Présentation de la sortie de négociation de débogage ppp

Contenu

Introduction

Dans les applications de numérotation, PPP est le type d'encapsulation le plus couramment utilisé. Le protocole PPP permet à deux machines sur une liaison de communication point à point de négocier différents paramètres pour l'authentification, la compression et les protocoles de couche 3 (L3), tels que IP. Une défaillance de la négociation PPP entre deux routeurs entraîne l'échec de la connexion.

La commande **debug ppp negotiation** vous permet d'afficher les transactions de négociation PPP, d'identifier le problème ou l'étape lorsque l'erreur se produit et de développer une résolution. Cependant, il est impératif que vous compreniez la sortie de la commande **debug ppp negotiation**. Ce document fournit une méthode complète pour lire la sortie de commande **debug ppp negotiation**.

Conditions préalables

Conditions requises

Les lecteurs de ce document doivent s'assurer que ces conditions sont remplies :

- Le protocole PPP doit être activé sur les interfaces des deux routeurs. Exécutez la commande **encapsulation ppp** pour cela.
- Exécutez cette commande pour activer les horodatages millisecondes sur le routeur :
  `Router(config)# service timestamp debug datetime msec`

  Pour plus d'informations sur les commandes de débogage, consultez Informations importantes sur les commandes de débogage.

Remarque : la négociation PPP entre deux homologues ne peut démarrer que si la couche inférieure (RNIS, interface physique, ligne commutée, etc.) sous PPP fonctionne parfaitement. Par exemple, si vous voulez exécuter PPP sur RNIS, toutes les couches RNIS doivent être actives ; sinon PPP ne démarre pas.

Components Used

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

Conventions

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

Phases de la négociation PPP

La liaison passe par plusieurs phases du processus de négociation PPP, comme indiqué dans ce tableau. Le résultat final est que le protocole PPP est activé ou désactivé.

Phase	Description
BAS	Dans cette phase, le protocole PPP est en panne. Ce message s'affiche après que la liaison et le protocole PPP ont été complètement désactivés : `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
ÉTABLISSEMENT	PPP passe à cette phase lorsqu'il reçoit une indication que la couche physique est active et prête à être utilisée. La négociation LCP[1] a lieu dans cette phase. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTHENTIFICATION	Si l'authentification PPP (CHAP[2] ou PAP [3]) est désirée sur la liaison, alors PPP passe à cette phase. N'oubliez pas que l'authentification PPP est facultative. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
HAUT	Une fois l'authentification terminée, le protocole PPP passe à la phase UP. La négociation NCP[4] a lieu dans cette phase. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMINAISON	Au cours de cette phase, le protocole PPP s'arrête.

