Oracle® Solaris 11.1에서 UUCP 및 PPP를 사용하여 직렬 네트워크 관리

부품 번호: E36525–02
2012년 10월

ORACLE

121210@25097

목차

그림

표

코드 예

머리말

Oracle Solaris 11.1에서 UUCP 및 PPP를 사용하여 직렬 네트워크 관리는 Oracle Solaris 시스템 관리 정보의 중요한 부분을 다루고 있는 여러 권으로 구성된 세트의 일부입니다. 이 설명서에서는 사용자가 이미 Oracle Solaris 운영 체제를 설치했으며 사용하려는 모든 네트워킹 소프트웨어를 설정했다고 가정합니다.

주 – 본 Oracle Solaris 릴리스는 프로세서 아키텍처의 SPARC 및 x86 제품군을 사용하는 시스템을 지원합니다. 지원되는 시스템은 **Oracle Solaris OS: 하드웨어 호환성 목록**을 참조하십시오. 이 설명서에서는 플랫폼 유형에 따른 구현 차이가 있는 경우 이에 대하여 설명합니다.

이 설명서의 대상

이 설명서는 Oracle Solaris 릴리스를 실행하는 하나 이상의 시스템을 관리하는 모든 사용자를 대상으로 합니다. 이 설명서를 사용하려면 UNIX 시스템 관리 경험이 1~2년 정도 있어야 합니다. UNIX 시스템 관리 교육 과정에 참석하는 것도 도움이 될 수 있습니다.

Oracle Support에 액세스

Oracle 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`를 참조하거나, 청각 장애가 있는 경우 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`를 방문하십시오.

활자체 규약

다음 표는 이 책에서 사용되는 활자체 규약에 대해 설명합니다.

표 P–1 활자체 규약

활자체	설명	예
`AaBbCc123`	명령, 파일, 디렉토리 이름 및 컴퓨터 화면에 출력되는 내용입니다.	`.login` 파일을 편집하십시오. 모든 파일 목록을 보려면 `ls -a` 명령을 사용하십시오. `machine_name% you have mail.`
`AaBbCc123`	사용자가 입력하는 내용으로 컴퓨터 화면의 출력 내용과 대조됩니다.	`machine_name%` **`su`** `Password:`
AaBbCc123	새로 나오는 용어, 강조 표시할 용어입니다. 명령줄 변수를 실제 이름이나 값으로 바꾸십시오.	`rm` *filename* 명령을 사용하여 파일을 제거합니다.
AaBbCc123	책 제목, 장, 절	**사용자 설명서**의 6장을 읽으십시오. **캐시**는 로컬로 저장된 복사본입니다. 파일을 저장하면 **안 됩니다**. **주:** 일부 강조된 항목은 온라인에서 굵은체로 나타납니다.

명령 예의 셸 프롬프트

다음 표에는 Oracle Solaris OS에 포함된 셸의 기본 UNIX 시스템 프롬프트 및 수퍼유저 프롬프트가 나와 있습니다. 명령 예제에 표시된 기본 시스템 프롬프트는 Oracle Solaris 릴리스에 따라 다릅니다.

표 P–2 셸 프롬프트

셸	프롬프트
Bash 셸, Korn 셸 및 Bourne 셸	`$`
수퍼유저용 Bash 셸, Korn 셸 및 Bourne 셸	`#`
C 셸	`machine_name%`
수퍼유저용 C 셸	`machine_name#`

◆ ◆ ◆ 1 장

1 Solaris PPP 4.0(개요)

이 절에서는 직렬 네트워킹 관련 항목을 다룹니다. 직렬 네트워킹은 데이터를 전송할 수 있도록 둘 이상의 컴퓨터를 연결하기 위해 RS-232 또는 V.35 포트와 같은 직렬 인터페이스를 사용하는 것을 가리킵니다. 이더넷과 같은 LAN 인터페이스와 달리 이러한 직렬 인터페이스는 서로 멀리 떨어져 있는 여러 시스템을 연결하는 데 사용됩니다. PPP(지점 간 프로토콜) 및 UUCP(UNIX 간 복사)는 직렬 네트워킹을 구현하는 데 사용할 수 있는 특별한 기술입니다. 네트워킹용으로 구성된 직렬 인터페이스는 이더넷과 같은 다른 네트워크 인터페이스와 거의 같은 방식으로 여러 사용자에게 제공됩니다.

이 장에서는 Solaris PPP 4.0을 소개합니다. 이 버전의 PPP를 사용하면 서로 다른 물리적 위치에 있는 두 컴퓨터가 다양한 매체를 통해 PPP를 사용하여 서로 통신할 수 있습니다. Solaris PPP 4.0은 기본 설치의 구성 요소입니다.

다음 항목을 다룹니다.

Solaris PPP 4.0 기본 사항

Solaris PPP 4.0은 TCP/IP 프로토콜 집합의 구성원이자 데이터 링크 프로토콜인 PPP(지점 간 프로토콜)를 구현합니다. PPP는 전화선과 같은 통신 매체를 통해 두 끝점 시스템 사이에서 데이터가 전송되는 방법을 기술합니다.

1990년대 초반부터 PPP는 통신 링크를 통해 데이터그램을 보내기 위한 인터넷 표준으로 널리 사용되고 있습니다. PPP 표준은 IETF(Internet Engineering Task Force)의 Point-to-Point Working Group에 의해 RFC 1661에 기술되어 있습니다. PPP는 원격 컴퓨터가 인터넷 서비스 제공업체(ISP)나 수신 호출을 받도록 구성된 회사 서버를 호출할 때 일반적으로 사용됩니다.

Solaris PPP 4.0은 공개적으로 사용 가능한 ANU(Australian National University) PPP-2.4를 기반으로 하며 PPP 표준을 구현합니다. 비동기 PPP 링크와 동기 PPP 링크가 모두 지원됩니다.

Solaris PPP 4.0 호환성

다양한 버전의 표준 PPP가 제공되어 인터넷 커뮤니티에서 널리 사용되고 있습니다. ANU PPP-2.4가 Linux, Tru64 UNIX 및 세 가지 모든 주요 BSD 변형에 대해 가장 많이 사용되고 있습니다.

- FreeBSD
- OpenBSD
- NetBSD

Solaris PPP 4.0은 원하는 대로 구성이 가능한 ANU PPP-2.4의 기능을 Oracle Solaris 운영 체제를 실행하는 시스템에 제공합니다. Solaris PPP 4.0을 실행하는 시스템은 표준 PPP의 구현을 실행하는 모든 시스템에 대한 PPP 링크를 손쉽게 설정할 수 있습니다.

ANU를 기반으로 하지 않는 일부 PPP 구현 중 Solaris PPP 4.0과 성공적으로 상호 운영되는 구현의 예는 다음과 같습니다.

- Solaris PPP(`asppp`라고도 하며 Solaris 2.4 ~ Solaris 8 릴리스에서 사용 가능함)
- Solstice PPP 3.0.1
- Microsoft Windows 98 DUN
- Cisco IOS 12.0(동기)

사용할 Solaris PPP 버전

Solaris PPP 4.0은 지원되는 PPP 구현입니다. Solaris 9 이상 릴리스에는 이전 버전의 비동기 Solaris PPP(`asppp`) 소프트웨어가 포함되어 있지 않습니다. 자세한 내용은 9 장, “비동기 Solaris PPP에서 Solaris PPP 4.0으로 마이그레이션(작업)”을 참조하십시오.

Solaris PPP 4.0을 사용하는 이유

현재 `asppp`를 사용하고 있는 경우 Solaris PPP 4.0으로 마이그레이션해 보십시오. 두 Solaris PPP 기술의 차이점은 다음과 같습니다.

- **전송 모드**

  `asppp`는 비동기 통신만 지원하고, Solaris PPP 4.0은 비동기 통신과 동기 통신을 모두 지원합니다.

- **구성 프로세스**

  `asppp`를 설정하려면 `asppp.cf` 구성 파일, 세 UUCP 파일 및 `ipadm` 명령을 구성해야 합니다. 또한 시스템에 로그인할 수 있는 모든 사용자에 대해 인터페이스를 미리 구성해야 합니다.

Solaris PPP 4.0을 설정하려면 PPP 구성 파일에 대한 옵션을 정의하거나 옵션을 사용하여 pppd 명령을 실행해야 합니다. 구성 파일과 명령줄 메소드를 조합하여 사용할 수도 있습니다. Solaris PPP는 인터페이스를 동적으로 만들고 제거합니다. 각 사용자에 대해 직접 PPP 인터페이스를 구성할 필요는 없습니다.

- **asppp에서 사용할 수 없는 Solaris PPP 4.0 기능**
  - MS-CHAPv1 및 MS-CHAPv2 인증
  - ADSL 브릿지를 지원하기 위한 PPPoE(PPP over Ethernet)
  - PAM 인증
  - 플러그인 모듈
  - IPv6 주소 지정
  - Deflate 또는 BSD 압축을 사용하는 데이터 압축
  - Microsoft 클라이언트측 콜백 지원

Solaris PPP 4.0 업그레이드 경로

기존 asppp 구성을 Solaris PPP 4.0으로 변환하는 경우 이 릴리스와 함께 제공되는 변환 스크립트를 사용할 수 있습니다. 자세한 내용은 152 페이지 “asppp에서 Solaris PPP 4.0으로 변환하는 방법”을 참조하십시오.

PPP에 대한 추가 정보

PPP에 대한 정보가 포함된 많은 리소스가 인쇄물 및 온라인으로 제공되어 있습니다. 다음 세부절에는 일부 제안 사항이 제공되어 있습니다.

PPP에 대한 전문 참조 설명서

널리 사용되는 PPP 구현(ANU PPP 포함)에 대한 자세한 내용은 다음 설명서를 참조하십시오.

- Carlson, James. **PPP Design, Implementation, and Debugging**. 제2판 Addison-Wesley, 2000.
- Sun, Andrew. **Using and Managing PPP**. O'Reilly & Associates, 1999.

PPP에 대한 웹 사이트

PPP에 대한 일반적인 정보를 얻으려면 다음 웹 사이트로 이동하십시오.

- 기술 정보, FAQ, Oracle Solaris 시스템 관리에 대한 설명 및 이전 버전의 PPP를 얻으려면 시스템 관리자 리소스인 http://www.sun.com/bigadmin/home/index.html로 이동하십시오.
- 다양한 PPP 구현을 위한 모뎀 구성 및 조언은 Stokely Consulting의 Web Project Management & Software Development 웹 사이트인 http://www.stokely.com/unix.serial.port.resources/ppp.slip.html을 참조하십시오.

PPP에 대한 RFC(Request for Comments)

PPP에 대한 일부 유용한 인터넷 RFC는 다음과 같습니다.

- 1661 및 1662 - PPP의 주요 기능을 기술합니다.
- 1334 - PAP(암호 인증 프로토콜) 및 CHAP(Challenge-Handshake 인증 프로토콜)와 같은 인증 프로토콜을 기술합니다.
- 1332 - PPPoE(PPP over Ethernet)를 기술하는 정보 RFC입니다.

PPP RFC 사본을 얻으려면 IETF RFC 웹 페이지(http://www.ietf.org/rfc.html)에서 RFC 번호를 지정하십시오.

PPP에 대한 매뉴얼 페이지

Solaris PPP 4.0 구현에 대한 기술 정보는 다음 매뉴얼 페이지를 참조하십시오.

- `pppd`(1M)
- `chat`(1M)
- `pppstats`(1M)
- `pppoec`(1M)
- `pppoed`(1M)
- `sppptun`(1M)
- `snoop`(1M)

`pppdump`(1M)에 대한 매뉴얼 페이지도 참조하십시오. PPP 관련 매뉴얼 페이지는 `man` 명령을 사용하여 찾을 수 있습니다.

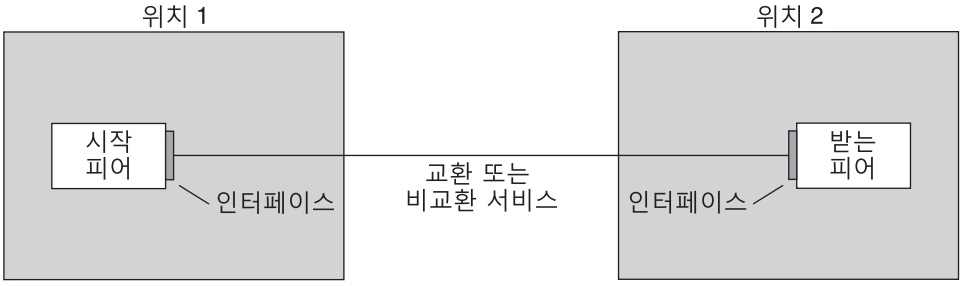
PPP 구성 및 용어

이 절에서는 PPP 구성을 소개합니다. 이 절에서는 이 설명서에 사용되는 용어도 정의합니다.

Solaris PPP 4.0은 많은 구성을 지원합니다.

- 교환 액세스 또는 **다이얼 업** 구성
- 기계적 연결 또는 **전용 회선** 구성

그림 1–1 PPP 링크의 각 부분



이전 그림에서는 기본 PPP 링크를 보여줍니다. 링크에는 다음과 같은 부분이 있습니다.

- 일반적으로 서로 다른 물리적 위치에 있는 두 시스템(**피어**라고 함). 피어는 사이트 요구 사항에 따라 개인용 컴퓨터, 엔지니어링 워크스테이션, 대규모 서버, 심지어는 상용 라우터일 수 있습니다.
- 각 피어의 직렬 인터페이스. Oracle Solaris 시스템에서 이 인터페이스는 관리자가 비동기 PPP를 구성하는지, 아니면 동기 PPP를 구성하는지에 따라 `cua`, `hihp` 또는 기타 인터페이스일 수 있습니다.
- 직렬 케이블 등의 물리적 링크, 모뎀 연결 또는 네트워크 공급자로부터 임대 받은 T1/T3 회선 등의 전용 회선

다이얼 업 PPP 개요

가장 일반적으로 사용되는 PPP 구성은 **다이얼 업 링크**입니다. 다이얼 업 링크에서 로컬 피어는 원격 피어를 **다이얼 업**하여 연결을 설정하고 PPP를 실행합니다. 다이얼 업 프로세스에서 로컬 피어는 원격 피어의 전화 번호로 전화를 걸어 링크를 시작합니다.

일반적인 다이얼 업 시나리오로는 수신 호출을 받도록 구성된 ISP에서 피어를 호출하는 홈 컴퓨터를 들 수 있습니다. 다른 시나리오로는 PPP 링크를 통해 다른 빌딩에 있는 피어로 데이터를 전송하는 로컬 시스템을 사용하는 회사 사이트를 들 수 있습니다.

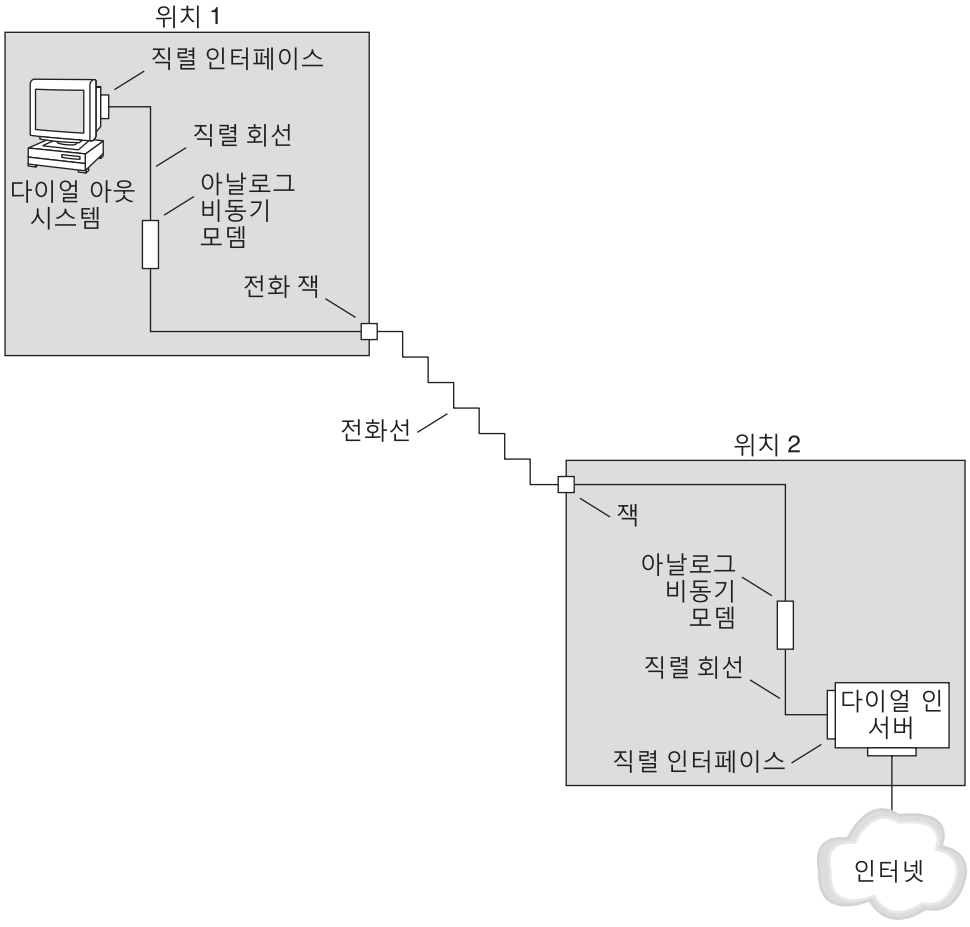
이 설명서에서는 다이얼 업 연결을 시작하는 로컬 피어를 **다이얼 아웃 시스템**이라고 합니다. 또한 수신 호출을 받는 피어를 **다이얼 인 서버**라고 합니다. 이 시스템은 실제로 다이얼 아웃 시스템의 대상 피어이며 실제 서버이거나 실제 서버가 아닐 수 있습니다.

PPP는 클라이언트-서버 프로토콜이 아닙니다. 일부 PPP 문서에서는 "클라이언트" 및 "서버"라는 용어가 전화 호출 설정을 가리키는 데 사용됩니다. 다이얼 인 서버는 파일 서버 또는 이름 서버와 같은 실제 서버가 아닙니다. 다이얼 인 시스템은 종종 둘 이상의 다이얼 아웃 시스템에 네트워크 접근성을 제공하는 데 사용되므로, 다이얼 인 서버라는 말은 널리 사용되는 PPP 용어입니다. 그럼에도 불구하고 다이얼 인 서버는 다이얼 아웃 시스템의 대상 피어입니다.

다이얼 업 PPP 링크의 각 부분

다음 그림을 참조하십시오.

그림 1–2 기본 아날로그 다이얼 업 PPP 링크



링크의 다이얼 아웃측인 위치 1에 대한 구성은 다음 요소로 구성되어 있습니다.

- 다이얼 아웃 시스템(일반적으로 사용자 집에 있는 개인용 컴퓨터 또는 워크스테이션)
- 다이얼 아웃 시스템에 있는 직렬 인터페이스. `/dev/cua/a` 또는 `/dev/cua/b`는 Oracle Solaris 소프트웨어를 실행하는 시스템에 있는 발신 호출을 위한 표준 직렬 인터페이스입니다.
- 전화 잭에 연결된 비동기 모뎀 또는 ISDN TA(터미널 어댑터)

- 전화 회사의 전화선 및 서비스

링크의 다이얼 인측인 위치 2에 대한 구성은 다음 요소로 구성되어 있습니다.

- 전화 네트워크에 연결된 전화 잭 또는 이와 유사한 커넥터
- 비동기 모뎀 또는 ISDN TA
- 다이얼 인 서버에 있는 직렬 인터페이스(수신 호출용 `ttya` 또는 `ttyb`)
- 회사 인트라넷과 같이 네트워크에 연결되어 있거나 전역 인터넷인 ISP의 인스턴스에 있는 다이얼 인 서버

다이얼 아웃 시스템에서 ISDN 터미널 어댑터 사용

외부 ISDN TA의 속도는 모뎀보다 빠르지만 TA는 기본적으로 동일하게 구성합니다. ISDN TA를 구성할 때의 주요 차이점은 채트 스크립트에 있습니다. 여기에는 TA 제조업체와 관련된 명령이 필요합니다. ISDN TA의 채트 스크립트에 대한 자세한 내용은 126 페이지 “외부 ISDN TA를 위한 채트 스크립트”를 참조하십시오.

다이얼 업 통신 중 발생하는 작업

다이얼 아웃 피어와 다이얼 인 피어 모두에 있는 PPP 구성 파일에 링크 설정 명령이 포함됩니다. 다이얼 업 링크를 시작하면 다음 프로세스가 발생합니다.

1. 다이얼 아웃 시스템에 있는 사용자 또는 프로세스가 `pppd` 명령을 실행하여 링크를 시작합니다.
2. 다이얼 아웃 시스템이 해당 PPP 구성 파일을 읽습니다. 그러면 다이얼 아웃 시스템이 직렬 회선을 통해 해당 모뎀으로 명령을 보냅니다(다이얼 인 서버의 전화 번호 포함).
3. 모뎀이 해당 전화 번호로 전화를 걸어 다이얼 인 서버에 있는 모뎀과 전화 연결을 설정합니다.

   다이얼 아웃 시스템이 모뎀 및 다이얼 인 서버로 보내는 일련의 텍스트 문자열이 **채트 스크립트**라는 파일에 포함됩니다. 필요한 경우 다이얼 아웃 시스템이 다이얼 인 서버에 명령을 보내 서버에서 PPP를 호출합니다.
4. 다이얼 인 서버에 연결된 모뎀이 다이얼 아웃 시스템에 있는 모뎀과 링크 협상을 시작합니다.
5. 모뎀 간 협상이 완료되면 다이얼 아웃 시스템에 있는 모뎀이 "CONNECT(연결)"를 보고합니다.
6. 두 피어 모두의 PPP가 *Establish(**설정**)* 단계로 들어갑니다. 이 단계에서는 LCP(링크 제어 프로토콜)가 기본 링크 매개변수와 인증 사용을 협상합니다.
7. 필요한 경우 피어가 서로를 인증합니다.
8. PPP의 NCP(Network Control Protocol)가 IPv4 또는 IPv6과 같은 네트워크 프로토콜의 사용을 협상합니다.

그러면 다이얼 아웃 시스템이 다이얼 인 서버를 통해 연결할 수 있는 호스트에 대해 `telnet` 또는 이와 유사한 명령을 실행할 수 있게 됩니다.

전용 회선 PPP 개요

기계적으로 연결된 **전용 회선** PPP 구성에는 링크로 연결된 두 피어가 사용됩니다. 이 링크는 공급자로부터 임대 받은 교환 또는 비교환 디지털 서비스로 구성됩니다. Solaris PPP 4.0은 어떠한 전이중 지점 간 전용 회선 매체를 통해서도 작동합니다. 일반적으로 회사는 네트워크 공급자로부터 기계적으로 연결된 링크를 임대 받아 ISP 또는 기타 원격 사이트에 연결합니다.

다이얼 업 링크와 전용 회선 링크 비교

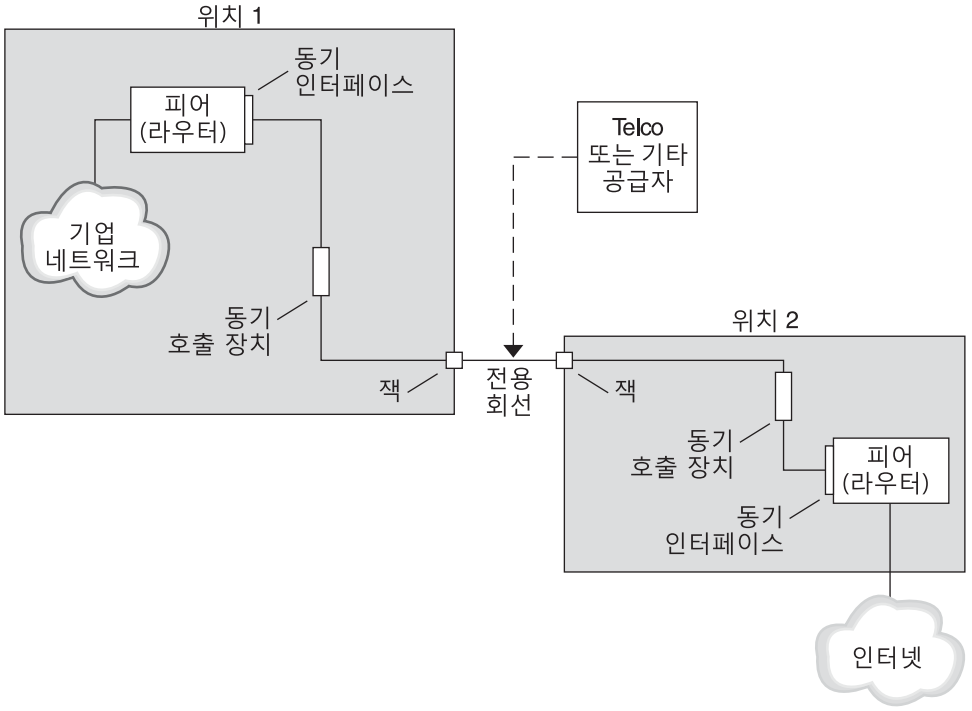
다이얼 업 링크와 전용 회선 링크 모두에는 통신 매체로 연결되는 두 피어가 사용됩니다. 다음 표에는 여러 링크 유형의 차이점이 요약되어 있습니다.

전용 회선	다이얼 업 회선
시스템 관리자나 전원 장애로 인해 전용 회선이 차단되지 않는 한 항상 연결되어 있습니다.	사용자가 원격 피어를 호출하려고 할 때 필요에 따라 시작됩니다.
동기 통신과 비동기 통신을 사용합니다. 비동기 통신의 경우 장거리 모뎀이 자주 사용됩니다.	비동기 통신을 사용합니다.
공급자로부터 임대 받습니다.	기존 전화선을 사용합니다.
동기 장치가 필요합니다.	보다 저렴한 모뎀을 사용합니다.
대부분의 SPARC 시스템에서 흔한 동기 포트가 필요합니다. 그러나 x86 시스템 및 최신 SPARC 시스템에서는 동기 포트가 흔하지 않습니다.	대부분의 컴퓨터에 포함되어 있는 표준 직렬 인터페이스를 사용합니다.

전용 회선 PPP 링크의 각 부분

다음 그림을 참조하십시오.

그림 1–3 기본 전용 회선 구성



전용 회선 링크에는 다음 부분이 포함되어 있습니다.

- **두 피어**(각 피어가 링크의 한쪽 끝에 있음). 각 피어는 워크스테이션 또는 서버일 수 있습니다. 피어는 해당 네트워크 또는 인터넷과 반대쪽 피어 간의 라우터 기능을 하는 경우가 많습니다.
- **각 피어의 동기 인터페이스**. Oracle Solaris 소프트웨어를 실행하는 일부 시스템에서는 HSI/P와 같은 동기 인터페이스 카드를 구입해야 전용 회선에 연결할 수 있습니다. UltraSPARC 워크스테이션과 같은 기타 시스템에는 내장 동기 인터페이스가 있습니다.
- **각 피어의 CSU/DSU 동기 디지털 장치**(동기 포트를 전용 회선에 연결함).

  위치에 따라 CSU를 DSU에 내장하거나, 직접 소유하거나, 공급자에게서 임대 받을 수 있습니다. DSU는 Oracle Solaris 시스템에 표준 동기 직렬 인터페이스를 제공합니다. FRAD(프레임 릴레이 액세스 장치)는 프레임 릴레이를 사용하여 직렬 인터페이스 적응을 수행합니다.
- **전용 회선**(교환 또는 비교환 디지털 서비스를 제공함). SONET/SDH, 프레임 릴레이 PVC, T1 등을 예로 들 수 있습니다.

전용 회선 통신 중 발생하는 작업

대부분의 전용 회선 유형에서 피어는 실제로 서로에게 전화를 걸지 않습니다. 대신 회사가 전용 회선 서비스를 구입하여 두 고정 위치를 명시적으로 연결합니다. 전용 회선의 각 끝에 있는 두 피어가 같은 회사의 서로 다른 물리적 위치에 있는 경우가 있습니다. ISP에 연결되어 있는 전용 회선에서 라우터를 설정하는 회사의 경우도 있습니다.

전용 회선은 다이얼 업 링크보다 덜 일반적으로 사용되지만 기계적으로 연결된 링크는 설정하기가 더 쉽습니다. 기계적으로 연결된 링크에는 채트 스크립트가 필요하지 않습니다. 회선을 임대 받는 경우에는 두 피어가 서로에게 알려져 있으므로 인증이 사용되지 않는 경우가 많습니다. 두 피어가 링크를 통해 PPP를 시작하면 링크가 활성 상태로 유지됩니다. 전용 회선 링크는 회선에 문제가 발생하거나 둘 중 하나의 피어가 명시적으로 링크를 종료하지 않는 한 활성 상태로 유지됩니다.

Solaris PPP 4.0을 실행하는 전용 회선의 피어는 다이얼 업 링크를 정의하는 구성 파일과 거의 동일한 구성 파일을 사용합니다.

전용 회선을 통해 통신을 시작하기 위해 발생하는 프로세스는 다음과 같습니다.

1. 각 피어 시스템이 부트 프로세스 또는 다른 관리 스크립트의 일환으로 `pppd` 명령을 실행합니다.
2. 피어가 해당 PPP 구성 파일을 읽습니다.
3. 피어가 통신 매개변수를 협상합니다.
4. IP 링크가 설정됩니다.

PPP 인증

인증은 개인의 자격을 확인하는 프로세스입니다. UNIX 로그인 절차는 간단한 인증 형태입니다.

1. `login` 명령이 사용자에게 이름 및 암호를 입력하라는 메시지를 표시합니다.
2. 그런 다음 `login`이 암호 데이터베이스에서 입력된 사용자 이름 및 암호를 조회하여 사용자에 대해 인증을 시도합니다.
3. 데이터베이스에 해당 사용자 이름 및 암호가 포함되어 있으면 사용자가 **인증**되고 시스템 액세스 권한을 부여받게 됩니다. 데이터베이스에 해당 사용자 이름 및 암호가 포함되어 있지 않으면 사용자에 대한 시스템 액세스 권한이 거부됩니다.

기본적으로 Solaris PPP 4.0은 기본 경로가 지정되어 있지 않은 시스템에서 인증을 요구하지 않습니다. 따라서 기본 경로가 없는 로컬 시스템은 원격 호출자를 인증하지 않습니다. 반대로, 시스템에 기본 경로가 정의되어 있으면 해당 시스템이 항상 원격 호출자를 인증합니다.

내 시스템에 대한 PPP 링크를 설정하려고 하는 호출자의 ID를 PPP 인증 프로토콜을 사용하여 확인할 수 있습니다. 반대로, 내 로컬 시스템이 호출자를 인증하는 피어를 호출해야 하는 경우 직접 PPP 인증 정보를 구성해야 합니다.

인증자 및 피인증자

PPP 링크의 호출 시스템이 **피인증자**로 간주됩니다. 이는 호출자가 자신의 ID를 원격 피어에게 증명해야 하기 때문입니다. 피어가 **인증자**로 간주됩니다. 인증자는 보안 프로토콜의 해당 PPP 파일에서 호출자의 ID를 조회하여 호출자를 인증하거나 인증하지 않습니다.

일반적으로 다이얼 업 링크에 대해 PPP 인증을 구성합니다. 호출이 시작되면 다이얼 아웃 시스템이 피인증자가 됩니다. 다이얼 인 서버는 인증자입니다. 이 서버에는 **암호** 파일의 형태로 데이터베이스가 있습니다. 이 파일에는 서버에 대한 PPP 링크를 설정할 수 있는 권한을 부여받은 모든 사용자의 목록이 나열됩니다. 이러한 사용자를 **신뢰할 수 있는 호출자**로 생각해 보십시오.

일부 다이얼 아웃 시스템에서는 원격 피어가 다이얼 아웃 시스템의 호출에 응답할 때 인증 정보를 제공해야 합니다. 그런 다음에는 역할이 바뀝니다. 즉, 원격 피어가 피인증자가 되고 다이얼 아웃 시스템이 인증자가 됩니다.

주 – PPP 4.0은 전용 회선 피어의 인증을 막지 않지만 전용 회선 링크에서는 인증이 자주 사용되지 않습니다. 전용 회선 계약의 특성상 회선 끝의 두 참가자 모두가 서로에게 알려져 있습니다. 일반적으로 두 참가자 모두를 신뢰할 수 있습니다. 그러나 PPP 인증은 관리가 그리 어렵지 않기 때문에 전용 회선에 대해 인증을 구현하는 것을 심각하게 고려해 보아야 합니다.

PPP 인증 프로토콜

PPP 인증 프로토콜은 PAP(암호 인증 프로토콜) 및 CHAP(Challenge-Handshake 인증 프로토콜)입니다. 각 프로토콜은 로컬 시스템에 연결할 수 있는 각 호출자에 대해 ID 정보가 포함된 **암호** 데이터베이스 또는 **보안 자격 증명**을 사용합니다. PAP에 대한 자세한 내용은 130 페이지 “PAP(암호 인증 프로토콜)”를 참조하십시오. CHAP 설명은 133 페이지 “CHAP(Challenge-Handshake 인증 프로토콜)”를 참조하십시오.

PPP 인증을 사용하는 이유

PPP 링크에서는 반드시 인증을 제공하지 않아도 됩니다. 또한 인증을 통해 피어를 신뢰할 수 있는지 확인할 수 있지만 PPP 인증은 데이터의 기밀성을 보장하지 않습니다. 기밀성 보장을 위해 IPsec, PGP, SSL, Kerberos 및 Secure Shell과 같은 암호화 소프트웨어를 사용하십시오.

주 – Solaris PPP 4.0은 RFC 1968에 기술되어 있는 PPP ECP(암호화 제어 프로토콜)를 구현하지 않습니다.

다음과 같은 경우 PPP 인증을 구현할 수 있습니다.

- 회사가 공개 교환 전화 네트워크를 통해 사용자로부터의 수신 호출을 받는 경우
- 회사 보안 정책상 원격 사용자가 회사 방화벽을 통해 네트워크에 액세스하거나 보안 트랜잭션에 참여할 때 인증 자격 증명을 제공해야 하는 경우
- 호출자를 `/etc/passwd`, NIS, LDAP 또는 PAM과 같은 표준 UNIX 암호 데이터베이스에 대해 인증하려는 경우. 이 시나리오의 경우 PAP 인증을 사용합니다.
- 회사의 다이얼 인 서버도 네트워크의 인터넷 연결을 제공하는 경우. 이 시나리오의 경우 PAP 인증을 사용합니다.
- 링크의 각 끝에 있는 시스템 또는 네트워크에서 직렬 회선은 암호 데이터베이스보다 덜 안전합니다. 이 시나리오의 경우 CHAP 인증을 사용합니다.

PPPoE를 통한 DSL 사용자 지원

많은 네트워크 공급자와 재택 근무 사용자가 DSL(디지털 가입자 회선) 기술을 사용하여 빠른 네트워크 액세스를 제공합니다. DSL 사용자를 지원하기 위해 Solaris PPP 4.0에는 PPPoE(PPP over Ethernet) 기능이 포함되어 있습니다. PPPoE 기술을 사용하면 여러 호스트가 하나의 이더넷 링크를 통해 하나 이상의 대상으로 PPP 세션을 실행할 수 있습니다.

다음 중 하나에 해당되는 경우 PPPoE를 사용해야 합니다.

- DSL 사용자(본인도 포함될 수 있음)를 지원합니다. DSL 서비스 공급자가 DSL 회선을 통해 서비스를 받으려는 사용자에게 PPPoE 터널을 구성할 것을 요청할 수 있습니다.
- 사이트가 고객에게 PPPoE를 제공하려는 ISP입니다.

이 절에서는 PPPoE와 관련된 용어를 소개하고 기본 PPPoE 토폴로지에 대한 개요를 제공합니다.

PPPoE 개요

*PPPoE*는 RedBack Networks의 독점 프로토콜입니다. PPPoE는 다른 버전의 표준 PPP가 아니라 검색 프로토콜입니다. PPPoE 시나리오에서는 먼저 PPP 통신을 시작하는 시스템이 PPPoE를 실행하는 피어를 찾거나 **발견**해야 합니다. PPPoE 프로토콜은 이더넷 브로드캐스트 패킷을 사용하여 피어를 찾습니다.

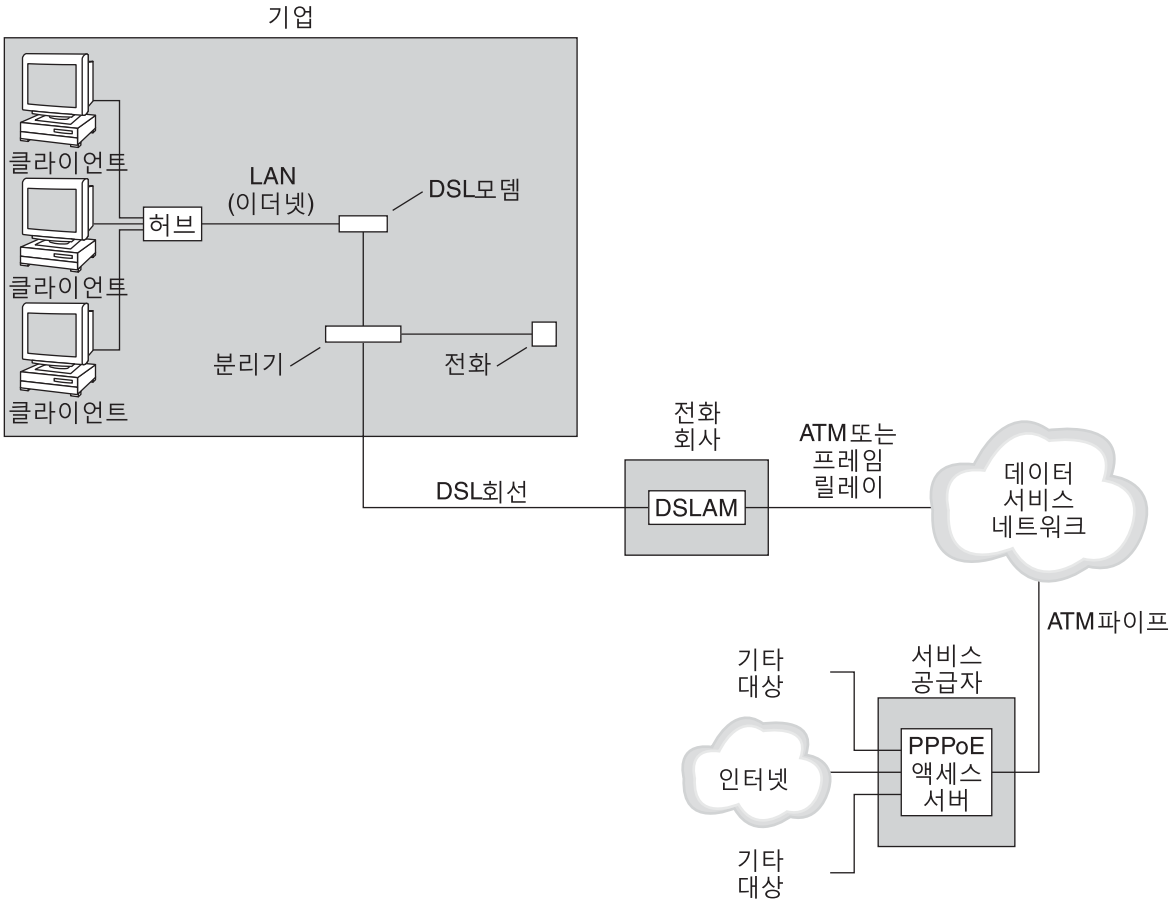
검색 프로세스 후에 PPPoE는 시작 호스트 또는 *PPPoE* **클라이언트**에서 피어 또는 *PPPoE* **액세스 서버**까지 이더넷 기반 터널을 설정합니다. **터널링**은 한 프로토콜을 기반으로 다른 프로토콜을 실행하는 방법입니다. Solaris PPP 4.0은 PPPoE를 사용하여 PPP over

Ethernet IEEE 802.2를 터널링합니다(둘 다 데이터 링크 프로토콜임). 결과 PPP 연결은 PPPoE 클라이언트와 액세스 서버 간의 전용 링크처럼 동작합니다. PPPoE에 대한 자세한 내용은 138 페이지 “DSL 지원을 위해 PPPoE 터널 만들기”를 참조하십시오.

PPPoE 구성의 각 부분

PPPoE 구성에는 다음 그림에서 볼 수 있는 것과 같이 소비자, 전화 회사 및 서비스 공급자라는 세 참가자가 포함됩니다.

그림 1–4 PPPoE 터널의 참가자



PPPoE 소비자

시스템 관리자는 소비자의 PPPoE 구성을 지원해야 할 수 있습니다. 일반적인 한 PPPoE 소비자 유형에는 DSL 회선을 통해 PPPoE를 실행해야 하는 사용자가 있습니다. 다른 PPPoE 소비자에는 이전 그림에서 볼 수 있는 것과 같이 직원이 PPPoE 터널을 실행할 수 있는 DSL 회선을 구입하는 회사가 있습니다.

기업 사용자는 고속 DSL 장치를 통해 여러 호스트에 PPP 통신을 제공하기 위해 주로 PPPoE를 사용합니다. 단일 PPPoE 클라이언트에 개별 *DSL* **모뎀**이 있는 경우가 많습니다. 또는 허브에 있는 클라이언트 그룹이 이더넷 회선으로 역시 허브에 연결되어 있는 DSL 모뎀을 공유할 수 있습니다.

주 – DSL 장치는 원칙적으로 모뎀이 아니라 브릿지입니다. 그러나 보통 이러한 장치를 모뎀이라고 지칭하므로 이 설명서에서는 "DSL 모뎀"이라는 용어를 사용합니다.

PPPoE는 DSL 모뎀에 연결되어 있는 이더넷 회선 상의 터널을 통해 PPP를 실행합니다. 해당 회선은 분리기에 연결되어 있고, 분리기는 전화선에 연결됩니다.

전화 회사의 PPPoE

전화 회사는 PPPoE 시나리오의 중간 계층입니다. 전화 회사는 전화선을 통해 받는 신호를 *DSLAM(Digital Subscriber Line Access Multiplexer)*이라는 장치를 사용하여 분리합니다. DSLAM은 신호를 별도의 전화선, 전화 서비스용 아날로그 전화선 및 PPPoE용 디지털 전화선으로 분리합니다. DSLAM에서 디지털 전화선은 터널을 ATM 데이터 네트워크를 통해 ISP로 확장합니다.

서비스 공급자의 PPPoE

ISP는 브릿지를 통해 ATM 데이터 네트워크에서 PPPoE 전송을 받습니다. ISP에서는 PPPoE를 실행하는 액세스 서버가 PPP 링크의 피어 역할을 합니다. 액세스 서버는 기능면에서 그림 1–2에서 소개된 다이얼 인 서버와 매우 유사하지만 액세스 서버는 모뎀을 사용하지 않습니다. 액세스 서버는 개별 PPPoE 세션을 일반 IP 트래픽(예: 인터넷 액세스)으로 변환합니다.

ISP의 시스템 관리자는 액세스 서버를 구성하고 유지 관리해야 할 수 있습니다.

PPPoE 터널의 보안

PPPoE 터널은 본질적으로 안전하지 않습니다. PAP 또는 CHAP를 사용하여 터널을 통해 실행되는 PPP 링크에 대한 사용자 인증을 제공할 수 있습니다.

◆ ◆ ◆ 2 장

2 PPP 링크 계획(작업)

PPP 링크를 설정하려면 여러 가지 별개의 작업(계획 작업 및 PPP와 관련되지 않은 기타 작업 포함)을 수행해야 합니다. 이 장에서는 가장 일반적인 PPP 링크, 인증 및 PPPoE를 계획하는 방법에 대해 설명합니다.

2 장, "PPP 링크 계획(작업)" 다음에 오는 작업 장에는 특정 링크를 설정하는 방법을 보여주기 위해 샘플 구성이 사용됩니다. 이러한 샘플 구성은 이 장에서 소개됩니다.

다음과 같은 항목을 다룹니다.

전반적인 PPP 계획(작업 맵)

링크를 설정하려면 PPP에 계획 작업이 필요합니다. 또한 PPPoE 터널링을 사용하려는 경우에는 먼저 PPP 링크를 설정한 다음 터널링을 제공해야 합니다. 다음 작업 맵에는 이 장에 설명되어 있는 대규모 계획 작업이 나열되어 있습니다. 구성할 링크 유형에 대해 일반적인 작업만 사용해야 할 수도 있습니다. 또는 링크, 인증 및 PPPoE에 대한 작업이 필요할 수 있습니다.

표 2–1 PPP 계획 작업 맵

작업	설명	수행 방법
다이얼 업 PPP 링크 계획	다이얼 아웃 시스템 또는 다이얼 인 서버를 설정하는 데 필요한 정보 수집	34 페이지 "다이얼 업 PPP 링크 계획"
전용 회선 링크 계획	전용 회선에서 클라이언트를 설정하는 데 필요한 정보 수집	37 페이지 "전용 회선 링크 계획"

표 2–1 PPP 계획 작업 맵 (계속)

작업	설명	수행 방법
PPP 링크에서 인증 계획	PPP 링크에서 PAP 또는 CHAP 인증을 구성하는 데 필요한 정보 수집	39 페이지 “링크에서 인증 계획”
PPPoE 터널 계획	PPP 링크를 실행할 수 있는 PPPoE 터널을 설정하는 데 필요한 정보 수집	44 페이지 “PPPoE 터널을 통한 DSL 지원 계획”

다이얼 업 PPP 링크 계획

다이얼 업 링크는 가장 일반적으로 사용되는 PPP 링크입니다. 이 절에는 다음과 같은 정보가 포함되어 있습니다.

- 다이얼 업 링크에 대한 계획 정보
- 3 장, “다이얼 업 PPP 링크 설정(작업)”에 사용될 샘플 링크에 대한 설명

일반적으로 다이얼 업 PPP 링크, 다이얼 아웃 시스템 또는 다이얼 인 서버의 한쪽 끝에서만 시스템을 구성합니다. 다이얼 업 PPP에 대한 소개는 23 페이지 “다이얼 업 PPP 개요”를 참조하십시오.

다이얼 아웃 시스템을 설정하기 전에

다이얼 아웃 시스템을 구성하기 전에 다음 표에 나열된 정보를 수집하십시오.

주 – 이 절의 계획 정보에는 인증 또는 PPPoE에 대해 수집할 정보는 포함되어 있지 않습니다. 인증 계획에 대한 자세한 내용은 39 페이지 “링크에서 인증 계획”을 참조하십시오. PPPoE 계획은 44 페이지 “PPPoE 터널을 통한 DSL 지원 계획”을 참조하십시오.

표 2–2 다이얼 아웃 시스템에 대한 정보

정보	작업
최대 모뎀 속도	모뎀 제조업체가 제공하는 설명서를 참조하십시오.
모뎀 연결 명령(AT 명령)	모뎀 제조업체가 제공하는 설명서를 참조하십시오.
링크의 다른 쪽 끝에서 다이얼 인 서버에 사용할 이름	다이얼 인 서버를 식별하는 데 도움이 되는 이름을 만듭니다.
다이얼 인 서버에 필요했던 로그인 절차	다이얼 인 서버의 관리자에게 문의하거나 다이얼 인 서버가 ISP에 있는 경우 ISP 설명서를 참조하십시오.

다이얼 인 서버를 설정하기 전에

다이얼 인 서버를 구성하기 전에 다음 표에 나열된 정보를 수집하십시오.

주 – 이 절의 계획 정보에는 인증 또는 PPPoE에 대해 수집할 정보는 포함되어 있지 않습니다. 인증 계획에 대한 자세한 내용은 39 페이지 “링크에서 인증 계획”을 참조하십시오. PPPoE 계획은 44 페이지 “PPPoE 터널을 통한 DSL 지원 계획”을 참조하십시오.

표 2–3 다이얼 인 서버에 대한 정보

정보	작업
최대 모뎀 속도	모뎀 제조업체가 제공하는 설명서를 참조하십시오.
다이얼 인 서버를 호출할 수 있는 사람의 사용자 이름	잠재적 사용자의 홈 디렉토리를 설정하기 전에 58 페이지 “다이얼 인 서버의 사용자를 구성하는 방법”에 설명된 대로 해당 사용자의 이름을 얻으십시오.
PPP 통신을 위한 전용 IP 주소	회사의 IP 주소 위임 담당자에게서 주소를 얻으십시오.

다이얼 업 PPP 구성의 예

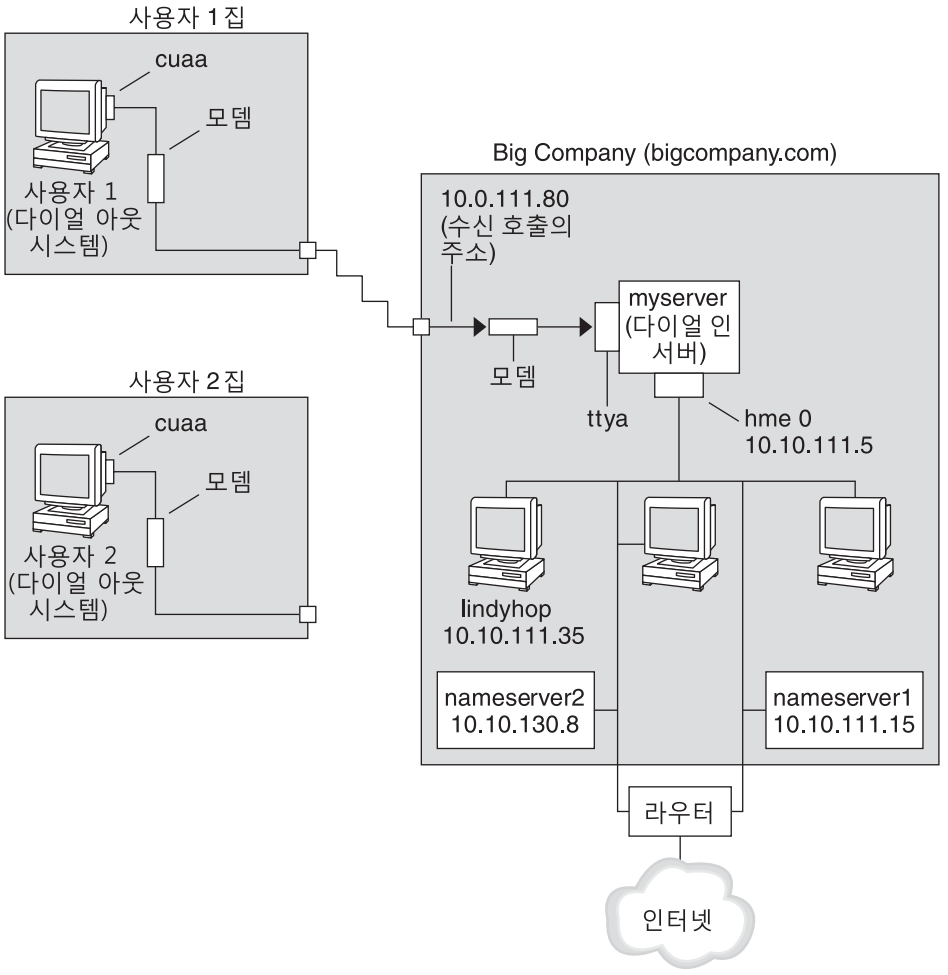
3 장, “다이얼 업 PPP 링크 설정(작업)”에서 소개될 작업은 직원들이 한 주에 몇 번은 집에서 일할 수 있도록 하려는 소기업의 요구 사항을 실행에 옮깁니다. 일부 직원의 경우 홈 시스템에 Oracle Solaris OS가 필요합니다. 또한 이러한 작업자는 회사 인트라넷에서 자신의 시스템으로 원격 로그인해야 합니다.

작업은 다음 기능과의 기본적인 다이얼 업 링크를 설정합니다.

- **다이얼 아웃** 시스템은 회사 인트라넷을 호출해야 하는 직원의 집에 있습니다.
- **다이얼 인** 서버는 회사 인트라넷에서 직원으로부터의 수신 호출을 받도록 구성된 시스템입니다.
- 다이얼 아웃 시스템을 인증하는 데에는 UNIX 스타일의 로그인이 사용됩니다. 회사의 보안 정책상 더 강력한 Solaris PPP 4.0 인증 방법이 필요하지 않습니다.

다음 그림에서는 3 장, “다이얼 업 PPP 링크 설정(작업)”에서 설정된 링크를 보여줍니다.

그림 2–1 샘플 다이얼 업 링크



이 그림에서는 원격 호스트가 전화선을 통해 모뎀을 사용하여 Big Company의 인트라넷으로 다이얼 아웃합니다. 다른 호스트도 Big Company로 다이얼 아웃하도록 구성되어 있지만 현재 비활성 상태입니다. 원격 사용자로부터의 호출은 Big Company에 있는 다이얼 인 서버에 연결된 모뎀이 받는 순서대로 응답됩니다. PPP 연결이 피어 간에 설정됩니다. 그러면 다이얼 아웃 시스템이 인트라넷에 있는 호스트 시스템에 원격 로그인할 수 있습니다.

다이얼 업 PPP에 대한 추가 정보

다음을 참조하십시오.

- 다이얼 아웃 시스템을 설정하려면 표 3–2를 참조하십시오.
- 다이얼 인 시스템을 설정하려면 표 3–3을 참조하십시오.
- 다이얼 업 링크에 대한 개요를 보려면 23 페이지 “다이얼 업 PPP 개요”를 참조하십시오.
- PPP 파일 및 명령에 대한 자세한 내용을 보려면 109 페이지 “파일 및 명령줄에서 PPP 옵션 사용”을 참조하십시오.

전용 회선 링크 계획

전용 회선 링크를 설정하려면 공급자에게서 임대 받은 교환 또는 비교환 서비스의 한쪽 끝에서 피어를 구성해야 합니다.

이 절에는 다음과 같은 정보가 포함되어 있습니다.

- 전용 회선 링크에 대한 계획 정보
- 그림 2–2에 나와 있는 샘플 링크에 대한 설명

전용 회선 링크에 대한 소개는 26 페이지 “전용 회선 PPP 개요”를 참조하십시오. 전용 회선 설정 작업은 4 장, “전용 회선 PPP 링크 설정(작업)”을 참조하십시오.

전용 회선 링크를 설정하기 전에

회사가 네트워크 공급자로부터 전용 회선 링크를 임대 받는 경우에는 일반적으로 링크의 본인 쪽 끝에 있는 시스템만 구성합니다. 링크의 다른 쪽 끝에 있는 피어는 다른 관리자가 유지 관리합니다. 이 사람은 회사의 원격 위치에 있는 시스템 관리자나 ISP에 있는 시스템 관리자일 수 있습니다.

전용 회선 링크에 필요한 하드웨어

링크의 본인 쪽 끝에는 링크 매체 외에 다음 하드웨어가 필요합니다.

