디버그 ppp 협상 출력 이해

목차

소개

다이얼 관련 애플리케이션에서 PPP는 가장 일반적으로 사용되는 캡슐화 유형입니다.PPP를 사용하면 포인트 투 포인트 통신 링크의 두 시스템에서 인증, 압축 및 IP와 같은 레이어 3(L3) 프로토콜에 대한 다양한 매개변수를 협상할 수 있습니다.두 라우터 간의 PPP 협상이 실패하면 연결이 실패합니다.

debug ppp **negotiation** 명령을 사용하면 PPP 협상 트랜잭션을 보고, 오류가 발생할 때 문제 또는 단계를 식별하고, 해결을 개발할 수 있습니다.그러나 debug ppp negotiation 명령 출력을 이해하는 것이 **필수적입니다**.이 문서에서는 debug ppp **negotiation** 명령 출력을 읽는 포괄적인 방법을 제공합니다.

사전 요구 사항

요구 사항

이 문서를 읽는 사람은 다음 조건을 충족해야 합니다.

- 두 라우터의 인터페이스에서 PPP를 활성화해야 합니다.이를 **수행하려면 encapsulation ppp** 명령을 실행합니다.

- 라우터에서 밀리초 타임스탬프를 활성화하려면 이 명령을 실행합니다.
  ```
  Router(config)# service timestamp debug datetime msec
  ```

  debug 명령에 대한 자세한 내용은 디버그 명령에 대한 중요 정보를 참조하십시오.

참고: PPP 함수에서 하위 레이어(ISDN, 물리적 인터페이스, 전화 접속 회선 등)가 완벽하게 작동하지 않는 한 두 피어 간의 PPP 협상이 시작될 수 없습니다.예를 들어 ISDN을 통해 PPP를 실행하려면 모든 ISDN 레이어가 작동해야 합니다.그렇지 않으면 PPP가 시작되지 않습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

PPP 협상의 단계

링크는 이 표에 표시된 것처럼 PPP 협상 프로세스의 여러 단계를 거칩니다.결과적으로 PPP가 작동 또는 다운된 상태입니다.

단계	설명
아래로	이 단계에서는 PPP가 다운되었습니다.이 메시지는 링크 및 PPP가 완전히 중단된 후에 표시됩니다. `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
설정	PPP는 물리적 레이어가 작동 중이고 사용할 준비가 되었다는 표시를 받으면 이 단계로 전환됩니다.LCP[1] 협상은 이 단계에서 발생합니다. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
인증	링크에서 PPP 인증(CHAP[2] 또는 PAP[3])을 원하는 경우 PPP가 이 단계로 전환됩니다.PPP 인증은 선택 사항이라는 점에 유의하십시오. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
위로	인증이 완료되면 PPP가 UP 단계로 전환됩니다.NCP[4] 협상은 이 단계에서 발생합니다. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
종료중	이 단계에서는 PPP가 종료됩니다. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

