

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Terminologie](#)

[Conventions](#)

[Dépannage des organigrammes](#)

[Phase du Link Control Protocol de PPP \(LCP\)](#)

[Options sortantes du PPP LCP](#)

[Phase d'authentification de PPP](#)

[Négociations de NCP de PPP](#)

[IPCP n'entre pas dans l'état ouvert dans la phase de négociation de NCP](#)

[Problèmes de stabilité de lien de PPP](#)

[Ne peut pas conduire des paquets au-dessus d'un lien de PPP IP](#)

[Erreurs de pool d'IP](#)

[D'autres questions de stabilité de lien pp](#)

[Pannes de grippage de la couche 2 IP](#)

[Informations connexes](#)

[Introduction](#)

Cet organigramme vous aide à dépanner le protocole point-à-point (PPP), largement utilisé pour les solutions technologiques à plusieurs accès.

Dans les organigrammes et le résultat présenté d'échantillon ci-dessous, nous avons installé une connexion PPP d'accès de base (BRI) d'Integrated Services Digital Network (le RNIS) à l'autre utilisant le routage existant de Numéroteur-sur-exigence (DDR). Cependant, les mêmes étapes de dépannage s'appliquent aux connexions à d'autres Routeurs (tels que des succursales) avec des connexions PPP en utilisant le groupe rotatif de routeurs d'appels, le profil du numéroteur, ou le PPP au-dessus des liaisons série.

Pour plus d'informations sur le protocole point-à-point, et ses caractéristiques prises en charge en logiciel de Cisco IOS®, référez-vous à [Cisco apprenant la connexion](#) (clients [enregistrés](#) seulement) et la recherche utilisant le **ppp de** mot clé dans le domaine de **formation de rechercher**.

Pour une explication détaillée des différentes phases de la négociation PPP et de la sortie du **debug ppp negotiation**, référez-vous [en configurant et dépannage du Password Authentication Protocol \(PAP\) de PPP](#).

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous rencontrez ces conditions préalables :

- **Debug ppp negotiation** et **debug ppp authentication** d'enable.
- Vous devez lire et comprendre la sortie de debug ppp negotiation. Pour plus d'informations, reportez-vous à [Comprendre les sorties de la commande debug ppp negotiation](#).
- La phase d'authentification de PPP ne commence pas jusqu'à ce que la phase du Link Control Protocol (LCP) soit complète et soit dans « ouvert » l'état. Si le **debug ppp negotiation** n'indique pas que LCP est ouvert, dépannez cette question avant que vous poursuiviez.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Terminologie

Ordinateur local (ou routeur local) : C'est le système que la session d'élimination des imperfections actuellement est exécutée en fonction. Comme vous déplacez la session de débogage d'un routeur à l'autre, appliquez le terme « ordinateur local » à l'autre routeur.

Pair : L'autre fin du lien point par point. Par conséquent, ce périphérique n'est pas l'ordinateur local.

Par exemple, si vous exécutez la commande de **debug ppp negotiation** sur le RouterA, c'est l'ordinateur local, et le RouterB est le pair. Cependant, si vous décalez l'élimination des imperfections plus d'au RouterB, puis ce devient l'ordinateur local et le RouterA va bien au pair.

Remarque: Les termes ordinateur local et pair n'impliquent pas des relations de client-serveur. Selon où la session de débogage est exécutée, le client entrant pourrait être l'ordinateur local ou le pair.

Conventions

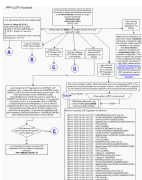
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Dépannage des organigrammes

Ce document comporte quelques organigrammes pour aider au dépannage.

Remarque: Afin de dépanner avec succès, n'ignorez pas les étapes l'unes des affichées dans ces organigrammes.

Phase du Link Control Protocol de PPP (LCP)



Modems asynchrones utilisés pour la Connectivité de PPP

Cette section explique comment des modems asynchrones peuvent être utilisés pour la Connectivité de PPP. Des trames LCP sortantes sont vues sur le routeur local, mais il n'y a aucune trame LCP entrante.