- 시스템을 위한 동기 인터페이스
- 동기 장치(CSU/DSU)
- 시스템

일부 네트워크 공급자의 경우 라우터, 동기 인터페이스 및 CSU/DSU를 CPE(고객 댁내 장치)의 일부로 포함합니다. 그러나 필요한 장비는 공급자와 현지 정부 제한에 따라 달라집니다. 네트워크 공급자가 필요한 장치에 대한 정보를 제공해 줄 수 있습니다(이 장비가 전용 회선에 제공되지 않은 경우).

전용 회선 링크에 대해 수집해야 하는 정보

로컬 피어를 구성하기 전에 다음 표에 나열된 항목을 수집해야 할 수 있습니다.

표 2–4 전용 회선 링크 계획

정보	작업
인터페이스의 장치 이름	인터페이스 카드 설명서를 참조하십시오.
동기 인터페이스 카드에 대한 구성 지침	인터페이스 카드 설명서를 참조하십시오. HSI/P 인터페이스를 구성하려면 이 정보가 필요합니다. 다른 유형의 인터페이스 카드를 구성해야 할 수도 있습니다.
(옵션) 원격 피어의 IP 주소	서비스 공급자 설명서를 참조하십시오. 또는 원격 피어의 시스템 관리자에게 문의하십시오. 이 정보는 두 피어 간에 IP 주소가 협상되지 않은 경우에만 필요합니다.
(옵션) 원격 피어의 이름	서비스 공급자 설명서를 참조하십시오. 또는 원격 피어의 시스템 관리자에게 문의할 수 있습니다.
(옵션) 링크의 속도	서비스 공급자 설명서를 참조하십시오. 또는 원격 피어의 시스템 관리자에게 문의할 수 있습니다.
(옵션) 원격 피어에 사용되는 압축	서비스 공급자 설명서를 참조하십시오. 또는 원격 피어의 시스템 관리자에게 문의할 수 있습니다.

전용 회선 링크 구성의 예

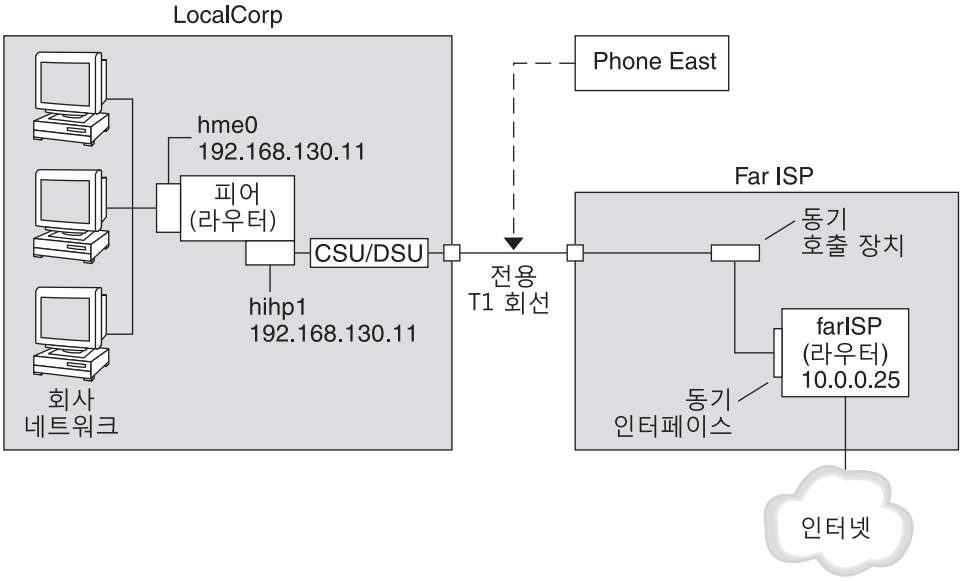
4 장, “전용 회선 PPP 링크 설정(작업)”의 작업에서는 직원에게 인터넷 액세스를 제공하려는 중소 규모 조직(LocalCorp)의 목표를 달성하는 방법을 보여줍니다. 현재는 직원의 컴퓨터가 개인 회사 인트라넷에서 연결되어 있습니다.

LocalCorp는 빠른 트랜잭션을 필요로 하며 인터넷에 있는 많은 리소스에 액세스해야 합니다. 이 기업은 자체 전용 회선을 설정할 수 있게 해 주는 서비스 공급자인 Far ISP와 계약을 맺고 있으며, 전화 회사인 Phone East로부터 T1 회선도 임대 받고 있습니다. Phone East는 전용 회선을 LocalCorp와 Far ISP 사이에 놓았습니다. 그리고 Phone East는 이미 LocalCorp로 구성되어 있는 CSU/DSU를 제공합니다.

작업은 다음 특징을 가지는 전용 회선 링크를 설정합니다.

- LocalCorp는 전용 회선을 통해 인터넷 상의 호스트로 패킷을 전달하는 게이트웨이 라우터로 시스템을 설정했습니다.
- Far ISP도 고객의 전용 회선이 연결되는 라우터로 피어를 설정했습니다.

그림 2–2 전용 회선 구성의 예



그림에서는 LocalCorp에서 PPP에 대해 라우터가 설정되어 있습니다. 이 라우터는 해당 `hme0` 인터페이스를 통해 회사 인트라넷에 연결됩니다. 두번째 연결은 시스템의 HSI/P 인터페이스(hihp1)를 통해 CSU/DSU 디지털 장치로 이루어집니다. 그런 다음 CSU/DSU가 설치된 전용 회선에 연결됩니다. LocalCorp의 관리자가 HSI/P 인터페이스와 PPP 파일을 구성합니다. 그런 다음 관리자는 `/etc/init.d/pppd`를 입력하여 LocalCorp와 Far ISP 간에 링크를 시작합니다.

전용 회선에 대한 추가 정보

다음을 참조하십시오.

- 4 장, “전용 회선 PPP 링크 설정(작업)”
- 26 페이지 “전용 회선 PPP 개요”

링크에서 인증 계획

이 절에는 PPP 링크에서 인증을 제공하기 위한 계획 정보가 포함되어 있습니다. 사이트에서 PPP 인증을 구현하는 작업은 5 장, “PPP 인증 설정(작업)”에 있습니다.

PPP는 PAP와 CHAP라는 두 가지 유형의 인증을 제공합니다. PAP는 130 페이지 “PAP(암호 인증 프로토콜)”에 자세히 설명되어 있고, CHAP는 133 페이지 “CHAP(Challenge-Handshake 인증 프로토콜)”에 설명되어 있습니다.

링크에서 인증을 설정하기 전에 사이트의 보안 정책에 가장 잘 맞는 인증 프로토콜이 무엇인지 선택해야 합니다. 그런 다음 다이얼 인 시스템 또는 호출자의 다이얼 아웃 시스템이나 두 시스템 유형 모두에 대해 암호 파일 및 PPP 구성 파일을 설정합니다. 사이트에 적합한 인증 프로토콜을 선택하는 방법에 대한 자세한 내용은 29 페이지 “PPP 인증을 사용하는 이유”를 참조하십시오.

이 절에는 다음과 같은 정보가 포함되어 있습니다.

- PAP 및 CHAP 인증 모두에 대한 계획 정보
- 그림 2–3 및 그림 2–4에 나와 있는 샘플 인증 시나리오에 대한 설명

인증 설정 작업은 5 장, “PPP 인증 설정(작업)”을 참조하십시오.

PPP 인증을 설정하기 전에

사이트에서 인증을 설정하는 작업은 전반적인 PPP 전략의 필수 요소가 되어야 합니다. 인증을 구현하기 전에 하드웨어를 조립하고, 소프트웨어를 구성하고, 링크를 테스트해야 합니다.

표 2–5 인증 구성 전의 필수 조건

정보	수행 방법
다이얼 업 링크 구성 작업	3 장, “다이얼 업 PPP 링크 설정(작업)”
링크 테스트 작업	7 장, “일반적인 PPP 문제 해결(작업)”
사이트의 보안 요구 사항	회사의 보안 정책입니다. 정책이 없는 경우 PPP 인증을 설정하면 보안 정책을 만들 수 있습니다.
사이트에서 PAP를 사용할지, 아니면 CHAP를 사용할지에 대한 제안 사항	29 페이지 “PPP 인증을 사용하는 이유” 이러한 프로토콜에 대한 자세한 내용은 130 페이지 “링크에서 호출자 인증”을 참조하십시오.

PPP 인증 구성의 예

이 절에는 5 장, “PPP 인증 설정(작업)”의 절차에 사용될 인증 시나리오의 예가 포함되어 있습니다.

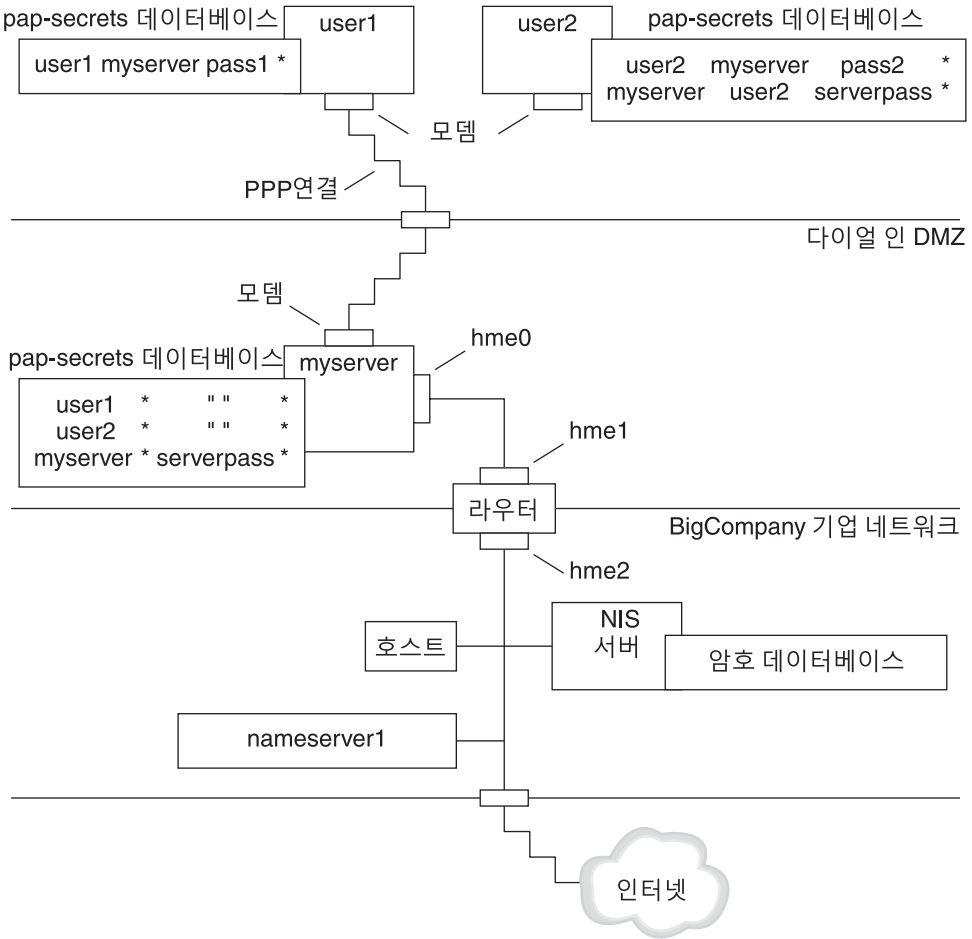
- 40 페이지 “PAP 인증을 사용한 구성의 예”
- 42 페이지 “CHAP 인증을 사용한 구성의 예”

PAP 인증을 사용한 구성의 예

70 페이지 “PAP 인증 구성”의 작업에서는 PPP 링크를 통해 PAP 인증을 설정하는 방법을 보여줍니다. 절차에는 35 페이지 “다이얼 업 PPP 구성의 예”에 나오는 가상 회사 “Big Company”에 대해 만들어진 PAP 시나리오가 예로 사용됩니다.

Big Company는 사용자가 집에서 일할 수 있게 만드는 것을 목표로 하고 있습니다. 시스템 관리자는 다이얼 인 서버에 연결되는 직렬 회선을 위한 보안 솔루션을 구현할 계획을 가지고 있습니다. 과거에는 NIS 암호 데이터베이스를 사용하는 UNIX 스타일의 로그인이 Big Company의 네트워크에서 충분히 그 역할을 했습니다. 시스템 관리자는 PPP 링크를 통해 네트워크로 들어오는 호출에 UNIX 스타일의 인증 체계를 구현하려고 합니다. 이에 따라 관리자는 PAP 인증을 사용하는 다음 시나리오를 구현합니다.

그림 2–3 PAP 인증 시나리오의 예(재택 근무)



시스템 관리자는 나머지 회사 네트워크와 라우터로 분리되는 전용 다이얼 인 DMZ를 만듭니다. DMZ라는 용어는 군사 용어인 "비무장 지대"에서 유래한 것입니다. DMZ는 보안을 위해 설정된 격리 네트워크입니다. 일반적으로 DMZ에는 웹 서버, 익명 FTP 서버,

데이터베이스 및 모뎀 서버와 같이 회사가 공개하는 리소스가 포함됩니다. 네트워크 디자이너는 종종 방화벽과 회사의 인터넷 연결 사이에 DMZ를 배치합니다.

그림 2–3에서 볼 수 있는 DMZ 점유자는 다이얼 인 서버 `myserver`와 라우터뿐입니다. 다이얼 인 서버를 사용하려면 호출자가 링크를 설정할 때 사용자 이름 및 암호를 포함한 PAP 자격 증명을 제공해야 합니다. 또한 다이얼 인 서버에는 PAP의 `login` 옵션이 사용됩니다. 따라서 호출자의 PAP 사용자 이름 및 암호가 다이얼 인 서버의 암호 데이터베이스에 있는 UNIX 사용자 이름 및 암호와 정확히 일치해야 합니다.

PPP 링크가 설정된 후에는 호출자의 패킷이 라우터로 전달됩니다. 라우터는 회사 네트워크 대상이나 인터넷 대상으로 전송을 전달합니다.

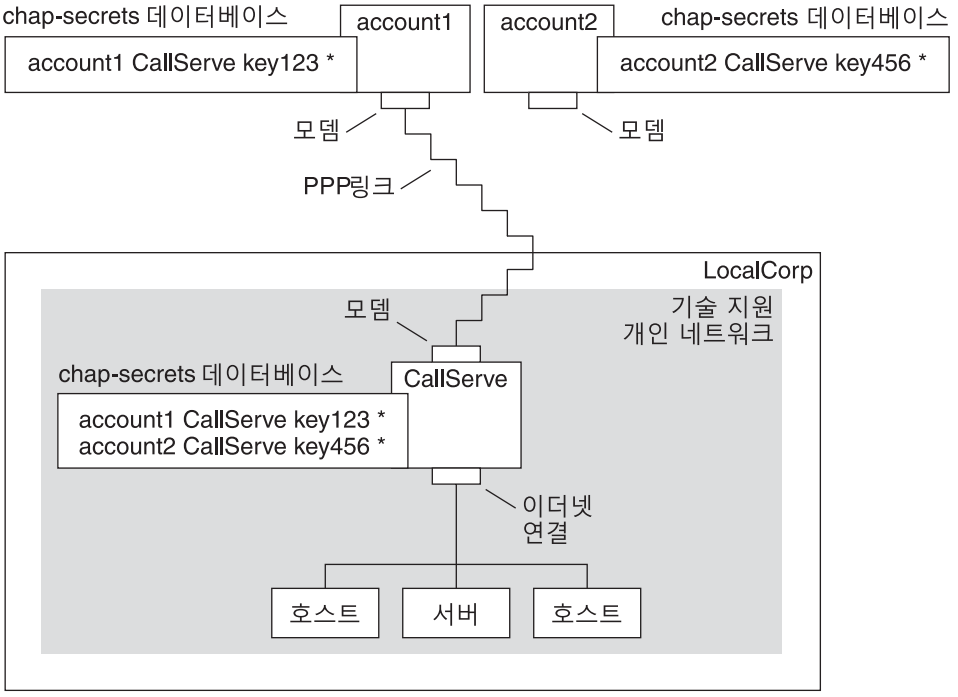
CHAP 인증을 사용한 구성의 예

77 페이지 “CHAP 인증 구성”의 작업에서는 CHAP 인증을 설정하는 방법을 보여줍니다. 절차에는 38 페이지 “전용 회선 링크 구성의 예”에서 소개된 가상 회사 LocalCorp에 대해 만들어질 CHAP 시나리오가 예로 사용됩니다.

LocalCorp는 ISP에 대한 전용 회선을 통해 인터넷 연결을 제공합니다. LocalCorp의 기술 지원부는 상당한 네트워크 트래픽을 발생시킵니다. 따라서 기술 지원부에는 격리된 자체 개인 네트워크가 필요합니다. 이 부서의 현장 기술자는 광범위한 지역을 다니며, 문제 해결 정보를 얻기 위해 원격 위치에서 기술 지원 네트워크에 액세스해야 합니다. 개인 네트워크의 데이터베이스에 있는 민감한 정보를 보호하기 위해 원격 호출자는 인증을 받아 로그인 권한을 부여받아야 합니다.

이에 따라 시스템 관리자는 다이얼 업 PPP 구성을 위해 다음 CHAP 인증 시나리오를 구현합니다.

그림 2–4 CHAP 인증 시나리오의 예(개인 네트워크 호출)



기술 지원 네트워크에서 외부 세계로 연결되는 링크는 링크의 다이얼 인 서버의 끝에 연결되는 직렬 회선뿐입니다. 시스템 관리자는 각 현장 서비스 담당자의 랩탑 컴퓨터를 CHAP 보안이 적용된 PPP(CHAP 암호 포함)용으로 구성합니다. 다이얼 인 서버에 있는 chap-secrets 데이터베이스에는 기술 지원 네트워크를 호출할 수 있는 모든 시스템의 CHAP 자격 증명이 포함되어 있습니다.

인증에 대한 추가 정보

다음 중에서 선택하십시오.

- 70 페이지 “PAP 인증 구성”을 참조하십시오.
- 77 페이지 “CHAP 인증 구성”을 참조하십시오.
- 130 페이지 “링크에서 호출자 인증” 및 pppd(1M) 매뉴얼 페이지를 참조하십시오.

PPPoE 터널을 통한 DSL 지원 계획

공급자의 DSL 회선 및 고속 디지털 네트워크를 통해 PPP를 실행하기 위해 사이트에 PPPoE 터널링을 설정할 것을 요청하는 DSL 공급자도 있습니다. PPPoE의 개요는 30 페이지 “PPPoE를 통한 DSL 사용자 지원”을 참조하십시오.

PPPoE 터널에는 소비자, 전화 회사 및 ISP라는 세 참가자가 관련됩니다. 소비자(회사에 있는 PPPoE 클라이언트 또는 개인 소비자)를 위해 PPPoE를 구성하거나 ISP에 있는 서버에서 PPPoE를 구성합니다.

이 절에는 클라이언트와 액세스 서버 모두에서 PPPoE를 실행하기 위한 계획 정보가 포함되어 있습니다. 다음 항목을 다룹니다.

- PPPoE 호스트 및 액세스 서버에 대한 계획 정보
- 45 페이지 “PPPoE 터널 구성의 예”에서 소개된 PPPoE 시나리오에 대한 설명

PPPoE 터널 설정 작업은 6 장, “PPPoE 터널 설정(작업)”을 참조하십시오.

PPPoE 터널을 설정하기 전에

미리 구성 작업은 터널의 클라이언트측을 구성하는지, 아니면 서버측을 구성하는지에 따라 달라집니다. 어떤 경우든 관리자나 기업은 전화 회사와 계약을 맺어야 합니다. 전화 회사는 클라이언트용 DSL 회선과 어떤 형태로든 브리징을 제공하며 액세스 서버용 ATM 파이프를 제공할 수도 있습니다. 대부분의 계약에서 전화 회사는 사이트에서 장비를 조립합니다.

PPPoE 클라이언트를 구성하기 전에

PPPoE 클라이언트 구현은 일반적으로 다음 장비로 구성됩니다.

- 개인용 컴퓨터 또는 개인이 사용하는 기타 시스템
- DSL 모뎀(일반적으로 전화 회사 또는 인터넷 액세스 공급자가 설치함)
- (옵션) 허브(기업 DSL 소비자와 같이 둘 이상의 클라이언트를 사용하는 경우)
- (옵션) 분리기(일반적으로 공급자가 설치함)

다양한 DSL 구성이 가능합니다. 구성은 사용자 또는 기업의 요구와 공급자가 제공하는 서비스에 따라 달라집니다.

표 2–6 PPPoE 클라이언트 계획

정보	작업
개인 또는 자신을 위해 홈 PPPoE 클라이언트를 설정하는 경우에는 PPPoE 범위 밖에 있는 모든 설정 정보를 가져와야 합니다.	필요한 설정 절차는 전화 회사나 ISP에 문의하십시오.

표 2–6 PPPoE 클라이언트 계획 *(계속)*

정보	작업
회사 사이트에서 PPPoE 클라이언트를 설정하는 경우에는 PPPoE 클라이언트 시스템을 지정받는 사용자의 이름을 수집해야 합니다. 원격 PPPoE 클라이언트를 구성하는 경우 홈 DSL 장비 추가에 대한 정보를 사용자에게 제공해 주어야 할 수 있습니다.	권한이 부여된 사용자 목록은 회사 관리부에 문의하십시오.
PPPoE 클라이언트에서 사용 가능한 인터페이스가 무엇인지 알아봅니다.	인터페이스 이름을 가져오려면 각 시스템에서 `ipadm show-addr` 명령을 실행합니다.
(옵션) PPPoE 클라이언트의 암호를 가져옵니다.	사용자에게 선호하는 암호가 무엇인지 물어보거나 사용자에게 암호를 지정합니다. 이 암호는 UNIX 로그인이 아니라 링크 인증에 사용됩니다.

PPPoE 서버를 구성하기 전에

PPPoE 액세스 서버를 계획할 때는 데이터 서비스 네트워크에 대한 연결을 제공하는 전화 회사와 협력해야 합니다. 전화 회사는 해당 회선(일반적으로 ATM 파이프)을 사이트에 설치하고 어떤 형태로든 액세스 서버에 브리징을 제공합니다. 관리자는 회사가 제공하는 서비스에 액세스하는 이더넷 인터페이스를 구성해야 합니다. 예를 들어, 관리자는 인터넷 액세스용 인터페이스와 전화 회사 브릿지의 이더넷 인터페이스를 구성해야 합니다.

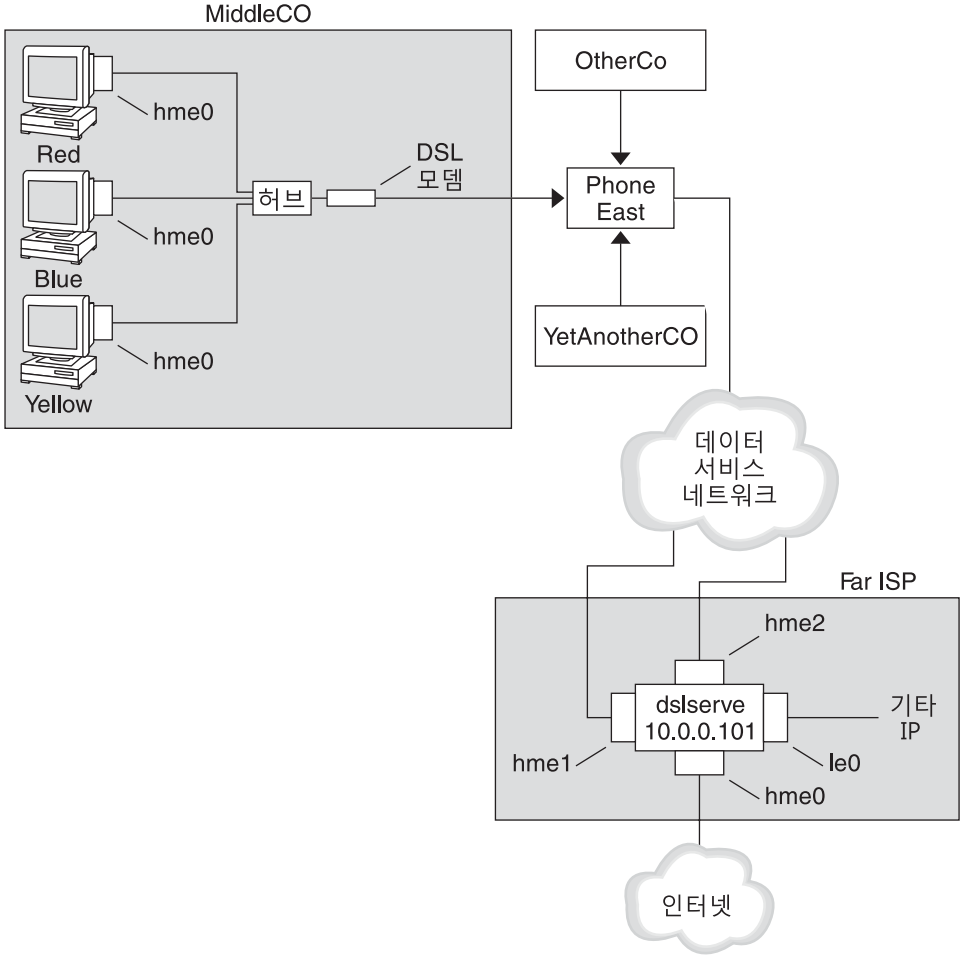
표 2–7 PPPoE 액세스 서버 계획

정보	작업
데이터 서비스 네트워크의 회선에 사용되는 인터페이스	인터페이스를 식별하려면 `ipadm show-addr` 명령을 실행합니다.
PPPoE 서버에서 제공할 서비스 유형	관리부와 네트워크 기획자에게 요구 사항 및 제안 사항이 있는지 문의하십시오.
(옵션) 소비자에게 제공할 서비스 유형	관리부와 네트워크 기획자에게 요구 사항 및 제안 사항이 있는지 문의하십시오.
(옵션) 원격 클라이언트의 호스트 이름 및 암호	네트워크 기획자와 사이트의 다른 사람에게 계약 협상 담당자가 누구인지 문의하십시오. 호스트 이름 및 암호는 UNIX 로그인이 아니라 PAP 또는 CHAP 인증에 사용됩니다.

PPPoE 터널 구성의 예

이 절에는 6 장, “PPPoE 터널 설정(작업)”의 작업에 대한 실례로 사용된 PPPoE 터널의 예가 포함되어 있습니다. 그림에는 터널의 모든 참가자가 표시되어 있지만 관리자는 클라이언트측 또는 서버측 중 한쪽 끝만 관리합니다.

그림 2–5 PPPoE 터널의 예



샘플에서는 MiddleCo가 직원들에게 고속 인터넷 액세스를 제공하려고 합니다. MiddleCo는 Phone East로부터 DSL 패키지를 구입하고 Phone East는 서비스 공급자인 Far ISP와 계약을 맺습니다. Far ISP는 Phone East로부터 DSL을 구입하는 고객에게 인터넷 및 기타 IP 서비스를 제공합니다.

PPPoE 클라이언트 구성의 예

MiddleCo가 사이트에 하나의 DSL 회선을 제공하는 Phone East로부터 패키지를 구입합니다. 패키지에는 MiddleCo의 PPPoE 클라이언트용 ISP에 대한 인증된 전용 연결이 포함되어 있습니다. 시스템 관리자가 잠재적 PPPoE 클라이언트를 허브에 케이블로 연결합니다. Phone East 기술자가 허브를 자사 DSL 장비에 케이블로 연결합니다.

PPPoE 서버 구성의 예

FarISP가 Phone East와 맺은 사업 계약을 이행하기 위해 FarISP의 시스템 관리자가 액세스 서버 `dslserve`를 구성합니다. 이 서버에는 다음과 같은 네 가지 인터페이스가 있습니다.

- `eri0` – 로컬 네트워크에 연결되는 주 네트워크 인터페이스
- `hme0` – FarISP가 고객에게 인터넷 서비스를 제공하는 데 사용하는 인터페이스
- `hme1` – 인증된 PPPoE 터널을 위해 MiddleCo가 계약한 인터페이스
- `hme2` – PPPoE 터널을 위해 다른 고객이 계약한 인터페이스

PPPoE에 대한 추가 정보

다음 중에서 선택하십시오.

- 84 페이지 “PPPoE 클라이언트 설정”을 참조하십시오.
- 87 페이지 “PPPoE 액세스 서버 설정”을 참조하십시오.
- 138 페이지 “DSL 지원을 위해 PPPoE 터널 만들기”, `pppoed`(1M), `pppoec`(1M) 및 `sppptun`(1M) 매뉴얼 페이지를 참조하십시오.

◆ ◆ ◆ 3 장

3 다이얼 업 PPP 링크 설정(작업)

이 장에서는 가장 일반적인 PPP 링크인 다이얼 업 링크를 구성하는 작업에 대해 설명합니다. 주요 항목은 다음과 같습니다.

다이얼 업 PPP 링크를 설정하는 주요 작업(작업 맵)

모뎀을 구성하고, 네트워크 데이터베이스 파일을 수정하고, 표 8–1에 설명된 PPP 구성 파일을 수정하여 다이얼 업 PPP 링크를 설정합니다.

다음 표에는 다이얼 업 PPP 링크의 양쪽을 구성하는 주요 작업이 나열되어 있습니다. 일반적으로는 링크의 한쪽 끝(다이얼 아웃 시스템 또는 다이얼 인 서버)만 구성합니다.

표 3–1 다이얼 업 PPP 링크 설정 작업 맵

작업	설명	수행 방법
1. 미리 구성 정보 수집	링크를 설정하기 전에 필요한 데이터(예: 피어 호스트 이름, 대상 전화 번호 및 모뎀 속도)를 수집합니다.	34 페이지 “다이얼 업 PPP 링크 계획”
2. 다이얼 아웃 시스템 구성	링크를 통해 호출 작업을 수행하는 시스템에서 PPP를 설정합니다.	50 페이지 “다이얼 아웃 시스템 구성 작업(작업 맵)”
3. 다이얼 인 서버 구성	수신 호출을 받는 시스템에서 PPP를 설정합니다.	56 페이지 “다이얼 인 서버 구성 작업(작업 맵)”
4. 다이얼 인 서버 호출	pppd 명령을 입력하여 통신을 시작합니다.	60 페이지 “다이얼 인 서버를 호출하는 방법”

다이얼 아웃 시스템 구성

이 절의 작업에서는 다이얼 아웃 시스템을 구성하는 방법에 대해 설명합니다. 작업에는 그림 2–1에서 소개된 집에서 다이얼 인 시나리오가 예로 사용됩니다. 잠재적 사용자에게 시스템을 전달하기 전에 회사에서 해당 작업을 수행할 수 있습니다. 또는 경험이 많은 사용자에게 홈 시스템 설정 지침을 제공해 줄 수 있습니다. 다이얼 아웃 시스템을 설정하는 모든 사용자에게는 해당 시스템에 대한 루트 권한이 있어야 합니다.

다이얼 아웃 시스템 구성 작업(작업 맵)

표 3–2 다이얼 아웃 시스템 설정 작업 맵

작업	설명	수행 방법
1. 미리 구성 정보 수집	링크를 설정하기 전에 필요한 데이터(예: 피어 호스트 이름, 대상 전화 번호 및 모뎀 속도)를 수집합니다.	34 페이지 “다이얼 업 PPP 링크 계획”
2. 모뎀 및 직렬 포트 구성	모뎀 및 직렬 포트를 설정합니다.	51 페이지 “모뎀 및 직렬 포트를 구성하는 방법(다이얼 아웃 시스템)”
3. 직렬 회선 통신 구성	직렬 회선을 통한 전송의 특징을 구성합니다.	52 페이지 “직렬 회선을 통해 통신을 정의하는 방법”
4. 다이얼 아웃 시스템과 피어 간의 대화 정의	채트 스크립트를 만들 때 사용할 통신 데이터를 수집합니다.	53 페이지 “피어 호출 명령을 만드는 방법”
5. 특정 피어에 대한 정보 구성	개별 다이얼 인 서버를 호출할 PPP 옵션을 구성합니다.	54 페이지 “개별 피어를 사용하여 연결을 정의하는 방법”
6. 피어 호출	`pppd` 명령을 입력하여 통신을 시작합니다.	60 페이지 “다이얼 인 서버를 호출하는 방법”

다이얼 업 PPP 템플리트 파일

Solaris PPP 4.0은 템플리트 파일을 제공합니다. 각 템플리트에는 특정 PPP 구성 파일에 대한 일반적인 옵션이 포함되어 있습니다. 다음 표에는 다이얼 업 링크를 설정하는 데 사용할 수 있는 샘플 템플리트와 해당 Solaris PPP 4.0 파일이 나열되어 있습니다.

템플리트 파일	PPP 구성 파일	수행 방법
`/etc/ppp/options.tmpl`	`/etc/ppp/options`	114 페이지 “`/etc/ppp/options.tmpl` 템플리트”
`/etc/ppp/options.ttya.tmpl`	`/etc/ppp/options.`*ttyname*	116 페이지 “`options.ttya.tmpl` 템플리트 파일”

템플리트 파일	PPP 구성 파일	수행 방법
/etc/ppp/myisp-chat.tmpl	채트 스크립트를 포함할 파일(원하는 이름 지정)	122 페이지 “/etc/ppp/myisp-chat.tmpl 채트 스크립트 템플리트”
/etc/ppp/peers/myisp.tmpl	/etc/ppp/peers/*peer-name*	119 페이지 “/etc/ppp/peers/myisp.tmpl 템플리트 파일”

템플리트 파일 중 하나를 사용할 경우 템플리트의 이름을 해당 PPP 구성 파일의 이름으로 변경해야 합니다. 유일한 예외는 채트 파일 템플리트 /etc/ppp/myisp-chat.tmpl입니다. 채트 스크립트의 경우 원하는 이름을 선택할 수 있습니다.

다이얼 아웃 시스템에서 장치 구성

다이얼 아웃 PPP 시스템을 설정하는 첫번째 작업은 직렬 회선에서 장치(모뎀 및 직렬 포트)를 구성하는 것입니다.

주 – 모뎀에 적용되는 작업은 일반적으로 ISDN TA에 적용됩니다.

후속 절차를 수행하려면 다음 작업을 완료해야 합니다.

- 다이얼 아웃 시스템에 Oracle Solaris 릴리스 설치
- 최적의 모뎀 속도 결정
- 다이얼 아웃 시스템에서 사용할 직렬 포트 결정
- 다이얼 아웃 시스템에 대한 루트 암호 획득

계획 정보는 34 페이지 “다이얼 아웃 시스템을 설정하기 전에”를 참조하십시오.

▼ 모뎀 및 직렬 포트를 구성하는 방법(다이얼 아웃 시스템)

1 모뎀을 프로그래밍합니다.

다양한 모뎀 유형을 사용할 수 있지만 대부분의 모뎀은 Solaris PPP 4.0에 맞는 설정으로 제공됩니다. 다음 목록에는 Solaris PPP 4.0을 사용하는 모뎀에 대한 기본적인 매개변수 설정이 나와 있습니다.

- **DCD –** 사업자 지침을 따릅니다.
- **DTR –** 모뎀이 on-hook(전화기를 놓은 상태, Hang-up) 상태가 되도록 낮게 설정합니다.
- **Flow Control(플로우 제어) –** 전이중 하드웨어 플로우 제어를 위해 RTS/CTS로 설정됩니다.

- **Attention Sequences(주의 시퀀스)** – 사용 안함으로 설정됩니다.

링크 설정 시 문제가 있으며 모뎀에 결함이 있다고 판단되는 경우에는 먼저 모뎀 제조업체의 설명서를 참조하십시오. 여러 웹 사이트에서 모뎀 프로그래밍 지원을 받을 수도 있습니다. 마지막으로, 100 페이지 "모뎀 문제를 진단하는 방법"에도 모뎀 문제를 해결하기 위한 제안 사항이 일부 제공되어 있습니다.

2 **모뎀 케이블을 다이얼 아웃 시스템의 직렬 포트와 전화 잭에 연결합니다.**

3 **다이얼 아웃 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

4 **모뎀 방향을 다이얼 아웃으로만 지정합니다.**

다이얼 아웃 시스템에서 통신 구성

이 절의 절차에서는 다이얼 아웃 시스템의 직렬 회선을 통해 통신을 구성하는 방법에 대해 설명합니다. 이러한 절차를 사용하려면 먼저 51 페이지 "모뎀 및 직렬 포트를 구성하는 방법(다이얼 아웃 시스템)"에 설명된 대로 모뎀 및 직렬 포트를 구성해야 합니다.

다음 작업에서는 다이얼 아웃 시스템이 다이얼 인 서버와 성공적으로 통신을 시작할 수 있게 만드는 방법을 보여줍니다. 통신은 PPP 구성 파일의 옵션에 정의된 대로 시작됩니다. 다음 파일을 만들어야 합니다.

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*
- 채트 스크립트
- `/etc/ppp/peers/`*peer-name*

Solaris PPP 4.0은 PPP 구성 파일 템플리트를 제공합니다. 이 템플리트는 필요에 맞게 사용자 정의할 수 있습니다. 이러한 파일에 대한 자세한 내용은 50 페이지 "다이얼 업 PPP 템플리트 파일"을 참조하십시오.

▼ 직렬 회선을 통해 통신을 정의하는 방법

1 **다이얼 아웃 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **다음 항목을 사용하여 `/etc/ppp/options`라는 파일을 만듭니다.**

```
lock
```

/etc/ppp/options 파일은 로컬 시스템의 모든 통신에 적용되는 전역 매개변수를 정의하는 데 사용됩니다. lock 옵션을 사용하면 /var/spool/locks/LK.xxx.yyy.zzz 형식의 UUCP 스타일 잠금이 가능해집니다.

주 – 다이얼 아웃 시스템에 /etc/ppp/options 파일이 없으면 수퍼 유저만 pppd 명령을 실행할 수 있습니다. 그러나 /etc/ppp/options는 비워 둘 수 있습니다.

/etc/ppp/options에 대한 전체 설명은 113 페이지 "/etc/ppp/options 구성 파일"을 참조하십시오.

3 (옵션) 특정 직렬 포트에서 통신이 시작되는 방법을 정의하기 위해 /etc/ppp/options.*ttyname*이라는 파일을 만듭니다.

다음 예에서는 /etc/ppp/options.*ttyname* 파일을 보여줍니다. 이 파일은 장치 이름이 /dev/cua/a인 포트에 대한 파일입니다.

```
# cat /etc/ppp/options.cua.a
crtscts
```

PPP 옵션 crtscts는 직렬 포트 a에 대해 하드웨어 플로우 제어를 켤 것을 pppd 데몬에 지시합니다.

/etc/ppp/options.ttyname 파일에 대한 자세한 내용을 보려면 115 페이지 "/etc/ppp/options.*ttyname* 구성 파일"로 이동하십시오.

4 57 페이지 "모뎀 속도를 설정하는 방법"에 설명된 대로 모뎀 속도를 설정합니다.

▼ 피어 호출 명령을 만드는 방법

다이얼 아웃 시스템이 PPP 링크를 시작할 수 있게 만들려면 관리자가 먼저 피어가 될 다이얼 인 서버에 대한 정보를 수집해야 합니다. 그런 다음 관리자는 이 정보를 사용하여 채트 스크립트를 만듭니다. 채트 스크립트는 다이얼 아웃 시스템과 피어 간의 실제 대화에 대해 설명합니다.

1 다이얼 아웃 시스템의 모뎀이 실행될 속도를 결정합니다.

자세한 내용은 120 페이지 "다이얼 업 링크를 위한 모뎀 속도 구성"을 참조하십시오.

2 다이얼 인 서버의 사이트에서 다음 정보를 가져옵니다.

- 서버의 전화 번호
- 사용된 인증 프로토콜(해당하는 경우)
- 채트 스크립트를 위해 피어에 필요한 로그인 절차

3 다이얼 인 서버의 사이트에서 이름 서버의 이름 및 IP 주소를 가져옵니다.

4 **채트 스크립트에서 특정 피어에 대한 호출을 시작하는 명령을 지정합니다.**

예를 들어, 다음 채트 스크립트 /etc/ppp/mychat을 만들어 다이얼 인 서버 myserver를 호출할 수 있습니다.

```
SAY "Calling the peer\n"
        TIMEOUT 10
        ABORT BUSY
        ABORT 'NO CARRIER'
        ABORT ERROR
        REPORT CONNECT
        "" AT&F1&M5S2=255
        TIMEOUT 60
        OK ATDT1-123-555-1234
        CONNECT \c
        SAY "Connected; logging in.\n"
        TIMEOUT 5
        ogin:--ogin: pppuser
        TIMEOUT 20
        ABORT 'ogin incorrect'
        ssword: \qmypassword
        "% " \c
        SAY "Logged in.  Starting PPP on peer system.\n"
        ABORT 'not found'
        "" "exec pppd"
        ~ \c
```

스크립트에는 로그인 절차를 필요로 하는 Oracle Solaris 다이얼 인 서버를 호출하는 명령이 포함되어 있습니다. 각 명령에 대한 자세한 내용은 124 페이지 "UNIX 스타일의 로그인을 위해 향상된 기본적인 채트 스크립트"를 참조하십시오. 채트 스크립트를 만드는 방법에 대한 자세한 내용을 보려면 120 페이지 "다이얼 업 링크에서 대화 정의" 절을 읽어 보십시오.

주 – 채트 스크립트는 직접 호출하지 않습니다. 대신, 채트 스크립트의 파일 이름을 스크립트를 호출하는 chat 명령에 대한 인수로 사용합니다.

피어가 Oracle Solaris 또는 이와 유사한 운영 체제를 실행하는 경우 이전 채트 스크립트를 다이얼 아웃 시스템에 대한 템플리트로 사용해 보십시오.

▼ 개별 피어를 사용하여 연결을 정의하는 방법

1 **다이얼 아웃 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **DNS 및 이름 서비스 스위치 서비스에 대한 저장소 정보를 업데이트합니다.**

```
# svccfg
svc:> select network/dns/client
svc:/network/dns/client> setprop config/domain = astring: "bigcompany.com"
svc:/network/dns/client> setprop config/nameserver = net_address: "10.10.111.15"
```

```
svc:/network/dns/client> addpropval config/nameserver "10.10.130.8"
svc:/network/dns/client> select network/dns/client:default
svc:/network/dns/client:default > refresh
svc:/network/dns/client:default > validate
svc:/network/dns/client:default > select system/name-service/switch
svc:/system/name-service/switch > setprop config/host = astring: "files dns"
 svc:/system/name-service/switch:default > select system/name-service/switch:default
svc:/system/name-service/switch:default > refresh
svc:/system/name-service/switch:default > validate
# svcadm enable network/dns/client
# svcadm refresh system/name-service/switch
```

3 피어에 대한 파일을 만듭니다.

예를 들어, 다음 파일을 만들어 다이얼 인 서버 myserver를 정의합니다.

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
noauth
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
```

/dev/cua/a
: /dev/cua/a 장치가 myserver에 대한 호출의 직렬 인터페이스로 사용되도록 지정합니다.

57600
: 링크의 속도를 정의합니다.

noipdefault
: 피어 myserver를 사용하는 트랜잭션의 경우 처음에 다이얼 아웃 시스템의 IP 주소가 0.0.0.0으로 설정됨을 지정합니다. myserver는 모든 다이얼 업 세션에서 다이얼 아웃 시스템에 IP 주소를 지정합니다.

idle 120
: 유휴 기간이 120초가 넘으면 링크 시간이 초과됨을 나타냅니다.

noauth
: 다이얼 아웃 시스템과 연결을 협상할 때 피어 myserver가 인증 자격 증명을 제공하지 않아도 됨을 지정합니다.

connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
: connect 옵션과 해당 인수를 지정합니다(피어의 전화 번호와 호출 명령이 있는 채트 스크립트 /etc/ppp/mychat 포함).

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 다른 다이얼 아웃 시스템을 구성하려면 51 페이지 “모뎀 및 직렬 포트를 구성하는 방법(다이얼 아웃 시스템)”을 참조하십시오.

- 다른 컴퓨터로 다이얼 아웃하여 모뎀 연결을 테스트하려면 cu(1C) 및 tip(1) 매뉴얼 페이지를 참조하십시오. 이러한 유틸리티를 사용하면 모뎀이 제대로 구성되었는지 테스트하는 데 도움이 됩니다. 이러한 유틸리티를 사용하여 다른 시스템과 연결을 설정할 수 있는지 테스트할 수도 있습니다.
- 구성 파일 및 옵션에 대한 자세한 내용은 109 페이지 "파일 및 명령줄에서 PPP 옵션 사용"을 참조하십시오.
- 다이얼 인 서버를 구성하려면 56 페이지 "다이얼 인 서버에서 장치 구성"을 참조하십시오.

다이얼 인 서버 구성

이 절의 작업은 다이얼 인 서버를 구성하기 위한 것입니다. 다이얼 인 서버는 다이얼 아웃 시스템에서 PPP 링크를 통해 호출을 받는 피어 시스템입니다. 작업에서는 다이얼 인 서버 myserver(그림 2–1에서 소개됨)를 구성하는 방법을 보여줍니다.

다이얼 인 서버 구성 작업(작업 맵)

표 3–3 다이얼 인 서버 설정 작업 맵

작업	설명	수행 방법
1. 미리 구성 정보 수집	링크를 설정하기 전에 필요한 데이터(예: 피어 호스트 이름, 대상 전화 번호 및 모뎀 속도)를 수집합니다.	34 페이지 "다이얼 업 PPP 링크 계획"
2. 모뎀 및 직렬 포트 구성	모뎀 및 직렬 포트를 설정합니다.	57 페이지 "모뎀 및 직렬 포트를 구성하는 방법(다이얼 인 서버)"
3. 호출 피어 정보 구성	다이얼 인 서버를 호출할 수 있는 모든 다이얼 아웃 시스템에 대해 사용자 환경과 PPP 옵션을 설정합니다.	58 페이지 "다이얼 인 서버의 사용자를 구성하는 방법"
4. 직렬 회선 통신 구성	직렬 회선을 통한 전송의 특징을 구성합니다.	59 페이지 "직렬 회선을 통해 통신을 정의하는 방법(다이얼 인 서버)"

다이얼 인 서버에서 장치 구성

다음 절차에서는 다이얼 인 서버에서 모뎀과 직렬 포트를 구성하는 방법에 대해 설명합니다.

후속 절차를 수행하려면 피어 다이얼 인 서버에서 다음 작업을 완료해야 합니다.

- Oracle Solaris 릴리스 설치
- 최적의 모뎀 속도 결정

- 사용할 직렬 포트 결정

▼ 모뎀 및 직렬 포트를 구성하는 방법(다이얼 인 서버)

1. **모뎀 제조업체의 설명서에 제공된 지침대로 모뎀을 프로그래밍합니다.**
   기타 제안 사항은 51 페이지 "모뎀 및 직렬 포트를 구성하는 방법(다이얼 아웃 시스템)"을 참조하십시오.
2. **다이얼 인 서버에 있는 직렬 포트에 모뎀을 연결합니다.**
3. **다이얼 인 서버에서 관리자로 전환합니다.**
   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.
4. **모뎀 방향을 다이얼 인으로만 지정합니다.**

▼ 모뎀 속도를 설정하는 방법

다음 절차에서는 다이얼 인 서버에 대해 모뎀 속도를 설정하는 방법에 대해 설명합니다. Sun Microsystems 컴퓨터에 사용할 속도에 대한 제안 사항은 120 페이지 "다이얼 업 링크를 위한 모뎀 속도 구성"을 참조하십시오.

1. **다이얼 인 서버에 로그인합니다.**
2. **`tip` 명령을 사용하여 모뎀에 연결합니다.**
   `tip`을 사용하여 모뎀 속도를 설정하는 지침은 `tip`(1) 매뉴얼 페이지에 있습니다.
3. **모뎀에서 고정 DTE 속도를 구성합니다.**
4. **`ttymon`을 사용하여 직렬 포트를 해당 속도로 고정합니다.**

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 57 페이지 "모뎀 및 직렬 포트를 구성하는 방법(다이얼 인 서버)"
- 58 페이지 "다이얼 인 서버의 사용자를 구성하는 방법"

다이얼 인 서버의 사용자 설정

다이얼 인 서버를 설정할 때는 알려진 각 원격 호출자에 대한 정보도 구성해야 합니다.

이 절의 절차를 시작하려면 먼저 다음 작업을 완료해야 합니다.

- 원격 다이얼 아웃 시스템에서 로그인할 수 있는 모든 사용자의 UNIX 사용자 이름 획득
- 57 페이지 "모뎀 및 직렬 포트를 구성하는 방법(다이얼 인 서버)"에 설명된 대로 모뎀 및 직렬 회선 설정
- 원격 사용자로부터의 수신 호출에 지정할 전용 IP 주소 지정. 잠재적 호출자의 수가 다이얼 인 서버에 있는 모뎀 및 직렬 포트의 수를 초과하는 경우에는 전용 수신 IP 주소를 만드십시오. 전용 IP 주소를 만드는 방법에 대한 자세한 내용을 보려면 136 페이지 "호출자를 위한 IP 주소 지정 체계 만들기"를 참조하십시오.

▼ 다이얼 인 서버의 사용자를 구성하는 방법

1. **다이얼 인 서버에서 관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **각 원격 PPP 사용자에 대해 다이얼 인 서버에서 새 계정을 만듭니다.**

   새 사용자를 만드는 방법에 대한 자세한 내용은 **Oracle Solaris 11.1에서 사용자 계정 및 사용자 환경 관리**의 "CLI를 사용하여 사용자 계정 설정 및 관리(작업 맵)"를 참조하십시오.

3. **각 호출자에 대해 사용자의 PPP 세션과 관련된 다양한 옵션이 포함된 `$HOME/.ppprc` 파일을 만듭니다.**

   예를 들어, 다음 `.ppprc` 파일을 `pppuser`에 대해 만들 수 있습니다.

   ```
   # cat /export/home/pppuser/.ppprc
   noccp
   ```

   `noccp`는 링크에서 압축 제어를 끕니다.

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 58 페이지 "다이얼 인 서버의 사용자를 구성하는 방법"
- 59 페이지 "직렬 회선을 통해 통신을 정의하는 방법(다이얼 인 서버)"

다이얼 인 서버를 통한 통신 구성

다음 작업에서는 다이얼 인 서버가 임의의 다이얼 아웃 시스템과 통신을 열 수 있게 만드는 방법을 보여줍니다. 다음 PPP 구성 파일에 정의된 옵션에 따라 통신이 설정되는 방법이 결정됩니다.

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*

이러한 파일에 대한 자세한 내용은 109 페이지 "파일 및 명령줄에서 PPP 옵션 사용"을 참조하십시오.

계속 진행하려면 다음 작업을 완료해야 합니다.

- 57 페이지 "모뎀 및 직렬 포트를 구성하는 방법(다이얼 인 서버)"에 설명된 대로 다이얼 인 서버에서 직렬 포트 및 모뎀 구성
- 58 페이지 "다이얼 인 서버의 사용자를 구성하는 방법"에 설명된 대로 다이얼 인 서버의 잠재적 사용자에 대한 정보 구성

▼ 직렬 회선을 통해 통신을 정의하는 방법(다이얼 인 서버)

1 다이얼 인 서버에서 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 다음 항목을 사용하여 `/etc/ppp/options` 파일을 만듭니다.

```
nodefaultroute
```

`nodefaultroute`는 로컬 시스템에 있는 어떤 `pppd` 세션도 `root` 권한 없이 기본 경로를 설정할 수 없음을 나타냅니다.

주 – 다이얼 인 서버에 `/etc/ppp/options` 파일이 없으면 수퍼 유저만 `pppd` 명령을 실행할 수 있습니다. 그러나 `/etc/ppp/options` 파일은 비워 둘 수 있습니다.

---

3 `/etc/options.`*ttyname* 파일을 만들어 직렬 포트 *ttyname*을 통해 받는 호출이 처리되는 방법을 정의합니다.

다음 `/etc/options.ttya` 파일은 다이얼 인 서버의 직렬 포트 `/dev/ttya`에서 수신 호출이 처리되는 방법을 정의합니다.

```
:10.0.0.80
xonxoff
```

`:10.0.0.80` IP 주소 10.0.0.80을 직렬 포트 `ttya`를 통해 호출하는 모든 피어에 지정합니다.

xonxoff 직렬 회선이 소프트웨어 플로우 제어를 사용으로 설정한 상태에서 모뎀으로부터의 통신을 처리할 수 있도록 허용합니다.

참조 이 장의 모든 절차를 따른 경우 다이얼 업 링크의 구성을 완료한 것입니다. 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 다른 컴퓨터로 다이얼 아웃하여 모뎀 연결을 테스트하려면 cu(1C) 및 tip(1) 매뉴얼 페이지를 참조하십시오. 이러한 유틸리티를 사용하면 모뎀이 제대로 구성되었는지 테스트하는 데 도움이 됩니다. 이러한 유틸리티를 사용하여 다른 시스템과 연결을 설정할 수 있는지 테스트할 수도 있습니다.
- 다이얼 인 서버에 대한 옵션을 더 구성하려면 56 페이지 "다이얼 인 서버 구성"을 참조하십시오.
- 다이얼 아웃 시스템을 더 구성하려면 50 페이지 "다이얼 아웃 시스템 구성"을 참조하십시오.
- 원격 시스템이 다이얼 인 서버를 호출하게 만들려면 60 페이지 "다이얼 인 서버 호출"을 참조하십시오.

다이얼 인 서버 호출

다이얼 아웃 시스템이 다이얼 인 서버를 호출하게 만들어 다이얼 업 PPP 링크를 설정합니다. 로컬 PPP 구성 파일에서 demand 옵션을 지정하여 다이얼 아웃 시스템이 서버를 호출하게 만들 수 있습니다. 그러나 사용자가 다이얼 아웃 시스템에서 pppd 명령을 실행하는 것이 링크를 설정하는 가장 일반적인 방법입니다.

후속 작업으로 계속 진행하려면 다음 작업 중 하나 또는 모두를 완료해야 합니다.

- 50 페이지 "다이얼 아웃 시스템 구성"에 설명된 대로 다이얼 아웃 시스템 설정
- 56 페이지 "다이얼 인 서버 구성"에 설명된 대로 다이얼 인 서버 설정

▼ 다이얼 인 서버를 호출하는 방법

1 root가 아니라 일반 사용자 계정을 사용하여 다이얼 아웃 시스템에 로그인합니다.

2 pppd 명령을 실행하여 다이얼 인 서버를 호출합니다.

예를 들어, 다음 명령을 실행하면 다이얼 아웃 시스템과 다이얼 인 서버 myserver 간에 링크가 시작됩니다.

```
% pppd 57600 call myserver
```

pppd pppd 데몬을 호출하여 호출을 시작합니다.

57600 호스트와 모뎀 간 회선의 속도를 설정합니다.

call myserver call 옵션(pppd)을 호출합니다. 그러면 pppd가 /etc/ppp/peers/myserver 파일(54 페이지 "개별 피어를 사용하여 연결을 정의하는 방법"에서 만들어짐)의 옵션을 읽습니다.

3 호스트 lindyhop(그림 2–1에 나와 있음)과 같이 서버의 네트워크에 있는 호스트에 연결합니다.

