Présentation de la sortie de négociation de débogage ppp

Contenu

Introduction

Dans des applications liées au cadran, le PPP est le type d'encapsulation le plus utilisé généralement. Le PPP permet à deux ordinateurs sur une liaison de communication point par point pour négocier de divers paramètres pour l'authentification, le compactage, et les protocoles de la couche 3 (L3), tels que l'IP. Une panne dans la négociation PPP entre deux Routeurs fait échouer la connexion.

Les commandes enables de **debug ppp negotiation** vous pour visualiser les transactions de négociation PPP, identifiez le problème ou l'étape quand l'erreur se produit, et élaborez une résolution. Cependant, il est impératif que vous comprenniez la sortie de commande de **debug ppp negotiation**. Ce document fournit une méthode complète pour lire la sortie de commande de **debug ppp negotiation**.

Conditions préalables

Conditions requises

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

- Le PPP doit être activé sur les interfaces sur les deux Routeurs. Émettez la commande d'**encapsulation ppp** d'accomplir ceci.
- Émettez cette commande d'activer des horodatages en millisecondes sur le routeur :`Router(config)# service timestamp debug datetime msec` Pour plus d'informations sur des commandes de débogage, voir les informations importantes sur des commandes de debug.

Remarque: La négociation PPP entre deux pairs ne peut pas commencer à moins que la couche inférieure (le RNIS, interface physique, ligne commutée, et ainsi de suite) sous le PPP fonctionne parfaitement. Par exemple, si vous voulez exécuter le PPP au-dessus du RNIS, puis toutes les couches RNIS doivent être en hausse ; autrement le PPP ne commence pas.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Phases de négociation PPP

Le lien passe par plusieurs phases en cours de négociation PPP, suivant les indications de cette table. Le résultat final est que le PPP est l'un ou l'autre en haut ou en bas.

Phase	Description
VERS LE BAS	Dans cette phase, le PPP est vers le bas. Ce message est vu après le lien et le PPP sont complètement réduits : `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
ÉTABLISSEMENT	Transitions de PPP à cette phase où il reçoit une indication que la couche physique est en hausse et prête à être utilisée. La négociation LCP[1] se produit dans cette phase. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTHENTIFIER	Si l'authentification de PPP (CHAP[2] ou PAP[3]) est désirée sur le lien, puis des transitions de PPP à cette phase. Maintenez dans l'esprit que l'authentification de PPP est facultative. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
VERS LE HAUT DE	Une fois que l'authentification est complète, des transitions de PPP à la phase HAUTE. La négociation du NCP[4] se produit dans cette phase. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMINAISON	Dans cette phase, le PPP s'est arrêté. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

1. LCP = Link Control Protocol

2. CHAP = authentification Protocol à échanges confirmés

3. PAP = protocole d'identification de mot de passe

4. NCP = protocole de contrôle de réseau

Ce diagramme affiche les transitions de phase de PPP :

Paquets de négociation PPP : Une description

Cette table inclut la description des paquets de négociation PPP qui sont utilisés dans la négociation LCP et de NCP :

Paquet	Code	Description
CONFREQ	Configure r-demande	Pour ouvrir une connexion au pair, le périphérique transmet ce message avec les options de configuration et évalue l'expéditeur souhaite le pair pour le prendre en charge. Toutes les options et valeurs sont négociées simultanément. Si le pair répond avec un message CONFREJ ou CONFNAK, alors le routeur envoie un autre CONFREQ avec un ensemble d'options ou des valeurs différent.
CONFREJ	Configure r-anomalie	Si une certaine option de configuration reçue dans le message CONFREQ n'est pas acceptable ou non reconnaissable, le routeur répond avec un message CONFREJ. L'option inacceptable (du message CONFREQ) est incluse dans le message CONFREJ.
CONFNAK	Configure r-NAK[1]	Si l'option de configuration reçue est reconnaissable et acceptable, mais une certaine valeur n'est pas acceptable, le routeur transmet un message CONFNAK. Le routeur ajoute l'option et la valeur qu'il peut recevoir dans le message CONFNAK de sorte que le pair puisse inclure cette option dans le prochain message CONFREQ.
CONFACK	Configure r-ACK[2]	Si toutes les options dans le message CONFREQ sont reconnaissables et toutes les valeurs sont acceptables, alors le routeur transmet un message CONFACK.
TERMRE	Terminer-demande	Ce message est utilisé pour initier un LCP étroitement.