	*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING

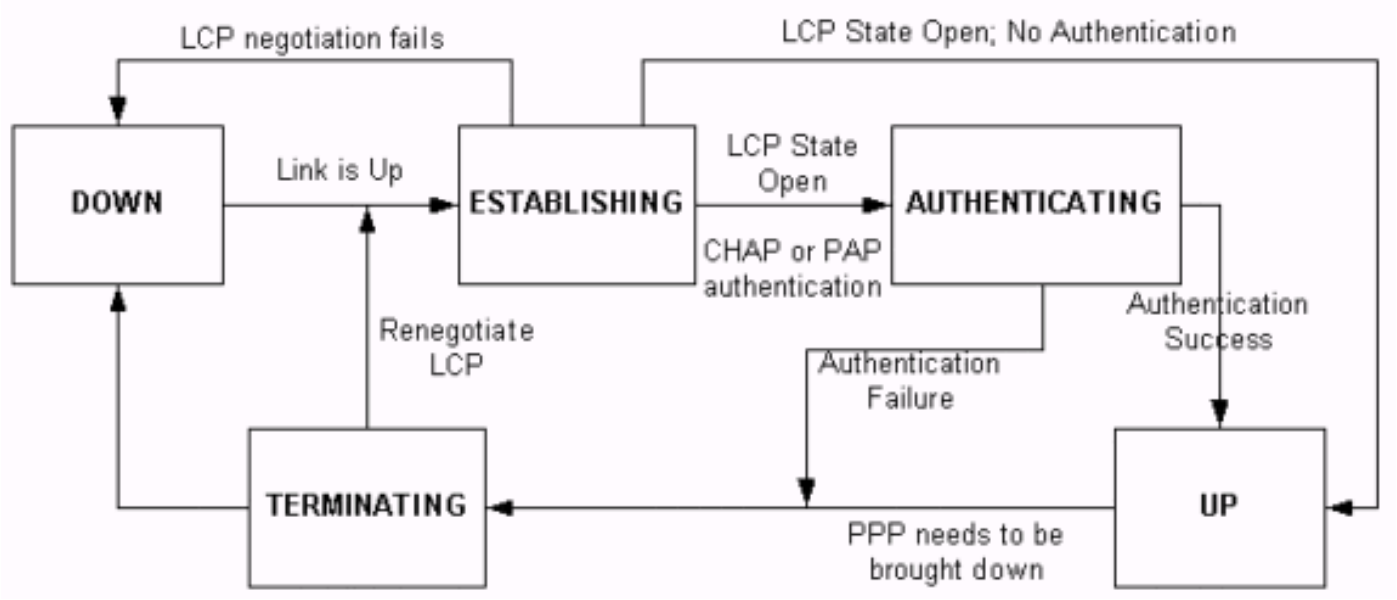
1. LCP = Link Control Protocol

2. CHAP = Protocole d'authentification à échanges confirmés

3. PAP = Password Authentication Protocol

4. NCP = Network Control Protocol

Ce diagramme montre les transitions de phase PPP :



Paquets de négociation PPP : Description

Ce tableau inclut une description des paquets de négociation PPP utilisés dans les négociations LCP et NCP :

Paquet	Code	Description
CONFRET	Configure-Request	Pour ouvrir une connexion à l'homologue, le périphérique transmet ce message, ainsi que les options de configuration et les valeurs que l'expéditeur souhaite prendre en charge. Toutes les options et valeurs sont négociées simultanément. Si l'homologue répond par un message CONFREJ ou CONFNAK, le routeur envoie un autre CONFREQ avec un autre ensemble d'options ou de valeurs.
CONFRET	Configure-Reject	Si une option de configuration reçue dans le message CONFREQ n'est pas acceptable ou n'est pas reconnaissable, le routeur répond par un message CONFREJ. L'option

		inacceptable (issue du message CONFREQ) est incluse dans le message CONFREJ.
CONFNATION	Configure-NAK[1]	Si l'option de configuration reçue est reconnaissable et acceptable, mais qu'une valeur n'est pas acceptable, le routeur transmet un message CONFNAK. Le routeur ajoute l'option et la valeur qu'il peut accepter dans le message CONFNAK afin que l'homologue puisse inclure cette option dans le prochain message CONFREQ.
CONFACTURE	Configure-ACK[2]	Si toutes les options du message CONFREQ sont reconnaissables et que toutes les valeurs sont acceptables, le routeur transmet un message CONFACK.
TERMREUR	Terminate-Request	Ce message est utilisé pour initier une fermeture LCP.
TERMACK	Terminate-ACK	Ce message est transmis en réponse au message TERMREQ.

1. NAK = Reconnaissance négative

2. ACK = Reconnaissance

Note : Chaque homologue peut envoyer des CONFREQ avec l'option ou la valeur qu'il veut que l'homologue prenne en charge. Cela peut faire en sorte que les options négociées dans chaque direction soient différentes. Par exemple, une partie peut souhaiter authentifier l'homologue, tandis que l'autre ne le peut pas.