```
ping lindyhop
```

링크가 올바르게 동작하지 않으면 7 장, "일반적인 PPP 문제 해결(작업)"을 참조하십시오.

4 PPP 세션 종료:

```
% pkill -x pppd
```

참조 이 장의 모든 절차를 따른 경우 다이얼 업 링크의 구성을 완료한 것입니다. 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 사용자가 자신의 다이얼 아웃 시스템에서 작업을 시작하게 만들려면 60 페이지 "다이얼 인 서버를 호출하는 방법"을 참조하십시오.
- 링크에서 문제를 해결하려면 7 장, "일반적인 PPP 문제 해결(작업)"을 참조하십시오.
- 이 장에 사용되는 파일 및 옵션에 대한 자세한 내용은 109 페이지 "파일 및 명령줄에서 PPP 옵션 사용"을 참조하십시오.

◆ ◆ ◆ 4 장

4 전용 회선 PPP 링크 설정(작업)

이 장에서는 피어 간에 전용 회선을 사용하는 PPP 링크를 구성하는 방법에 대해 설명합니다. 주요 절은 다음과 같습니다.

전용 회선 설정(작업 맵)

전용 회선 링크는 다이얼 업 링크에 비해 비교적 설정하기 쉽습니다. 대부분의 경우에서 CSU/DSU, 전화 걸기 서비스 또는 인증을 구성할 필요가 없습니다. CSU/DSU를 구성하지 않아도 되는 경우 제조업체 설명서를 통해 이 복잡한 작업에 대한 지원을 받으십시오.

다음 표의 작업 맵에서는 기본 전용 회선 링크를 설정하는 데 사용되는 모든 작업에 대해 설명합니다.

주 – 일부 전용 회선 유형에서는 CSU/DSU가 반대쪽 피어의 주소로 "전화를 걸어야" 합니다. 예를 들어, 프레임 릴레이는 SVC(가상 교환 회로) 또는 교환식 56 서비스를 사용합니다.

표 4–1 전용 회선 링크 설정 작업 맵

작업	설명	수행 방법
1. 사전 구성 정보 수집	링크를 설정하기 전에 필요한 데이터를 수집합니다.	38 페이지 "전용 회선 링크에 대해 수집해야 하는 정보"
2. 전용 회선 하드웨어 설정	CSU/DSU 및 동기 인터페이스 카드를 조립합니다.	64 페이지 "동기 장치를 구성하는 방법"
3. 필요한 경우 인터페이스 카드 구성	전용 회선 시작 시 사용할 인터페이스 스크립트를 구성합니다.	64 페이지 "동기 장치를 구성하는 방법"

표 4–1 전용 회선 링크 설정 작업 맵 (계속)

작업	설명	수행 방법
4. 원격 피어에 대한 정보 구성	로컬 시스템과 원격 피어 간의 통신이 이루어지는 방법을 정의합니다.	65 페이지 "전용 회선에서 시스템을 구성하는 방법"
5. 전용 회선 시작	시스템이 부트 프로세스의 일환으로 전용 회선을 통해 PPP를 시작하도록 구성합니다.	65 페이지 "전용 회선에서 시스템을 구성하는 방법"

전용 회선에서 동기 장치 구성

이 절의 작업에서는 38 페이지 "전용 회선 링크 구성의 예"에서 소개된 전용 회선 토폴로지에 필요한 장비를 구성합니다. 전용 회선에 연결하는 데 필요한 동기 장치에는 인터페이스와 모뎀이 있습니다.

동기 장치 설정을 위한 필수 조건

후속 절차를 수행하려면 다음 항목이 있어야 합니다.

- 공급자가 사이트에 설치한 전용 회선(작동해야 함)
- 동기 장치(CSU/DSU)
- 시스템에 설치된 Oracle Solaris 릴리스
- 시스템에 필요한 유형의 동기 인터페이스 카드

▼ 동기 장치를 구성하는 방법

1 **필요한 경우 로컬 시스템에 인터페이스 카드를 물리적으로 설치합니다.**
제조업체 설명서의 지침을 따르십시오.

2 **케이블로 CSU/DSU와 인터페이스를 연결합니다.**
필요한 경우 케이블로 CSU/DSU와 전용 회선 잭 또는 이와 유사한 커넥터를 연결합니다.

3 **제조업체 또는 네트워크 공급자의 설명서에 제공된 지침대로 CSU/DSU를 구성합니다.**

주 – 전용 회선을 임대해 준 공급자가 링크에 대한 CSU/DSU를 제공 및 구성해 줄 수도 있습니다.

---

4 **필요한 경우 인터페이스 설명서에 제공된 지침대로 인터페이스 카드를 구성합니다.**
인터페이스 카드를 구성할 때는 인터페이스에 대한 시작 스크립트를 생성해야 합니다. 그림 2–2에 나와 있는 전용 회선 구성에서 LocalCorp의 라우터에는 HSI/P 인터페이스 카드가 사용됩니다.

다음 스크립트 `hsi-conf`는 HSI/P 인터페이스를 시작합니다.

```
#!/bin/ksh
/opt/SUNWconn/bin/hsip_init hihp1 speed=1536000 mode=fdx loopback=no \
nrzi=no txc=txc rxc=rxc txd=txd rxd=rxd signal=no 2>&1 > /dev/null
```

`hihp1` HSI/P가 사용되는 동기 포트임을 나타냅니다.

`speed=1536000` CSU/DSU의 속도를 나타내기 위해 설정합니다.

참조 전용 회선에서 로컬 시스템을 구성하려면 65 페이지 "전용 회선에서 시스템을 구성하는 방법"을 참조하십시오.

전용 회선에서 시스템 구성

이 절의 작업에서는 전용 회선의 본인 쪽 끝에서 로컬 피어 역할을 하도록 라우터를 설정하는 방법에 대해 설명합니다. 작업에는 38 페이지 "전용 회선 링크 구성의 예"에서 예로 소개된 전용 회선이 사용됩니다.

전용 회선에서의 로컬 시스템 구성을 위한 필수 조건

후속 절차를 수행하려면 다음 작업을 완료해야 합니다.

- 64 페이지 "전용 회선에서 동기 장치 구성"에 설명된 대로 링크에 대한 동기 장치 설정 및 구성
- 전용 회선에서 로컬 시스템의 루트 암호 획득
- 전용 회선 공급자의 서비스를 사용하기 위해 네트워크에서 라우터로 실행되도록 로컬 시스템 설정

▼ 전용 회선에서 시스템을 구성하는 방법

1 로컬 시스템(라우터)에서 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 라우터의 `/etc/hosts` 파일에서 원격 피어에 대한 항목을 추가합니다.

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
192.168.130.10  local2-peer        loghost
```

```
192.168.130.11  local1-net
10.0.0.25       farISP
```

예제 /etc/hosts 파일은 가상 회사 LocalCorp에 있는 로컬 라우터를 위한 것입니다. 서비스 공급자측에 있는 원격 피어 farISP의 IP 주소 및 호스트 이름을 기록해 둡니다.

3 **공급자의 피어에 대한 정보를 보관할 /etc/ppp/peers/*peer-name* 파일을 만듭니다.**

이 예제 전용 회선 링크를 위해서는 /etc/ppp/peers/farISP 파일을 만듭니다.

```
# cat /etc/ppp/peers/farISP
init '/etc/ppp/conf_hsi'
local
/dev/hihp1
sync
noauth
192.168.130.10:10.0.0.25
passive
persist
noccp
nopcomp
novj
noaccomp
```

다음 표에는 /etc/ppp/peers/farISP에 사용되는 옵션 및 매개변수가 설명되어 있습니다.

옵션	정의
init '/etc/ppp/conf_hsi'	링크를 시작합니다. 그러면 init가 /etc/ppp/conf_hsi 스크립트의 매개변수를 사용하여 HSI 인터페이스를 구성합니다.
local	DTR(Data Terminal Ready) 신호의 상태를 변경하지 말 것을 pppd 데몬에 지시합니다. DCD(Data Carrier Detect) 입력 신호를 무시할 것도 pppd에 지시합니다.
/dev/hihp1	동기 인터페이스의 장치 이름을 제공합니다.
sync	링크에 대한 동기 인코딩을 설정합니다.
noauth	로컬 시스템이 피어로부터 인증을 요구하지 않아도 됨을 설정합니다. 그러나 피어는 인증을 요구할 수도 있습니다.
192.168.130.10:10.0.0.25	로컬 피어 및 원격 피어의 IP 주소를 콜론으로 구분하여 정의합니다.
passive	LCP 구성-요청을 최대 횟수로 실행한 후 침묵 상태로 전환하여 피어가 시작되기를 기다릴 것을 로컬 시스템에 있는 pppd 데몬에 지시합니다.
persist	연결이 끝난 후 링크를 다시 시작할 것을 pppd 데몬에 지시합니다.
noccp, nopcomp, novj, noaccomp	각각 CCP(Compression Control Protocol), 프로토콜 필드 압축, Van Jacobson 압축 및 주소/컨트롤 필드 압축을 사용 안함으로 설정합니다. 이러한 압축은 다이얼 업 링크에서 전송 속도를 높이지만 전용 회선의 속도를 낮출 수 있습니다.

4 부트 프로세스의 일환으로 PPP 링크를 만드는 demand라는 초기화 스크립트를 만듭니다.

```
# cat /etc/ppp/demand
#!/bin/sh
if [ -f /system/volatile/ppp-demand.pid ] &&
   /usr/bin/kill -s 0 `/bin/cat /system/volatile/ppp-demand.pid`
then
        :
else
        /usr/bin/pppd call farISP
fi
```

demand 스크립트에는 전용 회선 링크를 설정하기 위한 pppd 명령이 포함되어 있습니다. 다음 표에는 $PPPDIR/demand의 내용이 설명되어 있습니다.

코드 샘플	설명
`if [ -f /system/volatile/ppp-demand.pid ] && /usr/bin/kill -s 0 `/bin/cat /system/volatile/ppp-demand.pid``	이러한 행에서는 pppd가 실행되고 있는지 확인합니다. pppd가 실행되고 있는 경우 이를 시작하지 않아도 됩니다.
`/usr/bin/pppd call farISP`	이 행에서는 pppd를 시작합니다. pppd는 /etc/ppp/options에서 옵션을 읽습니다. 명령줄에서 call farISP 옵션을 실행하면 /etc/ppp/peers/farISP도 읽습니다

Solaris PPP 4.0 시작 스크립트 /etc/rc2.d/S47pppd는 부트 프로세스의 일환으로 demand 스크립트를 호출합니다. /etc/rc2.dS47pppd의 다음 행에서는 $PPPDIR/demand라는 파일이 있는지 확인하기 위해 검색을 수행합니다.

```
if [ -f $PPPDIR/demand ]; then
            . $PPPDIR/demand
    fi
```

$PPPDIR/demand가 발견되면 실행됩니다. $PPPDIR/demand를 실행하는 동안 링크가 설정됩니다.

주 – 로컬 네트워크 외부에 있는 시스템에 연결하려면 사용자가 telnet, ftp, rsh 또는 이와 유사한 명령을 실행하게 하십시오.

참조 이 장의 모든 절차를 따른 경우 전용 회선 링크의 구성을 완료한 것입니다. 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 문제 해결 정보를 찾으려면 107 페이지 “전용 회선 문제 해결”을 참조하십시오.
- 이 장에 사용되는 파일 및 옵션에 대한 자세한 내용은 109 페이지 “파일 및 명령줄에서 PPP 옵션 사용”을 참조하십시오.

◆ ◆ ◆ 5 장

5 PPP 인증 설정(작업)

이 장에는 PPP 인증을 설정하는 작업이 있습니다. 여기서 다루는 항목은 다음과 같습니다.

- 70 페이지 “PAP 인증 구성”
- 77 페이지 “CHAP 인증 구성”

인증을 위해 전용 회선 링크보다는 다이얼 업 링크가 구성되어 있을 확률이 크므로 절차에서는 다이얼 업 링크를 통해 인증을 구현하는 방법에 대해 설명합니다. 회사 보안 정책상 인증이 필요한 경우에는 전용 회선을 통해 인증을 구성할 수 있습니다. 전용 회선 인증의 경우 이 장의 작업을 지침으로 활용하십시오.

PPP 인증을 사용하고 싶지만 어떤 프로토콜을 사용해야 하는지 확실하지 않다면 29 페이지 “PPP 인증을 사용하는 이유” 절을 검토하십시오. PPP 인증에 대한 자세한 내용은 pppd(1M) 매뉴얼 페이지 및 130 페이지 “링크에서 호출자 인증”을 참조하십시오.

PPP 인증 구성(작업 맵)

이 절에는 PPP 인증 절차에 빠르게 액세스하는 데 도움이 되는 작업 맵이 있습니다.

표 5–1 일반 PPP 인증 작업 맵

작업	설명	수행 방법
PAP 인증 구성	이러한 절차를 사용하면 다이얼 인 서버 및 다이얼 아웃 시스템에서 PAP 인증을 사용으로 설정할 수 있습니다.	70 페이지 “PAP 인증 설정(작업 맵)”
CHAP 인증 구성	이러한 절차를 사용하면 다이얼 인 서버 및 다이얼 아웃 시스템에서 CHAP 인증을 사용으로 설정할 수 있습니다.	77 페이지 “CHAP 인증 설정(작업 맵)”

PAP 인증 구성

이 절의 작업에서는 PAP(암호 인증 프로토콜)를 사용하여 PPP 링크에 대해 인증을 구현하는 방법에 대해 설명합니다. 작업에는 다이얼 업 링크에 맞는 PAP 시나리오를 보여주기 위해 40 페이지 “PPP 인증 구성의 예”에 나와 있는 예가 사용됩니다. 지침을 기반으로 사용자 사이트에서 PAP 인증을 구현해 보십시오.

다음 절차를 수행하려면 먼저 다음 작업을 완료해야 합니다.

- 다이얼 인 서버와 신뢰할 수 있는 호출자에 속하는 다이얼 아웃 시스템 간에 다이얼 업 링크를 설정하고 테스트
- 다이얼 인 서버 인증의 경우 네트워크 암호 데이터베이스가 관리되는 시스템(예: LDAP, NIS 또는 로컬 파일)에 대한 수퍼 유저 사용 권한 획득(이상적인 상황)
- 로컬 시스템(다이얼 인 서버 또는 다이얼 아웃 시스템)에 대한 수퍼 유저 권한 획득

PAP 인증 설정(작업 맵)

다음 작업 맵을 사용하면 다이얼 인 서버 및 다이얼 아웃 시스템의 신뢰할 수 있는 호출자에 대한 PAP 관련 작업에 빠르게 액세스할 수 있습니다.

표 5–2 PAP 인증 작업 맵(다이얼 인 서버)

작업	설명	수행 방법
1. 미리 구성 정보 수집	인증에 필요한 사용자 이름 및 기타 데이터를 수집합니다.	39 페이지 “링크에서 인증 계획”
2. 필요한 경우 암호 데이터베이스 업데이트	모든 잠재적 호출자가 서버의 암호 데이터베이스에 있는지 확인합니다.	71 페이지 “PAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)”
3. PAP 데이터베이스 만들기	`/etc/ppp/pap-secrets`에서 모든 잠재적 호출자에 대한 보안 자격 증명을 만듭니다.	71 페이지 “PAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)”
4. PPP 구성 파일 수정	`/etc/ppp/options` 및 `/etc/ppp/peers/`*peer-name* 파일에 PAP 관련 옵션을 추가합니다.	73 페이지 “PPP 구성 파일에 PAP 지원을 추가하는 방법(다이얼 인 서버)”

표 5–3 PAP 인증 작업 맵(다이얼 아웃 시스템)

작업	설명	수행 방법
1. 미리 구성 정보 수집	인증에 필요한 사용자 이름 및 기타 데이터를 수집합니다.	39 페이지 “링크에서 인증 계획”

표 5–3 PAP 인증 작업 맵(다이얼 아웃 시스템) (계속)

작업	설명	수행 방법
2. 신뢰할 수 있는 호출자의 시스템에 대한 PAP 데이터베이스 만들기	/etc/ppp/pap-secrets에서 신뢰할 수 있는 호출자에 대한 보안 자격 증명을 만들고 필요한 경우 다이얼 아웃 시스템을 호출하는 다른 사용자에 대한 보안 자격 증명을 만듭니다.	74 페이지 “신뢰할 수 있는 호출자에 대해 PAP 인증 자격 증명을 구성하는 방법”
3. PPP 구성 파일 수정	/etc/ppp/options 및 /etc/ppp/peers/*peer-name* 파일에 PAP 관련 옵션을 추가합니다.	76 페이지 “PPP 구성 파일에 PAP 지원을 추가하는 방법(다이얼 아웃 시스템)”

다이얼 인 서버에서 PAP 인증 구성

PAP 인증을 설정하려면 다음 작업을 수행해야 합니다.

- PAP 자격 증명 데이터베이스 만들기
- PAP 지원을 위해 PPP 구성 파일 수정

▼ PAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)

이 절차에서는 링크의 호출자를 인증하는 데 사용되는 PAP 보안 자격 증명이 포함된 /etc/ppp/pap-secrets 파일을 수정합니다. /etc/ppp/pap-secrets는 PPP 링크의 두 시스템 모두에 있어야 합니다.

그림 2–3에 소개된 샘플 PAP 구성에는 PAP의 login 옵션이 사용됩니다. 이 옵션을 사용하려면 네트워크의 암호 데이터베이스를 업데이트해야 할 수도 있습니다. login 옵션에 대한 자세한 내용은 133 페이지 “/etc/ppp/pap-secrets에 login 옵션 사용”을 참조하십시오.

1 **신뢰할 수 있는 모든 잠재적 호출자의 목록을 어셈블합니다. 신뢰할 수 있는 호출자는 자신의 원격 시스템에서 다이얼 인 서버를 호출할 권한을 부여받을 사람입니다.**

2 **신뢰할 수 있는 각 호출자가 다이얼 인 서버의 암호 데이터베이스에서 이미 UNIX 사용자 이름 및 암호를 가지고 있는지 확인하십시오.**

주 – PAP의 login 옵션을 사용하여 호출자를 인증하는 샘플 PAP 구성의 경우 특히 확인 작업이 중요합니다. PAP의 login을 구현하지 않을 경우 호출자의 PAP 사용자 이름이 UNIX 사용자 이름에 해당하지 않아도 됩니다. 표준 /etc/ppp/pap-secrets에 대한 자세한 내용은 130 페이지 “/etc/ppp/pap-secrets 파일”을 참조하십시오.

신뢰할 수 있는 잠재적 호출자에게 UNIX 사용자 이름 및 암호가 없는 경우 다음을 수행하십시오.

a. 개인적으로 알고 있지 않은 호출자의 경우 해당 호출자의 관리자에게 이들이 다이얼 인 서버에 대한 액세스 권한을 가지고 있는지 확인합니다.

b. 회사 보안 정책에 명시된 방식으로 이러한 호출자의 UNIX 사용자 이름 및 암호를 만듭니다.

3 다이얼 인 서버에서 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

4 `/etc/ppp/pap-secrets` 파일을 편집합니다.

이번 릴리스는 `pap-secrets` 파일(`/etc/ppp`에 있음)을 제공합니다. 여기에는 PAP 인증을 사용하는 방법에 대한 설명이 포함되어 있지만 옵션은 포함되어 있지 않습니다. 설명 끝에 다음과 같은 옵션을 추가할 수 있습니다.

```
user1      myserver        ""          *
user2      myserver        ""          *
myserver   user2           serverpass  *
```

`login` 옵션(`/etc/ppp/pap-secrets`)을 사용하려면 신뢰할 수 있는 각 호출자의 UNIX 사용자 이름을 입력해야 합니다. 세번째 필드에 큰따옴표("") 세트가 나타날 때마다 서버의 암호 데이터베이스에서 호출자의 암호가 조회됩니다.

`myserver * serverpass *` 항목에는 다이얼 인 서버의 PAP 사용자 이름 및 암호가 포함되어 있습니다. 그림 2–3에서 신뢰할 수 있는 호출자인 `user2`에게는 원격 피어로부터의 인증 작업이 필요합니다. 따라서 `user2`와 링크가 설정된 경우 `myserver`의 `/etc/ppp/pap-secrets` 파일에 사용할 PAP 자격 증명이 포함됩니다.

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 72 페이지 "PAP를 위해 PPP 구성 파일 수정(다이얼 인 서버)"
- 74 페이지 "신뢰할 수 있는 호출자에 대해 PAP 인증 구성(다이얼 아웃 시스템)"

PAP를 위해 PPP 구성 파일 수정(다이얼 인 서버)

이 절의 작업에서는 다이얼 인 서버에서 PAP 인증을 지원하기 위해 기존 PPP 구성 파일을 업데이트하는 방법에 대해 설명합니다.

▼ PPP 구성 파일에 PAP 지원을 추가하는 방법(다이얼 인 서버)

절차에는 59 페이지 "직렬 회선을 통해 통신을 정의하는 방법(다이얼 인 서버)"에 소개된 PPP 구성 파일이 예로 사용됩니다.

1 다이얼 인 서버에서 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 /etc/ppp/options 파일에 인증 옵션을 추가합니다.

예를 들어 굵게 표시된 옵션을 기존 /etc/ppp/options 파일에 추가하면 PAP 인증이 구현됩니다.

```
lock
auth
login
nodefaultroute
proxyarp
ms-dns 10.0.0.1
idle 120
```

auth	서버에서 링크를 설정하기 전에 호출자를 인증해야 함을 지정합니다.
login	표준 UNIX 사용자 인증 서비스를 사용하여 원격 호출자를 인증해야 함을 지정합니다.
nodefaultroute	로컬 시스템에 있는 어떤 pppd 세션도 root 권한 없이 기본 경로를 설정할 수 없음을 나타냅니다.
proxyarp	피어의 IP 주소 및 시스템의 이더넷 주소를 지정하는 항목을 시스템의 ARP(주소 결정 프로토콜) 테이블에 추가합니다. 이 옵션을 사용하면 다른 시스템에서 피어가 로컬 이더넷에 있는 것처럼 보입니다.
ms-dns 10.0.0.1	pppd를 사용으로 설정하여 DNS(도메인 이름 서버) 주소인 10.0.0.1을 클라이언트에 제공합니다.
idle 120	유휴 사용자가 2분 후에 연결 해제되도록 지정합니다.

3 /etc/ppp/options.cua.a 파일에서 cua/a 사용자에 대해 다음 주소를 추가합니다.

```
:10.0.0.2
```

4 /etc/ppp/options.cua.b 파일에서 cua/b 사용자에 대해 다음 주소를 추가합니다.

```
:10.0.0.3
```

5 **/etc/ppp/pap-secrets 파일에서 다음 항목을 추가합니다.**

```
*       *           ""      *
```

주 – 앞서 설명한 `login` 옵션은 필요한 사용자 인증을 제공합니다. `/etc/ppp/pap-secrets` 파일에 이렇게 입력하는 것이 `login` 옵션을 사용하여 PAP를 사용으로 설정하는 표준 방법입니다.

참조 다이얼 인 서버의 신뢰할 수 있는 호출자에 대해 PAP 인증 자격 증명을 구성하려면 74 페이지 "신뢰할 수 있는 호출자에 대해 PAP 인증 구성(다이얼 아웃 시스템)"을 참조하십시오.

신뢰할 수 있는 호출자에 대해 PAP 인증 구성(다이얼 아웃 시스템)

이 절에는 신뢰할 수 있는 호출자의 다이얼 아웃 시스템에서 PAP 인증을 설정하는 작업이 있습니다. 시스템 관리자는 잠재적 호출자에 대한 배포 작업 전에 시스템에서 PAP 인증을 설정할 수 있습니다. 원격 호출자에게 이미 자신의 시스템이 있는 경우에는 이 절의 작업을 해당 호출자에게 할당할 수도 있습니다.

신뢰할 수 있는 호출자에 대해 PAP를 구성하기 위해 수행해야 하는 두 작업은 다음과 같습니다.

- 호출자의 PAP 보안 자격 증명 구성
- PAP 인증을 지원하기 위해 호출자의 다이얼 아웃 시스템 구성

▼ 신뢰할 수 있는 호출자에 대해 PAP 인증 자격 증명을 구성하는 방법

이 절차에서는 신뢰할 수 있는 두 호출자에 대해 PAP 자격 증명을 설정하는 방법을 보여줍니다. 둘 중 하나는 원격 피어로부터 인증 자격 증명을 받아야 합니다. 절차 단계에서는 시스템 관리자가 신뢰할 수 있는 호출자의 다이얼 아웃 시스템에서 PAP 자격 증명을 만든다고 가정합니다.

1 **다이얼 아웃 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

그림 2–3에 소개된 샘플 PAP 구성을 사용하여 다이얼 아웃 시스템이 `user1`에게 속한다고 가정합니다.

2 **호출자의 pap-secrets 데이터베이스를 수정합니다.**

이번 릴리스는 /etc/ppp/pap-secrets 파일을 제공합니다. 여기에는 유용한 설명이 포함되어 있지만 옵션은 포함되어 있지 않습니다. 이 /etc/ppp/pap-secrets 파일에 다음과 같은 옵션을 추가할 수 있습니다.

```
user1    myserver  pass1    *
```

user1의 암호인 pass1은 읽을 수 있는 ASCII 형식으로 링크를 통해 전달됩니다. myserver는 피어를 위한 호출자 user1의 이름입니다.

3 **다이얼 아웃 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

PAP 인증 예를 사용하여 이 다이얼 아웃 시스템이 호출자 user2에게 속한다고 가정합니다.

4 **호출자의 pap-secrets 데이터베이스를 수정합니다.**

기존 /etc/ppp/pap-secrets 파일의 끝에 다음 옵션을 추가할 수 있습니다.

```
user2     myserver   pass2       *
myserver  user2      serverpass  *
```

이 예에서 /etc/ppp/pap-secrets에는 두 항목이 있습니다. 첫번째 항목에는 user2가 인증을 위해 다이얼 인 서버 myserver에 전달하는 PAP 보안 자격 증명이 포함되어 있습니다.

user2에는 링크 협상의 일환으로 다이얼 인 서버에서 가져온 PAP 자격 증명이 필요합니다. 따라서 /etc/ppp/pap-secrets에 myserver의 두번째 행에 있어야 하는 PAP 자격 증명도 포함됩니다.

주 – 대부분의 ISP는 인증 자격 증명을 제공하지 않으므로 ISP와 통신하는 경우 이전 시나리오가 현실적이지 않을 수 있습니다.

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 71 페이지 "PAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)"
- 74 페이지 "신뢰할 수 있는 호출자에 대해 PAP 인증 자격 증명을 구성하는 방법"

PAP를 위해 PPP 구성 파일 수정(다이얼 아웃 시스템)

다음 작업에서는 신뢰할 수 있는 호출자의 다이얼 아웃 시스템에서 PAP 인증을 지원하기 위해 기존 PPP 구성 파일을 업데이트하는 방법에 대해 설명합니다.

절차에서는 다음 매개변수를 사용하여 user2(그림 2–3에 소개됨)에게 속하는 다이얼 아웃 시스템에서 PAP 인증을 구성합니다. user2는 수신 호출자가 다이얼 인 myserver로부터의 호출 등을 인증하도록 요구합니다.

▼ PPP 구성 파일에 PAP 지원을 추가하는 방법(다이얼 아웃 시스템)

이 절차에는 52 페이지 "직렬 회선을 통해 통신을 정의하는 방법"에 소개된 PPP 구성 파일이 예로 사용됩니다. 이 절차에서는 user2에게 속하는 다이얼 아웃 시스템을 그림 2–3에 나와 있는 대로 구성합니다.

1 **다이얼 아웃 시스템에 수퍼 유저로 로그인합니다.**

2 **/etc/ppp/options 파일을 수정합니다.**

다음 /etc/ppp/options 파일에는 PAP 지원을 위한 옵션(굵게 표시됨)이 포함되어 있습니다.

```
# cat /etc/ppp/options
lock
name user2
auth
require-pap
```

name user2 — user2를 로컬 시스템에 있는 사용자의 PAP 이름으로 설정합니다. login 옵션을 사용할 경우 PAP 이름이 암호 데이터베이스에 있는 UNIX 사용자 이름과 동일해야 합니다.

auth — 다이얼 아웃 시스템이 링크를 설정하기 전에 호출자를 인증해야 함을 지정합니다.

주 – 대부분의 다이얼 아웃 시스템은 인증을 요구하지 않지만 이 다이얼 아웃 시스템은 해당 피어로부터 인증을 요구합니다. 둘 모두 허용 가능합니다.

---

require-pap — 피어로부터 PAP 자격 증명을 요구합니다.

3 **/etc/ppp/peers/*peer-name* 파일을 원격 시스템 myserver에 대해 만듭니다.**

다음 예에서는 기존 /etc/ppp/peers/myserver 파일(54 페이지 "개별 피어를 사용하여 연결을 정의하는 방법"에서 만들어짐)에 PAP 지원을 추가하는 방법을 보여줍니다.

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
```

```
idle 120
user user2
remotename myserver
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

굵게 표시된 새 옵션은 피어 myserver에 대한 PAP 요구 사항을 추가합니다.

user user2	user2를 로컬 시스템의 사용자 이름으로 정의합니다.
remotename myserver	myserver를 로컬 시스템에서 인증 자격 증명을 가져와야 하는 피어로 정의합니다.

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 다이얼 인 서버를 호출하여 PAP 인증 설정을 테스트하려면 60 페이지 "다이얼 인 서버를 호출하는 방법"을 참조하십시오.
- PAP 인증에 대한 자세한 내용은 130 페이지 "PAP(암호 인증 프로토콜)"를 참조하십시오.

CHAP 인증 구성

이 절의 작업에서는 CHAP(Challenge-Handshake 인증 프로토콜)를 사용하여 PPP 링크에 대해 인증을 구현하는 방법에 대해 설명합니다. 작업에는 개인 네트워크에 대한 다이얼 업에 맞는 CHAP 시나리오를 보여주기 위해 그림 2–4에 나와 있는 예가 사용됩니다. 지침을 기반으로 사용자 사이트에서 CHAP 인증을 구현해 보십시오.

후속 절차를 수행하려면 다음 작업을 완료해야 합니다.

- 다이얼 인 서버와 신뢰할 수 있는 호출자에 속하는 다이얼 아웃 시스템 간에 다이얼 업 링크를 설정하고 테스트
- 로컬 시스템(다이얼 인 서버 또는 다이얼 아웃 시스템)에 대한 수퍼 유저 사용 권한 획득

CHAP 인증 설정(작업 맵)

표 5–4 CHAP 인증 작업 맵(다이얼 인 서버)

작업	설명	수행 방법
1. 신뢰할 수 있는 모든 호출자에게 CHAP 암호 지정	CHAP 암호를 만들거나 호출자가 CHAP 암호를 만들게 합니다.	79 페이지 "CHAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)"

표 5–4 CHAP 인증 작업 맵(다이얼 인 서버) *(계속)*

작업	설명	수행 방법
2. chap-secrets 데이터베이스 만들기	신뢰할 수 있는 모든 호출자에 대한 보안 자격 증명을 `/etc/ppp/chap-secrets` 파일에 추가합니다.	79 페이지 “CHAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)”
3. PPP 구성 파일 수정	`/etc/ppp/options` 및 `/etc/ppp/peers/`*peer-name* 파일에 CHAP 관련 옵션을 추가합니다.	80 페이지 “PPP 구성 파일에 CHAP 지원을 추가하는 방법(다이얼 인 서버)”

표 5–5 CHAP 인증 작업 맵(다이얼 아웃 시스템)

작업	설명	수행 방법
1. 신뢰할 수 있는 호출자의 시스템에 대한 CHAP 데이터베이스 만들기	`/etc/ppp/chap-secrets`에서 신뢰할 수 있는 호출자에 대한 보안 자격 증명을 만들고 필요한 경우 다이얼 아웃 시스템을 호출하는 다른 사용자에 대한 보안 자격 증명을 만듭니다.	79 페이지 “CHAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)”
2. PPP 구성 파일 수정	`/etc/ppp/options` 파일에 CHAP 관련 옵션을 추가합니다.	82 페이지 “PPP 구성 파일에 CHAP 지원을 추가하는 방법(다이얼 아웃 시스템)”

다이얼 인 서버에서 CHAP 인증 구성

CHAP 인증을 설정하는 첫번째 작업은 `/etc/ppp/chap-secrets` 파일을 수정하는 것입니다. 이 파일에는 링크의 호출자를 인증하는 데 사용되는 CHAP 보안 자격 증명(CHAP 암호 포함)이 포함되어 있습니다.

주 – UNIX 또는 PAM 인증 방식은 CHAP와 함께 작동하지 않습니다. 예를 들어 PPP `login` 옵션을 71 페이지 “PAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)”에 설명된 대로 사용할 수 없습니다. 인증 시나리오에 PAM 또는 UNIX 스타일의 인증이 필요한 경우에는 대신 PAP를 선택하십시오.

다음 절차에서는 개인 네트워크에 있는 다이얼 인 서버에 대해 CHAP 인증을 구현합니다. PPP 링크가 외부 세계에 대한 유일한 연결입니다. 네트워크 관리자가 네트워크에 액세스할 수 있는 호출자에게만 사용 권한을 부여했습니다(시스템 관리자 포함).

▼ CHAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)

1 **신뢰할 수 있는 모든 호출자의 사용자 이름이 포함된 목록을 어셈블합니다.**

신뢰할 수 있는 호출자에는 개인 네트워크를 호출할 수 있는 권한을 부여받은 모든 사람이 포함됩니다.

2 **각 사용자에게 CHAP 암호를 지정합니다.**

주 – 쉽게 추측할 수 없는 CHAP 암호를 선택하십시오. CHAP 암호 내용에 이 이외에 다른 제한은 없습니다.

CHAP 암호 지정 방법은 사이트 보안 정책에 따라 달라집니다. 즉, 관리자가 암호를 만들거나 호출자가 자신의 암호를 만들어야 합니다. 관리자가 CHAP 암호를 지정하지 않는 경우 신뢰할 수 있는 각 호출자가 만들었거나 이러한 호출자를 위해 만들어진 CHAP 암호를 받으십시오.

3 **다이얼 인 서버에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

4 **`/etc/ppp/chap-secrets` 파일을 수정합니다.**

이번 릴리스에는 `/etc/ppp/chap-secrets` 파일이 포함되어 있습니다. 여기에는 유용한 설명이 포함되어 있지만 옵션은 포함되어 있지 않습니다. 다음과 같은 `CallServe` 서버 옵션을 기존 `/etc/ppp/chap-secrets` 파일의 끝에 추가할 수 있습니다.

```
account1  CallServe   key123   *
account2  CallServe   key456   *
```

`key123` - 신뢰할 수 있는 호출자 `account1`의 CHAP 암호

`key456` - 신뢰할 수 있는 호출자 `account2`의 CHAP 암호

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 79 페이지 "CHAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)"
- 80 페이지 "PPP 구성 파일에 CHAP 지원을 추가하는 방법(다이얼 인 서버)"
- 80 페이지 "신뢰할 수 있는 호출자에 대해 CHAP 인증 구성(다이얼 아웃 시스템)"

CHAP를 위해 PPP 구성 파일 수정(다이얼 인 서버)

이 절의 작업에서는 기존 PPP 구성 파일을 업데이트하여 다이얼 인 서버에서 CHAP 인증을 지원하는 방법에 대해 설명합니다.

▼ PPP 구성 파일에 CHAP 지원을 추가하는 방법(다이얼 인 서버)

1 **다이얼 인 서버에 수퍼 유저로 로그인합니다.**

2 **/etc/ppp/options 파일을 수정합니다.**

CHAP 지원을 위해 굵게 표시된 옵션을 추가합니다.

```
# cat /etc/ppp/options
lock
nodefaultroute
name CallServe
auth
```

name *CallServe*	이 다이얼 인 서버 인스턴스에서 *CallServe*를 로컬 시스템에 있는 사용자의 CHAP 이름으로 정의합니다.
auth	로컬 시스템에서 링크를 설정하기 전에 호출자를 인증하게 만듭니다.

3 **신뢰할 수 있는 호출자를 지원하기 위해 나머지 PPP 구성 파일을 만듭니다.**

58 페이지 “다이얼 인 서버의 사용자를 구성하는 방법” 및 59 페이지 “직렬 회선을 통해 통신을 정의하는 방법(다이얼 인 서버)”을 참조하십시오.

참조 신뢰할 수 있는 호출자를 위한 CHAP 인증 자격 증명을 구성하려면 79 페이지 “CHAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)”을 참조하십시오.

신뢰할 수 있는 호출자에 대해 CHAP 인증 구성(다이얼 아웃 시스템)

이 절에는 신뢰할 수 있는 호출자의 다이얼 아웃 시스템에서 CHAP 인증을 설정하는 작업이 있습니다. 사이트 보안 정책에 따라 관리자나 신뢰할 수 있는 호출자가 CHAP 인증을 설정해야 할 수 있습니다.

CHAP를 구성하는 원격 호출자의 경우 호출자의 로컬 CHAP 암호가 다이얼 인 서버의 /etc/ppp/chap-secrets 파일에 있는 호출자의 해당 CHAP 암호와 일치해야 합니다. 그런 다음 호출자에게 이 절에 나와 있는 CHAP 구성 작업을 할당합니다.

신뢰할 수 있는 호출자에 대해 CHAP를 구성하기 위해 수행해야 하는 두 작업은 다음과 같습니다.

- 호출자의 CHAP 보안 자격 증명 만들기
- CHAP 인증을 지원하기 위해 호출자의 다이얼 아웃 시스템 구성

▼ 신뢰할 수 있는 호출자에 대해 CHAP 인증 자격 증명을 구성하는 방법

이 절차에서는 신뢰할 수 있는 두 호출자에 대해 CHAP 자격 증명을 설정하는 방법을 보여줍니다. 절차 단계에서는 시스템 관리자가 신뢰할 수 있는 호출자의 다이얼 아웃 시스템에서 CHAP 자격 증명을 만든다고 가정합니다.

1 **다이얼 아웃 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

42 페이지 "CHAP 인증을 사용한 구성의 예"의 샘플 CHAP 구성을 사용하여 다이얼 아웃 시스템이 신뢰할 수 있는 호출자 `account1`에 속한다고 가정합니다.

2 **호출자 `account1`의 chap-secrets 데이터베이스를 수정합니다.**

이번 릴리스에는 `/etc/ppp/chap-secrets` 파일이 포함되어 있습니다. 여기에는 유용한 설명이 포함되어 있지만 옵션은 포함되어 있지 않습니다. 다음과 같은 옵션을 기존 `/etc/ppp/chap-secrets` 파일에 추가할 수 있습니다.

```
account1   CallServe    key123    *
```

`CallServe`는 `account1`이 연결하려고 하는 피어의 이름입니다. `key123`은 `account1`과 `CallServer` 간의 링크에 사용될 CHAP 암호입니다.

3 **다이얼 아웃 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

이 시스템이 호출자 `account2`에게 속한다고 가정합니다.

4 **호출자 `account2`에 대한 `/etc/ppp/chap-secrets` 데이터베이스를 수정합니다.**

```
account2   CallServe    key456    *
```

이제 `account2`에 암호 `key456`이 해당 CHAP 자격 증명으로 설정되었습니다. 이를 피어 `CallServe`에 대한 링크에 사용할 수 있습니다.

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 79 페이지 "CHAP 자격 증명 데이터베이스를 만드는 방법(다이얼 인 서버)"
- 81 페이지 "신뢰할 수 있는 호출자에 대해 CHAP 인증 자격 증명을 구성하는 방법"

구성 파일에 CHAP 추가(다이얼 아웃 시스템)

CHAP 인증에 대한 자세한 내용은 133 페이지 “CHAP(Challenge-Handshake 인증 프로토콜)”를 참조하십시오. 다음 작업에서는 호출자 account1에 속하는 다이얼 아웃 시스템을 구성합니다. 이는 42 페이지 “CHAP 인증을 사용한 구성의 예”에 소개되어 있습니다.

▼ PPP 구성 파일에 CHAP 지원을 추가하는 방법(다이얼 아웃 시스템)

1 다이얼 아웃 시스템에 수퍼 유저로 로그인합니다.

2 /etc/ppp/options 파일에 다음과 같은 옵션이 있는지 확인합니다.

```
# cat /etc/ppp/options
lock
nodefaultroute
```

3 /etc/ppp/peers/*peer-name* 파일을 원격 시스템 CallServe에 대해 만듭니다.

```
# cat /etc/ppp/peers/CallServe
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user account1
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

user account1 옵션은 account1을 CallServe에 제공할 CHAP 사용자 이름으로 설정합니다. 이전 파일의 기타 옵션에 대한 자세한 내용은 유사한 /etc/ppp/peers/myserver 파일(54 페이지 “개별 피어를 사용하여 연결을 정의하는 방법”)을 참조하십시오.

참조 다이얼 인 서버를 호출하여 CHAP 인증을 테스트하려면 60 페이지 “다이얼 인 서버를 호출하는 방법”을 참조하십시오.

◆ ◆ ◆ 6 장

6 PPPoE 터널 설정(작업)

이 장에는 PPPoE 터널의 각 끝에서 참가자(PPPoE 클라이언트 및 PPPoE 액세스 서버)를 설정하는 작업이 포함되어 있습니다. 관련 항목은 다음과 같습니다.

- 83 페이지 “PPPoE 터널을 설정하는 주요 작업(작업 맵)”
- 84 페이지 “PPPoE 클라이언트 설정”
- 87 페이지 “PPPoE 액세스 서버 설정”

작업에는 44 페이지 “PPPoE 터널을 통한 DSL 지원 계획”에서 예로 소개된 시나리오가 사용됩니다. PPPoE의 개요는 30 페이지 “PPPoE를 통한 DSL 사용자 지원”을 참조하십시오.

PPPoE 터널을 설정하는 주요 작업(작업 맵)

다음 표에는 PPPoE 클라이언트 및 PPPoE 액세스 서버를 구성하는 주요 작업이 나열되어 있습니다. 사이트에서 PPPoE를 구현하려면 PPPoE 터널의 본인 쪽 끝(클라이언트측 또는 액세스 서버측)만 설정하면 됩니다.

표 6–1 PPPoE 클라이언트 설정 작업 맵

작업	설명	수행 방법
1. PPPoE용 인터페이스 구성	PPPoE 터널에 사용할 이더넷 인터페이스를 정의합니다.	84 페이지 “PPPoE 클라이언트용 인터페이스를 구성하는 방법”
2. PPPoE 액세스 서버에 대한 정보 구성	PPPoE 터널의 서비스 공급자 쪽 끝에서 액세스 서버에 대한 매개변수를 정의합니다.	85 페이지 “PPPoE 액세스 서버 피어를 정의하는 방법”
3. PPP 구성 파일 설정	클라이언트용 PPP 구성 파일을 아직 정의하지 않은 경우 하나 정의합니다.	52 페이지 “직렬 회선을 통해 통신을 정의하는 방법”
4. 터널 만들기	액세스 서버를 호출합니다.	85 페이지 “PPPoE 액세스 서버 피어를 정의하는 방법”

표 6–2 PPPoE 액세스 서버 설정 작업 맵

작업	설명	수행 방법
1. PPPoE 액세스 서버 설정	PPPoE 터널에 사용할 이더넷 인터페이스를 정의하고 액세스 서버가 제공하는 서비스를 정의합니다.	87 페이지 “PPPoE 액세스 서버를 설정하는 방법”
2. PPP 구성 파일 설정	클라이언트용 PPP 구성 파일을 아직 정의하지 않은 경우 하나 정의합니다.	59 페이지 “다이얼 인 서버를 통한 통신 구성”
3. (옵션) 인터페이스 사용 제한	PPPoE 옵션 및 PAP 인증을 사용하여 특정 클라이언트만이 특정 이더넷 인터페이스를 사용할 수 있도록 제한합니다.	88 페이지 “특정 클라이언트만 인터페이스를 사용할 수 있도록 제한하는 방법”

PPPoE 클라이언트 설정

DSL을 통해 클라이언트 시스템에 PPP를 제공하려면 먼저 모뎀 또는 허브에 연결된 인터페이스에서 PPPoE를 구성해야 합니다. 그런 다음 PPP 구성 파일을 변경하여 PPPoE의 반대쪽 끝에서 액세스 서버를 정의해야 합니다.

PPPoE 클라이언트 설정을 위한 필수 조건

PPPoE 클라이언트를 설정하려면 먼저 다음 작업을 완료해야 합니다.

- PPPoE 터널을 사용할 클라이언트 시스템에 Oracle Solaris 릴리스 설치
- 서비스 공급자에 해당 PPPoE 액세스 서버에 대한 정보 문의
- 전화 회사 또는 서비스 공급자에게 클라이언트 시스템에 사용되는 장치 조립 요청. 이러한 장치에는 관리자가 아니라 전화 회사가 조립하는 DSL 모뎀, 분리기 등이 포함됩니다.

▼ PPPoE 클라이언트용 인터페이스를 구성하는 방법

이 절차를 사용하여 PPPoE 터널에 사용할 이더넷 인터페이스를 정의할 수 있습니다.

1 **PPPoE 클라이언트에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 “지정된 관리 권한을 사용하는 방법”을 참조하십시오.

2 **DSL 연결이 있는 이더넷 인터페이스의 이름을 /etc/ppp/pppoe.if 파일에 추가합니다.**

예를 들어, 다음 항목을 /etc/ppp/pppoe.if에 추가합니다. 이는 hme0을 DSL 모뎀에 연결된 네트워크 인터페이스로 사용하는 PPPoE 클라이언트의 경우입니다.

```
hme0
```

/etc/ppp/pppoe.if에 대한 자세한 내용을 보려면 139 페이지 "/etc/ppp/pppoe.if 파일"로 이동하십시오.

3 **PPPoE용 인터페이스를 구성합니다.**

```
# /etc/init.d/pppd start
```

4 **(옵션) 인터페이스가 이제 PPPoE에 연결되었는지 확인합니다.**

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
```

/usr/sbin/sppptun 명령을 사용하여 인터페이스를 PPPoE에 수동으로 연결할 수도 있습니다. 지침은 139 페이지 "/usr/sbin/sppptun 명령"을 참조하십시오.

▼ PPPoE 액세스 서버 피어를 정의하는 방법

액세스 서버는 /etc/ppp/peers/*peer-name* 파일에서 정의합니다. 액세스 서버에 사용되는 옵션 중 상당수가 다이얼 업 시나리오에서 다이얼 인 서버를 정의하는 데에도 사용됩니다. /etc/ppp/peers.*peer-name*에 대한 자세한 내용은 118 페이지 "/etc/ppp/peers/*peer-name* 파일"을 참조하십시오.

1 **PPPoE 클라이언트에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **서비스 공급자의 PPPoE 액세스 서버를 /etc/ppp/peers/*peer-name* 파일에서 정의합니다.**

예를 들어, /etc/ppp/peers/dslserve 파일은 Far ISP의 액세스 서버 dslserve(45 페이지 "PPPoE 터널 구성의 예"에서 소개됨)를 정의합니다.

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

이 파일의 옵션에 대한 정의를 보려면 146 페이지 "액세스 서버 피어를 정의하기 위한 /etc/ppp/peers/*peer-name* 파일"로 이동하십시오.

3 **PPPoE 클라이언트에서 다른 PPP 구성 파일을 수정합니다.**

a. **/etc/ppp/options를 구성합니다. 이때 50 페이지 "다이얼 아웃 시스템 구성"에 나와 있는 다이얼 아웃 시스템 구성 지침을 따르십시오.**

b. **/etc/ppp/options.sppptun 파일을 만듭니다. /etc/ppp/options.sppptun은 PPPoE에 연결되는 인터페이스가 연결되는 직렬 포트에 대한 PPP 옵션을 정의합니다.**

/etc/ppp/options.*ttyname* 파일(115 페이지 "/etc/ppp/options.*ttyname* 구성 파일"에 설명되어 있음)에 대해 사용할 수 있는 모든 옵션을 사용할 수 있습니다. /etc/ppp/options.sppptun 파일의 이름을 지정해야 합니다. 이는 sppptun이 pppd 구성에서 지정된 장치 이름이기 때문입니다.

4 **모든 사용자가 클라이언트에서 PPP를 시작할 수 있는지 확인합니다.**

```
# touch /etc/ppp/options
```

5 **PPP를 DSL 회선을 통해 실행할 수 있는지 테스트합니다.**

```
% pppd debug updetach call dslserve
```

dslserve는 ISP의 액세스 서버(45 페이지 "PPPoE 터널 구성의 예"에 나와 있음)에 지정되는 이름입니다. debug updetach 옵션을 사용하면 디버깅 정보가 단말기 창에 표시됩니다.

PPP가 올바르게 실행되고 있는 경우 단말기 출력에서 링크가 활성 상태가 됩니다. PPP가 계속 실행되지 않는 경우 다음 명령을 실행하여 서버가 올바르게 실행되고 있는지 확인합니다.

```
# /usr/lib/inet/pppoec -i hme0
```

주 – 구성된 PPPoE 클라이언트의 사용자는 다음을 입력하여 DSL 회선을 통해 PPP 실행을 시작할 수 있습니다.

```
% pppd call ISP-server-name
```

그런 다음 사용자는 응용 프로그램 또는 서비스를 실행할 수 있습니다.

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- 84 페이지 "PPPoE 클라이언트 설정"을 참조하십시오.
- 138 페이지 "DSL 지원을 위해 PPPoE 터널 만들기"를 참조하십시오.
- 7 장, "일반적인 PPP 문제 해결(작업)"을 참조하십시오.
- 87 페이지 "PPPoE 액세스 서버 설정"을 참조하십시오.

PPPoE 액세스 서버 설정

서비스 공급업체의 경우 DSL 연결을 통해 사이트에 연결하는 클라이언트에 인터넷 및 기타 서비스를 제공할 수 있습니다. 절차에서는 PPPoE 터널에 사용할 서버의 인터페이스를 결정하고 사용자에게 제공할 서비스를 정의합니다.

▼ PPPoE 액세스 서버를 설정하는 방법

이 절차를 사용하여 PPPoE 터널에 사용할 이더넷 인터페이스를 정의하고 액세스 서버가 제공하는 서비스를 구성할 수 있습니다.

1 **액세스 서버에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **PPPoE 터널 전용 이더넷 인터페이스의 이름을 /etc/ppp/pppoe.if 파일에 추가합니다.**

예를 들어, /etc/ppp/pppoe.if 파일을 액세스 서버 dslserve(45 페이지 "PPPoE 터널 구성의 예"에 나와 있음)에 사용합니다.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
```

3 **액세스 서버가 제공하는 전역 서비스를 /etc/ppp/pppoe 파일에서 정의합니다.**

/etc/ppp/pppoe 파일은 액세스 서버 dslserve(그림 2–5에 나와 있음)가 제공하는 서비스를 나열합니다.

```
device hme1,hme2
service internet
    pppd "proxyarp 192.168.1.1:"
service debugging
    pppd "debug proxyarp 192.168.1.1:"
```

파일 예에서 인터넷 서비스는 dslserve의 이더넷 인터페이스 hme1 및 hme2에 대해 공지됩니다. 디버깅은 이더넷 인터페이스에서 PPP 링크에 대해 켜집니다.

4 **PPP 구성 파일을 다이얼 인 서버와 동일한 방식으로 설정합니다.**

자세한 내용은 136 페이지 "호출자를 위한 IP 주소 지정 체계 만들기"를 참조하십시오.

5 **pppoed 데몬을 시작합니다.**

```
# /etc/init.d/pppd start
```

pppd는 /etc/ppp/pppoe.if에 나열되어 있는 인터페이스도 연결합니다.

6 **(옵션) 서버의 인터페이스가 PPPoE에 연결되었는지 확인합니다.**

```
# /usr/sbin/sppptun query
hme1:pppoe
```

```
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

이전 샘플에서는 인터페이스 hme1 및 hme2가 현재 PPPoE에 연결되어 있음을 보여줍니다. /usr/sbin/sppptun 명령을 사용하여 인터페이스를 PPPoE에 수동으로 연결할 수도 있습니다. 지침은 139 페이지 "/usr/sbin/sppptun 명령"을 참조하십시오.

▼ 기존 /etc/ppp/pppoe 파일을 수정하는 방법

1. **액세스 서버에서 관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **필요에 따라 /etc/ppp/pppoe를 수정합니다.**

3. **pppoed 데몬이 새 서비스를 인식하게 만듭니다.**

   ```
   # pkill -HUP pppoed
   ```

▼ 특정 클라이언트만 인터페이스를 사용할 수 있도록 제한하는 방법

다음 절차에서는 한 PPPoE 클라이언트 그룹으로 인터페이스를 제한하는 방법을 보여줍니다. 이 작업을 수행하기 전에 인터페이스에 지정하는 클라이언트의 실제 이더넷 MAC 주소를 가져와야 합니다.

주 – 일부 시스템의 경우 이더넷 인터페이스에서 MAC 주소를 변경할 수 있습니다. 그러나 이 기능은 보안 조치가 아닌 편리한 옵션으로 보아야 합니다.

---

45 페이지 "PPPoE 터널 구성의 예"에 나와 있는 예를 사용하여 이러한 단계에서는 dslserve의 인터페이스 중 하나인 hme1을 MiddleCo의 클라이언트를 위해 예약하는 방법을 보여줍니다.

1. **87 페이지 "PPPoE 액세스 서버를 설정하는 방법"에 나와 있는 대로 액세스 서버의 인터페이스를 구성하고 서비스를 정의합니다.**

2. **클라이언트에 대한 항목을 서버의 /etc/ethers 데이터베이스에 만듭니다.**

   Red, Blue 및 Yellow라는 클라이언트에 대한 샘플 항목은 다음과 같습니다.

   ```
   8:0:20:1:40:30 redether
   8:0:20:1:40:10 yellowether
   8:0:20:1:40:25 blueether
   ```

샘플에서는 redether, yellowether 및 blueether라는 심볼릭 이름을 Red, Yellow 및 Blue라는 클라이언트의 이더넷 주소에 지정합니다. MAC 주소에 심볼릭 이름을 지정하는 작업은 선택 사항입니다.

3 /etc/ppp/pppoe.*device* 파일에서 다음 정보를 정의하여 특정 인터페이스에서 제공되는 서비스를 제한합니다.

이 파일에서 **장치**는 정의할 장치의 이름입니다.

```
# cat /etc/ppp/pppoe.hme1
service internet
     pppd "name dslserve-hme1"
     clients redether,yellowether,blueether
```

dslserve-hme1은 액세스 서버의 이름으로, pap-secrets 파일의 일치하는 항목에 사용됩니다. clients 옵션을 사용하면 hme1 인터페이스의 사용이 redether, yellowether 및 blueether라는 심볼릭 이더넷 이름이 지정된 클라이언트로 제한됩니다.

/etc/ethers에서 클라이언트의 MAC 주소를 위한 심볼릭 이름을 정의하지 않은 경우에는 숫자 주소를 clients 옵션의 인수로 사용할 수 있습니다. 와일드카드도 허용됩니다.

예를 들어, clients 8:0:20:*:*:*와 같이 숫자 주소를 지정할 수 있습니다. 와일드카드를 사용하면 /etc/ethers에서 일치하는 모든 주소가 허용됩니다.

