Informazioni sull'output del comando debug ppp negotiation

Sommario

Introduzione

Nelle applicazioni relative alle chiamate, il tipo di incapsulamento più comunemente usato è PPP. Il protocollo PPP consente a due computer su un collegamento di comunicazione point-to-point di negoziare vari parametri per l'autenticazione, la compressione e i protocolli di layer 3 (L3), ad esempio IP. Un errore nella negoziazione PPP tra due router determina il mancato completamento della connessione.

Il comando **debug ppp negotiation** consente di visualizzare le transazioni di negoziazione PPP, identificare il problema o la fase in cui si verifica l'errore e sviluppare una risoluzione. Tuttavia, è essenziale comprendere l'output del comando **debug ppp negotiation**. In questo documento viene illustrato un metodo completo per leggere l'output del comando di **negoziazione PPP per il debug**.

Prerequisiti

Requisiti

I lettori di questo documento devono assicurarsi che queste condizioni siano soddisfatte:

- Il protocollo PPP deve essere abilitato sulle interfacce di entrambi i router. A tale scopo, eseguire il comando **encapsulation ppp**.
- Utilizzare questo comando per abilitare i timestamp in millisecondi sul router:
  `Router(config)# service timestamp debug datetime msec`

  Per ulteriori informazioni sui comandi di debug, vedere Informazioni importanti sui comandi di debug.

Nota: la negoziazione PPP tra due peer non può iniziare a meno che il layer inferiore (ISDN, interfaccia fisica, linea remota e così via) non funzioni perfettamente in PPP. Ad esempio, se si desidera eseguire il protocollo PPP su ISDN, tutti i livelli ISDN devono essere attivi; in caso contrario il protocollo PPP non viene avviato.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Fasi della negoziazione PPP

Il collegamento passa attraverso diverse fasi del processo di negoziazione PPP, come illustrato nella tabella seguente. Il risultato finale è che il PPP è attivo o inattivo.

Fase	Descrizione
GIÙ	In questa fase, il PPP è inattivo. Questo messaggio viene visualizzato dopo che il collegamento e il protocollo PPP sono stati interrotti: `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
CREAZIONE	Il PPP passa a questa fase quando riceve un'indicazione che il livello fisico è attivo e pronto per essere utilizzato. In questa fase viene eseguita la negoziazione LCP[1]. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTENTICAZIONE	Se si desidera l'autenticazione PPP (CHAP[2] o PAP[3]) sul collegamento, PPP passa a questa fase. Tenere presente che l'autenticazione PPP è facoltativa. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
SU	Al termine dell'autenticazione, il PPP passa alla fase UP. In questa fase viene eseguita la negoziazione di NCP[4]. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMIN	In questa fase, il protocollo PPP viene