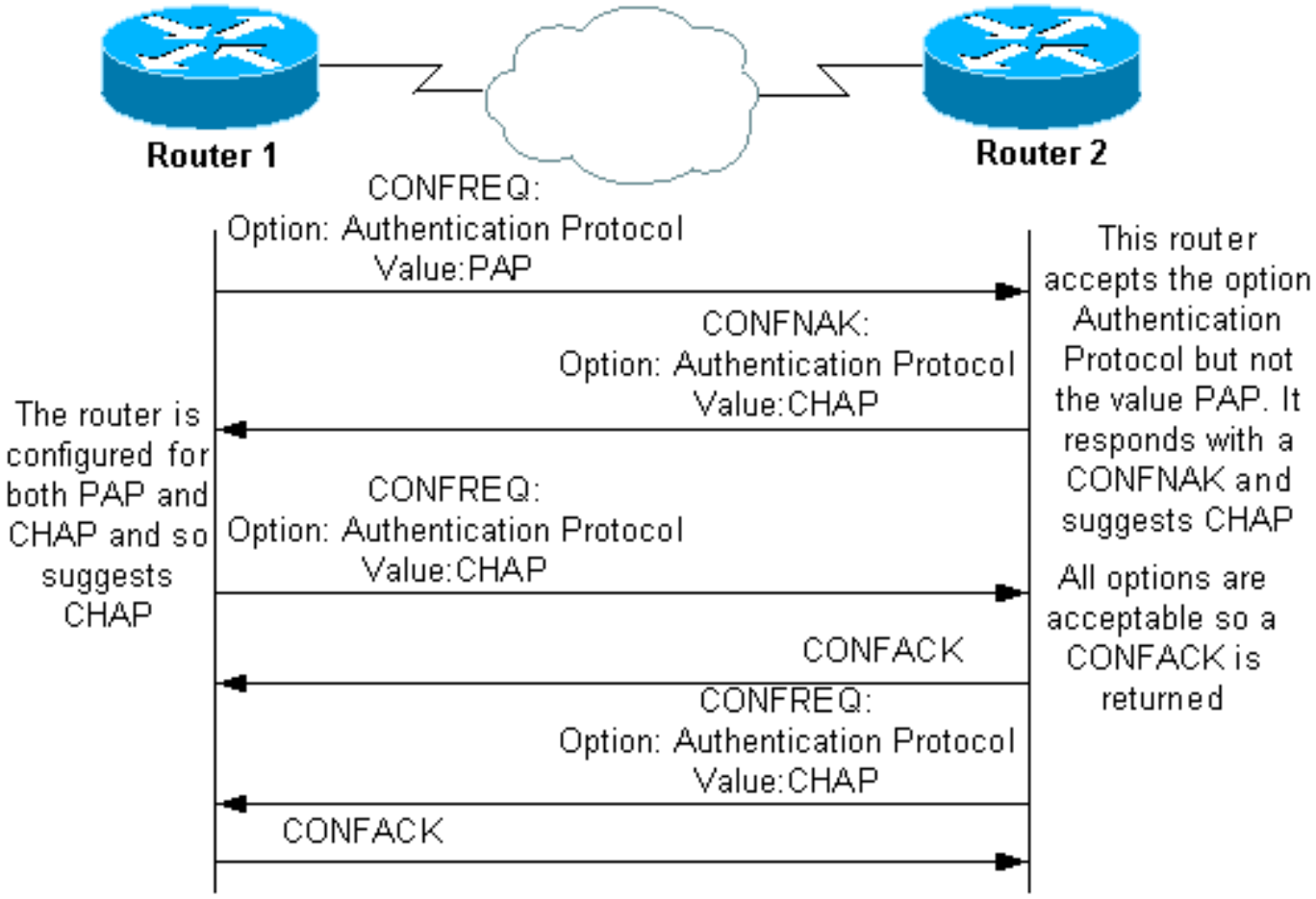
Étape LCP, Authentification et NCP

Dans certaines des phases PPP décrites précédemment, le protocole PPP entre également dans des étapes spécifiques telles que la négociation LCP, l'authentification et la négociation NCP. Pour plus d'informations, consultez RFC 1548 et RFC 1661 .

LCP (phase obligatoire)

LCP est une phase au cours de laquelle les paramètres permettant d'établir, de configurer et de tester la connexion de liaison de données sont négociés. Un état LCP ouvert signifie que le protocole LCP a été correctement terminé, tandis qu'un état LCP fermé indique une défaillance LCP.

Ce diagramme présente une vue conceptuelle d'une connexion LCP :



La négociation LCP utilise également un paramètre appelé MagicNumber, qui est utilisé pour déterminer si la liaison est bouclée. Une chaîne aléatoire est envoyée sur la liaison et, si la même valeur est renvoyée, le routeur détermine que la liaison est bouclée.

Authentification (Phase facultative par défaut)

Àcette étape, l'authentification est effectuée avec le protocole d'authentification (CHAP ou PAP) convenu lors de la négociation LCP. Pour obtenir des informations relatives au protocole PAP, reportez-vous à Configuration et dépannage du protocole PAP (PPP Password Authentication Protocol).

Pour plus d'informations sur CHAP, référez-vous à Comprendre et configurer l'authentification CHAP PPP.

Remarque : l'authentification est facultative et le protocole PPP n'entre dans cette étape que s'il doit s'authentifier.

