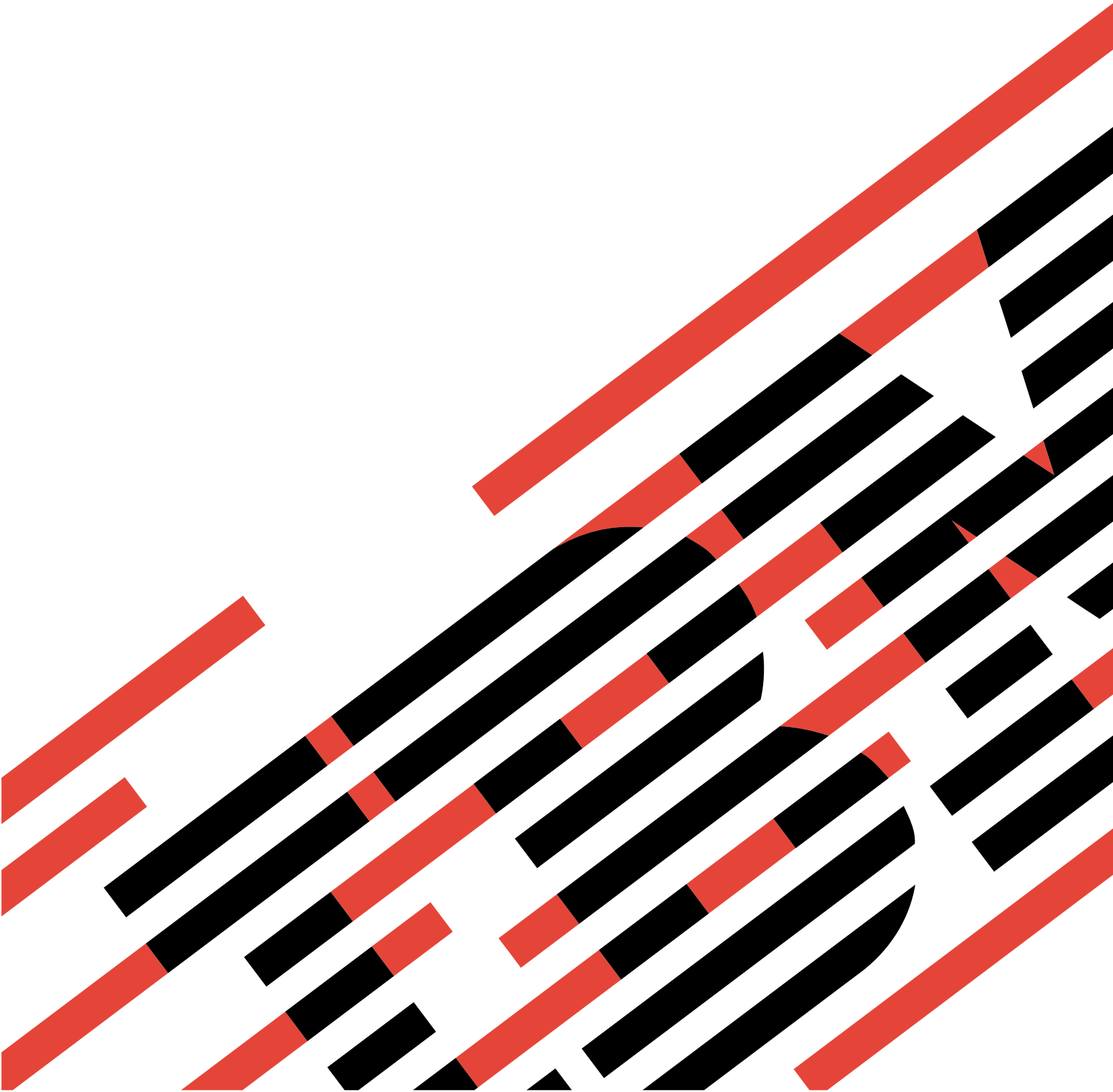
IBM

eserver

iSeries

리모트 액세스 서비스: PPP 연결



IBM

@server

iSeries

리모트 액세스 서비스: PPP 연결

목차

제 1 부 리모트 액세스 서비스: PPP 연결

지점 간 프로토콜(PPP)은 직렬 회선을 통해 자료를 전송하기 위한 인터넷 표준입니다. 이것은 인터넷 서비스 제공자(ISP) 사이에서 가장 널리 사용되는 연결 프로토콜입니다. PPP는 개별 컴퓨터가 네트워크에 액세스할 수 있게 함으로써 인터넷에 대한 액세스를 제공합니다. iSeries 서버는 광역 네트워크(WAN) 연결의 일부로서 TCP/IP PPP 지원을 포함하고 있습니다.