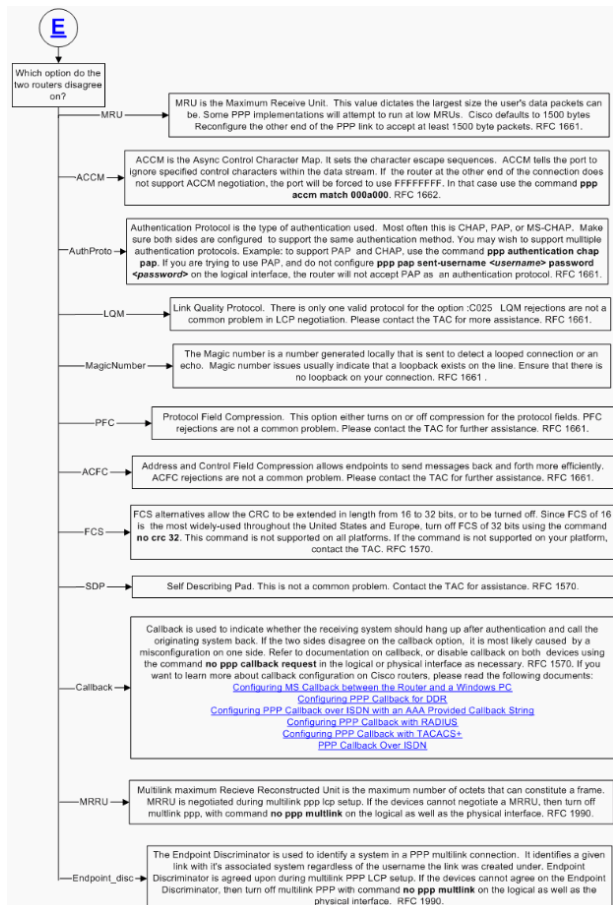
Dans ce cas, le problème a pu être dû à une de deux possibilités :

- Les Modems du routeur local et du routeur distant s'exercent, mais le PPP ne commence pas sur le routeur distant. Pour dépanner ce problème, référez-vous aux [Modems s'exercent vers le haut de l'ok, mais le PPP ne commence pas la](#) section dans le document de Modems de dépannage.
- Les Modems les des deux les routeurs locaux et distants s'exercent vers le haut de l'ok, et des débuts de PPP sur les deux Routeurs, mais l'appel chute immédiatement. Ceci détruit n'importe quelle possibilité de recevoir les trames LCP entrantes des Routeurs distants. Pour dépanner ce problème, référez-vous aux [Modems s'exercent vers le haut de l'ok, les débuts de PPP, mais la](#) section de [baisses d'appel plus tard](#) dans le document de Modems de dépannage.

Pour plus d'informations détaillées sur le dépannage de modem, référez-vous aux [Modems de dépannage](#).

Options sortantes du PPP LCP

L'organigramme ci-dessous met en valeur plusieurs des paramètres du PPP les plus communs LCP qui peuvent être négociés pendant la phase LCP. Cet organigramme vous aide à situer que les paramètres LCP votre ordinateur local de PPP n'est pas en pourparlers avec le pair de distant de PPP.