NCP (phase obligatoire)

Cette phase est utilisée pour établir et configurer différents protocoles de couche réseau. Le protocole de couche 3 le plus couramment négocié est IP. Les routeurs échangent des messages IPCP (IP Control Protocol) pour négocier des options spécifiques au protocole (IP dans cet exemple).

Le document RFC 1332 indique que le protocole IPCP négocie deux options : les affectations d'adresses IP et de compression. Cependant, le protocole IPCP est également utilisé pour

transmettre des informations liées au réseau, telles que les serveurs WINS (Windows Name Service) principal et de sauvegarde et DNS (Domain Name System).

La négociation a lieu avec l'utilisation de messages CONF, comme décrit dans les Paquets de négociation PPP : Une section Description de ce document.

Dépannage avec la sortie de la négociation debug ppp

Lorsque vous lisez la sortie de commande **debug ppp negotiation** à des fins de dépannage, suivez les instructions suivantes :

1. Identifiez les transitions de phase dans la sortie de commande **debug**. Déterminez la phase la plus avancée de la connexion, par exemple UP ou AUTHENTICATING. Cela peut vous aider à identifier la phase dans laquelle la connexion a échoué. Pour plus d'informations sur les phases, consultez la section Phases de la négociation PPP.
2. Pour la phase au cours de laquelle l'échec s'est produit, recherchez les messages qui indiquent que LCP, l'authentification ou NCP (selon le cas) ont réussi :L'état LCP doit être ouvert. Vous pouvez également consulter les derniers messages CONFACK entrants et sortants pour vérifier que les paramètres requis ont été négociés.L'authentification doit aboutir. Si vous utilisez l'authentification bidirectionnelle, chaque transaction doit aboutir. Pour plus d'informations sur le dépannage des échecs d'authentification PPP, référez-vous à Dépannage de l'authentification PPP (CHAP ou PAP).L'état IPCP doit être ouvert. Vérifiez que l'adressage est correct et qu'une route vers l'homologue est installée.

Lire la sortie de la négociation ppp de débogage

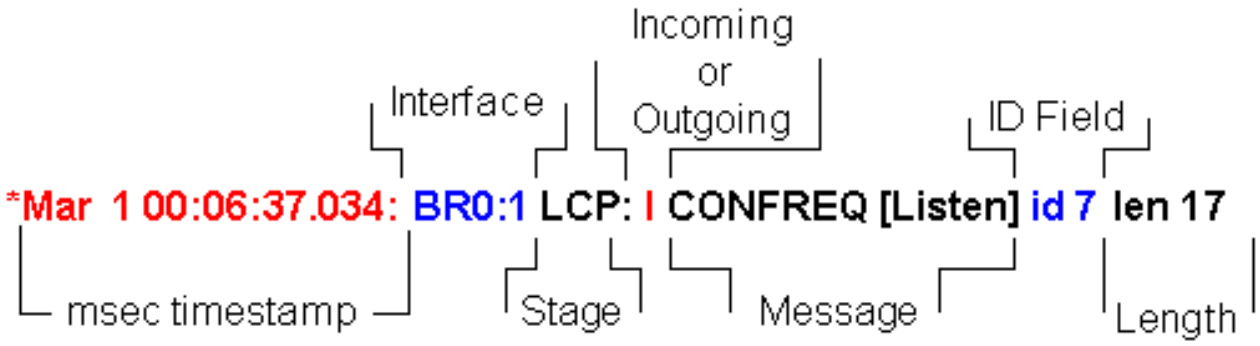
La plupart des lignes de la sortie de commande **debug ppp negotiation** sont caractérisées par :

1. **L'horodatage**—Les horodatages de millisecondes sont utiles. Consultez la section Conditions préalables de ce document pour plus d'informations.
2. **Interface and Interface number** : ce champ est utile lorsque les connexions de débogage utilisent plusieurs connexions ou lorsque la connexion passe par plusieurs interfaces. Par exemple, certaines connexions (telles que les appels multiliaison) sont contrôlées par l'interface physique au début, mais sont ensuite contrôlées par l'interface de numérotation ou l'interface d'accès virtuel.
3. **Type de message PPP** : ce champ indique si la ligne est un message général PPP, LCP, CHAP, PAP ou IPCP.
4. **Direction du message** : un **I** indique un paquet entrant et un **O** indique un paquet sortant. Ce champ peut être utilisé pour déterminer si le message a été généré ou reçu par le routeur.
5. **Message** : ce champ inclut la transaction particulière en cours de négociation.
6. **ID** : ce champ permet de faire correspondre et de coordonner les messages de demande aux messages de réponse appropriés. Vous pouvez utiliser le champ ID pour associer une réponse à un message entrant. Cette option est particulièrement utile lorsque le message entrant et la réponse sont très éloignés dans la sortie de débogage.
7. **Longueur** : le champ Longueur définit la longueur du champ d'informations. Ce champ n'est pas important pour le dépannage général.