리모트 컴퓨터를 iSeries 서버에 연결할 때 PPP를 사용하여 각 위치 간에 자료를 교환할 수 있습니다. iSeries 서버에 연결되어 있는 리모트 시스템은 PPP를 통해 서버 등 네트워크에 속해 있는 자원 또는 기타 시스템에 액세스할 수 있습니다. PPP를 사용하여 인터넷에 연결하도록 iSeries 서버를 구성할 수도 있습니다. iSeries Navigator 전화 접속 연결 마법사가 iSeries 서버를 인터넷 또는 내부 네트워크에 연결하는 프로세스를 통해 사용자를 안내합니다.

- V5R2의 새로운 사항 이 릴리스에서의 리모트 액세스 서비스 갱신 내용을 설명합니다.
- 이 주제 인쇄를 통해 PDF 버전을 다운로드하거나 인쇄할 수 있습니다.

리모트 액세스 서비스 이해: PPP 연결

iSeries 400 서버에 있는 리모트 액세스 서비스를 요약하여 소개합니다. 아래의 주제는 현재 네트워크에서 PPP 환경을 계획할 때 도움이 되는 내용입니다.

- **PPP 시나리오**는 여러 가지 유형의 PPP 연결을 구현하기 위한 샘플입니다. 예별로 PPP 연결 구성에 대한 지침 및 샘플 값을 제공합니다.
- **PPP 개념**은 PPP 개념 정보 및 PPP 연결을 위한 iSeries 400 서버 요구사항을 제공합니다.
- **PPP 계획**은 PPP 개념 정보 및 PPP 연결을 위한 iSeries 400 서버 요구사항을 제공합니다.

리모트 액세스 서비스 사용: PPP 연결

iSeries 400 서버에서 PPP 연결을 구성하고 관리할 때 도움이 되는 내용을 수록하고 있습니다.

- **PPP 구성**은 PPP 연결에 대한 기본 단계를 개괄적으로 설명합니다.
- **PPP 관리**는 PPP 연결 관리 안내서로 사용할 수 있는 정보를 제공합니다.
- **PPP 문제 해결**은 기본 PPP 연결 오류에 대해 설명하고 관련된 문제 해결 정보를 알려줍니다.

여기에서 PPP에 관한 기타 정보를 볼 수도 있습니다. 이 페이지에는 관련 iSeries 서버 정보에 대한 유용한 링크가 포함되어 있습니다.

제 1 장 V5R2의 새로운 사항

V5R2에서는 iSeries Navigator를 통해 iSeries 서버에서 시작되는 PPPoE(PPP over Ethernet) 연결을 사용할 수 있습니다. 이러한 지원은 물리적 이더넷 회선에 바인드된 신규 PPPoE 가상 회선 유형을 제공하여 DSL 모뎀에 접속된 이더넷 LAN 어댑터를 사용하는 PPP 연결을 설정합니다. 일단 iSeries와 ISP 간의 연결이 시작되었으면 LAN 상의 각 사용자들이 iSeries PPPoE 연결을 통해 ISP에 액세스할 수 있습니다. 또한 개시자(Originator) 연결 프로파일 대화 상자나 범용 연결 마법사를 사용하여 새로운 기능에 액세스할 수 있습니다.

자세한 정보는 iSeries 서버를 PPPoE 액세스 집중기에 연결을 참조하십시오.

이제 다음과 같은 iSeries Navigator에 대한 몇몇 추가 작업을 통해 보다 쉽게 PPP 연결을 구성하고 관리할 수 있습니다.

