PPP Troubleshooting Flowchart

Contents

Introduction

This flowchart helps you to troubleshoot Point-to-Point Protocol (PPP), which is widely used for multiple Access technology solutions.

In the flowcharts and sample output shown below, we have set up an Integrated Services Digital Network (ISDN) basic rate interface (BRI) PPP connection to another using Legacy Dialer-on-Demand Routing (DDR). However, the same troubleshooting steps apply to connections to other routers (such as branch offices) with PPP connections when using Dialer Rotary-Group, Dialer Profile, or PPP over serial links.

For further information on Point-to-Point Protocol, and its supported features in Cisco IOS® software, refer to Cisco Learning Connection (registered customers only) and search using the keyword **ppp** in the **Search for training** field.

For a detailed explanation of the different phases of PPP negotiation and the output of **debug ppp negotiation**, refer to Configuring and Troubleshooting PPP Password Authentication Protocol (PAP).

Prerequisites

Requirements

Make sure you meet these prerequisites:

- Enable **debug ppp negotiation** and **debug ppp authentication**.
- You must read and understand the debug ppp negotiation output. Refer to Understanding debug ppp negotiation Output for more information.
- The PPP authentication phase does not begin until the Link Control Protocol (LCP) phase is complete and is in "open" state. If **debug ppp negotiation** does not indicate that LCP is open, troubleshoot this issue before you proceed.

Components Used

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

Terminology

Local machine (or local router): This is the system the debugging session is currently being run on. As you move the debug session from one router to the other, apply the term "local machine" to the other router.

Peer: The other end of the point-to-point link. Therefore, this device is not the local machine.

For example, if you run the **debug ppp negotiation** command on RouterA, this is the local machine, and RouterB is the peer. However, if you shift the debugging over to RouterB, then it becomes the local machine and RouterA becomes the peer.

Note: The terms local machine and peer do not imply a client-server relationship. Depending on where the debug session is run, the dialin client could be the local machine or peer.

Conventions

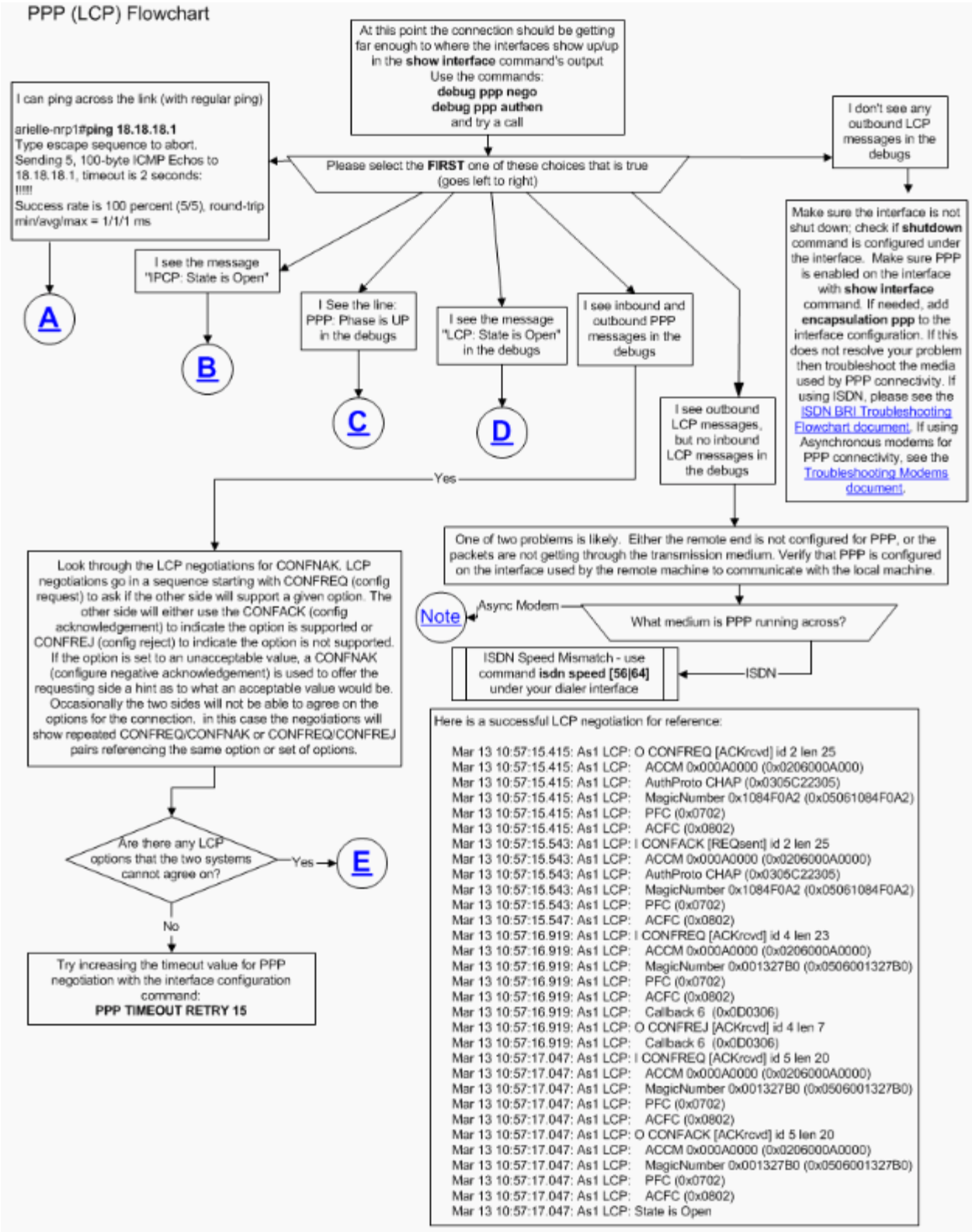
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Troubleshooting Flowcharts

This document includes some flowcharts to assist in troubleshooting.

Note: In order to troubleshoot successfully, do not skip any of the steps shown in these flowcharts.

PPP Link Control Protocol (LCP) Phase



Asynchronous Modems used for PPP Connectivity

This section explains how Asynchronous Modems can be used for PPP connectivity. Outgoing LCP frames are seen on the local router, but there are no incoming LCP frames.

