Debugging-PPP-Aushandlung

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[Phasen der PPP-Verhandlungen](#)
[PPP-Verhandlungspakete: Eine Beschreibung](#)
[LCP, Authentifizierung und NCP-Phase](#)
[Fehlerbehebung mit Debug-ppp-Aushandlung - Ausgabe](#)
[Lesen der Debug-ppp-Aushandlung](#)
[Beispielausgabe für Debug-ppp-Aushandlung](#)
[Glossar und allgemeine Meldungen](#)
[Allgemeines](#)
[LCP](#)
[Authentifizierung](#)
[NCP](#)
[Zugehörige Informationen](#)

Einführung

In Dial-Anwendungen ist PPP der am häufigsten verwendete Kapselungstyp. PPP ermöglicht es zwei Systemen auf einer Punkt-zu-Punkt-Kommunikationsverbindung, verschiedene Parameter für Authentifizierung, Komprimierung und die Layer-3-Protokolle (L3) auszuhandeln, z. B. IP. Ein Ausfall der PPP-Aushandlung zwischen zwei Routern führt zum Ausfall der Verbindung.

Mit dem Befehl **debug ppp negotiation** können Sie die PPP-Verhandlungstransaktionen anzeigen, das Problem oder die Phase bei Auftreten des Fehlers identifizieren und eine Lösung entwickeln. Es ist jedoch zwingend erforderlich, dass Sie die Befehlsausgabe des Befehls **debug ppp negotiation** verstehen. Dieses Dokument stellt eine umfassende Methode zum Lesen der Befehlsausgabe des **Debug-ppp-Aushandlungs-**Befehls bereit.

Voraussetzungen

Anforderungen

Leser dieses Dokuments müssen sicherstellen, dass folgende Bedingungen erfüllt sind:

- PPP muss auf den Schnittstellen auf beiden Routern aktiviert sein. Geben Sie den Befehl **encapsulation ppp** aus, um dies zu erreichen.

- Geben Sie diesen Befehl ein, um Millisekunde-Zeitstempel auf dem Router zu aktivieren:
  `Router(config)# service timestamp debug datetime msec`

  Weitere Informationen zu Debugbefehlen finden Sie unter Wichtige Informationen über Debugbefehle.

Hinweis: Die PPP-Aushandlung zwischen zwei Peers kann erst beginnen, wenn die untere Ebene (ISDN, physische Schnittstelle, Einwahlverbindung usw.) unter PPP einwandfrei funktioniert. Wenn Sie beispielsweise PPP über ISDN ausführen möchten, müssen alle ISDN-Ebenen aktiv sein. Andernfalls startet PPP nicht.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Phasen der PPP-Verhandlungen

Die Verbindung durchläuft mehrere Phasen der PPP-Aushandlung (siehe Tabelle). Das Endergebnis ist, dass PPP entweder aktiviert oder deaktiviert ist.

Phase	Beschreibung
HERUNTERFAHREN	In dieser Phase ist PPP ausgefallen. Diese Meldung wird angezeigt, nachdem der Link und PPP vollständig deaktiviert wurden: `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
EINRICHTUNG	PPP wechselt zu dieser Phase, wenn ein Hinweis darauf eingeht, dass die physische Schicht einsatzbereit ist. LCP[1] wird in dieser Phase ausgehandelt. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTHENTIFIZIERUNG	Wenn eine PPP-Authentifizierung (CHAP[2] oder PAP[3]) für die Verbindung gewünscht ist, wechselt PPP zu dieser Phase. Beachten Sie, dass die PPP-Authentifizierung optional ist. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
UP	Sobald die Authentifizierung abgeschlossen ist, wechselt PPP in die UP-Phase. In dieser Phase erfolgt die NCP[4]-Aushandlung. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
BEENDEN	In dieser Phase wird PPP heruntergefahren. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

