Entendendo a saída de negociação de debug ppp

Contents

Introduction

Em aplicativos relacionados a discagem, o PPP é o tipo de encapsulamento mais comumente usado. O PPP permite que duas máquinas em um link de comunicação ponto-a-ponto negociem vários parâmetros de autenticação, compactação e protocolos de Camada 3 (L3); por exemplo, IP. Uma falha na negociação do PPP entre dois roteadores faz com que a conexão falhe.

O comando **debug ppp negotiation** permite que você visualize as transações de negociação PPP, identifique o problema ou estágio quando o erro ocorre e desenvolva uma resolução. No entanto, é imperativo que você entenda a saída do comando **debug ppp negotiation**. Este documento fornece um método abrangente para ler a saída do comando debug ppp negotiation.

Prerequisites

Requirements

Os leitores deste documento devem garantir que essas condições sejam atendidas:

- O PPP deve ser habilitado na interface de ambos os roteadores. Emita o comando

encapsulation ppp para fazer isso.

- Emita este comando para ativar os timestamps de milissegundo no roteador:
  `Router(config)# service timestamp debug datetime msec`

  Para obter mais informações sobre comandos debug, consulte Informações importantes sobre comandos debug.

Observação: a negociação PPP entre dois pares não pode ser iniciada a menos que a camada inferior (ISDN, interface física, linha dial-up, etc.) sob o PPP funcione perfeitamente. Por exemplo, se você deseja executar o PPP sobre ISDN, todas as camadas ISDN devem estar ativas; caso contrário, o PPP não é iniciado.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

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

Fases da negociação de PPP

O link passa por várias fases no processo de negociação de PPP, como mostrado nesta tabela. O resultado final é que o PPP está ativado ou desativado.

Fase	Descrição
DOWN	Nesta fase, o PPP está inoperante. Esta mensagem é exibida após a derrubada do link e do PPP: `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
ESTABELECENDO	O PPP muda para essa fase quando recebe uma indicação de que a camada física está ativa e pronta para uso. A negociação do LCP [1] ocorre nesta fase. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTENTICAÇÃO	Se a autenticação PPP (CHAP[2] ou PAP[3]) for desejada no link, o PPP entrará nessa fase. Lembre-se de que a autenticação PPP é opcional. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
PARA CIMA	Quando a autenticação é concluída, o PPP faz a transição para a fase UP. A negociação de NCP [4] ocorre nesta fase. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMINANDO	Nesta fase, o PPP é desligado. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