Remarque : les champs 4 à 7 peuvent ne pas apparaître dans tous les messages PPP, selon

l'objectif du message.

Remarque : Cet exemple illustre les champs suivants :



Exemple de résultat de la négociation debug ppp

Il s'agit d'une description annotée de la sortie de commande **debug ppp negotiation** :

```
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 this 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 requests: !--- 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
!--- This is an 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 that indicates 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 !--- with 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 *!--- The 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 state to up *Mar 1 00:06:42.609: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to maui-soho-03

Glossaire et messages courants

Généralités

CONFREQ (Configure-Request) :

Lorsque la couche inférieure devient disponible (Up), un CONFREQ est envoyé pour démarrer la première phase PPP (phase LCP). Il est utilisé dans les phases LCP et NCP comme tentative de configuration de la connexion. Pour ouvrir une connexion à l'homologue, le périphérique transmet ce message, ainsi que les options de configuration et les valeurs que l'expéditeur souhaite prendre en charge. Toutes les options et valeurs sont négociées simultanément. Si l'homologue répond par un message CONFREJ ou CONFNAK, le routeur envoie un autre CONFREQ avec un autre ensemble d'options ou de valeurs.

CONFACK (Configurer-Reconnaître) :

Si toutes les options du message CONFREQ sont reconnaissables et que toutes les valeurs sont acceptables, le routeur transmet un message CONFACK.

CONFREJ (Configurer le rejet) :

Si une option de configuration reçue dans CONFREQ n'est pas acceptable ou n'est pas reconnaissable, le routeur répond par un message CONFREJ. L'option inacceptable (du CONFREQ) est incluse dans le message CONFREJ.

CONFNAK (Configurer l'accusé de réception négatif) :

Si l'option de configuration reçue est reconnaissable et acceptable, mais qu'une valeur n'est pas acceptable, le routeur transmet un message CONFNAK. Le routeur ajoute l'option et la valeur qu'il peut accepter dans le message CONFNAK afin que l'homologue puisse inclure cette option dans le prochain message CONFREQ.

ECHOREQ (Demande d'écho) et ECHOREP (Réponse d'écho) :

PPP utilise des keepalives afin de maintenir l'intégrité de la connexion. Ces keepalives sont la trame ECHOREQ qui est envoyée à l'homologue PPP distant, et l'homologue PPP distant doit répondre avec une trame ECHOREP dès réception d'une trame ECHOREQ. Par défaut, si le routeur manque cinq trames ECHOREP, la liaison est considérée comme désactivée et le protocole PPP est désactivé.

TERMREQ (Demande de résiliation) :

Cette trame indique que l'homologue PPP qui a envoyé cette trame termine la connexion PPP.

TERMACK (Renonciation) :

Ce message est transmis en réponse au message TERMREQ. Ceci ferme la connexion PPP.

TERMINAISON

Ce message indique que la connexion PPP a été désactivée. Une connexion LCP ou NCP peut être coupée :

- lors de la fermeture administrative (LCP uniquement).
- lorsque le niveau inférieur est hors service (ligne commutée, RNIS, etc.).

- lorsque les négociations sont terminées.
- Détection de boucle de ligne.

LCP

ACCM (Asynchronous Control Character Map) :

Il s'agit de l'une des options négociées LCP dans la trame CONFREQ. ACCM définit les séquences d'échappement des caractères. ACCM demande au port d'ignorer les caractères de contrôle spécifiés dans le flux de données. Si le routeur à l'autre extrémité de la connexion ne prend pas en charge la négociation ACCM, le port est forcé d'utiliser FFFFFFF. Dans ce cas, exécutez la commande suivante :

