2001)
- RFC 3579—RADIUS EAP (September 2003)
- RFC 3748—Extensible Authentication Protocol (EAP) (June 2004)

**NOTE:** IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

## Before You Configure PPP

Before you configure a PPP interface, configure the interface or tunnel over which PPP traffic will flow. See the following chapters:

- *JUNOSe Physical Layer Configuration Guide, Chapter 1, Configuring Channelized T3 Interfaces*
- *JUNOSe Physical Layer Configuration Guide, Chapter 2, Configuring T3 and E3 Interfaces*
- *JUNOSe Physical Layer Configuration Guide, Chapter 3, Configuring Unchannelized OCx/STMx Interfaces*
- *JUNOSe Physical Layer Configuration Guide, Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces*
- *Chapter 1, Configuring ATM*
- *Chapter 9, Configuring Packet over SONET*
- *Chapter 10, Configuring Point-to-Point Protocol over Ethernet*

The procedures described in this chapter assume that a physical interface has been configured.

## Configuration Tasks

The following procedure is an example of a PPP configuration on a serial interface. These steps are mandatory unless otherwise noted.

1. From Global Configuration mode, specify the physical interface on which you want to configure PPP.

   host1(config)#**interface serial 3/0:2/5**

2. Specify PPP as the encapsulation method (data-link protocol) on the interface.

   host1(config-if)#**encapsulation ppp**

3. Assign an IP address and subnet mask for the interface.

   host1(config-if)#**ip address 192.168.22.10 255.255.255.0**

4. Verify that your configuration changes are correct.

   host1#**show ppp interface serial 3/0:2/5 config**

***encapsulation ppp***

- Use to configure PPP as the encapsulation method.
- Example

  host1(config-if)#**encapsulation ppp**

- Use the **no** version to disable PPP on an interface.

***interface atm***

- Use to specify a previously configured ATM interface on which you want to configure PPP.
- To specify an ATM interface for ERX-7xx models, ERX-14xx models, and ERX-310 routers, use the *slot*/*port*.[*subinterface* ] format.
  - *slot*—Number of the chassis slot
  - *port*—Port number on the I/O module
  - *subinterface*—Number of the subinterface in the range 1–2147483647
- To specify an ATM interface for E120 and E320 routers, use the *slot*/*adapter*/*port*[.*subinterface* ] format.
  - *slot*—Number of the chassis slot
  - *adapter*—Identifier for the IOA within the E320 chassis, either 0 or 1, where:
    - 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router).
    - 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router).
  - *port*—Port number on the IOA
  - *subinterface*—Number of the subinterface in the range 1–2147483647
- For more information, see *Creating a Basic Configuration* in *Chapter 1, Configuring ATM*.
- Examples

  host1(config-if)#**interface atm 9/1.1**
  host1(config-if)#**interface atm 5/0/1.1**

- Use the **no** version to disable or remove the subinterface or the logical interface.

***interface pos***

- Use to specify a previously configured packet over SONET (POS) interface on which you want to configure PPP.
- To specify a POS interface for ERX-7xx models, ERX-14xx models, and ERX-310 routers, use the *slot*/*port*.[*subinterface* ] format.
  - *slot*—Number of the chassis slot
  - *port*—Port number on the I/O module
  - *subinterface*—Number of the subinterface

- To specify a POS interface for E120 and E320 routers, use the *slot/adapter/port* format.
  - *slot*—Number of the chassis slot
  - *adapter*—Identifier for the IOA within the E320 chassis, either 0 or 1, where:
    - 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router).
    - 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router).
  - *port*—Port number on the IOA
- For more information about modules that support POS interfaces, see *JUNOSe Physical Layer Configuration Guide, Chapter 3, Configuring Unchannelized OCx/STMx Interfaces*.
- Examples

  host1(config-if)#**interface pos 0/1**
  host1(config-if)#**interface pos 5/0/0**

- Use the **no** version to remove the POS interface.

### *interface serial*

- Use to specify a serial interface in the *slot/port:channel/subchannel* format by selecting a previously configured physical interface on which you want to configure PPP.
  - *slot*—Refers to a router chassis slot.
  - *port*—Refers to a CT3, T3, or E3 module I/O port.
  - *channel*—Refers to a T1 (DS1) channel.
  - *subchannel*—Represents a set of DS0 subchannels.
- Example

  host1(config)#**interface serial 3/0:2/5**

- Use the **no** version to disable or remove the subinterface or the logical interface.

### *ip address*

- Use to assign an IP address and subnet mask for a PPP interface.
- Example

  host1(config-if)#**ip address 192.168.22.10 255.255.255.0**

- Use the **no** version to remove an IP address or disable IP processing.

## Optional Configuration Tasks

You can perform the following optional PPP configuration tasks:

- Add a text description or alias to a PPP interface.
- Configure the IPCP netmask option (option 0x90).
- Specify the keepalive timeout value.
- Disable magic numbers.
- Control validation of the LCP peer magic number when the peer has not negotiated an LCP magic number.
- Specify the maximum receive units.
- Configure passive mode.
- Configure name server addressing.
- Stop or restart a PPP session.
- Configure PPP authentication.