AZIONE	arrestato. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

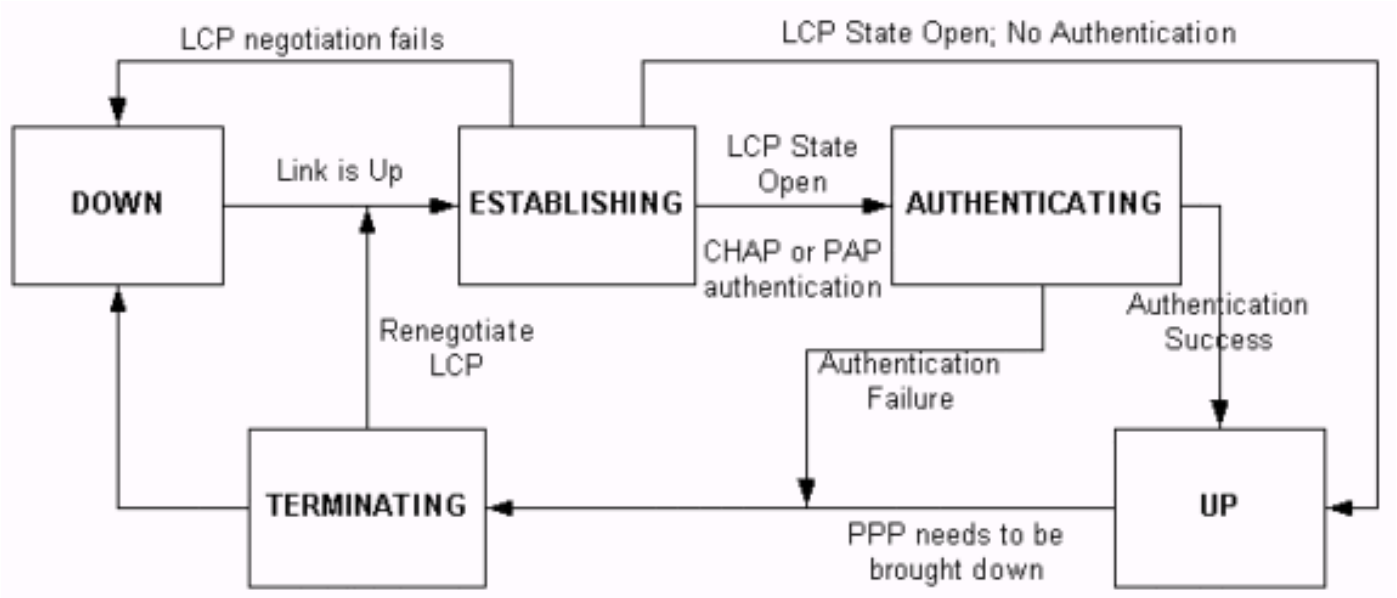
1. LCP = Link Control Protocol

2. CHAP = Challenge Handshake Authentication Protocol

3. PAP = Password Authentication Protocol

4. NCP = Network Control Protocol

Il diagramma mostra le transizioni di fase PPP:



Pacchetti di negoziazione PPP: Descrizione

In questa tabella viene fornita una descrizione dei pacchetti di negoziazione PPP utilizzati nelle negoziazioni LCP e NCP.

Pacchetto	Codice	Descrizione
CONFREQ	Configure-Request	Per aprire una connessione al peer, il dispositivo trasmette questo messaggio insieme alle opzioni di configurazione e ai valori che il mittente desidera siano supportati dal peer. Tutte le opzioni e i valori vengono negoziati contemporaneamente. Se il peer risponde con un messaggio CONFREJ o CONFNAK, il router invia un altro messaggio CONFREQ con un altro set di opzioni o valori.
CONFREJ	Configurazione-	Se alcune opzioni di configurazione ricevute nel messaggio CONFREQ

	Rifiuto	non sono accettabili o non sono riconoscibili, il router risponde con un messaggio CONFREJ. L'opzione inaccettabile (dal messaggio CONFREQ) è inclusa nel messaggio CONFREJ.
CONFNAK	Configure-NAK[1]	Se l'opzione di configurazione ricevuta è riconoscibile e accettabile, ma alcuni valori non sono accettabili, il router trasmette un messaggio CONFNAK. Il router aggiunge l'opzione e il valore che può accettare nel messaggio CONFREQ in modo che il peer possa includere tale opzione nel messaggio CONFREQ successivo.
SFACCETTARE	Configure-ACK[2]	Se tutte le opzioni nel messaggio CONFREQ sono riconoscibili e tutti i valori sono accettabili, il router trasmette un messaggio CONFACK.
REQ	Terminate-Request	Questo messaggio viene utilizzato per avviare una chiusura LCP.
TERMACK	Terminate-ACK	Questo messaggio viene trasmesso in risposta al messaggio TERMREQ.

1. NAK = Riconoscimento negativo

2. ACK = Conferma

Nota: ogni peer può inviare richieste CONFREQ con l'opzione o il valore che desidera che il peer supporti. Di conseguenza, le opzioni negoziate in ciascuna direzione possono essere diverse. Ad esempio, un lato potrebbe voler autenticare il peer, mentre l'altro no.