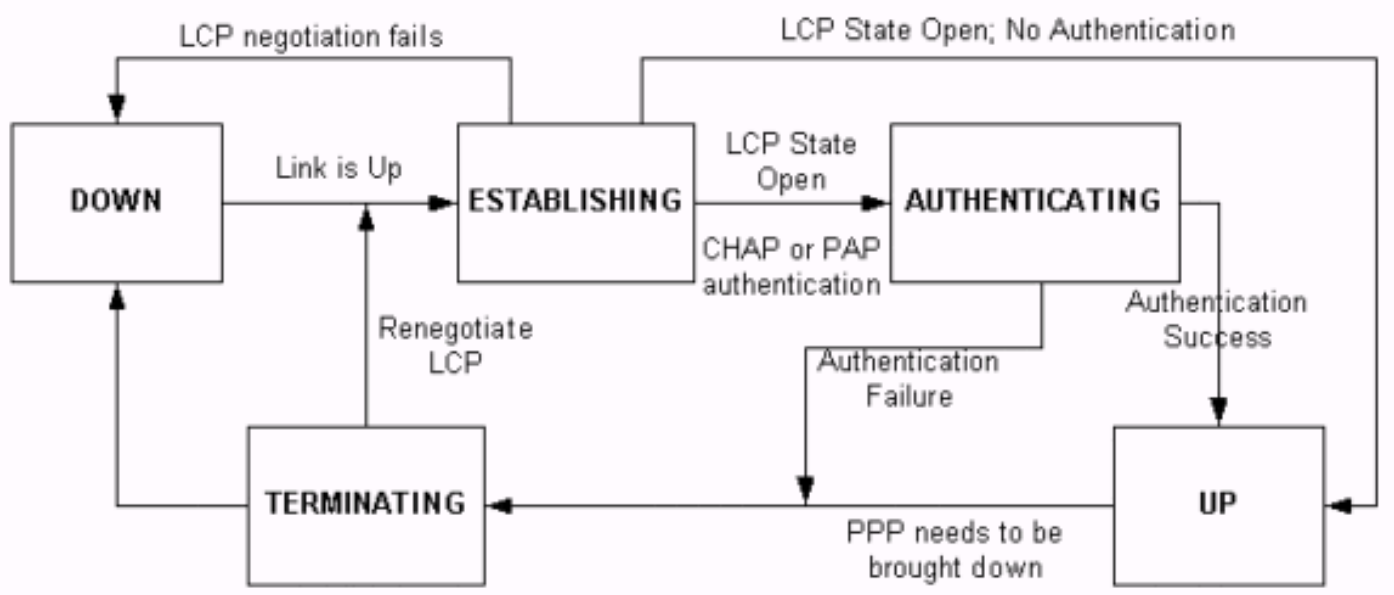
1. LCP = 링크 제어 프로토콜

2. CHAP = 챌린지 핸드셰이크 인증 프로토콜

3. PAP = 비밀번호 인증 프로토콜

4. NCP = 네트워크 제어 프로토콜

다음 다이어그램은 PPP 단계 전환을 보여줍니다.



PPP 협상 패킷:설명

이 테이블에는 LCP 및 NCP 협상 모두에서 사용되는 PPP 협상 패킷에 대한 설명이 포함됩니다.

패킷	코드	설명
콘프레크	구성 요청	피어에 대한 연결을 열려면 디바이스에서 컨피그레이션 옵션 및 값과 함께 이 메시지를 전송합니다. 발신자는 피어가 지원해야 합니다.모든 옵션과 값이 동시에 협상됩니다.피어가 CONFREJ 또는 CONFNAK 메시지로 응답하면 라우터는 다른 옵션 또는 값 집합과 함께 다른 CONFREQ를 전송합니다.
콘프레이	구성-거부	CONFREQ 메시지에서 수신한 일부 컨피그레이션 옵션을 사용할 수 없거나 인식할 수 없는 경우 라우터는 CONFREJ 메시지로 응답합니다.CONFREQ 메시지에서 허용되지 않는 옵션(CONFREQ 메시지의 옵션)이 CONFREJ 메시지에 포함됩니다.
컨나크	Configure-NAK[1]	수신된 컨피그레이션 옵션을 인식할 수 있고 허용하지만 일부 값이 허용되지 않으면 라우터가 CONNAK 메시지를 전송합니다.라우터는 피어가 다음 CONFREQ 메시지에 해당 옵션을 포함할 수 있도록 CONNAK 메시지에 수락할 수 있는 옵션 및 값을 추가합니다.
CONFACK	Configure-ACK[2]	CONFREQ 메시지의 모든 옵션을 인식할 수 있고 모든 값을 허용할 경우 라우터는 CONFACK 메시지를 전송합니다.
테레크	종료-요청	이 메시지는 LCP 닫기를 시작하는 데 사용됩니다.
테맥	종료-	이 메시지는 TERMREQ 메시지에 대한 응

	ACK	답으로 전송됩니다.

1. NAK = 음수 승인

2. ACK = 승인

참고: 각 피어는 피어가 지원하려는 옵션 또는 값으로 CONFREQ를 전송할 수 있습니다.따라서 각 방향으로 협상된 옵션이 다를 수 있습니다.예를 들어 한 쪽이 피어를 인증하고 다른 쪽은 인증하지 않을 수 있습니다.