In this case, the problem could be due to one of two possibilities:

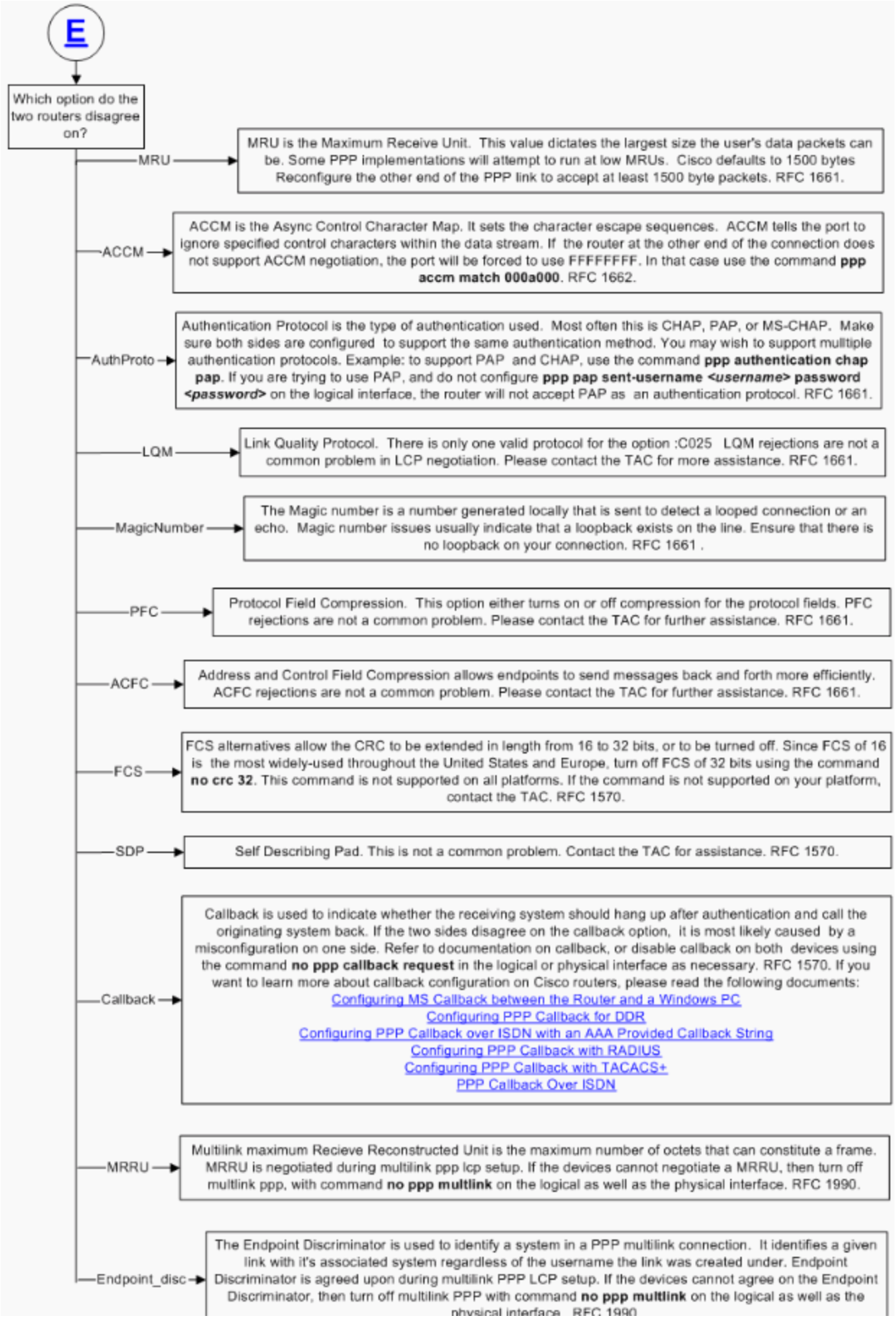
- The modems of both the local router and the remote router train up, but PPP does not start on the remote router. To troubleshoot this problem, refer to the Modems do train up okay, but PPP does not start section in the Troubleshooting Modems document.

- The modems of both the local and remote routers do train up okay, and PPP starts on both routers, but the call immediately drops. This destroys any chance of receiving incoming LCP frames from remote routers. To troubleshoot this problem, refer to the Modems do train up okay, PPP starts, but the call later drops section in the Troubleshooting Modems document.

For more detailed information on modem troubleshooting, refer to Troubleshooting Modems.

PPP Outgoing LCP Options

The flowchart below highlights several of the most common PPP LCP parameters that can be negotiated during the LCP phase. This flowchart helps you to locate which LCP parameters your PPP local machine is not negotiating with the PPP remote peer.


E
Which option do the two routers disagree on?
MRU
MRU is the Maximum Receive Unit. This value dictates the largest size the user's data packets can be. Some PPP implementations will attempt to run at low MRUs. Cisco defaults to 1500 bytes Reconfigure the other end of the PPP link to accept at least 1500 byte packets. RFC 1661.
ACCM
ACCM is the Async Control Character Map. It 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 will be forced to use FFFFFFFF. In that case use the command ppp accm match 000a000. RFC 1662.
AuthProto
Authentication Protocol is the type of authentication used. Most often this is CHAP, PAP, or MS-CHAP. Make sure both sides are configured to support the same authentication method. You may wish to support multiple authentication protocols. Example: to support PAP and CHAP, use the command ppp authentication chap pap. If you are trying to use PAP, and do not configure ppp pap sent-username <username> password <password> on the logical interface, the router will not accept PAP as an authentication protocol. RFC 1661.
LQM
Link Quality Protocol. There is only one valid protocol for the option :C025 LQM rejections are not a common problem in LCP negotiation. Please contact the TAC for more assistance. RFC 1661.
MagicNumber
The Magic number is a number generated locally that is sent to detect a looped connection or an echo. Magic number issues usually indicate that a loopback exists on the line. Ensure that there is no loopback on your connection. RFC 1661 .
PFC
Protocol Field Compression. This option either turns on or off compression for the protocol fields. PFC rejections are not a common problem. Please contact the TAC for further assistance. RFC 1661.
ACFC
Address and Control Field Compression allows endpoints to send messages back and forth more efficiently. ACFC rejections are not a common problem. Please contact the TAC for further assistance. RFC 1661.
FCS
FCS alternatives allow the CRC to be extended in length from 16 to 32 bits, or to be turned off. Since FCS of 16 is the most widely-used throughout the United States and Europe, turn off FCS of 32 bits using the command no crc 32. This command is not supported on all platforms. If the command is not supported on your platform, contact the TAC. RFC 1570.
SDP
Self Describing Pad. This is not a common problem. Contact the TAC for assistance. RFC 1570.
Callback
Callback is used to indicate whether the receiving system should hang up after authentication and call the originating system back. If the two sides disagree on the callback option, it is most likely caused by a misconfiguration on one side. Refer to documentation on callback, or disable callback on both devices using the command no ppp callback request in the logical or physical interface as necessary. RFC 1570. If you want to learn more about callback configuration on Cisco routers, please read the following documents:
Configuring MS Callback between the Router and a Windows PC
Configuring PPP Callback for DDR
Configuring PPP Callback over ISDN with an AAA Provided Callback String
Configuring PPP Callback with RADIUS
Configuring PPP Callback with TACACS+
PPP Callback Over ISDN
MRRU
Multilink maximum Recieve Reconstructed Unit is the maximum number of octets that can constitute a frame. MRRU is negotiated during multilink ppp lcp setup. If the devices cannot negotiate a MRRU, then turn off multlink ppp, with command no ppp multlink on the logical as well as the physical interface. RFC 1990.
Endpoint_disc
The Endpoint Discriminator is used to identify a system in a PPP multilink connection. It identifies a given link with it's associated system regardless of the username the link was created under. Endpoint Discriminator is agreed upon during multilink PPP LCP setup. If the devices cannot agree on the Endpoint Discriminator, then turn off multilink PPP with command no ppp multlink on the logical as well as the physical interface. RFC 1990

