Table of Contents

Understanding debug ppp negotiation Output

Introduction

In dial−related applications, PPP is the most commonly used encapsulation type. PPP allows two machines on a point−to−point communication link to negotiate various parameters for authentication, compression, and the Layer 3 (L3) protocols, such as IP. A failure in the PPP negotiation between two routers causes the connection to fail.

The **debug ppp negotiation** command enables you to view the PPP negotiation transactions, identify the problem or stage when the error occurs, and develop a resolution. However, it is imperative that you understand the **debug ppp negotiation** command output. This document provides a comprehensive method to read **debug ppp negotiation** command output.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

Readers of this document should ensure that the following conditions are met:

- PPP must be enabled on the interfaces on both routers. Issue the command **encapsulation ppp** to accomplish this.
- Activate millisecond timestamps on the router by issuing the following command:

```
Router(config)#service timestamp debug datetime msec
```

For more information on debug commands refer to Important Information on Debug Commands.

Note: PPP negotiation between two peers cannot start unless the lower layer (ISDN, physical interface, dial−up line, and so on) under PPP is functioning perfectly. For example, if you want to run PPP over ISDN, then all the ISDN layers should be up; otherwise PPP does not start.

Components Used

This document is not restricted to specific software and hardware versions.

Phases of PPP Negotiation

During PPP negotiation, the link goes through several phases, as shown below. The end result is that PPP is either up or down.

Phase	Description
DOWN	In this phase, PPP is down. This message is seen after the link and PPP are completely brought down: `*Mar  3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
ESTABLISHING	PPP transitions to this phase when it receives an indication that the physical layer is up and ready to be used. LCP[1] negotiation occurs in this phase. `*Mar  3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTHENTICATING	If PPP authentication (CHAP[2] or PAP[3]) is desired on the link, then PPP transitions to this phase. Keep in mind that PPP authentication is optional. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
UP	Once authentication is complete, PPP transitions to the UP phase. NCP[4] negotiation occurs in this phase. `*Mar  3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMINATING	In this phase, PPP is shutting down. `*Mar  3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

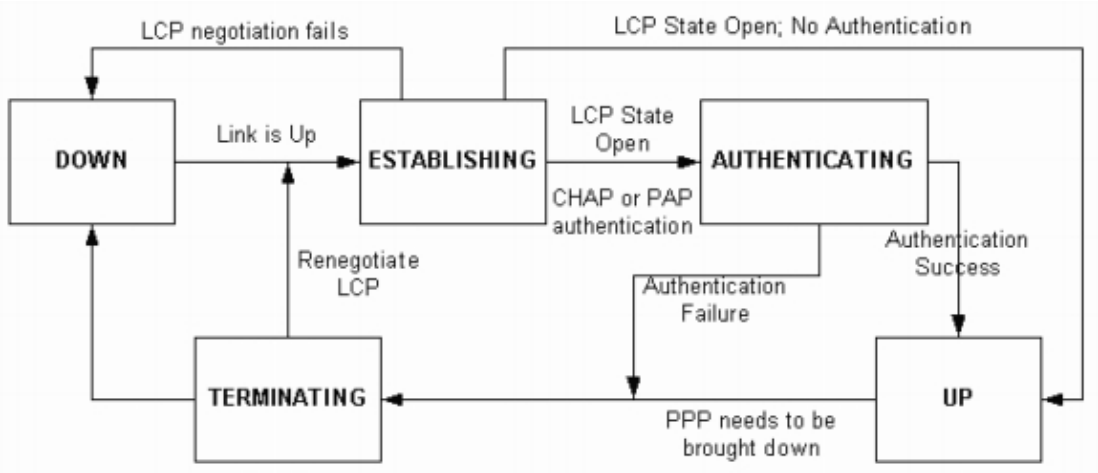
1. LCP = Link Control Protocol

2. CHAP = Challenge Handshake Authentication Protocol

3. PAP = Password Authentication Protocol

4. NCP = Network Control Protocol

The following diagram shows the PPP phase transitions:



PPP Negotiation Packets: A Description

The following table includes description of PPP negotiation packets that are used in both LCP and NCP negotiation:

Packet	Code	Description
CONFREQ	Configure−Request	The device opens a connection to the peer by transmitting this message along with the configuration options and values the sender wishes the peer to support. All options and values are negotiated simultaneously. If the peer responds with a CONFREJ or CONFNAK message, then the router sends another CONFREQ with another set of options or values.
CONFREJ	Configure−Reject	If some configuration option received in the CONFREQ message is not acceptable or not recognizable, the the router responds with a CONFREJ message. The unacceptable option (from the CONFREQ message) is included in the CONFREJ message.
CONFNAK	Configure−NAK[1]	If the received configuration option is recognizable and acceptable, but some value is not acceptable, the router transmits a CONFNAK message. The router appends

		the option and value that it can accept in the CONFNAK message so that the peer can include that option in the next CONFREQ message.
CONFACK	Configure−ACK[2]	If all options in the CONFREQ message are recognizable and all values are acceptable, then the router transmits a CONFACK message.
TERMREQ	Terminate−Request	This message is used to initiate an LCP close.
TERMACK	Terminate−ACK	This message is transmitted in response to the TERMREQ message.

1. NAK = Negative Acknowledge

2. ACK = Acknowledge

Note: Each peer can send CONFREQs with the option or value it wants the peer to support. This can cause the options negotiated in each direction to be different. For example, one side may wish to authenticate the peer while the other may not.

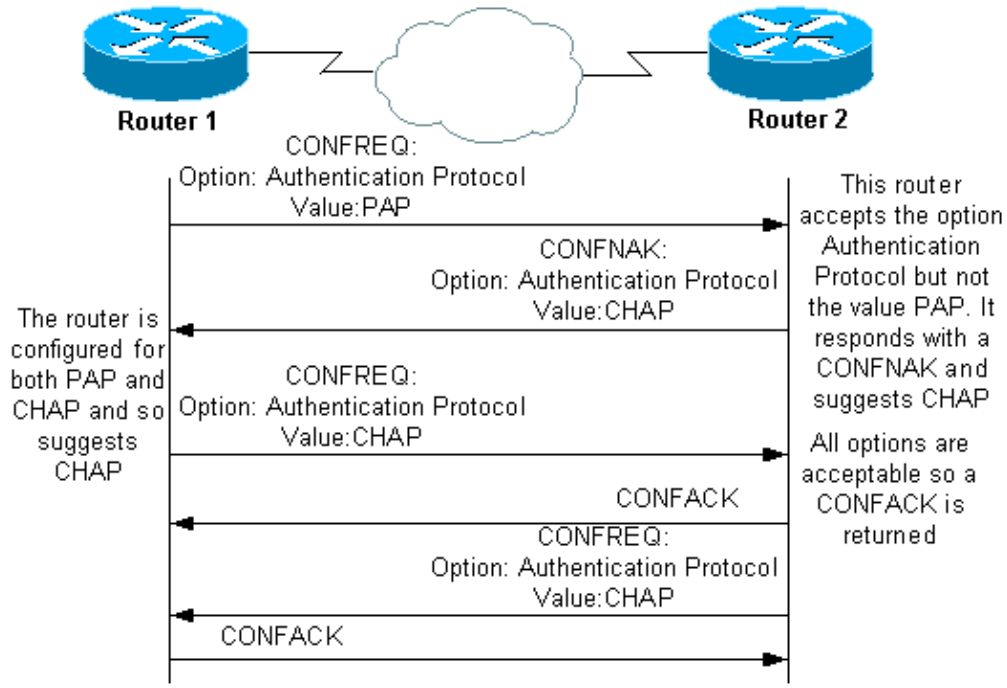
LCP, Authentication and NCP Stage

Within some of the PPP phases described previously, PPP also goes into specific stages such as LCP negotiation, authentication and NCP negotiation. For more information, refer to RFC 1548 and RFC 1661 .

LCP (Mandatory Phase)

LCP is a phase in which parameters for establishing, configuring, and testing the data−link connection are negotiated. An LCP state of open means that LCP was successfully completed, while an LCP state of closed indicates an LCP failure.

The diagram below shows a conceptual view of an LCP handshake:



The LCP negotiation also uses a parameter called MagicNumber, which is used to determine if the link is looped back. A random string is sent across the link and, if the same value is returned, then the router determines that the link is looped back.