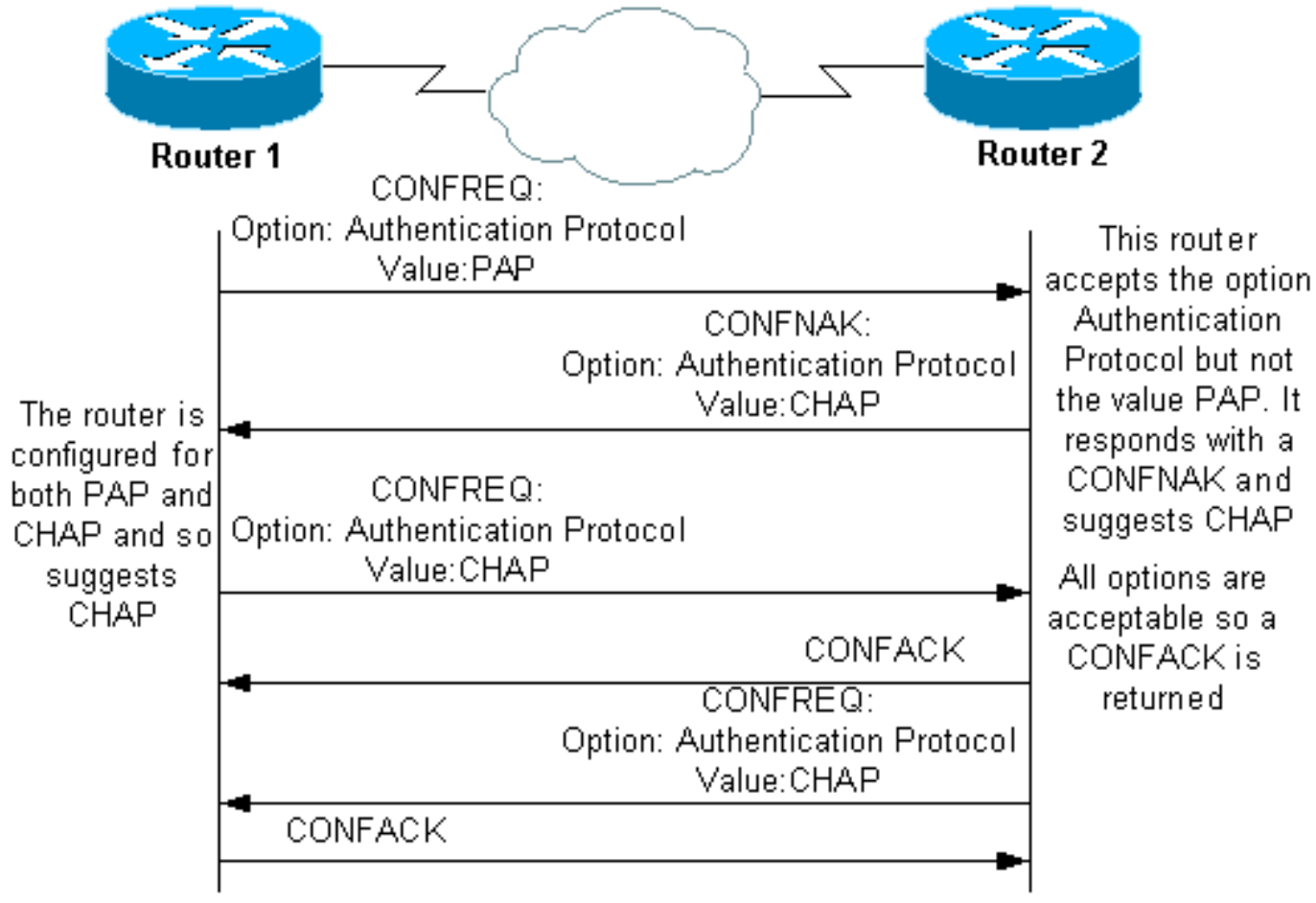
LCP, 인증 및 NCP 단계

앞서 설명한 일부 PPP 단계 내에서 PPP는 LCP 협상, 인증, NCP 협상 등과 같은 특정 단계로 이동합니다.자세한 내용은 RFC 1548 및 RFC 1661을 참조하십시오 .