- DHCP-WAN 구성 대화 상자가 자동으로 DHCP 서버 및 클라이언트 인터페이스에 연결되어 DHCP-WAN 클라이언트 인터페이스에 대한 IP 주소를 판별합니다. 이 대화 상자에 액세스하려면 다음과 같이 하십시오.
  - **네트워크 > 리모트 액세스 서비스**를 펼치십시오.
  - **리모트 액세스 서비스**를 마우스 오른쪽 버튼으로 클릭하십시오.
  - **서비스**를 선택하십시오.
  - **DHCP-WAN** 탭을 선택하십시오.
- 그 성능을 향상시킨 연결 상태 대화 상자를 통해 L2TP, L2TP 멀티홉, 멀티링크 및 PPPoE 연결에 대한 연결 세부사항을 표시되므로 보다 쉽게 PPP 연결을 관리할 수 있습니다.
- 개시자(Originator) 및 수신자 연결 프로파일과 그룹 액세스 정책을 작성할 수 있는 기능이 타스크 패드에 추가되었습니다.
- 신규 다이얼 연결 마법사 및 범용 연결 마법사의 이름이 신규 인터넷 또는 ISP 다이얼 연결 그리고 신규 IBM 범용 연결로 바뀌었습니다.
- 개시자(Originator) 연결 프로파일이 호출(들어오는)을 기다리는 수신자 연결 프로파일에 할당된 ppp 회선과 모뎀을 ″빌려올 수(borrow)″ 있습니다. 연결이 끝나면 연결을 시작한 PPP 회선과 모뎀을 수신자 연결 프로파일에 ″리턴″합니다. 이러한 새로운 기능을 작동할 수 있게 하려면 ppp 회선 구성 대화 상자의 모뎀 탭에서 **동적 자원 공유 사용** 옵션을 선택하십시오. 그러면 수신자 및 개시자(Originator) 연결 프로파일의 연결 탭에서 PPP 회선을 구성할 수 있습니다.
- 회선 풀(pool)이 사용 중인 경우에는 회선 풀 문제가 발생하는 것을 방지하기 위해 수정하지 못할 경우가 있습니다.
- 요구 시 개시자 및 요구 시 리모트 다이얼온 작동 모드가 L2TP 연결을 사용하는 Originator 연결 프로파일에서 삭제되었습니다.

제 2 장 이 주제 인쇄

이 문서를 PDF 버전으로 보거나 다운로드할 수 있습니다. PDF 파일을 보려면 Adobe® Acrobat® Reader가 필요합니다. Adobe 에서 사본을 다운로드 받을 수 있습니다.

PDF 버전을 보거나 다운로드하려면 리모트 액세스 서비스: PPP 연결 (277KB 또는 약 58 페이지)을 선택하십시오.

PDF를 워크스테이션에 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 여십시오. (위의 링크를 클릭하십시오.)
2. 브라우저 메뉴에서 **파일**을 클릭하십시오.
3. **다른 이름으로 저장**을 클릭하십시오.
4. PDF를 저장할 디렉토리로 이동하십시오.
5. **저장**을 클릭하십시오.

제 3 장 PPP 시나리오

다음 시나리오는 PPP가 작동하는 방식과 사용자 네트워크에 PPP 환경을 구현하는 방법을 이해하는 데 도움을 줄 것입니다. 이 시나리오는 초보 사용자와 전문 사용자 모두 계획 및 구성 타스크로 진행하기 전에 이용할 수 있는 기본 PPP 개념을 소개합니다.

시나리오: iSeries 서버를 PPPoE 액세스 집중기에 연결

많은 ISP가 PPPoE를 사용하는 DSL을 통해 고속의 인터넷 액세스를 제공합니다. iSeries 서버는 이러한 서비스 제공자에 연결하여 PPP의 장점을 활용하는 고속 연결을 제공합니다.

시나리오: 리모트 다이얼 인 클라이언트를 iSeries 서버에 연결

텔레커뮤터나 모바일 클라이언트와 같은 리모트 사용자의 경우 수시로 회사 네트워크에 액세스해야 할 것입니다. 이와 같은 다이얼 인 클라이언트는 PPP로 iSeries 서버에 액세스할 수 있습니다.

시나리오: 모뎀을 사용하여 오피스 LAN을 인터넷에 연결

일반적으로 관리자가 직원들이 인터넷에 액세스할 수 있는 오피스 네트워크를 설정합니다. 이때 모뎀을 사용하여 Iseries 서버를 인터넷 서비스 제공자(ISP)에 연결할 수 있습니다. LAN 접속 PC 클라이언트는 iSeries 서버를 게이트웨이로 사용하여 인터넷과 통신할 수 있습니다.

시나리오: 모뎀을 사용하여 기업과 리모트 네트워크 연결

모뎀은 두 개의 리모트 위치(예: 본사와 지사)에서 자료를 교환할 수 있게 해 줍니다. PPP는 본사에 있는 iSeries 서버와 지사에 있는 다른 iSeries 서버 간에 연결을 설정하여 두 개의 LAN을 연결합니다.

