PPP CHAP 인증 구성 및 이해

목차

소개

이 문서에서는 CHAP(Challenge Handshake Authentication Protocol)가 3방향 핸드셰이크를 통해 피어의 ID를 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 를 통해 인터페이스에서 PPP를 활성화하는 방법 encapsulation ppp 명령을 실행합니다.
- 이 **debug ppp negotiation** 명령 출력입니다. 자세한 내용은 디버그 ppp 협상 출력 이해를 참조하십시오.
- LCP(Link Control Protocol) 단계가 열린 상태가 아닐 때 문제를 해결하는 방법. 이는 LCP 단계가 완료될 때까지 PPP 인증 단계가 시작되지 않고 오픈 상태가 되기 때문이다. 이 debug ppp negotiation명령에서 LCP가 열려 있다고 표시하지 않습니다. 계속하기 전에 이 문제를 해결해야 합니다.

참고: 이 문서에서는 MS-CHAP(버전 1 또는 버전 2)를 다루지 않습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

배경 정보

CHAP(Challenge Handshake Authentication Protocol)(RFC 1994에 정의됨)는 3방향 핸드셰이크를 통해 피어의 ID를 확인합니다. 다음은 CHAP에서 수행되는 일반적인 단계입니다.

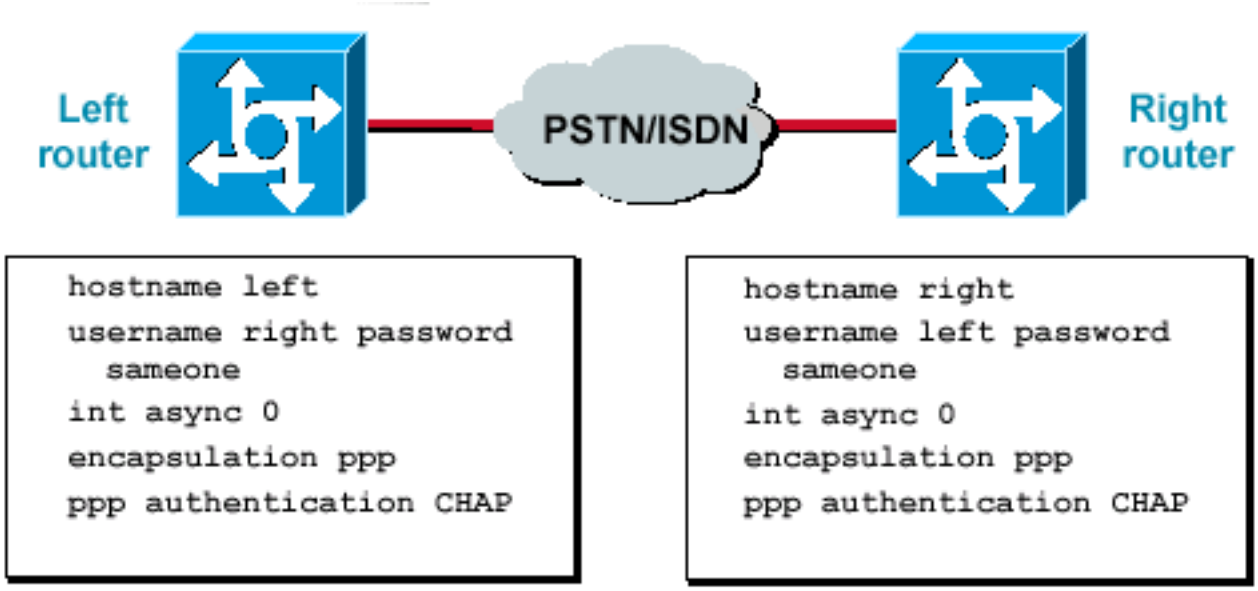
1. LCP(Link Control Protocol) 단계가 완료되고 두 디바이스 간에 CHAP가 협상되면 인증자가 피어에 챌린지 메시지를 보냅니다.
2. 피어는 단방향 해시 함수(MD5(Message Digest 5))를 통해 계산된 값으로 응답합니다.
3. 인증자는 예상 해시 값의 자체 계산에 대해 응답을 확인합니다. 값이 일치하면 인증에 성공합니다. 그렇지 않으면 연결이 종료됩니다.