Authentication (Optional Phase by Default)

In this stage, the authentication is performed using the authentication protocol (CHAP or PAP) agreed upon in LCP negotiation. For PAP related information, refer to Configuring and Troubleshooting PPP Password Authentication Protocol (PAP).

For CHAP related information, refer to Understanding and Configuring PPP CHAP Authentication.

Note: Authentication is optional and PPP only enters this stage if it needs to authenticate.

NCP (Mandatory Phase)

This phase is used for establishing and configuring different network−layer protocols. The most common L3 protocol negotiated is IP. The routers exchange IP Control Protocol (IPCP) messages negotiating options specific to the protocol (IP in this example).

According to RFC 1332 , IPCP negotiates two options: compression and IP address assignments. However, IPCP is also used to pass network related information such as primary and backup Windows Name Service (WINS) and Domain Name System (DNS) servers.

The negotiation occurs using the CONF messages described in the PPP Negotiation Packets: A Description section of this document.

Troubleshooting Using debug ppp negotiation Output

When reading the **debug ppp negotiation** command output for troubleshooting purposes, follow the instructions below:

1. Identify the phase transitions in the **debug** command output. Determine the furthest phase the connection achieved: for example, UP, AUTHENTICATING, and so on. This can help identify the phase in which the connection failed. For more information on the phases, refer to the section Phases of PPP Negotiation.
2. For the phase in which the failure occurred, look for the messages indicating that LCP, authentication or NCP (as appropriate) are successful:

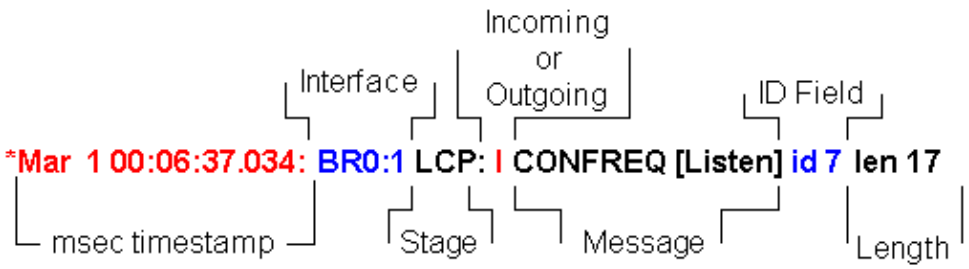
    - The LCP state should be open. You can also look at the last incoming and outgoing CONFACK messages to verify that the parameters you require have been negotiated.
    - Authentication should be successful. If you are using two−way authentication, then each transaction must be successful. For more information on troubleshooting PPP authentication failures refer to the document Troubleshooting PPP (CHAP or PAP) Authentication.
    - The IPCP state should be open. Verify that the addressing is correct and that a route to the peer is installed.

Reading debug ppp negotiation Output

Most lines in the **debug ppp negotiation** command output are characterized by:

1. **The timestamp** Millisecond timestamps are useful. Refer to the Prerequisites section of this document for more information.
2. **Interface and Interface number** This is useful when debug connections are using multiple connections, or when the connection transitions through several interfaces. For example, certain connections (such as multilink calls) are controlled by the physical interface at the beginning, but are later controlled by the dialer interface or virtual−access interface.
3. **Type of PPP message** This indicates whether the line is a general PPP, LCP, CHAP, PAP, or IPCP message.
4. **Direction of the message** An I indicates an incoming packet and an O indicates an outgoing packet. This can be used to determine if the message was generated or received by the router.
5. **Message** For negotiation transaction, this section includes the particular transaction being negotiated.
6. **ID Field** Used to match and coordinate request messages to the appropriate response messages. A response can be associated with an incoming message using the ID Field. This option is especially useful, when the incoming message and the response are far apart in the debug output.
7. **Length** The length field defines the length of the information field. This is not important for general troubleshooting.

    Note: Points 4 through 7 may not appear in all PPP messages, depending on the purpose of the message. The following example illustrates the above points.