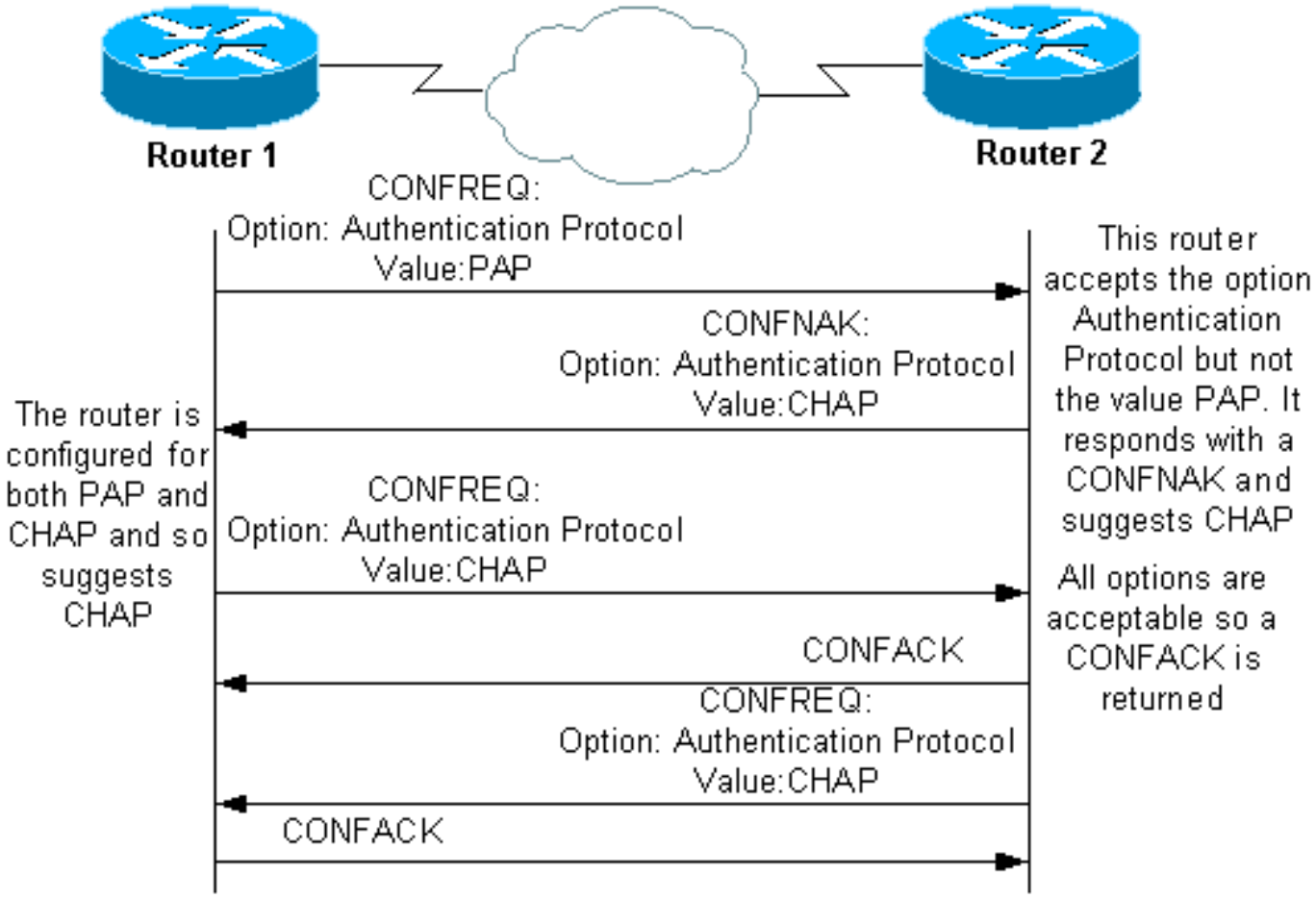
LCP, autenticazione e NCP Stage

In alcune delle fasi PPP descritte in precedenza, il PPP passa anche a fasi specifiche, quali la negoziazione LCP, l'autenticazione e la negoziazione NCP. Per ulteriori informazioni, fare riferimento alla RFC 1548 e alla RFC 1661 .