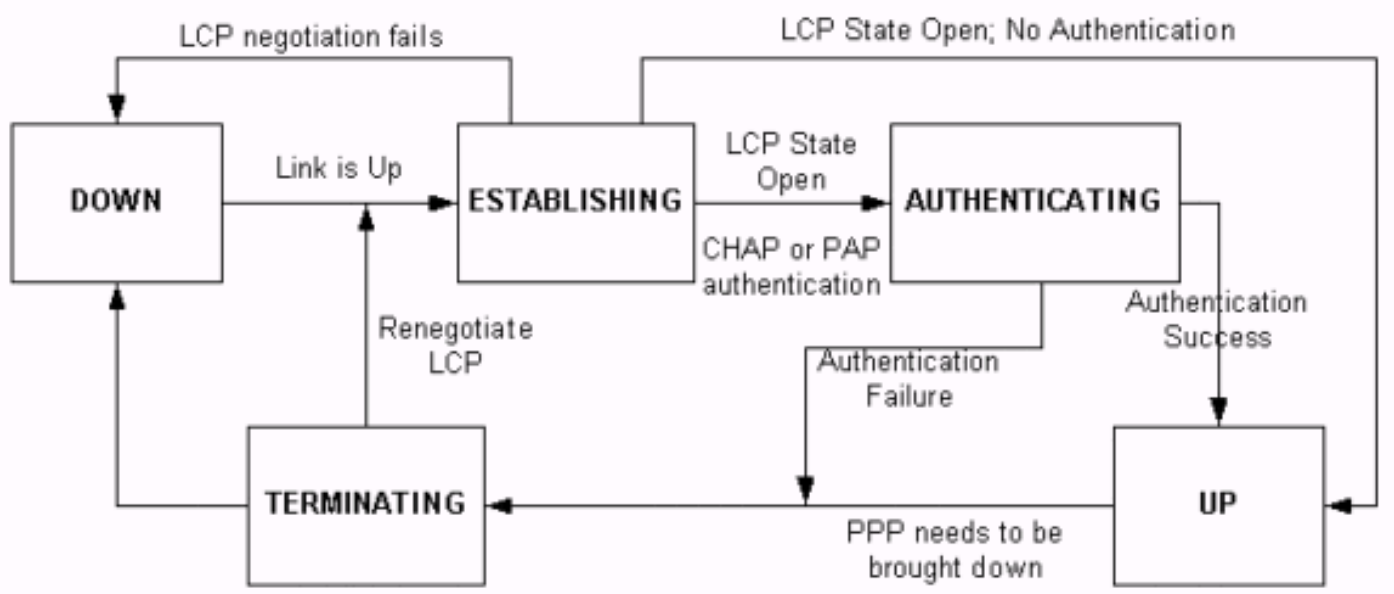
1. LCP = Link Control Protocol

2. CHAP = Challenge Handshake Authentication Protocol

3. PAP = Password Authentication Protocol

4. NCP = Network Control Protocol

Este diagrama mostra as transições da fase PPP:



Pacotes de negociação PPP: Uma descrição

Esta tabela inclui a descrição dos pacotes de negociação PPP usados na negociação de LCP e NCP:

Pacote	Code	Descrição
CONFREQ	Configure-Request	Para abrir uma conexão com o peer, o dispositivo transmite essa mensagem junto com as opções de configuração e os valores que o remetente deseja que o peer suporte. Todas as opções e valores são negociados simultaneamente. Se o peer responder com uma mensagem CONFREJ ou CONFNAK, o roteador enviará outro CONFREQ com outro conjunto de opções ou valores.
CONFREJ	Configure-Reject	Se alguma opção de configuração recebida na mensagem CONFREQ não for aceitável ou não for reconhecível, o roteador responde com uma mensagem CONFREJ. A opção inaceitável (a partir da mensagem de CONFREQ) está incluída na mensagem de CONFREJ.
CON	Configur	Se a opção de configuração recebida

FNAK	e-NAK[1]	for reconhecível e aceitável, mas algum valor não for aceitável, o roteador transmitirá uma mensagem CONFNAK. O roteador anexa a opção e o valor que podem ser aceitos na mensagem CONFNAK de modo que o correspondente possa incluir essa opção na mensagem CONFREQ.
CONFACK	Configure-ACK[2]	Se todas as opções na mensagem CONFREQ forem reconhecíveis e todos os valores forem aceitáveis, o roteador transmitirá uma mensagem CONFACK.
TERMREQ	Terminate-Request	Essa mensagem é utilizada para iniciar um fechamento de LCP.
TERMACK	Terminate-ACK	Essa mensagem é transmitida em resposta à mensagem TERMREQ.

1. NAK = Confirmação negativa

2. ACK = Confirmação

Observação: cada peer pode enviar CONFREQs com a opção ou valor que deseja que o peer suporte. Isso pode fazer com que as opções negociadas em cada direção sejam diferentes. Por exemplo, um lado pode desejar autenticar o peer, enquanto o outro não.

