Entendendo a saída de negociação de debug ppp

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Fases da negociação de PPP
Pacotes de negociação PPP: Uma descrição
LCP, autenticação, e estágio NCP
O Troubleshooting com debuga saídas de negociação ppp
Lido debugar saídas de negociação ppp
Exemplo de saída de debug ppp negotiation
Glossário e mensagens comuns
Geral
LCP
Autenticação
NCP
Informações Relacionadas

Introdução

Em aplicativos seletor-relacionados, o PPP é o tipo de encapsulamento o mais de uso geral. 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 de PPP entre dois Roteadores faz com que a conexão falhe.

O comando debug ppp negotiation permite-o de ver as transações da negociação de PPP, de identificar o problema ou de encená-lo quando o erro ocorre, e desenvolve-o uma definição. Contudo, é imperativo que você compreende a saída do **comando debug ppp negotiation**. Este documento fornece um método abrangente para ler a saída do comando debug ppp negotiation.

Pré-requisitos

Requisitos

Os leitores deste documento devem assegurar-se de que estas circunstâncias estejam estadas conformes:

- O PPP deve ser habilitado na interface de ambos os roteadores. Emita o **comando encapsulation ppp** realizar isto.
- Emita este comando permitir formatos de tempo de milisegundo no roteador:`Router(config)#` **`service timestamp debug datetime msec`** Para obter mais informações sobre dos comandos debug, veja a informação importante em comandos Debug.

Nota: A negociação de PPP entre dois pares não pode começar a menos que a camada mais baixa (ISDN, interface física, linha dial-up, e assim por diante) sob o PPP funcionar perfeitamente. Por exemplo, se você quer executar o PPP over ISDN, a seguir todas as camadas de ISDN devem estar acima; se não o PPP não começa.

Componentes Utilizados

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

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Fases da negociação de PPP

O link atravessa diversas fases em processo da negociação de PPP, segundo as indicações desta tabela. O resultado final é que o PPP está ativado ou desativado.

Fase	Descrição
DOWN	Nesta fase, o PPP está para baixo. Esta mensagem é exibida após a derrubada do link e do PPP: `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
ESTABELECIMENTO	O PPP muda para essa fase quando recebe uma indicação de que a camada física está ativa e pronta para uso. A negociação LCP1 ocorre nesta fase. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTENTICAÇÃO	Se a autenticação de PPP (CHAP2 ou PAP3) é desejada no link, então transições de PPP a esta fase. Mantenha na mente que a autenticação de PPP é opcional. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
PARA CIMA	Uma vez que a autenticação está completa, transições de PPP à fase ASCENDENTE. A negociação NCP4 ocorre nesta fase. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMINANDO	Nesta fase, o PPP fechou. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

1. LCP = link control protocol

2. RACHADURA = protocolo de autenticação de cumprimento do desafio

3. PAP = protocolo password authentication

4. NCP = protocolo network control

Este diagrama mostra as transições de fase PPP:

Pacotes de negociação PPP: Uma descrição

Esta tabela inclui a descrição dos pacotes de negociação PPP que são usados no LCP e na negociação de NCP:

Pacote	Código	Descrição
CONFREQ	Configure-Request	Para abrir uma conexão ao par, o dispositivo transmite esta mensagem junto com as opções de configuração e avalia o remetente deseja o par apoiar. Todas as opções e valores são negociados simultaneamente. Se o par responde com um CONFREJ ou um mensagem de CONFNAK, a seguir o roteador envia um outro CONFREQ com um outro conjunto de opções ou valores.
CONFREJ	Configurar-rejeição	Se alguma opção de configuração recebida no mensagem de CONFREQ não é aceitável ou não reconhecível, o roteador responde com um mensagem de CONFREJ. A opção inaceitável (a partir da mensagem de CONFREQ) está incluída na mensagem de CONFREJ.
CONFNAK	Configurar-NAK[1]	Se a opção de configuração recebida é reconhecível e aceitável, mas algum valor não é aceitável, o roteador transmite um mensagem de 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	Configurar-ACK[2]	Se todas as opções no mensagem de CONFREQ são reconhecíveis e todos os valores são aceitáveis, a seguir o roteador transmite um mensagem CONFACK.
TERMRE	Terminate-	Essa mensagem é utilizada para iniciar um fechamento de LCP.

Q	Request	
TERMACK	Terminar-ACK	Essa mensagem é transmitida em resposta à mensagem TERMREQ.