### *ppp description*

- Use to assign a text description or alias to a static PPP interface.
- Example

  host1(config-if)#**ppp description pah8999**

- Use the **no** version to remove the description.

### *ppp ipcp netmask*

- Use to specify the IPCP netmask option (option 0x90) for each PPP interface. By default, the IPCP netmask option is disabled on the interface.
- The IPCP netmask option is a nonstandard option that enables a peer to request the netmask associated with the assigned IP address.
- The netmask can be specified via RADIUS attribute 9, Framed-Ip-Netmask. If the netmask is 255.255.255.255, the option is not negotiated. See the **radius ignore framed-ip-netmask** command.
- You can enable the IPCP netmask option either in a profile or on a static interface.
- Example

  host1(config-subif)#**ppp ipcp netmask**

- Use the **no** version to disable the IPCP netmask option on the interface.

***ppp keepalive***

- Use to specify the keepalive timeout value.
- There are two keepalive modes of operation: high-density mode and low-density mode.
  - High-density keepalive mode is automatically selected if PPP is layered over ATM, L2TP, or PPPoE.
  - Low-density keepalive mode is selected if PPP is layered over HDLC. Keepalive mode selection is made per interface.
- High-density mode—This mode is also known as smart keepalive. When the keepalive timer expires, the interface first verifies whether any frames were received from the peer in the prior keepalive timeout interval. If so, the interface does not send an LCP echo request (keepalive). Keepalive packets are sent only if the peer is silent (that is, no traffic was received from the peer during the previous keepalive timeout interval). If both sides are configured with keepalive, receipt of an LCP echo request by one end suppresses the transmission of an LCP echo request by that end. Smart keepalive is disabled when the keepalive timeout value is at least 60 seconds, even when in high-density mode. Smart keepalive is always disabled when in low-density mode. This mode suppresses transmission of unnecessary LCP echo requests.
- For high-density keepalive mode, the range is 30–64800 seconds. The default value is 30 seconds.
- Low-density mode—When the keepalive timer expires, the interface *always* sends an LCP echo request, regardless of whether the peer is silent.
- For low-density keepalive mode, the range is 1–64800 seconds for POS uplink interfaces, and 10–64800 seconds for all other HDLC interfaces. The default value for all interfaces is 30 seconds.
- If the keepalive interval is 30 seconds, a failed link is detected between 90 and 120 seconds after failure.
- Use **ppp keepalive** without a value to restore the default, 30 seconds.
- Example

  host1(config-if)#**ppp keepalive 50**

- Use the **no** version to disable keepalive.

***ppp magic-number disable***

- Use to disable negotiation of the local magic number.
- Issuing this command prevents the router from detecting loopback configurations.
- Example

  host1(config-if)#**ppp magic-number disable**

- Use the **no** version to restore negotiation of the local magic number.

***ppp magic-number ignore-mismatch***

- Use to cause the router to ignore a mismatch of the LCP peer magic number and retain the PPP connection when the peer has not negotiated an LCP magic number.
- For more information about using this command, see *Validation of LCP Peer Magic Number* on page 224.
- Example

  host1(config-if)#**ppp magic-number ignore-mismatch**

- Use the **no** version to restore the default behavior, in which the router terminates the PPP connection if it detects an LCP peer magic number mismatch.

***ppp mru***

- Use to control the negotiation of the maximum receive unit (MRU).
- Specify the number of bytes, in the range 64–65535.
- We recommend you coordinate this value with the network administrator on the other end of the line.
- If the value configured for the PPP MRU is greater than the value of the lower-layer MRU minus the PPP header length, the router logs a warning message and uses the lesser of the configured MRU value or the lower-layer MRU value minus the PPP header length to negotiate the local MRU.
- If the value configured for the PPP MRU conflicts with a similar value configured for another protocol, such as the MTU value for PPPoE, the router uses the lesser of the two values.
- Example

  host1(config-if)#**ppp mru 576**

- Use the **no** version to restore the default value, which causes PPP to use the lower-layer MRU minus the PPP header length as the MRU value.

***ppp passive-mode***

- Use to force a static or dynamic PPP interface into passive mode before LCP negotiation begins, for a period of one second. This delay enables slow clients to start up and initiate the LCP negotiation.
- Example

  host1(config-if)#**ppp passive-mode**

- Use the **no** version to disable passive mode.

***ppp peer***

- Use to resolve conflicts when the router and the PPP peer have the primary and secondary DNS and WINS name server addresses configured with different values.
- By default, the DNS and WINS addresses configured on the router take precedence.

- Use the **dns** keyword or the **wins** keyword to configure which PPP peer address takes precedence. This command has no effect unless both routers have the address configured and the address is in conflict. If the PPP peer has the address and the router does not, the peer always supplies the address regardless of how you have configured the PPP peer.
- Example

  host1(config-if)#**ppp peer dns**

- Use the **no** version when you want the router to take precedence during setup negotiations between the router and the peer. If the IP addresses that the peer sends to the router differ from the ones configured on your router, the router returns the values that you configured as the correct values to the peer.