4 액세스 서버를 위한 /etc/ppp/pap-secrets 파일을 만듭니다.

```
Red         dslserve-hme1   redpasswd     *
Blue        dslserve-hme1   bluepasswd    *
Yellow      dslserve-hme1   yellowpassd   *
```

항목은 dslserve의 hme1 인터페이스를 통해 PPP를 실행하도록 허용된 클라이언트의 PAP 이름 및 암호입니다.

PAP 인증에 대한 자세한 내용은 70 페이지 “PAP 인증 구성”을 참조하십시오.

참조 다음 목록에는 관련 정보에 대한 참조가 나와 있습니다.

- PPPoE에 대한 자세한 내용은 138 페이지 “DSL 지원을 위해 PPPoE 터널 만들기”를 참조하십시오.
- PPPoE 및 PPP 문제를 해결하려면 95 페이지 “PPP 관련 문제 및 PPPoE 관련 문제 해결”을 참조하십시오.
- PPPoE 클라이언트를 구성하려면 84 페이지 “PPPoE 클라이언트 설정”을 참조하십시오.
- 클라이언트를 위해 PAP 인증을 구성하려면 74 페이지 “신뢰할 수 있는 호출자에 대해 PAP 인증 구성(다이얼 아웃 시스템)”을 참조하십시오.
- 서버에서 PAP 인증을 구성하려면 71 페이지 “다이얼 인 서버에서 PAP 인증 구성”을 참조하십시오.

◆ ◆ ◆ 7 장

7 일반적인 PPP 문제 해결(작업)

이 장에는 Solaris PPP 4.0에서 발생하는 일반적인 문제를 해결하는 방법에 대한 정보가 포함되어 있습니다. 다음 항목을 다룹니다.

- 92 페이지 “PPP 문제 해결 도구”
- 95 페이지 “PPP 관련 문제 및 PPPoE 관련 문제 해결”
- 107 페이지 “전용 회선 문제 해결”
- 107 페이지 “인증 문제 진단 및 해결”

PPP Design, Implementation, and Debugging(James Carlson 저) 및 Australian National University 웹 사이트와 같은 소스를 통해서도 PPP 문제를 해결하기 위한 상세 조언을 구할 수 있습니다. 자세한 내용은 21 페이지 “PPP에 대한 전문 참조 설명서” 및 21 페이지 “PPP에 대한 웹 사이트”를 참조하십시오.

PPP 문제 해결(작업 맵)

다음 작업 맵을 사용하면 일반적인 PPP 문제에 대한 조언 및 해결 방법에 빠르게 액세스할 수 있습니다.

표 7–1 PPP 문제 해결 작업 맵

작업	정의	수행 방법
PPP 링크에 대한 진단 정보 획득	PPP 진단 도구를 사용하여 문제 해결을 위한 출력을 얻을 수 있습니다.	93 페이지 “pppd에서 진단 정보를 가져오는 방법”
PPP 링크에 대한 디버깅 정보 획득	pppd debug 명령을 사용하여 문제 해결을 위한 출력을 생성할 수 있습니다.	94 페이지 “PPP 디버깅을 켜는 방법”
네트워크 계층에 발생하는 일반적인 문제 해결	일련의 검사를 통해 네트워크와 관련된 PPP 문제를 식별하고 해결합니다.	95 페이지 “네트워크 문제를 진단하는 방법”

표 7–1 PPP 문제 해결 작업 맵 *(계속)*

작업	정의	수행 방법
일반적인 통신 문제 해결	PPP 링크에 영향을 주는 통신 문제를 식별하고 해결합니다.	98 페이지 “통신 문제를 진단하고 해결하는 방법”
구성 문제 해결	PPP 구성 파일의 문제를 식별하고 해결합니다.	99 페이지 “PPP 구성을 사용하여 문제를 진단하는 방법”
모뎀 관련 문제 해결	모뎀 문제를 식별하고 해결합니다.	100 페이지 “모뎀 문제를 진단하는 방법”
채트 스크립트 관련 문제 해결	다이얼 아웃 시스템에서 채트 스크립트 문제를 식별하고 해결합니다.	101 페이지 “채트 스크립트에 대한 디버깅 정보를 가져오는 방법”
직렬 회선 속도 문제 해결	다이얼 인 서버에서 회선 속도 문제를 식별하고 해결합니다.	103 페이지 “직렬 회선 속도 문제를 진단하고 해결하는 방법”
전용 회선에 일반적으로 발생하는 문제 해결	전용 회선의 성능 문제를 식별하고 해결합니다.	107 페이지 “전용 회선 문제 해결”
인증 관련 문제 해결	인증 데이터베이스와 관련된 문제를 식별하고 해결합니다.	107 페이지 “인증 문제 진단 및 해결”
PPPoE의 문제 영역 해결	PPP 진단 도구를 사용하여 PPPoE 문제를 식별하고 해결하기 위한 출력을 얻을 수 있습니다.	104 페이지 “PPPoE에 대한 진단 정보를 가져오는 방법”

PPP 문제 해결 도구

일반적으로 PPP 링크의 경우 다음과 같은 세 영역에서 주로 오류가 발생합니다.

- 설정할 링크에 오류 발생
- 정상적으로 사용 중 링크의 성능 저하
- 링크의 각 측에 있는 네트워크가 원인인 문제

PPP의 작동 여부를 알아내는 가장 쉬운 방법은 링크를 통해 명령을 실행하는 것입니다. `ping` 또는 `traceroute`와 같은 명령을 피어의 네트워크에 있는 호스트에 대해 실행한 다음 결과를 관찰하십시오. 그러나 PPP 및 UNIX 디버깅 도구를 사용하여 설정된 링크의 성능을 모니터링하거나 문제가 되는 링크의 문제를 해결해야 합니다.

이 절에서는 `pppd` 및 연관된 해당 로그 파일에서 진단 정보를 가져오는 방법에 대해 설명합니다. 이 장의 나머지 절에서는 PPP 문제 해결 도구를 사용하여 발견하고 해결할 수 있는 일반적인 PPP 문제에 대해 설명합니다.

▼ pppd에서 진단 정보를 가져오는 방법

다음 절차에서는 로컬 시스템에서 링크의 현재 작업을 보는 방법을 보여줍니다.

1 **로컬 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **PPP에 대해 구성된 직렬 장치를 인수로 사용하여 pppd를 실행합니다.**

```
# pppd cua/b debug updetach
```

다음 예에서는 pppd를 전면에서 실행할 때 다이얼 업 링크 및 전용 회선 링크에 대해 표시되는 결과를 보여줍니다. pppd debug를 배경에서 실행하면 생성되는 출력이 /etc/ppp/connect-errors 파일로 전송됩니다.

예 7–1 제대로 작동하는 다이얼 업 링크의 출력

```
# pppd /dev/cua/b debug updetach
have route to 0.0.0.0/0.0.0.0 via 172.21.0.4
serial speed set to 230400 bps
Using interface sppp0
Connect: sppp0 <--> /dev/cua/b
sent [LCP ConfReq id=0x7b <asyncmap 0x0> <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP Ident id=0x79 magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6
    2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
    rcvd [LCP ConfRej id=0x7b <asyncmap 0x0>]
sent [LCP Ident id=0x7c magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Sep 15
    2004 09:38:33)"
sent [LCP ConfReq id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP Ident id=0x7e magic=0x73e981c8 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
    Sep 15 2004 09:38:33)"]
sent [IPCP ConfReq id=0x3d <addr 0.0.0.0> <compress VJ 0f 01>]
rcvd [LCP Ident id=0x7a magic=0xdd4ad820 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
    Oct  6 2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
rcvd [IPCP ConfReq id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
sent [IPCP ConfAck id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
rcvd [IPCP ConfNak id=0x3d <addr 10.0.0.2>]]
sent [IPCP ConfReq id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [IPCP ConfAck id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

예 7–2 제대로 작동하는 전용 회선 링크의 출력

```
# pppd /dev/se_hdlc1 default-asyncmap debug updetach
pppd 2.4.0b1 (Sun Microsystems, Inc., Oct 24 2004 07:13:18) started by root, uid 0
synchronous speed appears to be 0 bps
```

```
init option: '/etc/ppp/peers/syncinit.sh' started (pid 105122)
Serial port initialized.
synchronous speed appears to be 64000 bps
Using interface sppp0
Connect: sppp0 <--> /dev/se_hdlc1
sent [LCP ConfReq id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfAck id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP Ident id=0xea magic=0x474283c6 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
sent [IPCP ConfReq id=0xf7 <addr 0.0.0.0> <compress VJ 0f o1>]]
sent [CCP ConfReq id=0x3f <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [LCP Ident id=0x23 magic=0x8e3a53ff "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 22 2004 14:31:44)
rcvd [IPCP ConfReq id=0x25 <addr 10.0.0.1> <compress VJ 0f 01>]
sent [IPCP ConfAck id=0x25 <addr 10.0.0.1> <compress VJ 0f 01>]
rcvd [CCP ConfReq id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
sent [CCP ConfAck id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
rcvd [IPCP ConfNak id=0xf8 <addr 10.0.0.2>]
rcvd [IPCP ConfReq id=0xf7 <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [CCP ConfAck id=0x3f <deflate 15> <deflate(old#) 15 <bsd v1 15>]
Deflate (15) compression enabled
rcvd [IPCP ConfAck id=0xf8 <addr 10.0.0.2> <compress VJ 0f 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

▼ PPP 디버깅을 켜는 방법

다음 작업에서는 pppd 명령을 사용하여 디버깅 정보를 가져오는 방법을 보여줍니다.

주 – 각 호스트에 대해 1단계에서 3단계까지를 한번씩만 수행하면 됩니다. 그런 다음 4단계를 진행하여 호스트에 대해 디버깅을 켤 수 있습니다.

---

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 pppd의 출력을 보관할 로그 파일을 만듭니다.

```
# touch /var/log/pppdebug
```

3 /etc/syslog.conf에서 pppd에 대해 다음 syslog 기능을 추가합니다.

```
daemon.debug;local2.debug       /var/log/pppdebug
```

4 syslogd를 다시 시작합니다.

```
# pkill -HUP -x syslogd
```

5 **다음 pppd 구문을 사용하여 특정 피어에 대한 호출에 대해 디버깅을 켭니다.**

```
# pppd debug call peer-name
```

*peer-name*은 /etc/ppp/peers 디렉토리에 있는 파일의 이름이어야 합니다.

6 **로그 파일의 내용을 봅니다.**

```
# tail -f /var/log/pppdebug
```

로그 파일의 예는 단계 3을 참조하십시오.

PPP 관련 문제 및 PPPoE 관련 문제 해결

PPP 관련 문제 및 PPPoE 관련 문제를 해결하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

▼ 네트워크 문제를 진단하는 방법

PPP 링크가 활성 상태가 되지만 원격 네트워크에서 연결할 수 있는 네트워크가 거의 없는 경우 네트워크 문제가 표시될 수 있습니다. 다음 절차에서는 PPP 링크에 영향을 주는 네트워크 문제를 격리하고 해결하는 방법을 보여줍니다.

1 **로컬 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **문제가 되는 링크를 종료합니다.**

3 **PPP 구성에 다음 옵션을 추가하여 구성 파일에서 모든 선택적 프로토콜을 사용 안함으로 설정합니다.**

```
noccp novj nopcomp noaccomp default-asyncmap
```

이러한 옵션은 사용 가능한 PPP 중 압축되지 않은 가장 단순한 PPP를 제공합니다. 명령줄에서 pppd에 대한 인수로 이러한 옵션을 호출해 보십시오. 이전에 연결할 수 없었던 호스트에 연결할 수 있는 경우 다음 위치 중 하나에 옵션을 추가합니다.

- /etc/ppp/peers/*peer-name*에서 call 옵션 뒤
- /etc/ppp/options(옵션이 전역적으로 적용되는지 확인)

4 원격 피어를 호출합니다. 그런 다음 디버깅 기능을 사용으로 설정합니다.

```
% pppd debug call peer-name
```

5 chat의 -v 옵션을 사용하여 chat 프로그램에서 상세 정보 로그를 가져옵니다.

예를 들어, 모든 PPP 구성 파일에서 다음 형식을 사용합니다.

```
connect 'chat -v -f /etc/ppp/chatfile'
```

*/etc/ppp/chatfile*은 채트 파일의 이름을 나타냅니다.

6 Telnet 또는 기타 응용 프로그램을 통해 원격 호스트에 연결하여 문제를 재현해 봅니다.

디버깅 로그를 관찰합니다. 계속 원격 호스트에 연결할 수 없으면 PPP 문제가 네트워크 관련 문제일 수 있습니다.

7 원격 호스트의 IP 주소가 등록된 인터넷 주소인지 확인합니다.

일부 조직에서는 로컬 네트워크 내에서 알려져 있지만 인터넷으로 경로를 지정할 수 없는 내부 IP 주소를 지정합니다. 원격 호스트가 회사 내에 있는 경우 NAT(이름-주소 변환) 서버 또는 프록시 서버를 설정해야 인터넷에 연결할 수 있습니다. 원격 호스트가 회사 내에 있지 않은 경우에는 원격 조직에 문제를 보고해야 합니다.

8 경로 지정 테이블을 검사합니다.

a. 로컬 시스템과 피어 모두에서 경로 지정 테이블을 확인합니다.

b. 피어에서 원격 시스템으로 이어지는 경로에 있는 모든 라우터에 대해 경로 지정 테이블을 확인합니다. 또한 다시 피어로 이어지는 경로에 있는 모든 라우터에 대해 경로 지정 테이블을 확인합니다.

중간 라우터가 잘못 구성되지 않았는지 확인합니다. 다시 피어로 이어지는 경로에서 문제가 발견되는 경우가 많습니다.

9 (옵션) 시스템이 라우터인 경우 선택적 기능을 확인합니다.

```
# ndd -set /dev/ip ip_forwarding 1
```

ndd에 대한 자세한 내용은 ndd(1M) 매뉴얼 페이지를 참조하십시오.

Solaris 10 릴리스에서는 ndd(1M) 대신 routeadm(1M)을 사용할 수 있습니다.

```
# routeadm -e ipv4-forwarding -u
```

주 – ndd 명령은 지속되지 않습니다. 이 명령을 사용하여 설정하는 값은 시스템을 재부트할 때 손실됩니다. routeadm 명령은 지속됩니다. 이 명령을 사용하여 설정하는 값은 시스템을 재부트한 후에도 유지됩니다.

10 netstat -s 및 유사한 도구를 통해 얻은 통계를 확인합니다.

netstat에 대한 자세한 내용은 netstat(1M) 매뉴얼 페이지를 참조하십시오.

a. 로컬 시스템에서 통계를 실행합니다.

b. 피어를 호출합니다.

c. netstat -s를 통해 생성된 새로운 통계를 관찰합니다.

자세한 내용은 97 페이지 "PPP에 영향을 주는 일반적인 네트워크 문제"를 참조하십시오.

11 DNS 구성을 확인합니다.

잘못된 이름 서비스 구성을 사용하면 IP 주소를 확인할 수 없기 때문에 응용 프로그램에 오류가 발생합니다.

PPP에 영향을 주는 일반적인 네트워크 문제

netstat - s에 의해 생성되는 메시지를 사용하여 다음 표에 나와 있는 네트워크 문제를 해결할 수 있습니다. 관련 절차 정보는 95 페이지 "네트워크 문제를 진단하는 방법"을 참조하십시오.

표 7–2 PPP에 영향을 주는 일반적인 네트워크 문제

Message	문제점	해결 방법
IP packets not forwardable(IP 패킷 전달 불가)	로컬 호스트에 경로가 없습니다.	로컬 호스트의 경로 지정 테이블에 누락된 경로를 추가합니다.
ICMP input destination unreachable(ICMP 입력 대상에 연결할 수 없음)	로컬 호스트에 경로가 없습니다.	로컬 호스트의 경로 지정 테이블에 누락된 경로를 추가합니다.
ICMP time exceeded(ICMP 시간 초과)	두 라우터가 동일한 대상 주소를 서로에게 전달하고 있어 TTL(활성 시간) 값이 초과될 때까지 패킷이 앞뒤로 재발송됩니다.	traceroute를 사용하여 경로 지정 루프의 소스를 찾은 다음 오류가 발생한 라우터의 관리자에게 문의합니다. traceroute에 대한 자세한 내용은 traceroute(1M) 매뉴얼 페이지를 참조하십시오.

표 7–2 PPP에 영향을 주는 일반적인 네트워크 문제 (계속)

Message	문제점	해결 방법
IP packets not forwardable(IP 패킷 전달 불가)	로컬 호스트에 경로가 없습니다.	로컬 호스트의 경로 지정 테이블에 누락된 경로를 추가합니다.
ICMP input destination unreachable(ICMP 입력 대상에 연결할 수 없음)	로컬 호스트에 경로가 없습니다.	로컬 호스트의 경로 지정 테이블에 누락된 경로를 추가합니다.

▼ 통신 문제를 진단하고 해결하는 방법

통신 문제는 두 피어가 성공적으로 링크를 설정할 수 없을 때 발생합니다. 실제로는 이러한 문제가 잘못 구성된 채트 스크립트로 인해 발생하는 협상 문제인 경우도 있습니다. 다음 절차에서는 통신 문제를 해결하는 방법을 보여줍니다. 잘못된 채트 스크립트로 인해 발생하는 협상 문제를 해결하려면 표 7–5를 참조하십시오.

1 **로컬 시스템에서 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **피어를 호출합니다.**

3 **원격 피어를 호출합니다. 그런 다음 디버깅 기능을 사용으로 설정합니다.**

```
% pppd debug call peer-name
```

특정 통신 문제를 해결하려면 피어에서 디버깅 정보를 가져와야 할 수도 있습니다.

4 **결과 로그에서 통신 문제를 확인합니다. 자세한 내용은 98 페이지 "PPP에 영향을 주는 일반적인 통신 문제"를 참조하십시오.**

PPP에 영향을 주는 일반적인 통신 문제

다음 표에는 98 페이지 "통신 문제를 진단하고 해결하는 방법" 절차의 로그 출력과 관련된 증상이 설명되어 있습니다.

표 7–3 PPP에 영향을 주는 일반적인 통신 문제

증상	문제점	해결 방법
구성-요청이 너무 많습니다.	한 피어가 다른 피어를 들을 수 없습니다.	다음 문제가 있는지 확인합니다. ■ 시스템 또는 모뎀의 케이블 연결이 잘못되었을 수 있습니다. ■ 모뎀 구성에 잘못된 비트 설정이 있을 수 있습니다. 또는 구성에 중단된 플로우 제어가 있을 수 있습니다. ■ 채트 스크립트에 오류가 발생했을 수 있습니다. 이 경우 표 7–5를 참조하십시오.
`pppd debug` 출력에 LCP가 시작되지만 상위 레벨 프로토콜이 실패하거나 CRC 오류를 보인다고 표시됩니다.	ACCM(비동기 제어 문자 맵)이 잘못 설정되었습니다.	`default-async` 옵션을 사용하여 ACCM을 표준 기본값인 FFFFFFFF로 설정합니다. 먼저, 명령줄에서 `default-async`를 `pppd`에 대한 옵션으로 사용해 봅니다. 문제가 해결되면 `default-async`를 `/etc/ppp/options` 또는 `/etc/ppp/peers/`*peer-name*에 추가합니다(call 옵션 뒤).
`pppd debug` 출력에 IPCP가 시작되지만 즉시 종료된다고 표시됩니다.	IP 주소가 잘못 구성되었을 수 있습니다.	1. 채트 스크립트에 잘못된 IP 주소가 있는지 확인합니다. 2. 채트 스크립트가 올바른 경우 피어에 대한 디버그 로그를 요청하고 피어 로그에서 IP 주소를 확인합니다.
링크의 성능이 현저히 떨어집니다.	모뎀이 잘못 구성되었을 수 있습니다(플로우 제어 구성 오류, 모뎀 설정 오류 및 잘못 구성된 DTE 속도).	모뎀 구성을 확인합니다. 필요한 경우 구성을 조정합니다.

▼ PPP 구성을 사용하여 문제를 진단하는 방법

일부 PPP 문제는 PPP 구성 파일의 문제 때문에 발생할 수 있습니다. 다음 절차에서는 일반적인 구성 문제를 격리하고 해결하는 방법을 보여줍니다.

1 로컬 시스템에서 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 원격 피어를 호출합니다. 그런 다음 디버깅 기능을 사용으로 설정합니다.

```
% pppd debug call peer-name
```

3 결과 로그에서 구성 문제를 확인합니다. 자세한 내용은 100 페이지 "일반적인 PPP 구성 문제"를 참조하십시오.

일반적인 PPP 구성 문제

다음 표에는 99 페이지 "PPP 구성을 사용하여 문제를 진단하는 방법" 절차의 로그 출력과 관련된 증상이 설명되어 있습니다.

표 7–4 일반적인 PPP 구성 문제

증상	문제점	해결 방법
pppd debug 출력에 Could not determine remote IP address라는 오류 메시지가 포함되어 있습니다.	/etc/ppp/peers/*peer-name* 파일에 피어에 대한 IP 주소가 없습니다. 피어가 링크 협상 중 IP 주소를 제공하지 않습니다.	pppd 명령줄 또는 /etc/ppp/peers/*peer-name*에서 다음 형식을 사용하여 피어에 대한 IP 주소를 제공합니다. :10.0.0.10
pppd debug 출력에 CCP 데이터 압축이 실패했다고 표시됩니다. 또한 출력에 링크가 삭제되었다고 표시됩니다.	피어의 PPP 압축 구성에서 충돌이 발생했을 수 있습니다.	피어 중 하나에서 noccp 옵션을 /etc/ppp/options에 추가하여 CCP 압축을 사용 안함으로 설정합니다.

▼ 모뎀 문제를 진단하는 방법

모뎀은 다이얼 업 링크의 주요 문제 영역이 될 수 있습니다. 흔히 피어로부터 응답이 없을 때 모뎀 구성에 문제가 있다는 사실을 알 수 있습니다. 그러나 링크 문제가 정말로 모뎀 구성 문제의 결과인지는 확인하기가 어려울 수 있습니다.

모뎀 제조업체의 설명서 및 웹 사이트에 특정 장비 문제에 대한 해결 방법이 포함되어 있습니다. 다음 절차는 잘못된 모뎀 구성으로 인해 링크 문제가 발생했는지 여부를 확인하는 데 도움이 됩니다.

1. **94 페이지 "PPP 디버깅을 켜는 방법"에 설명된 대로 디버깅을 켠 채 피어를 호출합니다.**

2. **결과 /var/log/pppdebug 로그를 표시하여 잘못된 모뎀 구성을 확인합니다.**

3. **ping을 사용하여 다양한 크기의 패킷을 링크를 통해 보냅니다.**

   ping에 대한 자세한 내용은 ping(1M) 매뉴얼 페이지를 참조하십시오.

   작은 패킷을 받았지만 더 큰 패킷을 삭제한 경우에는 모뎀 문제가 표시됩니다.

4. **sppp0 인터페이스에서 오류를 확인합니다.**

```
% netstat -ni
Name  Mtu  Net/Dest    Address       Ipkts    Ierrs Opkts    Oerrs Collis Queue
lo0   8232 127.0.0.0   127.0.0.1     826808   0     826808   0     0      0
hme0  1500 172.21.0.0  172.21.3.228  13800032 0     1648464  0     0      0
sppp0 1500 10.0.0.2    10.0.0.1      210      0     128      0     0      0
```

   시간이 지남에 따라 인터페이스 오류가 늘어나면 모뎀 구성에 문제가 있을 수 있습니다.

일반 오류 결과 /var/log/pppdebug 로그를 표시할 때 출력에 다음 증상이 나타나면 모뎀 구성이 잘못된 것일 수 있습니다. 로컬 시스템은 피어를 들을 수 있지만 피어는 로컬 시스템을 들을 수 없습니다.

- 피어로부터 아무 "recvd" 메시지도 받지 못했습니다.
- 출력에 피어로부터 받은 LCP 메시지가 포함되어 있지만 로컬 시스템이 보낸 too many LCP Configure Requests 메시지와 함께 링크가 실패합니다.
- 링크가 SIGHUP 신호와 함께 종료됩니다.

▼ 채트 스크립트에 대한 디버깅 정보를 가져오는 방법

chat에서 디버깅 정보를 가져오기 위한 다음 절차와 일반적인 문제를 해결하는 방법에 대한 제안 사항을 사용하십시오. 자세한 내용은 101 페이지 "일반적인 채트 스크립트 문제"를 참조하십시오.

1. **다이얼 아웃 시스템에서 관리자로 전환합니다.**
   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **호출할 피어에 대한 /etc/ppp/peers/*peer-name* 파일을 편집합니다.**

3. **connect 옵션에 지정되어 있는 chat 명령에 대한 인수로 -v를 추가합니다.**

   ```
   connect "/usr/bin/chat -v -f /etc/ppp/chat-script-name"
   ```

4. **/etc/ppp/connect-errors 파일에서 채트 스크립트 오류를 봅니다.**
   다음은 chat에 대해 발생하는 주요 오류입니다.

   ```
   Oct 31 08:57:13 deino chat[107294]: [ID 702911 local2.info] expect (CONNECT)
   Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] alarm
   Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] Failed
   ```

   예에서는 (CONNECT) 문자열을 기다리는 동안 시간이 초과되었음을 보여줍니다. chat가 실패하면 pppd로부터 다음 메시지가 반환됩니다.

   ```
   Connect script failed
   ```

일반적인 채트 스크립트 문제

채트 스크립트는 다이얼 업 링크에 대해 문제가 발생하기 쉬운 영역입니다. 다음 표에는 일반적인 채트 스크립트 오류와 오류를 해결하기 위한 제안 사항이 나와 있습니다. 절차 정보는 101 페이지 "채트 스크립트에 대한 디버깅 정보를 가져오는 방법"을 참조하십시오.

표 7–5 일반적인 채트 스크립트 문제

증상	문제점	해결 방법
`pppd debug` 출력에 `Connect script failed`가 포함되어 있습니다.	채트 스크립트가 사용자 이름 및 암호를 제공합니다. `ogin:` *user-name* `ssword:` *password* 그러나 연결하려고 했던 피어가 이 정보를 요청하는 메시지를 표시하지 않습니다.	1. 채트 스크립트에서 로그인 및 암호를 삭제합니다. 2. 피어를 다시 호출해 봅니다. 3. 계속 메시지가 반환되면 ISP에 문의합니다. ISP에 올바른 로그인 절차가 무엇인지 문의합니다.

`/usr/bin/chat -v` 로그에 `"expect (login:)" alarm read timed out`이 포함되어 있습니다.	채트 스크립트가 사용자 이름 및 암호를 제공합니다.
	`ogin: pppuser`
	`ssword: \q\U`
	그러나 연결하려고 하는 피어가 이 정보를 요청하는 메시지를 표시하지 않습니다.
		1. 채트 스크립트에서 로그인 및 암호를 삭제합니다.
		2. 피어를 다시 호출해 봅니다.
		3. 계속 메시지가 반환되면 ISP에 문의합니다. ISP에 올바른 로그인 절차가 무엇인지 문의합니다.

`pppd debug` 출력에 `possibly looped-back`이 포함되어 있습니다.	로컬 시스템 또는 해당 피어가 명령줄에서 정지되어 있으며 PPP를 실행하고 있지 않습니다. 잘못 구성된 로그인 이름 및 암호가 채트 스크립트에 있습니다.	1. 채트 스크립트에서 로그인 및 암호를 삭제합니다. 2. 피어를 다시 호출해 봅니다. 3. 계속 메시지가 반환되면 ISP에 문의합니다. 올바른 로그인 절차가 무엇인지 문의합니다.
`pppd debug` 출력에 LCP가 활성화되지만 링크가 곧 종료된다고 표시됩니다.	채트 스크립트의 암호가 잘못되었을 수 있습니다.	1. 로컬 시스템의 암호가 올바른지 확인합니다. 2. 채트 스크립트에서 암호를 확인합니다. 잘못된 경우 암호를 수정합니다. 3. 피어를 다시 호출해 봅니다. 4. 계속 메시지가 반환되면 ISP에 문의합니다. ISP에 올바른 로그인 절차가 무엇인지 문의합니다.

피어로부터의 텍스트가 틸드(~)로 시작합니다.	채트 스크립트가 사용자 이름 및 암호를 제공합니다.
	`ogin: pppuser`
	`ssword: \q\U`
	그러나 연결하려고 하는 피어가 이 정보를 요청하는 메시지를 표시하지 않습니다.
		1. 채트 스크립트에서 로그인 및 암호를 삭제합니다.
		2. 피어를 다시 호출해 봅니다.
		3. 계속 메시지가 반환되면 ISP에 문의합니다. 올바른 로그인 절차를 요청합니다.

표 7–5 일반적인 채트 스크립트 문제 *(계속)*

증상	문제점	해결 방법
모뎀이 정지됩니다.	채트 스크립트에 로컬 시스템이 피어로부터 CONNECT 메시지를 기다리게 만드는 다음 행이 포함되어 있습니다. `CONNECT ”`	채트 스크립트가 피어로부터 CONNECT를 기다리게 만들려면 다음 행을 사용합니다. `CONNECT \c` ~\c로 채트 스크립트를 끝냅니다.
pppd debug 출력에 LCP: timeout sending Config-Requests가 포함되어 있습니다.	채트 스크립트에 로컬 시스템이 피어로부터 CONNECT 메시지를 기다리게 만드는 다음 행이 포함되어 있습니다. `CONNECT ”`	채트 스크립트가 피어로부터 CONNECT를 기다리게 만들려면 다음 행을 사용합니다. `CONNECT \c` ~\c로 채트 스크립트를 끝냅니다.
pppd debug 출력에 Serial link is not 8-bit clean이 포함되어 있습니다.	채트 스크립트에 로컬 시스템이 피어로부터 CONNECT 메시지를 기다리게 만드는 다음 행이 포함되어 있습니다. `CONNECT ”`	채트 스크립트가 피어로부터 CONNECT를 기다리게 만들려면 다음 행을 사용합니다. `CONNECT \c` ~\c로 채트 스크립트를 끝냅니다.
pppd debug 출력에 Loopback detected가 포함되어 있습니다.	채트 스크립트에 로컬 시스템이 피어로부터 CONNECT 메시지를 기다리게 만드는 다음 행이 포함되어 있습니다. `CONNECT ”`	채트 스크립트가 피어로부터 CONNECT를 기다리게 만들려면 다음 행을 사용합니다. `CONNECT \c` ~\c로 채트 스크립트를 끝냅니다.
pppd debug 출력에 SIGHUP가 포함되어 있습니다.	채트 스크립트에 로컬 시스템이 피어로부터 CONNECT 메시지를 기다리게 만드는 다음 행이 포함되어 있습니다. `CONNECT ”`	채트 스크립트가 피어로부터 CONNECT를 기다리게 만들려면 다음 행을 사용합니다. `CONNECT \c` ~\c로 채트 스크립트를 끝냅니다.

▼ 직렬 회선 속도 문제를 진단하고 해결하는 방법

속도 설정이 충돌하여 다이얼 인 서버에 문제가 발생할 수 있습니다. 다음 절차는 링크 문제의 원인을 충돌하는 직렬 회선 속도로 격리하는 데 도움이 됩니다.

다음 동작으로 인해 속도 문제가 발생합니다.

- /bin/login과 같은 프로그램을 통해 PPP를 호출하고 회선의 속도를 지정했습니다.
- mgetty에서 PPP를 시작하고 실수로 비트 속도를 제공했습니다.

pppd는 회선에 대해 원래 설정된 속도를 /bin/login 또는 mgetty에 의해 설정된 속도로 변경합니다. 결과적으로 회선에 문제가 발생합니다.

1. **다이얼 인 서버에 로그인합니다. 디버깅을 사용으로 설정한 채 피어를 호출합니다.**
   지침이 필요하면 94 페이지 "PPP 디버깅을 켜는 방법"을 참조하십시오.

2. **결과 /var/log/pppdebug 로그를 표시합니다.**
   출력에서 다음 메시지를 확인합니다.

   ```
   LCP too many configure requests
   ```

   이 메시지는 PPP에 대해 구성된 직렬 회선의 속도가 충돌했을 수 있음을 나타냅니다.

3. **/bin/login과 같은 프로그램을 통해 PPP가 호출되었는지 여부와 설정된 회선 속도를 확인합니다.**
   그런 경우 pppd가 원래 구성된 회선 속도를 /bin/login에 지정된 속도로 변경합니다.

4. **사용자가 mgetty 명령에서 PPP를 시작하고 실수로 비트 속도를 지정했는지 여부를 확인합니다.**
   이 작업도 직렬 회선 속도가 충돌하게 만듭니다.

5. **충돌하는 직렬 회선 속도 문제를 다음과 같이 해결합니다.**

   a. **모뎀에서 DTE 속도를 고정합니다.**

   b. **자동 변조를 사용하지 않습니다.**

   c. **구성 후에 회선 속도를 변경하지 않습니다.**

▼ PPPoE에 대한 진단 정보를 가져오는 방법

PPP 및 표준 UNIX 유틸리티를 사용하여 PPPoE 문제를 식별할 수 있습니다. PPPoE가 링크 문제의 원인으로 의심되는 경우 다음 진단 도구를 사용하여 문제 해결 정보를 얻으십시오.

1. **PPPoE 터널을 실행하는 시스템(PPPoE 클라이언트 또는 PPPoE 액세스 서버)에서 수퍼유저가 됩니다.**

2. **94 페이지 "PPP 디버깅을 켜는 방법" 절차에 설명된 대로 디버깅을 켭니다.**

3. **로그 파일 /var/log/pppdebug의 내용을 봅니다.**
   다음 예에서는 PPPoE 터널과의 링크에 대해 생성된 로그 파일의 일부분을 보여줍니다.

```
Sep  6 16:28:45 enyo pppd[100563]: [ID 702911 daemon.info] Plugin
  pppoe.so loaded.
Sep  6 16:28:45 enyo pppd[100563]: [ID 860527 daemon.notice] pppd
  2.4.0b1 (Sun Microsystems, Inc.,
Sep  5 2001 10:42:05) started by troot, uid 0
```

```
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] connect option:
   '/usr/lib/inet/pppoec
-v hme0' started (pid 100564)
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Serial connection established.
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Using interface sppp0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.notice] Connect: sppp0
   <--> /dev/sppptun
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/pap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/chap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] sent
  [LCP ConfReq id=0xef <mru 1492>
asyncmap 0x0 <magic 0x77d3e953><pcomp><acomp>
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] rcvd
  [LCP ConfReq id=0x2a <mru 1402>
asyncmap 0x0 <magic 0x9985f048><pcomp><acomp
```

디버깅 출력이 문제를 격리하는 데 도움이 되지 않는 경우 이 절차를 계속하십시오.

4 PPPoE에서 진단 메시지를 가져옵니다.

```
# pppd connect "/usr/lib/inet/pppoec -v interface-name"
```

pppoec는 진단 정보를 stderr로 보냅니다. 전면에서 pppd를 실행하면 화면에 출력이 나타납니다. 배경에서 pppd를 실행하면 출력이 /etc/ppp/connect-errors로 전송됩니다.

다음 예에서는 PPPoE 터널이 협상되면서 생성되는 메시지를 보여줍니다.

```
Connect option: '/usr/lib/inet/pppoec -v hme0' started (pid 100564)
/usr/lib/inet/pppoec: PPPoE Event Open (1) in state Dead (0): action SendPADI (2)
/usr/lib/inet/pppoec: Sending PADI to ff:ff:ff:ff:ff:ff: 18 bytes
/usr/lib/inet/pppoec: PPPoE State change Dead (0) -> InitSent (1)
/usr/lib/inet/pppoec: Received Active Discovery Offer from 8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADO+ (5) in state InitSent (1): action SendPADR+ (5)
/usr/lib/inet/pppoec: Sending PADR to 8:0:20:cd:c1:2: 22 bytes
/usr/lib/inet/pppoec: PPPoE State change InitSent (1) -> ReqSent (3)
/usr/lib/inet/pppoec: Received Active Discovery Session-confirmation from
   8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADS (7) in state ReqSent (3): action Open (7)
/usr/lib/inet/pppoec: Connection open; session 0002 on hme0:pppoe
/usr/lib/inet/pppoec: PPPoE State change ReqSent (3) -> Convers (4)
/usr/lib/inet/pppoec: connected
```

진단 메시지가 문제를 격리하는 데 도움이 되지 않는 경우 이 절차를 계속하십시오.

5 snoop을 실행합니다. 그런 다음 파일에 추적을 저장합니다.

snoop에 대한 자세한 내용은 snoop(1M) 매뉴얼 페이지를 참조하십시오.

```
# snoop -o pppoe-trace-file
```

6 snoop 추적 파일을 봅니다.

```
# snoop -i pppoe-trace-file -v pppoe

ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 1 arrived at 6:35:2.77
```

```
ETHER: Packet size = 32 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source      = 8:0:20:78:f3:7c, Sun
ETHER: Ethertype = 8863 (PPPoE Discovery)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 9 (Active Discovery Initiation)
PPPoE: Session Id = 0
PPPoE: Length = 12 bytes
PPPoE:
PPPoE: ----- Service-Name -----
PPPoE: Tag Type = 257
PPPoE: Tag Length = 0 bytes
PPPoE:
PPPoE: ----- Host-Uniq -----
PPPoE: Tag Type = 259
PPPoE: Tag Length = 4 bytes
PPPoE: Data = Ox00000002
PPPoE:
.
.
.
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 5 arrived at 6:35:2.87
ETHER: Packet size = 60 bytes
ETHER: Destination = 8:0:20:78:f3:7c, Sun)
ETHER: Source      = 0:2:fd:39:7f:7,
ETHER: Ethertype = 8864 (PPPoE Session)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 0 (PPPoE Session)
PPPoE: Session Id = 24383
PPPoE: Length = 20 bytes
PPPoE:
PPP: ----- Point-to-Point Protocol -----
PPP:
PPP-LCP: ----- Link Control Protocol -----
PPP-LCP:
PPP-LCP: Code = 1 (Configure Request)
PPP-LCP: Identifier = 80
PPP-LCP: Length = 18
```

전용 회선 문제 해결

전용 회선에 가장 흔히 발생하는 문제는 성능 저하입니다. 대부분의 경우 전화 회사에 문의하여 문제를 해결해야 합니다.

표 7–6 일반적인 전용 회선 문제

증상	문제점	해결 방법
링크가 시작되지 않습니다.	CSU 양극성 위반(CSU BPV)이 원인일 수 있습니다. 링크의 한쪽 끝은 AMI 회선용으로 설정되어 있고, 다른 쪽 끝은 ESF Bit 8 제로 대치(B8Zs)로 설정되어 있습니다.	미국 또는 캐나다에 있는 경우 CSU/DSU 메뉴에서 직접 이 문제를 해결할 수 있습니다. 자세한 내용은 CSU/DSU 제조업체의 설명서를 참조하십시오. 다른 위치에서는 공급자가 CSU BPV 문제를 해결해야 할 수 있습니다.
링크의 성능이 저하되었습니다.	링크에 지속 트래픽이 있을 때 `pppd debug` 출력에 CRC 오류가 표시됩니다. 전화 회사와 사용 중인 네트워크 간의 잘못된 구성으로 인해 회선에 클록킹 문제가 있을 수 있습니다.	전화 회사에 문의하여 "루프 클록킹"이 사용되고 있는지 확인합니다. 구조화되지 않은 일부 전용 회선에서는 클록킹을 제공해야 할 수 있습니다. 북미 사용자는 루프 클록킹을 사용해야 합니다.

인증 문제 진단 및 해결

다음 표에는 일반적인 인증 문제에 대한 해결 방법이 설명되어 있습니다.

표 7–7 일반적인 인증 문제

증상	문제점	해결 방법
`pppd debug` 출력에 `Peer is not authorized to use remote address` *address*(피어에게 해당 원격 주소를 사용할 권한이 부여되지 않음) 메시지가 표시됩니다.	PAP 인증을 사용하고 있는데 원격 피어의 IP 주소가 `/etc/ppp/pap-secrets` 파일에 없습니다.	`/etc/ppp/pap-secrets` 파일에서 피어에 대한 항목 다음에 별표(*)를 추가합니다.
`pppd debug` 출력에 LCP가 시작되지만 곧 종료된다고 표시됩니다.	암호가 특정 보안 프로토콜에 대한 데이터베이스에서 잘못되었을 수 있습니다.	`/etc/ppp/pap-secrets` 또는 `/etc/ppp/chap-secrets` 파일에서 피어의 암호를 확인합니다.

◆ ◆ ◆ 8 장

8 Solaris PPP 4.0(참조)

이 장에서는 Solaris PPP 4.0에 대한 자세한 개념 정보를 제공합니다. 항목은 다음과 같습니다.

파일 및 명령줄에서 PPP 옵션 사용

Solaris PPP 4.0에는 PPP 구성을 정의하는 데 사용할 수 있는 방대한 옵션 세트가 포함되어 있습니다. 이러한 옵션은 PPP 구성 파일 또는 명령줄에서 사용하거나 파일 및 명령줄 옵션을 조합하여 사용합니다. 이 절에는 PPP 옵션을 구성 파일에서 사용하거나 PPP 명령에 대한 인수로 사용하는 방법에 대한 자세한 내용이 포함되어 있습니다.

PPP 옵션을 정의하는 위치

Solaris PPP 4.0 구성은 매우 유연합니다. PPP 옵션은 다음 위치에서 정의할 수 있습니다.

- PPP 구성 파일
- 명령줄에서 실행되는 PPP 명령
- 두 위치의 조합

다음 표에는 PPP 구성 파일 및 명령이 나열되어 있습니다.

표 8–1 PPP 구성 파일 및 명령 요약

파일 또는 명령	설명	정보
`/etc/ppp/options`	시스템에 있는 모든 PPP 링크에 기본적으로 적용되는 특징(예: 피어가 자신을 인증할 것을 시스템이 요구하는지 여부)이 포함된 파일입니다. 이 파일이 없으면 비루트 사용자가 PPP를 사용할 수 없습니다.	113 페이지 "`/etc/ppp/options` 구성 파일"
`/etc/ppp/options.`*ttyname*	직렬 포트 *ttyname*을 통한 모든 통신의 특징을 기술하는 파일입니다.	115 페이지 "`/etc/ppp/options.`*ttyname* 구성 파일"
`/etc/ppp/peers`	다이얼 아웃 시스템이 연결하는 피어에 대한 정보가 일반적으로 포함되어 있는 디렉토리입니다. 이 디렉토리에 있는 파일은 `pppd` 명령의 `call` 옵션에 사용됩니다.	117 페이지 "다이얼 인 서버와의 통신을 위한 정보 지정"
`/etc/ppp/peers/`*peer-name*	원격 피어 *peer-name*의 특징이 포함된 파일입니다. 일반적인 특징에는 원격 피어의 전화 번호 및 피어와 링크를 협상하기 위한 채트 스크립트가 있습니다.	118 페이지 "`/etc/ppp/peers/`*peer-name* 파일"
`/etc/ppp/pap-secrets`	PAP(암호 인증 프로토콜) 인증에 필요한 보안 자격 증명이 포함된 파일입니다.	130 페이지 "`/etc/ppp/pap-secrets` 파일"
`/etc/ppp/chap-secrets`	CHAP(Challenge-Handshake 인증 프로토콜) 인증에 필요한 보안 자격 증명이 포함된 파일입니다.	133 페이지 "`/etc/ppp/chap-secrets` 파일"
`~/.ppprc`	PPP 사용자의 홈 디렉토리에 있는 파일로, 다이얼 인 서버에 가장 자주 사용됩니다. 이 파일에는 각 사용자 구성과 관련된 정보가 포함되어 있습니다.	117 페이지 "다이얼 인 서버에서 `$HOME/.ppprc` 구성"
`pppd` **옵션**	PPP 링크를 시작하고 해당 특징을 기술하기 위한 명령 및 옵션입니다.	110 페이지 "PPP 옵션이 처리되는 방법"

PPP 파일에 대한 자세한 내용은 pppd(1M) 매뉴얼 페이지를 참조하십시오. pppd(1M)에는 `pppd` 명령에 사용할 수 있는 모든 옵션에 대한 포괄적인 설명도 포함되어 있습니다. 모든 PPP 구성 파일에 대한 샘플 템플리트는 `/etc/ppp`에 제공되어 있습니다.

PPP 옵션이 처리되는 방법

1. `pppd` 데몬이 다음의 구문을 분석합니다.

모든 Solaris PPP 4.0 작업은 pppd 데몬에 의해 처리되며, 이 데몬은 사용자가 pppd 명령을 실행할 때 시작됩니다. 사용자가 원격 피어를 호출하면 다음이 발생합니다.

- /etc/ppp/options
- $HOME/.ppprc
- /etc/ppp/options 및 $HOME/.ppprc에서 file 또는 call 옵션으로 열리는 모든 파일

2. pppd가 명령줄을 스캔하여 사용 중인 장치를 확인합니다. 데몬은 발견하는 옵션을 아직 해석하지 않습니다.
3. pppd가 다음 조건을 사용하여 직렬 장치를 검색하려고 합니다.
   - 직렬 장치가 명령줄 또는 이전에 처리된 구성 파일에서 지정된 경우 pppd는 해당 장치의 이름을 사용합니다.
   - 명명된 직렬 장치가 없는 경우 pppd가 명령줄에서 notty, pty 또는 socket 옵션을 검색합니다. 이러한 옵션 중 하나가 지정된 경우에는 pppd가 장치 이름이 없다고 가정합니다.
   - 그렇지 않고 표준 입력이 tty에 연결되어 있음을 pppd가 발견하면 해당 tty의 이름이 사용됩니다.
   - pppd가 여전히 직렬 장치를 찾을 수 없는 경우 pppd는 연결을 종료하고 오류를 발생시킵니다.
4. 그런 다음 pppd가 /etc/ppp/options.*ttyname* 파일이 있는지 확인합니다. 해당 파일이 발견되면 pppd가 파일의 구문을 분석합니다.
5. pppd가 명령줄에서 모든 옵션을 처리합니다.
6. pppd가 링크를 설정하기 위해 LCP(링크 제어 프로토콜)를 협상합니다.
7. (옵션) 인증이 필요한 경우 pppd가 반대쪽 피어를 인증하기 위해 /etc/ppp/pap-secrets 또는 /etc/ppp/chap-secrets를 읽습니다.

/etc/ppp/peers/*peer-name* 파일은 pppd 데몬이 명령줄 또는 기타 구성 파일에서 call *peer-name* 옵션을 발견할 때 읽습니다.

PPP 구성 파일 권한의 작동 방식

Solaris PPP 4.0 구성에는 **권한**이라는 개념이 포함되어 있습니다. 권한은 특히 둘 이상의 위치에서 동일한 옵션이 호출될 때 구성 옵션의 우선 순위를 결정합니다. 권한 있는 소스에서 호출된 옵션이 권한 없는 소스에서 호출된 동일한 옵션보다 우선적으로 사용됩니다.

사용자 권한

권한 있는 사용자는 UID가 0인 수퍼 유저(root)뿐입니다. 다른 모든 사용자에게는 권한이 없습니다.

파일 권한

다음 구성 파일에 대한 권한은 소유권에 관계없이 부여됩니다.

- /etc/ppp/options
- /etc/ppp/options.*ttyname*
- /etc/ppp/peers/*peer-name*

$HOME/.ppprc 파일은 사용자가 소유합니다. $HOME/.ppprc 및 명령줄에서 읽는 옵션에 대한 권한은 pppd를 호출하는 사용자가 root인 경우에만 부여됩니다.

file 옵션 뒤에 오는 인수의 경우 권한이 부여됩니다.

옵션 권한의 영향

일부 옵션의 경우 호출 사용자 또는 소스에 권한이 있어야 작동합니다. 명령줄에서 호출되는 옵션에는 pppd 명령을 실행하는 사용자의 권한이 지정됩니다. pppd를 호출하는 사용자가 root여야 이러한 옵션에 권한이 부여됩니다.

옵션	상태	설명
도메인	권한이 부여됨	사용하려면 권한이 필요합니다.
linkname	권한이 부여됨	사용하려면 권한이 필요합니다.
noauth	권한이 부여됨	사용하려면 권한이 필요합니다.
nopam	권한이 부여됨	사용하려면 권한이 필요합니다.
pam	권한이 부여됨	사용하려면 권한이 필요합니다.
plugin	권한이 부여됨	사용하려면 권한이 필요합니다.
privgroup	권한이 부여됨	사용하려면 권한이 필요합니다.
allow-ip *addresses*	권한이 부여됨	사용하려면 권한이 필요합니다.
name *hostname*	권한이 부여됨	사용하려면 권한이 필요합니다.
plink	권한이 부여됨	사용하려면 권한이 필요합니다.
noplink	권한이 부여됨	사용하려면 권한이 필요합니다.
plumbed	권한이 부여됨	사용하려면 권한이 필요합니다.
proxyarp	noproxyarp가 지정된 경우 권한이 부여됨	권한 없는 사용자가 대체할 수 없습니다.
defaultroute	nodefaultroute가 권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한 없는 사용자가 대체할 수 없습니다.

옵션	상태	설명
disconnect	권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한 없는 사용자가 대체할 수 없습니다.
bsdcomp	권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한이 없는 사용자는 권한이 있는 사용자가 지정한 것보다 큰 코드 크기를 지정할 수 없습니다.
deflate	권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한이 없는 사용자는 권한이 있는 사용자가 지정한 것보다 큰 코드 크기를 지정할 수 없습니다.
connect	권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한이 없는 사용자가 대체할 수 없습니다.
init	권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한이 없는 사용자가 대체할 수 없습니다.
pty	권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한이 없는 사용자가 대체할 수 없습니다.
welcome	권한이 있는 파일에 설정되거나 권한 있는 사용자에 의해 설정되는 경우 권한이 부여됨	권한이 없는 사용자가 대체할 수 없습니다.
ttyname	권한이 있는 파일에 설정되는 경우 권한이 부여됨	pppd를 호출하는 사용자에 관계없이 루트 권한으로 열립니다.
	권한이 없는 파일에 설정되는 경우 권한이 부여되지 않음	pppd를 호출하는 사용자의 권한으로 열립니다.

/etc/ppp/options 구성 파일

/etc/ppp/options 파일을 사용하여 로컬 시스템에 있는 모든 PPP 통신에 대한 전역 옵션을 정의할 수 있습니다. /etc/ppp/options는 권한이 있는 파일입니다. /etc/ppp/options는 루트가 소유해야 합니다. 그러나 pppd에 의해 이 규칙이 강제로 적용되는 것은 아닙니다. /etc/ppp/options에 정의하는 옵션은 다른 모든 파일 및 명령줄에 있는 동일한 옵션의 정의보다 우선적으로 사용됩니다.

/etc/ppp/options에서 일반적으로 사용할 수 있는 옵션은 다음과 같습니다.

- **lock** – UUCP 스타일의 파일 잠금을 사용으로 설정합니다.
- **noauth** – 시스템이 호출자를 인증하지 않음을 나타냅니다.

주 – Solaris PPP 4.0 소프트웨어에는 기본 /etc/ppp/options 파일이 포함되어 있지 않습니다. pppd를 작동하는 데에는 /etc/ppp/options 파일이 필요하지 않습니다. 시스템에 /etc/ppp/options 파일이 없으면 root만 해당 시스템에서 pppd를 실행할 수 있습니다.

텍스트 편집기를 사용하여 /etc/ppp/options를 만들어야 합니다(52 페이지 "직렬 회선을 통해 통신을 정의하는 방법" 참조). 시스템에 전역 옵션이 필요하지 않으면 빈 /etc/ppp/options 파일을 만들 수 있습니다. 그러면 root 사용자와 일반 사용자가 모두 로컬 시스템에서 pppd를 실행할 수 있게 됩니다.

/etc/ppp/options.tmpl 템플리트

/etc/ppp/options.tmpl에는 /etc/ppp/options 파일에 대한 유용한 설명과 전역 /etc/ppp/options 파일에 대한 세 가지 일반적인 옵션이 포함되어 있습니다.

```
lock
nodefaultroute
noproxyarp
```

옵션	정의
lock	UUCP 스타일의 파일 잠금을 사용으로 설정합니다.
nodefaultroute	기본 경로가 정의되어 있지 않음을 지정합니다.
noproxyarp	proxyarp를 허용하지 않습니다.

/etc/ppp/options.tmpl을 전역 옵션 파일로 사용하려면 /etc/ppp/options.tmpl의 이름을 /etc/ppp/options로 바꾼 다음 사이트의 필요에 따라 파일 내용을 수정하십시오.

/etc/ppp/options 파일의 예를 찾을 수 있는 위치

/etc/ppp/options 파일의 예를 찾으려면 다음을 참조하십시오.

- 다이얼 아웃 시스템의 경우 52 페이지 "직렬 회선을 통해 통신을 정의하는 방법"을 참조하십시오.
- 다이얼 인 서버의 경우 59 페이지 "직렬 회선을 통해 통신을 정의하는 방법(다이얼 인 서버)"을 참조하십시오.
- 다이얼 인 서버에서의 PAP 지원의 경우 73 페이지 "PPP 구성 파일에 PAP 지원을 추가하는 방법(다이얼 인 서버)"을 참조하십시오.
- 다이얼 아웃 시스템에서의 PAP 지원의 경우 76 페이지 "PPP 구성 파일에 PAP 지원을 추가하는 방법(다이얼 아웃 시스템)"을 참조하십시오.
- 다이얼 인 서버에서의 CHAP 지원의 경우 80 페이지 "PPP 구성 파일에 CHAP 지원을 추가하는 방법(다이얼 인 서버)"을 참조하십시오.

/etc/ppp/options.*ttyname* 구성 파일

/etc/ppp/options.*ttyname* 파일에서 직렬 회선에 대해 통신의 특징을 구성할 수 있습니다. /etc/ppp/options.*ttyname*은 모든 기존 /etc/ppp/options 및 기존 $HOME/.pprc 파일의 구문을 분석한 후에 pppd가 읽는 권한이 있는 파일입니다. 그렇지 않은 경우 pppd는 /etc/ppp/options.*ttyname*을 /etc/ppp/options의 구문을 분석한 후에 읽습니다.

*ttyname*은 다이얼 업 링크와 전용 회선 링크 모두에 사용됩니다. *ttyname*은 모뎀 또는 ISDN TA가 연결될 수 있는 cua/a 또는 cua/b와 같은 시스템의 특정 직렬 포트를 나타냅니다.

/etc/ppp/options.*ttyname* 파일의 이름을 지정할 때는 장치 이름에 있는 슬래시(/)를 점(.)으로 바꿔야 합니다. 예를 들어, cua/b 장치의 options 파일은 이름을 /etc/ppp/options.cua.b로 지정해야 합니다.

주 – Solaris PPP 4.0의 경우 올바르게 작동하는 데 /etc/ppp/options.*ttyname* 파일을 필요로 하지 않습니다. 서버에는 PPP용 직렬 회선이 하나만 있을 수 있습니다. 또한 서버에는 옵션이 거의 필요하지 않습니다. 이러한 경우에는 다른 구성 파일 또는 명령줄에서 필요한 모든 옵션을 지정할 수 있습니다.