Phase d'authentification de PPP

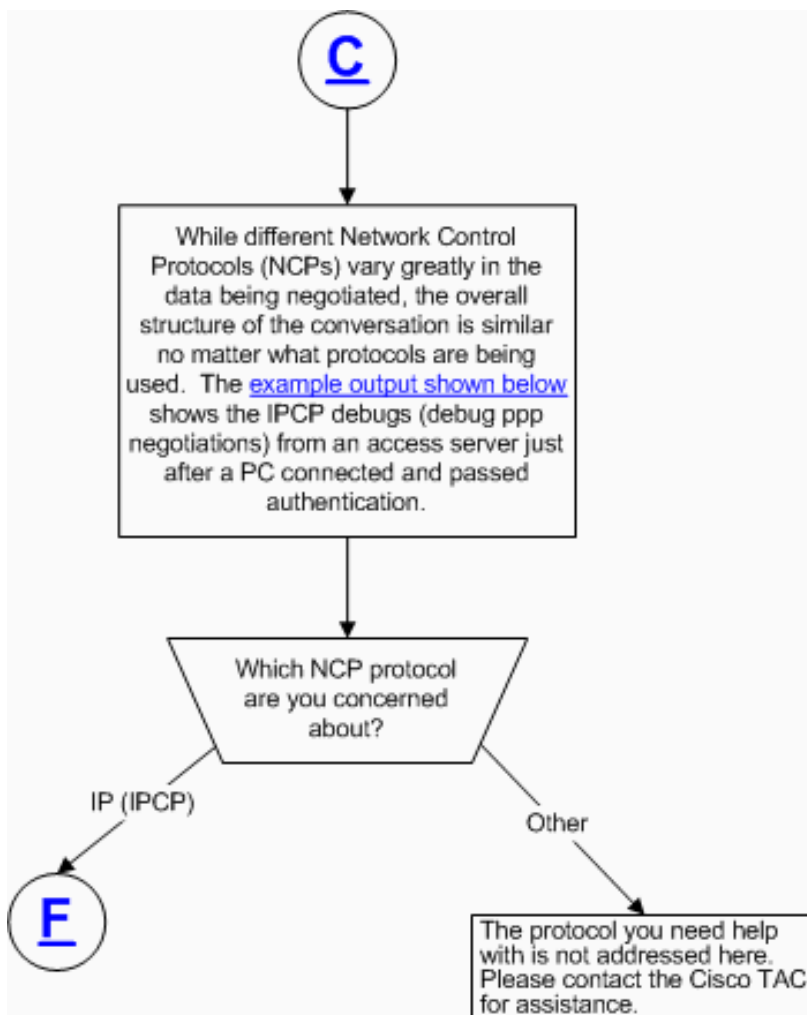
Le protocole point-à-point fournit une phase facultative qui garantit l'utilisateur du réseau une transmission de données sécurisée pour améliorer la sécurité des réseaux. Sur quelques liens il peut être désirable d'exiger d'un pair de PPP de s'authentifier avant de permettre des paquets de protocole de couche réseau à permuter. Pour n'importe quelle implémentation de PPP, la phase d'authentification est facultative par défaut. Si un administrateur réseau de PPP veut que le pair de PPP utilise un protocole d'authentification spécifique, il doit demander l'utilisation de ce protocole d'authentification pendant la phase du PPP LCP. C'est-à-dire, le protocole d'authentification utilisé doit être l'une des options négociées du PPP LCP entre les deux pairs de PPP.

À ce stade, on permet seulement le PPP LCP, le protocole d'authentification, et les paquets de surveillance de qualité de lien pendant la phase d'authentification. Assurez-vous qu'il n'y a aucun problème à ce stade avec aucun paramètre LCP-négocié par PPP avant de suivre les étapes de dépannage dans cette section.

Pour l'information de dépannage détaillée pour des problèmes de phase d'authentification de PPP, référez-vous à l'organigramme d'[authentification de PPP de dépannage \(CHAP ou PAP\)](#).