이 인증 방법은 인증자 및 피어에게만 알려진 "비밀"에 따라 달라집니다. 비밀은 링크를 통해 전송되지 않습니다. 인증은 단방향이지만, 상호 인증을 위해 동일한 암호 세트를 사용하여 양방향으로 CHAP를 협상할 수 있습니다.

CHAP의 장점과 단점에 대한 자세한 내용은 RFC 1994를 참조하십시오.

CHAP 구성

CHAP를 구성하는 절차는 매우 간단합니다. 예를 들어 그림 1과 같이 네트워크를 통해 연결된 두 개의 라우터(왼쪽 및 오른쪽)가 있다고 가정합니다.



네트

워크를 통해 연결된 라우터 2개

그림 1 — 네트워크를 통해 연결된 라우터 2개

CHAP 인증을 구성하는 절차는 다음과 같습니다.

1. 인터페이스에서 encapsulation ppp **명령을** 실행합니다.
2. 두 라우터에서 CHAP 인증 사용 ppp authentication chap 명령을 실행합니다.
3. 사용자 이름 및 비밀번호를 구성합니다. 이를 위해 username username password password명령, 여기서 usernameis는 피어의 호스트 이름입니다. 다음 사항을 확인합니다.비밀번호는 양쪽 끝에서 동일합니다.라우터 이름과 비밀번호는 대/소문자를 구분하기 때문에 정확히 동일합니다.

   참고: 기본적으로 라우터는 호스트 이름을 사용하여 피어를 식별합니다. 그러나 이 CHAP 사용자 이름은 ppp chap hostname 명령을 실행합니다. 자세한 내용은 ppp chap hostname 및 ppp authentication chap callin 명령을 사용한 PPP 인증을 참조하십시오.

단방향 및 양방향 인증

CHAP는 단방향 인증 방법으로 정의됩니다. 그러나 양방향 인증을 생성하기 위해 양방향으로 CHAP를 사용합니다. 따라서 양방향 CHAP를 사용하면 양쪽에서 별도의 3방향 핸드셰이크가 시작됩니다.

Cisco CHAP 구현에서는 기본적으로 수신자가 발신자를 인증해야 합니다(인증이 완전히 꺼지지 않은 경우). 따라서 수신자가 시작한 단방향 인증은 가능한 최소 인증입니다. 그러나 발신자는 수신자 ID를 확인할 수도 있으며, 이는 양방향 인증으로 이어집니다.

Cisco 이외의 디바이스에 연결할 때 단방향 인증이 필요한 경우가 많습니다.

단방향 인증의 경우 ppp authentication chap callin명령을 실행합니다.

표 1은 통화 옵션을 구성하는 시기를 보여줍니다.

표 1: 통화 옵션 구성 시기

인증 유형	클라이언트(통화)	NAS(호출됨)

단방향(단방향) **ppp 인증 chap 통화 ppp 인증 chap**
양방향(양방향) **ppp 인증 chap ppp 인증 chap**

자세한 내용은 ppp chap hostname 및 ppp authentication chap callin 명령을 사용한 PPP 인증을 참조하십시오.

CHAP 구성 명령 및 옵션

표 2에는 CHAP 명령과 옵션이 나와 있습니다.

