

Configuring Point-to-Point Protocol

This chapter describes how to configure a Point-to-Point Protocol (PPP) interface on your ERX system.

Topic	Page
Overview	13-1
References	13-5
Before You Configure PPP	13-5
Configuration Tasks	13-6
Optional Configuration Tasks	13-7
Monitoring PPP Interfaces	13-12
Troubleshooting	13-20

Overview

PPP provides a standard method for transporting multiprotocol datagrams over a point-to-point link. PPP uses 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, the OSI Network Layer Control Protocols (OSINLCPs), and Multiprotocol Label Switching (MPLS) run within PPP.

The system supports dynamic PPP interfaces. See *Configuring Dynamic Interfaces*.

The supported interfaces are:

- Channelized T3 (CT3)
- Unchannelized T3 (T3)
- Unchannelized E3 (E3)
- Channelized T1 (CT1)
- Channelized E1 (CE1)
- Optical Carrier 3 (OC3)
- Optical Carrier 12 (OC12)
- Tunnel Server (when used with L2TP)
- Ethernet – see *Chapter 16, Configuring Point-to-Point Protocol over Ethernet*

Framing

This software release 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 system does not support the following framing features:

- Numbered mode (RFC 1663)
- Autodetection of encapsulation

Error Frames

The system 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 systems initialize a PPP dialogue, each of them 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 system negotiates LCP, but then terminates LCP after 2-3 minutes. Previously, the behavior in such a circumstance was to negotiate LCP and then leave LCP open.

Whenever LCP achieves a stopped state, whether 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 system periodically attempts to negotiate with the other side according to an exponential timeout algorithm. The system 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 system attempts negotiation every 15 minutes until successful. When LCP reaches the open state, the timer resets to 15 seconds.

There are a large number of PPP options that LCP can negotiate. The system negotiates the following:

- 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 system always attempts to negotiate a local magic number. The peer can also determine whether to negotiate its magic number—the peer magic number. The system always accepts a peer attempt to negotiate its magic number.
- 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 14, 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 system uses the ACCM configuration data as supplied by the LAC via proxy LCP. The system 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.)

B-RAS Support

Broadband Remote Access Server (B-RAS) is a system 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 *Chapter 1, Configuring Remote Access to the ERX System*, for details on B-RAS.

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

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

References

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

- 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 2615 – PPP over SONET/SDH (June 1999)*
- RFC 3032 – MPLS Label Stack Encoding (January 2001)

Before You Configure PPP

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

- *Chapter 1, Configuring Channelized T3 Interfaces*
- *Chapter 2, Configuring T3 and E3 Interfaces*
- *Chapter 3, Configuring CT1 and CE1 Interfaces*
- *Chapter 5, Configuring Channelized OCx/STMx Interfaces*
- *Chapter 9, Managing Tunnel Service and IPSec Service Interfaces*
- *Chapter 10, Configuring ATM*
- *Chapter 15, Configuring Packet over SONET*
- *Chapter 16, Configuring Point-to-Point Protocol over Ethernet*

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

Configuration Tasks

Configure a PPP interface to perform the tasks described. These tasks are mandatory unless otherwise noted.

- 1 From the 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 an ATM interface in the *slot/port.subinterface* format by selecting a previously configured physical interface on which you want to configure PPP.
- A *slot* refers to a system chassis slot.
 - › A *port* refers to a CT3, T3, E3, CT1, or CE1 module I/O port.
 - › A *subinterface* is a mechanism that allows a single physical interface to support multiple logical interfaces or networks. Several logical interfaces or networks can be associated with a single hardware interface. Protocols, such as ATM, require that you create one or more virtual circuits over which your data traffic is transmitted to higher layers in the protocol stack. To identify the *subinterface*, specify a number from 1–4294967293.
- Use the **no** version to disable or remove the subinterface or the logical interface.

interface pos

- Use to specify a POS interface in the *slot/port* format by selecting a previously configured physical interface on which you want to configure PPP.
 - › A *slot* refers to a system chassis slot.
 - › A *port* refers to an OC3 module I/O port.
 - › Use the **no** version to disable or remove the subinterface or the logical 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.
 - › A *slot* refers to a system chassis slot.
 - › A *port* refers to a CT3, T3, E3, CT1, or CE1 module I/O port.
 - › A *channel* refers to a T1 (DS1) channel.
 - › A *subchannel* represents a set of DS0 subchannels.
- 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 configuration tasks:

- Stop or restart a PPP session.
- Configure name server addressing.
- Specify the keepalive timeout value.
- Specify the maximum receive units.
- Disable magic numbers.
- Configure passive mode.
- Configure PPP authentication.
- Configure IPCP netmask option (option 0x90).
- Add a text description or alias to a PPP interface.