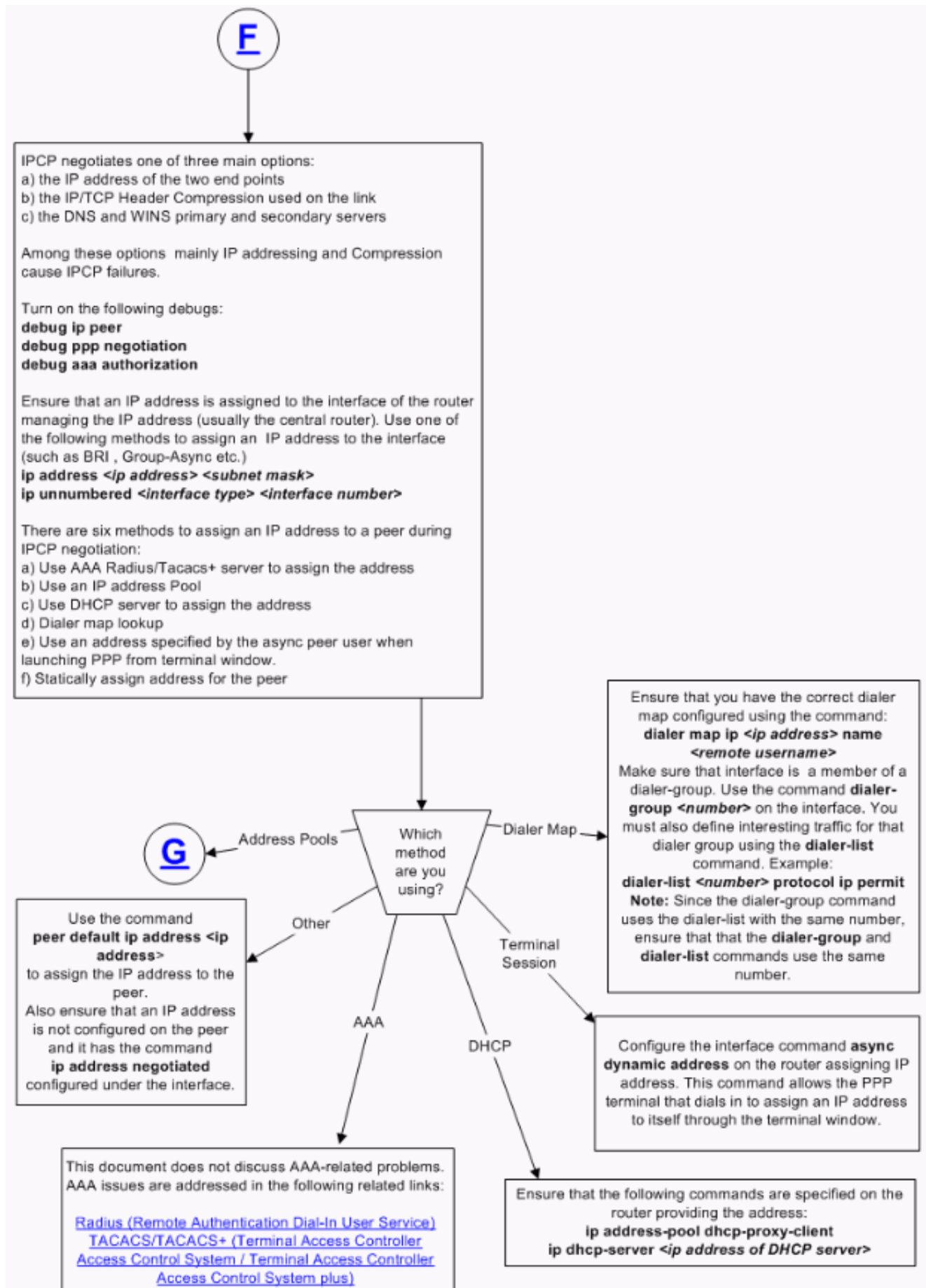
Négociations de NCP de PPP

Tandis que les différents protocoles de contrôle de réseau (NCPs) varient considérablement dans les données étant négociées, la structure globale de la conversation est semblable n'importe ce que des protocoles sont utilisés. Cette section couvre seulement la négociation de protocole de NCP IP (IPCP).