***ppp shutdown***
***ppp shutdown ip***
***ppp shutdown ipv6***
***ppp shutdown mpls***
***ppp shutdown osi***

- Use to terminate a PPP session.
- To administratively disable the interface, use the **ppp shutdown** command.
- To administratively disable IPCP, use the **ppp shutdown ip** command.
- To administratively disable IPv6CP, use the **ppp shutdown ipv6** command.
- To administratively disable MPLS, use the **ppp shutdown mpls** command.
- To administratively disable OSINLCP, use the **ppp shutdown osi** command.
- All PPP sessions are enabled by default.
- Example

  host1(config-if)#**ppp shutdown**

- Use the **no** version to restart a disabled session.

## *Configuring PPP Authentication*

Perform the following optional tasks to configure PPP authentication:

- Specify one or more PPP authentication types, and select an authentication virtual router context.
- Specify the CHAP challenge length.
- Specify the maximum number of retries.

**NOTE:** The JUNOSe software's PPP application accepts null usernames during PAP and CHAP authentication. When the PPP application receives an authentication request that includes a null username, PPP passes the request to AAA. To take advantage of this feature, configure your authentication server to support the use of null usernames.

***ppp authentication***

- Use to request authentication from a PPP peer and set the authentication method.
- To specify the name of a virtual router (VR) to be used as the authentication VR context, use the **virtual-router** keyword. Keep the following points in mind when you use the **ppp authentication virtual-router** command:
  - When you specify a VR in the **ppp authentication** command, AAA does not query the domain map for the assigned VR context. Instead, AAA uses the VR specified in the **ppp authentication** command as the authentication VR context and issues the authentication request to the authentication server in the assigned VR context.
  - If you specify the default VR as the authentication VR context, AAA loosely binds the user to the default VR. This means that RADIUS *can override* the default VR context with a new VR context during the authentication process. When the **ppp authentication virtual-router** command specifies the default VR, AAA returns either the default VR or the VR specified by RADIUS.
  - If you specify a VR other than the default VR as the authentication VR, AAA tightly binds the user to the specified VR. This means that RADIUS *cannot override* the specified VR context with a new VR context during the authentication process. When the **ppp authentication virtual-router** command specifies a nondefault VR, AAA returns the specified VR.
- The router supports the MD5 authentication algorithm for CHAP authentication.
- You can specify one or more authentication protocols in order of preference. If the peer router refuses the first choice, then the local router requests the next authentication protocol, if specified. If the peer refuses that protocol, then the local router requests the third protocol, if specified. If the peer refuses all specified authentication protocols, then the local router terminates the session.
- Example 1—Specifies the order of preference for the primary authentication protocol

  host1(config-if)#**ppp authentication pap chap eap**

  The router requests the use of PAP as the authentication protocol (because it appears first in the command line). If the peer refuses to use PAP, the router requests the CHAP protocol. If the peer refuses to use CHAP, the router requests the EAP protocol. If the peer refuses to negotiate authentication, the router terminates the PPP session.

- Example 2—Specifies a virtual router for the authentication virtual router context

  host1(config-if)#**ppp authentication virtual-router boston pap chap**

  This command is available in static configurations and in profiles.

- Example 3—Configures only EAP on a static PPP interface

  host1(config)#**interface atm 3/2.100**
  host1(config-subif)#**ppp authentication eap**

- Example 4—Configures EAP or PAP on a static PPP interface

  host1(config)#**interface atm 3/2.100**
  host1(config-subif)#**ppp authentication eap pap**

  EAP negotiation is attempted first. If PPP receives a NAK from the peer in response to the EAP request, then PAP is attempted. If PAP is also rejected, then PPP terminates the session.

- Example 5—Configures only EAP on a dynamic PPP interface

  host1(config)#**profile ppptest**
  host1(config-profile)#**ppp authentication eap**

- Example 6—Configures EAP or CHAP or PAP on a dynamic PPP interface

  host1(config)#**profile ppptest**
  host1(config-profile)#**ppp authentication eap chap pap**

  In this example, the router first attempts EAP negotiation. If PPP receives a NAK from the peer in response to the EAP request, then the router attempts CHAP negotiation. If PPP receives a NAK from the peer in response to the CHAP request, then the router attempts PAP negotiation. If PAP is also rejected, then PPP terminates the session.

- Use the **no** version to specify that the router does not require authentication.

### *ppp chap-challenge-length*

- Use to modify the length of the CHAP challenge by specifying the allowable minimum length and maximum length.
- Specify the minimum and maximum lengths in bytes in the range 8–63.

**CAUTION:** Do *not* decrease the range. Increasing the range is acceptable, provided that you do not lower the minimum to do so. The recommended minimum is 16. A longer challenge and a more unpredictable challenge length provide a higher level of security.

- The maximum length must be greater than or equal to the minimum length.
- Example

  host1(config-if)#**ppp chap-challenge-length 24 28**

- Use the **no** version to restore the default minimum (16 bytes) and default maximum (32 bytes).