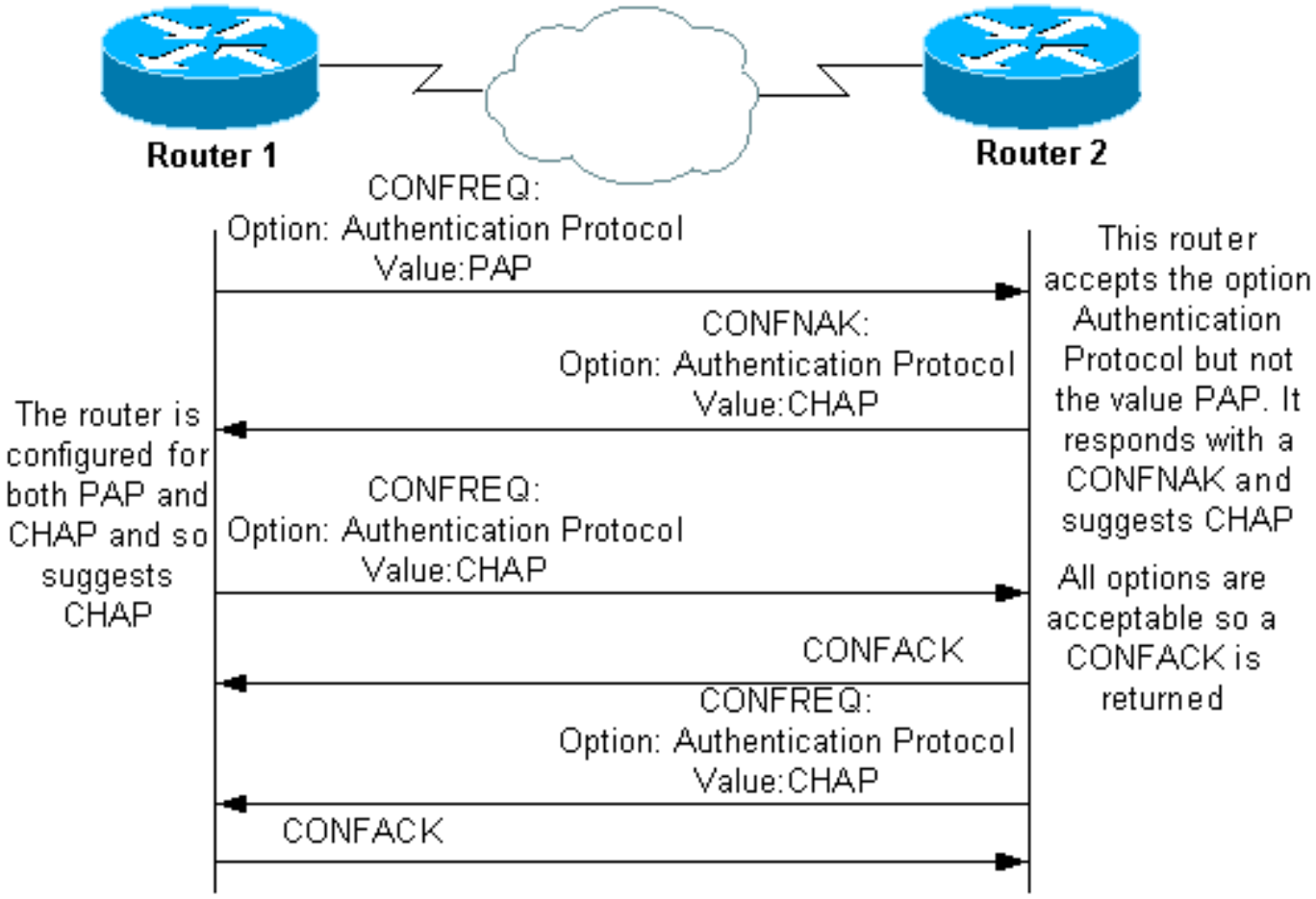
Estágio de LCP, Autenticação e NCP

Em algumas das fases do PPP descritas anteriormente, o PPP também entra em estágios específicos, como negociação de LCP, autenticação e negociação de NCP. Para obter mais informações, consulte RFC 1548 e RFC 1661 .

LCP (Fase obrigatória)

O LCP é uma fase na qual os parâmetros para estabelecer, configurar e testar a conexão de enlace de dados são negociados. Um estado de LCP de aberto significa que o LCP foi concluído com êxito, enquanto um estado de LCP fechado indica uma falha de LCP.

Este diagrama mostra uma visão conceitual de um handshake LCP:



A negociação LCP também utiliza um parâmetro chamado MagicNumber, utilizado para determinar se o enlace tem o loop fechado. Uma string aleatória é enviada através do link e, se o mesmo valor for retornado, o roteador determina que o link tem loopback.

Autenticação (Fase opcional por padrão)

Nesta etapa, a autenticação é executada com o protocolo de autenticação (CHAP ou PAP) acordado na negociação do LCP. Para obter informações relacionadas ao PAP, consulte Configuração e Troubleshooting do PPP Password Authentication Protocol (PAP).