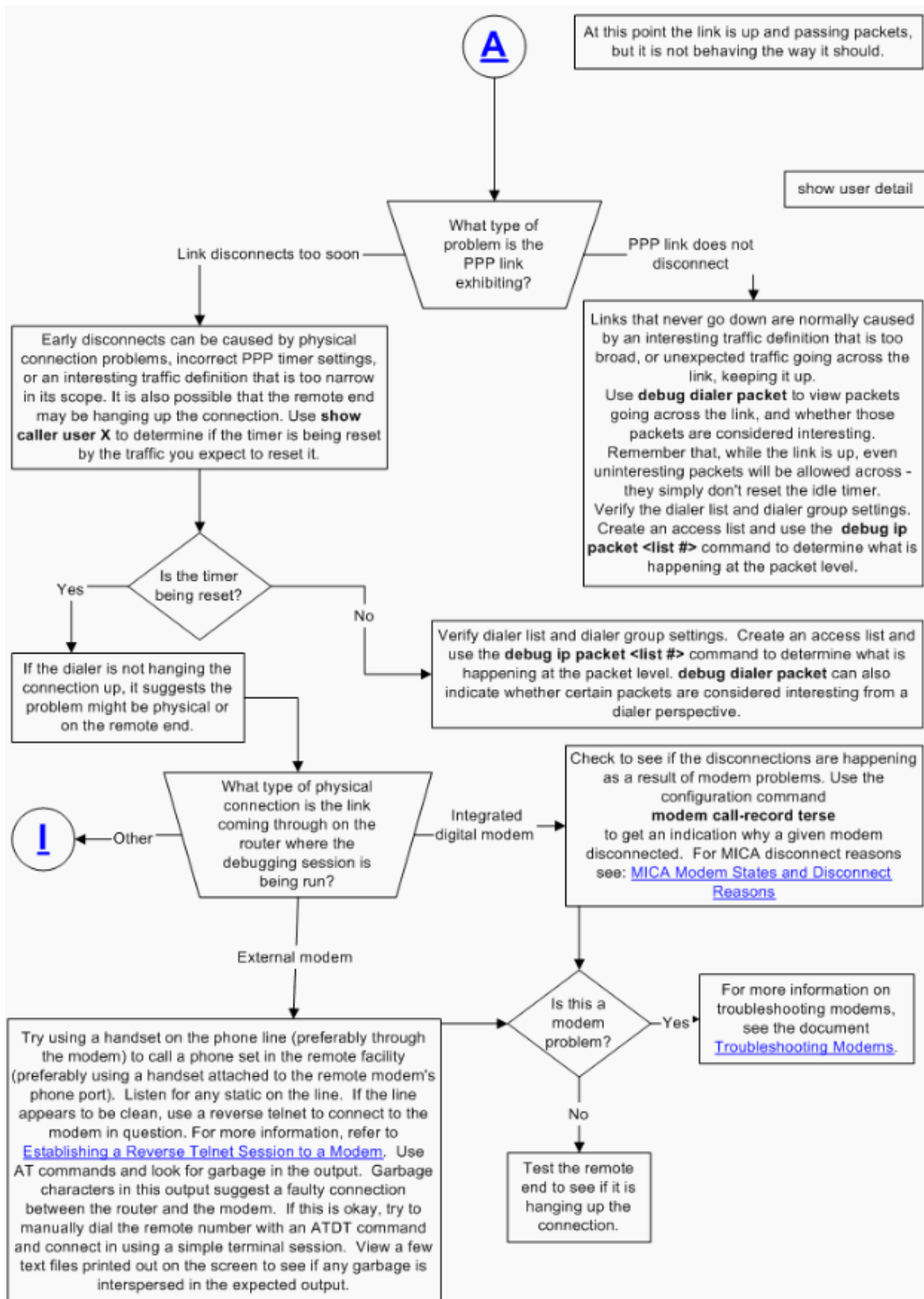
La sortie ci-dessous affiche la sortie de débogage pour une négociation réussie IP pendant la négociation de NCP de PPP :

[IPCP n'entre pas dans l'état ouvert dans la phase de négociation de NCP](#)



Problèmes de stabilité de lien de PPP

Comme stipulé dans l'organigramme ci-dessous, en ce moment, le lien est en hausse et passant des paquets, mais il ne se comporte pas comme il faudrait.