### *ppp max-bad-auth*

- Use to specify the maximum number of authentication retries the router allows before terminating a PPP session
- This value applies to PAP and CHAP authentication.
- The range is 0–7. The default is 0, which indicates that no retries are allowed.

- Example

  host1(config-if)#**ppp max-bad-auth 3**

- Use the **no** version to return the number of retries to the default, 0.

## PPP Accounting Statistics

The JUNOSe software begins the collection of accounting statistics for terminated PPP sessions following, but not including, authentication acknowledgement from the E-series router. The acknowledgment is either a CHAP success or PAP acknowledgement packet. All subsequent traffic is counted up the point that PPP at the router terminates the subscriber's session. The statistics are reported in the following RADIUS attributes:

| Attribute Number | Attribute Name |
|---|---|
| 42 | Acct-Input-Octets |
| 43 | Acct-Output-Octets |
| 47 | Acct-Input-Packets |
| 48 | Acct-Output-Packets |

PPP session termination can be initiated through a number of mechanisms: PPP shutdown at the client or router interface, subscriber logout at the router (by means of the **logout subscriber** command), lower layer down events, and silent client termination.

The following rules apply to all termination scenarios:

- Accounting statistics reported in RADIUS octet counts (Acct-Input-Octets and Acct-Output-Octets) for terminated PPP customers include the following data:
  - All upper layer control traffic, including IPCP, IPCPv6, OSICP, and MPLSNCP
  - All data traffic, including IP, IPv6, MPLS, and OSI
  - All PPP LCP echo requests and responses following authentication
  - Other PPP LCP packets following the PAP or CHAP acknowledgment
  - Retransmits of the PAP or CHAP traffic

- PPP accounting statistics reported in RADIUS octet counts (Acct-Input-Octets and Acct-Output-Octets) exclude the following data:
  - PPP traffic prior to completion of authentication
  - PPP LCP terminate-request or terminate-acknowledgement packets
  - PPPoE padding for PPP control and data packets
- Accounting statistics reported in RADIUS packet counts (Acct-Input-Packets and Acct-Output-Packets) for terminated PPP customers are based on packets delivered to or received from the upper transport layer: IP, IPv6, MPLS, and OSI.

For information on accounting statistics for tunneled PPP sessions, see *PPP Accounting Statistics* in *JUNOSe Broadband Access Configuration Guide, Chapter 13, Configuring an L2TP LNS*.

## Monitoring PPP Interfaces

Use the following versions of the **show ppp interface** command to monitor PPP interfaces:

- **show ppp interface**
- **show ppp interface summary**

You can set a statistics baseline for PPP interfaces using the **baseline ppp** commands. Use the optional **delta** keyword with PPP **show** commands to show baselined statistics.

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string that you specify. Refer to *show Commands* in *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*, for details.

**NOTE:** The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

### *baseline ppp interface*

- Use to establish a baseline for PPP statistics on an interface.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set, then subtracting this baseline whenever baseline-related statistics are retrieved.
- Use the optional **delta** keyword with PPP **show** commands to show baselined statistics.

- Examples

  host1#**baseline ppp interface atm 3/3.20**
  host1#**baseline ppp interface atm 3/0/3.20**

- There is no **no** version.

***show ppp interface***

- Use to display selective PPP interface information.
- You can filter the command display for characteristics of particular interest, such as interface type, data type, configured protocol, or interface state.
- Field descriptions
  - PPP interface—Interface type, interface specifier, and status (up, down, lowerDown, not present, passive, or tunnel). For more information about specifying the physical interface on which you want to configure PPP, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.
  - Interface alias—Alias or description of the PPP interface
  - Interface administrative status—Indicates whether the interface is administratively enabled (open), meaning that the **no ppp shutdown** command is operational; or administratively disabled (closed), which means that the **ppp shutdown** command is operational
  - Configured network protocol—Indicates the network protocol configured on the interface
  - Baseline status—Indicates whether a statistics baseline is set
  - Interface statistics
    - packets—Number of packets received (in) or transmitted (out) on the interface
    - octets—Number of octets received (in) or transmitted (out) on the interface
    - errors—Number of errors received (in) or transmitted (out) on the interface
    - discards—Number of packets discarded on receipt (in) or discarded before they were transmitted (out); for more information about the discards counter, see *Rate Limiting for PPP Control Packets* on page 225
  - IPCP protocol configuration
    - configured—IPCP is configured on this interface (true or false)
    - administrative-status—IPCP administrative status (open or closed)
    - ip-address—Address to be used for negotiation of the local IP address option
    - dns-precedence—Used to resolve conflicts during negotiation of DNS addresses; “local” indicates that the local side takes precedence and the **no ppp peer dns** command is operative; “peer” indicates that the remote side takes precedence and the **ppp peer dns** command is operative

- wins-precedence—Used to resolve conflicts during negotiation of WINS addresses; “local” indicates that the local side takes precedence and the **no ppp peer wins** command is operative; “peer” indicates that the remote side takes precedence and the **ppp peer wins** command is operative
- ipcp-netmask-option—Controls negotiation of the IPCP netmask option; disabled = do not negotiate, enabled = negotiate