다이얼 인 서버에서 /etc/ppp/options.*ttyname* 사용

다이얼 업 링크의 경우 모뎀이 연결된 다이얼 인 서버에서 모든 직렬 포트에 대해 개별 /etc/ppp/options.*ttyname* 파일을 만들 수 있습니다. 일반적인 옵션은 다음과 같습니다.

- 다이얼 인 서버에 필요한 IP 주소

  직렬 포트 *ttyname*의 수신 호출자가 특정 IP 주소를 사용해야 하는 경우 이 옵션을 설정합니다. 주소 공간에는 잠재적 호출자 수에 비해 PPP용으로 사용 가능한 IP 주소가 제한되어 있을 수 있습니다. 이 경우 다이얼 인 서버에서 PPP에 사용되는 각 직렬 인터페이스에 IP 주소를 지정해 보십시오. 이렇게 하면 PPP에 동적 주소 지정이 구현됩니다.

- asyncmap *map-value*

  asyncmap 옵션은 특정 모뎀 또는 ISDN TA로 직렬 회선을 통해 받을 수 없는 제어 문자를 매핑합니다. xonxoff 옵션을 사용하면 pppd가 asyncmap 0xa0000을 자동으로 설정합니다.

  *map-value*는 문제가 되는 제어 문자를 16진수 형식으로 나타냅니다.

- init "chat -U -f /etc/ppp/mychat"

  init 옵션은 chat - U 명령의 정보를 사용하여 직렬 회선을 통해 통신을 초기화하도록 모뎀에 지시합니다. 모뎀은 /etc/ppp/mychat 파일의 채트 문자열을 사용합니다.

- pppd(1m) 매뉴얼 페이지에 나열되어 있는 보안 매개변수

다이얼 아웃 시스템에서 /etc/ppp/options.*ttyname* 사용

다이얼 아웃 시스템의 경우 모뎀에 연결된 직렬 포트에 대해 /etc/ppp/options.*ttyname* 파일을 만들거나 /etc/ppp/options.*ttyname*을 사용하지 않도록 선택할 수 있습니다.

주 – Solaris PPP 4.0의 경우 올바르게 작동하는 데 /etc/ppp/options.*ttyname* 파일을 필요로 하지 않습니다. 다이얼 아웃 시스템에는 PPP용 직렬 회선이 하나만 있을 수 있습니다. 또한 다이얼 아웃 시스템에는 옵션이 거의 필요하지 않습니다. 다른 구성 파일 또는 명령줄에서 필요한 모든 옵션을 지정할 수 있습니다.

---

options.ttya.tmpl 템플리트 파일

/etc/ppp/options.ttya.tmpl 파일에는 /etc/ppp/options.*tty-name* 파일에 대한 유용한 설명이 포함되어 있습니다. 템플리트에는 /etc/ppp/options.*tty-name* 파일에 대한 세 가지 일반적인 옵션이 포함되어 있습니다.

```
38400
asyncmap 0xa0000
:192.168.1.1
```

옵션	정의
38400	포트 ttya에 대해 이 변조 속도를 사용합니다.
asyncmap 0xa0000	로컬 시스템이 연결이 끊어진 피어와 통신할 수 있도록 asyncmap 값 0xa0000을 지정합니다.
:192.168.1.1	링크를 통해 호출하는 모든 피어에 IP 주소 192.168.1.1을 지정합니다.

사이트에서 /etc/ppp/options.ttya.tmpl을 사용하려면 /etc/ppp/options.tmpl의 이름을 /etc/ppp/options.*ttya-name*으로 바꾸고, *ttya-name*을 모뎀이 있는 직렬 포트의 이름으로 바꾼 다음 사이트의 필요에 따라 파일 내용을 수정하십시오.

/etc/ppp/options.*ttyname* 파일의 예를 찾을 수 있는 위치

/etc/ppp/options.*ttyname* 파일의 예를 찾으려면 다음을 참조하십시오.

- 다이얼 아웃 시스템의 경우 52 페이지 “직렬 회선을 통해 통신을 정의하는 방법”을 참조하십시오.
- 다이얼 인 서버의 경우 59 페이지 “직렬 회선을 통해 통신을 정의하는 방법(다이얼 인 서버)”을 참조하십시오.

사용자별 옵션 구성

이 절에는 다이얼 인 서버에서 사용자를 설정하는 방법에 대한 자세한 내용이 포함되어 있습니다.

다이얼 인 서버에서 $HOME/.ppprc 구성

$HOME/.ppprc 파일은 기본 PPP 옵션을 구성하는 사용자를 위한 것입니다. 관리자는 사용자를 위해 $HOME/.ppprc도 구성할 수 있습니다.

$HOME/.ppprc의 옵션에는 해당 파일을 호출하는 사용자에게 권한이 있는 경우에만 권한이 부여됩니다.

호출자가 pppd 명령을 사용하여 호출을 시작하는 경우에는 .ppprc 파일이 pppd 데몬에 의해 확인되는 두번째 파일이 됩니다.

다이얼 인 서버에서 $HOME/.ppprc를 설정하는 방법에 대한 자세한 내용은 58 페이지 “다이얼 인 서버의 사용자 설정”을 참조하십시오.

다이얼 아웃 시스템에서 $HOME/.ppprc 구성

$HOME/.ppprc 파일은 올바른 Solaris PPP 4.0 작동을 위해 다이얼 아웃 시스템에 필요하지 않습니다. 또한 특별한 경우를 제외하고는 $HOME/.ppprc를 다이얼 아웃 시스템에 둘 필요가 없습니다. 다음과 같은 경우 하나 이상의 .ppprc 파일을 만드십시오.

- 다양한 통신 요구를 가진 여러 사용자가 동일한 시스템에서 원격 피어를 호출할 수 있게 허용합니다. 이러한 경우에는 다이얼 아웃해야 하는 각 사용자의 홈 디렉토리에서 개별 .ppprc 파일을 만드십시오.
- 본인의 링크와 관련된 문제를 제어하는 옵션을 지정해야 합니다(예: Van Jacobson 압축을 사용 안함으로 설정). 링크 문제 해결 관련 지원은 James Carlson의 *PPP Design, Implementation, and Debugging* 및 pppd(1M) 매뉴얼 페이지를 참조하십시오.

.ppprc 파일은 다이얼 인 서버를 구성할 때 가장 흔히 사용됩니다. .ppprc 구성 지침은 58 페이지 “다이얼 인 서버의 사용자를 구성하는 방법”을 참조하십시오.

다이얼 인 서버와의 통신을 위한 정보 지정

다이얼 인 서버와 통신하려면 서버에 대한 정보를 수집해야 합니다. 그런 다음 몇몇 파일을 편집합니다. 또한 다이얼 아웃 시스템이 호출해야 하는 모든 다이얼 인 서버의 통신 요구 사항을 구성하는 것이 가장 중요합니다. ISP 전화 번호와 같은 다이얼 인 서버에 대한 옵션을 /etc/ppp/options.*ttyname* 파일에 지정할 수 있습니다. 그러나 피어 정보를 구성하기에 가장 좋은 위치는 /etc/ppp/peers/*peer-name* 파일입니다.

/etc/ppp/peers/*peer-name* 파일

주 – /etc/ppp/peers/*peer-name* 파일은 Solaris PPP 4.0의 올바른 작동을 위해 다이얼 아웃 시스템에 필요하지 않습니다.

/etc/ppp/peers/*peer-name* 파일을 사용하여 특정 피어와 통신하기 위한 정보를 제공할 수 있습니다. /etc/ppp/peers/*peer-name*을 사용하면 사용자가 설정할 수 없는 미리 선택된 권한이 지정된 옵션을 일반 사용자가 호출할 수 있습니다.

예를 들어, 권한이 부여되지 않은 사용자는 noauth가 /etc/ppp/peers/*peer-name* 파일에 지정된 경우 noauth 옵션을 대체할 수 없습니다. 사용자가 인증 자격 증명을 제공하지 않는 peerB에 대한 링크를 설정하려고 하는 경우 수퍼 유저는 noauth 옵션이 포함된 /etc/ppp/peers/peerB 파일을 만들 수 있습니다. noauth는 로컬 시스템이 peerB로부터의 호출을 인증하지 않음을 나타냅니다.

pppd 데몬은 pppd가 다음 옵션을 발견할 때 /etc/ppp/peers/*peer-name*을 읽습니다.

call *peer-name*

다이얼 아웃 시스템이 통신해야 하는 각 대상 피어에 대해 /etc/ppp/peers/*peer-name* 파일을 만들 수 있습니다. 이는 일반 사용자가 루트 권한 없이 특정 다이얼 아웃 링크를 호출할 수 있게 허용하려는 경우 특히 유용합니다.

/etc/ppp/peers/*peer-name*에서 지정하는 일반적인 옵션은 다음과 같습니다.

- user *user-name*

  PAP 또는 CHAP를 사용하여 인증할 때 다이얼 인 서버에 *user-name*을 다이얼 아웃 시스템의 로그인 이름으로 제공합니다.

- remotename *peer-name*

  *peer-name*을 다이얼 인 시스템의 이름으로 사용합니다. /etc/ppp/pap-secrets 또는 /etc/ppp/chap-secrets 파일을 스캔할 때 remotename이 PAP 또는 CHAP 인증과 함께 사용됩니다.

- connect "chat *chat_script* ..."

  채트 스크립트의 명령을 사용하여 다이얼 인 서버에 대한 통신을 엽니다.

- noauth

  통신을 시작할 때 피어 *peer-name*을 인증하지 않습니다.

- noipdefault

  피어와 협상할 때 사용되는 초기 IP 주소를 0.0.0.0으로 설정합니다. 피어 간의 IPCP 협상에 도움이 되도록 대부분의 ISP에 대한 링크를 설정할 때 noipdefault를 사용하십시오.

- defaultroute

링크에서 IP가 설정될 때 기본 IPv4 경로를 설치합니다.

특정 대상 피어에 적용될 수 있는 추가 옵션은 pppd(1M) 매뉴얼 페이지를 참조하십시오.

/etc/ppp/peers/myisp.tmpl 템플리트 파일

/etc/ppp/peers/myisp.tmpl 파일에는 /etc/ppp/peers/*peer-name* 파일에 대한 유용한 설명이 포함되어 있습니다. 템플리트는 /etc/ppp/peers/*peer-name* 파일에 대해 사용할 수 있는 일반적인 옵션으로 끝납니다.

```
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"
user myname
remotename myisp
noauth
noipdefault
defaultroute
updetach
noccp
```

옵션	정의
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"	채트 스크립트 /etc/ppp/myisp-chat를 사용하여 피어를 호출합니다.
user myname	로컬 시스템에 이 계정 이름을 사용합니다. myname은 피어의 /etc/ppp/pap-secrets 파일에서 이 시스템의 이름입니다.
remotename myisp	myisp를 로컬 시스템의 /etc/ppp/pap-secrets 파일에서 피어의 이름으로 인식합니다.
noauth	인증 자격 증명을 제공하기 위해 피어를 호출하지 않아도 됩니다.
noipdefault	로컬 시스템에 기본 IP 주소를 사용하지 않습니다.
defaultroute	로컬 시스템에 지정된 기본 경로를 사용합니다.
updetach	오류를 표준 출력 대신 PPP 로그 파일에 기록합니다.
noccp	CCP 압축을 사용하지 않습니다.

사이트에서 /etc/ppp/peers/myisp.tmpl을 사용하려면 /etc/ppp/peers/myisp.tmpl의 이름을 /etc/ppp/peers/.*peer-name*으로 바꾸고, *peer-name*을 호출할 피어의 이름으로 바꾼 다음 사이트의 필요에 따라 파일 내용을 수정하십시오.

/etc/ppp/peers/*peer-name* 파일의 예를 찾을 수 있는 위치

/etc/ppp/peers/*peer-name* 파일의 예를 찾으려면 다음을 참조하십시오.

- 다이얼 아웃 시스템의 경우 54 페이지 "개별 피어를 사용하여 연결을 정의하는 방법"을 참조하십시오.
- 전용 회선에 있는 로컬 시스템의 경우 65 페이지 "전용 회선에서 시스템을 구성하는 방법"을 참조하십시오.
- 다이얼 아웃 시스템에서의 PAP 인증 지원의 경우 76 페이지 "PPP 구성 파일에 PAP 지원을 추가하는 방법(다이얼 아웃 시스템)"을 참조하십시오.
- 다이얼 아웃 시스템에서의 CHAP 인증 지원의 경우 82 페이지 "PPP 구성 파일에 CHAP 지원을 추가하는 방법(다이얼 아웃 시스템)"을 참조하십시오.
- 클라이언트 시스템에서의 PPPoE 지원의 경우 84 페이지 "PPPoE 클라이언트 설정"을 참조하십시오.

다이얼 업 링크를 위한 모뎀 속도 구성

모뎀 구성에서의 대표적인 문제는 모뎀 작동 속도를 지정하는 것입니다. 다음 지침은 Sun Microsystems 컴퓨터에 사용되는 모뎀에 적용됩니다.

- 이전 SPARC 시스템 – 시스템과 함께 제공되는 하드웨어 설명서를 확인하십시오. 대부분의 SPARCstation 시스템에서는 모뎀 속도가 38400bps를 넘지 않아야 합니다.
- UltraSPARC 시스템 – 모뎀 속도를 115200bps로 설정합니다. 이는 최신 모뎀에 유용하며 다이얼 업 링크에 사용하기에 충분히 빠릅니다. 압축과 함께 이중 채널 ISDN TA를 사용하려는 경우에는 모뎀 속도를 높여야 합니다. UltraSPARC에 대한 제한은 비동기 링크의 경우 460800bps입니다.

다이얼 아웃 시스템의 경우 /etc/ppp/peers/*peer-name*과 같은 PPP 구성 파일에서 모뎀 속도를 설정하거나 속도를 pppd에 대한 옵션으로 지정하십시오.

다이얼 인 서버의 경우 56 페이지 "다이얼 인 서버에서 장치 구성"에 설명된 대로 ttymon 기능을 사용하여 속도를 설정해야 합니다.

다이얼 업 링크에서 대화 정의

다이얼 아웃 시스템과 해당 원격 피어는 다양한 명령을 협상 및 교환하여 PPP 링크를 통해 통신합니다. 다이얼 아웃 시스템을 구성할 때는 로컬 및 원격 모뎀에 필요한 명령을 확인해야 합니다. 그런 다음 이러한 명령이 포함된 채트 스크립트라는 파일을 만듭니다. 이 절에는 모뎀 구성 및 채트 스크립트 만들기에 대한 정보가 설명되어 있습니다.

채트 스크립트의 내용

다이얼 아웃 시스템이 연결해야 하는 각 원격 피어에는 자체 채트 스크립트가 필요합니다.

주 – 채트 스크립트는 일반적으로 다이얼 업 링크에서만 사용됩니다. 전용 회선 링크의 경우 링크에 시작 구성이 필요한 비동기 인터페이스가 포함되어 있지 않은 한 채트 스크립트가 사용되지 않습니다.

채트 스크립트의 내용은 모뎀 모델 또는 ISDN TA 및 원격 피어의 요구 사항에 따라 결정됩니다. 이러한 내용은 expect-send 문자열 세트로 나타납니다. 다이얼 아웃 시스템과 해당 원격 피어는 통신 시작 프로세스의 일환으로 문자열을 교환합니다.

expect 문자열에는 다이얼 아웃 호스트 시스템이 대화를 시작하기 위해 원격 피어에게서 받아야 하는 문자가 포함되어 있습니다. *send* 문자열에는 다이얼 아웃 시스템이 expect 문자열을 받은 후 원격 피어에게 보내는 문자가 포함되어 있습니다.

채트 스크립트의 정보에는 일반적으로 다음이 포함되어 있습니다.

- 모뎀 명령 - 보통 *AT* **명령**이라고 하며, 모뎀이 전화를 통해 데이터를 전송할 수 있게 합니다.
- 대상 피어의 전화 번호

  이 전화 번호는 ISP, 회사 사이트에 있는 다이얼 인 서버 또는 개별 시스템에 필요한 번호일 수 있습니다.
- 시간 초과 값(필요한 경우)
- 원격 피어에 필요한 로그인 절차
- 다이얼 아웃 시스템이 보낸 로그인 절차

채트 스크립트 예

이 절에는 사용자 고유 채트 스크립트를 만들기 위한 참조로 사용할 수 있는 채트 스크립트가 포함되어 있습니다. 모뎀 제조업체의 설명서와 ISP 및 기타 대상 호스트가 제공하는 정보에는 모뎀 및 대상 피어에 대한 채트 요구 사항이 포함되어 있습니다. 또한 많은 PPP 웹 사이트에 샘플 채트 스크립트가 있습니다.

기본적인 모뎀 채트 스크립트

다음은 사용자 고유 채트 스크립트를 만들기 위한 템플리트로 사용할 수 있는 기본적인 채트 스크립트입니다.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
```

```
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myserver\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
ogin: pppuser
ssword: \q\U
% pppd
```

다음 표에서는 채트 스크립트의 내용에 대해 설명합니다.

스크립트 내용	설명
ABORT BUSY	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
ABORT 'NO CARRIER'	전화를 걸 때 모뎀이 ABORT 'NO CARRIER'를 보고하는 경우 전송을 중단합니다. 이 메시지는 일반적으로 전화 걸기 또는 모뎀 협상 실패로 인해 표시됩니다.
REPORT CONNECT	모뎀에서 CONNECT 문자열을 수집합니다. 문자열을 인쇄합니다.
TIMEOUT 10	초기 시간 초과 값을 10초로 설정합니다. 모뎀의 응답이 즉시 이루어집니다.
"" AT&F1M0&M5S2=255	M0 – 연결 중 스피커를 끕니다.
	&M5 – 모뎀에 오류 제어가 필요하게 만듭니다.
	S2=255 – TIES "+++" 중단 시퀀스를 사용 안함으로 설정합니다.
SAY "Calling myserver\n"	로컬 시스템에서 Calling myserver 메시지를 표시합니다.
TIMEOUT 60	링크 협상에 더 많은 시간이 사용될 수 있도록 시간 초과 값을 60초로 재설정합니다.
OK "ATDT1-123-555-1212"	전화 번호 123-555-1212를 사용하여 원격 피어를 호출합니다.
ogin: pppuser	UNIX 스타일의 로그인을 사용하여 피어에 로그인합니다. 사용자 이름 pppuser를 제공합니다.
ssword: \q\U	\q – -v 옵션을 사용하여 디버깅하는 경우 기록하지 않습니다.
	\U – -U(명령줄에 지정) 다음에 오는 문자열의 내용을 이 위치에 삽입합니다. 일반적으로 문자열에는 암호가 포함됩니다.
% pppd	% 셸 프롬프트를 기다렸다가 pppd 명령을 실행합니다.

/etc/ppp/myisp-chat.tmpl 채트 스크립트 템플리트

이번 릴리스에는 사용자 사이트에서 사용하기 위해 수정할 수 있는 /etc/ppp/myisp-chat.tmpl이 포함되어 있습니다. /etc/ppp/myisp-chat.tmpl은 템플리트에 로그인 절차가 포함되어 있지 않다는 점을 제외하고 기본적인 모뎀 채트 스크립트와 유사합니다.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
""      "AT&F1"
OK      "AT&C1&D2"
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
```

스크립트 내용	설명
ABORT BUSY	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
ABORT 'NO CARRIER	전화를 걸 때 모뎀이 ABORT 'NO CARRIER'를 보고하는 경우 전송을 중단합니다. 이 메시지는 일반적으로 전화 걸기 또는 모뎀 협상 실패로 인해 표시됩니다.
REPORT CONNECT	모뎀에서 CONNECT 문자열을 수집합니다. 문자열을 인쇄합니다.
TIMEOUT 10	초기 시간 초과 값을 10초로 설정합니다. 모뎀의 응답이 즉시 이루어집니다.
"" "AT&F1"	모뎀을 출하 시의 기본값으로 재설정합니다.
OK "AT&C1&D2"	&C1의 경우 모뎀의 DCD가 반송파를 따르도록 모뎀을 재설정합니다. 어떤 이유로 원격측이 전화를 끊으면 DCD가 감소합니다. &D2의 경우 DTR이 높음에서 낮음으로 전이될 때 모뎀이 "온후크" 상태가 되거나 정지됩니다.
SAY "Calling myisp\n"	로컬 시스템에서 "Calling myisp" 메시지를 표시합니다.
TIMEOUT 60	링크 협상에 더 많은 시간이 사용될 수 있도록 시간 초과 값을 60초로 재설정합니다.
OK "ATDT1-123-555-1212"	전화 번호 123-555-1212를 사용하여 원격 피어를 호출합니다.
CONNECT \c	반대쪽 피어의 모뎀에서 CONNECT 메시지를 기다립니다.

ISP 호출을 위한 모뎀 채트 스크립트

다음 채트 스크립트를 U.S. Robotics Courier 모뎀이 설치된 다이얼 아웃 시스템에서 ISP를 호출하기 위한 템플리트로 사용하십시오.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
```

```
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

다음 표에서는 채트 스크립트의 내용에 대해 설명합니다.

스크립트 내용	설명
ABORT BUSY	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
ABORT 'NO CARRIER'	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
REPORT CONNECT	모뎀에서 CONNECT 문자열을 수집합니다. 문자열을 인쇄합니다.
TIMEOUT 10	초기 시간 초과 값을 10초로 설정합니다. 모뎀의 응답이 즉시 이루어집니다.
"" AT&F1M0M0M0M0&M5S2=255	M0 – 연결 중 스피커를 끕니다.
	&M5 – 모뎀에 오류 제어가 필요하게 만듭니다.
	S2=255 – TIES "+++" 중단 시퀀스를 사용 안함으로 설정합니다.
SAY "Calling myisp\n"	로컬 시스템에서 Calling myisp 메시지를 표시합니다.
TIMEOUT 60	링크 협상에 더 많은 시간이 사용될 수 있도록 시간 초과 값을 60초로 재설정합니다.
OK "ATDT1-123-555-1212"	전화 번호 123-555-1212를 사용하여 원격 피어를 호출합니다.
CONNECT \c	반대쪽 피어의 모뎀에서 CONNECT 메시지를 기다립니다.
\r \d\c	CONNECT 메시지의 끝까지 기다립니다.
SAY "Connected; running PPP\n"	로컬 시스템에서 Connected; running PPP 정보 메시지를 표시합니다.

UNIX 스타일의 로그인을 위해 향상된 기본적인 채트 스크립트

다음 채트 스크립트는 원격 Oracle Solaris 피어 또는 기타 UNIX 유형의 피어를 호출하기 위해 향상된 기본적인 스크립트입니다. 이 채트 스크립트는 53 페이지 "피어 호출 명령을 만드는 방법"에 사용됩니다.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&F1&M5S2=255
TIMEOUT 60
OK ATDT1-123-555-1234
CONNECT \c
SAY "Connected; logging in.\n"
```

```
TIMEOUT 5
ogin:--ogin: pppuser
TIMEOUT 20
ABORT 'ogin incorrect'
ssword: \qmypassword
"% " \c
SAY "Logged in.  Starting PPP on peer system.\n"
ABORT 'not found'
"" "exec pppd"
~ \c
```

다음 표에서는 채트 스크립트의 매개변수에 대해 설명합니다.

스크립트 내용	설명
`TIMEOUT 10`	초기 시간 초과 값을 10초로 설정합니다. 모뎀의 응답이 즉시 이루어집니다.
`ABORT BUSY`	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
`ABORT 'NO CARRIER'`	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
`ABORT ERROR`	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
`REPORT CONNECT`	모뎀에서 `CONNECT` 문자열을 수집합니다. 문자열을 인쇄합니다.
`"" AT&F1&M5S2=255`	`&M5` – 모뎀에 오류 제어가 필요하게 만듭니다. `S2=255` – TIES "+++" 중단 시퀀스를 사용 안함으로 설정합니다.
`TIMEOUT 60`	링크 협상에 더 많은 시간이 사용될 수 있도록 시간 초과 값을 60초로 재설정합니다.
`OK ATDT1-123-555-1234`	전화 번호 123-555-1212를 사용하여 원격 피어를 호출합니다.
`CONNECT \c`	반대쪽 피어의 모뎀에서 `CONNECT` 메시지를 기다립니다.
`SAY "Connected; logging in.\n"`	사용자 상태를 제공하기 위해 `Connected; logging in` 정보 메시지를 표시합니다.
`TIMEOUT 5`	로그인 프롬프트를 빠르게 표시할 수 있도록 시간 초과 값을 변경합니다.
`ogin:--ogin: pppuser`	로그인 프롬프트를 기다립니다. 프롬프트를 받지 못하면 RETURN을 보내고 기다립니다. 그런 다음 사용자 이름 `pppuser`를 피어에게 보냅니다. 후속 절차는 대부분의 ISP가 PAP 로그인으로 참조합니다. 그러나 PAP 로그인은 어떤 방식으로도 PAP 인증과 관련되어 있지 않습니다.
`TIMEOUT 20`	암호가 더 천천히 확인될 수 있도록 시간 초과 값을 20초로 변경합니다.

스크립트 내용	설명
ssword: \qmysecrethere	피어로부터 암호 프롬프트를 기다립니다. 프롬프트를 받으면 암호 \qmysecrethere를 보냅니다. \q는 시스템 로그 파일에 암호가 기록되지 않게 합니다.
"% " \c	피어로부터 셸 프롬프트를 기다립니다. 채트 스크립트에는 C 셸이 사용됩니다. 사용자가 다른 셸을 사용하여 로그인하는 것을 선호하는 경우 이 값을 변경하십시오.
SAY "Logged in. Starting PPP on peer system.\n"	사용자 상태를 제공하기 위해 Logged in. Starting PPP on peer system 정보 메시지를 표시합니다.
ABORT 'not found'	셸에 오류가 발생하는 경우 전송을 중단합니다.
"" "exec pppd"	피어에서 pppd를 시작합니다.
~ \c	피어에서 PPP가 시작되기를 기다립니다.

CONNECT \c 바로 다음에 PPP를 시작하는 것을 ISP는 보통 *PAP* **로그인**이라고 부릅니다. 그러나 실제로 PAP 로그인은 PAP 인증의 일부가 아닙니다.

ogin:--ogin: pppuser라는 문구는 다이얼 인 서버의 로그인 프롬프트에 대한 응답으로 사용자 이름 pppuser를 보내도록 모뎀에 지시합니다. pppuser는 다이얼 인 서버에서 원격 user1에 대해 만들어진 특수 PPP 사용자 계정 이름입니다. 다이얼 인 서버에서 PPP 사용자 계정을 만드는 방법에 대한 자세한 내용은 58 페이지 "다이얼 인 서버의 사용자를 구성하는 방법"을 참조하십시오.

외부 ISDN TA를 위한 채트 스크립트

다음은 ZyXEL omni.net. ISDN TA를 사용하는 다이얼 아웃 시스템에서 호출하기 위한 채트 스크립트입니다.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255
OK ATDI18882638234
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

다음 표에서는 채트 스크립트의 매개변수에 대해 설명합니다.

스크립트 내용	설명
SAY "Calling the peer"	다이얼 아웃 시스템의 화면에 이 메시지를 표시합니다.

스크립트 내용	설명
`TIMEOUT 10`	초기 시간 초과 값을 10초로 설정합니다.
`ABORT BUSY`	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
`ABORT 'NO CARRIER'`	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
`ABORT ERROR`	모뎀이 반대쪽 피어로부터 이 메시지를 받는 경우 전송을 중단합니다.
`REPORT CONNECT`	모뎀에서 `CONNECT` 문자열을 수집합니다. 문자열을 인쇄합니다.
`"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255`	이 행에 있는 문자의 의미는 다음과 같습니다. ■ `&F` – 출하시의 기본값 사용 ■ `B40` – 비동기 PPP 변환 수행 ■ `S83.7=1` – DOSB(Data Over Speech Bearer) 사용 ■ `&K44` – CCP 압축을 사용으로 설정 ■ `&J3` – MP를 사용으로 설정 ■ `X7` – DCE측 속도 보고 ■ `S61.3=1` – 패킷 단편화 사용 ■ `S0=0` – 자동 응답 안함 ■ `S2=255` – TIES 제어를 사용 안함으로 설정
`OK ATDI18882638234`	ISDN 호출을 실행합니다. 다중 연결의 경우 두번째 호출이 동일한 전화 번호에 대해 실행됩니다(일반적으로 대부분의 ISP에서 이렇게 요구함). 원격 피어에 다른 두번째 전화 번호가 필요한 경우에는 "*+nnnn*"을 추가하십시오. *nnnn*은 두번째 전화 번호를 나타냅니다.
`CONNECT \c`	반대쪽 피어의 모뎀에서 `CONNECT` 메시지를 기다립니다.
`\r \d\c`	`CONNECT` 메시지의 끝까지 기다립니다.
`SAY "Connected; running PPP\n"`	다이얼 아웃 시스템의 화면에 이 메시지를 표시합니다.

옵션 설명 및 채트 스크립트에 대한 기타 자세한 내용은 chat(1M) 매뉴얼 페이지를 참조하십시오. expect-send 문자열에 대한 자세한 내용은 175 페이지 "/etc/uucp/Systems 파일의 Chat-Script 필드"를 참조하십시오.

추가 채트 스크립트 예

많은 웹 사이트에서 샘플 채트 스크립트를 얻고 채트 스크립트 만들기 작업에 대한 지원을 받을 수 있습니다. 예는 http://ppp.samba.org/ppp/index.html을 참조하십시오.

채트 스크립트 호출

채트 스크립트는 connect 옵션을 사용하여 호출합니다. connect "chat ..."를 모든 PPP 구성 파일 또는 명령줄에서 사용할 수 있습니다.

채트 스크립트는 실행 가능하지 않지만 connect로 호출하는 프로그램은 실행 가능해야 합니다. chat 유틸리티를 connect로 호출하는 프로그램으로 사용할 수 있습니다. 이 경우 -f 옵션을 통해 채트 스크립트를 외부 파일에 저장하면 채트 스크립트 파일을 실행할 수 없습니다.

chat(1m)에 설명된 chat 프로그램은 실제 채트 스크립트를 실행합니다. pppd 데몬은 pppd가 connect "chat ..." 옵션을 발견할 때마다 chat 프로그램을 호출합니다.

주 – Perl 또는 Tcl과 같은 임의의 외부 프로그램을 사용하여 고급 채트 스크립트를 만들 수 있습니다. chat 유틸리티는 편의상 제공됩니다.

▼ 채트 스크립트를 호출하는 방법(작업)

1. **채트 스크립트를 ASCII 파일로 만듭니다.**

2. **다음 구문을 사용하여 임의의 PPP 구성 파일에서 채트 스크립트를 호출합니다.**

   ```
   connect 'chat  -f /etc/ppp/chatfile'
   ```

   -f 플래그는 다음에 파일 이름이 나옴을 나타냅니다. */etc/ppp/chatfile*은 채트 파일의 이름을 나타냅니다.

3. **pppd 명령을 실행하는 사용자에게 외부 채트 파일에 대한 읽기 권한을 부여합니다.**

주의 – chat 프로그램은 connect 'chat ...' 옵션을 권한 있는 소스에서 호출한 경우에도 항상 사용자의 권한으로 실행됩니다. 따라서 -f 옵션으로 읽는 별도의 채트 파일은 호출 사용자가 읽을 수 있어야 합니다. 채트 스크립트에 암호나 기타 민감한 정보가 포함되어 있는 경우 이 권한으로 인해 보안 문제가 발생할 수 있습니다.

예 8–1 인라인 채트 스크립트

다음과 같이 전체 채트 스크립트 대화를 한 행에 넣을 수 있습니다.

```
connect 'chat "" "AT&F1" OK ATDT5551212 CONNECT "\c"'
```

전체 채트 스크립트가 chat 키워드 다음에 오고 "\c"'로 종료됩니다. 이 형식은 모든 PPP 구성 파일 또는 명령줄에서 pppd에 대한 인수로 사용합니다.

자세한 정보

외부 파일의 채트 스크립트

특정 피어에 필요한 채트 스크립트가 길거나 복잡한 경우 스크립트를 별도의 파일로 만들어 보십시오. 외부 채트 파일은 유지 관리 및 문서화가 쉽습니다. 설명 앞에 해시(#) 기호를 추가하여 채트 파일에 설명을 추가할 수 있습니다.

53 페이지 “피어 호출 명령을 만드는 방법” 절차에서는 외부 파일에 포함되어 있는 채트 스크립트의 사용을 보여줍니다.

실행 가능한 채트 파일 만들기

다이얼 업 링크가 시작될 때 자동으로 실행할 실행 가능한 스크립트로 채트 파일을 만들 수 있습니다. 이렇게 하면 링크 시작 중 기존 채트 스크립트에 포함된 명령 외에 추가 명령(예: 패리티 설정을 위한 stty)을 실행할 수 있습니다.

이 실행 가능한 채트 스크립트는 짝수 패리티가 포함된 7비트를 필요로 하는 기존 스타일의 UNIX 시스템에 로그인합니다. 그러면 시스템이 PPP를 실행할 때 패리티가 없는 8비트로 변경됩니다.

```
#!/bin/sh
chat "" "AT&F1" OK "ATDT555-1212" CONNECT "\c"
stty evenp
chat ogin: pppuser ssword: "\q\U" % "exec pppd"
stty -evenp
```

▼ 실행 가능한 chat 프로그램을 만드는 방법

1 텍스트 편집기를 사용하여 이전 예와 같은 실행 가능한 chat 프로그램을 만듭니다.

2 chat 프로그램을 실행 가능하게 만듭니다.

```
# chmod +x /etc/ppp/chatprogram
```

3 chat 프로그램을 호출합니다.

```
connect /etc/ppp/chatprogram
```

chat 프로그램은 /etc/ppp 파일 시스템 내에 있지 않아도 되며, 어느 위치에나 저장될 수 있습니다.

링크에서 호출자 인증

이 절에서는 PPP 인증 프로토콜의 작동 방법을 설명하고 인증 프로토콜과 연관된 데이터베이스에 대해 설명합니다.

PAP(암호 인증 프로토콜)

PAP 인증은 작동 면에서 UNIX `login` 프로그램과 유사합니다. 그러나 PAP는 사용자에게 셸 액세스 권한을 부여하지 않습니다. PAP는 `/etc/ppp/pap-secrets` 파일의 형태로 PPP 구성 파일 및 PAP 데이터베이스를 사용하여 인증을 설정합니다. 또한 PAP는 `/etc/ppp/pap-secrets`를 사용하여 PAP 보안 자격 증명을 정의합니다. 이러한 자격 증명에는 피어 이름, PAP 방식의 "사용자 이름" 및 암호가 포함되어 있습니다. 또한 PAP 자격 증명에는 로컬 시스템에 연결할 수 있는 각 호출자에 대한 관련 정보가 포함되어 있습니다. PAP 사용자 이름 및 암호는 암호 데이터베이스에 있는 UNIX 사용자 이름 및 암호와 같거나 다를 수 있습니다.

`/etc/ppp/pap-secrets` 파일

PAP 데이터베이스는 `/etc/ppp/pap-secrets` 파일에 구현됩니다. 인증에 성공하려면 PPP 링크의 양쪽에 있는 시스템의 `/etc/ppp/pap-secrets` 파일에서 PAP 자격 증명을 제대로 구성해야 합니다. 호출자(피인증자)는 사용되지 않는 `+ua` 파일이나 `/etc/ppp/pap-secrets` 파일의 `user` 및 `password` 열에서 자격 증명을 제공합니다. 서버(인증자)는 UNIX `passwd` 데이터베이스를 통해 `/etc/ppp/pap-secrets`의 정보를 기준으로 이러한 자격 증명을 검증하거나 PAM 기능의 정보를 기준으로 자격 증명을 검증합니다.

`/etc/ppp/pap-secrets` 파일의 구문은 다음과 같습니다.

```
myclient ISP-server mypassword *
```

매개변수의 의미는 다음과 같습니다.

`myclient`	호출자의 PAP 사용자 이름입니다. 이 이름은 호출자의 UNIX 사용자 이름과 동일한 경우가 많으며, 이는 다이얼 인 서버가 PAP의 `login` 옵션을 사용하는 경우에 특히 그렇습니다.
`ISP-server`	원격 시스템(보통 다이얼 인 서버)의 이름입니다.
`mypassword`	호출자의 PAP 암호입니다.
*	호출자에 연결된 IP 주소입니다. IP 주소를 나타낼 때는 별표(*)를 사용하십시오.

PAP 암호 만들기

PAP 암호는 **암호화되지 않은 형식**, 즉 읽을 수 있는 ASCII 형식으로 링크를 통해 전송됩니다. 호출자(피인증자)의 경우 PAP 암호를 암호화되지 않은 형식으로 다음 위치 중 하나에 저장해야 합니다.

- `/etc/ppp/pap-secrets`에
- 다른 외부 파일에
- `pap-secrets` @ 기능을 통해 명명된 파이프에
- `pppd`에 대한 옵션으로 명령줄 또는 PPP 구성 파일에
- `+ua` 파일을 통해

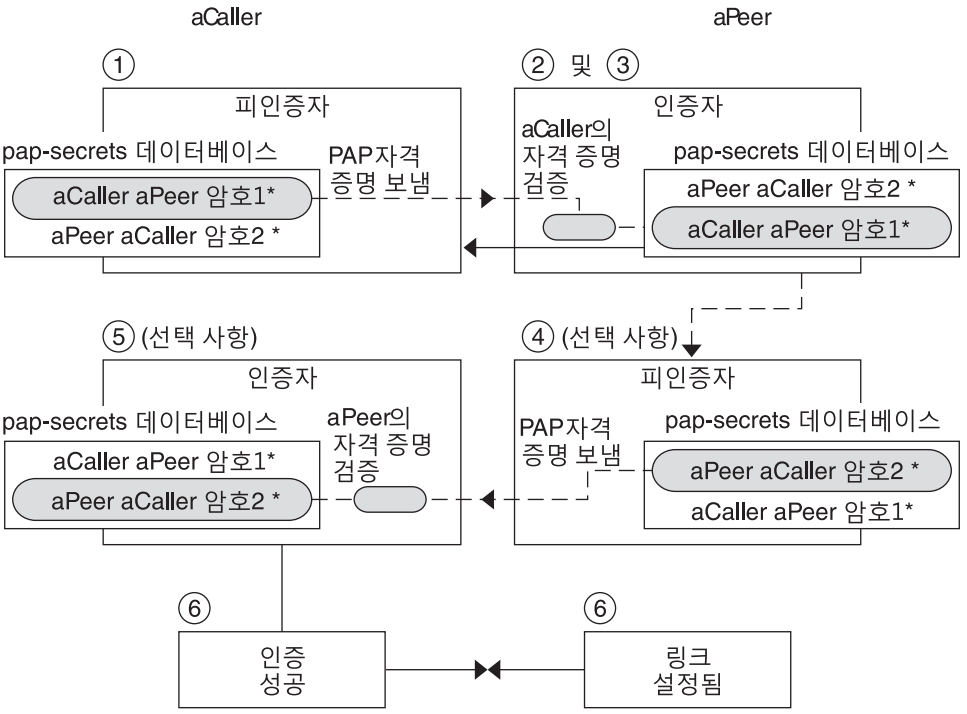
서버(인증자)에서는 다음 중 하나를 수행하여 PAP 암호를 숨길 수 있습니다.

- `pap-secrets` 파일에서 `papcrypt`를 지정하고 `crypt`(3C)로 해시된 암호 사용
- `pppd`에 `login` 옵션을 지정하고, 암호 열에 큰따옴표("")를 추가하여 `pap-secrets` 파일에서 암호 생략. 이 경우 인증은 UNIX passwd 데이터베이스 또는 PAM 방식을 통해 수행됩니다.

PAP 인증 중 발생하는 작업

PAP 인증은 다음 순서대로 발생합니다.

그림 8–1 PAP 인증 프로세스



1. 호출자(피인증자)가 원격 피어(인증자)를 호출하고 해당 PAP 사용자 이름 및 암호를 링크 협상의 일환으로 제공합니다.
2. 피어가 해당 `/etc/ppp/pap-secrets` 파일에서 호출자의 ID를 확인합니다. 피어가 PAP의 `login` 옵션을 사용하는 경우에는 피어가 해당 암호 데이터베이스에서 호출자의 사용자 이름 및 암호를 확인합니다.
3. 인증에 성공하면 피어가 호출자와 링크 협상을 계속합니다. 인증에 실패하면 링크가 삭제됩니다.
4. (옵션) 호출자가 원격 피어의 응답을 인증하는 경우 원격 피어가 자체 PAP 자격 증명을 호출자에게 보내야 합니다. 따라서 원격 피어가 피인증자가 되고 호출자가 인증자가 됩니다.
5. (옵션) 원래 호출자가 자체 `/etc/ppp/pap-secrets`를 읽어 원격 피어의 ID를 확인합니다.

주 – 원래 호출자가 원격 피어로부터 인증 자격 증명을 요구하는 경우에는 1단계와 4단계가 병렬로 발생합니다.

피어가 인증되면 협상이 계속됩니다. 그렇지 않으면 링크가 삭제됩니다.

6. 링크가 성공적으로 설정될 때까지 호출자와 피어 간의 협상이 계속됩니다.

/etc/ppp/pap-secrets에 login 옵션 사용

PAP 자격 증명을 인증하기 위한 login 옵션을 모든 PPP 구성 파일에 추가할 수 있습니다. /etc/ppp/options 등에 login을 지정하면 pppd가 호출자의 PAP 자격 증명이 암호 데이터베이스에 있는지 확인합니다. 다음은 login 옵션이 포함된 /etc/ppp/pap-secrets 파일의 형식입니다.

```
joe    *  ""  *
sally  *  ""  *
sue    *  ""  *
```

매개변수의 의미는 다음과 같습니다.

호출자 — joe, sally 및 sue가 권한이 부여된 호출자의 이름입니다.

서버 — 별표(*)로, 모든 서버 이름이 유효함을 나타냅니다. PPP 구성 파일에서는 name 옵션이 필요하지 않습니다.

암호 — 큰따옴표로, 모든 암호가 유효함을 나타냅니다.

이 열에 암호가 있는 경우에는 피어의 암호가 PAP 암호 및 UNIX passwd 데이터베이스 모두와 일치해야 합니다.

IP 주소 — 별표(*)로, 모든 IP 주소가 허용됨을 나타냅니다.

CHAP(Challenge-Handshake 인증 프로토콜)

CHAP 인증에는 **챌린지**와 **응답**이라는 개념이 사용됩니다. 즉, 피어(인증자)가 호출자(피인증자)에게 자신의 ID를 증명하도록 요구합니다. 챌린지에는 인증자가 생성한 고유한 ID와 난수가 포함됩니다. 호출자는 해당 ID, 난수 및 CHAP 보안 자격 증명을 사용하여 피어에게 보낼 적절한 응답(핸드셰이크)을 생성해야 합니다.

CHAP 보안 자격 증명에는 CHAP 사용자 이름 및 CHAP "암호"가 포함됩니다. CHAP 암호는 호출자와 피어가 PPP 링크를 협상하기 전에 양쪽 모두에 알려지는 임의 문자열입니다. CHAP 보안 자격 증명은 CHAP 데이터베이스인 /etc/ppp/chap-secrets에서 구성합니다.

/etc/ppp/chap-secrets 파일

CHAP 데이터베이스는 /etc/ppp/chap-secrets 파일에서 구현됩니다. 인증에 성공하려면 PPP 링크 양쪽에 있는 시스템의 해당 /etc/ppp/chap-secrets 파일에 서로의 CHAP 자격 증명이 있어야 합니다.

주 – PAP와 달리 공유 암호는 두 피어 모두에서 암호화되지 않은 형식으로 있어야 합니다. CHAP에서는 crypt, PAM 또는 PPP 로그인 옵션을 사용할 수 없습니다.

`/etc/ppp/chap-secrets` 파일의 구문은 다음과 같습니다.

```
myclient myserver secret5748 *
```

매개변수의 의미는 다음과 같습니다.

`myclient` 호출자의 CHAP 사용자 이름입니다. 이 이름은 호출자의 UNIX 사용자 이름과 같거나 다를 수 있습니다.

`myserver` 원격 시스템(보통 다이얼 인 서버)의 이름입니다.

`secret5748` 호출자의 CHAP 암호입니다.

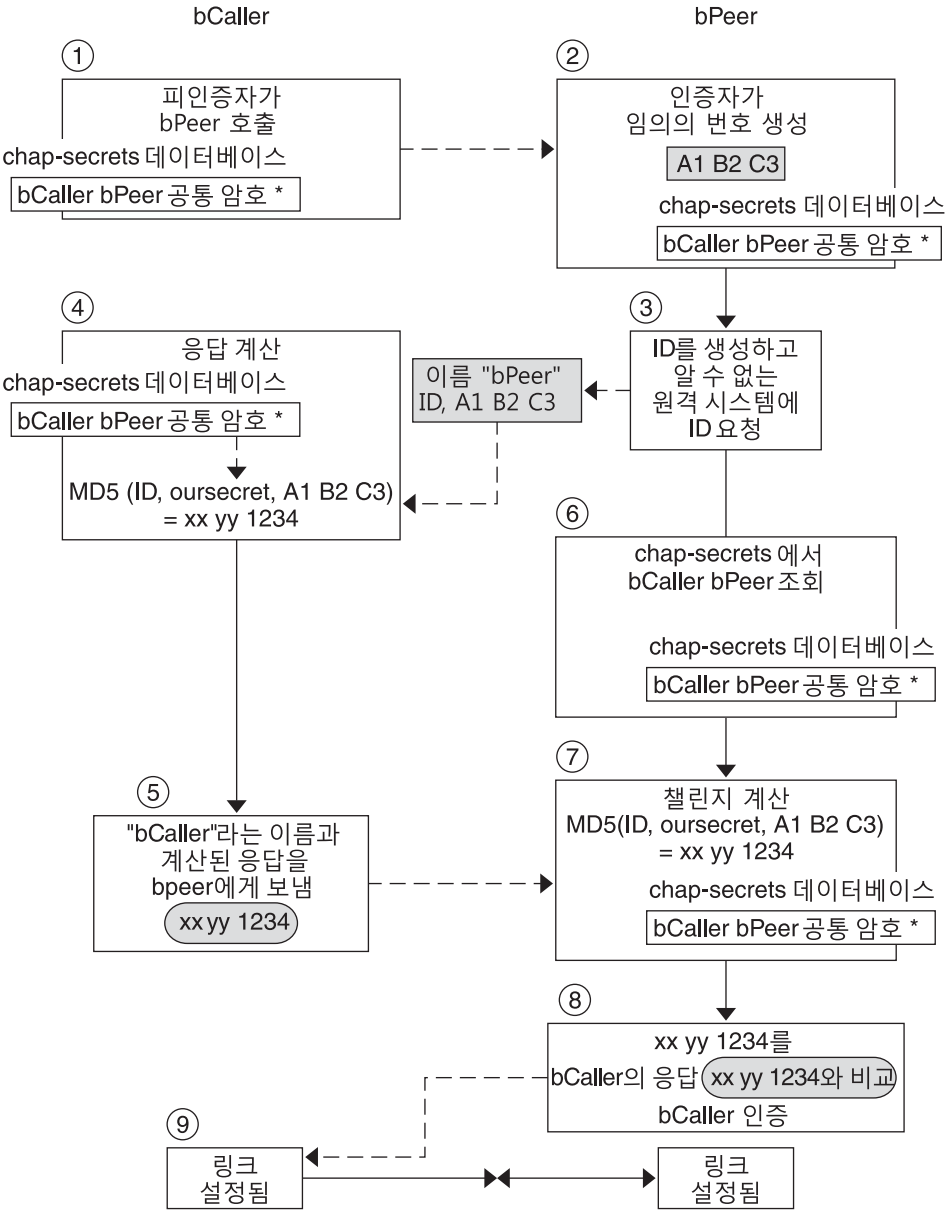
주 – PAP 암호와 달리 CHAP 암호는 절대 링크를 통해 전송되지 않습니다. 대신 CHAP 암호는 로컬 시스템이 응답을 계산할 때 사용됩니다.

`*` 호출자에 연결된 IP 주소입니다. IP 주소를 나타낼 때는 별표(*)를 사용하십시오.

CHAP 인증 중 발생하는 작업

CHAP 인증은 다음 순서대로 발생합니다.

그림 8–2 CHAP 인증 순서



1. 통신을 시작하려고 하는 두 피어가 PPP 링크 협상 중 인증에 사용될 암호에 대해 합의를 봅니다.

2. 두 시스템의 관리자가 암호, CHAP 사용자 이름 및 기타 CHAP 자격 증명을 해당 시스템의 /etc/ppp/chap-secrets 데이터베이스에 추가합니다.
3. 호출자(피인증자)가 원격 피어(인증자)를 호출합니다.
4. 인증자가 난수 및 ID를 생성하고 이 데이터를 피인증자에게 챌린지로 보냅니다.
5. 피인증자가 해당 /etc/ppp/chap-secrets 데이터베이스에서 피어의 이름 및 암호를 조회합니다.
6. 피인증자가 암호 및 피어의 난수 챌린지에 MD5 계산 알고리즘을 적용하여 응답을 계산합니다. 그런 다음 피인증자가 결과를 인증자에게 응답으로 보냅니다.
7. 인증자가 해당 /etc/ppp/chap-secrets 데이터베이스에서 피인증자의 이름 및 암호를 조회합니다.
8. 인증자가 /etc/ppp/chap-secrets에서 챌린지로 생성된 숫자와 피인증자의 암호에 MD5를 적용하여 자체 결과를 계산합니다.
9. 인증자가 자신의 결과를 호출자의 응답과 비교합니다. 두 숫자가 같으면 피어가 호출자를 성공적으로 인증한 것이며 링크 협상이 계속됩니다. 그렇지 않으면 링크가 삭제됩니다.

호출자를 위한 IP 주소 지정 체계 만들기

각 원격 사용자에게 고유한 IP 주소를 지정하는 대신 모든 수신 호출에 대해 하나 이상의 IP 주소를 만들어 보십시오. 전용 IP 주소는 잠재적 호출자의 수가 다이얼 인 서버에 있는 직렬 포트 및 모뎀의 수를 초과하는 경우 특히 중요합니다. 사이트의 요구에 따라 다양한 여러 시나리오를 구현할 수 있습니다. 여러 시나리오를 동시에 사용할 수도 있습니다.

호출자에게 동적 IP 주소 지정

동적 주소 지정 작업에서는 각 호출자에게 /etc/ppp/options.*ttyname*에 정의되어 있는 IP 주소를 지정합니다. 동적 주소 지정 작업은 직렬 포트별로 발생합니다. 호출이 직렬 회선을 통해 도착하면 호출자가 호출의 직렬 인터페이스에 대한 /etc/ppp/options.*ttyname* 파일에 있는 IP 주소를 받습니다.

수신 호출에 다이얼 업 서비스를 제공하는 직렬 인터페이스 4개가 다이얼 인 서버에 있는 경우를 예로 들어 보겠습니다.

- 직렬 포트 term/a의 경우 다음 항목을 사용하여 /etc/ppp/options.term.a 파일을 만듭니다.

  ```
  :10.1.1.1
  ```

- 직렬 포트 term/b의 경우 다음 항목을 사용하여 /etc/ppp/options.term.b 파일을 만듭니다.

```
:10.1.1.2
```

- 직렬 포트 term/c의 경우 다음 항목을 사용하여 /etc/ppp/options.term.c 파일을 만듭니다.

```
:10.1.1.3
```

- 직렬 포트 term/d의 경우 다음 항목을 사용하여 /etc/ppp/options.term.d 파일을 만듭니다.

```
:10.1.1.4
```

이전 주소 지정 체계를 사용하여 직렬 인터페이스 /dev/term/c에 있는 수신 호출에 호출 기간 동안 IP 주소 10.1.1.3이 지정됩니다. 첫번째 호출자가 전화를 끊으면 직렬 인터페이스 /dev/term/c를 통해 들어오는 후속 호출에도 IP 주소 10.1.1.3이 지정됩니다.

동적 주소 지정의 이점은 다음과 같습니다.

- 직렬 포트까지 PPP 네트워크 사용을 추적할 수 있습니다.
- PPP용으로 최소한의 IP 주소를 지정할 수 있습니다.
- IP 필터링을 보다 간편하게 관리할 수 있습니다.

호출자에게 정적 IP 주소 지정

사이트에서 PPP 인증을 구현하는 경우 개별 호출자에게 특정 **정적** IP 주소를 지정할 수 있습니다. 이 경우 다이얼 아웃 시스템이 다이얼 인 서버를 호출할 때마다 호출자가 동일한 IP 주소를 받습니다.

정적 주소는 pap-secrets 또는 chap-secrets 데이터베이스에서 구현합니다. 다음은 정적 IP 주소를 정의하는 /etc/ppp/pap-secrets 파일의 예입니다.

```
joe    myserver  joepasswd   10.10.111.240
sally  myserver  sallypasswd 10.10.111.241
sue    myserver  suepasswd   10.10.111.242
```

호출자 joe, sally 및 sue가 권한이 부여된 호출자의 이름입니다.

서버 myserver가 서버의 이름을 나타냅니다.

암호 joepasswd, sallypasswd 및 suepasswd가 각 호출자의 암호를 나타냅니다.

IP 주소 10.10.111.240, 10.10.111.241 및 10.10.111.242가 각 호출자에게 지정된 IP 주소입니다.

다음은 정적 IP 주소를 정의하는 /etc/ppp/chap-secrets 파일의 예입니다.

```
account1 myserver secret5748  10.10.111.244
account2 myserver secret91011 10.10.111.245
```

호출자 account1 및 account2가 호출자의 이름을 나타냅니다.

서버 myserver가 각 호출자에 대한 서버의 이름을 나타냅니다.

암호 secret5748 및 secret91011이 각 호출자의 CHAP 암호를 나타냅니다.

IP 주소 10.10.111.244 및 10.10.111.245가 각 호출자의 IP 주소입니다.

sppp 장치 번호별로 IP 주소 지정

PAP 또는 CHAP 인증을 사용하는 경우 sppp 장치 번호별로 호출자에게 IP 주소를 지정할 수 있습니다. 다음은 이러한 사용법의 예입니다.