PPP Authentication Phase

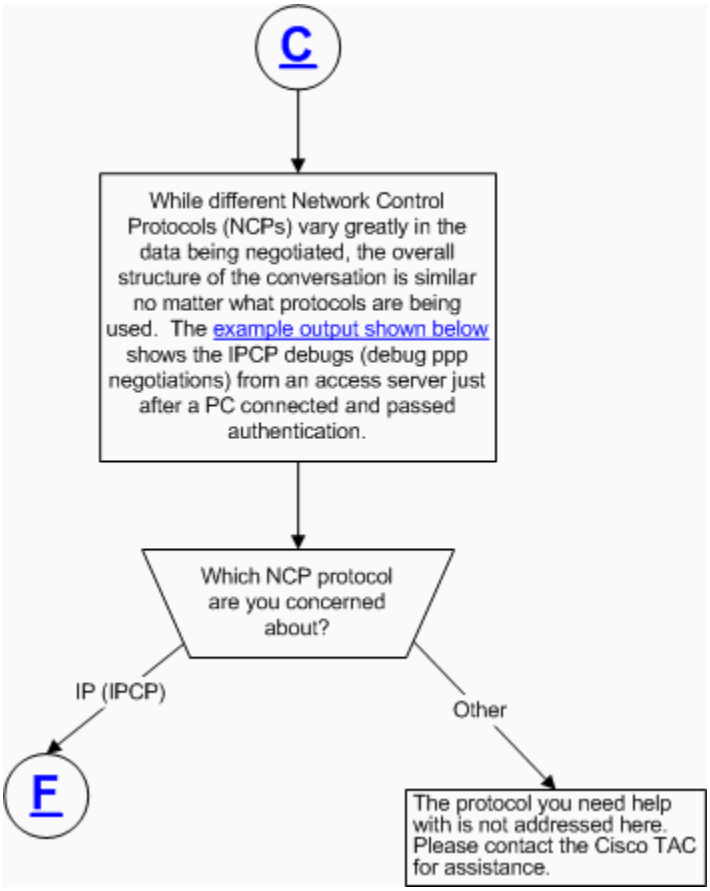
Point-to-Point Protocol provides an optional phase which guarantees the network user a secured data transmission to enhance network security. On some links it may be desirable to require a PPP peer to authenticate itself before allowing network-layer protocol packets to be exchanged. For any PPP implementation, the authentication phase is optional by default. If a PPP network administrator wants the PPP peer to use a specific authentication protocol, he must request the use of that authentication protocol during the PPP LCP phase. That is, the authentication protocol used must be one of the negotiated PPP LCP options between both PPP peers.

At this stage, only PPP LCP, authentication protocol, and link quality monitoring packets are allowed during authentication phase. Ensure that there are no problems at this stage with any PPP LCP-negotiated parameters before following the troubleshooting steps in this section.

For detailed troubleshooting information for PPP authentication phase problems, refer to the Troubleshooting PPP (CHAP or PAP) Authentication flowchart.

PPP NCP Negotiations

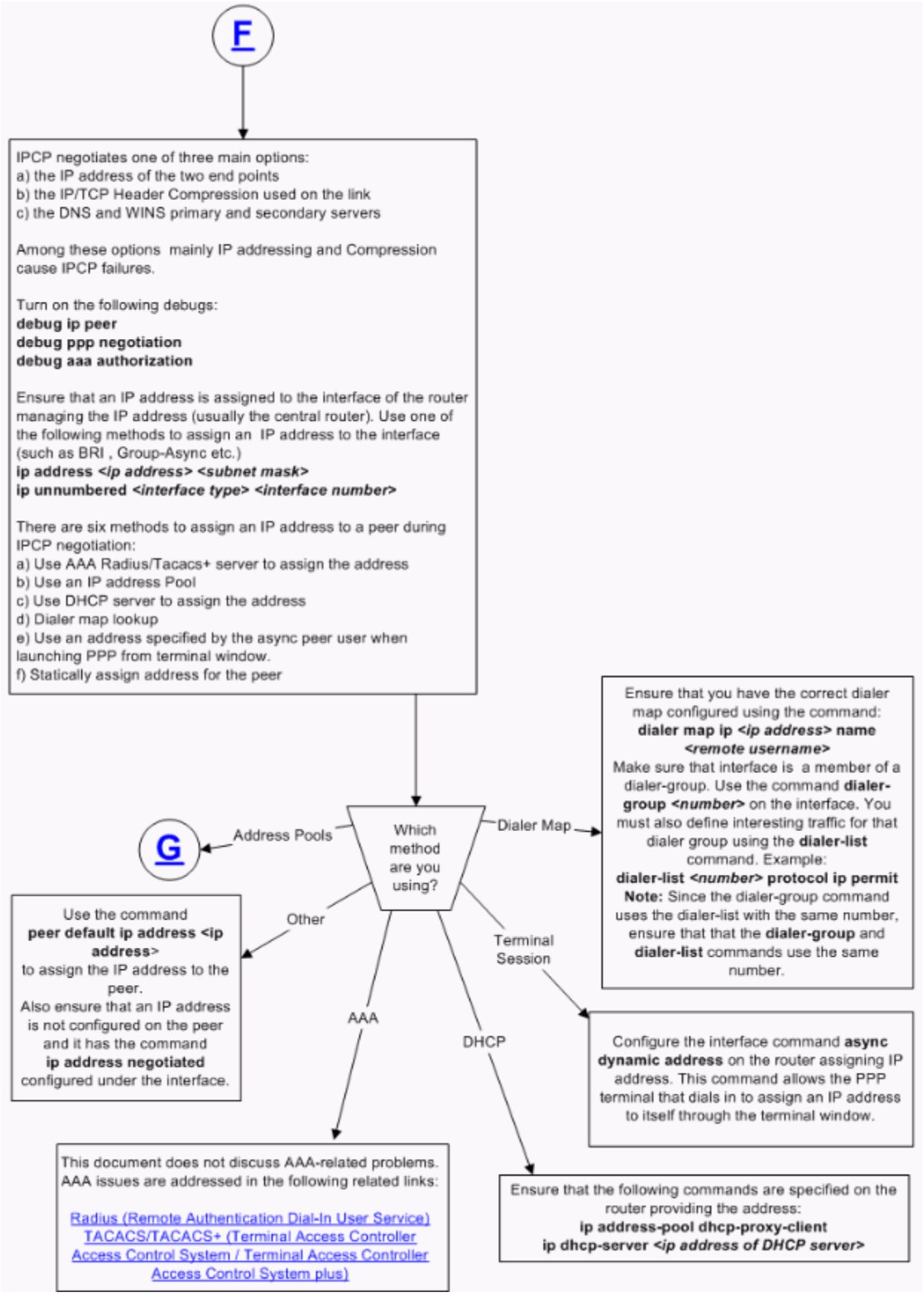
While different Network Control Protocols (NCPs) vary greatly in the data being negotiated, the overall structure of the conversation is similar no matter what protocols are being used. This section only covers IP (IPCP) NCP protocol negotiation.