Ne peut pas conduire des paquets au-dessus d'un lien de PPP IP

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.

```
*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.

Is there a route to the other side?

Yes

No

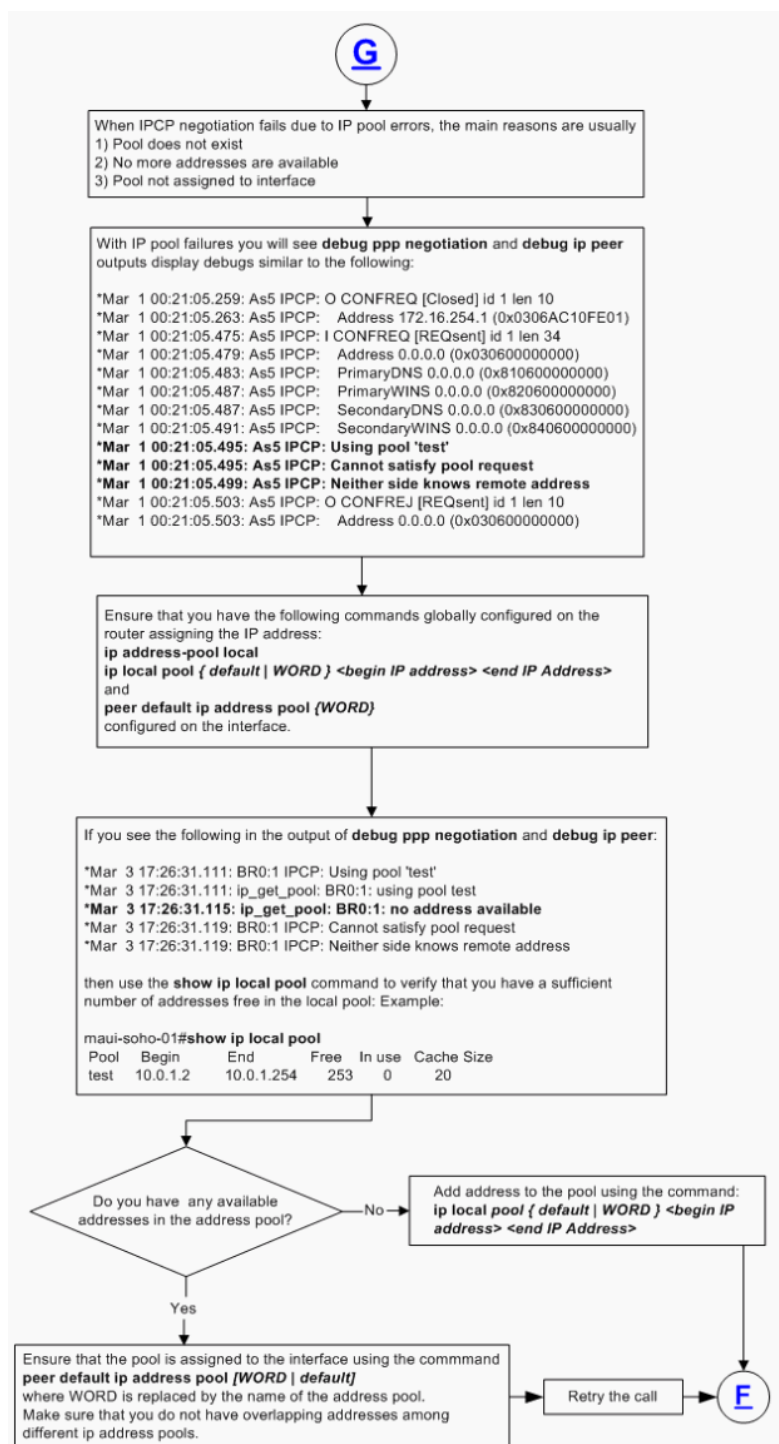
No installed route indicates an error binding to the interface. Check the IPCP negotiations to make sure an IP address was agreed upon by the two sides of the conversation. Also, make sure the names used for authentication and dialer map/profile match exactly. For authentication, the username can pass even if the case of the letters is different. Binding to a dialer profile or map is, however, case sensitive. The line "connected to UNKNOWN" may appear.

H

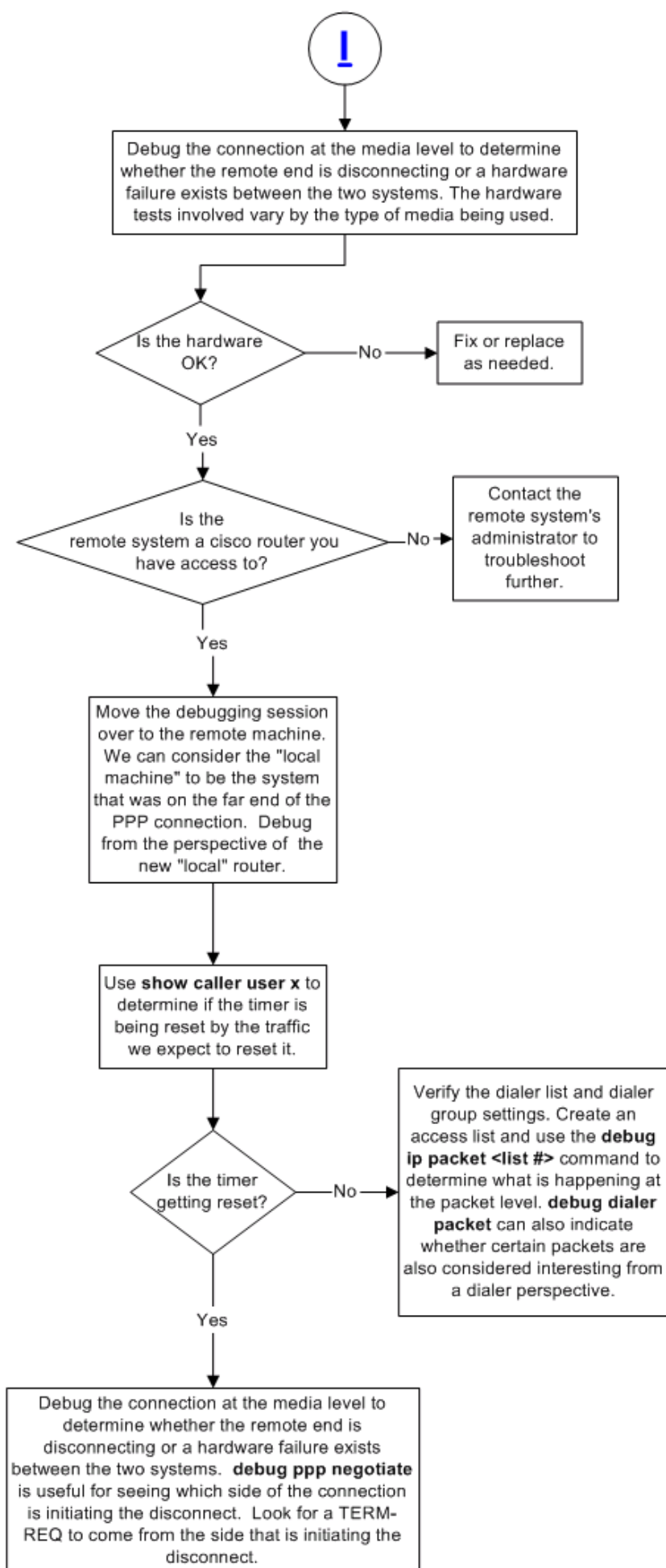
La sortie ci-dessous affiche que la **commande brief d'utilisateur et de show ip interface de show caller** a sorti quand un appel est terminé avec succès et des paquets IP peuvent être envoyés au pair distant au-dessus de la connexion PPP.