Q		
TERMACK	TERMINER-ACK	Ce message est transmis en réponse au message TERMREQ.

1. NAK = reconnaissance négative

2. L'ACK = reconnaissent

Remarque: Chaque pair peut envoyer CONFREQs avec l'option ou l'évaluer veut que le pair le prenne en charge. Ceci peut entraîner les options négociées dans chaque direction pour être différent. Par exemple, un côté peut souhaiter authentifier le pair, alors que l'autre ne peut pas.

LCP, authentification, et étape de NCP

Dans certaines des phases de PPP décrites précédemment, le PPP entre également dans les étapes spécifiques telles que la négociation LCP, l'authentification, et la négociation de NCP. Le pour en savoir plus, se rapportent à RFC 1548 et à RFC 1661 .

LCP (phase obligatoire)

LCP est une phase l'où des paramètres pour établir, configurer, et tester la connexion logique sont négociés. Un état LCP d'ouvert signifie que LCP a été avec succès terminé, alors qu'un état LCP de fermé indique une panne LCP.

Ce diagramme affiche une vue conceptuelle d'une prise de contact LCP :

La négociation LCP utilise également un paramètre appelé MagicNumber, qui est utilisé pour déterminer si le lien est fait une boucle - arrière. Une chaîne aléatoire est envoyée à travers le lien et, si la même valeur est retournée, alors le routeur détermine que le lien est fait une boucle - arrière.

Authentification (phase facultative par défaut)

Dans cette étape, l'authentification est exécutée avec le protocole d'authentification (CHAP ou PAP) convenu dans la négociation LCP. Pour les informations relatives PAP, référez-vous en configurant et dépannage du Password Authentication Protocol (PAP) de PPP.

Pour les informations relatives de CHAP, référez-vous à comprendre et à configurer l'authentification de PPP CHAP.

Remarque: L'authentification est facultative et le PPP écrit seulement cette étape s'il doit authentifier.

NCP (phase obligatoire)

Cette phase est utilisée pour établir et configurer différents protocoles de couche réseau. Le protocole L3 le plus commun négocié est IP. Les Routeurs permutent des messages du protocole de contrôle IP (IPCP) pour négocier des options spécifiques au protocole (IP dans cet exemple).

RFC 1332 indique qu'IPCP négocie deux options : compactage et affectations d'adresse IP. Cependant, IPCP est également utilisé pour passer les informations liées au réseau telles que les serveurs primaires et de fenêtres de sauvegarde de nom de service (WINS) et de Système de noms de domaine (DNS).

La négociation se produit avec l'utilisation TÉLÉCONFÉRENCE des messages, comme décrit dans les paquets de négociation PPP : Une section de description de ce document.

Dépannage avec la sortie de debug ppp negotiation

Quand vous lisez la sortie de commande de **debug ppp negotiation** pour dépannage des buts, suivez ces instructions :

1. Identifiez les transitions de phase dans la sortie de commande de **débogage**. Déterminez la autre phase la connexion réalisée, comme HAUT ou AUTHENTIFIER. Ceci peut vous aider à identifier la phase l'où la connexion a manqué. Pour plus d'informations sur les phases, voyez les phases de la section de négociation PPP.
2. Pour la phase l'où la panne s'est produite, recherchez les messages qui indiquent que LCP, authentification, ou NCP (en tant qu'approprié) sont réussis :L'état LCP devrait être ouvert. Vous pouvez également regarder les derniers messages entrants et sortants CONFACK pour vérifier que les paramètres que vous exigez ont été négociés.L'authentification devrait être réussie. Si vous utilisez l'authentification bi-directionnelle, alors chaque transaction doit être réussie. Pour plus d'informations sur des défaillances d'authentification PPP de dépannage, référez-vous à l'authentification de PPP de dépannage (CHAP ou PAP).L'état IPCP devrait être ouvert. Vérifiez que l'adressage est correct et qu'une artère au pair est installée.