- IPV6CP protocol configuration
  - configured—IPv6CP is configured on this interface (true or false)
  - administrative-status—IPv6CP administrative status (open or closed)
  - ipv6-interfaceId—Address to be used for negotiation of local IPv6 address option
- IPCP protocol status
  - operational-status—IPCP operational status (up, down, not present, or not present no resources)
  - terminate-reason—Reason for termination of IPCP service
- IPV6CP protocol status
  - operational-status—IPv6CP operational status (up, down, not present, or not present no resources)
  - terminate-reason—Reason for termination of IPv6CP service
- IPCP negotiated options—Shows the following negotiated addresses for the local and remote (peer) side of the link
  - ip-address—IP address
  - ip-address-mask—IP address mask
  - primary-dns-address—Primary DNS address
  - secondary-dns-address—Secondary DNS address
  - primary-wins-address—Primary WINS address
  - secondary-wins-address—Secondary WINS address

**NOTE:** The command displays a value of “none” for any negotiated option parameters if the option was not negotiated.

- OSINLCP protocol configuration
  - configured—OSINLCP is configured on this interface (true or false)
  - administrative-status—OSINLCP administrative status (open or closed)
- OSINLCP protocol status
  - operational-status—OSINLCP operational status (up, down, not present, or not present no resources)
  - terminate-reason—Reason for termination of OSINLCP service

- OSINLCP negotiated options
  - npdu-alignment—Negotiated NPDU alignment for the local and remote (peer) side of the link

**NOTE:** The command displays a value of "none" for any negotiated option parameters if the option was not negotiated.

- MPLSNLCP protocol configuration
  - configured—MPLSNLCP is configured on this interface (true or false)
  - administrative-status—MPLSNLCP administrative status (open or closed)
- MPLSNLCP protocol status
  - operational-status—MPLSNLCP operational status (up, down, not present, or not present no resources)
  - terminate-reason—Reason for termination of MPLSNLCP service
- MPLSNLCP negotiated options
  - npdu-alignment—Negotiated NPDU alignment for the local and remote (peer) side of the link

**NOTE:** The command displays a value of "none" for any negotiated option parameters if the option was not negotiated.

- LCP protocol configuration
  - max-receive-unit—Controls negotiation of the local MRU option; "use lower layer" indicates that the MRU of the layer below PPP defines the MRU to be negotiated; "disabled" indicates that the MRU option is not to be negotiated. A numeric value indicates the MRU value to be negotiated
  - authentication—Controls the negotiation of the local authentication option; "none" indicates do not negotiate; "chap" indicates negotiate chap; "pap" indicates negotiate pap; "chap/pap" indicates negotiate chap and, if it is rejected, negotiate pap; "pap/chap" indicates negotiate pap and, if it is rejected, negotiate chap.
  - magic-number—Controls whether the local magic number is negotiated: enabled (negotiate), or disabled (do not negotiate)
  - magic-number-mismatch—Indicates whether the router is configured to ignore the LCP peer magic number and retain the PPP connection when the peer has not negotiated an LCP magic number: ignore (ignore the peer magic number mismatch and retain the PPP connection), or reject (router terminates the PPP connection if it detects a peer magic number mismatch)
  - keepalive-timer—Rate of LCP echo requests
  - restart-timer—Retry frequency during LCP, IPCP, OSINLCP, and MPLS negotiations
  - max-terminate—Maximum number of terminate requests
  - max-configure—Maximum number of configure requests

- max-failure—Maximum number of configure NAKs
- passive-mode—Forces a PPP interface into a passive mode before LCP negotiation begins; “disabled” means do not wait for peer; “enabled” means wait for peer to initiate negotiation

- LCP protocol status
  - link-status—Overall status of LCP negotiations, including the following states: Initial (idle), Starting (ready to negotiate), Authenticate (authenticating), and Network (LCP is up)
- LCP negotiated options—Shows the following negotiated values for the local and remote (peer) side of the link:
  - max-receive unit—Maximum receive unit, in octets
  - authentication—Authentication method (none, pap, or chap)
  - magic-number—Magic number
  - pfc—PFC (none or enabled)
  - acfc—ACFC (none or enabled)

**NOTE:** The command displays a value of “none” for any negotiated option parameters if the option was not negotiated.

- LCP Endpoint Discriminator options
  - local discriminator class—Endpoint discriminator type, format, and address space for the local and remote (peer) router
  - local endpoint discriminator—Endpoint discriminator value for the local router within the specified class
  - peer discriminator class—Endpoint discriminator type, format, and address space for the remote router
  - peer endpoint discriminator—Endpoint discriminator value for the remote router within the specified class
- LCP protocol statistics—Shows the following statistics for the life of the interface (since system boot or interface creation, whichever is later)
  - in-keepalive-requests—Number of received keepalive requests (LCP Echo Requests)
  - out-keepalive-requests—Number of transmitted keepalive requests
  - in-keepalive-replies—Number of received keepalive replies
  - out-keepalive-replies—Number of transmitted keepalive replies
  - keepalive-failures—Number of keepalive failures reported on the interface
- Authentication configuration
  - authenticate-retry—Maximum number of authentication retries configured using the **ppp max-bad-auth** command
  - authentication-router—Virtual router for the authentication virtual router context