Sample debug ppp negotiation Output

Here is an annotated description of **debug ppp negotiation** command output:

```
maui-soho-01#debug ppp negotiation
PPP protocol negotiation debugging is on
maui-soho-01#
*Mar  1 00:06:36.645: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up

!--- The Physical Layer (BRI Interface) is up. Only now can PPP
!--- negotiation begin.

*Mar  1 00:06:36.661: BR0:1 PPP: Treating connection as a callin
*Mar  1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load]

!--- The PPP Phase is ESTABLISHING. LCP negotiation now occurs.

*Mar  1 00:06:36.669: BR0:1 LCP: State is Listen
*Mar  1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7 len 17

!--- This is the incoming CONFREQ. The ID field is 7.

*Mar  1 00:06:37.038: BR0:1 LCP:    AuthProto PAP (0x0304C023)
*Mar  1 00:06:37.042: BR0:1 LCP:    MagicNumber 0x507A214D (0x0506507A214D)
*Mar  1 00:06:37.046: BR0:1 LCP:    Callback 0  (0x0D0300)

!--- The peer has requested:
!--- Option: Authentication Protocol, Value: PAP
!--- Option: MagicNumber (This is used to detect loopbacks and is always sent.)
!--- Option: Callback, Value: 0 (This is for PPP Callback; MS Callback uses 6).

*Mar  1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15

!--- This is an outgoing CONFREQ, with parameters for the peer to implement.
!--- Note that the ID Field is 4, so is not related to the previous CONFREQ message.

*Mar  1 00:06:37.058: BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 00:06:37.062: BR0:1 LCP:    MagicNumber 0x1081E7E1 (0x05061081E7E1)

!--- This router is requesting:
!--- Option: Authentication Protocol, Value: CHAP
!--- Option: MagicNumber (This is used to detect loopbacks and is always sent.)

*Mar  1 00:06:37.066: BR0:1 LCP: O CONFREJ [Listen] id 7 len 7

!--- Outgoing CONFREJ for message with Field ID 7
!--- This is the response to the CONFREQ received first.

*Mar  1 00:06:37.070: BR0:1 LCP:    Callback 0  (0x0D0300)

!--- The option that this router rejects is Callback.
!--- If the router wanted to do MS Callback rather than PPP Callback, it
!--- would have sent a CONFNAK message instead.

*Mar  1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4 len 15

!--- This is an incoming CONFACK for a message with Field ID 4.

*Mar  1 00:06:37.102: BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 00:06:37.106: BR0:1 LCP:    MagicNumber 0x1081E7E1 (0x05061081E7E1)

!--- The peer can support all requested parameters.
```

```
*Mar  1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14

!--- This is an incoming CONFREQ message; the ID field is 8.
!--- This is a new CONFREQ message from the peer in response to the CONFREJ id:7.

*Mar  1 00:06:37.117: BR0:1 LCP:    AuthProto PAP (0x0304C023)
*Mar  1 00:06:37.121: BR0:1 LCP:    MagicNumber 0x507A214D (0x0506507A214D)

!--- The peer has requested:
!--- Option: Authentication Protocol, Value: PAP
!--- Option: MagicNumber (This is used to detect loopbacks and is always sent.)

*Mar  1 00:06:37.125: BR0:1 LCP: O CONFNAK [ACKrcvd] id 8 len 9

!--- This is an outgoing CONFNACK for a message with Field ID 8.

*Mar  1 00:06:37.129: BR0:1 LCP:    AuthProto CHAP (0x0305C22305)

!--- This router recognizes the option Authentication Protocol,
!--- but does not accept the value PAP. In the CONFNAK message, it suggests CHAP instead.

*Mar  1 00:06:37.165: BR0:1 LCP: I CONFREQ [ACKrcvd] id 9 len 15

!--- This is an incoming CONFREQ message with Field ID 9.

*Mar  1 00:06:37.169: BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 00:06:37.173: BR0:1 LCP:    MagicNumber 0x507A214D (0x0506507A214D)