LCP(필수 단계)

LCP는 데이터 링크 연결을 설정, 구성 및 테스트하는 매개변수가 협상되는 단계입니다.LCP 상태가 open이면 LCP가 성공적으로 완료되었음을 의미하고, LCP 상태가 closed이면 LCP 오류를 나타냅니다.

다음 다이어그램은 LCP 핸드셰이크의 개념적 보기를 보여줍니다.



LCP 협상에서는 MagicNumber라는 매개변수도 사용합니다. 이 매개변수는 링크가 다시 루프되었는지 확인하는 데 사용됩니다.임의의 문자열이 링크를 통해 전송되고, 동일한 값이 반환되면 라우터가 링크가 다시 반복되는 것으로 확인합니다.

인증(기본적으로 선택적 단계)

이 단계에서는 인증이 LCP 협상에서 동의한 인증 프로토콜(CHAP 또는 PAP)로 수행됩니다.PAP 관련 정보는 PPP PAP(Configuring and Troubleshooting PPP Password Authentication Protocol)를 참조하십시오.

CHAP 관련 정보는 PPP CHAP 인증 이해 및 구성을 참조하십시오.

참고: 인증은 선택 사항이며 PPP는 인증해야 하는 경우에만 이 단계로 들어갑니다.

NCP(필수 단계)

이 단계는 서로 다른 네트워크 레이어 프로토콜을 설정하고 구성하는 데 사용됩니다.가장 일반적인 L3 프로토콜은 IP입니다.라우터는 IPCP(IP Control Protocol) 메시지를 교환하여 프로토콜(이 예에서는 IP)에 해당하는 옵션을 협상합니다.

RFC 1332 에 따르면 IPCP는 두 가지 옵션을 협상합니다.압축 및 IP 주소 할당.그러나 IPCP는 기본 및 백업 WINS(Windows Name Service) 및 DNS(Domain Name System) 서버와 같은 네트워크 관련 정보를 전달하는 데에도 사용됩니다.

협상은 PPP 협상 패킷에 설명된 대로 CONF 메시지를 사용하여 발생합니다.이 문서의 설명 섹션입니다.

디버그 ppp 협상 출력 문제 해결

트러블슈팅을 위해 **debug ppp negotiation** 명령 출력을 읽을 때 다음 지침을 따르십시오.

1. **debug** 명령 출력에서 단계 전환을 식별합니다.UP 또는 AUTHENTICATING과 같이 연결이 달성한 가장 마지막 단계를 결정합니다.이렇게 하면 연결이 실패한 단계를 식별할 수 있습니다.단계에 대한 자세한 내용은 PPP 협상 단계 섹션을 참조하십시오.
2. 오류가 발생한 단계에 대해 LCP, 인증 또는 NCP(적절하게)가 성공했음을 나타내는 메시지를 찾습니다.LCP 상태가 열려 있어야 합니다.마지막 수신 및 발신 CONFACK 메시지를 확인하여 필요한 매개변수가 협상되었는지 확인할 수도 있습니다.인증에 성공해야 합니다.양방향 인증을 사용하는 경우 각 트랜잭션이 성공해야 합니다.PPP 인증 실패 문제 해결에 대한 자세한 내용은 PPP(CHAP 또는 PAP) 인증 문제 해결을 참조하십시오.IPCP 상태가 열려 있어야 합니다.주소 지정이 올바르고 피어에 대한 경로가 설치되어 있는지 확인합니다.

디버그 ppp 협상 출력 읽기

debug ppp **negotiation** 명령 출력의 대부분의 행은 다음과 같습니다.

