PPP PAP(Password Authentication Protocol) 구성 및 문제 해결

목차

소개

PPP(Point-to-Point Protocol)는 현재 두 가지 인증 프로토콜을 지원합니다.PAP(Password Authentication Protocol) 및 CHAP(Challenge Handshake Authentication Protocol) 입니다. 둘 다 RFC 1334에 지정되며 동기 및 비동기 인터페이스에서 지원됩니다.

- PAP는 양방향 핸드셰이크를 사용하여 원격 노드의 ID를 설정하는 간단한 방법을 제공합니다 .PPP 링크 설정 단계가 완료되면 인증이 승인될 때까지 또는 연결이 종료될 때까지 사용자 이름 및 비밀번호 쌍은 링크(일반 텍스트)를 통해 원격 노드에서 반복적으로 전송됩니다.
- PAP는 보안 인증 프로토콜이 아닙니다.비밀번호는 일반 텍스트로 링크를 통해 전송되며 재생 또는 시도/오류 공격으로부터 보호되지 않습니다.원격 노드가 로그인 시도 빈도와 타이밍을 제어합니다.

PAP 또는 CHAP를 사용하여 PPP 인증 문제 해결에 대한 자세한 내용은 PPP 인증 단계 문제 해결을 위한 전체 단계별 순서도에 대한 PPP(CHAP 또는 PAP) 인증 문제 해결을 참조하십시오.모든 PPP 단계(LCP, Authentication, NCP) 문제 해결에 대한 자세한 내용은 모든 관련 PPP 단계 및 협상

된 매개 변수에 대한 단계별 문제 해결을 위한 완전한 순서도를 보려면 PPP 문제 해결 순서도를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

배경 정보

CHAP는 사용자 암호를 연결 간에 보내지 않으므로 더 안전한 것으로 간주됩니다.CHAP에 대한 자세한 내용은 PPP CHAP 인증 이해 및 구성을 참조하십시오.

PAP는 단점에도 불구하고 다음 환경에서 사용할 수 있습니다.

- CHAP를 지원하지 않는 클라이언트 애플리케이션의 대규모 설치 기반
- CHAP의 여러 공급업체 구현 간 비호환성
- 원격 호스트에서 로그인을 시뮬레이션하기 위해 일반 텍스트 비밀번호를 사용해야 하는 상황

단방향 및 양방향 인증

대부분의 인증 유형과 마찬가지로 PAP는 양방향(양방향) 및 단방향(단방향) 인증을 지원합니다.단방향 인증을 사용하는 경우 통화 수신 측(NAS)만 원격 측(클라이언트)을 인증합니다. 원격 클라이언트가 서버를 인증하지 않습니다.

양방향 인증에서는 각 측에서 독립적으로 인증 요청(AUTH-REQ)을 전송하고 인증 승인(AUTH-ACK) 또는 인증되지 않음(AUTH-NAK)을 수신합니다. debug ppp authentication **명령**을 사용하면 이러한 **명령을 볼** 수 **있습니다**.클라이언트에서 이 디버그의 예는 다음과 같습니다.

```
*Mar  6 19:18:53.322: BR0:1 PAP: O AUTH-REQ id 7 len 18 from "PAPUSER"
 ! --- Outgoing PAP AUTH-REQ. We are sending out our username (PAPUSER)and password ! --- to the
NAS. The NAS will verify that the username/password is correct. *Mar 6 19:18:53.441: BR0:1 PAP:
I AUTH-ACK id 7 Len 5
! --- Incoming AUTH-ACK. ! --- The NAS verified the username and password and responded with an
AUTH-ACK. ! --- One-way authentication is complete at this point. *Mar 6 19:18:53.445: BR0:1
PAP: I AUTH-REQ id 1 Len 14 from "NAS"
 ! --- Incoming AUTH-REQ from the NAS. This means we now verify the identity of the NAS. *Mar 6
19:18:53.453: BR0:1 PAP: Authenticating peer NAS
! --- Performing a lookup for the username (NAS) and password. *Mar 6 19:18:53.457: BR0:1 PAP: O
AUTH-ACK id 1 Len 5
```

! --- Outgoing AUTH-ACK. ! --- We have verified the username/password of the NAS and responded with an AUTH-ACK. ! --- Two-way authentication is complete.