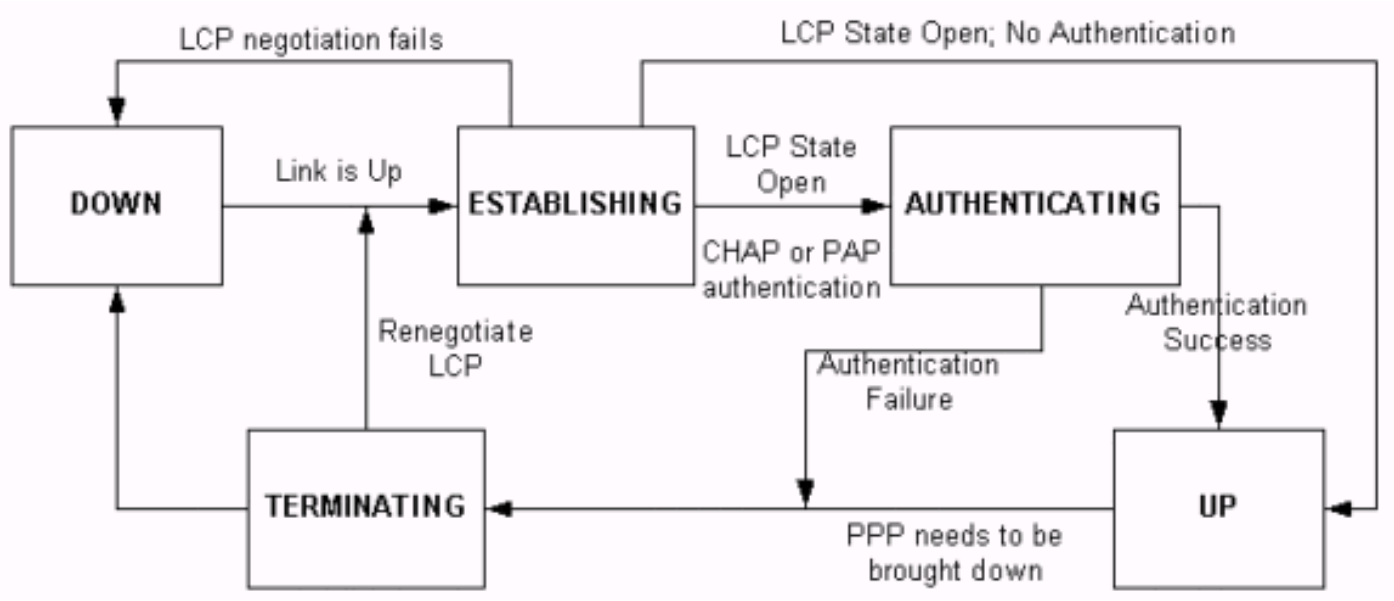
1. LCP = Link Control Protocol

2. CHAP = Challenge Handshake Authentication Protocol

3. PAP = Password Authentication Protocol

4. NCP = Network Control Protocol

Dieses Diagramm zeigt die PPP-Phasenübergänge:



PPP-Verhandlungspakete: Eine Beschreibung

Diese Tabelle enthält eine Beschreibung der PPP-Verhandlungspakete, die sowohl bei der LCP- als auch bei der NCP-Aushandlung verwendet werden:

Paket	Code	Beschreibung
KONFREQUENZ	Konfigurationsanforderung	Um eine Verbindung zum Peer zu öffnen, überträgt das Gerät diese Nachricht zusammen mit den Konfigurationsoptionen und Werten, die der Absender vom Peer unterstützen möchte. Alle Optionen und Werte werden gleichzeitig ausgehandelt. Wenn der Peer mit einer CONFREJ- oder CONFNAK-Nachricht antwortet, sendet der Router eine weitere CONFREQ-Nachricht mit einem anderen Satz von Optionen oder Werten.
KONFREI	Konfigurieren-Ablehnen	Wenn eine in der CONFREQ-Nachricht erhaltene Konfigurationsoption nicht akzeptabel oder nicht erkennbar ist, antwortet der Router mit einer CONFREJ-Nachricht. Die

		inakzeptable Option (aus der CONFREQ Nachricht) ist in der CONFREJ Nachricht enthalten.
KONFNATION	Konfigurieren - NAK[1]	Wenn die empfangene Konfigurationsoption erkennbar und akzeptabel ist, aber ein gewisser Wert nicht akzeptabel ist, sendet der Router eine CONFNAK-Nachricht. Der Router fügt die Option und den Wert, die er in der CONFNAK-Nachricht akzeptieren kann, an, sodass der Peer diese Option in die nächste CONFREQ-Nachricht aufnehmen kann.
KONFACK	Konfigurieren - ACK[2]	Wenn alle Optionen in der CONFREQ-Nachricht erkennbar sind und alle Werte akzeptiert werden können, sendet der Router eine CONFACK-Nachricht.
TERMREQ	Anfrage beenden	Diese Meldung wird verwendet, um einen LCP-Abschluss zu initiieren.
TERMACK	ACK beenden	Diese Nachricht wird als Antwort auf die TERMREQ-Nachricht übertragen.