1. NAK = reconhecimento negativo

2. O ACK = reconhece

Nota: Cada par pode enviar CONFREQ com a opção ou avaliá-la quer o par apoiar. Isto pode causar as opções negociadas em cada sentido para ser diferente. Por exemplo, um lado pode desejar autenticar o par, quando o outro não puder.

LCP, autenticação, e estágio NCP

Dentro de algumas das fases PPP descritas previamente, o PPP igualmente entra em fases específicas tais como a negociação de LCP, a autenticação, e a negociação de NCP. Para mais informação, refira o RFC 1548 e o RFC 1661 .

LCP (fase imperativa)

O LCP é uma fase em que os parâmetros a estabelecer, configuram, e testa a conexão de link de dados é negociado. Um estado LCP de aberto significa que o LCP esteve terminado com sucesso, quando um estado LCP de fechado indicar uma falha do LCP.

Este diagrama mostra uma vista conceptual de um handshake de LCP:

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

Autenticação (fase opcional à revelia)

Nesta fase, a autenticação é executada com o protocolo de autenticação (RACHADURA ou PAP) concordado na negociação de LCP. Para a informação relacionada PAP, refira configurar e pesquisando defeitos o protocolo ppp password authentication (PAP).

Para a informação relacionada da RACHADURA, refira a compreensão e configurar da autenticação PPP chap.

Nota: A autenticação é opcional e o PPP incorpora somente esta fase se precisa de autenticar.

NCP (fase imperativa)

Esta fase é usada para estabelecer e configurar protocolos de camada de rede diferentes. O protocolo L3 mais comumente negociado é o IP. O Roteadores troca mensagens do protocolo de controle de IP (IPCP) para negociar as opções específicas ao protocolo (IP neste exemplo).

O RFC 1332 diz que o IPCP negocia duas opções: compressão e atribuições do endereço IP de Um ou Mais Servidores Cisco ICM NT. Contudo, o IPCP é usado igualmente para passar a

informação ligada à rede tal como server preliminares e alternativos do Windows Name Service (VITÓRIAS) e do Domain Name System (DNS).

A negociação ocorre com o uso dos mensagens CONF, como descrito nos pacotes de negociação PPP: Uma seção da descrição deste documento.

O Troubleshooting com debuga saídas de negociação ppp

Quando você lê o **comando debug ppp negotiation** output para propósitos de Troubleshooting, siga estas instruções:

1. Identifique as transições de fase no **comando debug**. Determine a fase a mais adicional a conexão conseguida, como ASCENDENTE ou a AUTENTICAÇÃO. Isto pode ajudá-lo a identificar a fase em que a conexão falhou. Para obter mais informações sobre das fases, veja as fases de seção da negociação de PPP.
2. Para a fase em que a falha ocorreu, procure as mensagens que indicam que o LCP, a autenticação, ou o NCP (como apropriado) são bem sucedidos:O estado 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 usa a autenticação em dois sentidos, a seguir cada transação deve ser bem sucedida. Para obter mais informações sobre das falhas de autenticação de PPP do Troubleshooting, refira a pesquisa de defeitos da autenticação PPP (RACHADURA 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 debugam saídas de negociação ppp

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

1. **O timestamp** — Os formatos de tempo de milisegundo são úteis. Veja a seção das condições prévias deste documento para mais informação.
2. **Relação e número de interface** — Este campo é útil quando debugar conexões múltiplas do uso das conexões, ou quando as transições de conexão através de diversas relações. Por exemplo, determinadas conexões (tais como chamadas multilink) são controladas pela interface física no início, mas controladas mais tarde pela interface do discador ou pela interface de acesso virtual.
3. **Tipo de mensagem PPP** — Este campo indica se a linha é um PPP, um LCP, uma RACHADURA, um PAP, ou um mensagem IPCP geral.
4. **Sentido da mensagem** — **Um I** indica um pacote recebido, e um **O** indica um pacote de saída. Este campo pode ser usado para determinar se a mensagem foi gerada ou recebida pelo roteador.
5. **Mensagem** — Este campo inclui a transação particular sob a negociação.
6. **ID** — Este campo é usado para combinar e coordenar mensagens request aos mensagens de resposta apropriados. Você pode usar o campo ID para associar uma resposta com um mensagem recebida. Esta opção é especialmente útil quando o mensagem recebida e a resposta estão afastadas no resultado do debug.
7. **Comprimento** — O campo de comprimento define o comprimento do campo de informação.

Este campo não é importante para o Troubleshooting geral.

Nota: Os campos 4 com 7 não podem aparecer em todos os mensagens PPP, segundo a finalidade da mensagem.