```
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
```

Erreurs de pool d'IP



D'autres questions de stabilité de lien pp



Pannes de grippage de la couche 2 IP



At this point the link is up, but we cannot get packets to route across. A route exists in the route table.

You need to find out where the packets are going. To do this, create an access list to restrict the scope of an ip packet debug (so the CPU and console are not overwhelmed by debug output), and run the debug to show what is happening at the packet level to traffic destined for the other end of the PPP link. For example:

maui-soho-01#**config term**

Enter configuration commands, one per line. End with CNTL/Z.

maui-soho-01(config)# **access-list 173 permit ip any 10.0.1.2 0.0.0.0**

maui-soho-01(config)# **access-list 173 permit ip 10.0.1.2 0.0.0.0 any**

Access list 173 only matches on packets destined to or coming from the address 10.0.1.2.

Note: Fast switching **MUST** be turned off for this debugging technique to work. Do this by going into the interfaces involved and issuing the commands **no ip route-cache** and **no ip mroute-cache**. The command to turn on the debug is **debug ip packet 173**.

Does the line
"encapsulation failed"
appear?

No

Yes

Make sure the packets are being sent to the correct interface going out.

An encapsulation failure typically means a failure to add an encapsulation onto a packet. This typically occurs on serial links, when there are no "maps" available or the authenticated name does not exactly match the name on a dialer map or profile. If the connection is not using authentication, add authentication to allow the router to identify the dialer map that should be in use. If using a ping test, make sure the source address is a recognized address to the remote router. (i.e. make sure the remote router has a route back to whatever address the local router is advertising as it's source address). The source address is typically derived from the first Ethernet address.

Informations connexes

- [Numérotation et accès de l'assistance technique](#)
- [Présentation de la sortie de négociation de débogage ppp](#)
- [Présentation et configuration de l'authentification PPP CHAP](#)
- [Authentification PPP par le biais des commandes ppp chap hostname et ppp authentication chap callin](#)
- [Configuration et dépannage du protocole PAP \(Password Authentication Protocol\) pour PPP](#)
- [Dépannage de l'authentification PPP \(CHAP ou PAP\)](#)
- [Support et documentation techniques - Cisco Systems](#)