위의 디버그 출력에서 인증은 양방향 입니다.그러나 단방향 인증이 구성된 경우 처음 두 개의 디버그 라인만 표시됩니다.

구성 명령

아래 설명된 일반 PAP 인증에 필요한 세 가지 명령이 있습니다.

ppp 인증 pap [callin]

ppp authentication pap **명령**이 **구성된** 라우터는 PAP를 사용하여 다른 쪽(피어)의 ID를 확인합니다. 즉, 다른 쪽(피어)은 확인을 위해 로컬 디바이스에 사용자 이름/비밀번호를 제공해야 합니다.

callin 옵션에서는 ppp authentication pap callin **명령이 구성된 라우터가 수신 통화** 중에 다른 쪽만 인증한다고 말합니다.발신 통화의 경우 다른 쪽을 인증하지 않습니다.즉, 통화를 시작하는 라우터가 다른 쪽에서 인증(AUTH-REQ)을 요청하지 않아도 됩니다

다음 표는 통화 옵션을 구성하는 시기를 **보여줍니다**.

인증 유형	클라이언트(통화 중)	NAS(수신자)
단방향	ppp 인증 pap 호출	ppp 인증 pap
양방향	ppp 인증 pap	ppp 인증 pap

username <username> password <password>

로컬 라우터가 PPP 피어를 인증하기 위해 사용하는 사용자 이름 및 비밀번호입니다.피어가 PAP 사용자 이름 및 비밀번호를 전송하면 로컬 라우터는 해당 사용자 이름과 비밀번호가 로컬에서 구성되었는지 확인합니다.일치하는 결과가 있으면 피어가 인증됩니다.

참고: PAP에 대한 username 명령의 기능은 CHAP에 대한 기능과 다릅니다.CHAP에서는 이 사용자 이름과 암호를 사용하여 챌린지에 대한 응답을 생성하지만, PAP는 이를 사용하여 수신 사용자 이름과 비밀번호가 올바른지 확인합니다.

단방향 인증의 경우 이 명령은 호출된 라우터에서만 필요합니다.양방향 인증의 경우 이 명령은 양쪽에서 필요합니다.

PPP pap sent-username <username> password <password>

아웃바운드 PAP 인증을 활성화합니다.로컬 라우터는 ppp pap sent-username **명령**에 의해 지정된 사용자 이름 및 비밀번호**를** 사용하여 원격 디바이스에 자신을 인증합니다.다른 라우터에는 위에서 설명한 **username** 명령을 사용하여 구성된 것과 동일한 사용자 이름/비밀번호가 있어야 합니다.

단방향 인증을 사용하는 경우 이 명령은 통화를 시작하는 라우터에서만 필요합니다.양방향 인증의 경우 이 명령은 양쪽에서 구성해야 합니다.

컨피그레이션 예시

다음 컨피그레이션 섹션에서는 단방향 인증 시나리오에 필요한 PAP 명령을 보여줍니다.

참고: 컨피그레이션의 관련 섹션만 표시됩니다.

발신자(클라이언트) 컨피그레이션

```
interface BRI0
! --- BRI interface for the dialout. ip address negotiated encapsulation ppp
! --- Use PPP encapsulation. This command is a required for PAP. dialer string 3785555 class 56k
! --- Number to dial for the outgoing connection. dialer-group 1 isdn switch-type basic-ni isdn
spid1 51299611110101 9961111 isdn spid2 51299622220101 9962222  ppp authentication pap callin
! --- Use PAP authentication for incoming calls. ! --- The callin keyword has made this a one-
way authentication scenario. ! --- This router (client) will not request that the peer (server)
authenticate ! --- itself back to the client. ppp pap sent-username PAPUSER password 7
```

```
! --- Permit outbound authentication of this router (client) to the peer. ! --- Send a PAP AUTH-
REQ packet to the peer with the username PAPUSER and password. ! --- The peer must have the
username PAPUSER and password configured on it.
```