LCP (fase obbligatoria)

LCP è una fase in cui vengono negoziati i parametri per stabilire, configurare e verificare la connessione dati. Uno stato LCP aperto indica che LCP è stato completato correttamente, mentre uno stato LCP chiuso indica un errore LCP.

Il diagramma mostra una visualizzazione concettuale di un handshake LCP:



La negoziazione LCP utilizza anche un parametro denominato MagicNumber, che viene utilizzato per determinare se il collegamento viene ripristinato. Una stringa casuale viene inviata attraverso il collegamento e, se viene restituito lo stesso valore, il router determina che il collegamento viene rimandato indietro.

Autenticazione (fase facoltativa per impostazione predefinita)

In questa fase, l'autenticazione viene eseguita con il protocollo di autenticazione (CHAP o PAP) concordato nella negoziazione LCP. Per informazioni relative al protocollo PAP, consultare il documento sulla configurazione e la risoluzione dei problemi del protocollo PAP (PPP Password Authentication Protocol).

Per informazioni relative alla protezione CHAP, vedere Descrizione e configurazione dell'autenticazione CHAP PPP.

Nota: l'autenticazione è facoltativa e il protocollo PPP entra in questa fase solo se è necessario eseguire l'autenticazione.

NCP (fase obbligatoria)

Questa fase viene utilizzata per stabilire e configurare diversi protocolli a livello di rete. Il protocollo L3 più comune negoziato è IP. I router si scambiano messaggi IPCP (IP Control Protocol) per negoziare le opzioni specifiche del protocollo (IP in questo esempio).

La RFC 1332 dice che l'IPCP negozia due opzioni: assegnazioni di compressione e indirizzi IP. IPCP viene tuttavia utilizzato anche per passare informazioni relative alla rete, ad esempio server

WINS (Windows Name Service) primario e di backup e server DNS (Domain Name System).

La negoziazione viene eseguita con l'utilizzo dei messaggi CONF, come descritto in Pacchetti di negoziazione PPP: Sezione Descrizione di questo documento.

Risoluzione dei problemi con l'output della negoziazione PPP di debug

Quando si legge l'output del comando **debug ppp negotiation** a scopo di risoluzione dei problemi, attenersi alle seguenti istruzioni:

1. Identificare le transizioni di fase nell'output del comando **debug**. Determinare la fase più avanzata della connessione, ad esempio UP o AUTHENTICATING. Ciò consente di identificare la fase in cui la connessione non è riuscita. Per ulteriori informazioni sulle fasi, vedere la sezione Fasi della negoziazione PPP.
2. Per la fase in cui si è verificato l'errore, cercare i messaggi che indicano che LCP, autenticazione o NCP (a seconda dei casi) hanno esito positivo:Lo stato LCP deve essere aperto. È inoltre possibile esaminare gli ultimi messaggi CONFACK in entrata e in uscita per verificare che i parametri richiesti siano stati negoziati.L'autenticazione deve avere esito positivo. Se si utilizza l'autenticazione bidirezionale, ogni transazione deve avere esito positivo. Per ulteriori informazioni sulla risoluzione dei problemi relativi agli errori di autenticazione PPP, vedere Risoluzione dei problemi di autenticazione PPP (CHAP o PAP).Lo stato IPCP deve essere aperto. Verificare che l'indirizzamento sia corretto e che sia installato un percorso al peer.