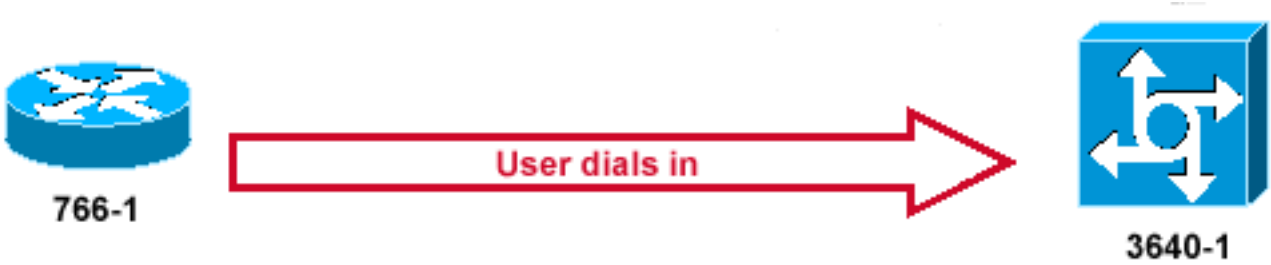
표 2: CHAP 명령 및 옵션

명령을 사용합니다	설명
ppp 인증 {chap | ms-chap | ms-chap-v2 | eap |pap} [callin]	이 명령은 지정된 프로토콜로 원격 PPP 피어의 로컬 인증을 활성화합니다.
ppp chap 호스트 이름 사용자 이름	이 명령은 인터페이스별 CHAP 호스트 이름을 정의합니다. 자세한 내용은 ppp chap 호스트 이름 및 ppp 인증 chap callin 명령을 사용한 PPP 인증을 참조하십시오.
ppp chap 비밀번호비밀번호	이 명령은 인터페이스별 CHAP 암호를 정의합니다.
ppp directioncallin | 콜아웃 | 전용	이 명령은 강제로 호출 방향을 지정합니다. 라우터에서 통화가 수신되는지 아니면 발신되는지 혼동할 때(예: 백투백으로 연결되거나 임대 회선으로 연결되고 채널 서비스 장치 또는 데이터 서비스 장치(CSU/DSU) 또는 ISDN 터미널 어댑터(TA)가 다이얼하도록 구성된 경우) 이 명령을 사용합니다.
ppp chap 거부 [callin]	이 명령은 피어에 의한 원격 인증을 비활성화합니다(기본적으로 활성화됨). 이 명령을 사용하면 모든 통화에 대해 CHAP 인증이 비활성화됩니다. 즉, 피어가 CHAP의 도움을 받아 사용자를 인증하도록 강요하려는 모든 시도가 거부됩니다. callin 옵션은 라우터가 피어에서 수신한 CHAP 인증 챌린지에 대한 응답을 거부하지만, 라우터가 전송하는 모든 CHAP 챌린지에 대해 피어가 응답하도록 지정합니다.
ppp chap 대기	이 명령은 호출자가 먼저 인증해야 함을 지정합니다(기본적으로 활성화됨). 이 명령은 피어가 라우터에 대해 자체적으로 인증될 때까지 라우터가 CHAP 인증을 요청하는 피어에 대해 인증하지 않도록 지정합니다.
ppp max-bad-auth 값	이 명령은 허용되는 인증 재시도 횟수를 지정합니다(기본값은 0). 이 명령은 포인트-투-포인트 인터페이스가 인증 실패 후 바로 재설정되지 않고 지정된 횟수의 인증 재시도를 허용하도록 구성합니다.
ppp chap splitnames	이 숨겨진 명령은 CHAP 챌린지 및 응답에 대해 서로 다른 호스트 이름을 허용합니다(기본값은 비활성화됨).
ppp chap ignoreus	이 숨겨진 명령은 로컬 이름의 CHAP 문제를 무시합니다(기본값은 활성화됨).

트랜잭션 예

이 섹션의 다이어그램에는 두 라우터 간의 CHAP 인증 중에 발생하는 일련의 이벤트가 나와 있습니다. 이러한 메시지는 debug ppp negotiation명령 출력입니다. 자세한 내용은 debug ppp 협상 출력 이해를 참조하십시오.