수신 측(서버) 컨피그레이션

```
username PAPUSER password 0 cisco
! --- Username PAPUSER is the same as the one sent by the client. ! --- Upon receiving the AUTH-
REQ packet from the client, we will verify that the ! --- username and password match the one
configured here. interface Serial0:23 ! --- This is the D-channel for the PRI on the access
server receiving the call. ip unnumbered Ethernet0 no ip directed-broadcast  encapsulation ppp
! --- Use PPP encapsulation. This command is a required for PAP. dialer-group 1 isdn switch-type
primary-ni isdn incoming-voice modem peer default ip address pool default fair-queue 64 256 0
ppp authentication pap
! --- Use PAP authentication for incoming calls. ! --- This router (server) will request that
the peer authenticate itself to us. ! --- Note: the callin option is not used as this router is
not initiating the call.
```

디버그 출력

PPP PAP 문제를 디버깅하려면 debug ppp negotiation 및 **debug ppp authentication 명령을** 사용합니다.주의해야 할 두 가지 주요 문제는 다음과 같습니다.

1. 양측이 PAP가 인증 방법이라는 데 동의합니까?
2. 그렇다면 PAP 인증이 성공합니까?

이러한 질문에 올바르게 대답하는 방법에 대한 자세한 내용은 아래 디버그를 참조하십시오.또한 PPP 인증을 포함하여 다른 PPP 단계 동안 상대적인 의미와 함께 서로 다른 모든 디버깅 라인에 대한 설명은 디버그 ppp 협상 출력 이해를 참조하십시오.이 문서는 PPP 협상 실패의 원인을 신속하게 파악하는 데 유용합니다.PAP 또는 CHAP를 사용하여 PPP 인증 문제 해결에 대한 자세한 내용은 PPP 인증 단계 문제 해결을 위한 전체 단계별 순서도에 대한 PPP(CHAP 또는 PAP) 인증 문제 해결을 참조하십시오.

성공적인 단방향 PAP 인증을 위한 발신측(클라이언트) 디버그

```
maui-soho-01#show debug
PPP:
  PPP authentication debugging is on
```

```
  PPP protocol negotiation debugging is on
maui-soho-01#ping 172.22.53.144

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.53.144, timeout is 2 seconds:

*Mar  6 21:33:26.412: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
*Mar  6 21:33:26.432: BR0:1 PPP: Treating connection as a callout
*Mar  6 21:33:26.436: BR0:1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0 load]
*Mar  6 21:33:26.440: BR0:1 PPP: No remote authentication for call-out
! --- The client will not authenticate the server for an outgoing call. ! --- Remember this is a
one-way authentication example. *Mar 6 21:33:26.444: BR0:1 LCP: O CONFREQ [Closed] id 82 Len 10
*Mar  6 21:33:26.448: BR0:1 LCP:    MagicNumber 0x2F1A7C63 (0x05062F1A7C63)
! --- Outgoing CONFREQ (CONFigure-REQuest). ! --- Notice that we do not specify an
authentication method, ! --- since only the peer will authenticate us. *Mar 6 21:33:26.475:
BR0:1 LCP: I CONFREQ [REQsent] id 13 Len 14
*Mar  6 21:33:26.479: BR0:1 LCP:    AuthProto PAP (0x0304C023)
! --- Incoming LCP CONFREQ (Configure-Request) indicating that ! --- the peer(server) wishes to
use PAP. *Mar 6 21:33:26.483: BR0:1 LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B) *Mar 6
21:33:26.491: BR0:1 LCP: O CONFACK [REQsent] id 13 Len 14
*Mar  6 21:33:26.495: BR0:1 LCP:    AuthProto PAP (0x0304C023)
! --- This shows the outgoing LCP CONFACK (CONFigure-ACKnowledge) indicating that ! --- the
client can do PAP. *Mar 6 21:33:26.499: BR0:1 LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B) *Mar
6 21:33:26.511: BR0:1 LCP: I CONFACK [ACKsent] id 82 Len 10 *Mar 6 21:33:26.515: BR0:1 LCP:
MagicNumber 0x2F1A7C63 (0x05062F1.A7C63) *Mar 6 21:33:26.519: BR0:1 LCP: State is Open
! --- This shows LCP negotiation is complete. *Mar 6 21:33:26.523: BR0:1 PPP: Phase is
AUTHENTICATING, by the peer [0 sess, 0 load]
! --- The PAP authentication (by the peer) begins. *Mar 6 21:33:26.531: BR0:1 PAP: O AUTH-REQ id
20 Len 18 from "PAPUSER"
 ! --- The client sends out a PAP AUTH-REQ with username PAPUSER. ! --- This username is
configured with the ppp pap sent-username command. *Mar 6 21:33:26.555: BR0:1 PAP: I AUTH-ACK id
20 Len 5
! --- The Peer responds with a PPP AUTH-ACK, indicating that ! --- it has successfully
authenticated the client.
```