Para obter informações relacionadas ao CHAP, consulte Compreendendo e Configurando a Autenticação CHAP PPP.

Observação: a autenticação é opcional e o PPP somente entra nessa etapa se precisar autenticar.

NCP (Fase obrigatória)

Essa fase é usada para estabelecer e configurar diferentes protocolos da camada de rede. O protocolo L3 mais comumente negociado é o IP. Os roteadores trocam mensagens de IP Control Protocol (IPCP) para negociar opções específicas ao protocolo (IP neste exemplo).

RFC 1332 diz que o IPCP negocia duas opções: compactação e atribuições de endereço IP. No entanto, o IPCP também é usado para transmitir informações relacionadas à rede, como servidores WINS (Windows Name Service) principal e de backup e DNS (Domain Name System).

A negociação ocorre com o uso de mensagens CONF, conforme descrito em Pacotes de Negociação PPP: Uma seção Descrição deste documento.

Solução de problemas com a saída debug ppp negotiation

Ao ler a saída do comando **debug ppp negotiation** para fins de solução de problemas, siga estas instruções:

1. Identifique as transições de fase na saída do comando **debug**. Determine a fase mais distante da conexão obtida, como UP ou AUTHENTICATING. Isso pode ajudá-lo a identificar a fase em que a conexão falhou. Para obter mais informações sobre as fases, consulte a seção Fases da Negociação PPP.
2. Para a fase em que a falha ocorreu, procure mensagens que indicam que o LCP, a autenticação ou o NCP (conforme apropriado) são bem-sucedidos:O estado do LCP deve estar aberto. Você também pode observar as últimas mensagens CONFACK de entrada e de saída para verificar se os parâmetros que você exige têm sido negociados.A autenticação deve ser bem-sucedida. Se você usar a autenticação bidirecional, cada transação deverá ser bem-sucedida. Para obter mais informações sobre Troubleshooting de falhas de autenticação PPP, consulte Troubleshooting de Autenticação PPP (CHAP ou PAP).O estado do IPCP deve ser aberto. Verifique se o endereçamento está correto e se uma rota para o peer está instalada.

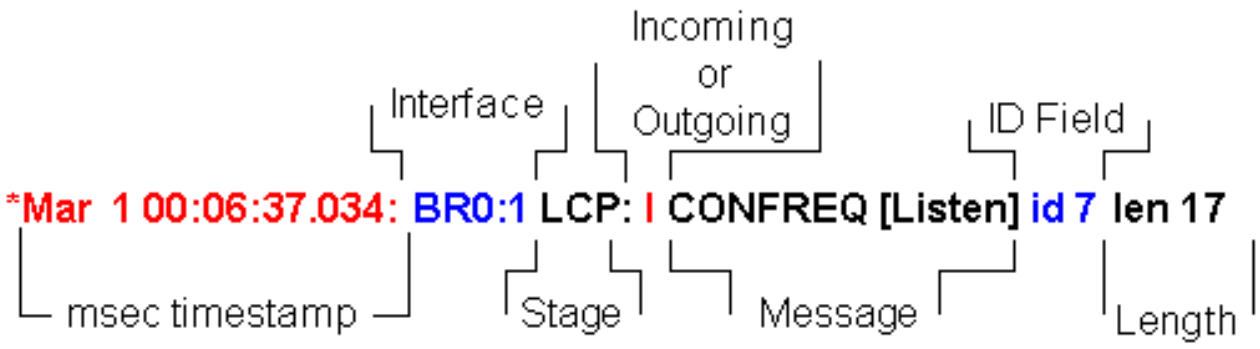
Leia a saída de negociação de debug ppp

A maioria das linhas na saída do comando **debug ppp negotiation** são caracterizadas por:

1. **O timestamp** — Milissegundos timestamps são úteis. Consulte a seção Pré-requisitos deste documento para obter mais informações.
2. **Interface e número de interface** —Este campo é útil quando as conexões de depuração usam várias conexões ou quando a conexão passa por várias interfaces. Por exemplo, certas conexões (como chamadas multilink) são controladas pela interface física no início, mas são posteriormente controladas pela interface do discador ou pela interface de acesso virtual.
3. **Tipo de mensagem PPP** —Este campo indica se a linha é uma mensagem geral PPP, LCP, CHAP, PAP ou IPCP.
4. **Direção da mensagem**—Uma **I** indica um pacote de entrada e uma **O** indica um pacote de saída. Esse campo pode ser usado para determinar se a mensagem foi gerada ou recebida pelo roteador.
5. **Mensagem** — Este campo inclui a transação específica em negociação.
6. **ID** — Este campo é usado para corresponder e coordenar mensagens de solicitação com as mensagens de resposta apropriadas. Você pode usar o campo ID para associar uma resposta a uma mensagem de entrada. Essa opção é especialmente útil quando a mensagem de entrada e a resposta estão muito separadas na saída de depuração.
7. **Comprimento** — O campo de comprimento define o comprimento do campo de informações. Esse campo não é importante para a solução de problemas geral.

Observação: os campos de 4 a 7 podem não aparecer em todas as mensagens PPP, dependendo da finalidade da mensagem.

Observação: este exemplo ilustra os campos:



Exemplo de saída de debug ppp negotiation

Esta é uma descrição anotada da saída do 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

Glossário e mensagens comuns

General

CONFREQ (Configure-Request):

Quando a camada inferior se torna disponível (Ativa), um CONFREQ é enviado para iniciar a

primeira fase PPP (fase LCP). É usado nas fases LCP e NCP como uma tentativa de configurar a conexão. Para abrir uma conexão com o peer, o dispositivo transmite essa mensagem junto com as opções de configuração e os valores que o remetente deseja que o peer suporte. Todas as opções e valores são negociados simultaneamente. Se o peer responder com uma mensagem CONFREJ ou CONFNAK, o roteador enviará outro CONFREQ com outro conjunto de opções ou valores.

CONFACK (Configure-Acknowledge):

Se todas as opções na mensagem CONFREQ forem reconhecíveis e todos os valores forem aceitáveis, o roteador transmitirá uma mensagem CONFACK.

CONFREJ (Configurar Rejeição):

Se alguma opção de configuração recebida no CONFREQ não for aceitável ou não for reconhecível, o roteador responde com uma mensagem CONFREJ. A opção inaceitável (de CONFREQ) está inclusa na mensagem CONFREJ.

CONFNAK (Configurar reconhecimento negativo):

Se a opção de configuração recebida for reconhecível e aceitável, mas algum valor não for aceitável, o roteador transmitirá uma mensagem CONFNAK. O roteador anexa a opção e o valor que podem ser aceitos na mensagem CONFNAK de modo que o correspondente possa incluir essa opção na mensagem CONFREQ.

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

O PPP usa keepalives para manter a integridade da conexão. Esses keepalives são o quadro ECHOREQ que é enviado ao peer PPP remoto, e o peer PPP remoto deve responder com um quadro ECHOREP após o recebimento de um quadro ECHOREQ. Por padrão, se o roteador perder cinco quadros ECHOREP, o link será considerado inativo e o PPP será desativado.

TERMREQ (Solicitação de término):

Esse quadro indica que o peer PPP que enviou esse quadro encerra a conexão PPP.

TERMACK (reconhecimento de terminação)

Essa mensagem é transmitida em resposta à mensagem TERMREQ. Isso encerra a conexão PPP.

TERMINANDO

Essa mensagem indica que a conexão PPP foi desativada. Uma conexão LCP ou NCP pode ser cortada:

- ao fechar administrativo (somente LCP).
- quando o nível inferior vai para fora de serviço (linha de discagem, ISDN e assim por diante).
- quando negociações fracassam.

- detecção de circuito on-line.

LCP

ACCM (Asynchronous Control Character Map):

Essa é uma das opções negociadas para LCP dentro da estrutura CONFREQ. O ACCM define as sequências de escape de caracteres. O ACCM instrui a porta a ignorar os caracteres de controle especificados no fluxo de dados. Se o roteador na outra extremidade da conexão não suportar a negociação ACCM, a porta será forçada a usar FFFFFFF. Nesse caso, emita este comando:

```
ppp accm match 000a000
```

ACFC (Compactação de campo de endereço e controle):

ACFC é uma opção de LCP que permite que os terminais enviem mensagens para frente e para trás com mais eficiência.