Lisez la sortie de debug ppp negotiation

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

1. **L'horodateur** — Les horodatages en millisecondes sont utiles. Voyez la section de conditions préalables de ce pour en savoir plus de document.
2. **Nombre d'interface et d'interface** — Ce champ est utile quand mettez au point connexions d'utilisation de connexions les plusieurs, ou quand les transitions de connexion par plusieurs interfaces. Par exemple, certaines connexions (telles que des appels multiliaisons) sont contrôlées par l'interface physique au début, mais plus tard sont contrôlées par l'interface de numérotation ou l'interface d'accès virtuel.
3. **Type de message de PPP** — Ce champ indique si la ligne est un message général de PPP, LCP, de 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 était généré ou reçu par le routeur.
5. **Message** — Ce champ inclut la transaction particulière sous la négociation.
6. **ID** — Ce champ est utilisé pour apparier et coordonner des messages de demande aux messages de réponse appropriés. Vous pouvez employer le champ d'ID pour associer une réponse avec un message entrant. Cette option est particulièrement utile quand le message entrant et la réponse sont éloignés dans la sortie de débogage.

7. **Longueur** — Le champ de longueur définit la longueur de la zone 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 de PPP, selon le but du message.

Remarque: Cet exemple montre les champs :

Sortie de debug ppp negotiation d'échantillon

C'est une description annotée de sortie de commande de **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 communs

Généralités

CONFREQ (Configurer-demande) :

Quand la couche inférieure devient disponible (), un CONFREQ est envoyé pour commencer la première phase de PPP (phase LCP). Il est utilisé en quelques phases LCP et de NCP comme tentative de configurer la connexion. Pour ouvrir une connexion au pair, le périphérique transmet ce message avec les options de configuration et évalue l'expéditeur souhaite le pair pour le prendre en charge. Toutes les options et valeurs sont négociées simultanément. Si le pair répond avec un message CONFREJ ou CONFNAK, alors le routeur envoie un autre CONFREQ avec un ensemble d'options ou des valeurs différent.

CONFACK (Configurer-reconnaissez) :

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

CONFREJ (configurez l'anomalie) :

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

CONFNAK (configurez la reconnaissance négative) :

Si l'option de configuration reçue est reconnaissable et acceptable, mais une certaine valeur n'est pas acceptable, le routeur transmet un message CONFNAK. Le routeur ajoute l'option et la valeur

qu'il peut recevoir dans le message CONFNAK de sorte que le pair puisse inclure cette option dans le prochain message CONFREQ.

ECHOREQ (requête d'écho) et ECHOREP (réponse d'écho) :

Le PPP emploie le Keepalives afin de mettre à jour l'intégrité de la connexion. Ce Keepalives est la trame ECHOREQ qui est envoyée au pair distant de PPP, et le pair distant de PPP devrait répondre avec une trame ECHOREP dès réception d'une trame ECHOREQ. Par défaut, si le routeur manque cinq trames ECHOREP, puis le lien est considéré vers le bas et le PPP est réduit.

TERMREQ (demande d'arrêt) :

Cette trame indique que le pair de PPP qui a envoyé cette trame termine la connexion PPP.

TERMACK (l'arrêt reconnaissent) :

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

TERMINAISON

Ce message indique que la connexion PPP a été réduite. Une connexion LCP ou de NCP peut être découpée :

- sur la fin administrative (LCP seulement).
- quand le niveau plus bas disparaît hors service (ligne commutée, le RNIS, et ainsi de suite).
- quand les négociations tombent.
- sur la ligne détection de boucle.

LCP

ACCM (table de caractères de contrôle asynchrone) :

C'est l'une des options LCP-négociées dans la trame CONFREQ. ACCM place les séquences d'échappement de caractère. ACCM indique le port ignorer les caractères de commande spécifiés dans le flux de données. Si le routeur à l'autre bout de la connexion ne prend en charge pas la négociation ACCM, le port est forcé pour utiliser FFFFFFFF. Dans ce cas, émettez cette commande :

```
ppp accm match 000a000
```

ACFC (compactage d'adresse et de champ de contrôle) :

ACFC est une option LCP qui permet à des points finaux pour l'envoyer message dans les deux sens plus efficacement.