1. NAK = Negatives Bestätigung

2. ACK = Bestätigen

Hinweis: Jeder Peer kann CONFREQs mit der Option oder dem Wert senden, die der Peer unterstützen soll. Dies kann dazu führen, dass sich die in jeder Richtung ausgehandelten Optionen unterscheiden. Eine Seite möchte beispielsweise den Peer authentifizieren, die andere nicht.

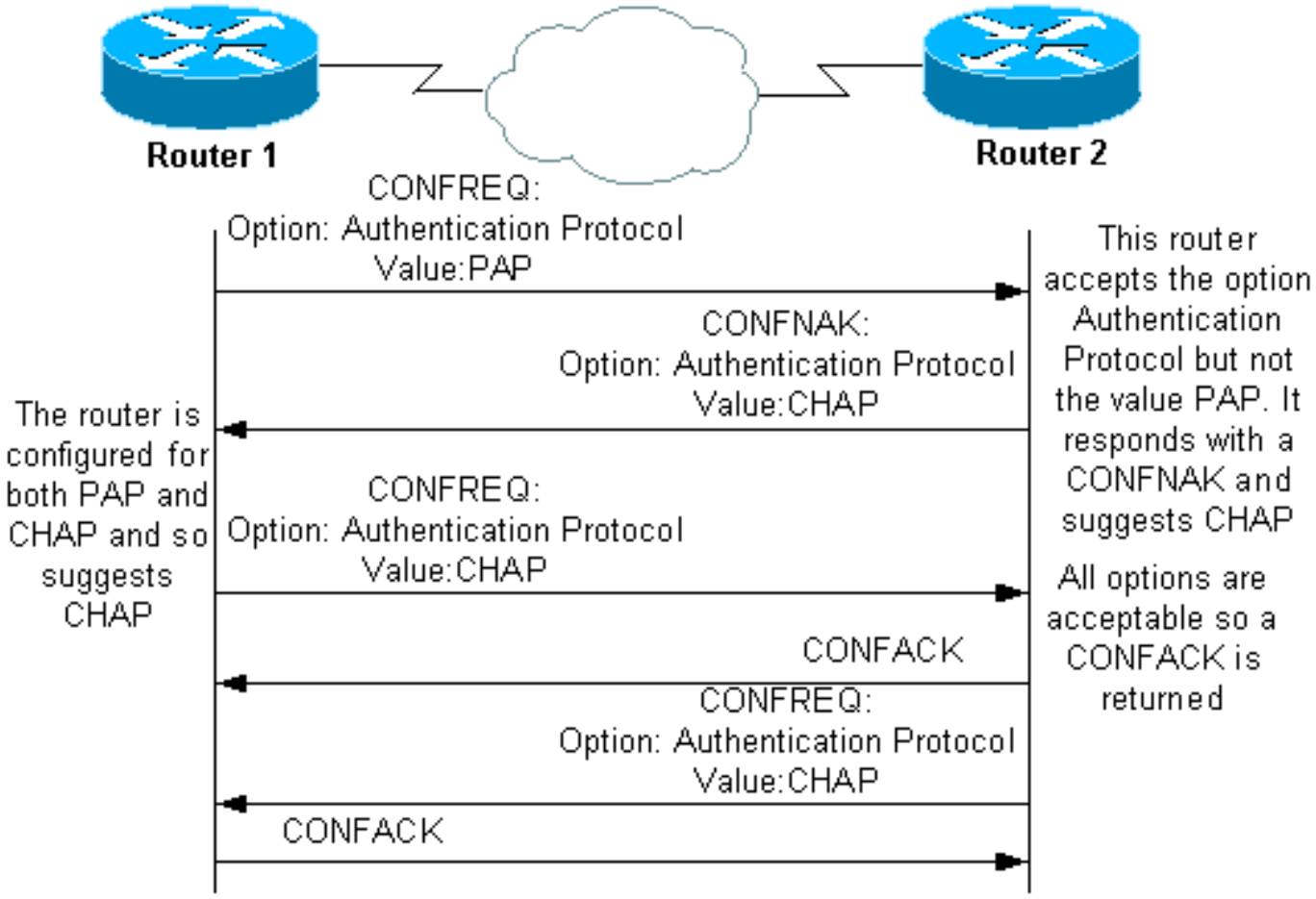
LCP, Authentifizierung und NCP-Phase

In einigen der zuvor beschriebenen PPP-Phasen wird PPP auch in spezifische Phasen wie LCP-Aushandlung, Authentifizierung und NCP-Aushandlung integriert. Weitere Informationen finden Sie unter RFC 1548 und RFC 1661 .