The output below shows the debug output for a successful IP negotiation during PPP NCP negotiation:

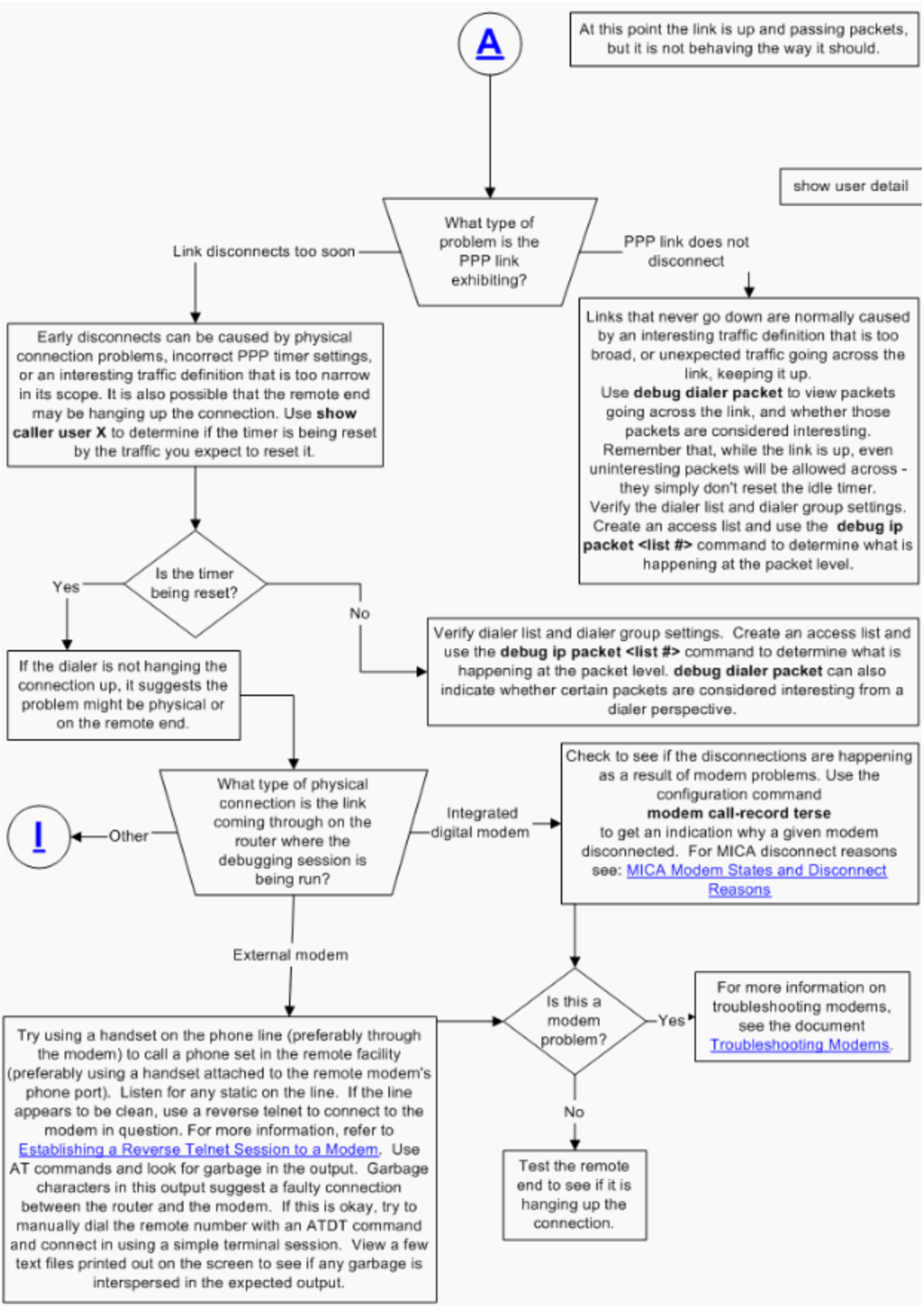
```
As4 PPP: Phase is UP
 As4 IPCP: O CONFREQ [Not negotiated] id 1 len 10
 As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
 As4 IPCP: I CONFREQ [REQsent] id 1 len 28
 As4 IPCP:    CompressType VJ 15 slots CompressSlotID (0x0206002D0F01)
 As4 IPCP:    Address 0.0.0.0 (0x030600000000)
 As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
 As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
 As4 IPCP: O CONFREJ [REQsent] id 1 len 10
 As4 IPCP:    CompressType VJ 15 slots CompressSlotID (0x0206002D0F01)
 As4 CCP: I CONFREQ [Not negotiated] id 1 len 15
 As4 CCP:    MS-PPC supported bits 0x00000001 (0x120600000001)
 As4 CCP:    Stacker history 1 check mode EXTENDED (0x1105000104)
 As4 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
 As4 LCP:  (0x80FD0101000F12060000000111050001)
 As4 LCP:  (0x04)
 As4 IPCP: I CONFACK [REQsent] id 1 len 10
 As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
 %LINEPROTO-5-UPDOWN: Line protocol on Interface Async4, changed state to up
 As4 IPCP: I CONFREQ [ACKrcvd] id 2 len 22
 As4 IPCP:    Address 0.0.0.0 (0x030600000000)
 As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
 As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
 As4 IPCP: O CONFNAK [ACKrcvd] id 2 len 22
 As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
 As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
 As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
 As4 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
 As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
 As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
 As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
 ip_get_pool: As4: validate address = 10.1.2.2
 ip_get_pool: As4: using pool default
 ip_get_pool: As4: returning address = 10.1.2.2
 set_ip_peer_addr: As4: address = 10.1.2.2 (3) is redundant
 As4 IPCP: O CONFACK [ACKrcvd] id 3 len 22
 As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
 As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
 As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
 As4 IPCP: State is Open
 As4 IPCP: Install route to 10.1.2.2
```