통화



전

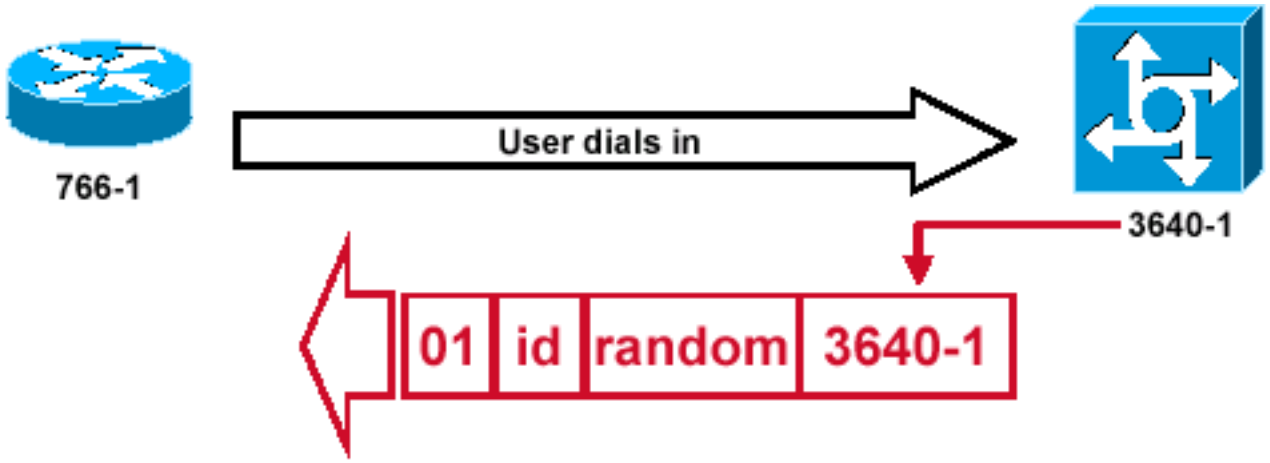
화가 걸려옵니다.

그림 2 — 통화 수신

그림 2에는 다음 단계가 나와 있습니다.

1. 전화가 3640-1에 옵니다. 수신 인터페이스는 ppp authentication chap 명령을 실행합니다.
2. LCP는 CHAP 및 MD5를 협상합니다. 이를 확인하는 방법에 대한 자세한 내용은 debug ppp 협상 출력 이해를 참조하십시오.
3. 이 통화에는 3640-1에서 발신 라우터로의 CHAP 챌린지가 필요합니다.