```
myclient ISP-server mypassword 10.10.111.240/28+
```

플러스 기호(+)는 장치 번호가 IP 주소에 추가되었음을 나타냅니다. 다음 사항에 유의하십시오.

- 10.10.111.240부터 10.10.111.255까지의 주소는 원격 사용자에게 지정됩니다.
- sppp0은 IP 주소 10.10.111.240을 받습니다.
- sppp1은 IP 주소 10.10.111.241을 받습니다. 이런 식으로 계속됩니다.

DSL 지원을 위해 PPPoE 터널 만들기

PPPoE를 사용하면 하나 이상의 DSL 모뎀을 사용하고 있는 여러 클라이언트에게 고속 디지털 서비스를 통해 PPP를 제공할 수 있습니다. PPPoE는 세 참가자(기업, 전화 회사 및 서비스 공급자)를 통해 이더넷 터널을 만들어 이러한 서비스를 구현합니다.

- PPPoE의 작동 방법에 대한 개요 및 설명은 30 페이지 “PPPoE 개요”를 참조하십시오.
- PPPoE 터널 설정 작업은 6 장, “PPPoE 터널 설정(작업)”을 참조하십시오.

이 절에는 다음 표에 요약되어 있는 PPPoE 명령 및 파일에 대한 자세한 정보가 포함되어 있습니다.

표 8–2 PPPoE 명령 및 구성 파일

파일 또는 명령	설명	수행 방법
/etc/ppp/pppoe	시스템에서 PPPoE에 의해 설정된 모든 터널에 기본적으로 적용되는 특징이 포함된 파일입니다.	141 페이지 “/etc/ppp/pppoe 파일”
/etc/ppp/pppoe.*device*	PPPoE가 터널에 사용하는 특정 인터페이스의 특징이 포함된 파일입니다.	143 페이지 “/etc/ppp/pppoe.*device* 파일”
/etc/ppp/pppoe.if	PPPoE에 의해 설정된 터널이 실행되는 이더넷 인터페이스가 나열된 파일입니다.	139 페이지 “/etc/ppp/pppoe.if 파일”

표 8–2 PPPoE 명령 및 구성 파일 (계속)

파일 또는 명령	설명	수행 방법
/usr/sbin/sppptun	PPPoE 터널에 참여하는 이더넷 인터페이스를 구성하기 위한 명령입니다.	139 페이지 "/usr/sbin/sppptun 명령"
/usr/lib/inet/pppoed	터널 설정을 위해 PPPoE를 사용하기 위한 명령 및 옵션입니다.	141 페이지 "/usr/lib/inet/pppoed 데몬"

PPPoE용 인터페이스를 구성하기 위한 파일

PPPoE 터널의 각 끝에서 사용되는 인터페이스를 구성해야 해당 터널이 PPP 통신을 지원할 수 있습니다. 이렇게 하려면 /usr/sbin/sppptun 및 /etc/ppp/pppoe.if 파일을 사용하십시오. 이러한 도구를 사용하여 모든 Oracle Solaris PPPoE 클라이언트 및 PPPoE 액세스 서버에서 이더넷 인터페이스를 구성해야 합니다.

/etc/ppp/pppoe.if 파일

/etc/ppp/pppoe.if 파일에는 PPPoE 터널에 사용될 호스트의 모든 이더넷 인터페이스 이름이 나열됩니다. 이 파일은 나열된 인터페이스가 PPPoE 터널에 사용될 수 있도록 연결될 때 시스템 부트 도중 처리됩니다.

/etc/ppp/pppoe.if를 명시적으로 만들어야 합니다. PPPoE용으로 구성할 한 인터페이스의 이름을 각 행에 입력하십시오.

다음 예에서는 PPPoE 터널을 위한 세 가지 인터페이스를 제공하는 서버에 대한 /etc/ppp/pppoe.if 파일을 보여줍니다.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
hme3
```

PPPoE 클라이언트에는 일반적으로 /etc/ppp/pppoe.if에 나열된 하나의 인터페이스만 있습니다.

/usr/sbin/sppptun 명령

/usr/sbin/sppptun 명령을 사용하여 PPPoE 터널에 사용될 이더넷 인터페이스를 수동으로 연결 및 연결 취소할 수 있습니다. 반대로 /etc/ppp/pppoe.if는 시스템 부트 시에만 읽힙니다. 이러한 인터페이스는 /etc/ppp/pppoe.if에 나열된 인터페이스와 일치해야 합니다.

sppptun은 PPPoE 터널에 사용되는 이더넷 인터페이스를 ipadm 명령과 유사한 방식으로 연결합니다. 그러나 두 개의 이더넷 프로토콜 번호가 사용되므로 ipadm과 달리 PPPoE를 지원하기 위해 인터페이스를 두 번 연결해야 합니다.

sppptun의 기본 구문은 다음과 같습니다.

```
# /usr/sbin/sppptun plumb pppoed device-name
      device-name:pppoed
# /usr/sbin/sppptun plumb pppoe device-name
      device-name:pppoe
```

이 구문에서 *device-name*은 PPPoE에 연결될 장치의 이름입니다.

sppptun 명령을 처음 실행하면 검색 프로토콜 pppoed가 인터페이스에서 연결됩니다. sppptun을 두번째로 실행하면 세션 프로토콜 pppoe가 연결됩니다. sppptun은 방금 연결된 인터페이스의 이름을 인쇄합니다. 필요한 경우 이 이름을 사용하여 인터페이스의 연결을 취소합니다.

자세한 내용은 sppptun(1M) 매뉴얼 페이지를 참조하십시오.

인터페이스 관리를 위한 sppptun 명령의 예

다음 예에서는 /usr/sbin/sppptun을 사용하여 PPPoE용 인터페이스를 수동으로 연결하는 방법을 보여줍니다.

```
# /usr/sbin/sppptun plumb pppoed hme0
hme0:pppoed
# /dev/sppptun plumb pppoe hme0
 hme0:pppoe
```

이 예에서는 PPPoE에 연결된 액세스 서버의 인터페이스를 나열하는 방법을 보여줍니다.

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

이 예에서는 인터페이스의 연결을 취소하는 방법을 보여줍니다.

```
# sppptun unplumb hme0:pppoed
# sppptun unplumb hme0:pppoe
```

PPPoE 액세스 서버 명령 및 파일

DSL 서비스 또는 지원을 고객에게 제공하는 서비스 공급자는 PPPoE를 실행하는 액세스 서버를 사용할 수 있습니다. PPPoE 액세스 서버 및 클라이언트는 기존의 클라이언트-서버 관계에서 동작합니다. 이 관계는 다이얼 업 링크에 있는 다이얼 인 서버와 다이얼 아웃 시스템의 관계와 유사합니다. 한 PPPoE 시스템이 통신을 시작하고 한 PPPoE 시스템이 응답합니다. 반대로 PPP 프로토콜에는 클라이언트-서버 관계라는 개념이 없습니다. PPP는 두 시스템을 모두 동등한 피어로 간주합니다.

PPPoE 액세스 서버를 설정하는 명령 및 파일은 다음과 같습니다.

- 139 페이지 “/usr/sbin/sppptun 명령”
- 141 페이지 “/usr/lib/inet/pppoed 데몬”
- 141 페이지 “/etc/ppp/pppoe 파일”
- 143 페이지 “/etc/ppp/pppoe.*device* 파일”
- 146 페이지 “pppoe.so 공유 객체”

/usr/lib/inet/pppoed 데몬

pppoed 데몬은 잠재적 PPPoE 클라이언트로부터 서비스용 브로드캐스트를 받습니다. 또한 pppoed는 PPPoE 터널의 서버측을 협상하고 PPP 데몬인 pppd를 해당 터널을 통해 실행합니다.

pppoed 서비스는 /etc/ppp/pppoe 및 /etc/ppp/pppoe.*device* 파일에서 구성합니다. 시스템 부트 시 /etc/ppp/pppoe가 있으면 pppoed가 자동으로 실행됩니다. 명령줄에서 /usr/lib/inet/pppoed를 입력하여 pppoed 데몬을 명시적으로 실행할 수도 있습니다.

/etc/ppp/pppoe 파일

/etc/ppp/pppoe 파일에는 액세스 서버가 제공하는 서비스와 PPP가 PPPoE 터널을 통해 실행되는 방법을 정의하는 방법이 설명되어 있습니다. 개별 인터페이스에 대해 서비스를 정의하거나 액세스 서버에 있는 모든 인터페이스에 대해 전역적으로 서비스를 정의할 수 있습니다. 액세스 서버는 잠재적 PPPoE 클라이언트로부터 받은 브로드캐스트에 대한 응답으로 /etc/ppp/pppoe 파일의 정보를 보냅니다.

/etc/ppp/pppoe의 기본 구문은 다음과 같습니다.

```
global-options
service  service-name
        service-specific-options
        device  interface-name
```

매개변수의 의미는 다음과 같습니다.

global-options

/etc/ppp/pppoe 파일에 대한 기본 옵션을 설정합니다. 이러한 옵션은 pppoed 또는 pppd를 통해 사용 가능한 모든 옵션일 수 있습니다. 전체 옵션 목록은 pppoed(1M) 및 pppd(1M) 매뉴얼 페이지를 참조하십시오.

예를 들어, PPPoE 터널에 대해 사용 가능한 이더넷 인터페이스를 *global options*의 일부로 나열해야 합니다. /etc/ppp/pppoe에서 장치를 정의하지 않으면 어떤 인터페이스에서도 서비스가 제공되지 않습니다.

devices를 전역 옵션으로 정의하려면 다음 형식을 사용하십시오.

device interface <,interface>

*interface*는 서비스가 잠재적 PPPoE 클라이언트에 대해 수신 대기하는 인터페이스를 지정합니다. 둘 이상의 인터페이스가 서비스와 연관되는 경우에는 각 이름을 쉼표로 구분하십시오.

service service-name — *service-name* 서비스의 정의를 시작합니다. *service-name*은 제공되는 서비스에 적합한 모든 구문일 수 있는 문자열입니다.

service-specific-options — 이 서비스와 관련된 PPPoE 및 PPP 옵션을 나열합니다.

`device` *interface-name* — 이전에 나열된 서비스를 사용할 수 있는 인터페이스를 지정합니다.

`/etc/ppp/pppoe`에 대한 추가 옵션은 pppoed(1M) 및 pppd(1M) 매뉴얼 페이지를 참조하십시오.

일반적인 `/etc/ppp/pppoe` 파일은 다음과 같을 수 있습니다.

예 8–2 기본적인 `/etc/ppp/pppoe` 파일

```
device hme1,hme2,hme3
service internet
   pppd "name internet-server"
service intranet
   pppd "192.168.1.1:"
service debug
   device hme1
   pppd "debug name internet-server"
```

이 파일에서는 다음 값이 적용됩니다.

`hme1,hme2,hme3` — PPPoE 터널에 사용될 액세스 서버의 세 인터페이스입니다.

`service internet` — `internet`이라는 서비스를 잠재적 클라이언트에게 알립니다. 서비스를 제공하는 공급자가 `internet`의 정의 방법도 결정합니다. 예를 들어, `internet`이 다양한 IP 서비스와 인터넷에 대한 액세스를 의미하는 것으로 공급자가 해석할 수 있습니다.

`pppd` — 호출자가 `pppd`를 호출할 때 사용되는 명령줄 옵션을 설정합니다. `"name internet-server"` 옵션은 로컬 시스템(액세스 서버)의 이름을 `internet-server`로 제공합니다.

`service intranet` — `intranet`이라는 다른 서비스를 잠재적 클라이언트에게 알립니다.

`pppd "192.168.1.1:"`	호출자가 `pppd`를 호출할 때 사용되는 명령줄 옵션을 설정합니다. 호출자가 `pppd`를 호출하면 192.168.1.1이 로컬 시스템(액세스 서버)의 IP 주소로 설정됩니다.
`service debug`	PPPoE에 대해 정의된 인터페이스에서 세번째 서비스인 디버깅을 알립니다.
`device hme1`	PPPoE 터널에 대한 디버깅을 `hme1`로 제한합니다.
`pppd "debug name internet-server"`	호출자가 `pppd`를 호출할 때 사용되는 명령줄 옵션을 설정합니다. 이 경우에는 로컬 시스템인 `internet-server`의 PPP 디버깅입니다.

`/etc/ppp/pppoe.`*device* 파일

`/etc/ppp/pppoe.`*device* 파일에는 PPPoE 액세스 서버의 한 인터페이스에서 제공되는 서비스가 설명되어 있습니다. `/etc/ppp/pppoe.`*device*에는 PPP가 PPPoE 터널을 통해 실행되는 방법을 정의하는 옵션도 포함되어 있습니다. `/etc/ppp/pppoe.`*device*는 전역 `/etc/ppp/pppoe`와 동일하게 동작하는 선택적 파일입니다. 그러나 `/etc/ppp/pppoe.`*device*가 인터페이스에 대해 정의되어 있으면 해당 매개변수가 `/etc/ppp/pppoe`에 정의된 전역 매개변수보다 해당 인터페이스에 대해 우선적으로 사용됩니다.

`/etc/ppp/pppoe.`*device*의 기본 구문은 다음과 같습니다.

`service` *service-name*
service-specific-options
`service` *another-service-name*
service-specific-options

이 구문과 `/etc/ppp/pppoe`의 구문은 141 페이지 “`/etc/ppp/pppoe` 파일”에 나와 있는 `device` 옵션을 사용할 수 없다는 점에서만 다릅니다.

`pppoe.so` 플러그인

`pppoe.so`는 PPPoE 액세스 서버 및 클라이언트가 호출해야 하는 PPPoE 공유 객체 파일입니다. 이 파일은 `pppoed`와 함께 MTU 및 MRU를 1492로 제한하고, 드라이버로부터의 패킷을 필터링하고, PPPoE 터널을 협상합니다. 액세스 서버측에서 `pppoe.so`는 `pppd` 데몬을 통해 자동으로 호출됩니다.

PPPoE 및 PPP 파일을 사용하여 액세스 서버 구성

이 절에는 액세스 서버를 구성하는 데 사용되는 모든 파일의 샘플이 포함되어 있습니다. 액세스 서버는 멀티홈 방식을 사용합니다. 이 서버는 `green`, `orange` 및 `purple`이라는 세 서브넷에 연결됩니다. `pppoed`는 서버에서 `root`로 실행됩니다(기본값).

PPPoE 클라이언트는 hme0 및 hme1 인터페이스를 통해 orange 및 purple 네트워크에 액세스합니다. 클라이언트는 표준 UNIX 로그인을 사용하여 서버에 로그인합니다. 서버는 PAP를 사용하여 클라이언트를 인증합니다.

green 네트워크는 클라이언트에게 알려지지 않습니다. 클라이언트는 직접 "green-net"을 지정하고 CHAP 인증 자격 증명을 제공해야만 green에 액세스할 수 있습니다. 또한 joe 및 mary 클라이언트만 정적 IP 주소를 사용하여 green 네트워크에 액세스할 수 있습니다.

예 8–3 액세스 서버를 위한 /etc/ppp/pppoe 파일

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
service purple-net
     device hme0,hme1
     pppd "require-pap login name purple-server purple-server:"
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

이 샘플에서는 액세스 서버에서 사용 가능한 서비스에 대해 설명합니다. 첫번째 서비스 섹션에서는 orange 네트워크의 서비스에 대해 설명합니다.

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
```

클라이언트는 hme0 및 hme1 인터페이스를 통해 orange 네트워크에 액세스합니다. pppd 명령에 제공되는 옵션으로 인해 서버가 잠재적 클라이언트에게 PAP 자격 증명을 요구해야 합니다. 또한 pppd 옵션은 pap-secrets 파일에 사용되는 대로 서버의 이름을 orange-server로 설정합니다.

purple 네트워크의 서비스 섹션은 네트워크 및 서버 이름만 제외하고 orange 네트워크의 서비스 섹션과 동일합니다.

다음 섹션에서는 green 네트워크의 서비스에 대해 설명합니다.

```
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

이 섹션에서는 클라이언트 액세스를 hme1 인터페이스로 제한합니다. pppd 명령에 제공되는 옵션으로 인해 서버가 잠재적 클라이언트에게 CHAP 자격 증명을 요구해야 합니다. 또한 pppd 옵션은 chap-secrets 파일에 사용될 대로 서버 이름을 green-server로 설정합니다. nowildcard 옵션은 green 네트워크의 존재 여부를 클라이언트에 알리지 않도록 지정합니다.

방금 설명한 이 액세스 서버 시나리오의 경우 다음 /etc/ppp/options 파일을 설정할 수 있습니다.

예 8–4 액세스 서버를 위한 /etc/ppp/options 파일

```
auth
proxyarp
nodefaultroute
name no-service    # don't authenticate otherwise
```

name no-service 옵션은 PAP 또는 CHAP 인증 중 일반적으로 검색되는 서버 이름을 대체합니다. 서버의 기본 이름은 /usr/bin/hostname 명령을 통해 검색되는 이름입니다. 이전 예에 있는 name 옵션은 서버의 이름을 no-service로 변경합니다. 이름 no-service는 pap 또는 chap-secrets 파일에서 검색될 확률이 적습니다. 이 작업을 수행하면 임의 사용자가 pppd를 실행하고 /etc/ppp/options에 설정된 auth 및 name 옵션을 대체하지 못하게 됩니다. 그러면 서버 이름이 no-service인 클라이언트에 대해 암호가 검색될 수 없기 때문에 pppd가 실패합니다.

액세스 서버 시나리오에는 다음 /etc/hosts 파일이 사용됩니다.

예 8–5 액세스 서버를 위한 /etc/hosts 파일

```
172.16.0.1    orange-server
172.17.0.1    purple-server
172.18.0.1    green-server
172.18.0.2    joes-pc
172.18.0.3    marys-pc
```

orange 및 purple 네트워크에 액세스하려고 시도하는 클라이언트에 대한 PAP 인증에 사용되는 /etc/ppp/pap-secrets 파일은 다음과 같습니다.

예 8–6 액세스 서버를 위한 /etc/ppp/pap-secrets 파일

```
* orange-server "" 172.16.0.2/16+
* purple-server "" 172.17.0.2/16+
```

CHAP 인증에 사용되는 /etc/ppp/chap-secrets 파일은 다음과 같습니다. joe 및 mary 클라이언트만 이 파일에 나열됩니다.

예 8–7 액세스 서버를 위한 /etc/ppp/chap-secrets 파일

```
 joe green-server "joe's secret" joes-pc
mary green-server "mary's secret" marys-pc
```

PPPoE 클라이언트 명령 및 파일

DSL 모뎀을 통해 PPP를 실행하려면 시스템이 PPPoE 클라이언트가 되어야 합니다. PPPoE를 실행하려면 인터페이스를 연결한 다음 pppoec 유틸리티를 사용하여 액세스 서버의 존재 여부를 "발견"해야 합니다. 그러면 클라이언트가 DSL 모뎀을 통해 PPPoE 터널을 만들어 PPP를 실행할 수 있게 됩니다.

PPPoE 클라이언트는 기존의 클라이언트-서버 모델에서 액세스 서버와 관련됩니다. PPPoE 터널은 다이얼 업 링크가 아니지만 거의 동일한 방식으로 구성되어 작동합니다.

PPPoE 클라이언트를 설정하는 명령 및 파일은 다음과 같습니다.

- 139 페이지 "/usr/sbin/sppptun 명령"
- 146 페이지 "/usr/lib/inet/pppoec 유틸리티"
- 146 페이지 "pppoe.so 공유 객체"
- 118 페이지 "/etc/ppp/peers/*peer-name* 파일"
- 113 페이지 "/etc/ppp/options 구성 파일"

/usr/lib/inet/pppoec 유틸리티

/usr/lib/inet/pppoec 유틸리티는 PPPoE 터널의 클라이언트측을 협상합니다. pppoec는 chat 유틸리티와 유사합니다. pppoec는 직접 호출하지 않습니다. 대신 pppd의 connect 옵션에 대한 인수로 /usr/lib/inet/pppoec를 시작합니다.

pppoe.so 공유 객체

pppoe.so는 PPPoE 기능을 액세스 서버 및 클라이언트에 제공하기 위해 PPPoE가 로드해야 하는 PPPoE 공유 객체입니다. pppoe.so 공유 객체는 MTU 및 MRU를 1492로 제한하고, 드라이버로부터의 패킷을 필터링하고, 런타임 PPPoE 메시지를 처리합니다.

클라이언트측에서 pppd는 사용자가 plugin pppoe.so 옵션을 지정할 때 pppoe.so를 로드합니다.

액세스 서버 피어를 정의하기 위한 /etc/ppp/peers/*peer-name* 파일

pppoec를 통해 발견된 액세스 서버를 정의할 때는 pppoec와 pppd 데몬 모두에 적용되는 옵션을 사용합니다. 액세스 서버를 위한 /etc/ppp/peers/*peer-name* 파일에 필요한 매개변수는 다음과 같습니다.

- sppptun – PPPoE 터널에 사용되는 직렬 장치의 이름입니다.
- plugin pppoe.so – pppoe.so 공유 객체를 로드하도록 pppd에 지시합니다.
- connect "/usr/lib/inet/pppoec *device*" – 연결을 시작합니다. 그러면 connect가 PPPoE에 연결된 인터페이스인 *device*를 통해 pppoec 유틸리티를 호출합니다.

/etc/ppp/peers/*peer-name* 파일의 나머지 매개변수는 서버의 PPP 링크에 적용되어야 합니다. 다이얼 아웃 시스템에서 /etc/ppp/peers/*peer-name*에 대해 사용할 것과 같은 옵션을 사용하십시오. PPP 링크에 필요한 옵션의 수를 최소한으로 제한하는 것이 좋습니다.

다음 예는 85 페이지 “PPPoE 액세스 서버 피어를 정의하는 방법”에 소개되어 있습니다.

예 8–8 원격 액세스 서버를 정의하기 위한 /etc/ppp/peers/*peer-name*

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

이 파일은 액세스 서버 dslserve에 대해 PPPoE 터널과 PPP 링크를 설정할 때 사용될 매개변수를 정의합니다. 포함되는 옵션은 다음과 같습니다.

옵션	설명
sppptun	sppptun을 직렬 장치의 이름으로 정의합니다.
plugin pppoe.so	pppoe.so 공유 객체를 로드하도록 pppd에 지시합니다.
connect "/usr/lib/inet/pppoec hme0"	pppoec를 실행하고 hme0을 PPPoE 터널 및 PPP 링크에 대한 인터페이스로 지정합니다.
noccp	링크에서 CCP 압축을 끕니다. **주 –** 많은 ISP가 독점 압축 알고리즘만 사용합니다. 공개적으로 사용 가능한 CCP 알고리즘을 끄면 협상 시간을 절약하고 드물기는 하지만 때로 발생하는 상호 운용성 문제를 방지할 수 있습니다.
noauth	pppd가 액세스 서버에 인증 자격 증명을 더 이상 요구하지 않게 만듭니다. 대부분의 ISP가 고객에게 인증 자격 증명을 제공하지 않습니다.
user Red	Red라는 이름을 클라이언트의 사용자 이름으로 설정합니다. 이 이름은 액세스 서버의 PAP 인증에 필요합니다.
password redsecret	redsecret을 PAP 인증을 위해 액세스 서버에 제공할 암호로 정의합니다.
noipdefault	0.0.0.0을 초기 IP 주소로 지정합니다.

옵션	설명
`defaultroute`	IPCP 협상 후에 기본 IPv4 경로를 설치하도록 `pppd`에 지시합니다. 링크가 인터넷에 대한 시스템의 링크인 경우(PPPoE 클라이언트에 해당) `/etc/ppp/peers/`*peer-name*에 `defaultroute`를 포함해야 합니다.

◆ ◆ ◆ 9 장

9 비동기 Solaris PPP에서 Solaris PPP 4.0으로 마이그레이션(작업)

이전 버전의 Oracle Solaris OS에는 다른 PPP 구현인 비동기 Solaris PPP(asppp)가 포함되어 있었습니다. asppp를 실행하는 피어를 최신 PPP 4.0으로 변환하려면 변환 스크립트를 실행해야 합니다. 이 장에서는 PPP 변환에 대한 다음 항목을 다룹니다.

- 149 페이지 “asppp 파일을 변환하기 전에”
- 152 페이지 “asppp2pppd 변환 스크립트 실행(작업)”

이 장에서는 샘플 asppp 구성을 사용하여 PPP 변환을 수행하는 방법에 대해 설명합니다. Solaris PPP 4.0과 asppp의 차이점에 대한 자세한 내용을 보려면 20 페이지 “사용할 Solaris PPP 버전”으로 이동하십시오.

asppp 파일을 변환하기 전에

변환 스크립트 /usr/sbin/asppp2pppd를 사용하여 표준 asppp 구성을 이루는 파일을 변환할 수 있습니다.

- /etc/asppp.cf – 비동기 PPP 구성 파일
- /etc/uucp/Systems – 원격 피어의 특징을 설명하는 UUCP 파일
- /etc/uucp/Devices – 로컬 시스템의 모뎀을 설명하는 UUCP 파일
- /etc/uucp/Dialers – /etc/uucp/Devices 파일에 설명된 모뎀에 사용될 로그인 절차가 포함된 UUCP 파일

asppp에 대한 자세한 내용은 *Solaris 8 System Administration Collection, Volume 3*(http://docs.sun.com에서 제공)을 참조하십시오.

/etc/asppp.cf 구성 파일의 예

152 페이지 “asppp에서 Solaris PPP 4.0으로 변환하는 방법”에 나와 있는 절차에는 다음 /etc/asppp.cf 파일이 사용됩니다.

```
#
ipadm create-if ipdptp0
ipadm create-addr -T static -a local=mojave,remote=gobi ipdptp0/ppaddr

path
 inactivity_timeout 120     # Approx. 2 minutes
    interface ipdptp0
    peer_system_name Pgobi    # The name we log in with (also in
                                  # /etc/uucp/Systems
```

이 파일에 포함된 매개변수는 다음과 같습니다.

`ifpadm create-if ipdptp0`
: `ipadm` 명령을 실행하여 `ipdptp0`이라는 인터페이스를 만듭니다.

`ipadm create-addr -T static -a local=mojave,remote=gobi ipdptp0/ppadd`
: `ipadm` 명령을 실행하여 PPP 인터페이스 `ipdptp0`(로컬 시스템 `mojave`에 있음)에서 원격 피어 `gobi`로의 링크를 구성합니다.

`inactivity_timeout 120`
: 2분 동안 작업이 없을 경우 회선을 종료합니다.

`interface ipdptp0`
: 비동기 PPP를 위해 다이얼 아웃 시스템에서 `ipdptp0` 인터페이스를 구성합니다.

`peer_system_name Pgobi`
: 원격 피어의 이름인 `Pgobi`를 제공합니다.

/etc/uucp/Systems 파일의 예

152 페이지 “asppp에서 Solaris PPP 4.0으로 변환하는 방법”에 나와 있는 절차에는 다음 `/etc/uucp/Systems` 파일이 사용됩니다.

```
#ident  "@(#)Systems    1.5  92/07/14 SMI"  /* from SVR4 bnu:Systems 2.4 */
#

# .
# .
Pgobi Any ACU 38400 15551212 in:--in: mojave word: sand
```

이 파일에 포함된 매개변수는 다음과 같습니다.

`Pgobi`	원격 피어의 호스트 이름으로 `Pgobi`를 사용합니다.
`Any ACU`	다이얼 아웃 시스템 `mojave`의 모뎀에 하루 중 임의의 시간에 `Pgobi`에 있는 모뎀과 링크를 설정하도록 지시합니다. Any ACU는 “`/etc/uucp/Devices` 파일에서 ACU를 찾을 것”을 의미합니다.
`38400`	38400을 링크의 최대 속도로 설정합니다.
`15551212`	`Pgobi`의 전화 번호를 제공합니다.

`in:–in: mojave word: sand`	Pgobi가 다이얼 아웃 시스템 `mojave`를 인증하는 데 필요한 로그인 스크립트를 정의합니다.

/etc/uucp/Devices 파일의 예

152 페이지 “asppp에서 Solaris PPP 4.0으로 변환하는 방법”에 나와 있는 절차에는 다음 `/etc/uucp/Devices` 파일이 사용됩니다.

```
#ident  "@(#)Devices  1.6  92/07/14 SMI"  /* from SVR4 bnu:Devices 2.7 */

.
.
#

TCP,et - - Any TCP -
.
.
#
ACU cua/b - Any hayes
# 0-7 are on a Magma 8 port card
Direct cua/0 - Any direct
Direct cua/1 - Any direct
Direct cua/2 - Any direct
Direct cua/3 - Any direct
Direct cua/4 - Any direct
Direct cua/5 - Any direct
Direct cua/6 - Any direct
Direct cua/7 - Any direct
# a is the console port (aka "tip" line)
Direct cua/a - Any direct
# b is the aux port on the motherboard
Direct cua/b - Any direct
# c and d are high speed sync/async ports
Direct cua/c - Any direct
Direct cua/d - Any direct
```

이 파일은 직렬 포트 `cua/b`에 연결된 모든 Hayes 모뎀을 지원합니다.

/etc/uucp/Dialers 파일의 예

152 페이지 “asppp에서 Solaris PPP 4.0으로 변환하는 방법”에 나와 있는 절차에는 다음 `/etc/uucp/Dialers` 파일이 사용됩니다.

```
#
#       <Much information about modems supported by Oracle Solaris UUCP>


penril    =W-P    "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
ventel    =&-%    "" \r\p\r\c $ k\c ONLINE!
```

```
vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE
develcon ""    "" \pr\ps\c est:\007 \E\D\e \n\007
micom    ""    "" \s\c NAME? \D\r\c GO
direct
#
#
#
#   Hayes Smartmodem -- modem should be set with the configuration
#   switches as follows:
#
#       S1 - UP        S2 - UP        S3 - DOWN    S4 - UP
#       S5 - UP        S6 - DOWN    S7 - ?        S8 - DOWN
#
hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT
```

<much more information about modems supported by Oraccle Solaris UUCP>

이 파일에는 /etc/uucp/Dialers 파일에서 지원되는 Hayes 모뎀을 비롯한 모든 유형의 모뎀에 대한 채트 스크립트가 포함되어 있습니다.

asppp2pppd 변환 스크립트 실행(작업)

/usr/sbin/asppp2pppd 스크립트는 /etc/asppp.cf의 PPP 정보와 PPP 관련 UUCP 파일을 Solaris PPP 4.0 파일의 적절한 위치로 복사합니다.

작업 필수 조건

그 다음 작업을 수행하기 전에 다음 작업을 완료해야 합니다.

- asppp 및 UUCP 구성 파일도 있는 시스템에 Oracle Solaris 릴리스 설치
- PPP 파일이 있는 시스템(예: mojave 시스템)에서 수퍼 유저 되기

▼ asppp에서 Solaris PPP 4.0으로 변환하는 방법

1 변환 스크립트를 시작합니다.

```
# /usr/sbin/asppp2pppd
```

변환 프로세스가 시작되고 다음 화면 출력이 제공됩니다.

```
This script provides only a suggested translation for your existing aspppd
configuration.  You will need to evaluate for yourself whether the translation
is appropriate for your operating environment.
Continue [Yn]?
```

2 "Y"를 입력하여 계속합니다.

다음 출력이 제공됩니다.

```
Chat cannot do echo checking; requests for this removed.
Adding 'noauth' to /etc/ppp/options

Preparing to write out translated configuration:
    1 chat file:
        1.  /etc/ppp/chat.Pgobi.hayes
    2 option files:
        2.  /etc/ppp/peers/Pgobi
        3.  /etc/ppp/options
    1 script file:
        4.  /etc/ppp/demand
```

새 Solaris PPP 4.0 파일이 생성되었습니다.

▼ 변환 결과를 보는 방법

변환 프로세스가 끝나면 `/usr/sbin/asppp2pppd` 변환 스크립트를 통해 만들어진 Solaris PPP 4.0 파일을 볼 수 있습니다. 이 스크립트는 다음 옵션 목록을 표시합니다.

```
Enter option number:
        1 - view contents of file on standard output
        2 - view contents of file using /usr/bin/less
        3 - edit contents of file using /usr/bin/vi
        4 - delete/undelete file from list
        5 - rename file in list
        6 - show file list again
        7 - escape to shell (or "!")
        8 - abort without saving anything
        9 - save all files and exit (default)
Option:
```

1 1을 입력하여 화면에서 파일 내용을 봅니다.

스크립트가 표시할 파일 수를 요청합니다.

```
File number (1 .. 4):
```

숫자는 이전의 2단계에 나와 있는 것과 같이 변환 프로세스 중 나열되는 변환된 파일의 수를 나타냅니다.

2 1을 입력하여 채트 파일 `/etc/ppp/chat.Pgobi.hayes`를 봅니다.

```
File number (1 .. 4):  1
"" \d\dA\p\pTE1V1X1Q0S2=255S12=255\r\c
OK\r ATDT\T\r\c
CONNECT \c
in:--in: mojave
word: sand
```

채트 스크립트에는 샘플 `/etc/uucp/Dialers` 파일의 hayes 행에 나타나는 모뎀 "채트" 정보가 포함되어 있습니다. `/etc/ppp/chat.Pgobi.hayes`에는 `Pgobi`의 로그인 절차(샘플

/etc/uucp/Systems 파일에 나타남)도 포함되어 있습니다. 채트 스크립트가 이제 /etc/ppp/chat.Pgobi.hayes 파일에 있습니다.

3 2를 입력하여 피어 파일인 /etc/ppp/peers/Pgobi를 봅니다.

```
File number (1 .. 4):  2
/dev/cua/b
38400
demand
idle 120
connect "/usr/bin/chat -f /etc/ppp/chat.Pgobi.hayes -T '15551212'"
user NeverAuthenticate
mojave:gobi
```

직렬 포트 정보(/dev/cua/b)는 /etc/uucp/Devices 파일에서 가져온 것입니다. 링크 속도, 유휴 시간, 인증 정보 및 피어 이름은 /etc/asppp.cf 파일에서 가져온 것입니다. "demand"는 다이얼 아웃 시스템이 피어 Pgobi에 연결하려고 할 때 호출할 "demand" 스크립트를 나타냅니다.

4 3을 입력하여 /etc/ppp/options 파일(다이얼 아웃 시스템 mojave에 대해 만들어짐)을 봅니다.

```
File number (1 .. 4):  3
#lock
noauth
```

/etc/ppp/options의 정보는 /etc/asppp.cf 파일에서 가져온 것입니다.

5 4를 입력하여 demand 스크립트의 내용을 봅니다.

```
File number (1 .. 4):  4
/usr/bin/pppd file /etc/ppp/peers/Pgobi
```

호출 시 이 스크립트는 pppd 명령을 실행한 다음 /etc/ppp/peers/Pgobi를 읽어 mojave와 Pgobi 간의 링크를 시작합니다.

6 9를 입력하여 만들어진 파일을 저장합니다. 그런 다음 변환 스크립트를 종료합니다.

◆ ◆ ◆ 10장

10 UUCP(개요)

이 장에서는 UNIX-to-UNIX Copy Program(UUCP) 및 해당 데몬에 대해 소개합니다. 다음 항목을 다룹니다.

UUCP는 컴퓨터에서 파일을 전송하고 서로 메일을 교환할 수 있도록 합니다. 또한 이 프로그램을 통해 컴퓨터에서 Usenet과 같은 대규모 네트워크에 참가할 수 있습니다.

Oracle Solaris OS는 UUCP의 BNU(기본 네트워크 유틸리티) 버전을 제공합니다. 이 버전은 HoneyDanBer UUCP라고도 합니다. *UUCP*라는 용어는 시스템을 구성하는 파일 및 유틸리티의 전체 범위를 나타냅니다. `uucp`는 이 시스템에 포함되는 한 요소입니다. 컴퓨터 간에 파일을 복사하는 데 사용되는 유틸리티(`uucp` 및 `uuto`)에서 원격 로그인 및 명령 실행에 사용되는 유틸리티(`cu` 및 `uux`)에 이르기까지 다양한 UUCP 유틸리티가 있습니다.

UUCP 하드웨어 구성

UUCP는 다음과 같은 하드웨어 구성을 지원합니다.

직접 링크 — 두 시스템의 직렬 포트 간에 RS-232 케이블을 연결하여 다른 컴퓨터로의 직접 링크를 만들 수 있습니다. 직접 링크는 두 컴퓨터가 정기적으로 통신하며 15미터 이내 등 서로 물리적으로 가까운 거리에 있는 경우 유용합니다. 제한 거리 모뎀을 사용하면 두 컴퓨터 사이의 거리를 어느 정도 늘릴 수 있습니다.

전화선 — 고속 모뎀 등의 ACU(자동 호출 단위)를 사용하면 시스템에서 표준 전화선을 통해 다른 컴퓨터와 통신할 수 있습니다. 모뎀은 UUCP에서 요청하는 전화 번호로 전화를 겁니다. 수신자 시스템에는 수신 전화를 받을 수 있는 모뎀이 있어야 합니다.

네트워크 UUCP는 TCP/IP 또는 다른 프로토콜 제품군을 실행하는 네트워크를 통해서도 통신할 수 있습니다. 네트워크에서 호스트로 설정된 컴퓨터는 네트워크에 연결된 다른 호스트에 연결할 수 있습니다.

이 장에서는 UUCP 하드웨어가 이미 어셈블 및 구성되었다고 가정합니다. 모뎀을 설정해야 하는 경우 해당 모뎀에 포함된 설명서를 참조하십시오.

UUCP 소프트웨어

UUCP 소프트웨어는 Oracle Solaris 설치 프로그램을 실행하고 전체 배포를 선택하면 자동으로 포함됩니다. `pkgadd`를 사용하여 UUCP 소프트웨어를 추가할 수도 있습니다. UUCP 프로그램은 세 가지 범주인 데몬, 관리 프로그램 및 사용자 프로그램으로 구분할 수 있습니다.

UUCP 데몬

UUCP 시스템에는 `uucico`, `uuxqt`, `uusched` 및 `in.uucpd`의 4개 데몬이 있습니다. 이러한 데몬은 UUCP 파일 전송 및 명령 실행을 처리합니다. 필요한 경우 셸에서 명령을 실행할 수도 있습니다.

`uucico` 링크에 사용되는 장치를 선택하고, 원격 컴퓨터에 대한 링크를 설정하고, 필요한 로그인 시퀀스 및 권한 확인을 수행합니다. 또한 `uucico`는 데이터 파일을, 실행 파일 및 로그로부터의 결과를 전송하고 사용자에게 전송 완료 메일을 보내 통지합니다. `uucico`는 UUCP 로그인 계정의 "로그인 셸"로 작동합니다. 로컬 `uucico` 데몬은 원격 시스템을 호출할 때 세션 중에 원격 `uucico` 데몬과 직접 통신합니다.

모든 필수 파일을 만들고 나면 `uucp`, `uuto` 및 `uux` 프로그램은 `uucico` 데몬을 실행하여 원격 컴퓨터에 연결합니다. `uusched` 및 `Uutry`는 모두 `uucico`를 실행합니다. 자세한 내용은 `uucico`(1M) 매뉴얼 페이지를 참조하십시오.

`uuxqt` 원격 실행 요청을 실행합니다. 이 데몬은 스풀 디렉토리에서 원격 컴퓨터로부터 발송된 실행 파일(이름이 항상 `X.`**파일**로 지정됨)을 검색합니다. `X.`**파일** 파일이 있으면 `uuxqt`는 해당 파일을 열어 실행에 필요한 데이터 파일 목록을 가져옵니다. 그런 다음 `uuxqt`는 필수 데이터 파일을 사용 및 액세스할 수 있는지를 확인합니다. 파일을 사용할 수 있으면 `uuxqt`는 `Permissions` 파일에서 요청된 명령을 실행할 권한이 있는지 확인합니다. `uuxqt` 데몬은 `uudemon.hour` 셸 스크립트를 통해 실행되며, 이 스크립트는 `cron`을 통해 시작됩니다. 자세한 내용은 `uuxqt`(1M) 매뉴얼 페이지를 참조하십시오.

`uusched` 스풀 디렉토리에서 대기열에 있는 작업을 예약합니다. `uusched`는 부트 시에 `uudemon.hour` 셸 스크립트를 통해 처음 실행되며, 이 스크립트는 `cron`을

통해 시작됩니다. 자세한 내용은 uusched(1M) 매뉴얼 페이지를 참조하십시오. uucico 데몬을 시작하기 전에 uusched는 원격 컴퓨터가 호출되는 순서를 무작위화합니다.

in.uucpd 네트워크를 통한 UUCP 연결을 지원합니다. 원격 호스트의 inetd는 UUCP 연결을 설정할 때마다 in.uucpd를 호출합니다. 그러면 uucpd가 로그인 이름 프롬프트를 표시합니다. 호출하는 호스트의 uucico는 로그인 이름으로 응답해야 합니다. 그리고 나면 in.uucpd가 암호 프롬프트를 표시합니다. 암호가 필요하지 않은 경우에는 제외합니다. 자세한 내용은 in.uucpd(1M) 매뉴얼 페이지를 참조하십시오.

UUCP 관리 프로그램

대부분의 UUCP 관리 프로그램은 /usr/lib/uucp에 있습니다. 가장 기본적인 데이터베이스 파일은 /etc/uucp에 있습니다. 단, uulog는 /usr/bin에 있습니다. uucp 로그인 ID의 홈 디렉토리는 /usr/lib/uucp입니다. su 또는 login을 통해 관리 프로그램을 실행할 때는 uucp 사용자 ID를 사용합니다. 사용자 ID는 프로그램 및 스풀된 데이터 파일을 소유합니다.

uulog 지정된 컴퓨터의 로그 파일 컨텐츠를 표시합니다. 로그 파일은 시스템이 통신하는 각 원격 컴퓨터에 대해 만들어집니다. 로그 파일에는 각 uucp, uuto 및 uux 사용이 기록됩니다. 자세한 내용은 uucp(1C) 매뉴얼 페이지를 참조하십시오.

uucleanup 스풀 디렉토리를 정리합니다. uucleanup은 일반적으로 uudemon.cleanup 셸 스크립트에서 실행되며, 이 스크립트는 cron을 통해 시작됩니다. 자세한 내용은 uucleanup(1M) 매뉴얼 페이지를 참조하십시오.

Uutry 통화 처리 기능을 테스트하고 적절한 디버깅을 수행합니다. Uutry는uucico 데몬을 호출하여 시스템과 지정한 원격 컴퓨터 간에 통신 링크를 설정합니다. 자세한 내용은 Uutry(1M) 매뉴얼 페이지를 참조하십시오.

uucheck UUCP 디렉토리, 프로그램 및 지원 파일이 있는지 확인합니다. uucheck는 /etc/uucp/Permissions 파일의 특정 부분에 명백한 구문 오류가 있는지도 확인할 수 있습니다. 자세한 내용은 uucheck(1M) 매뉴얼 페이지를 참조하십시오.

UUCP 사용자 프로그램

UUCP 사용자 프로그램은 /usr/bin에 있습니다. 특수한 권한이 없어도 이러한 프로그램을 사용할 수 있습니다.

cu	두 시스템에 동시 로그인할 수 있도록 원격 컴퓨터에서 시스템에 연결합니다. cu를 실행하면 두 시스템 중 하나에서 파일을 전송하거나 명령을 실행할 수 있으며 초기 링크가 삭제되지 않습니다. 자세한 내용은 cu(1C) 매뉴얼 페이지를 참조하십시오.
uucp	시스템 간에 파일을 복사할 수 있습니다. uucp는 작업 파일과 데이터 파일을 만들고, 전송할 작업을 대기열에 넣고, uucico 데몬을 호출합니다. 이 데몬은 원격 컴퓨터 연결을 시도합니다. 자세한 내용은 uucp(1C) 매뉴얼 페이지를 참조하십시오.
uuto	파일을 로컬 시스템에서 원격 시스템의 공개 스풀 디렉토리 /var/spool/uucppublic/receive로 복사합니다. 원격 시스템의 모든 액세스 가능 디렉토리에 파일을 복사하는 데 사용할 수 있는 uucp와는 달리, uuto는 적절한 스풀 디렉토리에 파일을 저장하고 원격 사용자에게 uupick을 사용하여 파일을 선택하라는 메시지를 표시합니다. 자세한 내용은 uuto(1C) 매뉴얼 페이지를 참조하십시오.
uupick	uuto를 사용하여 컴퓨터로 파일을 전송할 때 /var/spool/uucppublic/receive의 파일을 검색합니다. uuto(1C) 매뉴얼 페이지를 참조하십시오.
uux	원격 시스템에서 명령을 실행하는 데 필요한 작업, 데이터 및 실행 파일을 만듭니다. 자세한 내용은 uux(1C) 매뉴얼 페이지를 참조하십시오.
uustat	요청된 전송(uucp, uuto 또는 uux)의 상태를 표시합니다. uustat를 통해 대기열에 있는 전송을 제어할 수도 있습니다. 자세한 내용은 uustat(1C) 매뉴얼 페이지를 참조하십시오.

UUCP 데이터베이스 파일

UUCP 데이터베이스를 구성하는 파일의 구성은 UUCP 설정에서 중요한 요소입니다. 이러한 파일은 /etc/uucp 디렉토리에 있습니다. 시스템에서 UUCP 또는 asppp를 설정하려면 이러한 파일을 편집해야 합니다. 이 파일에는 다음이 포함됩니다.

Config	변수 매개변수 목록이 포함되어 있습니다. 이러한 매개변수를 수동으로 설정하여 네트워크를 구성할 수 있습니다.
Devconfig	네트워크 통신을 구성하는 데 사용됩니다.
Devices	네트워크 통신을 구성하는 데 사용됩니다.
Dialcodes	Systems 파일 항목의 전화 번호 필드에서 사용할 수 있는 다이얼 코드 약어가 포함되어 있습니다. Dialcodes는 반드시 사용해야 하는 것은 아니지만 asppp와 UUCP에서 모두 사용할 수 있습니다.
Dialers	모뎀과 협상하여 원격 컴퓨터와의 연결을 설정하는 데 필요한 문자열이 포함되어 있습니다. Dialers는 asppp와 UUCP에서 모두 사용됩니다.

`Grades`	작업 등급 및 각 작업 등급과 연관된 권한을 정의합니다. 사용자는 원격 컴퓨터 대기열에 작업을 넣기 위해 권한을 지정할 수 있습니다.
`Limits`	시스템에서 허용되는 동시 `uucico`, `uuxqt` 및 `uusched`의 최대 수를 정의합니다.
`Permissions`	시스템에서 명령을 실행하거나 파일을 전송하려고 시도하는 원격 호스트에 대해 부여되는 액세스 레벨을 정의합니다.
`Poll`	시스템에서 폴링할 시스템과 폴링 시간을 정의합니다.
`Sysfiles`	`uucico` 및 `cu`에서 사용할 서로 다른 파일이나 여러 파일을 `Systems`, `Devices` 및 `Dialers` 파일에 지정합니다.
`Sysname`	TCP/IP 호스트 이름과 함께 시스템에 대해 고유한 UUCP 이름을 정의할 수 있습니다.
`Systems`	`uucico` 데몬, `cu` 및 `asppp`에서 원격 컴퓨터에 대한 링크를 설정하는 데 필요한 정보가 포함되어 있습니다. 이 정보에는 다음이 포함됩니다. ■ 원격 호스트의 이름 ■ 원격 호스트와 연관된 연결 장치의 이름 ■ 호스트에 연결할 수 있는 시간 ■ 전화 번호 ■ 로그인 ID ■ 암호

기타 여러 파일은 지원 데이터베이스의 일부분으로 간주될 수는 있지만 링크를 설정하고 파일을 전송하는 데 직접 사용되지는 않습니다.

UUCP 데이터베이스 파일 구성

UUCP 데이터베이스는 158 페이지 “UUCP 데이터베이스 파일”에 나와 있는 파일로 구성됩니다. 그러나 기본 UUCP 구성에는 다음과 같은 중요 파일만 포함됩니다.

- `/etc/uucp/Systems`
- `/etc/uucp/Devices`
- `/etc/uucp/Dialers`

`asppp`는 UUCP 데이터베이스 중 일부를 사용하므로 `asppp`를 구성하려면 최소한 이와 같은 중요 데이터베이스 파일에 대해 알고 있어야 합니다. 이러한 데이터베이스 파일을 구성하고 나면 UUCP 관리를 간단하게 수행할 수 있습니다. 일반적으로는 `Systems` 파일을 먼저 편집한 후에 `Devices` 파일을 편집합니다. 기본 파일에 없는 전화 걸기를 추가하려는 경우가 아니면 보통 기본 `/etc/uucp/Dialers` 파일을 사용할 수 있습니다. 또한 기본 UUCP 및 `asppp` 구성에 대해 다음 파일을 사용할 수도 있습니다.

- `/etc/uucp/Sysfiles`
- `/etc/uucp/Dialcodes`

- `/etc/uucp/Sysname`

이러한 파일은 서로 긴밀하게 연관되어 함께 사용되므로 해당 컨텐츠를 모두 파악한 후에 파일을 변경해야 합니다. 특정 파일의 항목을 변경하는 경우 다른 파일의 관련 항목을 변경해야 할 수 있습니다. 158 페이지 "UUCP 데이터베이스 파일"에 나와 있는 나머지 파일은 크게 영향을 받지 않습니다.

주 – `asppp`는 이 절에서 설명하는 파일만 사용합니다. 즉, `asppp`는 다른 UCCP 데이터베이스 파일을 사용하지 않습니다.

◆ ◆ ◆ 11장

11 UUCP 관리(작업)

이 장에서는 시스템과 관련된 데이터베이스 파일을 수정한 후에 UUCP 작업을 시작하는 방법에 대해 설명합니다. 이 장에는 다음과 같이 Oracle Solaris OS를 실행하는 시스템에서 UUCP를 설정 및 유지 관리하기 위한 절차 및 문제 해결 정보가 포함되어 있습니다.

UUCP 관리(작업 맵)

다음 표에서는 이 장에서 다루는 절차에 대한 포인터와 각 절차의 간단한 설명이 나와 있습니다.

표 11–1 UUCP 관리용 작업 맵

작업	설명	수행 방법
원격 시스템이 시스템에 액세스하도록 허용	시스템 액세스가 허용되는 시스템을 식별하기 위한 항목을 추가하려면 /etc/passwd 파일을 편집합니다.	162 페이지 “UUCP 로그인을 추가하는 방법”
UUCP 시작	제공된 셸 스크립트를 사용하여 UUCP를 시작합니다.	163 페이지 “UUCP를 시작하는 방법”
TCP/IP와 함께 작동하도록 UUCP 설정	TCP/IP에 대해 UUCP를 활성화하려면 /etc/inetd.conf 및 /etc/uucp/Systems 파일을 편집합니다.	165 페이지 “TCP/IP에 대해 UUCP를 활성화하는 방법”
몇 가지 일반적인 UUCP 문제 해결	진단 단계를 수행하여 고장난 모뎀 또는 ACU를 확인합니다.	167 페이지 “고장난 모뎀이나 ACU를 확인하는 방법”

표 11–1 UUCP 관리용 작업 맵 (계속)

작업	설명	수행 방법
	진단 단계를 수행하여 전송을 디버그합니다.	168 페이지 "전송을 디버그하는 방법"

UUCP 로그인 추가

원격 시스템에서 받는 UUCP(uucico) 요청을 올바르게 처리하려면 시스템의 각 시스템에 로그인이 있어야 합니다.

▼ UUCP 로그인을 추가하는 방법

원격 시스템의 시스템 액세스를 허용하려면 다음과 같이 /etc/passwd 파일에 대한 항목을 추가해야 합니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **/etc/passwd 파일을 편집하여 시스템 액세스가 허용되는 시스템을 식별하기 위한 항목을 추가합니다.**

UUCP 연결을 통해 시스템에 액세스할 수 있도록 허용되는 원격 시스템에 대한 /etc/passwd 파일에는 일반적으로 다음 항목을 추가합니다.

```
Ugobi:*:5:5:gobi:/var/spool/uucppublic:/usr/lib/uucp/uucico
```

원격 시스템의 로그인 이름은 대문자 U 뒤에 시스템 이름이 오는 형식입니다. 이름은 8자 이내여야 합니다. 그렇지 않은 경우에는 이름을 자르거나 축약해야 합니다.

위 항목은 Ugobi의 로그인 요청에 대해 /usr/lib/uucp/uucico로 대답함을 보여줍니다. 홈 디렉토리는 /var/spool/uucppublic입니다. 암호는 /etc/shadow 파일에서 가져옵니다. 원격 시스템의 UUCP 관리자와 함께 암호와 로그인 이름을 조정해야 합니다. 원격 관리자는 원격 시스템의 Systems 파일에 로그인 이름과 암호화되지 않은 암호가 포함된 적절한 항목을 추가해야 합니다.

3 **시스템 이름은 다른 시스템의 UUCP 관리자와 함께 조정합니다.**

마찬가지로, UUCP를 통해 연결하려는 모든 컴퓨터의 UUCP 관리자와 함께 시스템 이름과 암호를 조정해야 합니다.

UUCP 시작

UUCP에는 원격 시스템을 폴링하고, 전송을 다시 예약하고, 오래된 로그 파일과 실패한 전송을 정리하는 4개의 셸 스크립트가 포함되어 있습니다. 이러한 스크립트는 다음과 같습니다.

- `uudemon.poll`
- `uudemon.hour`
- `uudemon.admin`
- `uudemon.cleanup`

이러한 셸 스크립트를 정기적으로 실행하여 UUCP가 원활하게 실행되는지 확인해야 합니다. 스크립트를 실행할 `crontab` 파일은 전체 설치를 선택하는 경우 Oracle Solaris 설치 프로세스의 일부분으로 `/usr/lib/uucp/uudemon.crontab`에서 자동으로 만들어집니다. 그렇지 않으면 UUCP 패키지를 설치할 때 파일이 만들어집니다.

UUCP 셸 스크립트를 수동으로 실행할 수도 있습니다. 특정 시스템용으로 조정할 수 있는 프로토타입 `uudemon.crontab` 파일은 다음과 같습니다.

```
#
#ident  "@(#)uudemon.crontab    1.5     97/12/09 SMI"
#
# This crontab is provided as a sample. For systems
# running UUCP edit the time schedule to suit, uncomment
# the following lines, and use crontab(1) to activate the
# new schedule.
#
#48 8,12,16 * * * /usr/lib/uucp/uudemon.admin
#20 3 * * * /usr/lib/uucp/uudemon.cleanup
#0 * * * * /usr/lib/uucp/uudemon.poll
#11,41 * * * * /usr/lib/uucp/uudemon.hour
```

주 – 기본적으로 UUCP 작업은 사용 안함으로 설정됩니다. UUCP를 사용으로 설정하려면 시간 일정을 편집하고 `uudemon.crontab` 파일에서 해당 행의 주석 처리를 해제합니다.

▼ UUCP를 시작하는 방법

`uudemon.crontab` 파일을 활성화하려면 다음을 수행합니다.

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **`/usr/lib/uucp/uudemon.crontab` 파일을 편집하고 필요한 대로 항목을 변경합니다.**

3. **다음 명령을 실행하여 `uudemon.crontab` 파일을 활성화합니다.**

   ```
   crontab < /usr/lib/uucp/uudemon.crontab
   ```

uudemon.poll 셸 스크립트

기본 uudemon.poll 셸 스크립트는 /etc/uucp/Poll 파일을 1시간마다 읽습니다. Poll 파일의 시스템이 폴링되도록 예약되어 있으면 작업 파일(C. *sysnxxxx*)이 /var/spool/uucp/ *nodename* 디렉토리에 저장됩니다. *nodename*은 시스템의 UUCP 노드 이름을 나타냅니다.

셸 스크립트는 uudemon.hour 전에 1시간마다 실행되도록 예약되므로 uudemon.hour를 호출하면 작업 파일이 해당 위치에 배치됩니다.

uudemon.hour 셸 스크립트

기본 uudemon.hour 셸 스크립트는 다음을 수행합니다.

- uusched 프로그램을 호출하여 처리되지 않은 작업 파일(C.)에 대한 스풀 디렉토리를 검색합니다. 그런 다음 스크립트는 이러한 파일을 원격 파일로 전송하도록 예약합니다.
- uuxqt 데몬을 호출하여 컴퓨터로 전송되었으며 전송 시 처리되지 않은 실행 파일(X.)에 대한 스풀 디렉토리를 검색합니다.