Nota: Este exemplo ilustra os campos:

Exemplo de saída de debug ppp negotiation

Isto é anotado uma descrição do **comando debug ppp negotiation** output:

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

Geral

CONFREQ (Configure-Request):

Quando a camada mais baixa se tornar disponível (acima), um CONFREQ está enviado para começar a primeira fase PPP (fase LCP). É usado em fases LCP e NCP como uma tentativa de configurar a conexão. Para abrir uma conexão ao par, o dispositivo transmite esta mensagem junto com as opções de configuração e avalia o remetente deseja o par apoiar. Todas as opções e valores são negociados simultaneamente. Se o par responde com um CONFREJ ou um mensagem de CONFNAK, a seguir o roteador envia um outro CONFREQ com um outro conjunto de opções ou valores.

CONFACK (Configurar-reconheça):

Se todas as opções no mensagem de CONFREQ são reconhecíveis e todos os valores são aceitáveis, a seguir o roteador transmite um mensagem CONFACK.

CONFREJ (configurar a rejeição):

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

CONFNAK (configurar o reconhecimento negativo):

Se a opção de configuração recebida é reconhecível e aceitável, mas algum valor não é aceitável, o roteador transmite um mensagem de 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 (requisição de eco) e ECHOREP (resposta de eco):

O PPP usa o Keepalives a fim manter a integridade da conexão. Este Keepalives é o echoreq frame que é enviado ao par remoto PPP, e o par remoto PPP deve responder com um quadro ECHOREP após recepção de um echoreq frame. À revelia, se o roteador falta cinco quadros ECHOREP, a seguir o link é considerado para baixo e o PPP é derrubado.

TERMREQ (Solicitação de término):

Este quadro indica que o par PPP que enviou este quadro termina a conexão PPP.

TERMACK (reconhecimento de terminação)

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

TERMINANDO

Esta mensagem indica que a conexão PPP esteve derrubada. Um LCP ou uma conexão NCP podem ser eliminados:

- no fim administrativo (LCP somente).
- 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 (mapa de caractere do controle assíncrono):

Essa é uma das opções negociadas para LCP dentro da estrutura CONFREQ. O ACCM ajusta as sequências de escape do caráter. O ACCM diz a porta para ignorar caráteres de controle especificados dentro do fluxo de dados. Se o roteador no outro extremo da conexão não apoia a negociação ACCM, a porta está forçada para usar o FFFFFFFF. Nesse caso, emita este comando:

```
ppp accm match 000a000
```

ACFC (compressão do endereço e do campo de controle):

O ACFC é uma opção de LCP que permita que os valores-limite enviem mensagens para a frente e para trás mais eficientemente.

AuthProto (protocolo de autenticação):

O AuthProto é o tipo de protocolo de autenticação negociado no frame CONFREQ entre ambos os pares da conexão PPP para o uso na fase de autenticação. Se nenhuma autenticação de PPP é configurada, esta saída não está considerada em parâmetros negociados frame CONFREQ. Os valores possíveis são CHAP ou PAP.

Rechamada “#”:

Esta mensagem indica que a opção de chamada de volta está sob a negociação. O número depois que a sintaxe de rechamada indica que opção de chamada de volta está negociada. O número 0 é callback PPP normal, quando o número 6 indicar a opção da rechamada Microsoft (que está automaticamente disponível no Software Release 11.3(2)T ou Mais Recente de Cisco IOS®).

RACHADURA (protocolo de autenticação de cumprimento do desafio):

Esta mensagem indica que o protocolo de autenticação sob a negociação é RACHADURA.

EndpointDisc (discriminador do ponto final):

Esta é uma opção de LCP usada para identificar um correspondente PPP em uma conexão PPP Multilink. Para mais informação, refira critérios nomeando conjuntos de PPP multilink.

LCP: O estado está aberto

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

LQM (monitoramento de qualidade de link)

O LQM está disponível em todas as interfaces serial que executam o PPP. O LQM monitora a qualidade do link e toma o link para baixo quando a qualidade deixa cair abaixo de um porcentagem configurada. As porcentagens são calculadas para os sentidos de entrada e saída. A qualidade contínua é calculada pela comparação do número total de pacotes e de bytes enviados com o número total de pacotes e de bytes recebidos pelo par. A qualidade recebida é calculada pela comparação do número total de pacotes e de bytes recebidos com o número total de pacotes e de bytes enviados pelo par.

