

PPP 인증 ppp chap 호스트 이름 및 ppp 인증 chap 호출 명령 사용

목차

[소개](#)

[사전 요구 사항](#)

[표기 규칙](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 이론](#)

[구성](#)

[단방향 CHAP 인증 구성](#)

[라우터 이름과 다른 사용자 이름 구성](#)

[네트워크 다이어그램](#)

[구성](#)

[구성 설명](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[디버그 출력 샘플](#)

[관련 정보](#)

[소개](#)

PPP 협상에는 LCP(Link Control Protocol) 협상, 인증, NCP(Network Control Protocol) 협상과 같은 여러 단계가 포함됩니다. 양측이 올바른 매개변수에 동의할 수 없으면 연결이 종료됩니다. 링크가 설정되면 LCP 협상 중에 결정된 인증 프로토콜을 사용하여 양측이 서로를 인증합니다. NCP 협상을 시작하기 전에 인증이 성공해야 합니다.

PPP는 두 가지 인증 프로토콜을 지원합니다. PAP>Password Authentication Protocol) 및 CHAP(Challenge Handshake Authentication Protocol)입니다.

[사전 요구 사항](#)

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

[요구 사항](#)

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 11.2 이상

배경 이론

PAP 인증에는 사용자 이름과 비밀번호가 일반 텍스트로 링크를 통해 전송되는 양방향 핸드셰이크가 포함됩니다. 따라서 PAP 인증은 재생 및 회선 스니핑을 차단하지 않습니다.

반면 CHAP 인증은 3방향 핸드셰이크를 사용하여 원격 노드의 ID를 주기적으로 확인합니다. PPP 링크가 설정되면 호스트는 원격 노드에 "과제" 메시지를 보냅니다. 원격 노드는 단방향 해시 함수를 사용하여 계산된 값으로 응답합니다. 호스트는 예상 해시 값에 대한 자체 계산과 비교하여 응답을 확인합니다. 값이 일치하면 인증이 승인됩니다. 그렇지 않으면 연결이 종료됩니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에서 사용되는 명령에 대한 추가 정보를 찾으려면 IOS 명령 조회 도구를 사용하십시오.

단방향 CHAP 인증 구성

일반적으로 두 개의 디바이스가 CHAP 인증을 사용하는 경우, 각 쪽은 다른 쪽이 응답하고 챌린저에 의해 인증되는 문제를 보냅니다. 양측은 서로 독립적으로 인증한다. 발신 라우터 또는 디바이스의 인증을 지원하지 않는 비 Cisco 라우터로 작동하려면 `ppp authentication chap callin` 명령을 사용해야 합니다. `callin` 키워드와 함께 `ppp authentication` 명령을 사용할 경우, 원격 디바이스가 통화를 시작한 경우(예: 원격 디바이스가 "콜인"인 경우), 액세스 서버는 원격 디바이스만 인증합니다. 이 경우 수신(수신) 통화에만 인증이 지정됩니다.

라우터 이름과 다른 사용자 이름 구성

원격 Cisco 라우터가 다른 관리 제어, 인터넷 서비스 공급자(ISP) 또는 중앙 라우터 로터리의 Cisco 또는 비 Cisco 중앙 라우터에 연결되는 경우 호스트 이름과 다른 인증 사용자 이름을 구성해야 합니다. 이 경우 라우터의 호스트 이름이 제공되지 않거나 다른 시간(회전)에 다릅니다. 또한 ISP에서 할당된 사용자 이름과 비밀번호는 원격 라우터의 호스트 이름이 아닐 수 있습니다. 이 경우 `ppp chap hostname` 명령은 인증에 사용할 대체 사용자 이름을 지정하는 데 사용됩니다.

예를 들어, 여러 원격 디바이스가 중앙 사이트로 다이얼하는 상황을 가정해보겠습니다. 일반 CHAP 인증을 사용하면 각 원격 디바이스의 사용자 이름(호스트 이름일 수 있음)과 공유 암호를 중앙 라우터에 구성해야 합니다. 이 시나리오에서는 중앙 라우터의 컨피그레이션이 관리 시간이 오래 걸리고 번거로울 수 있습니다. 그러나 원격 디바이스가 호스트 이름과 다른 사용자 이름을 사용하는 경우 이를 방지할 수 있습니다. 중앙 사이트는 단일 사용자 이름과 공유 암호를 사용하여 구성할 수 있으며, 이 암호를 사용하여 여러 다이얼인 클라이언트를 인증할 수 있습니다.

네트워크 다이어그램

라우터 1이 라우터 2에 대한 통화를 시작하면 라우터 2가 라우터 1에 도전하지만 라우터 1은 라우터 2에 도전하지 않습니다. 이 문제는 라우터 1에서 **ppp authentication chap callin** 명령이 구성되어 있기 때문입니다. 단방향 인증의 예입니다.