- Authentication status
  - grant—Authentication status (true = access granted, false = access not granted)
  - session-timeout—Session timeout, in seconds; session is terminated at expiration
  - inactivity-timeout—Inactivity timeout, in seconds; session is terminated if it is not active for specified timeout
  - accounting-timeout—Accounting timeout in seconds; frequency of accounting updates to the authentication server
  - peer-ip-address—IP address to be used in negotiation of peer IP address
  - peer-ip-address-mask—IP address mask to be used in negotiation of the peer IP address mask
  - peer-primary-dns-address—IP address to be used in negotiation of the peer primary DNS address
  - peer-secondary-dns-address—IP address to be used in negotiation of the peer secondary DNS address
  - peer-primary-wins-address—IP address to be used in negotiation of the peer primary WINS address
  - peer-secondary-wins-address—IP address to be used in negotiation of the peer secondary WINS address

**NOTE:** The command displays the authentication status as "none" for any parameters not provided by the authentication server.

- Authentication statistics—Shows statistics accumulated since the session was established
  - up-time—Time the session has been up, in seconds
  - in-octets—Number of octets received on the interface
  - out-octets—Number of octets transmitted out the interface
  - in-packets—Number of packets received on the interface
  - out-packets—Number of packets transmitted out the interface
- PAP protocol configuration
  - request-timeout—Maximum time, in seconds, to wait for an authentication request packet
- CHAP protocol configuration
  - name—Name toM be used in challenge packets
  - challenge-retry—Maximum number of challenge packets to be transmitted
  - challenge-timeout—Frequency, in seconds, of challenge packet retransmission
  - minimum-challenge-length—Minimum length of challenge packet

- maximum-challenge-length—Maximum length of challenge packet; the size of the challenge used for each challenge packet is a random number between minimum-challenge-length and maximum-challenge-length
- minimum-rechallenge-timeout—Minimum time, in seconds, before initiating a rechallenge to peer
- maximum-rechallenge-timeout—Maximum time, in seconds, before initiating a rechallenge to peer; the actual time before a rechallenge is a random number between minimum-rechallenge-timeout and maximum-rechallenge-timeout

- If the operational status is down for a specific interface, one of the following termination reasons might appear in parentheses:
  - administrative disable—Interface has been administratively disabled, which means that the **ppp shutdown** command is in effect. This applies to an interface, IPCP, IPv6CP, OSINLCP, and MPLS.
  - administrative logout—Interface has been administratively logged out, which means that the **logout subscriber** command has been issued. This applies to an interface only.
  - no upper interface—No upper layer is configured. This applies to an interface only.
  - authentication failure—Authentication is required and has failed. This applies to an interface only.
  - no local *xxx*—local option, *xxx,* is required and could not be negotiated (for example, IP address). This applies to an interface, IPCP, IPv6CP, OSINLCP, and MPLS.
  - no peer *xxx*—Remote peer option, *xxx*, is required and could not be negotiated (for example, authentication). This applies to an interface, IPCP, IPv6CP, OSINLCP, and MPLS.
  - keepalive drop count exceeded—Keepalive drop count has been exceeded. This applies to an interface only.
  - session timeout—Session timeout period has expired. This applies to an interface only.
  - inactivity timeout—Inactivity timeout period has expired. This applies to an interface only.
  - address lease expired—Address lease period has expired. This applies to an interface only.
  - not configured—Protocol is not configured on the interface. This applies to IPCP, IPv6CP, OSINLCP, and MPLS.
  - link down—Link is down and the protocol is not operationally up. This applies to IPCP, IPv6CP, OSINLCP, and MPLS.
  - lower layer down—Lower protocol layer is down. This applies to an interface only.

- max configure exceeded—Maximum number of configure requests was exceeded while negotiations were in progress. This means that there was no response from the peer, or the peer refused to negotiate. This applies to an interface, IPCP, IPv6CP, OSINLCP, and MPLS.
- peer requested termination—Remote peer requested termination of the connection, which means that a terminate request was received while the session was in an open state. This applies to an interface, IPCP, IPv6CP, OSINLCP, and MPLS.