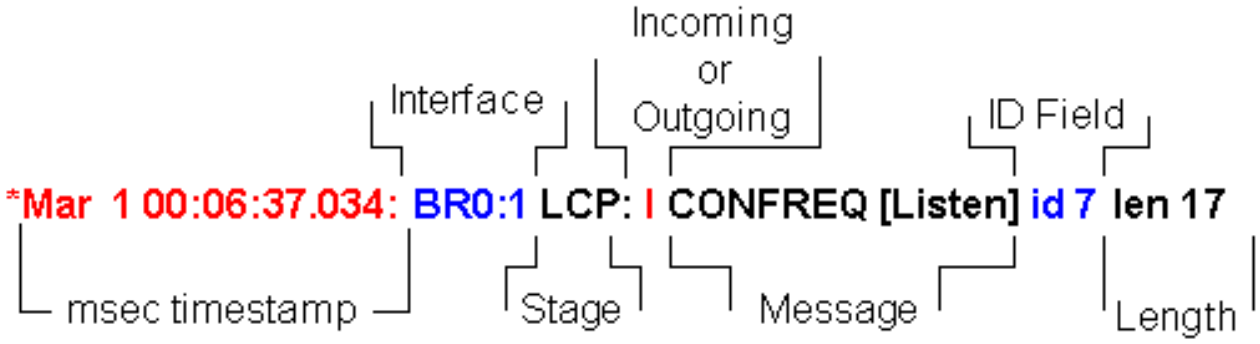
1. **타임스탬프**—밀리초 타임스탬프가 유용합니다.자세한 내용은 이 문서의 전제 조건 섹션을 참조하십시오.
2. **Interface and Interface number(인터페이스 및 인터페이스 번호)** - 이 필드는 디버그 연결에서 여러 연결을 사용하거나 여러 인터페이스를 통해 연결이 전환될 때 유용합니다.예를 들어, 멀티링크 호출과 같은 특정 연결은 처음에 물리적 인터페이스에 의해 제어되지만 나중에 다이얼러 인터페이스 또는 가상 액세스 인터페이스에 의해 제어됩니다.
3. **Type of PPP message(PPP 메시지 유형)** - 이 필드는 회선이 일반 PPP, LCP, CHAP, PAP 또

는 IPCP 메시지인지 여부를 나타냅니다.

4. **메시지 방향** - I는 수신 패킷을 나타내고 O는 발신 패킷을 나타냅니다.이 필드를 사용하여 라우터에서 메시지가 생성되었는지 또는 수신되었는지 확인할 수 있습니다.
5. **메시지** - 이 필드에는 협상 중인 특정 트랜잭션이 포함됩니다.
6. **ID** - 이 필드는 요청 메시지를 적절한 응답 메시지와 일치시키고 조정하는 데 사용됩니다.ID 필드를 사용하여 응답을 수신 메시지와 연결할 수 있습니다.이 옵션은 수신 메시지와 응답이 디버그 출력에서 멀리 떨어져 있는 경우 특히 유용합니다.
7. **길이** - 길이 필드는 정보 필드의 길이를 정의합니다.이 필드는 일반적인 문제 해결에 중요하지 않습니다.

참고: 메시지 목적에 따라 필드 4~7이 모든 PPP 메시지에 표시되지 않을 수 있습니다.

참고: 다음 예에서는 필드를 보여 줍니다.



샘플 디버그 ppp 협상 출력

다음은 debug ppp negotiation 명령 출력에 대한 주석이 있는 설명입니다.

```
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
```

용어집 및 공통 메시지

일반

CONFREQ(Configure-Request):

하위 레이어를 사용할 수 있게 되면(작동) CONFREQ가 전송되어 첫 번째 PPP 단계(LCP 단계)를 시작합니다. LCP 및 NCP 단계에서 연결을 구성하기 위한 시도로 사용됩니다.피어에 대한 연결을 열려면 디바이스에서 컨피그레이션 옵션 및 값과 함께 이 메시지를 전송합니다. 발신자는 피어가 지원해야 합니다.모든 옵션과 값이 동시에 협상됩니다.피어가 CONFREJ 또는 CONFNAK 메시지로 응답하면 라우터는 다른 옵션 또는 값 집합과 함께 다른 CONFREQ를 전송합니다.

CONFACK(구성-승인):

CONFREQ 메시지의 모든 옵션을 인식할 수 있고 모든 값을 허용할 경우 라우터는 CONFACK 메시지를 전송합니다.