LCP (obligatorische Phase)

LCP ist eine Phase, in der Parameter für die Einrichtung, Konfiguration und das Testen der Datenverbindungsverbindung ausgehandelt werden. Ein offener LCP-Status bedeutet, dass das LCP erfolgreich abgeschlossen wurde, während ein geschlossener LCP-Zustand auf einen LCP-Fehler hinweist.

Dieses Diagramm zeigt eine konzeptionelle Ansicht eines LCP-Handshake:



Die LCP-Aushandlung verwendet auch einen Parameter namens MagicNumber, der verwendet wird, um zu bestimmen, ob die Verbindung zurückschleift. Eine zufällige Zeichenfolge wird über die Verbindung gesendet, und wenn der gleiche Wert zurückgegeben wird, bestimmt der Router, dass die Verbindung zurückgeschleift wird.

Authentifizierung (optionale Phase in der Standardeinstellung)

In dieser Phase wird die Authentifizierung mit dem in der LCP-Aushandlung vereinbarten Authentifizierungsprotokoll (CHAP oder PAP) durchgeführt. Informationen zu PAPs finden Sie unter Konfigurieren und Beheben von Problemen mit dem PPP Password Authentication Protocol (PAP).

Informationen zu CHAPs finden Sie unter Grundlagen und Konfigurieren der PPP CHAP-Authentifizierung.

Hinweis: Die Authentifizierung ist optional, und PPP tritt nur dann in diese Phase ein, wenn eine Authentifizierung erforderlich ist.

NCP (obligatorische Phase)

In dieser Phase werden verschiedene Protokolle auf Netzwerkebene eingerichtet und konfiguriert. Das häufigste ausgehandelte L3-Protokoll ist IP. Die Router tauschen IP Control Protocol (IPCP)-Nachrichten aus, um protokollspezifische Optionen auszuhandeln (in diesem Beispiel IP).

Laut RFC 1332 handelt IPCP zwei Optionen aus: Komprimierung und IP-Adressenzuweisungen. IPCP wird jedoch auch verwendet, um netzwerkbezogene Informationen wie primäre und Backup-

Windows Name Service (WINS)- und Domain Name System (DNS)-Server zu übergeben.

Die Aushandlung findet mit der Verwendung von CONF-Meldungen statt, wie in den PPP-Verhandlungspaketen beschrieben: Ein Abschnitt Beschreibung dieses Dokuments.

Fehlerbehebung mit Debug-ppp-Aushandlung - Ausgabe

Wenn Sie die Befehlsausgabe für die **Debug-ppp-Aushandlung** zur Fehlerbehebung lesen, befolgen Sie die folgenden Anweisungen:

1. Identifizieren Sie die Phasenübergänge in der **Debug-**Befehlsausgabe. Bestimmen Sie die restliche Verbindungsphase, z. B. UP oder AUTHENTICATION. So können Sie die Phase identifizieren, in der die Verbindung fehlschlug. Weitere Informationen zu den Phasen finden Sie im Abschnitt Phasen der PPP-Verhandlungen.
2. Suchen Sie in der Fehlerphase nach Meldungen, die darauf hinweisen, dass LCP, Authentifizierung oder NCP (falls zutreffend) erfolgreich ist:Der LCP-Status sollte offen sein. Sie können auch die letzten ein- und ausgehenden CONFACK-Nachrichten ansehen, um zu überprüfen, ob die von Ihnen benötigten Parameter ausgehandelt wurden.Die Authentifizierung sollte erfolgreich sein. Wenn Sie eine Zwei-Wege-Authentifizierung verwenden, muss jede Transaktion erfolgreich sein. Weitere Informationen zur Behebung von Fehlern bei der PPP-Authentifizierung finden Sie unter Fehlerbehebung bei der PPP-Authentifizierung (CHAP oder PAP).Der IPCP-Status sollte offen sein. Überprüfen Sie, ob die Adressierung korrekt ist und eine Route zum Peer installiert ist.