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 keepalive

- Use to specify the keepalive timeout value.
- High-density keepalive mode is automatically selected if PPP is layered over ATM, L2TP, or PPPoE. Low-density mode is selected if PPP is layered over an HDLC interface. Keepalive mode selection is made per interface.
- High-density mode – mode of operation known as smart keepalive; disabled when the keepalive timer expires, the interface first checks to see if any frames were received from the peer in the prior keepalive timeout interval. If so, it assumes the peer is alive and well and does not send an LCP echo request (keepalive). Keepalive packets are sent only if the peer is silent (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.mode of operation known as smart keepalive. 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 30–300 seconds. The default value is 30 seconds.
- Low-density mode – mode of operation. 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 – range is 10–300 seconds; default value is 30 seconds.
- If the keepalive interval is 30 seconds, a failed link is detected between 90 and 120 seconds after failure.
- Example

```
host1(config-if)#ppp keepalive 50
```
- Use the **no** version to disable keepalive.

ppp ipcp netmask

- Use to specify Internet Protocol Control Protocol (IPCP) netmask option (option 0x90) for each PPP interface. By default, IPCP netmask option is disabled on the interface.
- IPCP netmask option is a nonstandard option that allows 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 **radius ignore framed-ip-netmask**.
- You can enable **ppp ipcp netmask** either in a profile or on a static interface.
- Example

```
host1(config-subif)#ppp ipcp netmask
```
- Use the **no** version to disable IPCP netmask option on the interface.

ppp magic-number disable

- Use to disable negotiation of the local magic number.
- Example

```
host1(config-if)#ppp magic-number disable
```
- Issuing this command prevents the system from detecting loopback configurations.
- Use the **no version** to restore negotiation of the local magic number.

ppp mru

- Use to control the negotiation of the maximum receive unit (MRU).
- You should coordinate this value with the network administrator on the other end of the line.
- If you set this value with a different value for another protocol, such as IP, the system uses the lower value. This could produce unexpected behavior in your network.
- The range is 64–65535.
- Example

```
host1(config-if)#ppp mru 576
```
- Use the **no** version to restore the default value, which causes PPP to negotiate MRU based on the MRU of the layer immediately below PPP, less the PPP protocol overhead.

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 system 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 system take precedence.
- Use the **dns** and/or the **wins** keywords to configure which PPP peer address takes precedence. This command has no effect unless both systems have the address configured and the address is in conflict. If the PPP peer has the address and the system 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 system to take precedence during setup negotiations between the system and the peer. If the IP addresses that the peer sends to the system differ from the ones configured on your system, the system returns the values that you configured as the correct values to the peer.

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

- Use to terminate a PPP session.
- The **ppp shutdown** command administratively disables the interface.
- The **ppp shutdown ip** command administratively disables IPCP.
- The **ppp shutdown mpls** command administratively disables MPLS.
- The **ppp shutdown osi** command administratively disables OSINLCP.
- Example

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

- All PPP sessions are enabled by default.
- Use the **no** version to restart a disabled session.

Configuring PPP Authentication

Perform the following optional tasks to configure PPP authentication.

- Specify the PPP authentication type(s), and select an authentication virtual router context.
- Specify the maximum number of retries.
- Specify the CHAP challenge length.

Authentication Virtual Router

When you specify a virtual router (VR) in the **ppp authentication** command, AAA does not query 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.

ppp authentication

- Use to require authentication from the PPP peer.
- Specify PAP or CHAP as the primary authentication protocol and the other authentication protocol as the alternative. For example, suppose you specify **pap** as the primary authentication protocol and **chap** as the alternate:

```
host1(config-if)#ppp authentication pap chap
```

The system 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 system requests the CHAP protocol. If the peer refuses to negotiate authentication, the system terminates the PPP session.

- Specify 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.

- The system supports the MD5 authentication algorithm for CHAP authentication.
- Use the **no** version to specify that the system 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: We recommend that you do NOT decrease the range. Increasing the range is OK, provided 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 system 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.

Monitoring PPP Interfaces

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

- **show ppp interface** <*selective control*>
- **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 specify that baselined statistics are to be shown.