IPCP Does Not go Into Open State in NCP Negotiation Phase

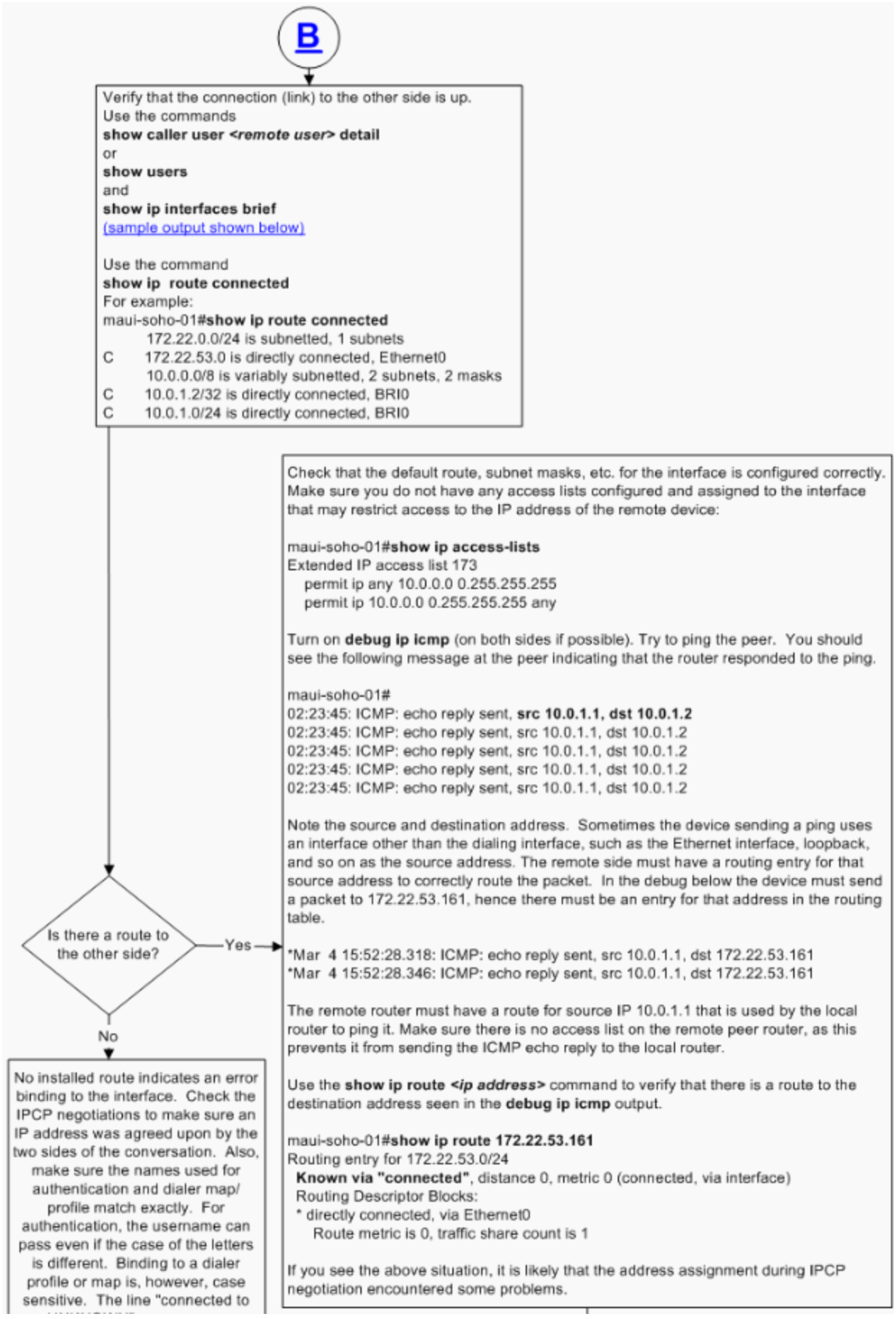


PPP Link Stability Problems

As stated in the flowchart below, at this point, the link is up and passing packets, but it is not behaving as it should.


A
At this point the link is up and passing packets, but it is not behaving the way it should.
show user detail
What type of problem is the PPP link exhibiting?
Link disconnects too soon
PPP link does not disconnect
Early disconnects can be caused by physical connection problems, incorrect PPP timer settings, or an interesting traffic definition that is too narrow in its scope. It is also possible that the remote end may be hanging up the connection. Use show caller user X to determine if the timer is being reset by the traffic you expect to reset it.
Links that never go down are normally caused by an interesting traffic definition that is too broad, or unexpected traffic going across the link, keeping it up.
Use debug dialer packet to view packets going across the link, and whether those packets are considered interesting.
Remember that, while the link is up, even uninteresting packets will be allowed across - they simply don't reset the idle timer.
Verify the dialer list and dialer group settings.
Create an access list and use the debug ip packet <list #> command to determine what is happening at the packet level.
Is the timer being reset?
Yes
No
If the dialer is not hanging the connection up, it suggests the problem might be physical or on the remote end.
Verify dialer list and dialer group settings. Create an access list and use the debug ip packet <list #> command to determine what is happening at the packet level. debug dialer packet can also indicate whether certain packets are considered interesting from a dialer perspective.
What type of physical connection is the link coming through on the router where the debugging session is being run?
I
Other
Integrated digital modem
Check to see if the disconnections are happening as a result of modem problems. Use the configuration command
modem call-record terse
to get an indication why a given modem disconnected. For MICA disconnect reasons see: MICA Modem States and Disconnect Reasons
External modem
Is this a modem problem?
Yes
For more information on troubleshooting modems, see the document Troubleshooting Modems.
No
Try using a handset on the phone line (preferably through the modem) to call a phone set in the remote facility (preferably using a handset attached to the remote modem's phone port). Listen for any static on the line. If the line appears to be clean, use a reverse telnet to connect to the modem in question. For more information, refer to Establishing a Reverse Telnet Session to a Modem. Use AT commands and look for garbage in the output. Garbage characters in this output suggest a faulty connection between the router and the modem. If this is okay, try to manually dial the remote number with an ATDT command and connect in using a simple terminal session. View a few text files printed out on the screen to see if any garbage is interspersed in the expected output.
Test the remote end to see if it is hanging up the connection.