CONFREJ(거부 구성):

CONFREQ에서 수신한 일부 컨피그레이션 옵션을 사용할 수 없거나 인식할 수 없는 경우 라우터는 CONFREJ 메시지로 응답합니다.허용되지 않는 옵션(CONFREQ에서)은 CONFREJ 메시지에 포함됩니다.

CONNAK(Configure Negative Acknowledge)(부정 승인 구성):

수신된 컨피그레이션 옵션을 인식할 수 있고 허용하지만 일부 값이 허용되지 않으면 라우터가 CONNAK 메시지를 전송합니다.라우터는 피어가 다음 CONFREQ 메시지에 해당 옵션을 포함할 수 있도록 CONNAK 메시지에 수락할 수 있는 옵션 및 값을 추가합니다.

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

PPP는 연결 무결성을 유지하기 위해 keepalive를 사용합니다.이러한 keepalive는 원격 PPP 피어로 전송되는 ECHOREQ 프레임이며 ECHOREQ 프레임을 수신하면 원격 PPP 피어가 ECHOREP 프레임으로 응답해야 합니다.기본적으로 라우터가 5개의 ECHOREP 프레임을 누락하면 링크가 다운된 것으로 간주되고 PPP가 다운됩니다.

TERMREQ(종료 요청):

이 프레임은 이 프레임을 보낸 PPP 피어가 PPP 연결을 종료함을 나타냅니다.

TERMACK(종료 승인):

이 메시지는 TERMREQ 메시지에 대한 응답으로 전송됩니다.이렇게 하면 PPP 연결이 닫힙니다.

종료 중

이 메시지는 PPP 연결이 해제되었음을 나타냅니다.LCP 또는 NCP 연결은 다음과 같이 차단될 수 있습니다.

- 관리 닫기(LCP만 해당)를 참조하십시오.
- 하위 수준이 서비스 중단되는 경우(전화 접속 회선, ISDN 등)
- 협상이 결렬될 때
- 온라인 루프 탐지

LCP

ACCM(비동기 제어 문자 맵):

CONFREQ 프레임 내에서 LCP 협상 옵션 중 하나입니다.ACCM은 문자 이스케이프 시퀀스를 설정합니다.ACCM은 데이터 스트림 내에서 지정된 제어 문자를 무시하도록 포트에 지시합니다.연결의 반대쪽에 있는 라우터가 ACCM 협상을 지원하지 않는 경우 포트는 FFFFFFFF를 사용해야 합니다.이 경우 다음 명령을 실행합니다.

```
ppp accm match 000a000
```

ACFC(주소 및 제어 필드 압축):

ACFC는 엔드포인트가 메시지를 보다 효율적으로 주고받을 수 있도록 하는 LCP 옵션입니다.

AuthProto(인증 프로토콜):

AuthProto는 인증 단계에서 사용하기 위해 두 PPP 연결 피어 간에 CONFREQ 프레임에서 협상된 인증 프로토콜 유형입니다.PPP 인증이 구성되지 않은 경우 이 출력은 CONFREQ 프레임 협상된 매개변수에 표시되지 않습니다.가능한 값은 CHAP 또는 PAP입니다.

콜백 "#":

이 메시지는 콜백 옵션이 협상 중임을 나타냅니다.콜백 구문 이후의 숫자는 협상되는 콜백 옵션을 나타냅니다.숫자 0은 일반 PPP 콜백이고 숫자 6은 Microsoft 콜백 옵션(Cisco IOS® Software Release 11.3(2)T 이상에서 자동으로 사용 가능)을 나타냅니다.

CHAP(챌린지 핸드셰이크 인증 프로토콜):

이 메시지는 협상 중인 인증 프로토콜이 CHAP임을 나타냅니다.

EndpointDisc(엔드포인트 판별자):

PPP 멀티링크 연결에서 PPP 피어를 식별하는 데 사용되는 LCP 옵션입니다.자세한 내용은 Naming Multilink PPP Bundles(멀티링크 PPP 번들 이름 지정 기준)를 참조하십시오.