이 설정에서 **ppp chap hostname alias-r1** 명령은 라우터 1에 구성됩니다. 라우터 1은 "r1" 대신 CHAP 인증을 위한 호스트 이름으로 "alias-r1"을 사용합니다. 라우터 2 다이얼러 맵 이름은 라우터 1의 **ppp chap** 호스트 이름과 일치해야 합니다. 그렇지 않으면 각 방향에 하나씩 두 개의 B 채널이 설정됩니다.



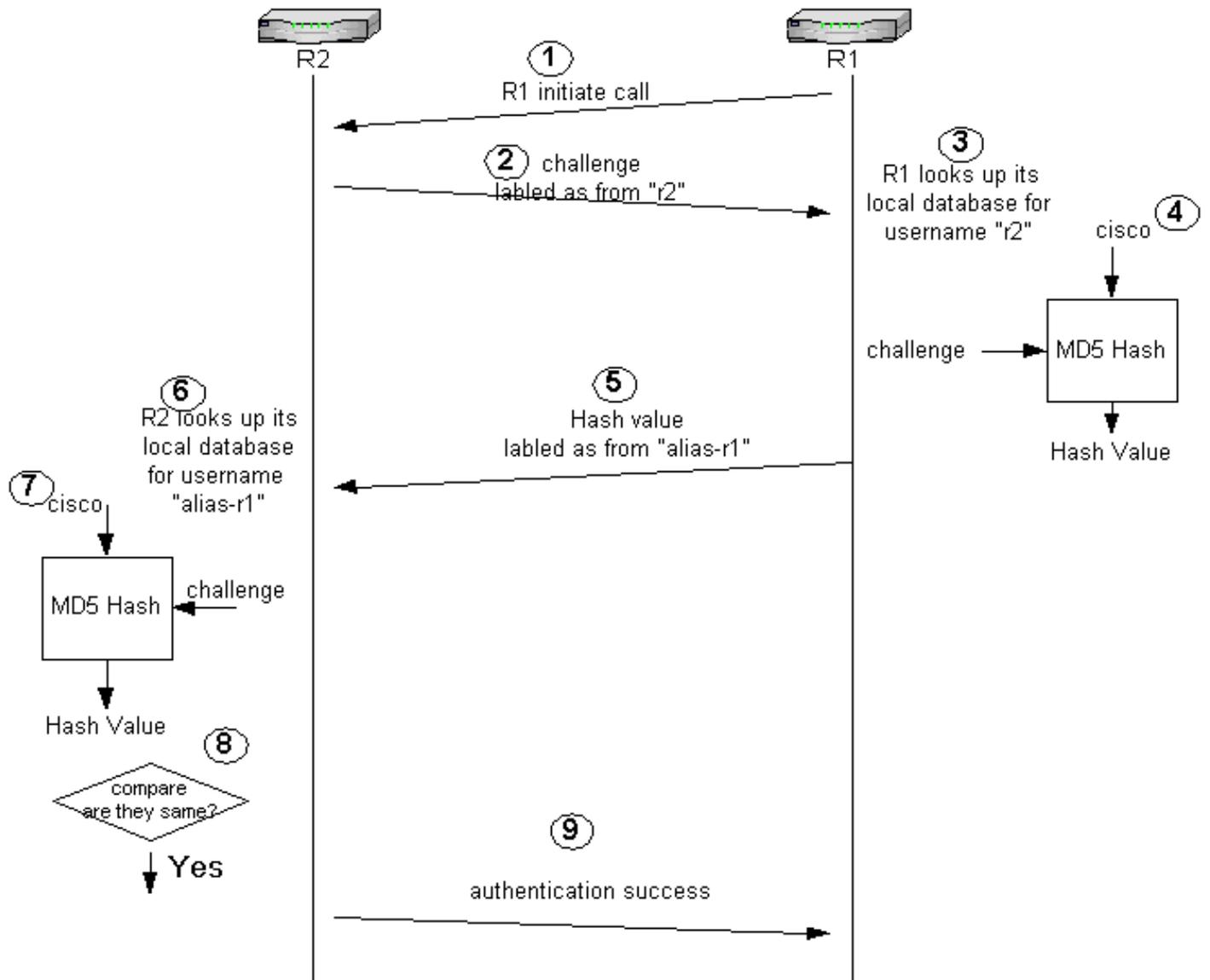
구성

라우터 1
<pre> ! isdn switch-type basic-5ess ! hostname r1 ! username r2 password 0 cisco ! -- Hostname of other router and shared secret ! interface BRI0/0 ip address 20.1.1.1 255.255.255.0 no ip directed-broadcast encapsulation ppp dialer map ip 20.1.1.2 name r2 broadcast 5772222 dialer-group 1 isdn switch-type basic-5ess ppp authentication chap callin ! -- Authentication on incoming calls only ppp chap hostname alias-r1 ! -- Alternate CHAP hostname ! access-list 101 permit ip any any dialer-list 1 protocol ip list 101 ! </pre>
라우터 2
<pre> ! isdn switch-type basic-5ess ! hostname r2 ! username alias-r1 password 0 cisco ! -- Alternate CHAP hostname and shared secret. ! -- The username must match the one in the ppp chap hostname ! -- command on the remote router. ! interface BRI0/0 ip address 20.1.1.2 255.255.255.0 no ip directed-broadcast encapsulation ppp dialer map ip 20.1.1.1 name alias-r1 broadcast 5771111 ! -- Dialer map name matches alternate hostname </pre>

```
"alias-r1". dialer-group 1 isdn switch-type basic-5ess
ppp authentication chap ! access-list 101 permit ip any
any dialer-list 1 protocol ip list 101 !
```

구성 설명

자세한 내용은 이 그래픽 아래의 숫자를 참조하십시오.