시나리오: RADIUS NAS를 이용한 전화 접속 연결 인증

iSeries 서버에서 실행 중인 NAS(Network Access Server)는 다이얼 인 클라이언트에서 RADIUS 서버로 요구하는 인증을 라우트할 수 있습니다. 인증이 이루어지면 RADIUS 또한 사용자의 IP 주소 및 포트를 제어할 수 있습니다.

시나리오: 그룹 정책 및 IP 필터링을 사용하여 자원에 대한 리모트 사용자 액세스 관리

그룹 액세스 정책을 통해 연결에 대한 고유한 사용자 그룹을 식별하여 일부 공통된 연결 속성과 보안 설정을 전체 그룹에 적용할 수 있습니다. 또한 이 기능을 IP 필터링과 조합하여 네트워크 상의 특정 IP 주소에 대한 액세스를 허용하거나 제한할 수 있습니다.

시나리오: 단일 iSeries 서버에 있는 PPP 및 DHCP

다이얼 인 클라이언트나 리모트 사용자는 PPP를 사용하여 회사 네트워크에 있는 iSeries 서버에 액세스할 수 있습니다. 동일한 iSeries 상의 DHCP 광역 네트워크(WAN) 클라이언트를 사용할 경우 리모트 사용자가 LAN 접속 사용자와 동일한 서비스로 동적으로 할당된 IP 주소를 확보할 수 있습니다.

시나리오: 다른 iSeries 서버에 있는 DHCP 및 PPP 프로파일

보안 문제 또는 네트워크의 물리적 배치 문제로 인해 대부분의 회사들은 네트워크 서비스를 분리시키고 이를 여러 서버에 분산시킵니다. 이 시나리오는 별도의 PPP 서버와 DHCP 서버를 가진 더욱 복잡한 상황을 다루고 있습니다. 이전 시나리오와 마찬가지로 이 설정 또한 리모트 사용자가 회사 네트워크에 다이얼하여 액세스할 수 있게 해 줍니다.

시나리오: PPP 및 VPN: VPN에 의해 보호되는 L2TP 자발적 터널

지사에서는 계층 2 터널 프로토콜(L2TP)을 통해 본사에 연결할 수 있습니다. L2TP 자발적 터널은 가상 PPP 링크를 설정합니다. 실제로 L2TP는 본사의 네트워크를 확장하여 지사가 기업 서브네트의 일부로 나타나게 됩니다. VPN은 L2TP 터널 상의 자료 통신을 보호합니다.

시나리오: iSeries 서버를 PPPoE 액세스 집중기에 연결

상황: 업무 상 보다 빠른 인터넷 연결이 필요하여 로컬ISP를 사용하는 DSL 서비스에 관심을 갖고 있습니다. 사전 조사 결과 ISP가 PPPoE를 사용하여 클라이언트에 연결한다는 것을 알게 되었습니다. 따라서 이 PPPoE 연결을 사용하여 iSeries 서버를 통한 고속 인터넷 연결을 제공하려고 합니다.

그림 1. PPPoE를 사용하는 ISP에 iSeries 서버 연결

솔루션: iSeries 서버를 통해 ISP에 대한 PPPoE 연결을 지원할 수 있습니다. iSeries 서버는 2838 유형의 이더넷 어댑터를 사용하기 위해 구성된 물리적 이더넷 회선에 바인드시킨 신규 PPPoE 가상 회선 유형을 사용합니다. 이 가상 회선은 리모트 ISP에 대한 게이트웨이를 제공하는 DSL 모뎀에 연결된 이더넷 LAN을 통해 PPP 세션 프로토콜을 지원합니다. 이렇게 함으로써 LAN 연결 사용자가 iSeries 서버 PPPoE 연결을 사용하

여 고속의 인터넷 액세스를 사용할 수 있습니다. 일단 iSeries와 ISP 간의 연결이 시작되면 LAN 상의 각 사용자들이 iSeries 서버에 할당된 IP 주소를 사용하여 PPPoE를 통해 ISP에 액세스할 수 있습니다. 추가 보안을 제공하려면 필터 규칙을 PPPoE 가상 회선에 적용하여 특정 인바운드 인터넷 통신을 제한하면 됩니다.