!--- CHAP authentication is requested.

*Mar  1 00:06:37.177: BR0:1 LCP: O CONFACK [ACKrcvd] id 9 len 15

!--- This is an outgoing CONFACK for a message with Field ID 9.

*Mar  1 00:06:37.181: BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 00:06:37.185: BR0:1 LCP:    MagicNumber 0x507A214D (0x0506507A214D)
*Mar  1 00:06:37.189: BR0:1 LCP: State is Open

!--- This indicates that the LCP state is Open.

*Mar  1 00:06:37.193: BR0:1 PPP: Phase is AUTHENTICATING, by both [0 sess, 0 load]

!--- The PPP Phase is AUTHENTICATING. PPP Authentication occurs now.
!--- Two-way authentication is now performed (indicated by the both keyword).

*Mar  1 00:06:37.201: BR0:1 CHAP: O CHALLENGE id 4 len 33 from "maui-soho-01"

!--- This is the outgoing CHAP Challenge.
!--- In LCP the routers had agreed upon CHAP as the authentication protocol.

*Mar  1 00:06:37.225: BR0:1 CHAP: I CHALLENGE id 3 len 33 from "maui-soho-03"

!--- This is an incoming Challenge message from the peer.

*Mar  1 00:06:37.229: BR0:1 CHAP: Waiting for peer to authenticate first
*Mar  1 00:06:37.237: BR0:1 CHAP: I RESPONSE id 4 len 33 from "maui-soho-03"

!--- This is an incoming response from the peer.

*Mar  1 00:06:37.244: BR0:1 CHAP: O SUCCESS id 4 len 4

!--- This router has successfully authenticated the peer.

*Mar  1 00:06:37.248: BR0:1 CHAP: Processing saved Challenge, id 3
```

```
*Mar  1 00:06:37.260: BR0:1 CHAP: O RESPONSE id 3 len 33 from "maui-soho-01"
*Mar  1 00:06:37.292: BR0:1 CHAP: I SUCCESS id 3 len 4

!--- This is an incoming Success message. Each side has
!--- successfully authenticated the other.

*Mar  1 00:06:37.296: BR0:1 PPP: Phase is UP [0 sess, 0 load]

!--- The PPP status is now UP. NCP (IPCP) negotiation begins.

*Mar  1 00:06:37.304: BR0:1 IPCP: O CONFREQ [Closed] id 4 len 10
*Mar  1 00:06:37.308: BR0:1 IPCP:    Address 172.22.1.1 (0x0306AC160101)

!--- This is an outgoing CONFREQ message. It indicates that
!--- the local machine address is 172.22.1.1.

*Mar  1 00:06:37.312: BR0:1 CDPCP: O CONFREQ [Closed] id 4 len 4
*Mar  1 00:06:37.320: BR0:1 CDPCP: I CONFREQ [REQsent] id 4 len 4
*Mar  1 00:06:37.324: BR0:1 CDPCP: O CONFACK [REQsent] id 4 len 4

!--- These messages are for CDP Control Protocol (CDPCP).

*Mar  1 00:06:37.332: BR0:1 IPCP: I CONFREQ [REQsent] id 4 len 10
*Mar  1 00:06:37.336: BR0:1 IPCP:    Address 172.22.1.2 (0x0306AC160102)

!--- This is an incoming CONFREQ message indicating that the peer
!--- address is 172.22.1.2.  An address of 0.0.0.0 indicates that the peer
!--- does not have an address and requests the local router to provide it
!--- an address in IPCP negotiation.

*Mar  1 00:06:37.344: BR0:1 IPCP: O CONFACK [REQsent] id 4 len 10
*Mar  1 00:06:37.348: BR0:1 IPCP:    Address 172.22.1.2 (0x0306AC160102)
*Mar  1 00:06:37.356: BR0:1 IPCP: I CONFACK [ACKsent] id 4 len 10
*Mar  1 00:06:37.360: BR0:1 IPCP:    Address 172.22.1.1 (0x0306AC160101)
*Mar  1 00:06:37.363: BR0:1 IPCP: State is Open

!--- IPCP state is open. Note that in the IPCP negotiation, each side
!--- accepted the IP address of the peer, and one was assigned to the peer.

*Mar  1 00:06:37.371: BR0:1 CDPCP: I CONFACK [ACKsent] id 4 len 4
*Mar  1 00:06:37.375: BR0:1 CDPCP: State is Open

!--- This indicates that the CDPCP state is Open.

*Mar  1 00:06:37.387: BR0 IPCP: Install route to 172.22.1.2

!--- A route to the peer is installed.

*Mar  1 00:06:38.288: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed stat
*Mar  1 00:06:42.609: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to  maui-soho-03
```