1. 이 예에서 라우터 1은 통화를 시작합니다. 라우터 1은 ppp 인증 chap callin 명령으로 구성되었으므로 발신자(라우터 2)에 대한 챌린지는 수행하지 않습니다.
2. 라우터 2가 통화를 수신하면 라우터 1에서 인증을 요청합니다. 기본적으로 이 인증에서는 라우터의 호스트 이름이 자신을 식별하는 데 사용됩니다. ppp chap hostname name 명령이 구성된 경우 라우터는 호스트 이름 대신 이름을 사용하여 자신을 식별합니다. 이 예에서 챌린지는 "r2"에서 오는 것으로 표시됩니다.
3. 라우터 1은 라우터 2의 과제를 수신하고 로컬 데이터베이스에서 사용자 이름 "r2"를 찾습니다.
4. 라우터 1은 "cisco"인 "r2" 비밀번호를 찾습니다. 라우터 1에서는 이 암호와 라우터 2의 챌린지를 MD5 해시 기능의 입력 매개변수로 사용합니다. 해시 값이 생성됩니다.
5. 라우터 1은 해시 출력 값을 라우터 2로 보냅니다. 여기에서 ppp chap hostname 명령은 "alias-r1"으로 구성되므로 회신은 "alias-r1"에서 오는 것으로 레이블이 지정됩니다.
6. 라우터 2가 회신을 수신하고 로컬 데이터베이스에서 비밀번호를 찾기 위해 "alias-r1" 사용자 이름을 찾습니다.

- 라우터 2는 "alias-r1"의 비밀번호가 "cisco"임을 확인합니다. 라우터 2는 비밀번호 및 MD5 해시 기능에 대한 입력 매개변수로 라우터 1에 앞서 전송한 챌린지를 사용합니다. 해시 함수는 해시 값을 생성합니다.
- 라우터 2는 생성된 해시 값과 라우터 1에서 수신하는 해시 값을 비교합니다.
- 입력 매개 변수(챌린지 및 비밀번호)가 동일하므로 해시 값이 동일하므로 인증에 성공합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

debug 명령을 시도하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

디버그 출력 샘플

다음은 debug ppp authentication 명령의 샘플 출력입니다.

라우터 1

```
r1#ping 20.1.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:
```

```
*Mar 1 20:06:27.179: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
```

```
*Mar 1 20:06:27.183: %ISDN-6-CONNECT:
```

```
Interface BRI0/0:1 is now connected to 5772222
```

```
*Mar 1 20:06:27.187: BR0/0:1 PPP: Treating connection as a callout
```

```
*Mar 1 20:06:27.223: BR0/0:1 CHAP: I CHALLENGE id 57 len 23 from "r2"
```

```
! -- Received a CHAP challenge from other router (r2) *Mar 1 20:06:27.223: BR0/0:1 CHAP:
```

```
Using alternate hostname alias-r1
```

```
! -- Using alternate hostname configured with ! -- ppp chap hostname command *Mar 1
```

```
20:06:27.223: BR0/0:1 CHAP: O RESPONSE id 57 Len 29 from "alias-r1" ! -- Sending response from
```

```
"alias-r1" ! -- which is the alternate hostname for r1 *Mar 1 20:06:27.243: BR0/0:1 CHAP: I
```

```
SUCCESS id 57 Len 4 ! -- Received CHAP authentication is successful ! -- Note that r1 is not
```

```
challenging r2 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms r1#
```

```
*Mar 1 20:06:28.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to
```

```
up r1# *Mar 1 20:06:33.187: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 r2
```

라우터 2

```
r2#
```

```
20:05:20: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
```

```
20:05:20: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111
```

```
20:05:20: BR0/0:1 PPP: Treating connection as a callin
```

```
20:05:21: BR0/0:1 CHAP: O CHALLENGE id 57 Len 23 from "r2"
```

```
! -- r2 is sending out a challenge 20:05:21: BR0/0:1 CHAP: I RESPONSE id 57 Len 29 from
```

```
"alias-r1"
```

```
! -- Received a response from alias-r1, ! -- which is the alternate hostname on r1 20:05:21:
```

BR0/0:1 CHAP: 0 SUCCESS id 57 Len 4 ! -- *Sending out CHAP authentication is successful* 20:05:22:
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up 20:05:26: %ISDN-6-
CONNECT: Interface BRI0/0:1 is now connected to 57711111 alias-r1

관련 정보

- [광역 네트워킹을 위한 PPP 명령](#)
- [PPP 및 PPP 인증 이해](#)
- [ISDN 디버그 정보](#)