- Example 1—Provides detailed output for a particular IP interface

```
host1#show ppp interface atm 3/3.20 full
PPP interface ATM 3/3.20 is up
Interface alias is 'interface ezu19xuy'
Interface administrative status is open
Configured network protocol is IPCP
IPCP protocol configuration
   configured                    true
   administrative-status         open
   ip-address                    180.1.0.1
   dns-precedence                local
   wins-precedence               local
   ipcp-netmask-option           enabled
IPCP protocol status
   operational-status            up
IPCP negotiated options          local              peer
   ip-address                    180.1.0.1          195.0.1.13
   ip-address-mask               none               255.255.255.252
   primary-dns-address           none               192.168.10.10
   secondary-dns-address         none               none
   primary-wins-address          none               192.168.100.100
   secondary-wins-address        none               none
OSINLCP protocol configuration
   configured                    false
   administrative-status         open
OSINLCP protocol status
   operational-status            not present
   terminate-reason              not configured
MPLSNLCP protocol configuration
   configured                    false
   administrative-status         open
MPLSNLCP protocol status
   operational-status            not present
   terminate-reason              not configured
Interface statistics             in                 out
   packets                       0                  0
   octets                        617                1008
   errors                        0                  0
   discards                      384723             0
LCP protocol configuration
   max-receive-unit              use lower layer
   authentication                chap/pap
   magic-number                  enabled
   magic-number-mismatch         ignore
   keepalive-timer               0 seconds
   restart-timer                 3 seconds
   max-terminate                 2
   max-configure                 10
   max-failure                   5
   passive-mode                  disabled
```

```
LCP protocol status
   link-status                    network
LCP negotiated options            local              peer
   max-receive-unit               9178               9178
   authentication                 chap               none
   magic-number                   0x667cdfaa         0x27012f05
   accm                           none               none
   pfc                            none               none
   acfc                           none               none
LCP protocol statistics
   in-keepalive-requests          0
   out-keepalive-requests         0
   in-keepalive-replies           0
   out-keepalive-replies          0
   keepalive-failures             0
Authentication configuration
   authenticate-retry             0
   authentication-router          ''
Authentication status
   grant                          true
   session-timeout                none
   inactivity-timeout             none
   accounting-timeout             none
   peer-ip-address                none
   peer-ip-address-mask           255.255.255.252
   peer-primary-dns-address       192.168.10.10
   peer-secondary-dns-address     none
   peer-primary-wins-address      none
   peer-secondary-wins-address    none
Authentication statistics
   up-time                        53 seconds
   in-octets                      72
   out-octets                     60
   in-packets                     0
   out-packets                    0
PAP protocol configuration
   request-timeout                20 seconds
CHAP protocol configuration
   name                           ''
   challenge-retry                10
   challenge-timeout              4 seconds
   minimum-challenge-length       16
   maximum-challenge-length       32
   minimum-rechallenge-timeout    0 seconds
   maximum-rechallenge-timeout    0 seconds
```

- Example 2—Provides detailed output for a particular IPv6 interface

```
host1#show ppp interface fastEthernet 12/0.1.1 full
PPP interface FastEthernet 12/0.1.1 is lowerDown
Interface administrative status is open
Configured network protocol is IPV6CP
IPCP protocol configuration
   configured                     false
   administrative-status          open
   ip-address                     0.0.0.0
   dns-precedence                 local
   wins-precedence                local
   ipcp-netmask-option            disabled
IPCP protocol status
   operational-status             not present
```

```
IPV6CP protocol configuration
   configured                    true
   administrative-status         open
   ipv6-interfaceId              90:1a00:140:4b39
IPV6CP protocol status
   operational-status            down
   terminate-reason              link down
OSINLCP protocol configuration
   configured                    false
   administrative-status         open
OSINLCP protocol status
   operational-status            not present
Interface statistics             in                  out
   packets                       0                   0
   octets                        1163                706
   errors                        0                   0
   discards                      153482              0
LCP protocol configuration
   max-receive-unit              use lower layer
   authentication                none
   magic-number                  enabled
   magic-number-mismatch         reject
   keepalive-timer               30 seconds
   restart-timer                 3 seconds
   max-terminate                 2
   max-configure                 10
   max-failure                   5
   passive-mode                  disabled
LCP protocol status
   link-status                   initial
LCP protocol statistics
   in-keepalive-requests         11
   out-keepalive-requests        11
   in-keepalive-replies          11
   out-keepalive-replies         11
   keepalive-failures            0
Authentication configuration
   authenticate-retry            0
   authentication-router         ''
   aaa-profile                   ''
Authentication status
   grant                         false
   terminate-reason              lower layer down
PAP protocol configuration
   request-timeout               20 seconds
CHAP protocol configuration
   name                          ''
   challenge-retry               10
   challenge-timeout             4 seconds
   minimum-challenge-length      16
   maximum-challenge-length      32
   minimum-rechallenge-timeout   0 seconds
   maximum-rechallenge-timeout   0 seconds
```

- Example 3—Displays a termination reason (administrative disable) when the operational status of the interface is down

```
host1#show ppp interface
PPP interface pos 0/1:1 is lowerDown
PPP interface pos 4/0:1 is lowerDown
PPP interface pos 12/1:1 is lowerDown
3 ppp interfaces found
PPP interface serial 0/0:1/1 is Up
PPP interface serial 0/0:1/2 is Down (administrative disable)
```