성공적인 단방향 PAP 인증을 위해 호출된 사이드(서버) 디버그

```
maui-nas-06#show debug
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
maui-nas-06#
*Jan  3 14:07:57.872: %LINK-3-UPDOWN: Interface Serial0:4, changed state to up
*Jan  3 14:07:57.876: Se0:4 PPP: Treating connection as a callin
! --- Since the connection is incoming, we will authenticate the client. *Jan 3 14:07:57.876:
Se0:4 PPP: Phase is ESTABLISHING, Passive Open *Jan 3 14:07:57.876: Se0:4 LCP: State is Listen
*Jan 3 14:07:58.120: Se0:4 LCP: I CONFREQ [Listen] id 83 Len 10 *Jan 3 14:07:58.120: Se0:4 LCP:
MagicNumber 0x2F319828 (0x05062F319828) *Jan 3 14:07:58.124: Se0:4 LCP: O CONFREQ [Listen] id 13
Len 14
*Jan  3 14:07:58.124: Se0:4 LCP:    AuthProto PAP (0x0304C023)
! --- Outgoing CONFREQ (Configure-Request) ! --- use PAP for the peer authentication. *Jan 3
14:07:58.124: Se0:4 LCP: MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9) *Jan 3 14:07:58.124: Se0:4 LCP:
O CONFACK [Listen] id 83 Len 10 *Jan 3 14:07:58.124: Se0:4 LCP: MagicNumber 0x2F319828
(0x05062F319828) *Jan 3 14:07:58.172: Se0:4 LCP: I CONFACK [ACKsent] id 13 Len 14
*Jan  3 14:07:58.172: Se0:4 LCP:    AuthProto PAP (0x0304C023)
! --- This shows the incoming LCP CONFACK (Configure-Acknowledge) indicating that ! --- the
client can do PAP. *Jan 3 14:07:58.172: Se0:4 LCP: MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9) *Jan
3 14:07:58.172: Se0:4 LCP: State is Open *Jan 3 14:07:58.172: Se0:4 PPP: Phase is
AUTHENTICATING, by this end
! --- The PAP authentication (by this side) begins. *Jan 3 14:07:58.204: Se0:4 PAP: I AUTH-REQ
id 21 Len 18 from "PAPUSER"
! --- Incoming AUTH-REQ from the peer. This means we must now verify ! --- the identity of the
peer. *Jan 3 14:07:58.204: Se0:4 PPP: Phase is FORWARDING *Jan 3 14:07:58.204: Se0:4 PPP: Phase
```

```
is AUTHENTICATING *Jan 3 14:07:58.204: Se0:4 PAP: Authenticating peer PAPUSER
! --- Performing a lookup for the username (PAPUSER) and password. *Jan 3 14:07:58.208: Se0:4
PAP: O AUTH-ACK id 21 Len 5 ! --- This shows the outgoing AUTH-ACK. ! --- We have verified the
username and password and responded with an AUTH-ACK. ! --- One-way authentication is complete.
```

PAP 문제 해결

PAP를 트러블슈팅할 때 Debug Output(디버그 출력) 섹션에 나와 있는 동일한 질문에 답합니다.

1. 양측이 PAP가 인증 방법이라는 데 동의합니까?
2. 그렇다면 PAP 인증이 성공합니까?

PAP 또는 CHAP를 사용하여 PPP 인증 문제 해결에 대한 자세한 내용은 PPP 인증 단계 문제 해결을 위한 전체 단계별 순서도에 대한 PPP(CHAP 또는 PAP) 인증 문제 해결을 참조하십시오.