Output Filtering

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 *ERX System Basics Configuration Guide, Chapter 2, Command Line Interface*, for details.

baseline ppp interface

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

```
host1#baseline ppp interface atm 3/3.20
```

show ppp interface

- Displays selective PPP interface information.
- Field descriptions
 - › PPP interface – interface type, interface specifier, and status (up or down)
 - › 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)
- 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 local IP address option
 - › dns-precedence – used to resolve conflicts during negotiation of DNS addresses; “local” indicates that the local side takes precedence and that 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 that 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
- IPCP protocol status
 - › operational-status – IPCP operational status (up or down)
 - › terminate-reason – reason for termination of IPCP 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 or 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 or down)
 - › 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 or down)
 - › 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 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 that 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 the negotiation of the local magic number option; “disabled” indicates do not negotiate; “enabled” indicates negotiate.
 - 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 = do not wait for peer; enabled = 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) system
 - › local endpoint discriminator – endpoint discriminator value for the local system within the specified class
 - › peer discriminator class – endpoint discriminator type, format, and address space for the remote system
 - › peer endpoint discriminator – endpoint discriminator value for the remote system 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 Request)
 - › 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 peer IP address mask
- › peer-primary-dns-address – IP address to be used in negotiation of peer primary DNS address
- › peer-secondary-dns-address – IP address to be used in negotiation of peer secondary DNS address
- › peer-primary-wins-address – IP address to be used in negotiation of peer primary WINS address
- › peer-secondary-wins-address – IP address to be used in negotiation of 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 since the session was established
 - › up-time – time in seconds
 - › in-octets – received octets
 - › out-octets – transmitted octets
 - › in-packets – received packets
 - › out-packets – transmitted packets
- PAP protocol configuration
 - › request-timeout – maximum time in seconds to wait for an authentication request packet
- CHAP protocol configuration
 - › name – name to 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.

- Example

This example provides detailed output for a particular interface.

```
host1#show ppp interface atm 3/3.20 full
PPP interface ATM 3/3.20 is up
Interface alias is 'interface ezul9xuy'
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 down
> terminate-reason not configured
MPLSNLCP protocol configuration
> configured false
> administrative-status open
MPLSNLCP protocol status
> operational-status down
> terminate-reason not configured
Interface statistics in out
> packets 0 0
> octets 617 1008
> errors 0 0
> discards 0 0
LCP protocol configuration
> max-receive-unit use lower layer
> authentication chap/pap
> magic-number enabled
> 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
```

show ppp interface summary

- Displays a summary of all the non-multilinked and multilinked PPP interfaces configured on the system.
- Field descriptions
 - › PPP Status – non-multilinked PPP interfaces
 - › Configuration status – indicates the configuration state of the PPP interfaces, IPCP, 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, OSINLCP, or MPLS
 - open – **no ppp shutdown** command is operative
 - closed – **ppp shutdown** command is operative
 - › Operational status – indicates the operational state of the PPP interface, IPCP, OSINLCP, or MPLS
 - up – interface or protocol is operational
 - down – interface or protocol is not operational because of some problem in the PPP layer
 - lowerDown – interface or protocol is not operational because a lower layer in the protocol stack is down
 - notPresent – interface or protocol 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
 - › PPP Multilink Status – multilinked PPP interfaces
- Example

```
host1#show ppp interface summary
```

```
PPP Status
Configuration status   configured notConfigured
  Interface            17          n/a
  Ip                   15          2
  Osi                   0          17
  Mpls                  0          17
Administrative status  open        closed
  Interface            16          1
  Ip                   17          0
  Osi                   17          0
  Mpls                  17          0
Operational status     up          down
```

```

Interface          7          5
Ip                 5          12
Osi                0          17
Mpls               0          17
Operational status lowerDown  passive   tunnel    notPresent
Interface          5          0          0          0

PPP Multilink Status
Configuration status configured notConfigured
Link Interface     4          n/a
Network Interface  2          n/a
Ip                 2          0
Osi                0          2
Mpls               0          2
Administrative status open        closed
Link Interface     3          1
Network Interface  2          0
Ip                 2          0
Osi                2          0
Mpls               2          0
Operational status up          down
Link Interface     2          1
Network Interface  2          0
Ip                 2          0
Osi                0          2
Mpls               0          2
Operational status lowerDown  passive   tunnel    notPresent
Link Interface     0          1          0          0
Network Interface  0          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. See *ERX Physical and Link Layers Configuration Guide, Chapter 21, 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 location. Refer to the *ERX Command Reference Guide* for information on logging configuration commands.
- 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
```

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.