과제



C

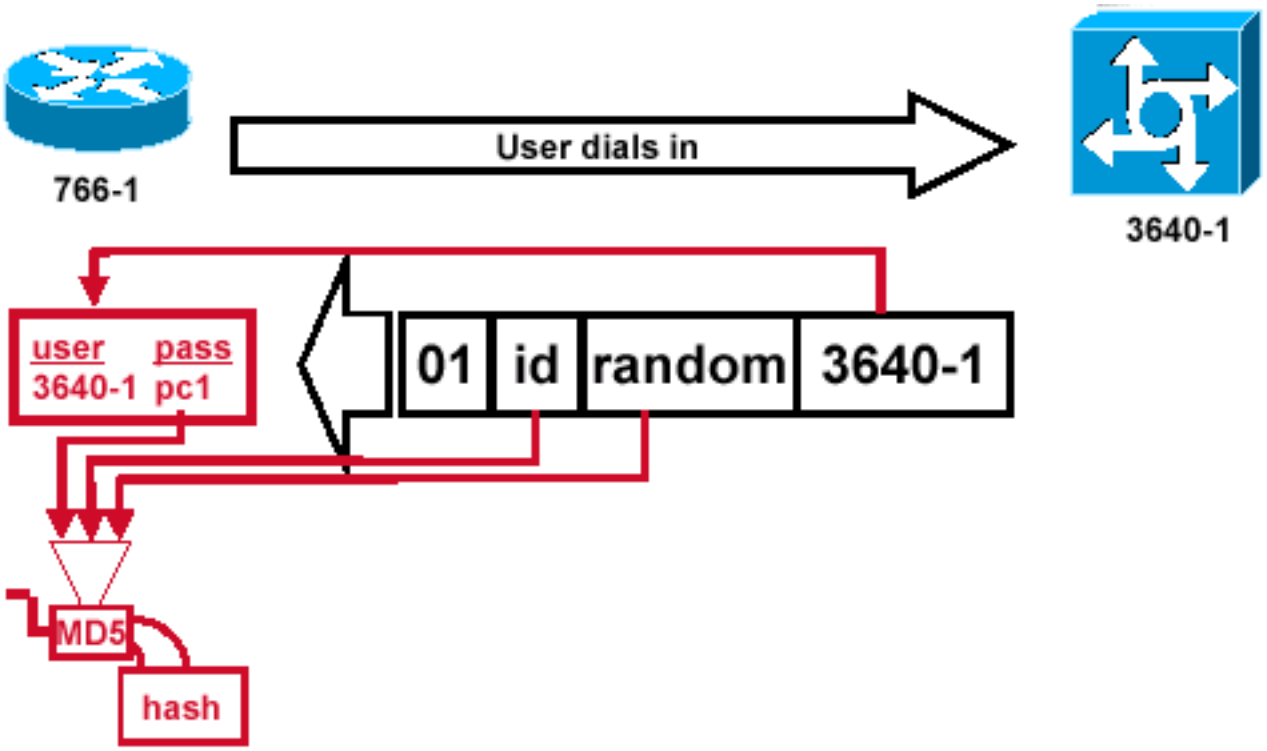
HAP 챌린지 패킷이 구축됨

그림 3 — CHAP 챌린지 패킷 구축

그림 3은 두 라우터 간의 CHAP 인증에서 다음 단계를 보여줍니다.

1. CHAP 챌린지 패킷은 다음과 같은 특성으로 구성됩니다.01 = 챌린지 패킷 유형 식별자.ID = 챌린지를 식별하는 순차적 번호입니다.random = 라우터에서 생성된 합리적인 난수입니다 .3640-1 = 챌린저의 인증 이름.
2. ID 및 임의 값은 호출된 라우터에 유지됩니다.
3. 챌린지 패킷이 발신 라우터로 전송됩니다. 뛰어난 과제 목록이 유지됩니다.

응답



피어에서

챌린지 패킷 수신 및 MD5 처리

그림 4 — 피어에서 챌린지 패킷 수신 및 MD5 처리

그림 4는 피어에서 챌린지 패킷을 수신하여 처리하는 방법(MD5)을 보여줍니다. 라우터는 다음과 같은 방법으로 수신 CHAP 챌린지 패킷을 처리합니다.

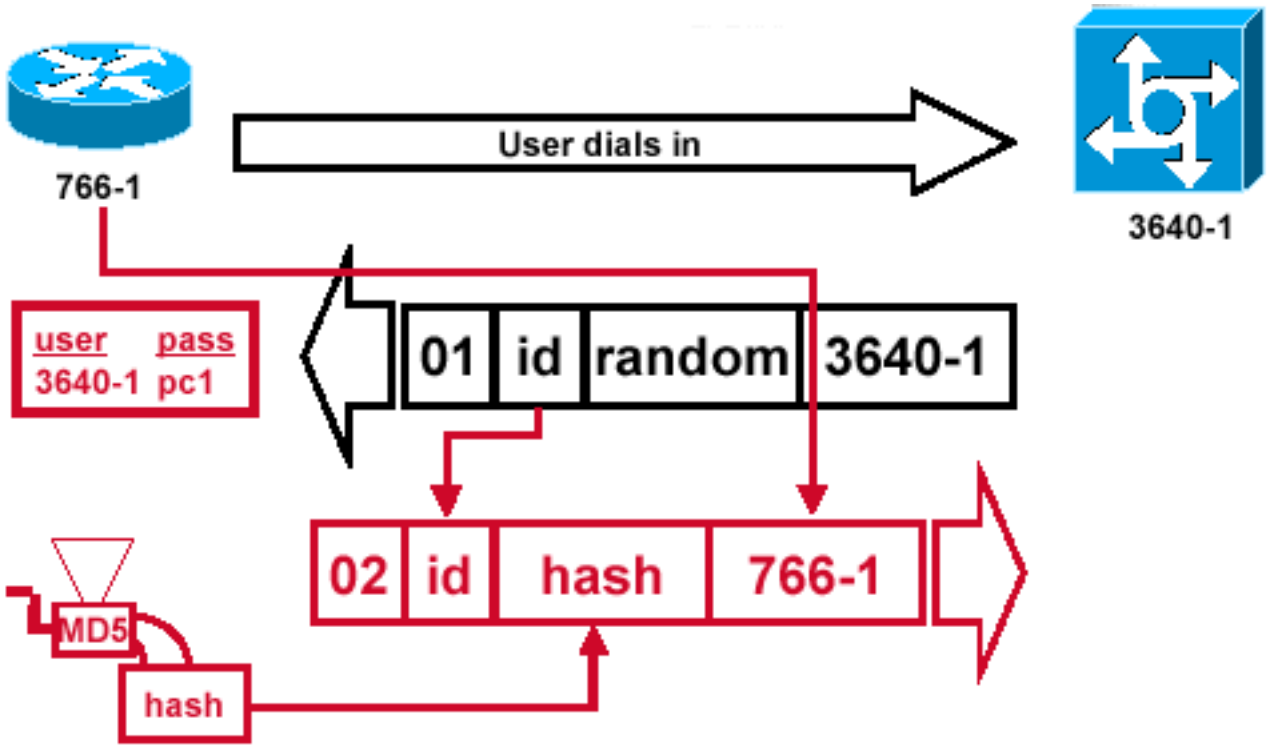
1. ID 값은 MD5 해시 생성기에 입력됩니다.
2. 무작위 값은 MD5 해시 생성기에 입력됩니다.
3. 이름 3640-1은 비밀번호를 조회하는 데 사용됩니다. 라우터는 챌린지의 사용자 이름과 일치하는 항목을 찾습니다. 이 예에서는 다음을 찾습니다.

```
username 3640-1 password pc1
```