Lesen der Debug-ppp-Aushandlung

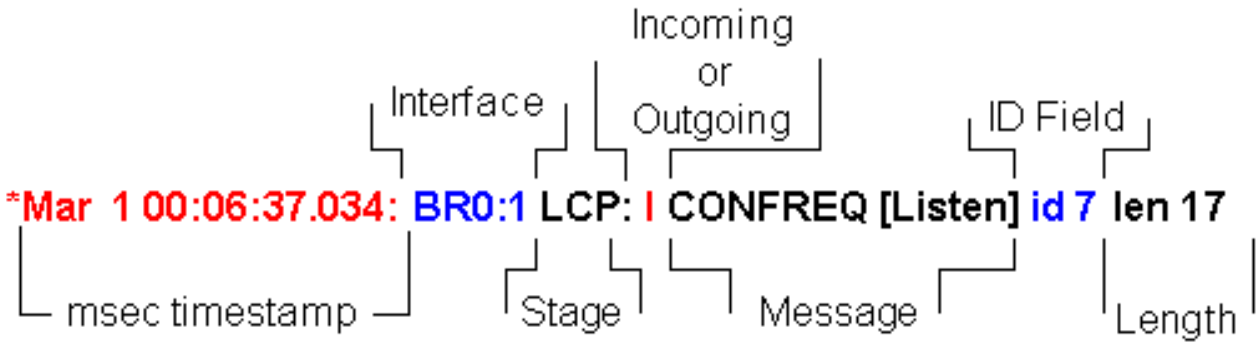
Die meisten Zeilen in der Befehlsausgabe für **Debug-ppp-Aushandlung** zeichnen sich durch Folgendes aus:

1. **Zeitstempel** - Millisekunden-Zeitstempel sind nützlich. Weitere Informationen finden Sie im Abschnitt Voraussetzungen dieses Dokuments.
2. **Schnittstellen- und Schnittstellennummer** - Dieses Feld ist nützlich, wenn Debugverbindungen mehrere Verbindungen verwenden oder wenn die Verbindung über mehrere Schnittstellen übertragen wird. So werden beispielsweise bestimmte Verbindungen (z. B. Multilink-Anrufe) anfangs von der physischen Schnittstelle gesteuert, später jedoch von der Dialer-Schnittstelle oder der Virtual-Access-Schnittstelle gesteuert.
3. **Type of PPP message (Typ der PPP-Nachricht)**: Dieses Feld gibt an, ob es sich bei der Leitung um eine allgemeine PPP-, LCP-, CHAP-, PAP- oder IPCP-Nachricht handelt.
4. **Richtung der Nachricht** - Eine **I** gibt ein eingehendes Paket an, und ein **O** zeigt ein ausgehendes Paket an. Dieses Feld kann verwendet werden, um festzustellen, ob die Nachricht vom Router generiert oder empfangen wurde.
5. **Message** (**Nachricht**): Dieses Feld enthält die Transaktion, die verhandelt wird.
6. **ID** - Dieses Feld wird verwendet, um Anforderungsnachrichten den entsprechenden Antwortnachrichten zuzuordnen und zu koordinieren. Sie können das ID-Feld verwenden, um eine Antwort einer eingehenden Nachricht zuzuordnen. Diese Option ist besonders nützlich, wenn die eingehende Nachricht und die Antwort in der Debugausgabe weit voneinander entfernt sind.

7. **Length** (Länge): Das Längenfeld definiert die Länge des Informationsfelds. Dieses Feld ist für die allgemeine Fehlerbehebung nicht wichtig.

Hinweis: Die Felder 4 bis 7 werden je nach Zweck der Nachricht möglicherweise nicht in allen PPP-Nachrichten angezeigt.

Hinweis: In diesem Beispiel werden die Felder veranschaulicht:



Beispielausgabe für Debug-ppp-Aushandlung

Dies ist eine kommentierte Beschreibung der Befehlsausgabe des **Debug-ppp**-Befehls:

```
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

Glossar und allgemeine Meldungen

Allgemeines

CONFREQ (Configure-Request):

Wenn die untere Ebene verfügbar ist (Up), wird ein CONFREQ gesendet, um die erste PPP-Phase (LCP-Phase) zu starten. Sie wird in den LCP- und NCP-Phasen als Versuch verwendet, die Verbindung zu konfigurieren. Um eine Verbindung zum Peer zu öffnen, überträgt das Gerät diese Nachricht zusammen mit den Konfigurationsoptionen und Werten, die der Absender vom Peer unterstützen möchte. Alle Optionen und Werte werden gleichzeitig ausgehandelt. Wenn der Peer mit einer CONFREJ- oder CONFNAK-Nachricht antwortet, sendet der Router eine weitere CONFREQ-Nachricht mit einem anderen Satz von Optionen oder Werten.

KONFACK (Configure-Acknowley):

Wenn alle Optionen in der CONFREQ-Nachricht erkennbar sind und alle Werte akzeptiert werden können, sendet der Router eine CONFACK-Nachricht.

CONFREJ (Configure Reject):

Wenn eine in der CONFREQ erhaltene Konfigurationsoption nicht akzeptabel oder nicht erkennbar ist, antwortet der Router mit einer CONFREJ-Nachricht. Die inakzeptable Option (aus der CONFREQ) ist in der CONFREJ Nachricht enthalten.

CONFNAK (Negative Bestätigung konfigurieren):

Wenn die empfangene Konfigurationsoption erkennbar und akzeptabel ist, aber ein gewisser Wert nicht akzeptabel ist, sendet der Router eine CONFNAK-Nachricht. Der Router fügt die Option und den Wert, die er in der CONFNAK-Nachricht akzeptieren kann, an, sodass der Peer diese Option in die nächste CONFREQ-Nachricht aufnehmen kann.

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

PPP verwendet Keepalives, um die Integrität der Verbindung aufrechtzuerhalten. Diese Keepalives sind der ECHOREQ-Frame, der an einen Remote-PPP-Peer gesendet wird, und der Remote-PPP-Peer sollte nach Erhalt eines ECHOREQ-Frames mit einem ECHOREP-Frame antworten. Wenn der Router fünf ECHOREP-Frames verpasst, wird die Verbindung standardmäßig als inaktiv angesehen und PPP wird deaktiviert.

TERMREQ (Terminierungsanfrage):

Dieser Frame gibt an, dass der PPP-Peer, der diesen Frame gesendet hat, die PPP-Verbindung beendet.

TERMACK (Kündigungsbestätigung):

Diese Nachricht wird als Antwort auf die TERMREQ-Nachricht übertragen. Dadurch wird die PPP-Verbindung geschlossen.

BEENDEN

Diese Meldung weist darauf hin, dass die PPP-Verbindung abgebrochen wurde. Eine LCP- oder

NCP-Verbindung kann unterbrochen werden:

- auf administrativem Schließen (nur LCP).
- wenn die untere Servicestufe ausfällt (Einwahlverbindung, ISDN usw.).
- wenn Verhandlungen abgeschlossen werden.
- Online-Loop-Erkennung.

LCP

ACCM (Asynchronous Control Character Map):

Dies ist eine der LCP-Negotiated-Optionen im CONFREQ Frame. ACCM legt die Escapesequenzen für Zeichen fest. ACCM weist den Port an, bestimmte Kontrollzeichen im Datenstrom zu ignorieren. Wenn der Router am anderen Ende der Verbindung keine ACCM-Aushandlung unterstützt, ist der Port gezwungen, FFFFFFFF zu verwenden. Führen Sie in diesem Fall den folgenden Befehl aus:

```
ppp accm match 000a000
```

ACFC (Address and Control Field Compression):

ACFC ist eine LCP-Option, mit der Endpunkte Nachrichten effizienter hin und her senden können.

AuthProto (Authentifizierungsprotokoll):

AuthProto ist der Authentifizierungsprotokolltyp, der im CONFREQ Frame zwischen beiden PPP-Verbindungspersonen ausgehandelt wird und in der Authentifizierungsphase verwendet werden kann. Wenn keine PPP-Authentifizierung konfiguriert ist, wird diese Ausgabe nicht in den CONFREQ Frame Negotiated-Parametern angezeigt. Mögliche Werte sind CHAP oder PAP.

Rückruf "#":

Diese Meldung weist darauf hin, dass die Rückrufoption ausgehandelt wird. Die Zahl nach der Rückrufsyntax gibt an, welche Rückrufoption ausgehandelt wird. Die Zahl 0 ist ein normaler PPP-Rückruf, die Zahl 6 steht für die Microsoft-Rückrufoption (die automatisch in Cisco IOS® Software Release 11.3(2)T oder höher verfügbar ist).

CHAP (Challenge Handshake Authentication Protocol):

Diese Meldung weist darauf hin, dass das Authentifizierungsprotokoll, über das verhandelt wird, CHAP ist.

EndpointDisc (Endpunkt-Diskriminierung):

Diese LCP-Option wird verwendet, um einen PPP-Peer in einer PPP-Multilink-Verbindung zu identifizieren. Weitere Informationen finden Sie unter Kriterien für die Benennung von Multilink PPP-Paketen.

LCP: Staat ist offen

Diese Meldung weist darauf hin, dass die LCP-Aushandlung erfolgreich abgeschlossen wurde.

LQM (Überwachung der Verbindungsqualität)

LQM ist auf allen seriellen Schnittstellen verfügbar, auf denen PPP ausgeführt wird. LQM überwacht die Verbindungsqualität und reduziert die Verbindung, wenn die Qualität unter einen konfigurierten Prozentsatz fällt. Die Prozentsätze werden sowohl für die eingehende als auch die ausgehende Richtung berechnet. Die Ausgangsqualität wird durch einen Vergleich der Gesamtzahl der gesendeten Pakete und Bytes mit der Gesamtzahl der Pakete und Bytes berechnet, die vom Peer empfangen wurden. Die eingehende Qualität wird durch einen Vergleich der Gesamtzahl der empfangenen Pakete und Bytes mit der Gesamtzahl der vom Peer gesendeten Pakete und Bytes berechnet.

Wenn LQM aktiviert ist, werden Link Quality Reports (LQRs) über jeden Keepalive-Zeitraum gesendet. LQR werden anstelle von Keepalives gesendet. Alle eingehenden Keepalives werden ordnungsgemäß beantwortet. Wenn LQM nicht konfiguriert ist, werden Keepalives für jeden Keepalive-Zeitraum gesendet, und alle eingehenden LQRs werden mit einem LQR beantwortet.

MagicNumber

Magic Number-Unterstützung ist auf allen seriellen Schnittstellen verfügbar. PPP versucht immer, für Magic Numbers zu verhandeln, die zum Erkennen von Looped-Back-Netzwerken verwendet werden. Eine zufällige Zeichenfolge wird über die Verbindung gesendet. Wenn der gleiche Wert zurückgegeben wird, legt der Router fest, dass die Verbindung zurückgeschleift wird.

Die Verbindung wird bei der Looped-Back-Erkennung möglicherweise deaktiviert. Es hängt von der Verwendung des **Befehls** Down-when-Looped ab.

PAP (Password Authentication Protocol)

Diese Meldung weist darauf hin, dass das Authentifizierungsprotokoll, über das verhandelt wird, für PPP-Peers verwendet wird, PAP ist. Weitere Informationen zu PAP finden Sie unter Konfigurieren und Fehlerbehebung für PPP Password Authentication Protocol (PAP).

PFC (Protokollfeldkomprimierung)

Mit dieser Option wird die Komprimierung für die Protokollfelder entweder ein- oder ausgeschaltet.

MRRU (Max. rekonstruierte Empfangseinheit)

Dies ist eine LCP-Option, die im Prozess der PPP-Einrichtung für Multilink-LCP ausgehandelt wird. Diese Option legt die maximale Anzahl von Bytes fest, die einen Frame bilden können. Wenn in LCP kein MRRU ausgehandelt wird, kann Multilink PPP (MPPP) für die Verbindung nicht ausgeführt werden.

MRU (Maximum Received Unit)

MRU ist eine im CONFREQ-Frame ausgehandelte LCP-Option zur Aushandlung der Größe der ausgetauschten Pakete.

Authentifizierung

AUTH-REQ (Authentifizierungsanfrage)

Dieser Frame wird vom lokalen PPP-Peer (auf dem die Authentifizierung aktiviert ist) an den Remote-Peer gesendet. Der Remote-Peer wird aufgefordert, einen gültigen Benutzernamen und ein gültiges Kennwort für die Authentifizierung der PPP-Verbindung zu senden. Dieser Frame wird nur mit PAP verwendet.

AUTH-ACK (Authentifizierungsbestätigung)

Dieser Frame wird vom authentifizierten PPP-Peer an den authentifizierenden PPP-Peer gesendet. Dieser Frame enthält das gültige Benutzername- und Kennwortpaar. Dieser Frame wird nur verwendet, wenn PAP für die PPP-Verbindungsauthentifizierung verwendet wird.