LCP:상태가 열림

이 메시지는 LCP 협상이 성공적으로 완료되었음을 나타냅니다.

LQM(링크 품질 모니터링)

LQM은 PPP를 실행하는 모든 직렬 인터페이스에서 사용할 수 있습니다.LQM은 링크 품질을 모니터링하고 품질이 구성된 퍼센트 아래로 떨어지면 링크를 중단합니다.수신 방향과 발신 방향 모두에 대해 백분율이 계산됩니다.발신 품질은 피어가 수신한 총 패킷 및 바이트 수와 함께 전송된 총 패킷 및 바이트 수를 비교하여 계산됩니다.수신 품질은 피어가 보낸 총 패킷 및 바이트 수와 받은 총 패킷 수 및 바이트를 비교하여 계산됩니다.

LQM이 활성화된 경우 LQR(Link Quality Reports)은 keepalive 기간마다 전송됩니다.LQR은 keepalive 대신 전송됩니다.모든 수신 keepalive가 올바르게 응답합니다.LQM이 구성되지 않은 경우 keepalive는 모든 keepalive 기간이 전송되고 모든 수신 LQR이 LQR로 응답됩니다.

매직 넘버

Magic Number는 모든 직렬 인터페이스에서 지원됩니다.PPP는 루프백 네트워크를 탐지하는 데 사용되는 Magic Numbers에 대해 항상 협상을 시도합니다.임의의 문자열이 링크를 통해 전송되고 동일한 값이 반환되면 라우터가 링크가 다시 반복되는 것으로 확인합니다.

루프백 탐지 시 링크가 해제되거나 해제되지 않을 수도 있습니다.down-when-looted **명령**의 사용에 따라 달라집니다.

PAP(비밀번호 인증 프로토콜)

이 메시지는 PPP 피어에서 사용하기 위해 협상 중인 인증 프로토콜이 PAP임을 나타냅니다.PAP에 대한 자세한 내용은 PPP PAP(Configuring and Troubleshooting PPP Password Authentication Protocol)를 참조하십시오.

PFC(프로토콜 필드 압축)

이 옵션은 프로토콜 필드의 압축을 설정 또는 해제합니다.

MRRU(최대 수신 재구성된 단위)

이는 PPP 멀티링크 LCP 설정 과정에서 협상된 LCP 옵션입니다.이 옵션은 프레임을 구성할 수 있는 최대 바이트 수를 결정합니다.LCP에서 MRRU가 협상되지 않은 경우 링크에서 MPPP(Multilink PPP)를 실행할 수 없습니다.

MRU(최대 수신 단위)

MRU는 교환된 패킷의 크기를 협상하기 위해 CONFREQ 프레임에서 협상되는 LCP 옵션입니다.

인증

AUTH-REQ(인증 요청)

이 프레임은 로컬 PPP 피어(인증이 활성화됨)에서 원격 피어로 전송됩니다.원격 피어에 PPP 연결 인증을 위한 유효한 사용자 이름 및 비밀번호를 전송하도록 요청합니다.이 프레임은 PAP에서만 사용됩니다.

AUTH-ACK(인증 승인)

이 프레임은 인증된 PPP 피어에서 인증 PPP 피어로 전송됩니다.이 프레임은 유효한 사용자 이름과 비밀번호 쌍을 전달합니다.이 프레임은 PAP가 PPP 연결 인증에 사용되는 경우에만 사용됩니다.

인증-NAK 또는 실패

이 프레임은 인증 PPP 피어에서 인증이 실패했을 때 인증 PPP 피어에서 전송됩니다.

과제

인증 PPP 피어에서 인증된 PPP 피어로 전송되는 CHAP 챌린지 프레임입니다.챌린지 프레임은 ID, 임의의 번호, 로컬 통신 서버의 호스트 이름 또는 원격 디바이스의 사용자 이름으로 구성됩니다.이 프레임은 CHAP가 PPP 연결 인증에 사용되는 경우에만 사용됩니다.

응답

이 프레임은 인증된 PPP 피어에서 인증 PPP 피어로 전송되는 CHAP 응답입니다.