기본적으로 uudemon.hour는 시간당 두 번 실행됩니다. 원격 시스템에 대한 호출 오류율이 높을 것으로 예상되면 uudemon.hour 실행 빈도를 높일 수 있습니다.

uudemon.admin 셸 스크립트

기본 uudemon.admin 셸 스크립트는 다음을 수행합니다.

- p 및 q 옵션을 포함하여 uustat 명령을 실행합니다. q는 대기열에 있는 작업 파일(C.), 데이터 파일(D.) 및 실행 파일(X.)의 상태를 보고합니다. p는 잠금 파일(/var/spool/locks)에 나열된 네트워킹 프로세스에 대한 프로세스 정보를 인쇄합니다.
- mail 명령을 사용하여 결과 상태 정보를 uucp 관리 로그로 보냅니다.

uudemon.cleanup 셸 스크립트

기본 uudemon.cleanup 셸 스크립트는 다음을 수행합니다.

- /var/uucp/.Log 디렉토리에서 개별 시스템의 로그 파일을 수집하여 병합한 다음 기타 오래된 로그 정보와 함께 /var/uucp/.Old 디렉토리에 저장합니다.
- 7일 이상 된 작업 파일(C.), 7일 이상 된 데이터 파일(D.) 및 2일 이상 된 실행 파일(X.)을 스풀 파일에서 제거합니다.
- 보낸 사람에게 배달할 수 없는 메일을 반송합니다.

- 현재 날짜 동안 수집된 상태 정보의 요약을 UUCP 관리 로그인(uucp)에게 메일로 보냅니다.

TCP/IP를 통해 UUCP 실행

TCP/IP 네트워크에서 UUCP를 실행하려면 이 절에서 설명하는 것처럼 몇 가지 사항을 수정해야 합니다.

▼ TCP/IP에 대해 UUCP를 활성화하는 방법

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 /etc/uucp/Systems 파일을 편집하여 항목에 다음 필드가 포함되도록 합니다.

System-Name Time TCP Port networkname Standard-Login-Chat

일반적인 항목은 다음과 같습니다.

```
rochester Any TCP - ur-seneca login: Umachine password: xxx
```

networkname 필드는 TCP/IP 호스트 이름을 명시적으로 지정할 수 있도록 합니다. 일부 사이트에서는 이 기능이 중요합니다. 이전 예에서 사이트에는 UUCP 노드 이름 `rochester`가 있습니다. 이 이름은 해당 TCP/IP 호스트 이름 `ur-seneca`와는 다릅니다. 또한 완전히 다른 시스템에서 UUCP를 쉽게 실행하고 TCP/IP 호스트 이름 `rochester`를 소유할 수 있습니다.

`Systems` 파일의 Port 필드에는 `-` 항목이 있어야 합니다. 이 구문은 항목을 `uucp`로 나열하는 것에 해당합니다. 거의 모든 상황에서 *networkname*은 시스템 이름과 같고 Port 필드는 `-`입니다(즉, `services` 데이터베이스에서 표준 uucp 포트 사용). `in.uucpd` 데몬은 원격 시스템이 해당 로그인 및 암호를 인증용으로 보낸다고 가정하며, `in.uucpd`는 `getty` 및 `login`과 비슷하게 로그인 및 암호 프롬프트를 표시합니다.

3 /etc/inet/services 파일을 편집하여 UUCP용 포트를 설정합니다.

```
uucp    540/tcp    uucpd        # uucp daemon
```

항목은 변경할 필요가 없습니다. 그러나 시스템에서 이름 서비스로 NIS를 실행하는 경우에는 `svc:/system/name-service/switch` 서비스의 `config/service`가 `nis` 전에 `files`를 확인하도록 해야 합니다. `config/service` 등록 정보가 정의되어 있지 않으면 `config/default` 등록 정보를 확인합니다.

4 UUCP가 사용으로 설정되어 있는지 확인합니다.

```
# svcs network/uucp
```

UUCP 서비스는 서비스 관리 기능을 통해 관리됩니다. 이 서비스의 상태를 질의하려면 svcs 명령을 사용하면 됩니다. 서비스 관리 기능의 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, "서비스 관리(개요)"를 참조하십시오.

5 **(옵션) 필요한 경우 다음을 입력하여 UUCP를 사용으로 설정합니다.**

```
# inetadm -e network/uucp
```

UUCP 보안 및 유지 관리

UUCP를 설정한 후에는 유지 관리를 쉽게 수행할 수 있습니다. 이 절에서는 보안, 유지 관리 및 문제 해결과 관련된 진행 중인 UUCP 작업에 대해 설명합니다.

UUCP 보안 설정

기본 /etc/uucp/Permissions 파일은 UUCP 링크에 대한 최대 보안 레벨을 제공합니다. 기본 Permissions 파일에는 항목이 없습니다.

각 원격 시스템에 대해 추가 매개변수를 설정하여 다음을 정의할 수 있습니다.

- 원격 시스템에서 사용자 시스템의 파일을 받을 수 있는 방식
- 원격 시스템에 읽기 및 쓰기 권한이 있는 디렉토리
- 원격 시스템에서 원격 실행에 사용할 수 있는 명령

일반적인 Permissions 항목은 다음과 같습니다.

```
MACHINE=datsun LOGNAME=Udatsun VALIDATE=datsun
COMMANDS=rmail REQUEST=yes SENDFILES=yes
```

이 항목은 시스템의 모든 위치가 아닌 "일반" UUCP 디렉토리로 파일을 보내고 해당 디렉토리에서 파일을 받을 수 있도록 합니다. 또한 이 항목은 로그인 시 UUCP 사용자 이름을 검증하도록 합니다.

정기 UUCP 유지 관리

UUCP에서는 많은 유지 관리 작업을 수행하지 않아도 됩니다. 그러나 163 페이지 "UUCP를 시작하는 방법" 절에 설명된 대로 crontab 파일이 있는지는 확인해야 합니다. 구체적으로는 메일 파일 및 공개 디렉토리의 확장을 파악해야 합니다.

UUCP에 대해 전자 메일 보내기

UUCP 프로그램과 스크립트에 의해 생성되는 모든 전자 메일 메시지는 사용자 ID uucp에게 발송됩니다. 해당 사용자만큼 자주 로그인하지 않는 경우에는 메일이 누적되어 디스크 공간을 많이 사용하는 것을 모를 수도 있습니다. 이 문제를 해결하려면

/etc/mail/aliases에 별칭을 만들고 전자 메일을 root 또는 UUCP 유지 관리 담당자(자신이나 다른 사람)에게로 재지정합니다. aliases 파일을 수정한 후에는 newaliases 명령을 실행해야 합니다.

UUCP 공개 디렉토리

/var/spool/uucppublic 디렉토리는 UUCP에서 기본적으로 파일을 복사할 수 있는 모든 시스템의 위치 중 하나입니다. 모든 사용자는 해당 디렉토리에서 /var/spool/uucppublic을 변경하는 권한과 파일을 읽고 쓰는 권한을 가집니다. 그러나 디렉토리에 고정 비트가 설정되어 있으므로 디렉토리 모드는 01777입니다. 따라서 사용자는 해당 디렉토리로 복사한 파일(uucp에 속함)을 제거할 수 없습니다. root 또는 uucp로 로그인한 UUCP 관리자만 이 디렉토리에서 파일을 제거할 수 있습니다. 이 디렉토리에서 파일이 통제할 수 없을 정도로 누적되지 않도록 하려면 디렉토리의 파일을 정기적으로 제거해야 합니다.

사용자가 이러한 유지 관리 작업을 수행하기 어려운 경우에는 보안상의 이유로 설정되는 고정 비트를 제거하는 대신 uuto 및 uupick을 사용하도록 합니다. uuto 및 uupick 사용 지침은 uuto(1C) 매뉴얼 페이지를 참조하십시오. 디렉토리의 모드를 단일 사용자 그룹으로만 제한할 수도 있습니다. 특정 사용자가 디스크를 모두 사용하지 않도록 하려면 UUCP의 디스크 액세스를 거부할 수도 있습니다.

UUCP 문제 해결

이 절차에서는 일반적인 UUCP 문제를 해결하는 방법에 대해 설명합니다.

▼ 고장난 모뎀이나 ACU를 확인하는 방법

여러 가지 방법으로 모뎀이나 기타 ACU가 정상적으로 작동하지 않는지를 확인할 수 있습니다.

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **다음 명령을 실행하여 연결 실패의 횟수와 이유를 표시합니다.**

   ```
   # uustat -q
   ```

3. **특정 전화선을 호출하여 해당 호출 시도에 대한 디버깅 정보를 인쇄합니다.**

   해당 행은 /etc/uucp/Devices 파일에서 direct로 정의해야 합니다. 전화선이 자동 전화 걸기에 연결되거나 장치를 direct로 설정해야 하는 경우에는 명령줄 끝에 전화 번호를 추가해야 합니다. 다음을 입력합니다.

   ```
   # cu -d -l line
   ```

*line*은 /dev/cua/a입니다.

▼ 전송을 디버그하는 방법

특정 시스템에 연결할 수 없는 경우에는 Uutry 및 uucp를 사용하여 해당 시스템에 대한 통신을 확인할 수 있습니다.

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 연결을 시도합니다.

```
# /usr/lib/uucp/Uutry -r machine
```

*machine*은 연결할 수 없는 시스템의 호스트 이름으로 대체합니다. 이 명령은 다음을 수행합니다.

- 디버깅과 함께 전송 데몬(uucico)을 시작합니다. 작업을 수행하는 사용자가 root이면 추가 디버깅 정보를 확인할 수 있습니다.
- 디버깅 출력을 /tmp/*machine*으로 보냅니다.
- 다음 명령을 실행하여 디버깅 출력을 터미널로 출력합니다.

  ```
  # tail -f
  ```

  출력을 종료하려면 Ctrl+C를 누릅니다. 출력을 저장하려면 /tmp/*machine*에서 출력을 복사할 수 있습니다.

3 Uutry를 실행해도 문제를 확인할 수 없으면 작업을 대기열에 추가해 보십시오.

```
# uucp -r file machine\!/dir/file
```

file 전송할 파일의 이름을 사용합니다.

machine 복사 대상 시스템의 이름을 사용합니다.

/dir/file 다른 시스템에 대해 파일 위치를 지정합니다.

4 다음 명령을 실행합니다.

```
# Uutry
```

그래도 문제를 해결할 수 없으면 해당 지역의 지원 담당자에게 문의해야 할 수 있습니다. 문제 진단에 도움이 되는 디버깅 출력을 저장합니다.

주 – `-x` *n* 옵션을 통해 `Uutry`에서 제공하는 디버그 레벨을 높이거나 낮출 수도 있습니다. *n*이 디버그 레벨을 나타냅니다. `Uutry` 의 기본 디버그 레벨은 5입니다.

디버그 레벨 3에서는 연결 설정 시간 및 방법에 대한 기본적인 정보를 제공하지만, 전송에 대한 많은 정보가 제공되지는 않습니다. 그러나 디버그 레벨 9에서는 전송 프로세스에 대한 모든 정보가 제공됩니다. 디버깅은 전송의 양쪽 끝에서 모두 수행됩니다. 비교적 많은 양의 텍스트에 대해 5보다 높은 레벨을 사용하려는 경우에는 다른 사이트 관리자와 논의하여 레벨 변경 여부를 결정하십시오.

UUCP `/etc/uucp/Systems` 파일 확인

특정 시스템에 연결하는 데 문제가 있으면 `Systems` 파일에 최신 정보가 포함되어 있는지 확인합니다. 시스템에 대해 오래되었을 수 있는 일부 정보는 다음과 같습니다.

- 전화 번호
- 로그인 ID
- Password

UUCP 오류 메시지 확인

UUCP의 오류 메시지는 `ASSERT` 및 `STATUS`의 두 가지 유형입니다.

- 프로세스가 중지되면 `ASSERT` 오류 메시지가 `/var/uucp/.Admin/errors`에 기록됩니다. 이러한 메시지에는 파일 이름(`sccsid`), 행 번호 및 텍스트가 포함됩니다. 보통 시스템 문제가 발생하면 이러한 메시지가 생성됩니다.
- `STATUS` 오류 메시지는 `/var/uucp/.Status` 디렉토리에 저장됩니다. 이 디렉토리에는 컴퓨터에서 통신을 시도하는 각 원격 컴퓨터에 대한 별도의 파일이 포함되어 있습니다. 이러한 파일에는 시도한 통신에 대한 상태 정보와 통신 성공 여부가 포함되어 있습니다.

기본 정보 확인

여러 명령을 사용하여 기본 네트워킹 정보를 확인할 수 있습니다.

- `uuname` 명령을 사용하여 시스템이 연결할 수 있는 시스템을 나열합니다.
- `uulog` 명령을 사용하여 특정 호스트에 대한 로그 디렉토리의 컨텐츠를 표시합니다.
- `uucheck -v` 명령을 사용하여 `uucp`에 필요한 파일 및 디렉토리가 있는지 확인합니다. 또한 이 명령은 `Permissions` 파일을 확인하여 사용자가 설정한 권한에 대한 정보를 표시합니다.

◆ ◆ ◆ 12 장

12 UUCP(참조)

이 장에서는 UUCP 작업에 대한 참조 정보를 제공합니다. 다음 항목을 다룹니다.

UUCP /etc/uucp/Systems 파일

/etc/uucp/Systems 파일에는 uucico 데몬이 원격 컴퓨터에 대한 통신 링크를 설정하는 데 필요한 정보가 포함됩니다. /etc/uucp/Systems는 UUCP를 구성할 때 첫번째로 편집해야 하는 파일입니다.

Systems 파일의 각 항목은 호스트가 통신하는 원격 컴퓨터를 나타냅니다. 특정 호스트의 항목이 둘 이상일 수 있습니다. 추가 항목은 대체 통신 경로를 나타내며 순차적으로 시도됩니다. 또한 기본적으로 UUCP에서는 /etc/uucp/Systems에 표시되지 않은 컴퓨터가 호스트에 로그인하지 못하게 합니다.

Sysfiles 파일을 사용하면 Systems 파일로 사용할 여러 파일을 정의할 수 있습니다. Sysfiles에 대한 설명은 189 페이지 “UUCP /etc/uucp/Sysfiles 파일”을 참조하십시오.

Systems 파일에 있는 항목의 구문은 다음과 같습니다.

```
System-Name     Time     Type     Speed     Phone     Chat Script
```

Systems 파일의 항목에 대한 다음 예를 참조하십시오.

예 12–1 /etc/uucp/Systems의 항목

```
Arabian     Any  ACUEC 38400 111222  ogin: Puucp ssword:beledi
```

Arabian	System-Name 필드의 항목입니다. 자세한 내용은 172 페이지 "/etc/uucp/Systems 파일의 System-Name 필드"를 참조하십시오.
Any	Time 필드의 항목입니다. 자세한 내용은 172 페이지 "/etc/uucp/Systems 파일의 Time 필드"를 참조하십시오.
ACUEC	Type 필드의 항목입니다. 자세한 내용은 173 페이지 "/etc/uucp/Systems 파일의 Type 필드"를 참조하십시오.
38400	Speed 필드의 항목입니다. 자세한 내용은 174 페이지 "/etc/uucp/Systems 파일의 Speed 필드"를 참조하십시오.
111222	Phone 필드의 항목입니다. 자세한 내용은 174 페이지 "/etc/uucp/Systems 파일의 Phone 필드"를 참조하십시오.
ogin: Puucp ssword:beledi	Chat Script 필드의 항목입니다. 자세한 내용은 175 페이지 "/etc/uucp/Systems 파일의 Chat-Script 필드"를 참조하십시오.

/etc/uucp/Systems 파일의 System-Name 필드

이 필드에는 원격 컴퓨터의 노드 이름이 포함됩니다. TCP/IP 네트워크에서 이 이름은 시스템의 호스트 이름이거나 /etc/uucp/Sysname 파일을 통해 UUCP 통신용으로 특별히 만든 이름일 수 있습니다. 171 페이지 "UUCP /etc/uucp/Systems 파일"을 참조하십시오. 예 12–1에서는 System-Name 필드에 원격 호스트 Arabian에 대한 항목이 포함됩니다.

/etc/uucp/Systems 파일의 Time 필드

이 필드는 원격 컴퓨터를 호출할 수 있는 요일 및 시간을 지정합니다. Time 필드의 형식은 다음과 같습니다.

```
daytime[;retry]
```

Time 필드의 *day* 부분

day 부분은 다음 항목 중 일부를 포함하는 목록일 수 있습니다.

`Su Mo Tu We Th Fr Sa`	개별 요일입니다.
`Wk`	평일인 경우입니다.
`Any`	요일을 지정하지 않습니다.
`Never`	호스트에서 원격 컴퓨터에 대한 호출을 초기화하지 않습니다. 원격 컴퓨터에서 호출을 초기화해야 합니다. 그러면 호스트가 **수동 모드**로 작동합니다.

Time 필드의 *time* 부분

예 12–1에서는 Time 필드에 `Any`가 표시되어 있습니다. 이는 `Arabian` 호스트를 언제든지 호출할 수 있음을 나타냅니다.

time 부분은 24시간 표기법으로 지정된 시간 범위(예: 오전 8시 30분에서 오후 12시 30분까지인 경우 `0800-1230`)여야 합니다. *time* 부분을 지정하지 않으면 언제든지 호출할 수 있는 것으로 간주됩니다.

0000을 포함하는 시간 범위를 사용할 수 있습니다. 예를 들어 `0800-0600`은 오전 6시에서 오전 8시 사이의 시간을 제외한 모든 시간이 허용됨을 의미합니다.

Time 필드의 *retry* 부분

retry 하위 필드를 사용하여 실패한 시도 이후 재시도 전까지의 최소 시간(분)을 지정할 수 있습니다. 기본 대기는 60분입니다. 하위 필드 구분자는 세미콜론입니다. 예를 들어 `Any;9`는 언제든지 호출하지만 실패가 발생한 후 9분 이상 기다린 다음 다시 시도하는 것으로 해석됩니다.

retry 항목을 지정하지 않으면 지수 백오프 알고리즘이 사용됩니다. 이는 UUCP가 기본 대기 시간으로 시작하고 실패한 시도 수가 늘어남에 따라 대기 시간이 증가함을 의미합니다. 예를 들어 초기 재시도 시간이 5분이라고 가정합니다. 응답이 발생하지 않으면 다음 재시도는 10분 후입니다. 그리고 다음 재시도는 20분 후가 되는 식으로 최대 재시도 시간인 23시간에 도달할 때까지 계속됩니다. *retry*를 지정하는 경우 지정된 값이 항상 재시도 시작이 됩니다. 그렇지 않으면 백오프 알고리즘이 사용됩니다.

/etc/uucp/Systems 파일의 Type 필드

이 필드에는 원격 컴퓨터에 대한 통신 링크를 설정하는 데 사용해야 하는 장치 유형이 포함됩니다. 이 필드에 사용되는 키워드는 `Devices` 파일 항목의 첫번째 필드와 일치합니다.

예 12–2 Type 필드의 키워드

```
Arabian    Any    ACUEC, g    38400    1112222    ogin: Puucp ssword:beledi
```

Type 필드에 프로토콜을 추가하여 시스템에 연결하는 데 사용되는 프로토콜을 정의할 수 있습니다. 앞의 예에서는 g 프로토콜을 장치 유형 ACUEC에 연결하는 방법을 보여줍니다. 프로토콜에 대한 자세한 내용은 183 페이지 “/etc/uucp/Devices 파일의 프로토콜 정의”를 참조하십시오.

/etc/uucp/Systems 파일의 Speed 필드

이 필드는 Class 필드라고도 하며 통신 링크를 설정하는 데 사용되는 장치의 전송 속도를 지정합니다. UUCP 속도 필드에는 전화 걸기 클래스를 구분하는 문자와 숫자(예: C1200 또는 D1200)가 포함됩니다. 180 페이지 “/etc/uucp/Devices 파일의 Class 필드”를 참조하십시오.

일부 장치는 모든 속도로 사용할 수 있으므로 Any 키워드를 사용할 수 있습니다. 이 필드는 관련 Devices 파일 항목의 Class 필드와 일치해야 합니다.

예 12–3 Speed 필드의 항목

```
eagle    Any    ACU, g    D1200    NY3251    ogin: nuucp ssword:Oakgrass
```

이 필드의 정보가 필요하지 않은 경우 대시(-)를 필드의 위치 표시자로 사용합니다.

/etc/uucp/Systems 파일의 Phone 필드

이 필드에서는 **포트 선택기**라고 하는 자동 전화 걸기용 원격 컴퓨터의 전화 번호(**토큰**이라고 함)를 지정할 수 있습니다. 전화 번호는 선택적 영문자 약어와 숫자 부분으로 구성됩니다. 약어를 사용하는 경우 약어가 Dialcodes 파일에 나열되어 있어야 합니다.

예 12–4 Phone 필드의 항목

```
nubian    Any    ACU       2400    NY555-1212    ogin: Puucp ssword:Passuan
eagle     Any    ACU, g    D1200   NY=3251       ogin: nuucp ssword:Oakgrass
```

Phone 필드에서 등호(=)는 ACU가 2차 발신음이 들릴 때까지 대기한 다음 나머지 숫자를 걸도록 합니다. 문자열의 대시(-)는 ACU가 4초 일시 중지한 후 다음 숫자를 걸도록 합니다.

컴퓨터가 포트 선택기에 연결되어 있으면 해당 선택기에 연결된 다른 컴퓨터에 액세스할 수 있습니다. 이러한 원격 컴퓨터의 Systems 파일 항목에서는 Phone 필드에 전화 번호가 없어야 합니다. 대신 이 필드에는 스위치에 전달되는 토큰이 포함되어

있어야 합니다. 따라서 포트 선택기는 호스트에서 통신할 원격 컴퓨터를 일반적으로 시스템 이름만 압니다. 연결된 Devices 파일 항목에는 끝에 \D가 있어야 합니다. 그래야만 이 필드가 Dialcodes 파일을 사용하여 해석되지 않습니다.

/etc/uucp/Systems 파일의 Chat-Script 필드

Login 필드라고도 하는 이 필드에는 **채트 스크립트**라는 문자열이 포함됩니다. 채트 스크립트에는 로컬 및 원격 컴퓨터가 초기 대화에서 서로에게 전달해야 하는 문자가 포합됩니다. 채트 스크립트의 형식은 다음과 같습니다.

expect send [expect send] ....

*expect*는 로컬 호스트가 대화를 시작하기 위해 원격 호스트에서 받아야 하는 문자열을 나타냅니다. *send* 는 로컬 호스트가 원격 호스트에서 *expect* 문자열을 받은 후 보내는 문자열입니다. 채트 스크립트에는 expect-send 시퀀스가 둘 이상 있을 수 있습니다.

기본 채트 스크립트에는 다음이 포함될 수 있습니다.

- 로컬 호스트가 원격 컴퓨터에서 받아야 하는 로그인 프롬프트
- 로컬 호스트가 로그인하기 위해 원격 컴퓨터에 보내는 로그인 이름
- 로컬 호스트가 원격 컴퓨터에서 받아야 하는 암호 프롬프트
- 로컬 호스트가 원격 컴퓨터에 보내는 암호

expect 필드는 다음 형식의 하위 필드로 구성될 수 있습니다.

expect[-send-expect]...

*-send*는 이전 *expect*를 읽지 못한 경우에 전송됩니다. *-send* 다음에 오는 *-expect*는 필요한 다음 문자열입니다.

예를 들어 login--login 문자열을 사용하면 로컬 호스트의 UUCP에 login이 필요합니다. UUCP가 원격 컴퓨터에서 login을 받으면 UUCP는 다음 필드로 이동합니다. UUCP가 login을 받지 못하면 UUCP는 캐리지 리턴을 보낸 다음 login을 다시 찾습니다. 처음에 로컬 컴퓨터에 아무 문자도 필요하지 않은 경우 *expect* 필드에서 널 문자열에 대해 ""을 사용합니다. *send* 문자열을 \c로 종결하지 않은 경우 모든 *send* 필드는 캐리지 리턴이 첨부되어 전송됩니다.

다음은 *expect-send* 문자열을 사용하는 Systems 파일 항목의 예입니다.

```
sonora Any ACUEC 9600 2223333 "" \r \r ogin:-BREAK-ogin: Puucpx ssword:xyzzy
```

이 예에서는 로컬 호스트의 UUCP가 두 개의 캐리지 리턴을 보내고 ogin:(Login:에 해당)을 대기하도록 합니다. ogin:을 받지 못하면 BREAK를 보냅니다. ogin:을 받으면 로그인 이름 Puucpx를 보냅니다. ssword:(Password:에 해당)를 받으면 암호 xyzzy를 보냅니다.

다음 표에서는 몇 가지 유용한 제어 문자가 나와 있습니다.

표 12–1 Systems 파일의 Chat-Script 필드에서 사용되는 제어 문자

제어 문자	의미
\b	백스페이스 문자를 보내거나 이 문자가 필요합니다.
\c	문자열의 끝에 있는 경우 정상적으로 보낸 캐리지 리턴을 표시하지 않습니다. 다른 경우에는 무시됩니다.
\d	추가 문자를 보내기 전에 1-3초 지연합니다.
\E	에코 검사를 시작합니다. 이 때부터 문자가 전송될 때마다 UUCP는 문자를 받을 때까지 기다린 다음 검사를 계속합니다.
\e	검사 해제를 에코 설정합니다.
\H	행업 하나를 무시합니다. 다이얼 백 모뎀의 경우 이 옵션을 사용합니다.
\K	BREAK 문자를 보냅니다.
\M	CLOCAL 플래그를 켭니다.
\m	CLOCAL 플래그를 끕니다.
\n	개행 문자를 보내거나 이 문자가 필요합니다.
\N	널 문자(ASCII NUL)를 보냅니다.
\p	약 0.25-0.5초 동안 일시 중지합니다.
\r	캐리지 리턴을 보내거나 캐리지 리턴이 필요합니다.
\s	공백 문자를 보내거나 이 문자가 필요합니다.
\t	탭 문자를 보내거나 이 문자가 필요합니다.
EOT	개행 두 번 다음에 EOT를 보냅니다.
BREAK	BREAK 문자를 보냅니다.
ddd	8진수로 표시되는 문자(*ddd*)를 보내거나 이 문자가 필요합니다.

채트 스크립트를 통해 다이얼 백을 사용으로 설정

일부 회사에서는 원격 컴퓨터에서의 호출을 처리하는 다이얼 인 서버를 설정합니다. 예를 들어 회사에 다이얼 백 모뎀이 포함된 다이얼 인 서버가 있고 직원이 집에 있는 컴퓨터에서 이 서버를 호출할 수 있습니다. 다이얼 인 서버가 원격 컴퓨터를 식별한 후 다이얼 인 서버는 원격 컴퓨터와의 연결을 끊은 다음 원격 컴퓨터를 다시 호출합니다. 그런 다음 통신 링크가 다시 설정됩니다.

Systems 파일 채트 스크립트에서 다이얼 백이 있어야 하는 위치에 \H 옵션을 사용하여 다이얼 백을 용이하게 할 수 있습니다. 다이얼 인 서버가 행업해야 하는 위치에서 예상 문자열의 일부로 \H를 포함합니다.

예를 들어 다이얼 인 서버를 호출하는 채트 스크립트에 다음 문자열이 포함되어 있다고 가정합니다.

```
INITIATED\Hogin:
```

로컬 컴퓨터의 UUCP 전화 걸기 기능은 다이얼 인 서버에서 INITIATED 문자를 받아야 합니다. INITIATED 문자가 일치된 후 전화 걸기 기능은 다이얼 인 서버가 행업할 때까지 전화 걸기 기능이 받는 모든 후속 문자를 비웁니다. 그런 다음 로컬 전화 걸기 기능은 expect 문자열의 다음 부분인 ogin: 을 다이얼 인 서버에서 받을 때까지 기다립니다. ogin: 을 받으면 전화 걸기 기능은 채트 스크립트를 계속합니다.

앞의 샘플 문자열에 나온 것처럼 문자열이 \H 바로 앞이나 뒤에 오지 않아도 됩니다.

/etc/uucp/Systems 파일의 하드웨어 플로우 제어

pseudo-send STTY= **값** 문자열을 사용하여 모뎀 특성을 설정할 수도 있습니다. 예를 들어 STTY=crtscts는 하드웨어 플로우 제어를 사용으로 설정합니다. STTY에는 모든 stty 모드를 사용할 수 있습니다. 자세한 내용은 stty(1) 및 termio(7I) man 페이지를 참조하십시오.

다음 예에서는 Systems 파일 항목에서 하드웨어 플로우 제어를 사용으로 설정합니다.

```
unix Any ACU 2400 12015551212 "" \r ogin: Puucp ssword:Passuan "" \ STTY=crtscts
```

이 pseudo-send 문자열은 Dialers 파일의 항목에서 사용할 수도 있습니다.

/etc/uucp/Systems 파일에서 패리티 설정

경우에 따라 호출하는 시스템에서 포트 패리티를 확인하고 잘못된 경우 연결을 끊기 때문에 패리티를 재설정해야 할 수 있습니다. expect-send 쌍 "" P_ZERO는 상위 비트(패리티 비트)를 0으로 설정합니다. 다음 예의expect-send 쌍을 참조하십시오.

```
unix Any ACU 2400 12015551212 "" P_ZERO "" \r ogin: Puucp ssword:Passuan
```

다음은 expect-send 쌍 "" P_ZERO 다음에 올 수 있는 패리티 쌍입니다.

"" P_EVEN 패리티를 짝수로 설정합니다(기본값).

"" P_ODD 패리티를 홀수로 설정합니다.

"" P_ONE 패리티 비트를 1로 설정합니다.

이러한 패리티 쌍은 채트 스크립트에서 원하는 위치에 삽입할 수 있습니다. 패리티 쌍은 채트 스크립트에서 expect-send 쌍 "" P_ZERO 다음에 오는 모든 정보에 적용됩니다. 패리티 쌍을 Dialers 파일의 항목에서 사용할 수도 있습니다. 다음 예에서는 패리티 쌍 "" P_ONE이 포함되어 있습니다.

```
unix Any ACU 2400 12015551212 "" P_ZERO "" P_ONE "" \r ogin: Puucp ssword:Passuan
```

UUCP /etc/uucp/Devices 파일

/etc/uucp/Devices 파일에는 원격 컴퓨터에 대한 링크를 설정하는 데 사용할 수 있는 모든 장치에 대한 정보가 포함됩니다. 이러한 장치에는 ACU(고속 모뎀 포함), 직접 링크 및 네트워크 연결이 포함됩니다.

/etc/uucp/Devices 파일의 항목은 다음과 같은 구문을 사용합니다.

```
Type   Line   Line2   Class   Dialer-Token-Pairs
```

다음은 포트 A에 연결되어 38,400bps로 실행되는 U.S. Robotics V.32bis 모델에 대한 Devices 파일의 항목입니다.

```
ACUEC   cua/a   -   38400   usrv32bis-ec
```

ACUEC	Type 필드의 항목입니다. 자세한 내용은 178 페이지 "/etc/uucp/Devices 파일의 Type 필드"를 참조하십시오.
cua/a	Line 필드의 항목입니다. 자세한 내용은 180 페이지 "/etc/uucp/Devices 파일의 Line 필드"를
-	Line2 필드의 항목입니다. 자세한 내용은 180 페이지 "/etc/uucp/Devices 파일의 Line2 필드"를 참조하십시오.
38400	Class 필드의 항목입니다. 자세한 내용은 180 페이지 "/etc/uucp/Devices 파일의 Class 필드"를 참조하십시오.
usrv32bis-ec	Dialer-Token-Pairs 필드의 항목입니다. 자세한 내용은 181 페이지 "/etc/uucp/Devices 파일의 Dialer-Token-Pairs 필드"를 참조하십시오.

각 필드에 대해서는 다음 절에서 설명합니다.

/etc/uucp/Devices 파일의 Type 필드

이 필드는 장치에서 설정하는 링크 유형에 대해 설명합니다. UUCP Type 필드는 다음에 이어지는 절에서 설명하는 키워드 중 하나를 포함할 수 있습니다.

Direct 키워드

Direct 키워드는 주로 cu 연결에 대한 항목에 표시됩니다. 이 키워드는 링크가 다른 컴퓨터나 포트 선택기에 대한 직접 링크임을 나타냅니다. 참조할 각 회선에 대해 cu의 -l 옵션을 통해 별도의 항목을 만드십시오.

ACU 키워드

ACU 키워드는 cu, UUCP, asppp 또는 Solaris PPP 4.0 중 무엇을 사용하든 원격 컴퓨터와 모뎀을 통해 연결된다는 것을 나타냅니다. 이 모뎀은 컴퓨터에 직접 연결하거나 포트 선택기를 통해 간접적으로 연결할 수 있습니다.

포트 선택기

Port Selector는 Type 필드에서 포트 선택기 이름으로 대체되는 변수입니다. 포트 선택기는 네트워크에 연결된 장치로, 호출하는 모뎀의 이름을 물은 다음 액세스를 허가하는 역할을 합니다. /etc/uucp/Dialers 파일에는 micom 및 develcon 포트 선택기에 대한 호출자 스크립트만 포함되어 있습니다. 사용자 고유의 포트 선택기 항목을 Dialers 파일에 추가할 수 있습니다. 자세한 내용은 184 페이지 “UUCP /etc/uucp/Dialers 파일”을 참조하십시오.

System-Name 변수

이 변수는 Type 필드의 시스템 이름으로 대체되며 링크가 이 특정 컴퓨터에 대한 직접 링크임을 나타냅니다. 이 이름 지정 체계는 이 Devices 항목의 행을 *System-Name* 컴퓨터에 대한 /etc/uucp/Systems의 항목과 연결하는 데 사용됩니다.

Devices 파일 및 Systems 파일의 Type 필드

예 12–5에서는 /etc/uucp/Devices의 필드와 /etc/uucp/Systems의 필드를 비교하여 표시합니다. Devices 파일의 Type 필드에서 사용되는 키워드는 Systems 파일 항목의 세번째 필드와 일치합니다. Devices 파일에서 Type 필드에는 자동 호출 장치(여기서는 V.32bis 모뎀)를 나타내는 ACUEC 항목이 있습니다. 이 값은 Systems 파일의 Type 필드와 일치합니다. 이 필드에도 ACUEC 항목이 포함되어 있습니다. 자세한 내용은 171 페이지 “UUCP /etc/uucp/Systems 파일”을 참조하십시오.

예 12–5 Devices 파일 및 Systems 파일의 Type 필드 비교

다음은 Devices 파일에 있는 항목의 예입니다.

```
ACUEC cua/a - 38400 usrv32bis-ec
```

다음은 Systems 파일에 있는 항목의 예입니다.

```
Arabian Any ACUEC 38400 111222 ogin: Puucp ssword:beledi
```

/etc/uucp/Devices 파일의 Line 필드

이 필드에는 Devices 항목과 연결된 회선(포트라고 함)의 장치 이름이 포함됩니다. 특정 항목과 연관된 모뎀이 /dev/cua/a 장치(직렬 포트 A)에 연결된 경우 이 필드에 입력하는 이름은 cua/a입니다. 선택적 모뎀 제어 플래그 M을 Line 필드에 사용하여 반송파를 기다리지 않고 장치를 열도록 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
cua/a,M
```

/etc/uucp/Devices 파일의 Line2 필드

이 필드는 위치 표시자입니다. 여기서는 항상 하이픈(-)을 사용하십시오. Oracle Solaris OS에서 지원되지 않는 801 유형 전화 걸기에서 Line2 필드를 사용합니다. 801 외의 전화 걸기에서는 일반적으로 이 구성을 사용하지 않지만 여전히 이 필드에 하이픈이 있어야 합니다.

/etc/uucp/Devices 파일의 Class 필드

Type 필드에 ACU 또는 Direct 키워드를 사용한 경우 Class 필드에는 장치의 속도가 포함됩니다. 그러나 Class 필드는 Centrex 또는 Dimension PBX와 같은 전화 걸기 클래스를 구분하는 문자와 숫자(예: C1200 또는 D1200)를 포함할 수 있습니다.

많은 대형 사무실에서 두 가지가 넘는 유형의 전화 네트워크를 사용할 수 있으므로 이러한 구분이 필요합니다. 하나의 네트워크는 사무실 내부 통신을 지원하는 데에만 사용하고 다른 네트워크는 외부 통신을 처리할 수 있습니다. 이런 경우 내부 통신에 사용할 회선과 외부 통신에 사용할 회선을 구분해야 합니다.

Devices 파일의 Class 필드에서 사용되는 키워드는 Systems 파일의 Speed 필드와 일치합니다.

예 12–6 Devices 파일의 Class 필드

```
ACU    cua/a    -    D2400    hayes
```

일부 장치는 모든 속도로 사용할 수 있으므로 Class 필드에 Any 키워드를 사용할 수 있습니다. Any를 사용하는 경우 이 행은 Systems 파일의 Speed 필드에 필요한 모든 속도와 일치합니다. 이 필드가 Any이고 Systems 파일 Speed 필드가 Any이면 속도는 기본적으로 2400bps입니다.

/etc/uucp/Devices 파일의 Dialer-Token-Pairs 필드

Dialer-Token-Pairs(DTP) 필드에는 전화 걸기 이름과 이 전화 걸기에 전달할 토큰이 포함됩니다. DTP 필드의 구문은 다음과 같습니다.

dialer token [dialer token]

dialer 부분은 포트 모니터인 모뎀의 이름이거나 직접 링크 장치의 경우 `direct` 또는 `uudirect`일 수 있습니다. DTP(Dialer-Token Pairs)를 원하는 수만큼 포함할 수 있습니다. *dialer* 부분이 없으면 `Systems` 파일의 관련 항목에서 가져옵니다. dialer 부분 바로 뒤에 *token* 부분을 지정할 수 있습니다.

연결된 전화 걸기에 따라서는 마지막 DTP(Dialer-Token Pairs)가 없을 수도 있습니다. 대부분의 경우 마지막 쌍에는 *dialer* 부분만 포함됩니다. *token* 부분은 연결된 `Systems` 파일 항목의 Phone 필드에서 가져옵니다.

dialer 부분의 유효한 항목은 `Dialers` 파일에서 정의하거나 여러 특수 전화 걸기 유형 중 하나일 수 있습니다. 이러한 특수 전화 걸기 유형은 소프트웨어에 컴파일되어 있으므로 `Dialers` 파일에 항목을 포함하지 않고도 사용할 수 있습니다. 다음 목록에 특수 전화 걸기 유형이 나와 있습니다.

`TCP`	TCP/IP 네트워크
`TLI`	전송 레벨 인터페이스 네트워크(STREAMS 포함 안함)
`TLIS`	전송 레벨 인터페이스 네트워크(STREAMS 포함)

자세한 내용은 183 페이지 “/etc/uucp/Devices 파일의 프로토콜 정의”를 참조하십시오.

/etc/uucp/Devices 파일의 Dialer-Token-Pairs 필드 구조

항목과 연결된 장치에 따라 DTP 필드는 네 가지 다른 방법으로 구성할 수 있습니다.

DTP 필드를 구성할 수 있는 첫번째 방법을 참조하십시오.

직접 연결된 모뎀 – 모뎀이 컴퓨터의 포터에 직접 연결된 경우 연결된 `Devices` 파일 항목의 DTP 필드에는 한 쌍만 포함됩니다. 이 쌍은 일반적으로 모뎀의 이름입니다. 이 이름을 사용하여 특정 `Devices` 파일 항목을 `Dialers` 파일의 항목과 일치시킵니다. 따라서 Dialer 필드는 `Dialers` 파일 항목의 첫번째 필드와 일치해야 합니다.

예 12–7 직접 연결 모뎀의 Dialers 필드

```
Dialers   hayes =,-,  ""          \\dA\pTE1V1X1Q0S2=255S12=255\r\c
                                  \EATDT\T\r\c CONNECT
```

Devices 파일 항목의 DTP 필드에 dialer 부분(hayes)만 있습니다. 이는 전화 걸기에 전달할 *token*(이 경우 전화 번호)을 Systems 파일 항목의 Phone 필드에서 가져온다는 것을 나타냅니다. Example 12–9에서 설명한 대로 예 12–9에 암시되어 있습니다.

DTP 필드를 구성할 수 있는 두번째와 세번째 방법을 참조하십시오.

- **직접 링크** – 특정 컴퓨터에 대한 직접 링크의 경우 연결된 항목의 DTP 필드에는 direct 키워드가 포함됩니다. 이 조건은 직접 링크 항목의 유형인 Direct 및 *System-Name* 모두에 적용됩니다. 178 페이지 "/etc/uucp/Devices 파일의 Type 필드"를 참조하십시오.
- **동일한 포트 선택기의 컴퓨터** – 통신하려는 컴퓨터가 사용자 컴퓨터와 동일한 포트 선택기 스위치에 있는 경우 먼저 스위치에 액세스해야 합니다. 그런 다음 스위치를 통해 다른 컴퓨터에 연결됩니다. 이러한 유형의 항목에는 쌍이 하나만 있습니다. *dialer* 부분은 Dialers 파일 항목과 일치시키는 데 사용됩니다.

예 12–8 동일한 포트 선택기에 있는 컴퓨터의 UUCP Dialers 필드

```
Dialers    develcon ,""   ""            \pr\ps\c est:\007 \E\D\e \007
```

표시된 대로 *token* 부분은 비워 둡니다. 이러한 지정은 토큰을 Systems 파일에서 가져온다는 것을 나타냅니다. 이 컴퓨터의 Systems 파일 항목에는 일반적으로 컴퓨터의 전화 번호용으로 예약된 Phone 필드의 토큰이 포함되어 있습니다. 자세한 내용은 171 페이지 "UUCP /etc/uucp/Systems 파일"을 참조하십시오. 이 유형의 DTP에는 Phone 필드의 내용이 Dialcodes 파일의 유효한 항목으로 해석되지 않도록 하는 제어 문자(\D)가 포함됩니다,

DTP 필드를 구성할 수 있는 네번째 방법을 참조하십시오.

포트 선택기에 연결된 모뎀 – 고속 모뎀이 포트 선택기에 연결된 경우 컴퓨터는 먼저 포트 선택기 스위치에 액세스해야 합니다. 그런 다음 스위치를 통해 모뎀에 연결됩니다. 이러한 유형의 항목에는 전화 걸기-토큰 쌍이 두 개 필요합니다. 각 쌍의 *dialer* 부분(항목의 다섯번째와 일곱번째 필드)은 다음과 같이 Dialers 파일의 항목과 일치시키는 데 사용됩니다.

예 12–9 포트 선택기에 연결된 모뎀의 UUCP Dialers 필드

```
develcon ""     ""    \pr\ps\c  est:\007    \E\D\e      \007
ventel   =&-%   t""   \r\p\r\c  $           <K\T%\r>\c  ONLINE!
```

첫번째 쌍에서 develcon은 전화 걸기이고 vent는 컴퓨터에 연결할 장치(예: Ventel 모뎀)를 알려 주기 위해 Develcon 스위치에 전달되는 토큰입니다. 각 스위치가 다르게 설정될 수 있으므로 이 토큰은 각 포트 선택기에 대해 고유합니다. Ventel 모뎀이 연결되면 두번째 쌍에 액세스합니다. Ventel은 전화 걸기이고 토큰은 Systems 파일에서 가져옵니다.

다음과 같은 두 개의 제어 문자가 DTP 필드에 표시될 수 있습니다.

- \T – Phone(*token*) 필드를 /etc/uucp/Dialcodes 파일을 사용하여 해석해야 함을 나타냅니다. 일반적으로 이 제어 문자는 Hayes, U.S. Robotics 등의 모뎀과 연결된 각 호출자 스크립트의 /etc/uucp/Dialers 파일에 있습니다. 따라서 호출자 스크립트에 액세스할 때까지는 해석되지 않습니다.
- \D – Phone(*token*) 필드를 /etc/uucp/Dialcodes 파일을 사용하여 해석하지 않아야 함을 나타냅니다. Devices 항목 끝에 제어 문자를 지정하지 않으면 \D(기본값)로 간주됩니다. \D도 /etc/uucp/Dialers 파일에서 네트워크 스위치 develcon 및 micom과 연결된 항목에 사용됩니다.

/etc/uucp/Devices 파일의 프로토콜 정의

/etc/uucp/Devices의 각 장치에서 사용할 프로토콜을 정의할 수 있습니다. 기본값을 사용하거나 호출하는 특정 시스템에서 프로토콜을 정의할 수 있으므로 일반적으로 이 지정은 필요하지 않습니다. 자세한 내용은 171 페이지 “UUCP /etc/uucp/Systems 파일”을 참조하십시오. 프로토콜을 지정하는 경우 다음과 같은 형식을 사용해야 합니다.

Type,*Protocol [parameters]*

예를 들어 TCP,te를 사용하여 TCP/IP 프로토콜을 지정할 수 있습니다.

다음 표에서는 Devices 파일에서 사용할 수 있는 프로토콜이 나와 있습니다.

표 12–2 /etc/uucp/Devices에서 사용되는 프로토콜

프로토콜	설명
t	이 프로토콜은 일반적으로 TCP/IP를 통한 전송 및 다른 신뢰할 수 있는 연결에 대해 사용됩니다. t에서는 오류 없는 전송을 가정합니다.
g	이 프로토콜은 UUCP의 기본 프로토콜입니다. g는 느리고 신뢰할 수 있으며 잡음이 많은 전화선을 통한 전송에 적합합니다.
e	이 프로토콜에서는 TCP/IP와 같은 바이트 스트림 지향이 아닌 메시지 지향인 오류 없는 채널을 통한 전송을 가정합니다.
f	이 프로토콜은 X.25 연결을 통한 전송에 사용됩니다. f는 데이터 스트림에 대한 플로우 제어를 사용하며 거의 오류가 없다고 보장할 수 있는 링크(특히 X.25/PAD 링크)를 통해 작동하기 위한 것입니다. 체크섬은 전체 파일에 대해서만 시행됩니다. 전송이 실패하는 경우 받는 사람은 재전송을 요청할 수 있습니다.

다음은 장치 항목에 대한 프로토콜 지정을 보여주는 예입니다.

```
TCP,te - - Any TCP -
```

이 예에서는 TCP 장치에 대해 t 프로토콜을 사용해 보아야 한다는 것을 나타냅니다. 전송의 다른 한쪽이 거부하면 e 프로토콜을 사용합니다.

e도 t도 모뎀을 통해 사용하는 데에는 적합하지 않습니다. 모뎀에서 오류 없는 전송을 보장하더라도 여전히 모뎀과 CPU 사이에서 데이터가 삭제될 수 있습니다.

UUCP /etc/uucp/Dialers 파일

/etc/uucp/Dialers 파일에는 일반적으로 사용되는 모뎀의 전화 걸기 명령이 포함됩니다. 비표준 모뎀을 사용하거나 UUCP 환경을 사용자 정의하려는 계획이 없는 경우 이 파일의 항목을 변경하거나 추가할 필요가 없을 것입니다. 그렇지만 파일에 무엇이 있고 이것이 Systems 및 Devices 파일과 어떤 관련이 있는지 알아야 합니다.

텍스트에서는 회선을 데이터 전송에 사용할 수 있으려면 회선에서 수행해야 하는 초기 대화를 지정합니다. 채트 스크립트라고 하는 이 대화는 일반적으로 전송되며 필요한 ASCII 문자열의 시퀀스입니다. 채트 스크립트는 종종 전화 번호로 전화를 거는 데 사용됩니다.

178 페이지 “UUCP /etc/uucp/Devices 파일”의 예에 나온 대로 Devices 파일 항목의 다섯번째 필드는 Dialers 파일의 색인이거나 TCP, TLI, TLIS 등과 같은 특수 전화 걸기 유형입니다. uucico 데몬은 Devices 파일의 다섯번째 필드를 각 Dialers 파일 항목의 첫번째 필드와 일치시키려고 합니다. 또한 일곱번째 위치에서 시작하는 홀수 번호가 매겨진 각 Devices 필드는 Dialers 파일의 인덱스로 사용됩니다. 일치에 성공하면 Dialers 항목은 전화 걸기 대화를 수행하는 것으로 해석됩니다.

Dialers 파일의 각 항목은 다음과 같은 구문을 사용합니다.

```
dialer   substitutions   expect-send
```

다음 예에서는 U.S. Robotics V.32bis 모뎀의 항목을 보여줍니다.

예 12–10 /etc/uucp/Dialers 파일의 항목

```
usrv32bis-e    =,-,  ""    dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
                           \EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

usrv32bis-e
: Dialer 필드의 항목입니다. Dialer 필드는 Devices 파일의 다섯번째 필드 및 추가 홀수 번호 필드와 일치합니다.

=,-, ""
: Substitutions 필드의 항목입니다. Substitutions 필드는 변환 문자열입니다. 각 문자 쌍의 첫번째는 쌍의 두번째 문자에 매핑됩니다. 이 매핑은 일반적으로 = 및 - 를 전화 걸기에 필요한 “wait for dial tone” 및 “pause”와 같은 문자열로 변환하는 데 사용됩니다

dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
: Expect-Send 필드의 항목입니다. Expect-Send 필드는 문자열입니다.

\EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
Expect-Send 필드의 추가 항목입니다.

다음 예에서는 UUCP를 Oracle Solaris 설치 프로그램의 일부로 설치할 때 배포되는 Dialers 파일의 샘플 항목을 보여줍니다.

예 12–11 /etc/uucp/Dialers의 인용구

```
penril    =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK

ventel    =&-%    "" \r\p\r\c $ <K\T%%\r>\c ONLINE!

vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE

develcon    ""    "" \pr\ps\c est:\007

\E\D\e \n\007 micom    ""    "" \s\c NAME? \D\r\c GO

hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT

#   Telebit TrailBlazer
tb1200    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=2\r\c OK\r
\EATDT\T\r\c CONNECT\s1200
tb2400    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=3\r\c OK\r
\EATDT\T\r\c CONNECT\s2400
tbfast    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=255\r\c OK\r
\EATDT\T\r\c CONNECT\sFAST

# USrobotics, Codes, and DSI modems

dsi-ec  =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts,crtsxoff

dsi-nec =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E0*F3*M1*S1\r\c OK\r \EATDT\T\r\c CONNECT
STTY=crtscts,crtsxoff

usrv32bis-ec =,-,  "" \dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r \EATDT\T\r\c
CONNECT\s14400/ARQ STTY=crtscts,crtsxoff

usrv32-nec =,-, "" \dA\pT&FE1V1X1Q0S2=255S12=255&A0&H1&M0&B0&W\r\c OK\r \EATDT\T\r\c
CONNECT STTY=crtscts,crtsxoff

codex-fast =,-, "" \dA\pT&C1&D2*MF0*AA1&R1&S1*DE15*FL3S2=255S7=40S10=40*TT5&W\r\c OK\r
\EATDT\T\r\c CONNECT\s38400 STTY=crtscts,crtsxoff

tb9600-ec =W-,  "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6\r\c OK\r
\EATDT\T\r\cCONNECT\s9600 STTY=crtscts,crtsxoff

tb9600-nec =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6S180=0\r\c OK\r \EATDT\T\r\c
CONNECT\s9600 STTY=crtscts,crtsxoff
```

다음 표에서는 Dialers 파일의 보내기 문자열에서 일반적으로 사용되는 제어 문자가 나와 있습니다.

표 12–3 /etc/uucp/Dialers의 백슬래시 문자

문자	설명
\b	백스페이스 문자를 보내거나 이 문자가 필요합니다.
\c	개행 또는 캐리지 리턴이 없습니다.
\d	약 2초 동안 지연됩니다.
\D	Dialcodes 변환이 없는 전화 번호 또는 토큰입니다.
\e	에코 검사를 사용 안함으로 설정합니다.
\E	느린 장치에 대한 에코 검사를 사용으로 설정합니다.
\K	Break 문자를 삽입합니다.
\n	개행을 보냅니다.
\nnn	8진수를 보냅니다. 사용할 수 있는 추가 제어 문자는 171 페이지 "UUCP /etc/uucp/Systems 파일" 절에 나와 있습니다.
\N	널 문자(ASCII NUL)를 보내거나 이 문자가 필요합니다.
\p	약 12-14초 동안 일시 중지합니다.
\r	반환합니다.
\s	공백 문자를 보내거나 이 문자가 필요합니다.
\T	Dialcodes 변환이 있는 전화 번호 또는 토큰입니다.

다음은 Dialers 파일의 penril 항목입니다.

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

먼저 =는 W(발신음 대기)로 대체되고 -는 P(일시 중지)로 대체되도록 전화 번호 인수에 대한 대체 방식이 설정됩니다.

행의 나머지에 주어진 핸드셰이크는 다음과 같이 작동합니다.

- "" – 다음 단계로 진행하는 것을 의미하는 없음을 대기합니다.
- \d – 2초 지연한 다음 캐리지 리턴을 보냅니다.
- > – >를 대기합니다.
- Q\c – 캐리지 리턴 없이 Q를 보냅니다.
- : – :이 필요합니다.
- \d- – 2초 지연하고 -와 캐리지 리턴을 보냅니다.
- > – >를 대기합니다.
- s\p9\c – s를 보내고 일시 중지하고 캐리지 리턴 없이 9를 보냅니다.

-)-W\p\r\ds\p9\c-) –)를 대기합니다.)를 받지 못하면 뒤에 오는 - 문자 사이의 문자열을 처리합니다. W를 보내고, 일시 중지하고, 캐리지 리턴을 보내고, 지연하고, s를 보내고, 일시 중지하고, 캐리지 리턴 없이 9를 보낸 다음)를 대기합니다.
- y\c – 캐리지 리턴 없이 y를 보냅니다.
- : – :을 대기합니다.
- \E\TP – \E는 에코 검사를 사용으로 설정합니다. 이때부터 문자가 전송될 때마다 UUCP는 문자를 받을 때까지 대기한 다음 진행합니다. 그런 다음 UUCP는 전화 번호를 보냅니다. \T는 전달된 전화 번호를 인수로 사용한다는 것을 의미합니다. \T는 Dialcodes 변환 및 이 항목의 필드 2에서 지정하는 모뎀 기능 변환에 적용됩니다. 그런 다음 \T는 P와 캐리지 리턴을 보냅니다.
- > – >를 대기합니다.
- 9\c – 개행 없이 9를 보냅니다.
- OK – OK 문자열을 대기합니다.

/etc/uucp/Dialers 파일에서 하드웨어 플로우 제어를 사용으로 설정

pseudo-send STTY=*value* 문자열을 사용하여 모뎀 특성을 설정할 수도 있습니다. 예를 들어 STTY=crtscts는 아웃바운드 하드웨어 플로우 제어를 사용으로 설정 STTY=crtsxoff는 인바운드 하드웨어 플로우 제어를 사용으로 설정합니다. STTY=crtscts,crtsxoff는 아웃바운드 및 인바운드 하드웨어 플로우 제어를 사용으로 설정합니다.

STTY에는 모든 stty 모드를 사용할 수 있습니다. stty(1) 및 termio(7I) man 페이지를 참조하십시오.