```
ppp accm match 000a000
```

ACFC (Compression des champs d'adresse et de contrôle) :

ACFC est une option LCP qui permet aux terminaux d'envoyer des messages plus efficacement.

AuthProto (Authentication Protocol) :

AuthProto est le type de protocole d'authentification négocié dans la trame CONFREQ entre les deux homologues de connexion PPP pour une utilisation dans la phase d'authentification. Si aucune authentification PPP n'est configurée, ce résultat n'est pas visible dans les paramètres négociés de trames CONFREQ. Les valeurs possibles sont CHAP ou PAP.

Rappel "#" :

Ce message indique que l'option de rappel est en cours de négociation. Le numéro après la syntaxe de rappel indique quelle option de rappel est négociée. Le nombre 0 est un rappel PPP normal, tandis que le nombre 6 indique l'option de rappel Microsoft (qui est automatiquement disponible dans le logiciel Cisco IOS® Version 11.3(2)T ou ultérieure).

CHAP (Challenge Handshake Authentication Protocol) :

Ce message indique que le protocole d'authentification en cours de négociation est CHAP.

DisquePointDeTerminaison (Discriminateur De Point De Fin) :

Il s’agit d’une option LCP utilisée pour identifier un homologue PPP dans une connexion multiliaison PPP. Pour plus d'informations, référez-vous à Critères de dénomination des packs PPP multiliaison.

LCP : État ouvert

Ce message indique que la négociation LCP s'est terminée correctement.

LQM (Link Quality Monitoring)

LQM est disponible sur toutes les interfaces série qui exécutent le protocole PPP. LQM surveille la qualité de la liaison et désactive la liaison lorsque la qualité tombe sous un pourcentage configuré. Les pourcentages sont calculés pour les directions entrantes et sortantes. La qualité sortante est calculée par comparaison du nombre total de paquets et d'octets envoyés avec le nombre total de paquets et d'octets reçus par l'homologue. La qualité entrante est calculée par comparaison du nombre total de paquets et d'octets reçus avec le nombre total de paquets et d'octets envoyés par l'homologue.

Lorsque LQM est activé, les rapports de qualité de liaison (LQR) sont envoyés à chaque période de veille. Les LQR sont envoyés à la place des keepalives. Toutes les keepalives entrantes reçoivent une réponse correcte. Si LQM n'est pas configuré, des messages de test d'activité sont envoyés à chaque période de test d'activité et tous les LQR entrants reçoivent une réponse avec un LQR.

MagicNumber

La prise en charge du numéro magique est disponible sur toutes les interfaces série. PPP tente toujours de négocier des numéros magiques, qui sont utilisés pour détecter les réseaux en boucle. Une chaîne aléatoire est envoyée sur la liaison et si la même valeur est renvoyée, le routeur détermine que la liaison est bouclée.

La liaison peut être arrêtée ou non lors de la détection de bouclage ; cela dépend de l'utilisation de la commande **down-when-looped**.

PAP (Password Authentication Protocol)

Ce message indique que le protocole d'authentification en cours de négociation pour être utilisé par les homologues PPP est PAP. Pour plus d'informations sur PAP, référez-vous à Configuration et dépannage du protocole PAP (PPP Password Authentication Protocol).

PFC (Protocol Field Compression)

Cette option active ou désactive la compression pour les champs de protocole.

MRRU (unité de réception reconstruite max.)

Il s'agit d'une option LCP négociée dans le processus de configuration LCP multiliaison PPP. Cette option détermine le nombre maximal d’octets pouvant constituer une trame. Si MRRU n'est pas négocié dans LCP, le protocole Multilink PPP (MPPP) ne peut pas s'exécuter sur la liaison.

MRU (unité reçue maximale)

MRU est une option LCP négociée dans la trame CONFREQ pour négocier la taille des paquets échangés.

Authentification

AUTH-REQ (demande d'authentification)

Cette trame est envoyée de l'homologue PPP local (sur lequel l'authentification est activée) à l'homologue distant. Il demande à l'homologue distant d'envoyer un nom d'utilisateur et un mot de passe valides pour l'authentification de connexion PPP. Cette trame est utilisée uniquement avec PAP.

AUTH-ACK (Authentification reconnue)