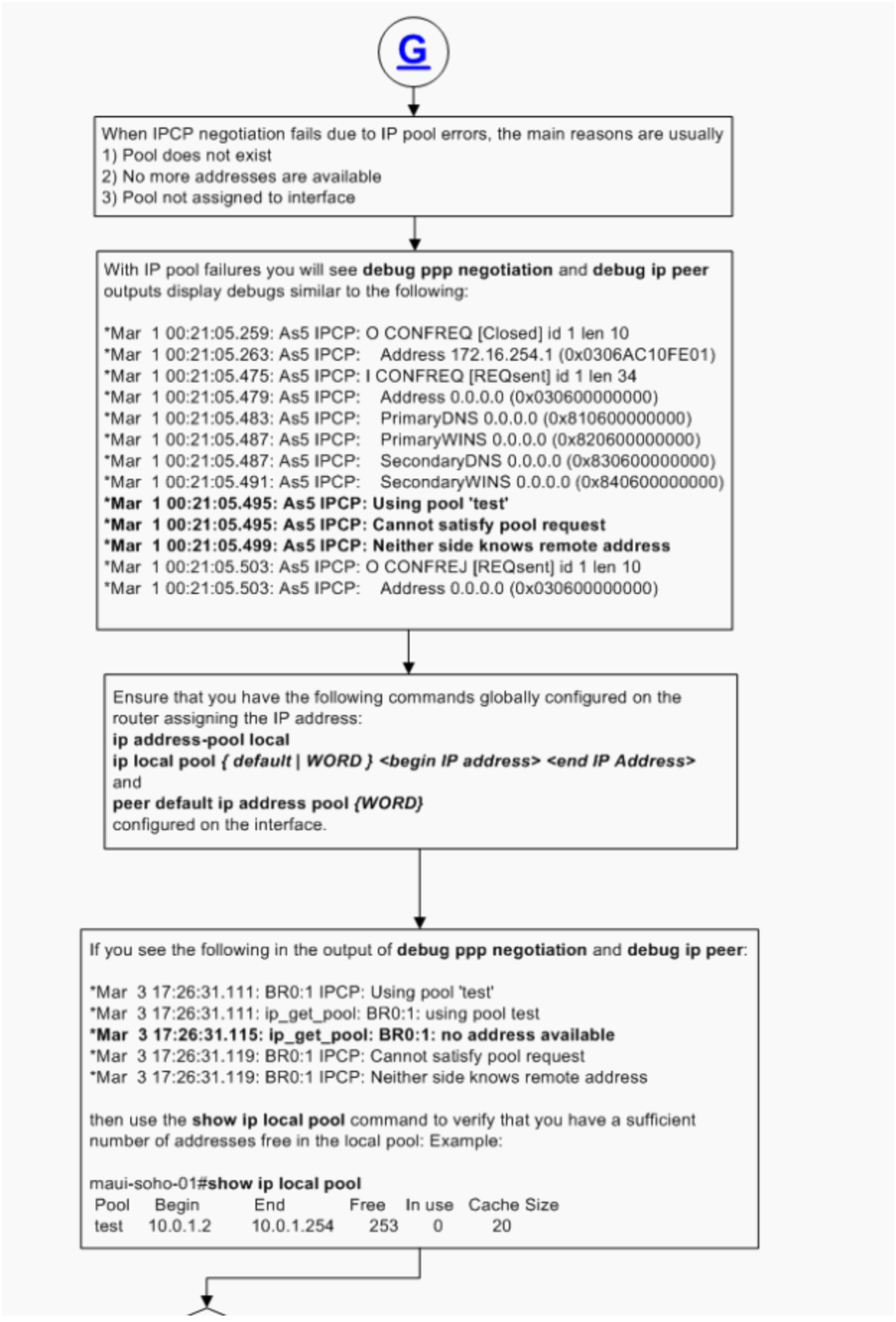
Cannot Route Packets Over an IP PPP Link


B
Verify that the connection (link) to the other side is up.
Use the commands
show caller user <remote user> detail
or
show users
and
show ip interfaces brief
(sample output shown below)
Use the command
show ip route connected
For example:
maui-soho-01#show ip route connected
172.22.0.0/24 is subnetted, 1 subnets
C 172.22.53.0 is directly connected, Ethernet0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.1.2/32 is directly connected, BRI0
C 10.0.1.0/24 is directly connected, BRI0
Check that the default route, subnet masks, etc. for the interface is configured correctly. Make sure you do not have any access lists configured and assigned to the interface that may restrict access to the IP address of the remote device:
maui-soho-01#show ip access-lists
Extended IP access list 173
permit ip any 10.0.0.0 0.255.255.255
permit ip 10.0.0.0 0.255.255.255 any
Turn on debug ip icmp (on both sides if possible). Try to ping the peer. You should see the following message at the peer indicating that the router responded to the ping.
maui-soho-01#
02:23:45: ICMP: echo reply sent, src 10.0.1.1, dst 10.0.1.2
02:23:45: ICMP: echo reply sent, src 10.0.1.1, dst 10.0.1.2
02:23:45: ICMP: echo reply sent, src 10.0.1.1, dst 10.0.1.2
02:23:45: ICMP: echo reply sent, src 10.0.1.1, dst 10.0.1.2
02:23:45: ICMP: echo reply sent, src 10.0.1.1, dst 10.0.1.2
Note the source and destination address. Sometimes the device sending a ping uses an interface other than the dialing interface, such as the Ethernet interface, loopback, and so on as the source address. The remote side must have a routing entry for that source address to correctly route the packet. In the debug below the device must send a packet to 172.22.53.161, hence there must be an entry for that address in the routing table.
Is there a route to the other side?
Yes
*Mar 4 15:52:28.318: ICMP: echo reply sent, src 10.0.1.1, dst 172.22.53.161
*Mar 4 15:52:28.346: ICMP: echo reply sent, src 10.0.1.1, dst 172.22.53.161
The remote router must have a route for source IP 10.0.1.1 that is used by the local router to ping it. Make sure there is no access list on the remote peer router, as this prevents it from sending the ICMP echo reply to the local router.
Use the show ip route <ip address> command to verify that there is a route to the destination address seen in the debug ip icmp output.
maui-soho-01#show ip route 172.22.53.161
Routing entry for 172.22.53.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via Ethernet0
Route metric is 0, traffic share count is 1
If you see the above situation, it is likely that the address assignment during IPCP negotiation encountered some problems.
No
No installed route indicates an error binding to the interface. Check the IPCP negotiations to make sure an IP address was agreed upon by the two sides of the conversation. Also, make sure the names used for authentication and dialer map/ profile match exactly. For authentication, the username can pass even if the case of the letters is different. Binding to a dialer profile or map is, however, case sensitive. The line "connected to