AUTH-NAK oder FEHLER

Dieser Frame wird vom authentifizierenden PPP-Peer gesendet, wenn die Authentifizierung auf dem authentifizierenden PPP-Peer fehlgeschlagen ist.

HERAUSFORDERUNG

Dies ist der CHAP-Challenge-Frame, der vom authentifizierenden PPP-Peer an den authentifizierten PPP-Peer gesendet wird. Der Challenge-Frame besteht aus einer ID, einer zufälligen Nummer und entweder dem Hostnamen des lokalen Kommunikationsservers oder dem Namen des Benutzers auf dem Remote-Gerät. Dieser Frame wird nur verwendet, wenn CHAP für die PPP-Verbindungsauthentifizierung verwendet wird.

ANTWORT

Dieser Frame ist die CHAP-Antwort, die vom authentifizierten PPP-Peer an den authentifizierenden PPP-Peer gesendet wird.

Die erforderliche Antwort besteht aus zwei Teilen:

- Eine MD5-Hashausgabe des freigegebenen geheimen Codes.
- Entweder der Hostname des Remote-Geräts oder der Name des Benutzers auf dem Remote-Gerät.

Dieser Frame wird nur verwendet, wenn CHAP für die PPP-Verbindungsauthentifizierung verwendet wird.

NCP

Adresse a.b.c.d

- Bei einer ausgehenden CONFREQ-Nachricht gibt dieser Wert die IP-Adresse an, die der lokale Router verwenden möchte. Wenn die angegebene Adresse 0.0.0.0 lautet, fordert der lokale Computer den Peer auf, ihm eine IP-Adresse zur Verfügung zu stellen, die er verwenden kann.
- Bei einer eingehenden CONFREQ-Nachricht gibt dieser Wert die IP-Adresse an, die der Peer verwenden möchte. Wenn die angegebene Adresse 0.0.0.0 lautet, fordert der Peer den lokalen Computer auf, ihm eine IP-Adresse zur Verfügung zu stellen, die er verwenden kann.
- Bei einer ausgehenden CONFNAK-Nachricht gibt dieser Wert die IP-Adresse an, die der Peer verwenden sollte, und nicht die IP-Adresse, die der Peer in der CONFREQ-Nachricht vorgeschlagen hat.
- Bei einer eingehenden CONFNAK-Nachricht gibt dieser Wert die IP-Adresse an, die der lokale Computer verwenden soll, und nicht die IP-Adresse, die in der vorherigen CONFREQ-Nachricht vorgeschlagen wurde.
- Bei einer ausgehenden CONFACK-Nachricht gibt dieser Wert an, dass die vom Peer angeforderte IP-Adresse für den lokalen Computer zulässig ist.
- Bei einer eingehenden CONFACK-Nachricht gibt dieser Wert an, dass die vom lokalen Computer angeforderte IP-Adresse für den Peer akzeptabel ist.

CCP (Compression Control Protocol)

Diese Meldung weist darauf hin, dass ein Komprimierungsprotokoll zwischen beiden PPP-Peers ausgehandelt wird. Die Cisco IOS-Software unterstützt diese Komprimierungsprotokolle, die über eine PPP-Verbindung ausgehandelt werden:

- MS-Point-to-Point-Komprimierung (MS-PPC)
- Stacker
- Vorhersager

CDPCP (Cisco Discovery Protocol Control Protocol)

Diese Meldung weist darauf hin, dass die CDP-Aushandlung in der NCP-Phase stattfindet. Führen Sie den Befehl **no cdp run** aus, um CDP auf dem Router zu deaktivieren.

CODEREJ (Code Reject)

Ein CODEREJ-Paket wird nach Erhalt eines uninterpretierbaren Pakets vom Remote-PPP-Peer gesendet.

Installation der Route zu a.b.c.d

Wenn der Router die IPCP-Phase (NCP-Phase für IP-L3-Protokoll) beendet, muss er die angegebene IP-Adresse für den Remote-PPP-Peer in der Routing-Tabelle installieren und in der Routing-Tabelle als verbundene Route angesehen werden. Wenn Sie diese Meldung nicht sehen, stellen Sie sicher, dass der Befehl **no peer neighbor-route** nicht konfiguriert ist.

IPCP (IP Control Protocol)

Dieser Wert gibt an, dass IP die Netzwerkschicht ist, die in der NCP-Phase ausgehandelt wird.

Der IPCP-Status ist offen.

Diese Meldung weist darauf hin, dass die IPCP-Phase (NCP-Phase für IP-L3-Protokoll) erfolgreich abgeschlossen wurde.

PROTREJ (Protokoll-Ablehnung)

Der PPP-Peer gibt nach Erhalt eines PPP-Pakets mit einem unbekannten Protokollfeld mithilfe der PROTREJ-Nachricht an, dass der Peer versucht hat, ein Protokoll zu verwenden, das nicht unterstützt wird. Wenn ein PPP-Gerät eine PROTREJ-Nachricht empfängt, muss es so bald wie möglich die Übermittlung von Paketen des angegebenen Protokolls einstellen.

Zugehörige Informationen

- Konfiguration und Fehlerbehebung für PPP Password Authentication Protocol (PAP)
- PPP-Authentifizierung mit dem PPP-chap-Hostnamen und den ppp-Authentifizierungschap-Callin-Befehlen
- PPP CHAP-Authentifizierung verstehen und konfigurieren
- Fehlerbehebung Authentifizierung nach PPP (CHAP oder PAP)
- Support-Seiten für Wähltechnologie
- Technischer Support - Cisco Systems