AuthProto (authentification Protocol) :

AuthProto est le type de protocole d'authentification négocié dans la trame CONFREQ entre les

deux pairs de connexion PPP pour l'usage pendant la phase d'authentification. Si aucune authentification de PPP n'est configurée, cette sortie n'est pas vue dans des paramètres négociés par trame CONFREQ. Les valeurs possibles sont CHAP ou PAP.

Rappel « # » :

Ce message indique que l'option de rappel est sous la négociation. Le nombre après que la syntaxe de rappel indique quelle option de rappel est négociée. Le numéro 0 est rappel normal de PPP, alors que le numéro 6 indique l'option de rappel de service Microsoft (qui est automatiquement disponible dans la version de logiciel 11.3(2)T ou ultérieures de Cisco IOS®).

CHAP (authentification Protocol à échanges confirmés) :

Ce message indique que le protocole d'authentification sous la négociation est CHAP.

EndpointDisc (discriminateur de point final) :

C'est une option LCP utilisée pour identifier un pair de PPP dans la connexion de ppp multilink. Le pour en savoir plus, se rapportent à des critères pour nommer des ensembles Multilink PPP.

LCP : L'état est ouvert

Ce message indique que la négociation LCP a été terminée avec succès.

LQM (surveillance de qualité de lien)

LQM est disponible sur toutes les interfaces série qui exécutent le PPP. LQM surveille la qualité de lien et prend le lien vers le bas quand la qualité chute au-dessous d'un pourcentage configuré. Les pourcentages sont calculés pour les directions entrantes et sortantes. La qualité sortante est calculée par la comparaison du nombre total de paquets et d'octets envoyés avec le nombre total de paquets et d'octets reçus par le pair. La qualité entrante est calculée par la comparaison du nombre total de paquets et d'octets reçus avec le nombre total de paquets et d'octets envoyés par le pair.

Quand LQM est activé, des rapports qualité de lien (LQRs) sont envoyés chaque période de keepalive. LQRs sont envoyés au lieu du Keepalives. Tout le Keepalives entrant est répondu à correctement. Si LQM n'est pas configuré, le Keepalives est envoyé chaque période de keepalive, et tout le LQRs entrant sont répondus à avec un LQR.

MagicNumber

Le support de nombre magique est disponible sur toutes les interfaces série. De PPP les tentatives toujours de négocier pour les nombres magiques, qui sont utilisés pour les détecter ont fait une boucle-de retour des réseaux. Une chaîne aléatoire est envoyée à travers le lien et si la même valeur est retournée, alors le routeur détermine que le lien est fait une boucle - arrière.

Le lien pourrait ou ne pourrait pas être pris vers le bas sur la détection faite une boucle-de retour ; il dépend de l'utilisation de la commande de down-when-looped.

PAP (protocole d'identification de mot de passe)

Ce message indique que le protocole d'authentification sous la négociation à l'usage des pairs de PPP est PAP. Pour plus d'informations sur le PAP, référez-vous en configurant et dépannage du Password Authentication Protocol (PAP) de PPP.

PFC (compactage de champ de Protocol)

Cette option tourne le compactage pour le protocole met en place l'un ou l'autre "Marche/Arrêt".

MRRU (maximum recevez l'unité reconstruite)

C'est une option LCP négociée en cours d'installation du ppp multilink LCP. Cette option détermine le nombre maximal d'octets qui peut constituer une trame. Si MRRU n'est pas négocié dans LCP, alors le PPP à liaisons multiples (MPPP) ne peut pas fonctionner sur le lien.

MRU (unité reçue par maximum)

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

Authentification

AUTHENTIC-REQ (demande d'authentification)

Cette trame est envoyée du pair local de PPP (sur quelle authentification est activée) au pair distant. Il demande au pair distant d'envoyer un nom d'utilisateur valide et un mot de passe pour l'authentification de connexion PPP. Cette trame est utilisée seulement avec le PAP.