Cette trame est envoyée de l'homologue PPP authentifié à l'homologue PPP authentifiant. Cette trame porte le nom d'utilisateur et le mot de passe valides. Cette trame est utilisée uniquement lorsque PAP est utilisé pour l'authentification de connexion PPP.

AUTH-NAK ou FAILURE

Cette trame est envoyée depuis l'homologue PPP d'authentification lorsque l'authentification a échoué sur l'homologue PPP d'authentification.

DÉFI

Il s'agit de la trame de défi CHAP qui est envoyée de l'homologue PPP d'authentification à l'homologue PPP authentifié. La trame de demande de confirmation se compose d'un ID, d'un numéro aléatoire et du nom d'hôte du serveur de communication local ou du nom de l'utilisateur sur le périphérique distant. Cette trame est utilisée uniquement lorsque CHAP est utilisé pour l'authentification de connexion PPP.

RÉPONSE

Cette trame est la réponse CHAP envoyée de l'homologue PPP authentifié à l'homologue PPP authentifiant.

La réponse requise se compose de deux parties :

- Sortie de hachage MD5 du secret partagé.
- Nom d'hôte du périphérique distant ou nom de l'utilisateur du périphérique distant.

Cette trame est utilisée uniquement lorsque CHAP est utilisé pour l'authentification de connexion PPP.

NCP

Adresse a.b.c.d

- Sur un message CONFREQ sortant, cette valeur indique l'adresse IP que le routeur local souhaite utiliser. Si l'adresse incluse est 0.0.0.0, la machine locale demande à l'homologue de lui fournir une adresse IP qu'il peut utiliser.
- Sur un message CONFREQ entrant, cette valeur indique l'adresse IP que l'homologue souhaite utiliser. Si l'adresse incluse est 0.0.0.0, l'homologue demande à la machine locale de lui fournir une adresse IP qu'elle peut utiliser.

- Sur un message CONFNAK sortant, cette valeur indique l'adresse IP que l'homologue doit utiliser plutôt que celle que l'homologue suggère dans le message CONFREQ.
- Sur un message CONFNAK entrant, cette valeur indique l'adresse IP que la machine locale doit utiliser, au lieu de celle qu'elle a suggérée dans le message CONFREQ précédent.
- Sur un message CONFACK sortant, cette valeur indique que l'adresse IP demandée par l'homologue est acceptable pour la machine locale.
- Sur un message CONFACK entrant, cette valeur indique que l'adresse IP demandée par la machine locale est acceptable pour l'homologue.

CCP (Compression Control Protocol)

Ce message indique qu'un protocole de compression est en cours de négociation entre les deux homologues PPP. Le logiciel Cisco IOS prend en charge ces protocoles de compression à négocier sur une connexion PPP :

- Compression MS-Point-to-Point (MS-PPC)
- empileur
- prédicteur

CDPCP (Cisco Discovery Protocol Control Protocol)

Ce message indique que la négociation CDP a lieu dans la phase NCP. Pour désactiver le protocole CDP sur le routeur, exécutez la commande **no cdp run**.

CODEREJ (Rejet du code)

Un paquet CODEREJ est envoyé à la réception d'un paquet non interprétable compressé à partir de l'homologue PPP distant.

Installer la route vers a.b.c.d

Lorsque le routeur termine le protocole IPCP (phase NCP pour le protocole IP L3), il doit installer l'adresse IP donnée à l'homologue PPP distant dans la table de routage et être considéré comme une route connectée dans la table de routage. Si ce message ne s'affiche pas, vérifiez que la commande **no peer neighbor-route** n'est pas configurée.

IPCP (IP Control Protocol)

Cette valeur indique qu'IP est la couche réseau en cours de négociation dans la phase NCP.

État IPCP ouvert

Ce message indique que la phase IPCP (phase NCP pour le protocole IP L3) a été effectuée avec succès.

PROTREJ (Refus de protocole)

L'homologue PPP, à la réception d'un paquet PPP avec un champ de protocole inconnu, utilise le

message PROTREJ pour indiquer que l’homologue a tenté d’utiliser un protocole non pris en charge. Lorsqu’un périphérique PPP reçoit un message PROTREJ, il doit cesser à la première occasion d’envoyer des paquets du protocole indiqué.

Informations connexes

- Configuration et dépannage du protocole PAP (Password Authentication Protocol) pour PPP
- Authentification PPP par le biais des commandes ppp chap hostname et ppp authentication chap callin
- Présentation et configuration de l'authentification PPP CHAP
- Dépannage de l'authentification PPP (CHAP ou PAP)
- Pages d'assistance sur la technologie de numérotation
- Support technique - Cisco Systems