4. 비밀번호가 MD5 해시 생성기에 입력됩니다.

그러면 CHAP 응답으로 다시 전송되는 단방향 MD5 해시 CHAP 챌린지가 생성됩니다.

응답(계속)



인증자에게 전송된 CHAP 응답 패킷이 작성되었습니다.

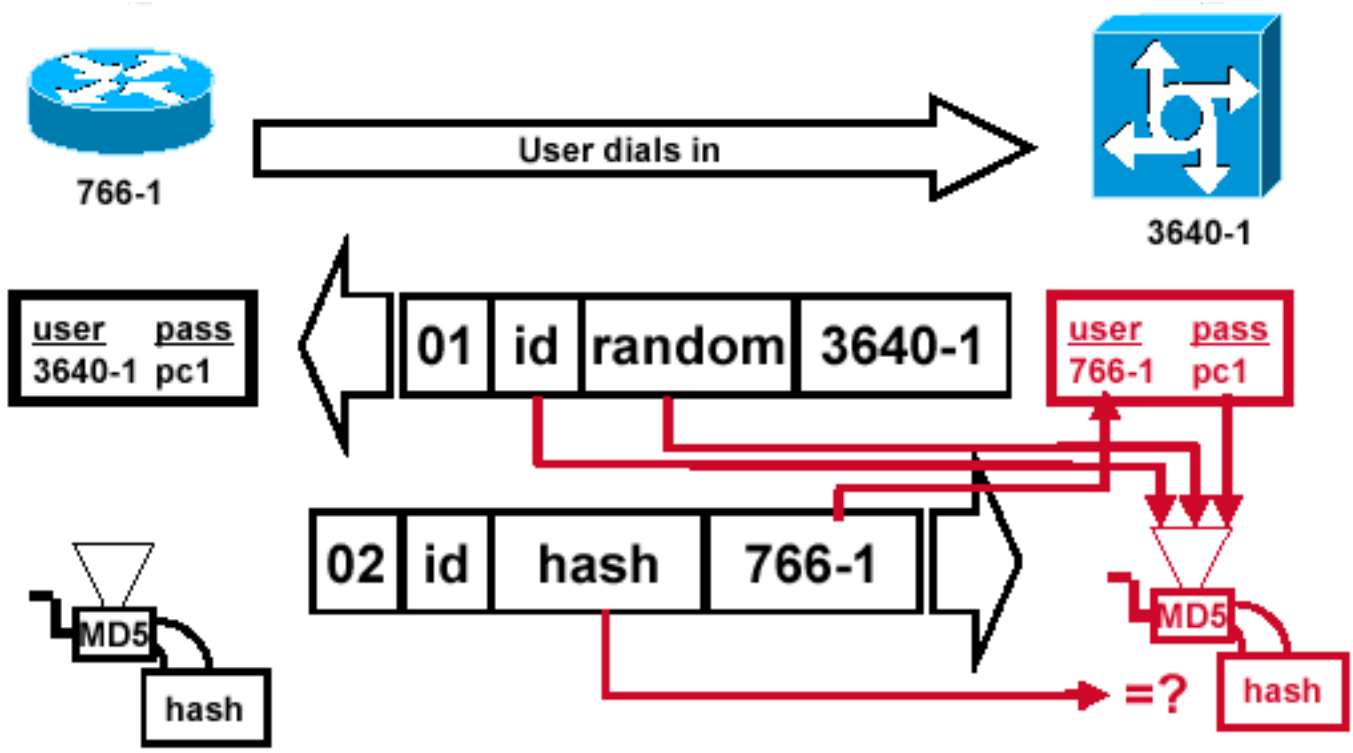
그림 5 — 인증자에게 전송되는 CHAP 응답 패킷이 작성되었습니다.