AuthProto (Protocolo de Autenticação):

AuthProto é o tipo de protocolo de autenticação negociado no quadro CONFREQ entre os dois pares de conexão PPP para uso na fase de autenticação. Se nenhuma autenticação PPP estiver configurada, essa saída não será vista nos parâmetros negociados do quadro CONFREQ. Os valores possíveis são CHAP ou PAP.

Retorno de chamada "#":

Essa mensagem indica que a opção de retorno de chamada está em negociação. O número após a sintaxe de retorno de chamada indica qual opção de retorno de chamada é negociada. O número 0 é um retorno de chamada PPP normal, enquanto o número 6 indica a opção de retorno de chamada da Microsoft (que está automaticamente disponível no Cisco IOS® Software Release 11.3(2)T ou posterior).

CHAP (Challenge Handshake Authentication Protocol):

Essa mensagem indica que o protocolo de autenticação em negociação é CHAP.

EndpointDisc (Discriminador de ponto final):

Esta é uma opção de LCP usada para identificar um correspondente PPP em uma conexão PPP Multilink. Para obter mais informações, consulte Critérios para Nomear Pacotes PPP Multilink.

LCP: Estado está aberto

Essa mensagem indica que uma negociação de LCP foi concluída com sucesso.

LQM (Monitoramento da qualidade do link)

O LQM está disponível em todas as interfaces seriais que executam o PPP. O LQM monitora a qualidade do link e diminui quando a qualidade cai abaixo de uma porcentagem configurada. As porcentagens são calculadas para os sentidos de entrada e saída. A qualidade de saída é calculada por comparação do número total de pacotes e bytes enviados com o número total de pacotes e bytes recebidos pelo peer. A qualidade de entrada é calculada por comparação do número total de pacotes e bytes recebidos com o número total de pacotes e bytes enviados pelo peer.

Quando o LQM está ativado, os LQRs (Link Quality Reports, Relatórios de qualidade de link) são enviados a cada período de manutenção de atividade. Os LQRs são enviados no lugar dos keepalives. Todos os keepalives de entrada são respondidos corretamente. Se o LQM não estiver configurado, os keepalives serão enviados em cada período de keepalive e todos os LQRs de entrada serão respondidos com um LQR.

MagicNumber

O suporte para Magic Number está disponível em todas as interfaces seriais. O PPP sempre tenta negociar números mágicos, que são usados para detectar redes loopback. Uma string aleatória é enviada através do link e se o mesmo valor for retornado, o roteador determina que o link tem loopback.

O link pode ou não ser desativado na detecção de loopback; depende do uso do comando **down-when-looped.**

PAP (Password Authentication Protocol)

Essa mensagem indica que o protocolo de autenticação em negociação para uso pelos pares PPP é PAP. Para obter mais informações sobre PAP, consulte Configuração e Troubleshooting do PPP Password Authentication Protocol (PAP).

PFC (Protocol Field Compression)

Esta opção ativa ou desativa a compressão dos campos do protocolo.

MRRU (Máx. de Unidade Reconstruída de Recepção)

Essa é uma opção de LCP negociada no processo de configuração de LCP multilink PPP. Essa opção determina o número máximo de bytes que podem constituir um quadro. Se o MRRU não for negociado no LCP, o PPP Multilink (MPPP) não poderá ser executado no link.

MRU (Unidade máxima recebida)

A MRU é uma opção de LCP negociada no quadro CONFREQ para negociar o tamanho dos pacotes trocados.

Autenticação

AUTH-REQ (Solicitação de Autenticação)

Esse quadro é enviado do peer PPP local (no qual a autenticação está habilitada) para o peer remoto. Pede que o peer remoto envie um nome de usuário e uma senha válidos para a autenticação de conexão PPP. Esse quadro é usado somente com PAP.

AUTH-ACK (Confirmação de Autenticação)

Esse quadro é enviado no correspondente PPP autenticado para o correspondente PPP de autenticação. Este quadro transporta o par válido de nome de usuário e senha. Esse quadro é usado somente quando PAP é usado para autenticação de conexão PPP.