양측이 인증 프로토콜로서 PAP에 동의하지 않음

특정 컨피그레이션에서는 양쪽이 PAP에 인증 프로토콜로 동의하지 않거나 CHAP에 대해 동의하지 않음을 확인할 수 있습니다(PAP를 원할 때). 이러한 문제를 해결하려면 다음 단계를 수행하십시오.

1. 통화를 수신하는 라우터에 다음 인증 명령 중 하나가 있는지 확인합니다.

```
ppp authentication pap
       or
ppp authentication pap chap
       or
ppp authentication chap pap
```

2. 통화를 하는 라우터에 ppp 인증 pap 통화가 구성되어 있는지 확인합니다.
3. 발신측에 ppp pap sent-username *username password 비밀번호*가 올바르게 구성되었는지 확인합니다. 여기서 사용자 이름과 비밀번호는 수신 라우터에 구성된 비밀번호와 일치됩니다.
4. 발신 라우터의 인터페이스 컨피그레이션 모드에서 ppp chap refuse 명령을 구성합니다.Cisco 라우터는 기본적으로 CHAP를 인증 프로토콜로 승인합니다.클라이언트가 PAP를 수행하려고 하지만 액세스 서버가 PAP 또는 CHAP(ppp 인증 chap pap가 구성된 PPP)를 수행할 수 있는 경우, ppp chap refuse 명령을 사용하여 클라이언트가 인증 프로토콜로 PAP를 수락하도록 할 수 있습니다.

```
maui-soho-01(config)#interface BRI 0
maui-soho-01(config-if)#ppp chap refuse
```

PAP 인증 실패

양측이 인증 프로토콜로 PAP에 동의하지만 PAP 연결이 실패하면 사용자 이름/비밀번호 문제가 발생할 가능성이 높습니다.

1. 발신측에 ppp pap sent-username *username* password *비밀번호가* 올바르게 구성되었는지 확인합니다. 여기서 사용자 이름과 비밀번호는 수신 라우터에 구성된 비밀번호와 일치됩니다.
2. 양방향 인증의 경우 수신 측에서 명령 ppp pap sent-username *username* password *password가* 올바르게 구성되었는지 확인합니다. 여기서 사용자 이름과 비밀번호는 호출 라우터에 구성된 비밀번호와 일치됩니다.양방향 인증을 수행할 때 ppp pap sent-username *username* password *password* 명령이 수신 라우터에 없고 PPP 클라이언트가 서버를 원격으로 인증하려고 시도하는 경우 debug ppp 협상(또는 ppp debug authentication)의 출력이 표시

됩니다.

```
*Jan  3 16:47:20.259: Se0:1 PAP: Failed request for PAP credentials.  Username maui-nas-06
```

이 오류 메시지는 컨피그레이션 문제를 나타내며 보안 침해일 필요는 없습니다.

3. 3. 사용자 이름 및 비밀번호가 피어에서 **ppp pap sent-username** ***username*** **password** ***비밀번호에*** 구성된 것과 일치하는지 확인합니다.일치하지 않으면 다음 메시지가 표시됩니다.

```
*Jan  3 17:18:57.559: Se0:3 PAP: I AUTH-REQ id 25 Len 18 from "PAPUSER"
*Jan  3 17:18:57.559: Se0:3 PPP: Phase is FORWARDING
*Jan  3 17:18:57.559: Se0:3 PPP: Phase is AUTHENTICATING
*Jan  3 17:18:57.559: Se0:3 PAP: Authenticating peer PAPUSER
*Jan  3 17:18:57.559: Se0:3 PAP: O AUTH-NAK id 25 Len 32 msg is
 "Password validation failure"
! --- This is an outgoing AUTH-NAK. This means that the mismatch occurred ! --- on this
router. Verify that the username and password configured locally is ! --- identical to that
on the peer.
```

관련 정보

- 인증 구성
- PPP 문제 해결 순서도
- PPP(CHAP 또는 PAP) 인증 문제 해결
- 디버그 ppp 협상 출력 이해
- PPP 인증 ppp chap 호스트 이름 및 ppp 인증 chap 호출 명령 사용
- 전화 접속 기술:개요 및 설명
- 기술 지원 및 문서 – Cisco Systems