그림 5는 인증자에게 전송된 CHAP 응답 패킷이 구축되는 방법을 보여줍니다. 이 다이어그램에는 다음 단계가 나와 있습니다.

1. 응답 패킷은 다음 구성 요소에서 어셈블됩니다.02 = CHAP 응답 패킷 유형 식별자.ID = 챌린지 패킷에서 복사됨.hash = MD5 해시 생성기의 출력(챌린지 패킷의 해시된 정보).766-1 = 이 디바이스의 인증 이름. 피어가 ID를 확인하는 데 필요한 사용자 이름 및 비밀번호 항목을 조회하는 데 필요합니다(CHAP 확인 섹션에서 자세히 설명).
2. 그러면 응답 패킷이 챌린저에게 전송됩니다.

CHAP 확인

이 섹션에서는 컨피그레이션을 확인하는 방법에 대한 팁을 제공합니다.



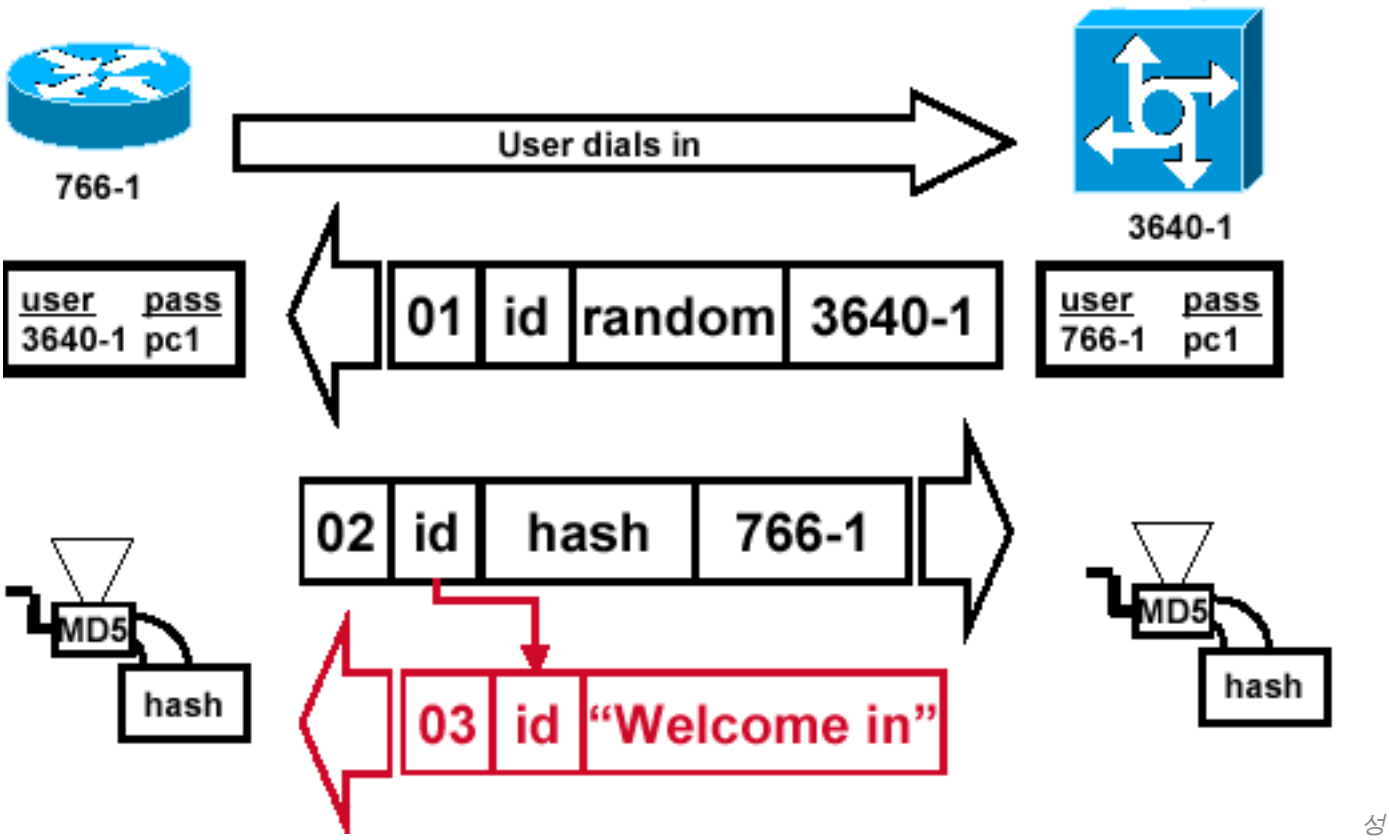
챌린저가 응답 패킷을 처리합니다.