AUTH-NAK ou FALHA

Esse quadro é enviado do peer PPP de autenticação quando a autenticação falhou no peer PPP de autenticação.

DESAFIO

Esse é o quadro de desafio CHAP que é enviado do peer PPP de autenticação ao peer PPP autenticado. O quadro de desafio consiste em um ID, um número aleatório e o nome do host do servidor de comunicação local ou o nome do usuário no dispositivo remoto. Esse quadro é usado somente quando o CHAP é usado para autenticação de conexão PPP.

RESPOSTA

Esse quadro é a resposta CHAP enviada do peer PPP autenticado para o peer PPP de autenticação.

A resposta necessária consiste em duas partes.

- Uma saída hash MD5 do segredo compartilhado.
- O nome do host do dispositivo remoto ou o nome do usuário no dispositivo remoto.

Esse quadro é usado somente quando o CHAP é usado para autenticação de conexão PPP.

NCP

Endereço a.b.c.d

- Em uma mensagem CONFREQ de saída, esse valor indica o endereço IP que o roteador local deseja usar. Se o endereço incluído for 0.0.0.0, a máquina local solicitará ao peer que lhe forneça um endereço IP que possa usar.
- Em uma mensagem CONFREQ recebida, esse valor indica o endereço IP que o peer deseja usar. Se o endereço incluído for 0.0.0.0, o peer solicitará à máquina local que lhe forneça um endereço IP que possa usar.
- Em uma mensagem CONFNAK de saída, esse valor indica o endereço IP que o peer deve utilizar, e não o endereço que o peer sugeriu na mensagem CONFREQ.
- Em uma mensagem CONFNAK recebida, este valor indica o endereço IP que a máquina

local deve usar, em vez daquele sugerido na mensagem CONFREQ anterior.
- Em uma mensagem CONFACK de saída, este valor indica que o endereço IP solicitado pelo peer é aceitável para a máquina local.
- Em uma mensagem CONFACK recebida, esse valor indica que o endereço IP solicitado pela máquina local é aceitável para o peer.

CCP (Compression Control Protocol)

Essa mensagem indica que um protocolo de compactação está em negociação entre os dois pares PPP. O Cisco IOS Software suporta estes protocolos de compactação a serem negociados em uma conexão PPP:

- Compactação MS-Point-to-Point (MS-PPC)
- empilhador
- preditor

CDPCP (Cisco Discovery Protocol Control Protocol)

Essa mensagem indica que a negociação do CDP ocorre na fase NCP. Para desativar o CDP no roteador, execute o comando **no cdp run**.

CODEREJ (Rejeição de Código)

Um pacote CODEREJ é enviado após o recebimento de um pacote ininterpretável do peer PPP remoto.

Instalar rota para a.b.c.d

Quando o roteador termina o IPCP (fase NCP para o protocolo IP L3), ele deve instalar o endereço IP fornecido para o peer PPP remoto na tabela de roteamento e ser visto como uma rota conectada na tabela de roteamento. Se você não vir esta mensagem, verifique se o comando **no peer neighbor-route** não está configurado.

IPCP (IP Control Protocol)

Esse valor indica que o IP é a camada de rede em negociação na fase NCP.

Estado de IPCP aberto

Esta mensagem indica que o IPCP (fase NCP para o protocolo IP L3) foi concluído com êxito.

PROTREJ (Protocol Reject)

O peer PPP, ao receber um pacote PPP com um campo de protocolo desconhecido, usa a mensagem PROTREJ para indicar que o peer tentou usar um protocolo não suportado. Quando um dispositivo PPP recebe uma mensagem PROTREJ, ele deve, o mais rápido possível, deixar de enviar pacotes do protocolo indicado.

Informações Relacionadas

- Configurando e Troubleshooting de PPP Password Authentication Protocol (PAP)
- Autenticação PPP Usando os Comandos ppp chap hostname e ppp authentication chap callin
- Entendendo e configurando a autenticação de PPP CHAP
- Troubleshooting de Autenticação de PPP (CHAP ou PAP)
- Página de suporte da tecnologia de discagem
- Suporte Técnico - Cisco Systems