AUTHENTIC-ACK (l'authentification reconnaissent)

Cette trame est envoyée du pair authentifié de PPP au pair authentifiant de PPP. Cette trame porte les paires de nom d'utilisateur valide et de mot de passe. Cette trame est utilisée seulement quand le PAP est utilisé pour l'authentification de connexion PPP.

AUTHENTIC-NAK ou PANNE

Cette trame est envoyée du pair authentifiant de PPP quand l'échec de l'authentification sur le pair authentifiant de PPP.

DÉFI

C'est la trame de défi de CHAP qui est envoyée du pair authentifiant de PPP au pair authentifié de PPP. La trame de défi se compose d'un ID, un nombre aléatoire, et le nom d'hôte du serveur de communication local ou le nom d'utilisateur sur le périphérique distant. Cette trame est utilisée seulement quand le CHAP est utilisé pour l'authentification de connexion PPP.

RÉPONSE

Cette trame est la réponse de CHAP envoyée du pair authentifié de PPP au pair authentifiant de PPP.

La réponse exigée se compose de deux parts :

- Un résultat d'informations parasites de MD5 du secret partagé.
- Le nom d'hôte du périphérique distant ou le nom d'utilisateur sur le périphérique distant.

Cette trame est utilisée seulement quand le CHAP est utilisé pour l'authentification de connexion PPP.

NCP

Adresse a.b.c.d

- Sur un message sortant CONFREQ, cette valeur indique que l'adresse IP que le routeur local souhaite l'utiliser. Si l'adresse incluse est 0.0.0.0, l'ordinateur local invite le pair au fournir une adresse IP qu'il peut l'utiliser.
- Sur un message entrant CONFREQ, cette valeur indique que l'adresse IP que le pair souhaite l'utiliser. Si l'adresse incluse est 0.0.0.0, le pair invite l'ordinateur local pour le fournir une adresse IP qu'il peut l'utiliser.
- Sur un message sortant CONFNAK, cette valeur indique que l'adresse IP que le pair devrait l'utiliser plutôt que celui le pair a suggéré dans le message CONFREQ.
- Sur un message entrant CONFNAK, cette valeur indique que l'adresse IP que l'ordinateur local devrait l'utiliser, au lieu de celui il a suggéré dans le message précédent CONFREQ.
- Sur un message sortant CONFACK, cette valeur indique que l'adresse IP demandée par le pair semble acceptable à l'ordinateur local.
- Sur un message entrant CONFACK, cette valeur indique que l'adresse IP demandée par l'ordinateur local semble acceptable au pair.

CCP (Control Protocol de compactage)

Ce message indique qu'un protocole de compression est sous la négociation entre les deux pairs de PPP. Supports logiciels de Cisco IOS ces protocoles de compression à négocier au-dessus d'une connexion PPP :

- Compactage Ms Point à point (MS-PPC)
- stacker
- predictor

CDPCP (Control Protocol de Cisco Discovery Protocol)

Ce message indique que la négociation de CDP se produit pendant la phase de NCP. Pour arrêter le CDP sur le routeur, n'émettez l'**aucune** commande de **cdp run**.

CODEREJ (anomalie de code)

Un paquet CODEREJ est envoyé dès réception d'un ininterprétable emballé du pair distant de PPP.

Installez l'artère sur a.b.c.d

Quand le routeur termine IPCP (phase de NCP pour le protocole IP L3), il doit installer l'adresse IP donnée au pair distant de PPP dans la table de routage et voir comme route connectée dans la table de routage. Si vous ne voyez pas ce message, vérifiez que l'**aucune** commande de voisin-**artère de pair** n'est configurée.

IPCP (protocole de contrôle IP)

Cette valeur indique que l'IP est la couche réseau sous la négociation pendant la phase de NCP.

L'état IPCP est ouvert

Ce message indique que l'IPCP (phase de NCP pour le protocole IP L3) a été terminé avec succès.

PROTREJ (anomalie de Protocol)

Le pair de PPP, dès réception d'un paquet PPP avec un champ inconnu de protocole, emploie le message PROTREJ pour indiquer que le pair a tenté d'utiliser un protocole qui est non vérifié. Quand un périphérique de PPP reçoit un message PROTREJ, il doit le plus tôt possible cesser 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