Quando o LQM é permitido, os relatórios da qualidade do link (LQR) estão enviados cada período de keepalive. Os LQR são enviados no lugar do Keepalives. Todas as manutenções de atividade recebida são respondidas a corretamente. Se o LQM não é configurado, o Keepalives está enviado cada período de keepalive, e todos os LQR entrantes são respondidos com a um LQR.

MagicNumber

O apoio do número mágico está disponível em todas as interfaces serial. O PPP tenta sempre negociar para os números mágicos, que são usados para detectar redes do loop. Uma série aleatória é enviada através do link e se o mesmo valor é retornado, a seguir do roteador determina que o link é loop.

O link pôde ou não pôde ser tomado para baixo em cima da detecção do loop; depende do uso do comando down-when-looped.

PAP (protocolo password authentication)

Esta mensagem indica que o protocolo de autenticação sob a negociação para o uso dos pares PPP é PAP. Para obter mais informações sobre do PAP, refira configurar e pesquisando defeitos o protocolo ppp password authentication (PAP).

PFC (compactação de campo de protocolo)

Esta opção gerencie a compressão para o protocolo coloca qualquer um de ligar/desligar.

MRRU (máximo receba a unidade reconstruída)

Esta é uma opção de LCP negociada em processo da instalação do multilink de PPP LCP. Esta opção determina o máximo número de bytes que pode constituir um quadro. Se o MRRU não é negociado no LCP, a seguir o Multilink PPP (MPPP) não pode ser executado no link.

MRU (unidade máxima recebida)

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

Autenticação

AUTH-REQ (pedido de autenticação)

Este quadro é enviado do par local PPP (em que autenticação é permitida) ao peer remoto. Pede que o peer remoto envie um nome de usuário válido e uma senha para autenticação da conexão PPP. Este quadro é usado somente com PAP.

AUTH-ACK (a autenticação reconhece)

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. Este quadro é usado somente quando o PAP é usado para a autenticação de conexão PPP.

AUTH-NAK ou FALHA

Este quadro é mandado do par de autenticação PPP quando a autenticação falhou no par de autenticação PPP.

DESAFIO

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

RESPOSTA

Este quadro é a resposta da RACHADURA enviada do par autenticado PPP ao par de autenticação PPP.

A resposta necessária consiste em duas partes.

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

Este quadro é usado somente quando a RACHADURA é usada para a 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 é 0.0.0.0, a máquina local pede o par fornecê-lo um endereço IP de Um ou Mais Servidores Cisco ICM NT que pode se usar.
- Em um mensagem de CONFREQ entrante, este valor indica que o endereço IP de Um ou Mais Servidores Cisco ICM NT que o par deseja se usar. Se o endereço incluído é 0.0.0.0, as solicitações de peer a máquina local fornecê-lo um endereço IP de Um ou Mais Servidores Cisco ICM NT que possa se 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 um mensagem CONFACK recebido, este valor indica que o endereço IP de Um ou Mais Servidores Cisco ICM NT pedido pela máquina local é aceitável ao par.

CCP (protocolo compression control)

Esta mensagem indica que um protocolo de compactação está sob a negociação entre ambos os pares PPP. O Cisco IOS Software apoia estes protocolos de compactação a ser negociados sobre uma conexão PPP:

- Compressão do MS-Ponto-à-ponto (MS-PPC)
- empilhador
- predictor

CDPCP (protocolo de controle do protocolo cisco discovery)

Esta mensagem indica que a negociação CDP ocorre na fase NCP. Para desligar o CDP no roteador, emita o **comando no cdp run**.

CODEREJ (rejeição do código)

Um pacote CODEREJ é enviado após recepção de um uninterpretable embalado do par remoto

PPP.

Instale a rota a a.b.c.d

Quando o roteador terminar IPCP (fase NCP para o protocolo IP L3), deve-se instalar o endereço IP de Um ou Mais Servidores Cisco ICM NT dado ao par remoto PPP na tabela de roteamento e vê-lo como uma rota conectada na tabela de roteamento. Se você não vê esta mensagem, verifique que o **comando no peer neighbor-route** não está configurado.

IPCP (protocolo de controle de IP)

Este valor indica que o IP é a camada de rede sob a negociação na fase NCP.

O estado IPCP está aberto

Esta mensagem indica que o IPCP (fase NCP para o protocolo IP L3) esteve terminado com sucesso.

PROTREJ (rejeição do protocolo)

O par PPP, após recepção de um pacote PPP com um campo do protocolo desconhecido, usa o mensagem protrej para indicar que o par tentou usar um protocolo que seja unsupported. Quando um dispositivo PPP recebe um mensagem protrej, deve o mais cedo possível cessar 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