***show ppp interface summary***

- Use to display a summary of all the multilinked and nonmultilinked PPP interfaces configured on the router.
- Field descriptions
  - PPP Status—Nonmultilinked PPP interfaces
  - Configuration status—Indicates the configuration state of the PPP interface, IPCP, IPv6CP, OSINLCP, or MPLS
    - configured—Interface or protocol is configured
    - notConfigured—Interface or protocol is not configured
  - Administrative status—Indicates the administrative state of the PPP interface, IPCP, IPv6CP, OSINLCP, or MPLS
    - open—Interface or protocol is administratively enabled
    - closed—Interface or protocol is administratively disabled
  - Operational status (Interface)—Indicates the operational state of the PPP interface
    - up—Interface is operational
    - down—Interface is not operational because of a problem in the PPP layer
    - lowerDown—Interface is not operational because a lower layer in the protocol stack is down
    - notPresent—Interface is not operational because the hardware is unavailable
    - passive—Interface is waiting for the peer to send an LCP confReq message
    - tunnel—Interface is being redirected through a tunnel
  - Operational status (Ip, Ipv6, Osi. Mpls)—Indicates the operational state of the IPCP, IPv6CP, OSINLCP, or MPLS protocol
    - up—Protocol is operational
    - down—Protocol is not operational because of a problem in the PPP layer
    - notPresent—Protocol is not operational because it does not exist
    - noResources—Protocol is not operational because it does not exist due to a lack of resources
  - PPP Multilink Status—Multilinked PPP interfaces

- Example

```
host1#show ppp interface summary
PPP Status
Configuration status     configured notConfigured
   Interface             4000       n/a
   Ip                    4000       0
   Ipv6                  0          4000
   Osi                   0          4000
   Mpls                  0          4000
Administrative status    open       closed
   Interface             4000       0
   Ip                    4000       0
   Ipv6                  4000       0
   Osi                   4000       0
   Mpls                  4000       0
Operational status       up         down       notPresent noResources
   Interface             4000       0          0          n/a
   Ip                    4000       0          0          0
   Ipv6                  0          0          4000       0
   Osi                   0          0          4000       0
   Mpls                  0          0          4000       0
Operational status       lowerDown  passive    tunnel
   Interface             0          0          0

PPP Multilink Status
Configuration status     configured notConfigured
   Link Interface        8000       n/a
   Network Interface     2000       n/a
   Ip                    2000       0
   Ipv6                  0          2000
   Osi                   0          2000
   Mpls                  0          2000
Administrative status    open       closed
   Link Interface        8000       0
   Network Interface     2000       0
   Ip                    2000       0
   Ipv6                  2000       0
   Osi                   2000       0
   Mpls                  2000       0
Operational status       up         down       notPresent noResources
   Link Interface        8000       0          0          n/a
   Network Interface     2000       0          0          n/a
   Ip                    2000       0          0          0
   Ipv6                  0          0          2000       0
   Osi                   0          0          2000       0
   Mpls                  0          0          2000       0
Operational status       lowerDown  passive    tunnel
   Link Interface        0          0          0
   Network Interface     0          0          0
```

## Troubleshooting

Use the **pppPacket** log to diagnose problems on your PPP interfaces. On dynamic PPP interfaces, you can use the **ppp log** command within the profile, as described in *Chapter 15, Configuring Dynamic Interfaces*.

### *log severity debug pppPacket*

- Use to configure a trace log file for a PPP interface.
- Specify one of the following interface types and an *interface specifier*. For example, specify *slot/port:channel/subchannel* for a serial POS PPP interface.
  - serial—Serial interface
  - atm—ATM interface
  - pos—Packet over SONET interface
- You also configure logging to direct the output to a specific destination. For information, see *JUNOSe System Event Logging Reference Guide, Chapter 1, System Logging Overview*.
- Example

```
host1(config-if)#log severity debug pppPacket serial 0/0:1/1
DEBUG 01/01/1970 00:16:58 pppPacket (1000001,*): interface:0/0:1/11/0:1,
time: 0.00, tx lcp confReq, id = 226, length = 19, mru = 32759,
authentication = chap MD5,magicNumber = 0x5387f9a2

DEBUG 01/01/1970 00:16:58 pppPacket (1000001,*): interface:
0/0:1/11/0:1,
time: 0.01, rx lcp confReq, id = 156, length = 18, mru = 32759,
magicNumber = 0x2d8eac91, pfc, acfc

DEBUG 01/01/1970 00:16:58 pppPacket (1000001,*): interface:
0/0:1/11/0:1,
time: 0.01, tx lcp confAck, id = 156, length = 18, mru = 32759,
magicNumber = 0x2d8eac91, pfc, acfc
```

- Use the **no** version to return the severity changes to their default setting or to the systemwide setting.

### *ppp log*

- Use to enable PPP packet or state machine logging on any dynamic interface that uses the profile being configured. Specify one of the following keywords:
  - **pppPacket**—Enables PPP packet logging
  - **pppStateMachine**—Enables PPP state machine logging
- Example

```
host1(config-profile)#ppp log pppPacket
```

**NOTE:** This command is equivalent to the **log severity debug pppPacket** and **log severity debug pppStateMachine** commands.

- Use the **no** version to disable packet or state machine logging.