필요한 응답은 두 부분으로 구성됩니다.

- 공유 암호의 MD5 해시 출력입니다.
- 원격 디바이스의 호스트 이름 또는 원격 디바이스에 있는 사용자의 이름입니다.

이 프레임은 CHAP가 PPP 연결 인증에 사용되는 경우에만 사용됩니다.

NCP

주소 a.b.c.d

- 발신 CONFREQ 메시지에서 이 값은 로컬 라우터가 사용하려는 IP 주소를 나타냅니다.포함된 주소가 0.0.0.0이면 로컬 시스템은 피어에 사용할 수 있는 IP 주소를 제공하도록 요청합니다.
- 수신 CONFREQ 메시지에서 이 값은 피어가 사용하려는 IP 주소를 나타냅니다.포함된 주소가 0.0.0.0인 경우 피어는 로컬 시스템에 사용할 수 있는 IP 주소를 제공하도록 요청합니다.
- 발신 CONNAK 메시지에서 이 값은 CONFREQ 메시지에서 피어가 제안한 IP 주소가 아니라 피어가 사용해야 하는 IP 주소를 나타냅니다.
- 수신 CONNAK 메시지에서 이 값은 이전 CONFREQ 메시지에서 제안한 IP 주소 대신 로컬 시스템에서 사용해야 하는 IP 주소를 나타냅니다.
- 발신 CONFACK 메시지에서 이 값은 피어가 요청한 IP 주소가 로컬 시스템에서 허용됨을 나타냅니다.
- 수신 CONFACK 메시지에서 이 값은 로컬 시스템에서 요청한 IP 주소가 피어에서 허용됨을 나타냅니다.

CCP(압축 제어 프로토콜)

이 메시지는 두 PPP 피어 간에 압축 프로토콜이 협상 중임을 나타냅니다.Cisco IOS Software는 PPP 연결을 통해 협상되는 다음과 같은 압축 프로토콜을 지원합니다.

- MS-Point-to-Point 압축(MS-PPC)
- 스태커
- 예측자

CDPCP(Cisco Discovery Protocol Control Protocol)

이 메시지는 CDP 협상이 NCP 단계에서 발생함을 나타냅니다.라우터에서 CDP를 끄려면 **no cdp run** 명령**을** 실행합니다.

CODEREJ(코드 거부)

원격 PPP 피어에서 비 통역 가능한 패킷을 받으면 CODEREJ 패킷이 전송됩니다.

a.b.c.d에 대한 경로 설치

라우터가 IPCP(IP L3 프로토콜의 NCP 단계)를 완료하면 라우팅 테이블의 원격 PPP 피어에 지정된 IP 주소를 설치해야 하며 라우팅 테이블에서 연결된 경로로 간주됩니다.이 메시지가 표시되지 않으면 **no peer neighbor-route** 명령이 구성되지 않았는지 확인합니다.

IPCP(IP 제어 프로토콜)

이 값은 IP가 NCP 단계에서 협상 중인 네트워크 계층임을 나타냅니다.

IPCP 상태가 열림

이 메시지는 IP L3 프로토콜의 IPCP(NCP 단계)가 성공적으로 완료되었음을 나타냅니다.

PROTREJ(프로토콜 거부)

알 수 없는 프로토콜 필드가 있는 PPP 패킷을 수신한 PPP 피어는 PROTREJ 메시지를 사용하여 피어가 지원되지 않는 프로토콜을 사용하려고 시도했음을 나타냅니다.PPP 디바이스가 PROTREJ 메시지를 수신할 경우, 지정된 프로토콜의 패킷 전송을 중지할 수 있는 빠른 기회가 종료되어야 합니다.

관련 정보

- PPP PAP(Password Authentication Protocol) 구성 및 문제 해결
- PPP 인증 ppp chap 호스트 이름 및 ppp 인증 chap 호출 명령 사용
- PPP CHAP 인증 이해 및 구성
- PPP(CHAP 또는 PAP) 인증 문제 해결
- 다이얼 기술 지원 페이지
- Technical Support - Cisco Systems