다음 예에서는 Dialers 항목에서 하드웨어 플로우 제어를 사용으로 설정합니다.

```
dsi =,–, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts
```

pseudo-send 문자열을 Systems 파일의 항목에서도 사용할 수 있습니다.

/etc/uucp/Dialers 파일에서 패리티 설정

경우에 따라 호출하는 시스템에서 포트 패리티를 확인하고 잘못된 경우 연결을 끊기 때문에 패리티를 재설정해야 할 수 있습니다. 다음과 같은 expect-send 쌍 P_ZERO는 패리티를 0으로 설정합니다.

```
foo =,-, "" P_ZERO "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r\EATDT\T\r\c CONNECT
```

다음은 expect-send 쌍 다음에 올 수 있는 패리티 쌍입니다.

"" P_EVEN 패리티를 짝수로 설정합니다(기본값).

"" P_ODD 패리티를 홀수로 설정합니다.

"" P_ONE 패리티를 1로 설정합니다.

pseudo-send 문자열을 Systems 파일의 항목에서 사용할 수도 있습니다.

다른 기본 UUCP 구성 파일

기본 UUCP 구성을 수행할 때 Systems , Devices 및 Dialers 파일과 더불어 이 절에서 설명하는 파일을 사용할 수 있습니다.

UUCP /etc/uucp/Dialcodes 파일

/etc/uucp/Dialcodes 파일을 사용하여 /etc/uucp/Systems 파일의 Phone 필드에서 사용할 수 있는 다이얼 번호 약어를 정의할 수 있습니다. Dialcodes 파일을 사용하여 동일한 사이트의 여러 시스템에서 사용하는 기본 전화 번호에 대한 추가 정보를 제공할 수 있습니다.

각 항목의 구문은 다음과 같습니다.

```
Abbreviation   Dial-Sequence
```

Abbreviation 이 필드에서는 Systems 파일의 Phone 필드에서 사용되는 약어를 제공합니다.

Dial-Sequence 이 필드에서는 특정 Systems 파일 항목에 액세스할 때 전화 걸기에 전달되는 전화 걸기 시퀀스를 제공합니다.

두 파일의 필드를 비교하십시오. 다음은 Dialcodes 파일의 필드입니다.

```
Abbreviation   Dial-Sequence
```

다음은 Systems 파일의 필드입니다.

```
System-Name   Time   Type   Speed   Phone   Chat Script
```

다음 표에는 Dialcodes 파일에 있는 필드의 샘플 내용이 나와 있습니다.

표 12–4 Dialcodes 파일의 항목

약어	Dial-Sequence
NY	1=212

표 12–4 Dialcodes 파일의 항목 (계속)

약어	Dial-Sequence
jt	9+847

첫번째 행에서 NY는 Systems 파일의 Phone 필드에 표시되는 약어입니다. 예를 들어 Systems 파일에는 다음과 같은 항목이 있을 수 있습니다.

```
NY5551212
```

uucico가 Systems 파일에서 NY를 읽으면 uucico는 Dialcodes 파일에서 NY를 검색하고 전화 걸기 시퀀스 1=212 를 가져옵니다. 1=212는 뉴욕에 거는 모든 전화에 필요한 전화 걸기 시퀀스입니다. 이 시퀀스에는 숫자 1, 일시 중지하고 두번째 발신음을 대기하는 것을 의미하는 "등호"(=) 및 지역 번호 212가 포함됩니다. uucico는 이 정보를 전화 걸기에 보낸 다음 Systems 파일로 돌아와 나머지 전화 번호 5551212를 찾습니다.

jt 9=847- 항목은 Systems 파일의 Phone 필드(예: jt7867)와 함께 작동합니다. uucico가 Systems 파일에서 jt7867을 포함하는 항목을 읽으면 uucico는 DTP(Dialer-Token Pairs)의 토큰이 \T인 경우 9=847-7867 시퀀스를 전화 걸기에 보냅니다.

UUCP /etc/uucp/Sysfiles 파일

/etc/uucp/Sysfiles 파일에서는 uucp 및 cu에서 사용할 Systems, Devices 및 Dialers 파일과 같은 여러 파일을 지정할 수 있습니다. cu에 대한 자세한 내용은 cu(1C) man 페이지를 참조하십시오. Sysfiles를 다음 파일에 대해 사용할 수 있습니다.

- 다른 Systems 파일. uucp 서비스와 다른 주소로 로그인 서비스를 요청할 수 있습니다.
- 다른 Dialers 파일. cu 및 uucp에 대해 다른 핸드셰이크를 지정할 수 있습니다.
- 여러 Systems, Dialers 및 Devices 파일. 특히 Systems 파일은 커질 수 있으므로 여러 작은 파일로 분할하면 더 간편해집니다.

Sysfiles 파일의 구문은 다음과 같습니다.

service=*w* systems=*x*:*x* dialers=*y*:*y* devices=*z*:*z*

w uucico, cu 또는 두 명령 모두를 콜론으로 구분하여 나타냅니다

x Systems 파일로 사용할 하나 이상의 파일을 나타내며, 각 파일 이름을 콜론으로 구분하고 제공되는 순서대로 읽습니다

y Dialers 파일로 사용할 하나 이상의 파일을 나타냅니다.

z Devices 파일로 사용할 하나 이상의 파일을 나타냅니다.

각 파일 이름은 전체 경로를 제공하지 않은 경우 /etc/uucp 디렉토리에 대한 상대 경로로 간주됩니다.

다음 샘플 /etc/uucp/Sysfiles에서는 로컬 Systems 파일(Local_Systems) 및 표준 /etc/uucp/Systems 파일을 정의합니다.

```
service=uucico:cu systems=Systems :Local_Systems
```

이 항목이 /etc/uucp/Sysfiles에 있으면 uucico 및 cu는 모두 먼저 표준 /etc/uucp/Systems를 확인합니다. 호출되는 시스템의 항목이 이 파일에 없거나 파일의 항목이 실패하는 경우 두 명령은 모두 /etc/uucp/Local_Systems를 확인합니다.

이전 항목에 지정된 대로 cu 및 uucico는 Dialers 및 Devices 파일을 공유합니다.

uucico 및 cu 시스템에 대해 서로 다른 Systems 파일을 정의한 경우 시스템에서는 두 가지 다른 Systems 목록을 저장합니다. uucico 목록을 인쇄하려면 uuname 명령을 사용하고 cu 목록을 인쇄하려면 uuname -C 명령을 사용합니다. 다음은 먼저 대체 파일을 참조하고 필요한 경우 기본 파일을 참조하는 것을 보여주는 파일의 다른 예입니다.

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
devices=Devices.cico:Devices
  service=cu systems=Systems.cu:Systems \
dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

UUCP /etc/uucp/Sysname 파일

UUCP를 사용하는 모든 시스템에는 식별 이름(**노드 이름**이라고도 함)이 있어야 합니다. 노드 이름은 원격 시스템의 /etc/uucp/Systems 파일에 채트 스크립트 및 다른 식별 정보와 함께 표시됩니다. 일반적으로 UUCP에서는 uname -n 명령으로 반환되는 것과 동일한 노드 이름을 사용하며 이 이름은 TCP/IP에서도 사용됩니다.

/etc/uucp/Sysname 파일을 만들면 UUCP 노드 이름을 TCP/IP 호스트 이름과 별개로 지정할 수 있습니다. 파일에는 시스템의 UUCP 노드 이름을 포함하는 한 행 항목이 있습니다.

UUCP /etc/uucp/Permissions 파일

/etc/uucp/Permissions 파일에서는 원격 컴퓨터의 로그인, 파일 액세스 및 명령 실행을 위한 사용 권한을 지정합니다. 일부 옵션은 원격 컴퓨터가 파일을 요청하고 로컬 컴퓨터에 대기된 파일을 받을 수 있는 기능을 제한합니다. 다른 옵션은 원격 컴퓨터가 로컬 컴퓨터에서 실행할 수 있는 명령을 지정하는 데 사용할 수 있습니다.

UUCP 구성 항목

각 항목은 논리적 행이며, 연속을 나타내는 백슬래시(\)로 끝나는 물리적 행을 포함합니다. 항목은 공백으로 구분된 옵션으로 구성됩니다. 각 옵션은 다음과 같은 형식의 이름-값 쌍입니다.

name=value

*Values*는 콜론으로 구분된 목록일 수 있습니다. 옵션 지정 내에 공백은 사용할 수 없습니다.

주석 행은 파운드 기호(#)로 시작하며 개행 문자까지의 전체 행을 사용합니다. 여러 행 항목 내에 있는 것을 포함하여 빈 행은 무시됩니다.

Permissions 파일 항목의 유형은 다음과 같습니다.

- LOGNAME – 원격 컴퓨터가 사용자 컴퓨터에 로그인(호출)할 때 적용되는 사용 권한을 지정합니다.

  주 – 원격 컴퓨터가 호출할 때 고유한 로그인 및 검증 가능한 암호를 사용하지 않는 경우 신원이 의심스러울 수 있습니다.

- MACHINE – 사용자 컴퓨터가 원격 컴퓨터에 로그인(호출)할 때 적용되는 사용 권한을 지정합니다.

LOGNAME 항목에는 LOGNAME 옵션이 있고, MACHINE 항목에는 MACHINE 옵션이 있습니다. 하나의 항목에 두 옵션을 모두 포함할 수 있습니다.

UUCP 고려 사항

Permissions 파일을 사용하여 원격 컴퓨터에 부여되는 액세스 레벨을 제한하려면 다음을 고려해야 합니다.

- 원격 컴퓨터가 UUCP 통신을 위해 로그인하는 데 사용하는 로그인 ID는 하나의 LOGNAME 항목에만 표시되어야 합니다.
- MACHINE 항목에 표시되지 않은 이름으로 호출되는 모든 사이트에는 다음과 같은 기본 사용 권한 또는 제한 사항이 적용됩니다.
  - 로컬 보내기 및 수신 요청이 실행됩니다.
  - 원격 컴퓨터는 파일을 사용자 컴퓨터의 /var/spool/uucppublic 디렉토리로 보낼 수 있습니다.
  - 원격 컴퓨터가 사용자 컴퓨터에서 실행하기 위해 보내는 명령은 기본 명령 중 하나(일반적으로 rmail)여야 합니다.

UUCP REQUEST 옵션

원격 컴퓨터가 사용자 컴퓨터를 호출하여 파일 수신을 요청하면 이 요청을 허용하거나 거부할 수 있습니다. REQUEST 옵션은 원격 컴퓨터가 사용자 컴퓨터에서 파일 전송을 설정하도록 요청할 수 있는지 여부를 지정합니다. REQUEST=yes 문자열은 원격 컴퓨터가 사용자 컴퓨터에서 파일 전송을 요청할 수 있도록 지정합니다. REQUEST=no 문자열은 원격 컴퓨터가 사용자 컴퓨터에서 파일 전송을 요청할 수 없도록 지정합니다. REQUEST=no(기본값)는 REQUEST 옵션을 지정하지 않는 경우에 사용됩니다. REQUEST 옵션은 원격 컴퓨터가 사용자를 호출할 수 있도록 LOGNAME 항목에 표시되거나 사용자가 원격 컴퓨터를 호출할 수 있도록 MACHINE 항목에 표시될 수 있습니다.

UUCP SENDFILES 옵션

원격 컴퓨터가 사용자 컴퓨터를 호출하고 작업을 완료하면 원격 컴퓨터는 사용자 컴퓨터의 대기열에 있는 작업을 검색하려고 할 수 있습니다. SENDFILES 옵션은 사용자 컴퓨터가 원격 컴퓨터의 대기열에 있는 작업을 보낼 수 있는지 여부를 지정합니다.

SENDFILES=yes 문자열은 사용자 컴퓨터가 LOGNAME 옵션의 이름 중 하나로 로그인한 경우 원격 컴퓨터의 대기열에 있는 작업을 보낼 수 있는지 여부를 지정합니다. /etc/uucp/Systems의 Time 필드에 Never를 입력한 경우 이 문자열은 **필수**입니다. 이렇게 지정하면 로컬 컴퓨터가 수동 모드로 설정되지만 이 특정 원격 컴퓨터에 대한 호출을 시작할 수 없습니다. 자세한 내용은 171 페이지 “UUCP /etc/uucp/Systems 파일”을 참조하십시오.

SENDFILES=call 문자열은 사용자 컴퓨터의 대기열에 있는 파일이 사용자 컴퓨터에서 원격 컴퓨터를 호출할 때만 전송되도록 지정합니다. call 값은 SENDFILES 옵션의 기본값입니다. MACHINE 항목은 호출이 원격 컴퓨터로 전송될 때 적용되므로 이 옵션은 LOGNAME 항목에서만 중요합니다. MACHINE 항목에 사용하는 경우 이 옵션은 무시됩니다.

UUCP MYNAME 옵션

이 옵션을 사용하여 컴퓨터의 고유한 UUCP 노드 이름과 hostname 명령으로 반환되는 TCP/IP 호스트 이름을 지정할 수 있습니다. 예를 들어 실수로 호스트 이름을 다른 시스템과 동일하게 지정한 경우 Permissions 파일의 MYNAME 옵션을 설정할 수 있습니다. 자신의 조직을 widget으로 알리려 한다고 가정합니다. 모든 모뎀이 호스트 이름이 gadget인 시스템에 연결된 경우 gadget의 Permissions 파일의 항목은 다음과 같을 수 있습니다.

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
  devices=Devices.cico:Devices
service=cu systems=Systems.cu:Systems \
```

```
dialers=Dialers.cu:Dialers \
devices=Devices.cu:Devices
```

이제 시스템 world가 widget에 로그인하는 것처럼 컴퓨터 gadget에 로그인할 수 있습니다. 사용자가 컴퓨터 world를 호출할 때 사용자도 가칭된 이름 widget으로 인식되도록 하려면 다음과 같은 항목이 있을 수 있습니다.

```
MACHINE=world MYNAME=widget
```

MYNAME 옵션은 컴퓨터가 자신을 호출하는 것도 허용하므로 테스트 용도로도 사용할 수 있습니다. 그러나 이 옵션은 컴퓨터의 실제 신원을 마스킹하는 데 사용될 수 있으므로 196 페이지 "UUCP VALIDATE 옵션"에 설명된 VALIDATE 옵션을 사용해야 합니다.

UUCP READ 및 WRITE 옵션

이러한 옵션은 uucico가 읽거나 쓸 수 있는 파일 시스템의 여러 부분을 지정합니다. READ 및 WRITE 옵션은 MACHINE 또는 LOGNAME 항목에 지정할 수 있습니다.

READ 및 WRITE 옵션의 기본값은 모두 다음 문자열에 표시된 uucppublic 디렉토리입니다.

```
READ=/var/spool/uucppublic WRITE=/var/spool/uucppublic
```

READ=/ 및 WRITE=/ 문자열은 기타 권한을 가진 로컬 사용자가 액세스할 수 있는 모든 파일에 액세스할 수 있는 권한을 지정합니다.

이러한 항목의 값은 콜론으로 구분한 경로 이름 목록입니다. READ 옵션은 파일을 요청하기 위한 것이고 WRITE 옵션은 파일을 배치하기 위한 것입니다. 값 중 하나는 입력하는 파일이나 기존 파일에 대한 전체 경로 이름의 접두어여야 합니다. 파일을 /usr/news 및 공용 디렉토리에 배치할 수 있는 권한을 부여하려면 WRITE 옵션에 다음 값을 사용합니다.

```
WRITE=/var/spool/uucppublic:/usr/news
```

READ 및 WRITE 옵션을 사용하는 경우 경로 이름은 기본 목록에 추가되지 않으므로 경로 이름을 모두 지정해야 합니다. 예를 들어 /usr/news 경로 이름만 WRITE 옵션에 지정한 경우 파일을 공용 디렉토리에 배치하는 권한은 거부됩니다.

원격 시스템이 액세스하여 읽고 쓸 수 있게 할 디렉토리를 주의해서 선택해야 합니다. 예를 들어 /etc 디렉토리에는 중요한 시스템 파일이 많이 포함되어 있습니다. 원격 사용자는 이 디렉토리에 파일을 배치할 수 있는 권한이 없어야 합니다.

UUCP NOREAD 및 NOWRITE 옵션

NOREAD 및 NOWRITE 옵션은 READ 및 WRITE 옵션 또는 기본값에 대한 예외를 지정합니다. 다음 항목은 /etc 디렉토리와 그 하위 디렉토리에 있는 파일을 제외한 모든 파일의 읽기를 허용합니다. 이러한 옵션은 접두어입니다.

```
READ=/ NOREAD=/etc WRITE=/var/spool/uucppublic
```

이 항목은 기본 /var/spool/uucppublic 디렉토리에만 쓰기를 허용합니다. NOWRITE 옵션은 NOREAD 옵션과 작동 방식이 동일합니다. NOREAD 및 NOWRITE 옵션은 LOGNAME 및 MACHINE 항목 모두에 지정할 수 있습니다.

UUCP CALLBACK 옵션

LOGNAME 항목에서 **콜백** 옵션을 사용하여 호출 시스템이 콜백할 때까지 트랜잭션이 발생하지 않도록 지정할 수 있습니다. CALLBACK을 설정하는 이유는 다음과 같습니다.

- 보안 목적 - 컴퓨터에 콜백하는 경우 올바른 컴퓨터인지 확인할 수 있습니다.
- 회계 목적 – 긴 데이터 전송을 수행하는 경우 장거리 전화에 대해 청구되는 컴퓨터를 선택할 수 있습니다.

CALLBACK=yes 문자열은 사용자 컴퓨터가 원격 컴퓨터에 콜백한 이후에만 파일 전송이 이루어질 수 있도록 지정합니다.

CALLBACK 옵션의 기본값은 CALLBACK=no입니다. CALLBACK을 yes로 설정하는 경우 나머지 대화에 영향을 주는 권한을 호출자에 해당하는 MACHINE 항목에 지정해야 합니다. LOGNAME 또는 원격 컴퓨터가 사용자 호스트에 대해 설정했을 수 있는 LOGNAME 항목에는 이러한 권한을 지정하지 마십시오.

주 – 두 사이트가 서로에 대해 **콜백** 옵션을 설정한 경우 대화가 시작되지 않습니다.

UUCP COMMANDS 옵션

주의 – COMMANDS 옵션은 시스템의 보안을 손상할 수 있습니다. 이 옵션은 특히 주의해서 사용하십시오.

MACHINE 항목에서 COMMANDS 옵션을 사용하면 원격 컴퓨터가 사용자 컴퓨터에서 실행할 수 있는 명령을 지정할 수 있습니다. uux 프로그램은 원격 실행 요청을 생성하고 원격

컴퓨터에 전송할 요청을 대기열에 대기시킵니다. 파일 및 명령은 대상 컴퓨터로 전송되어 원격 실행됩니다. 이는 시스템이 콜아웃할 때만 MACHINE 항목이 적용된다는 규칙에 대한 예외입니다.

COMMANDS는 LOGNAME 항목에서 사용되지 않습니다. MACHINE 항목의 COMMANDS는 사용자가 원격 시스템을 호출하거나 원격 시스템이 사용자를 호출하는 두 경우 모두에 명령 권한을 정의합니다.

COMMANDS=rmail 문자열은 원격 컴퓨터가 사용자 컴퓨터에서 실행할 수 있는 기본 명령을 지정합니다. MACHINE 항목에서 명령 문자열을 사용하는 경우 기본 명령이 대체됩니다. 예를 들어 다음 항목은 COMMAND 기본값을 대체하여 owl, raven, hawk 및 dove라는 컴퓨터가 사용자 컴퓨터에서 rmail, rnews 및 lp를 실행할 수 있게 합니다.

```
MACHINE=owl:raven:hawk:dove COMMANDS=rmail:rnews:lp
```

방금 지정한 이름뿐 아니라 명령의 전체 경로 이름도 포함할 수 있습니다. 예를 들어 다음 항목은 rmail 명령에서 기본 검색 경로를 사용하도록 지정합니다.

```
COMMANDS=rmail:/usr/local/rnews:/usr/local/lp
```

UUCP의 기본 검색 경로는 /bin 및 /usr/bin입니다. 원격 컴퓨터에서 rnews 또는 /usr/local/rnews를 실행할 명령으로 지정하는 경우 /usr/local/rnews는 기본 경로와 상관없이 실행됩니다. 마찬가지로 /usr/local/lp는 실행되는 lp 명령입니다.

목록에 ALL 값을 포함하면 항목에 지정된 원격 컴퓨터의 모든 명령이 실행됩니다. 이 값을 사용하는 경우 원격 컴퓨터에게 사용자 컴퓨터에 대한 모든 권한을 부여합니다.

주의 – 이 값을 사용하면 일반 사용자보다 더 많은 액세스 권한이 허용됩니다. 이 값은 두 컴퓨터가 동일한 사이트에 있고 밀접하게 연결되어 있으며 사용자를 신뢰할 수 있는 경우에만 사용해야 합니다.

다음은 ALL 값이 추가된 문자열입니다.

```
COMMANDS=/usr/local/rnews:ALL:/usr/local/lp
```

이 문자열에서는 다음 두 가지를 보여줍니다.

- ALL 값은 문자열에서 아무 곳에나 표시될 수 있습니다.
- 요청된 명령에 rnews 또는 lp의 전체 경로 이름이 포함되지 않은 경우 rnews 및 lp에 대해 지정한 경로 이름이 기본값 대신 사용됩니다.

COMMANDS 옵션에 cat 및 uucp와 같은 위험할 수 있는 명령을 사용하는 경우에는 항상 VALIDATE 옵션을 함께 사용해야 합니다. 파일을 읽거나 쓰는 모든 명령은 UUCP 원격 실행 데몬(uuxqt)에서 실행할 경우 로컬 보안에 잠재적으로 위험할 수 있습니다.

UUCP VALIDATE 옵션

컴퓨터 보안에 잠재적으로 위험할 수 있는 명령을 지정할 때는 항상 VALIDATE 옵션을 COMMANDS 옵션과 함께 사용합니다. VALIDATE는 COMMANDS 옵션의 맨 위에서 보안 레벨을 추가할 뿐이지만 ALL보다 안전한 명령 액세스를 여는 방법입니다.

VALIDATE를 사용하면 호출 컴퓨터의 호스트 이름과 사용하는 로그인 이름을 교차 확인하여 호출자의 신원을 일정 수준으로 검증할 수 있습니다. 다음 문자열은 widget 또는 gadget 외의 컴퓨터가 Uwidget으로 로그인하려고 하면 연결을 거부하도록 합니다.

```
LOGNAME=Uwidget VALIDATE=widget:gadget
```

VALIDATE 옵션을 사용하면 권한 있는 컴퓨터가 UUCP 트랜잭션을 위해 고유한 로그인 및 암호를 사용해야 합니다. 이 검증의 중요한 측면은 이 항목과 연관된 로그인 및 암호가 보호된다는 것입니다. 외부인이 이 정보를 얻게 되면 이 특정 VALIDATE 옵션은 더 이상 안전하다고 볼 수 없습니다.

UUCP 트랜잭션에 대한 권한이 있는 로그인 및 암호를 부여할 원격 컴퓨터를 신중히 선택하십시오. 원격 컴퓨터에 파일 액세스 및 원격 실행 기능이 있는 특별 로그인 및 암호를 제공하는 것은 해당 컴퓨터의 모든 사람에게 사용자 컴퓨터의 일반 로그인 및 암호를 제공하는 것과 같습니다. 따라서 원격 컴퓨터에 신뢰할 수 없는 사람이 있으면 해당 컴퓨터에 권한이 있는 로그인과 암호를 제공하지 마십시오.

다음 LOGNAME 항목은 eagle, owl 또는 hawk라고 주장하는 원격 컴퓨터 중 하나가 컴퓨터에 로그인하려고 하는 경우 uucpfriend 로그인을 사용했어야 한다고 지정합니다.

```
LOGNAME=uucpfriend VALIDATE=eagle:owl:hawk
```

외부인이 uucpfriend 로그인과 암호를 얻는 경우 쉽게 가장할 수 있습니다.

하지만 이 항목은 MACHINE 항목에만 표시되는 COMMANDS 옵션과 어떤 관련이 있습니까? 이 항목은 MACHINE 항목 및 COMMANDS 옵션을 권한 있는 로그인과 연관된 LOGNAME 항목에 연결합니다. 원격 컴퓨터가 로그인한 동안에는 실행 데몬이 실행되지 않기 때문에 이 연결이 필요합니다. 실제로 이 링크는 실행 요청을 보낸 컴퓨터를 알지 못하는 비동기 프로세스입니다. 따라서 사용자 컴퓨터에서 실행 파일의 출처를 어떻게 아는지가 실질적인 질문이 됩니다.

각 원격 컴퓨터는 사용자의 로컬 컴퓨터에 자체의 스풀 디렉토리가 있습니다. 이러한 스풀 디렉토리에는 UUCP 프로그램에만 부여된 쓰기 권한이 있습니다. 원격 컴퓨터의 실행 파일은 사용자 컴퓨터로 전송된 후 스풀 디렉토리에 저장됩니다. uuxqt 데몬이 실행되면 스풀 디렉토리 이름을 사용하여 Permissions 파일에서 MACHINE 항목을 찾고 COMMANDS 목록을 가져올 수 있습니다. 또는 컴퓨터 이름이 Permissions 파일에 표시되어 있지 않으면 기본 목록이 사용됩니다.

이 예에서는 MACHINE 및 LOGNAME 항목 간의 관계를 보여줍니다.

```
MACHINE=eagle:owl:hawk REQUEST=yes \
COMMANDS=rmail:/usr/local/rnews \
READ=/ WRITE=/
LOGNAME=uucpz VALIDATE=eagle:owl:hawk \
REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

COMMANDS 옵션의 값은 원격 사용자가 rmail 및 /usr/local/rnews를 실행할 수 있다는 것을 나타냅니다.

첫번째 항목에서는 나열된 컴퓨터 중 하나를 호출하려면 eagle, owl 또는 hawk를 호출한다고 가정해야 합니다. 따라서 eagle, owl 또는 hawk 스풀 디렉토리 중 하나로 저장되는 모든 파일은 이러한 컴퓨터 중 하나에 의해 거기에 저장됩니다. 원격 컴퓨터가 로그인하여 이러한 세 컴퓨터 중 하나라고 주장하는 경우 해당 실행 파일도 권한이 있는 스풀 디렉토리에 저장됩니다. 따라서 컴퓨터에 권한이 있는 로그인 uucpz가 있는지 확인해야 합니다.

OTHER에 대한 UUCP MACHINE 항목

특정 MACHINE 항목에서 언급하지 않은 원격 컴퓨터에 대해 다른 옵션 값을 지정할 수도 있습니다. 여러 컴퓨터가 사용자 호스트를 호출하고 명령 세트가 가끔 변경되는 경우에 이렇게 할 필요가 생길 수 있습니다. 다음 예에 나온 것처럼 이 항목에서는 컴퓨터 이름에 OTHER 이름을 사용합니다.

```
MACHINE=OTHER \
COMMANDS=rmail:rnews:/usr/local/Photo:/usr/local/xp
```

MACHINE 항목에 사용할 수 있는 다른 모든 옵션도 다른 MACHINE 항목에서 언급하지 않은 컴퓨터에 대해 설정할 수 있습니다.

UUCP의 MACHINE 및 LOGNAME 항목 결합

공통 옵션이 동일한 경우 MACHINE 및 LOGNAME 항목을 결합할 수 있습니다. 예를 들어 다음에 나오는 두 항목 세트는 동일한 REQUEST, READ 및 WRITE 옵션을 공유합니다.

```
MACHINE=eagle:owl:hawk REQUEST=yes \
READ=/ WRITE=/
```

및

```
LOGNAME=uupz REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

표시된 대로 이들 항목을 병합할 수 있습니다.

```
MACHINE=eagle:owl:hawk REQUEST=yes \
logname=uucpz SENDFILES-yes \
READ=/ WRITE=/
```

MACHINE 및 LOGNAME 항목을 결합하면 Permissions 파일을 보다 효율적으로 관리할 수 있습니다.

UUCP 전달

일련의 컴퓨터를 통해 파일을 보낼 경우 중개 컴퓨터의 COMMANDS 옵션에 uucp 명령이 포함되어 있어야 합니다. 다음 명령을 입력하는 경우 willow 컴퓨터에서 oak 컴퓨터가 uucp 프로그램을 실행할 수 있도록 허용하는 경우에만 전달 작업이 작동합니다.

```
% uucp sample.txt oak\!willow\!pine\!/usr/spool/uucppublic
```

또한 oak 컴퓨터에서도 사용자 컴퓨터가 uucp 프로그램을 실행할 수 있도록 허용해야 합니다. 마지막 컴퓨터로 지정된 pine 컴퓨터는 전달 작업을 수행하지 않으므로 uucp 명령을 허용하지 않아도 됩니다. 일반적으로는 컴퓨터를 이와 같이 설정하지 않습니다.

UUCP /etc/uucp/Poll 파일

/etc/uucp/Poll 파일에는 원격 컴퓨터 폴링에 필요한 정보가 포함됩니다. Poll 파일의 각 항목에는 호출할 원격 컴퓨터 이름, 탭 문자 또는 공백, 컴퓨터를 호출할 시간이 차례로 포함됩니다. Poll 파일에 있는 항목의 형식은 다음과 같습니다.

sys-name hour ...

예를 들어 **eagle 0 4 8 12 16 20** 항목을 사용하면 eagle 컴퓨터를 네 시간마다 폴링할 수 있습니다.

uudemon.poll 스크립트는 Poll 파일을 처리하지만 폴링을 실제로 수행하지는 않습니다. 이 스크립트는 스풀 디렉토리에서 항상 C.*file*이라는 폴링 작업 파일을 설정할 뿐입니다. uudemon.poll 셸 스크립트에서 스케줄러를 시작하고 스케줄러는 스풀 디렉토리의 모든 작업 파일을 검사합니다.

UUCP /etc/uucp/Config 파일

/etc/uucp/Config 파일을 사용하여 특정 매개변수를 수동으로 대체할 수 있습니다. Config 파일에 있는 각 항목의 형식은 다음과 같습니다.

parameter=value

구성 가능한 매개변수 이름의 전체 목록은 시스템과 함께 제공되는 Config 파일을 참조하십시오.

다음 Config 항목은 기본 프로토콜 순서를 Gge로 설정하고 G 프로토콜 기본값을 7개 창과 512바이트 패킷으로 변경합니다.

```
Protocol=G(7,512)ge
```

UUCP/etc/uucp/Grades 파일

/etc/uucp/Grades 파일에는 작업을 원격 컴퓨터의 대기열에 넣는 데 사용할 수 있는 작업 등급에 대한 정의가 포함됩니다. 이 파일에는 각 작업 등급에 대한 사용 권한도 포함됩니다. 이 파일의 각 항목은 사용자가 작업을 대기열에 넣을 수 있도록 하는 관리자 정의 작업 등급에 대한 정의를 나타냅니다.

Grades 파일에 있는 각 항목의 형식은 다음과 같습니다.

User-job-grade System-job-grade Job-size Permit-type ID-list

각 항목에는 공백으로 구분된 필드가 포함되어 있습니다. 항목의 마지막 필드는 역시 공백으로 구분된 하위 필드로 구성되어 있습니다. 한 항목이 둘 이상의 행을 차지하는 경우 백슬래시를 사용하여 항목을 다음 행으로 연결할 수 있습니다. 주석 행은 파운드 기호(#)로 시작하며 전체 행을 사용합니다. 빈 행은 항상 무시됩니다.

UUCP User-job-grade 필드

이 필드에는 최대 64자로 이루어진 관리자 정의 사용자 작업 등급 이름이 포함됩니다.

UUCP System-job-grade 필드

이 필드에는 *User-job-grade*가 매핑되는 단일 문자 작업 등급이 포함됩니다. 유효한 문자 목록은 A–Z, a–z이며, 우선 순위는 A가 가장 높고 z가 가장 낮습니다.

사용자 및 시스템 작업 등급 간 관계

사용자 작업 등급은 둘 이상의 시스템 작업 등급에 바인딩될 수 있습니다. Grades 파일에서 사용자 작업 등급 항목을 순서대로 검색합니다. 따라서 최대 작업 크기에 대한 제한에 따라 여러 시스템 작업 등급 항목이 나열되어야 합니다.

사용자 작업 등급에 대한 최대 개수는 없지만 허용되는 최대 시스템 작업 등급 수는 52개입니다. 둘 이상의 *User-job-grade*를 하나의 *System-job-grade*에 매핑할 수 있지만 각 *User-job-grade*는 파일에서 별도의 행에 있어야 하기 때문입니다. 다음은 예입니다.

```
mail N Any User Any netnews N Any User Any
```

이 구성이 Grades 파일에 있는 경우 이러한 두 *User-job-grade* 필드는 동일한 *System-job-grade*를 공유합니다. *Job-grade*에 대한 사용 권한은 *System-job-grade*가 아닌 *User-job-grade*와 연결되므로 두 *User-job-grade*는 동일한 *System-job-grade*를 공유하지만 사용 권한 세트는 서로 다를 수 있습니다.

기본 등급

기본 *User-job-grade*와 시스템 작업 등급의 바인딩을 정의할 수 있습니다. 키워드 기본값을 Grades 파일의 *User-job-grade* 필드에 있는 사용자 작업 등급 및 이 등급이 바인딩된 시스템 작업 등급으로 사용해야 합니다. 모든 사용자 및 모든 크기의 작업을 이 등급의 대기열에 넣을 수 있도록 Restrictions 및 ID 필드는 Any로 정의해야 합니다. 다음은 예입니다.

```
default a Any User Any
```

기본 사용자 작업 등급을 정의하지 않으면 내장 기본 등급인 Z가 사용됩니다. 제한 필드 기본값은 Any이므로 기본 등급 항목이 여러 개인지는 확인하지 않습니다.

UUCP Job-size 필드

이 필드는 대기열에 입력할 수 있는 최대 작업 크기를 지정합니다. *Job-size*는 바이트 단위로 측정되며 다음 목록에 설명된 옵션 목록일 수 있습니다.

nnnn	이 작업 등급의 최대 작업 크기를 지정하는 정수입니다.
*n*K	킬로바이트 수를 나타내는 10진수입니다(K는 킬로바이트의 약어).
*n*M	메가바이트 수를 나타내는 10진수입니다(M는 메가바이트의 약어).
Any	최대 작업 크기가 없음을 지정하는 키워드입니다.

다음은 몇 가지 예입니다.

- 5000은 5000바이트를 나타냅니다.
- 10K는 10KB를 나타냅니다.
- 2M은 2MB를 나타냅니다.

UUCP Permit-type 필드

이 필드에는 ID 목록을 해석할 방법을 나타내는 키워드가 포함됩니다. 다음 표에서는 키워드와 그 의미가 나와 있습니다.

표 12–5 Permit-type 필드

키워드	ID 목록 내용
User	이 작업 등급을 사용할 수 있는 사용자의 로그인 이름
Non-user	이 작업 등급을 사용할 수 없는 사용자의 로그인 이름
Group	구성원이 이 그룹을 사용할 수 있는 그룹 이름
Non-group	구성원이 이 작업 등급을 사용할 수 없는 그룹 이름

UUCP ID-list 필드

이 필드에는 이 작업 등급에 대한 대기열 할당이 허용되거나 정의된 로그인 이름 또는 그룹 이름의 목록이 포함됩니다. 이름 목록은 공백으로 구분되며 개행 문자로 끝납니다. Any 키워드를 사용하면 누구나 이 작업 등급의 대기열에 넣을 수 있도록 지정할 수 있습니다.

기타 UUCP 구성 파일

이 절에서는 자주 수정되지 않으며 UUCP 기능 사용에 영향을 주는 세 가지 파일에 대해 설명합니다.

UUCP /etc/uucp/Devconfig 파일

/etc/uucp/Devconfig 파일을 사용하여 uucp 또는 cu와 같은 서비스별로 장치를 구성할 수 있습니다. Devconfig 항목은 특정 장치에 사용되는 STREAMS 모듈을 정의합니다. 이러한 항목의 형식은 다음과 같습니다.

service=*x* device= *y* push= *z*[:*z*...]

*x*는 cu, uucico 또는 두 서비스 모두일 수 있으며 각 서비스는 콜론으로 구분됩니다. *y*는 네트워크 이름이며 Devices 파일의 항목과 일치해야 합니다. *z*는 STREAMS 모듈의 이름으로 대체되며, 그 순서는 모듈이 스트림에 푸시되는 순서와 같습니다. cu 및 uucp 서비스에 대해 모듈과 장치를 다르게 정의할 수 있습니다.

다음 항목은 STARLAN 네트워크에 적용되며 이 파일에서 가장 일반적으로 사용됩니다.

```
service=cu       device=STARLAN     push=ntty:tirdwr
service=uucico   device=STARLAN     push=ntty:tirdwr
```

이 예에서는 ntty, tirdwr을 순서대로 푸시합니다.

UUCP /etc/uucp/Limits 파일

/etc/uucp/Limits 파일은 uucp 네트워킹에서 실행 중인 동시 uucico, uuxqt 및 uusched의 최대 수를 제어합니다. 대부분의 경우 기본값을 사용 가능하며 변경할 필요가 없습니다. 변경하려면 텍스트 편집기를 사용하십시오.

Limits 파일의 형식은 다음과 같습니다.

service=*x* max= *y*:

*x*는 uucico, uuxqt 또는 uusched일 수 있고 *y*는 해당 서비스에 허용되는 한계입니다. 필드는 순서에 상관이 없고 소문자입니다.

다음 항목은 Limits 파일에서 가장 일반적으로 사용됩니다.

```
service=uucico max=5
service=uuxqt max=5
service=uusched max=2
```

이 예는 컴퓨터에서 uucico 5개, uuxqt 5개 및 uusched 2개를 실행할 수 있게 합니다.

UUCP remote.unknown 파일

통신 기능 사용에 영향을 주는 다른 파일은 remote.unknown 파일입니다. 이 파일은 Systems 파일에 없는 컴퓨터가 대화를 시작할 때 실행되는 이진 프로그램입니다. 이 프로그램은 대화 시도를 기록하고 연결을 끊습니다.

주의 – remote.unknown 파일의 사용 권한을 변경하여 파일을 실행할 수 없도록 하는 경우 시스템에서 모든 시스템의 연결을 허용합니다.

이 프로그램은 Systems에 없는 컴퓨터가 대화를 시작하면 실행됩니다. 이 프로그램은 대화를 시도했지만 연결하지 못한 경우를 기록합니다. 이 파일의 사용 권한을 변경하여 파일을 실행할 수 없도록 하는 경우(chmod 000 remote.unknown) 시스템에서 모든 대화 요청을 허용합니다. 이러한 변경은 단순하지 않습니다. 변경할 충분한 이유가 있어야 합니다.

UUCP 관리 파일

다음에서는 UUCP 관리 파일에 대해 설명합니다. 이러한 파일은 스풀 디렉토리에 만들며 장치를 잠그거나, 임시 데이터를 보관하거나, 원격 전송 또는 실행에 대한 정보를 보관하는 데 사용됩니다.

- *Temporary data files*(TM) – 이러한 데이터 파일은 다른 컴퓨터에서 파일을 받을 때 UUCP 프로세스가 스풀 디렉토리 /var/spool/uucp/*x* 아래에 만듭니다. *x* 디렉토리의 이름은 파일을 보내는 원격 컴퓨터와 같습니다. 임시 데이터 파일의 이름은 다음 형식을 사용합니다.

  TM.*pid.ddd*

  *pid*는 프로세스 ID이고 *ddd*는 0에서 시작하는 순차적 세 자리 숫자입니다.

  전체 파일을 받으면 TM.*pid.ddd* 파일은 전송의 원인이 된 C.*sysnxxxx* 파일(나중에 설명)에 지정된 경로 이름으로 이동됩니다. 처리가 비정상적으로 종료되면 TM.*pid.ddd* 파일이 *x* 디렉토리에 유지될 수 있습니다. 이러한 파일은 uucleanup에 의해 자동으로 제거됩니다.
- *Lock files*(LCK) – 잠금 파일은 사용 중인 각 장치의 /var/spool/locks 디렉토리에 만들어집니다. 잠금 파일은 중복된 대화와 동일한 호출 장치를 여러 번 사용하려는 시도를 방지합니다. 다음 표에서는 여러 유형의 UUCP 잠금 파일을 보여줍니다.

표 12–6 UUCP 잠금 파일

파일 이름	설명
LCK.*sys*	*sys*는 파일을 사용 중인 컴퓨터의 이름을 나타냅니다.
LCK.*dev*	*dev*는 파일을 사용 중인 장치의 이름을 나타냅니다.
LCK.*LOG*	*LOG*는 잠긴 UUCP 로그 파일을 나타냅니다.

컴퓨터가 충돌하는 경우와 같이 통신 링크가 예기치 않게 끊기는 경우 이러한 파일이 스풀 디렉토리에 남을 수 있습니다. 부모 프로세스가 더 이상 활성 상태가 아니면 잠금 파일은 무시(제거)됩니다. 잠금 파일에는 잠금을 만든 프로세스의 프로세스 ID가 포함됩니다.

- *Work file*(C.) – 작업 파일은 파일 전송, 원격 명령 실행 등의 작업을 원격 컴퓨터의 대기열에 넣은 경우 스풀 디렉토리에 만들어집니다. 작업 파일의 이름은 다음 형식을 사용합니다.

  C.*sysnxxxx*

  *sys*는 원격 컴퓨터의 이름이고, *n*은 작업의 등급(우선 순위)을 나타내는 ASCII 문자이고, *xxxx*는 UUCP에서 지정하는 4자리 작업 시퀀스 번호입니다. 작업 파일에는 다음 정보가 포함됩니다.
  - 보내거나 요청할 파일의 전체 경로 이름
  - 대상, 사용자 또는 파일 이름의 전체 경로 이름
  - 사용자 로그인 이름
  - 옵션 목록
  - 스풀 디렉토리에 있는 관련 데이터 파일의 이름. uucp -C 또는 uuto -p 옵션을 지정한 경우 임시 이름(D.0)이 사용됩니다.

- 소스 파일의 모드 비트
- 전송 완료 시 알림을 받는 원격 사용자의 로그인 이름

- *Data file*(`D.`) – 데이터 파일은 명령줄에 지정하여 소스 파일을 스풀 디렉토리로 복사할 때 만들어집니다. 데이터 파일의 이름은 다음 형식을 사용합니다.

  `D.`*systmxxxxyyy* – *systm*은 원격 컴퓨터 이름에서 처음 5개 문자입니다. *xxxx*는 `uucp`에서 지정하는 4자리 작업 시퀀스 번호입니다. 4자리 작업 시퀀스 번호 다음에서 후속 번호가 올 수 있습니다. *yyy*는 작업(`C.`) 파일에 대해 여러 `D.` 파일을 만드는 경우에 사용됩니다.

- `X.`*(execute file)* – 실행 파일은 원격 명령 실행 전에 스풀 디렉토리에 만들어집니다. 실행 파일의 이름은 다음 형식을 사용합니다.

  `X.`*sysnxxxx*

  *sys*는 원격 컴퓨터의 이름이고, *n*은 작업의 등급(우선 순위)을 나타내는 문자이고, *xxxx*는 UUCP에서 지정하는 4자리 작업 시퀀스 번호입니다. 실행 파일에는 다음 정보가 포함됩니다.

  - 요청자의 로그인 및 컴퓨터 이름
  - 실행해야 하는 파일의 이름
  - 명령 문자열의 표준 입력으로 사용할 입력
  - 명령 실행의 표준 출력을 받을 컴퓨터 및 파일 이름
  - 명령 문자열
  - 반환 상태 요청에 대한 옵션 행

UUCP 오류 메시지

이 절에서는 UUCP와 관련된 오류 메시지를 나열합니다.

UUCP ASSERT 오류 메시지

다음 표에서는 ASSERT 오류 메시지를 나열합니다.

표 12–7 ASSERT 오류 메시지

오류 메시지	설명 또는 작업
`CAN'T OPEN`	`open()` 또는 `fopen()`이 실패했습니다.
`CAN'T WRITE`	`write()`, `fwrite()`, `fprint()` 또는 유사한 명령이 실패했습니다.
`CAN'T READ`	`read()`, `fgets()` 또는 유사한 명령이 실패했습니다.
`CAN'T CREATE`	`creat()` 호출이 실패했습니다.
`CAN'T ALLOCATE`	동적 할당이 실패했습니다.

표 12–7 ASSERT 오류 메시지 (계속)

오류 메시지	설명 또는 작업
CAN'T LOCK	LCK(잠금) 파일을 만들지 못했습니다. 경우에 따라 치명적인 오류일 수 있습니다.
CAN'T STAT	stat() 호출이 실패했습니다.
CAN'T CHMOD	chmod() 호출이 실패했습니다.
CAN'T LINK	link() 호출이 실패했습니다.
CAN'T CHDIR	chdir() 호출이 실패했습니다.
CAN'T UNLINK	unlink() 호출이 실패했습니다.
WRONG ROLE	내부 논리 문제입니다.
CAN'T MOVE TO CORRUPTDIR	일부 잘못된 C. 또는 X. 파일을 /var/spool/uucp/.Corrupt 디렉토리로 이동하지 못했습니다. 디렉토리가 없거나 모드 또는 소유자가 잘못되었습니다.
CAN'T CLOSE	close() 또는 fclose() 호출이 실패했습니다.
FILE EXISTS	C. 또는 D. 파일을 생성하려고 했지만 파일이 이미 있습니다. 일반적으로 소프트웨어 오류를 나타내는 시퀀스 파일 액세스 관련 문제가 발생하는 경우 이 오류가 발생합니다.
NO uucp SERVICE NUMBER	TCP/IP 호출을 시도했지만 /etc/services에서 UUCP에 대한 항목이 없습니다.
BAD UID	사용자 ID가 암호 데이터베이스에 없습니다. 이름 서비스 구성을 확인하십시오.
BAD LOGIN_UID	이전 설명과 동일합니다.
BAD LINE	Devices 파일에 잘못된 행이 있습니다. 하나 이상의 행에 인수가 부족합니다.
SYSLST OVERFLOW	gename.c의 내부 테이블이 오버플로우되었습니다. 단일 작업에서 30개 이상의 시스템과 대화하려고 했습니다.
TOO MANY SAVED C FILES	이전 설명과 동일합니다.
RETURN FROM fixline ioctl	실패하면 안 되는 ioctl(2)이 실패했습니다. 시스템 드라이버 문제가 발생했습니다.
BAD SPEED	Devices 또는 Systems 파일(Class 또는 Speed 필드)에 잘못된 회선 속도가 표시됩니다.
BAD OPTION	Permissions 파일에 잘못된 행 또는 옵션이 있습니다. 이 오류는 바로 수정해야 합니다.
PKCGET READ	원격 컴퓨터가 행업된 것 같습니다. 아무 작업도 필요하지 않습니다.
PKXSTART	원격 컴퓨터가 복구할 수 있는 방식으로 중단되었습니다. 이 오류는 일반적으로 무시할 수 있습니다.
TOO MANY LOCKS	내부 문제가 발생했습니다. 시스템 공급업체에 문의하십시오.
XMV ERROR	일부 파일 또는 디렉토리에 문제가 발생했습니다. 스풀 디렉토리가 원인일 수 있으므로 이 프로세스를 시도하기 전에 대상 모드를 확인했어야 합니다.
CAN'T FORK	fork 및 exec를 수행하지 못했습니다. 현재 작업은 손실되지 않으며 나중에 시도됩니다(uuxqt). 아무 작업도 필요하지 않습니다.

UUCP STATUS 오류 메시지

다음 표에서는 일반적인 STATUS 오류 메시지를 나열합니다.

표 12–8 UUCP STATUS 메시지

오류 메시지	설명/작업
OK	상태가 적합합니다.
NO DEVICES AVAILABLE	호출에 사용할 수 있는 장치가 현재 없습니다. 특정 시스템의 Devices 파일에 유효한 장치가 있는지 확인하십시오. 시스템 호출에 사용할 장치가 있는지 Systems 파일에 있는지 확인하십시오.
WRONG TIME TO CALL	Systems 파일에 지정된 시간과 다른 시간에 시스템을 호출했습니다.
TALKING	설명이 필요하지 않습니다.
LOGIN FAILED	특정 컴퓨터에 로그인하지 못했습니다. 로그인 또는 암호가 잘못되었거나, 번호가 잘못되었거나, 컴퓨터가 느리거나, Dialer-Token-Pairs 스크립트를 실행하지 못했기 때문일 수 있습니다.
CONVERSATION FAILED	성공적인 시작 후 대화에 실패했습니다. 일반적으로 한 쪽이 다운되었거나, 프로그램이 중단되었거나, 회선(링크)이 끊긴 것을 나타냅니다.
DIAL FAILED	원격 컴퓨터가 응답하지 않습니다. 전화 걸기가 잘못되었거나 전화 번호가 틀릴 수 있습니다.
BAD LOGIN/MACHINE COMBINATION	Permissions 파일과 일치하지 않는 로그인/컴퓨터 이름을 사용하여 컴퓨터를 호출했습니다. 이 오류는 가장하려는 시도일 수 있습니다.
DEVICE LOCKED	사용할 호출 장치가 현재 잠겨 있고 다른 프로세스에서 사용되고 있습니다.
ASSERT ERROR	ASSERT 오류가 발생했습니다. /var/uucp/.Admin/errors 파일의 오류 메시지를 확인하고 204 페이지 “UUCP ASSERT 오류 메시지” 절을 참조하십시오.
SYSTEM NOT IN Systems FILE	시스템이 Systems 파일에 없습니다.
CAN’T ACCESS DEVICE	시도된 장치가 없거나 모드가 잘못되었습니다. Systems 및 Devices 파일에서 적절한 항목을 확인하십시오.
DEVICE FAILED	장치를 열 수 없습니다.
WRONG MACHINE NAME	호출된 컴퓨터가 예상과 다른 이름을 보고합니다.
CALLBACK REQUIRED	호출된 컴퓨터가 사용자 컴퓨터를 호출해야 합니다.
REMOTE HAS A LCK FILE FOR ME	원격 컴퓨터에 사용자 컴퓨터의 LCK 파일이 있습니다. 호출된 컴퓨터가 사용자 컴퓨터를 호출하려고 할 수 있습니다. 원격 컴퓨터에 이전 버전의 UUCP가 있는 경우 사용자 컴퓨터와 대화하던 프로세스가 실패하여 LCK 파일이 남았을 수 있습니다. 원격 컴퓨터가 최신 버전의 UUCP가 있고 사용자 컴퓨터와 통신하고 있지 않은 경우 LCK 파일을 사용하는 프로세스가 중단된 것입니다.
REMOTE DOES NOT KNOW ME	원격 컴퓨터의 Systems 파일에 사용자 컴퓨터의 노드 이름이 없습니다.

표 12–8 UUCP STATUS 메시지 *(계속)*

오류 메시지	설명/작업
REMOTE REJECT AFTER LOGIN	컴퓨터가 로그인할 때 사용한 로그인이 원격 컴퓨터가 예상한 것과 일치하지 않습니다.
REMOTE REJECT, UNKNOWN MESSAGE	원격 컴퓨터가 알 수 없는 이유로 사용자 컴퓨터와의 통신을 거부했습니다. 원격 컴퓨터에서 표준 버전의 UUCP를 실행하고 있지 않을 수 있습니다.
STARTUP FAILED	로그인에 성공했지만 초기 핸드셰이크가 실패했습니다.
CALLER SCRIPT FAILED	이 오류는 일반적으로 DIAL FAILED와 동일합니다. 그러나 이 오류가 자주 발생하는 경우 Dialers 파일의 호출자 스크립트가 원인일 수 있습니다. Uutry를 사용하여 확인하십시오.

UUCP 숫자 오류 메시지

다음 표에서는 /usr/include/sysexits.h 파일에서 생성하는 오류 상태 메시지의 종료 코드 번호를 나열합니다. 일부는 현재 uucp에서 사용되지 않습니다.

표 12–9 번호별 UUCP 오류 메시지

메시지 번호	설명	의미
64	오류 메시지의 기준 값	오류 메시지가 이 값에서 시작됩니다.
64	명령줄 사용 오류	명령을 잘못 사용했습니다. 예를 들어 잘못된 인수 수, 잘못된 플래그 또는 잘못된 구문을 사용했습니다.
65	데이터 형식 오류	입력 데이터가 잘못되었습니다. 이 데이터 형식은 사용자 데이터에만 사용해야 하며 시스템 파일에 사용하면 안 됩니다.
66	입력을 열 수 없음	시스템 파일이 아닌 입력 파일이 없거나 읽지 못했습니다. 이 문제는 메일러의 “No message(메시지가 없습니다)”와 같은 오류도 포함할 수 있습니다.
67	알 수 없는 주소	지정된 사용자가 없습니다. 이 오류는 메일 주소 또는 원격 로그인에 사용할 수 있습니다.
68	알 수 없는 호스트 이름	호스트가 없습니다. 이 오류는 메일 주소 또는 네트워크 요청에서 사용됩니다.
69	사용할 수 없는 서비스	서비스를 사용할 수 없습니다. 지원 프로그램 또는 파일이 없는 경우 오류가 발생할 수 있습니다. 또한 이 메시지는 일부 서비스가 작동하지 않지만 현재 그 이유를 알 수 없음을 나타내기도 합니다.
70	내부 소프트웨어 오류	내부 소프트웨어 오류가 감지되었습니다. 이 오류는 가급적 운영 체제와 관련 없는 오류로 제한됩니다.
71	시스템 오류	운영 체제 오류가 감지되었습니다. 이 오류는 “포크할 수 없음”, “파이프를 만들 수 없음”과 같은 상태에 사용하기 위한 것입니다. 예를 들어 이 오류에는 passwd 파일에 없는 사용자의 getuid 반환이 포함됩니다.

표 12–9 번호별 UUCP 오류 메시지 *(계속)*

메시지 번호	설명	의미
72	중요한 OS 파일 누락	/etc/passwd 또는 /var/admin/utmpx와 같은 시스템 파일이 없거나 열 수 없거나 구문 오류 같은 오류가 있습니다.
73	출력 파일을 만들 수 없음	사용자 지정 출력 파일을 만들 수 없습니다.
74	입출력 오류	일부 파일에서 I/O 수행 시 오류가 발생했습니다.
75	임시 오류. 사용자 재시도 유도	실제 오류가 아닌 임시 오류입니다. sendmail에서는 예를 들어 메일러에서 연결을 만들 수 없어 요청을 나중에 다시 시도해야 함을 나타냅니다.
76	프로토콜의 원격 오류	원격 시스템이 프로토콜 교환 중 "가능하지 않은" 항목을 반환했습니다.
77	사용 권한 거부	권한이 부족하여 작업을 수행할 수 없습니다. 이 메시지는 NOINPUT 또는 CANTCREAT를 사용해야 하는 시스템 문제에 적용되지 않고 상위 레벨 권한에 적용됩니다. 예를 들어 kre는 이 메시지를 사용하여 메일을 보낼 수 있는 학생을 제한할 수 있습니다.
78	구성 오류	구성에서 오류가 감지되었습니다.
79	항목을 찾을 수 없음	항목을 찾지 못했습니다.
79	나열된 최대 값	오류 메시지의 최상위 값입니다.

색인

D

E

G

I

V

대

데

동

디