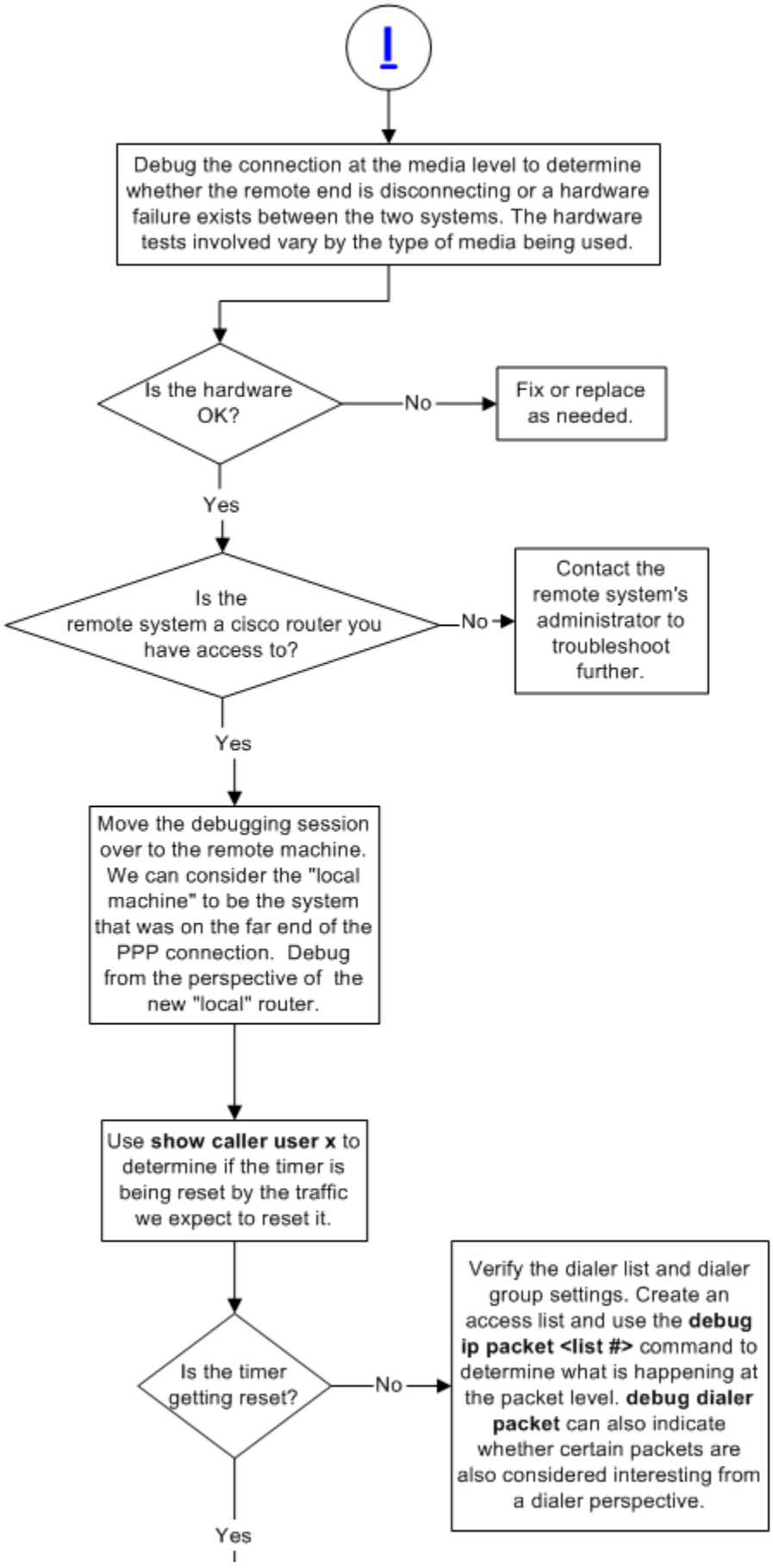
The output below shows the **show caller user** and **show ip interface brief** command output when a call is terminated successfully and IP packets can be sent to the remote peer over the PPP connection.

```
maui-soho-01#show caller user maui-soho-02 detail
   User: maui-soho-02, line BR0:1, service PPP
   Active time 00:02:21, Idle time 00:00:57
   Timeouts: Absolute Idle
   Limits: - 00:02:00
   Disconnect in: - 00:01:02
   PPP: LCP Open, CHAP (local <--> local), IPCP
   LCP: -> peer, AuthProto, MagicNumber
   <- peer, AuthProto, MagicNumber
   NCP: Open IPCP
   IPCP: <- peer, Address
   -> peer, Address
   Dialer: Connected to #, inbound
   Idle timer 120 secs, idle 57 secs
   Type is ISDN, group BRI0
   IP: Local 10.0.1.1/24, remote 10.0.1.2
   Counts: 123 packets input, 3246 bytes, 0 no buffer
   0 input errors, 0 CRC, 0 frame, 0 overrun
   119 packets output, 2940 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   maui-soho-01#show ip interface brief
   Interface IP-Address OK? Method Status Protocol
   BRI0 10.0.1.1 YES NVRAM up up
   BRI0:1 unassigned YES unset up up
   BRI0:2 unassigned YES unset down down
   Ethernet0 172.22.53.160 YES NVRAM up up
   Serial0 unassigned YES NVRAM administratively down down
```