그림 6 — 챌린저가 응답 패킷을 처리합니다.

그림 6은 챌린저가 응답 패킷을 처리하는 방법을 보여줍니다. 인증자에서 CHAP 응답 패킷이 처리될 때 포함되는 단계는 다음과 같습니다.

1. ID는 원래 챌린지 패킷을 찾는 데 사용됩니다.
2. ID는 MD5 해시 생성기에 입력됩니다.
3. 원래의 챌린지 랜덤 값은 MD5 해시 생성기에 공급된다.
4. 이름 766-1은 다음 소스 중 하나에서 비밀번호를 조회하는 데 사용됩니다.로컬 사용자 이름 및 비밀번호 데이터베이스RADIUS 또는 TACACS+ 서버
5. 비밀번호는 MD5 해시 생성기에 입력됩니다.
6. 응답 패킷에서 수신된 해시 값이 계산된 MD5 해시 값과 비교됩니다. 계산된 해시 값과 수신된 해시 값이 같으면 CHAP 인증이 성공합니다.

결과



성

공 메시지가 발신 라우터로 전송됨

그림 7 — 성공 메시지가 호출 라우터로 전송됨

그림 7은 발신 라우터로 전송된 성공 메시지를 보여줍니다. 여기에는 다음 단계가 포함됩니다.

1. 인증에 성공하면 다음 구성 요소에서 CHAP 성공 패킷이 작성됩니다.03 = CHAP 성공 메시지 유형ID = 응답 패킷에서 복사됨."Welcome in"은 사용자가 읽을 수 있는 설명을 제공하는 문자 메시지입니다.
2. 인증이 실패할 경우 다음 구성 요소에서 CHAP 실패 패킷이 생성됩니다.04 = CHAP 오류 메시지 유형ID = 응답 패킷에서 복사됨."인증 실패" 또는 사용자가 읽을 수 있는 설명을 제공하는 기타 텍스트 메시지입니다.
3. 그런 다음 성공 또는 실패 패킷이 발신 라우터로 전송됩니다.

참고: 이 예에서는 단방향 인증을 보여 줍니다. 양방향 인증에서는 이 전체 프로세스가 반복됩니다. 그러나 발신 라우터는 초기 챌린지를 시작합니다.

CHAP 문제 해결

문제 해결에 대한 자세한 내용은 PPP (CHAP 또는 PAP) 인증 문제 해결을 참조하십시오.

관련 정보

- 디버그 ppp 협상 출력 이해
- ppp chap hostname 및 ppp authentication chap callin 명령을 사용한 PPP 인증
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.