Leggi output negoziazione ppp debug

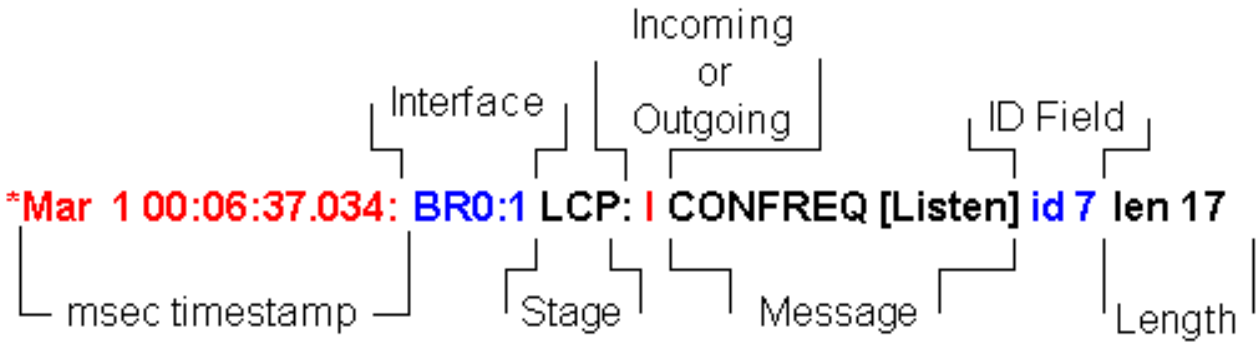
La maggior parte delle righe nell'output del comando **debug ppp negotiation** sono caratterizzate da:

1. **Timestamp**: i timestamp in millisecondi sono utili. Per ulteriori informazioni, vedere la sezione Prerequisiti di questo documento.
2. **Numero interfaccia e numero interfaccia** - Questo campo è utile quando le connessioni di debug utilizzano più connessioni o quando la connessione passa attraverso più interfacce. Alcune connessioni, ad esempio le chiamate a connessione multipla, sono controllate dall'interfaccia fisica all'inizio, ma in seguito dall'interfaccia dialer o dall'interfaccia di accesso virtuale.
3. **Tipo di messaggio PPP**: questo campo indica se la linea è un messaggio PPP, LCP, CHAP, PAP o IPCP generale.
4. **Direzione del messaggio**: un **I** indica un pacchetto in entrata e un **O** indica un pacchetto in uscita. Questo campo può essere utilizzato per determinare se il messaggio è stato generato o ricevuto dal router.
5. **Messaggio**: questo campo include la transazione specifica in fase di negoziazione.
6. **ID** - Questo campo viene utilizzato per associare e coordinare i messaggi di richiesta ai messaggi di risposta appropriati. È possibile utilizzare il campo ID per associare una risposta a un messaggio in ingresso. Questa opzione è particolarmente utile quando il messaggio in arrivo e la risposta sono distanti nell'output del comando debug.

7. **Lunghezza (Length)** - Il campo della lunghezza definisce la lunghezza del campo di informazioni. Questo campo non è importante per la risoluzione dei problemi generali.

Nota: i campi da 4 a 7 potrebbero non essere visualizzati in tutti i messaggi PPP, a seconda dello scopo del messaggio.

Nota: nell'esempio vengono illustrati i campi seguenti:



Output di esempio della negoziazione ppp di debug

Questa è una descrizione annotata dell'output del comando **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

Glossario e messaggi comuni

Generale

CONFREQ (Configure-Request):

Quando il livello inferiore diventa disponibile (Su), viene inviato un messaggio CONFREQ per avviare la prima fase PPP (fase LCP). Viene utilizzato nelle fasi LCP e NCP come tentativo di configurare la connessione. Per aprire una connessione al peer, il dispositivo trasmette questo messaggio insieme alle opzioni di configurazione e ai valori che il mittente desidera siano supportati dal peer. Tutte le opzioni e i valori vengono negoziati contemporaneamente. Se il peer risponde con un messaggio CONFREJ o CONFNAK, il router invia un altro messaggio CONFREQ con un altro set di opzioni o valori.