Glossary and Common Messages

General

CONFREQ (Configure−Request):

When the lower layer becomes available (Up), a Configure−Request is sent to start the first PPP phase (LCP phase). It is used in LCP and NCP phases as an attempt to configure the connection. The device opens a connection to the peer by transmitting this message along with the configuration options and values the sender

wishes the peer to support. All options and values are negotiated simultaneously. If the peer responds with a CONFREJ or CONFNAK message, then the router sends another CONFREQ with another set of options or values.

CONFACK (Configure−Acknowledge):

If all options in the CONFREQ message are recognizable and all values are acceptable, then the router transmits a CONFACK message.

CONFREJ (Configure Reject):

If some configuration option received in the CONFREQ is not acceptable or not recognizable, the the router responds with a CONFREJ message. The unacceptable option (from the CONFREQ) is included in the CONFREJ message.

CONFNAK (Configure Negative Acknowledge):

If the received configuration option is recognizable and acceptable, but some value is not acceptable, the router transmits a CONFNAK message. The router appends the option and value that it can accept in the CONFNAK message so that the peer can include that option in the next CONFREQ message.

ECHOREQ (Echo Request) and ECHOREP (Echo Reply):

PPP uses keep−alives in order to maintain the integrity of the connection. These keep−alives are the ECHOREQ frame that is sent to remote PPP peer, and the remote PPP peer should respond with an ECHOREP frame upon receipt of an ECHOREQ frame. By default, if the router misses five ECHOREP frames, then the link is considered down and PPP is brought down.

TERMREQ (Termination Request):

This frame indicates that the PPP peer that sent this frame terminates the PPP connection.

TERMACK (Termination Acknowledge):

This message is transmitted in response to the TERMREQ message. This closes down the PPP connection.

TERMINATING:

This message indicates that the PPP connection has been brought to down. An LCP or NCP connection can be cut off:

- on administrative closing (LCP only).
- when the lower level goes out of service (dial−up line, ISDN, and so on).
- when negotiations fall through.
- on line loop detection.

LCP

ACCM (Asynchronous Control Character Map):

This is one of the LCP−negotiated options within the CONFREQ frame. ACCM sets the character escape sequences. ACCM tells the port to ignore specified control characters within the data stream. If the router at

the other end of the connection does not support ACCM negotiation, the port is forced to use FFFFFFFF. In that case, issue the following command:

```
ppp accm match 000a000
```

ACFC (Address and Control Field Compression):

LCP option that allows endpoints to send messages back and forth more efficiently.

AuthProto (Authentication Protocol):

This is the authentication Protocol Type negotiated in the CONFREQ frame to be agreed between both PPP connection peers to use it in the authentication phase. If no PPP authentication is configured, this output is not be seen in CONFREQ frame negotiated parameters. The possible values are CHAP or PAP.

Callback "#":

This message indicates that the callback option is being negotiated. The number after the callback syntax indicates which callback option is being negotiated. Number 0 is normal PPP callback, while Number 6 indicates the Microsoft callback option (which is automatically available in Cisco IOS® Software Release 11.3(2)T or later).

CHAP (Challenge Handshake Authentication Protocol):

This message indicates that the authentication protocol being negotiated is CHAP.

EndpointDisc (End Point Discriminator):

This is an LCP option used to identify a PPP peer in PPP multilink connection. For more information, refer to Criteria for Naming Multilink PPP Bundles.

LCP: State is Open :

This message indicates that the LCP negotiation has been completed successfully.

LQM (Link Quality Monitoring):

LQM is available on all serial interfaces running PPP. LQM monitors the link quality and takes the link down when the quality drops below a configured percentage. The percentages are calculated for both the incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent with the total number of packets and bytes received by the peer. The incoming quality is calculated by comparing the total number of packets and bytes received with the total number of packets and bytes sent by the peer.

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

MagicNumber:

Magic Number support is available on all serial interfaces. PPP always attempts to negotiate for Magic Numbers, which are used to detect looped−back networks. A random string is sent across the link and if the same value is returned, then the router determines that the link is looped back.

The link might or might not be taken down upon looped−back detection, depending on the use of the **down−when−looped** command.

PAP (Password Authentication Protocol):

This message indicates that the authentication protocol being negotiated to be used by PPP peers is PAP. For more information on PAP, refer to the document Configuring and Troubleshooting PPP Password Authentication Protocol (PAP).

PFC (Protocol Field Compression):

This option is either turns on or off compression for the protocol fields.