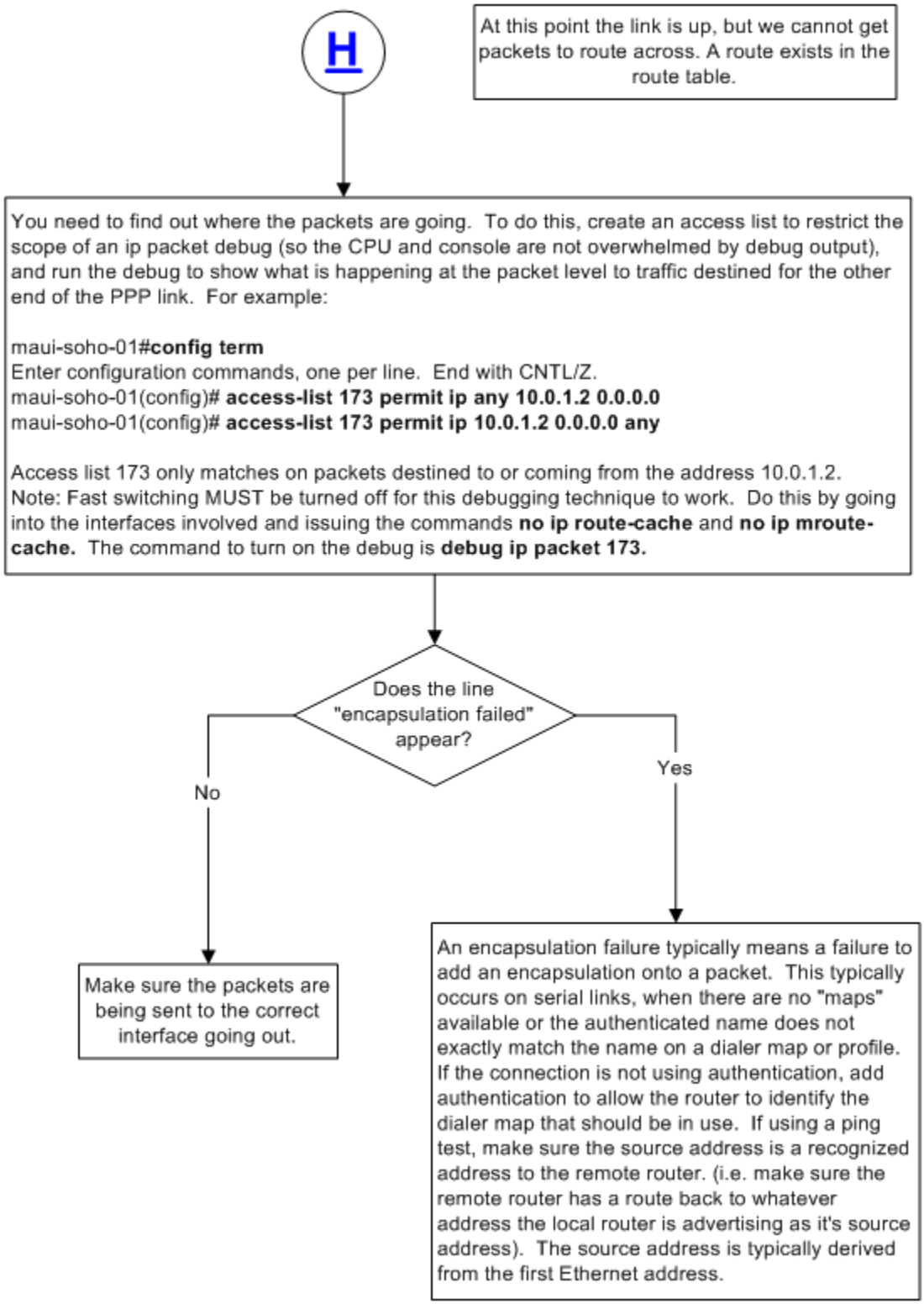
IP Pool Errors


G
When IPCP negotiation fails due to IP pool errors, the main reasons are usually
1) Pool does not exist
2) No more addresses are available
3) Pool not assigned to interface
With IP pool failures you will see debug ppp negotiation and debug ip peer outputs display debugs similar to the following:
*Mar 1 00:21:05.259: As5 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 1 00:21:05.263: As5 IPCP: Address 172.16.254.1 (0x0306AC10FE01)
*Mar 1 00:21:05.475: As5 IPCP: I CONFREQ [REQsent] id 1 len 34
*Mar 1 00:21:05.479: As5 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 1 00:21:05.483: As5 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 1 00:21:05.487: As5 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 1 00:21:05.487: As5 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 1 00:21:05.491: As5 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 1 00:21:05.495: As5 IPCP: Using pool 'test'
*Mar 1 00:21:05.495: As5 IPCP: Cannot satisfy pool request
*Mar 1 00:21:05.499: As5 IPCP: Neither side knows remote address
*Mar 1 00:21:05.503: As5 IPCP: O CONFREJ [REQsent] id 1 len 10
*Mar 1 00:21:05.503: As5 IPCP: Address 0.0.0.0 (0x030600000000)
Ensure that you have the following commands globally configured on the router assigning the IP address:
ip address-pool local
ip local pool { default | WORD } <begin IP address> <end IP Address>
and
peer default ip address pool {WORD}
configured on the interface.
If you see the following in the output of debug ppp negotiation and debug ip peer:
*Mar 3 17:26:31.111: BR0:1 IPCP: Using pool 'test'
*Mar 3 17:26:31.111: ip_get_pool: BR0:1: using pool test
*Mar 3 17:26:31.115: ip_get_pool: BR0:1: no address available
*Mar 3 17:26:31.119: BR0:1 IPCP: Cannot satisfy pool request
*Mar 3 17:26:31.119: BR0:1 IPCP: Neither side knows remote address
then use the show ip local pool command to verify that you have a sufficient number of addresses free in the local pool: Example:
maui-soho-01#show ip local pool
Pool Begin End Free In use Cache Size
test 10.0.1.2 10.0.1.254 253 0 20

Other PP Link Stability Issues


I
Debug the connection at the media level to determine whether the remote end is disconnecting or a hardware failure exists between the two systems. The hardware tests involved vary by the type of media being used.
Is the hardware OK?
No
Fix or replace as needed.
Yes
Is the remote system a cisco router you have access to?
No
Contact the remote system's administrator to troubleshoot further.
Yes
Move the debugging session over to the remote machine. We can consider the "local machine" to be the system that was on the far end of the PPP connection. Debug from the perspective of the new "local" router.
Use **show caller user x** to determine if the timer is being reset by the traffic we expect to reset it.
Is the timer getting reset?
No
Verify the dialer list and dialer group settings. Create an access list and use the **debug ip packet <list #>** command to determine what is happening at the packet level. **debug dialer packet** can also indicate whether certain packets are also considered interesting from a dialer perspective.
Yes

IP Layer 2 Bind Failures



Related Information

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