CONFACK (Configura-Riconoscimento):

Se tutte le opzioni nel messaggio CONFREQ sono riconoscibili e tutti i valori sono accettabili, il router trasmette un messaggio CONFACK.

CONFREJ (Configura rifiuto):

Se alcune opzioni di configurazione ricevute in CONFREQ non sono accettabili o non sono riconoscibili, il router risponde con un messaggio CONFREJ. L'opzione inaccettabile (da CONFREQ) è inclusa nel messaggio CONFREJ.

CONFNAK (Configura riconoscimento negativo):

Se l'opzione di configurazione ricevuta è riconoscibile e accettabile, ma alcuni valori non sono accettabili, il router trasmette un messaggio CONFNAK. Il router aggiunge l'opzione e il valore che può accettare nel messaggio CONFREQ in modo che il peer possa includere tale opzione nel messaggio CONFREQ successivo.

ECHOREQ (richiesta echo) e ECHOREP (risposta echo):

Il protocollo PPP utilizza i pacchetti keepalive per mantenere l'integrità della connessione. Questi keepalive sono il frame ECHOREQ inviato al peer PPP remoto, e il peer PPP remoto deve rispondere con un frame ECHOREP alla ricezione di un frame ECHOREQ. Per impostazione predefinita, se il router perde cinque frame ECHOREP, il collegamento viene considerato inattivo e il protocollo PPP viene interrotto.

TERMREQ (richiesta di interruzione):

Questo frame indica che il peer PPP che ha inviato il frame interrompe la connessione PPP.

TERMACK (conferma della terminazione):

Questo messaggio viene trasmesso in risposta al messaggio TERMREQ. La connessione PPP viene chiusa.

TERMINAZIONE

Questo messaggio indica che la connessione PPP è stata interrotta. Una connessione LCP o NCP può essere interrotta:

- alla chiusura amministrativa (solo LCP).
- quando il livello inferiore è fuori servizio (linea remota, ISDN e così via).
- al termine dei negoziati.
- rilevamento loop in linea.

LCP

ACM (mappa caratteri controllo asincrono):

Questa è una delle opzioni negoziate da LCP all'interno del frame CONFREQ. ACCM imposta le sequenze di escape dei caratteri. ACCM indica alla porta di ignorare i caratteri di controllo specificati all'interno del flusso di dati. Se il router all'altra estremità della connessione non supporta la negoziazione ACM, la porta è costretta a utilizzare FFFFFF. In tal caso, usare questo comando:

```
ppp accm match 000a000
```

ACFC (Address and Control Field Compression):

ACFC è un'opzione LCP che consente agli endpoint di inviare messaggi avanti e indietro in modo più efficiente.

AuthProto (protocollo di autenticazione):

AuthProto è il tipo di protocollo di autenticazione negoziato nel frame CONFREQ tra entrambi i peer di connessione PPP da utilizzare nella fase di autenticazione. Se non è configurata alcuna autenticazione PPP, questo output non viene visualizzato nei parametri negoziati con frame CONFREQ. I valori possibili sono CHAP o PAP.

Callback "#":

Questo messaggio indica che l'opzione di richiamata è in fase di negoziazione. Il numero che segue la sintassi di richiamata indica l'opzione di richiamata negoziata. Il numero 0 è un normale callback PPP, mentre il numero 6 indica l'opzione di callback Microsoft (disponibile automaticamente nel software Cisco IOS® versione 11.3(2)T o successive).

CHAP (Challenge Handshake Authentication Protocol):

Questo messaggio indica che il protocollo di autenticazione in fase di negoziazione è CHAP.