MRRU (Max Receive Reconstructed Unit):

This is an LCP option negotiated during PPP multilink LCP setup which determines the maximum number of bytes that can constitute a frame. If MRRU is not negotiated in LCP, then MPPPP cannot run on the link.

MRU (Maximum Received Unit):

An LCP option negotiated in the CONFREQ frame to negotiate the size of the exchanged packets.

Authentication

AUTH−REQ (Authentication Request):

This frame is sent from the local PPP peer, on which authentication is enabled, to remote peer asking it to send valid username and password for authenticating the PPP connection. This frame is only used with PAP.

AUTH−ACK (Authentication Acknowledge):

This frame is sent out from the authenticated PPP peer to the authenticating PPP peer. This frame carries the valid username and password pair. This frame is only used when PAP is used for authenticating the PPP connection.

AUTH−NAK or FAILURE:

This frame is sent out from the authenticating PPP peer when the authentication failed on the authenticating PPP peer.

CHALLENGE:

This is the CHAP challenge frame that is sent from the authenticating PPP peer to the authenticated PPP peer. The challenge frame consists of an ID, a random number, and either the host name of the local communication server or the name of the user on the remote device. This frame is only used when CHAP is used for authenticating the PPP connection.

RESPONSE :

This is the CHAP response frame that sent from the authenticated PPP peer to the authenticating PPP peer.

The required response consists of two parts:

- An MD5 hash output of the shared secret.
- Either the host name of the remote device or the name of the user on the remote device.

This frame is only used when CHAP is used for authenticating the PPP connection.

NCP

Address a.b.c.d

- On an outgoing CONFREQ message, this value indicates the IP address the local router wishes to use. If the address included is 0.0.0.0, the local machine requests the peer to supply it an IP address it can use.
- On an incoming CONFREQ message, this value indicates the IP address the peer wishes to use. If the address included is 0.0.0.0, the peer requests the local machine to supply it an IP address it can use.
- On an outgoing CONFNAK message, this value indicates the IP address the peer should use rather than the one the peer suggested in the CONFREQ message.
- On an incoming CONFNAK message, this value indicates the IP address the local machine should use, instead of the one it suggested in the previous CONFREQ message.
- On an outgoing CONFACK message, this value indicates that the IP address requested by the peer is acceptable to the local machine.
- On an incoming CONFACK message, this value indicates that the IP address requested by the local machine is acceptable to the peer.

CCP (Compression Control Protocol):

This message indicates that a compression protocol is being negotiated between both PPP peers. Cisco IOS Software supports the following compression protocols to be negotiated over a PPP connection: MS−Point−to−Point Compression (MS−PPC), stacker, predictor.

CDPCP (Cisco Discovery Protocol Control Protocol):

This message indicates that CDP negotiation is occurring in the NCP phase. To turn off CDP on the router, issue the command **no cdp run**.

CODEREJ (Code Reject):

A code−reject packet is sent in response of receiving unknown code event occurs when an un−interpretable packet is received from the remote PPP peer.

Install route to a.b.c.d:

The router upon finishing IPCP (NCP phase for IP L3 protocol) must install the given IP address to the remote PPP peer in the routing table and seen as connected route in the routing table. If you do not see this message, verify that the **no peer neighbor−route** command is not configured.

IPCP (IP Control Protocol):

This value indicates that IP is the network layer that being negotiated in the NCP phase.

IPCP State is Open:

This indicates the IPCP (NCP phase for IP L3 protocol) has been completed successfully.

PROTREJ (Protocol Reject):

The PPP peer, upon reception of a PPP packet with an unknown protocol field, uses the PROTREJ message to indicate that the peer is attempting to use a protocol that is unsupported. Upon reception of a protocol−reject, the receiving PPP device must stop sending packets of the indicated protocol at the earliest opportunity.

Related Information

- **Configuring and Troubleshooting PPP Password Authentication Protocol (PAP)**
- **Understanding PPP and PPP Authentication**
- **PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands**
- **Understanding and Configuring PPP CHAP Authentication**
- **Troubleshooting PPP (CHAP or PAP) Authentication**
- **Cisco Technology Support − Dial**
- **Access Technology Support Pages**
- **Technical Support − Cisco Systems**