Disco endpoint (discriminatore endpoint):

Opzione LCP utilizzata per identificare un peer PPP nella connessione a connessione multipla PPP. Per ulteriori informazioni, fare riferimento a Criteri per la denominazione dei pacchetti Multilink PPP.

LCP Stato aperto

Questo messaggio indica che la negoziazione LCP è stata completata correttamente.

LQM (Link Quality Monitoring)

LQM è disponibile su tutte le interfacce seriali con PPP. LQM controlla la qualità del collegamento e lo riduce quando la qualità scende al di sotto di una percentuale configurata. Le percentuali vengono calcolate sia per le direzioni in entrata che in uscita. La qualità in uscita viene calcolata confrontando il numero totale di pacchetti e byte inviati con il numero totale di pacchetti e byte ricevuti dal peer. La qualità in ingresso viene calcolata confrontando il numero totale di pacchetti e byte ricevuti con il numero totale di pacchetti e byte inviati dal peer.

Quando LQM è abilitato, vengono inviati i report LQR (Link Quality Report) a ogni periodo keepalive. I moduli LQR vengono inviati al posto dei pacchetti keepalive. A tutti i pacchetti keepalive in ingresso viene fornita una risposta adeguata. Se LQM non è configurato, i pacchetti keepalive vengono inviati a ogni periodo keepalive e a tutti i moduli LQR in arrivo viene risposto con un LQR.

NumeroMagico

Il supporto di Magic Number è disponibile su tutte le interfacce seriali. Il protocollo PPP tenta sempre di negoziare i numeri magici, utilizzati per rilevare le reti di loopback. Una stringa casuale viene inviata attraverso il collegamento e se viene restituito lo stesso valore, il router determina che il collegamento viene rimandato indietro.

Il collegamento potrebbe essere interrotto o meno al rilevamento di loop-back; dipende dall'uso del comando down-when-looped.

PAP (Password Authentication Protocol)

Questo messaggio indica che il protocollo di autenticazione in fase di negoziazione per l'utilizzo da parte dei peer PPP è PAP. Per ulteriori informazioni su PAP, consultare il documento sulla configurazione e risoluzione dei problemi relativi al protocollo PAP (PPP Password Authentication Protocol).

PFC (Protocol Field Compression)

Questa opzione attiva o disattiva la compressione per i campi del protocollo.

MRRU (unità ricostruita ricezione massima)

Si tratta di un'opzione LCP negoziata durante il processo di configurazione di LCP Multilink PPP. Questa opzione determina il numero massimo di byte che possono costituire un frame. Se MRRU non viene negoziato in LCP, non sarà possibile eseguire Multilink PPP (MPPP) sul collegamento.

MRU (Unità massima ricevuta)

MRU è un'opzione LCP negoziata nel frame CONFREQ per negoziare le dimensioni dei pacchetti scambiati.

Autenticazione

AUTH-REQ (richiesta di autenticazione)

Questo frame viene inviato dal peer PPP locale (sul quale è abilitata l'autenticazione) al peer remoto. Richiede al peer remoto di inviare un nome utente e una password validi per l'autenticazione della connessione PPP. Questo frame viene utilizzato solo con PAP.

AUTH-ACK (autenticazione riconosciuta)

Questo frame viene inviato dal peer PPP autenticato al peer PPP autenticato. Questo frame contiene la coppia valida di nome utente e password. Questo frame viene utilizzato solo quando si utilizza PAP per l'autenticazione della connessione PPP.

AUTH-NAK o ERRORE

Questo frame viene inviato dal peer PPP di autenticazione quando l'autenticazione sul peer PPP di autenticazione non è riuscita.

RICHIESTA

Frame di richiesta CHAP inviato dal peer PPP di autenticazione al peer PPP autenticato. Il frame di verifica è costituito da un ID, un numero casuale e dal nome host del server di comunicazione locale o dal nome dell'utente sul dispositivo remoto. Questo frame viene utilizzato solo quando si utilizza la protezione CHAP per l'autenticazione della connessione PPP.

RISPOSTA

Questo frame è la risposta CHAP inviata dal peer PPP autenticato al peer PPP autenticato.

La risposta richiesta è costituita da due parti:

- Output hash MD5 del segreto condiviso.
- Il nome host del dispositivo remoto o il nome dell'utente del dispositivo remoto.

Questo frame viene utilizzato solo quando si utilizza la protezione CHAP per l'autenticazione della connessione PPP.

NCP

Indirizzo a.b.c.d

- In un messaggio CONFREQ in uscita, questo valore indica l'indirizzo IP che il router locale desidera utilizzare. Se l'indirizzo incluso è 0.0.0.0, il computer locale richiede al peer di fornire un indirizzo IP utilizzabile.
- In un messaggio CONFREQ in ingresso, questo valore indica l'indirizzo IP che il peer desidera utilizzare. Se l'indirizzo incluso è 0.0.0.0, il peer richiede al computer locale di fornire un indirizzo IP utilizzabile.
- In un messaggio CONFREQ in uscita, questo valore indica l'indirizzo IP che il peer deve

utilizzare anziché quello suggerito nel messaggio CONFREQ.
- In un messaggio CONFREQ in ingresso, questo valore indica l'indirizzo IP che il computer locale deve utilizzare, anziché quello suggerito nel precedente messaggio CONFREQ.
- In un messaggio CONFACK in uscita, questo valore indica che l'indirizzo IP richiesto dal peer è accettabile per il computer locale.
- In un messaggio CONFACK in ingresso, questo valore indica che l'indirizzo IP richiesto dal computer locale è accettabile per il peer.

CCP (Compression Control Protocol)

Questo messaggio indica che è in corso la negoziazione di un protocollo di compressione tra entrambi i peer PPP. Il software Cisco IOS supporta questi protocolli di compressione da negoziare su una connessione PPP:

- Compressione MS-Point-to-Point (MS-PC)
- impilatore
- predittore

CDPCP (Cisco Discovery Protocol Control Protocol)

Questo messaggio indica che la negoziazione CDP ha luogo nella fase NCP. Per disattivare il CDP sul router, usare il comando **no cdp run**.

CODEREJ (Rifiuto del codice)

Un pacchetto CODEREJ viene inviato alla ricezione di un pacchetto non interpretabile compresso dal peer PPP remoto.

Installa route verso a.b.c.d

Quando il router termina la fase IPCP (NCP per il protocollo IP L3), deve installare l'indirizzo IP specificato nel peer PPP remoto nella tabella di routing e deve essere visto come un percorso connesso nella tabella di routing. Se questo messaggio non viene visualizzato, verificare che il comando **no peer neighbors-route** non sia configurato.

IPCP (IP Control Protocol)

Questo valore indica che IP è il livello di rete in negoziazione nella fase NCP.

Stato IPCP aperto

Questo messaggio indica che la fase IPCP (NCP per il protocollo IP L3) è stata completata correttamente.

PROTREJ (Rifiuto protocollo)

Il peer PPP, alla ricezione di un pacchetto PPP con un campo di protocollo sconosciuto, utilizza il messaggio PROTREJ per indicare che il peer ha tentato di utilizzare un protocollo non supportato.

Quando un dispositivo PPP riceve un messaggio PROTREJ, deve al più presto cessare di inviare i pacchetti del protocollo indicato.

Informazioni correlate

- Configurazione e risoluzione dei problemi del protocollo PAP (PPP Password Authentication Protocol)
- Autenticazione PPP utilizzando i comandi ppp chap hostname e ppp authentication chap callin
- Descrizione e configurazione dell'autenticazione CHAP nei server PPP
- Risoluzione dei problemi di autenticazione PPP (CHAP o PAP)
- Pagine di supporto per la tecnologia di composizione
- Supporto tecnico – Cisco Systems