샘플 구성:

1. ISP와 함께 사용할 수 있도록 연결 장치를 구성하십시오.
2. iSeries 서버에서 개시자 연결 프로파일을 구성하십시오.

   다음 정보를 반드시 입력하십시오.

   - **프로토콜 유형**: PPP
   - **연결 유형**: 이더넷을 통한 PPP
   - **작동 모드**: 개시자
   - **링크 구성**: 단일 회선
3. 신규 지점 간 프로파일 등록 정보의 **일반** 페이지에서 작성자 프로파일에 대한 이름과 설명을 입력하십시오. 이 이름이 연결 프로파일과 가상 PPPoE 회선을 모두 지칭합니다.
4. **연결** 페이지를 클릭하십시오. 이 연결 프로파일의 이름에 해당되는 **PPPoE 가상 회선 이름**을 선택하십시오. 회선을 선택하면 iSeries Navigator가 회선 등록 정보 대화 상자를 표시합니다.
   a. **일반** 페이지에서 PPPoE 가상 회선에 대해 의미 있는 설명을 입력하십시오.
   b. **링크** 페이지를 클릭하십시오. 물리적 회선 이름 선택 목록에서 그 연결에 사용할 이더넷 회선을 선택하고 **열기**를 클릭하십시오. 또는 신규 이더넷 회선을 정의해야 할 경우 회선 이름을 입력하고 **신규**를 클릭하십시오. 그러면 iSeries Navigator가 회선 등록 정보 대화 상자를 표시합니다.
      주: PPPoE에는 2838 유형의 이더넷 어댑터가 필요합니다.
      1) **일반** 페이지에서 Ethernet 회선에 대해 의미 있는 설명을 입력한 후 회선 정의가 원하는 하드웨어 자원을 사용하고 있는지 확인하십시오.
      2) **링크** 페이지를 클릭하십시오. 물리적 이더넷 회선에 대한 등록 정보를 입력하십시오. 자세한 정보는 이더넷 카드 및 온라인 도움말에 대한 문서를 참조하십시오.
      3) **기타** 페이지를 클릭하십시오. 기타 사용자들이 이 회선에 대해 필요로 하는 액세스 레벨과 권한을 지정하십시오.
      4) **확인**을 클릭하여 PPPoE 가상 회선 등록 정보 페이지로 가십시오.
   c. **제한**을 클릭하여 LCP 인증에 대한 등록 정보를 정의하거나 **확인**을 클릭하여 신규 지점 간 프로파일 **연결** 페이지로 가십시오.
5. ISP에 iSeries 서버 자체 인증이 필요하거나 iSeries가 리모트 서버를 인증해야 할 경우 **인증** 페이지를 클릭하십시오. 자세한 정보는 시스템 인증을 참조하십시오.
6. **TCP/IP 설정** 페이지를 클릭하고, 이 연결 프로파일에 대한 IP 주소 처리 매개변수를 지정하십시오. LAN 연결 사용자가 iSeries 서버에 할당된 IP 주소를 사용하여 ISP에 연결하도록 하려면 **숨겨진 주소(전체 가장)**을 선택하십시오.
7. **DNS** 페이지를 클릭하고 ISP가 제공한 DNS 서버의 IP 주소를 입력하십시오.

8. 연결 작업을 실행하기 위한 서브시스템을 지정하려면 **기타** 페이지를 클릭하십시오.

9. 프로파일을 완료하려면 **확인**을 클릭하십시오.

사용자 액세스를 외부 IP 주소나 또는 iSeries 자원으로 제한하는 것에 대한 정보는 IP 필터링 및 그룹 액세스 정책을 참조하십시오.

시나리오: 리모트 다이얼 인 클라이언트를 iSeries 서버에 연결

상황: 회사의 네트워크 관리자로서 본인이 iSeries 서버와 네트워크 클라이언트를 모두 유지보수해야 합니다. 이 경우 문제를 해결하고 수정하기 위해 사무실에 나오는 대신 자신의 집과 같은 리모트 위치에서 작업하는 것을 원할 수 있습니다. 그러나 회사에 인터넷 바운드 네트워크 연결이 설정되어 있지 않으므로 PPP 연결을 사용하여 iSeries 서버에 접속해야 할 것입니다. 또한 현재 사용 중인 유일한 모뎀이 7852-400 ECS 모뎀이므로 이 모뎀을 연결에 활용할 수도 있습니다.

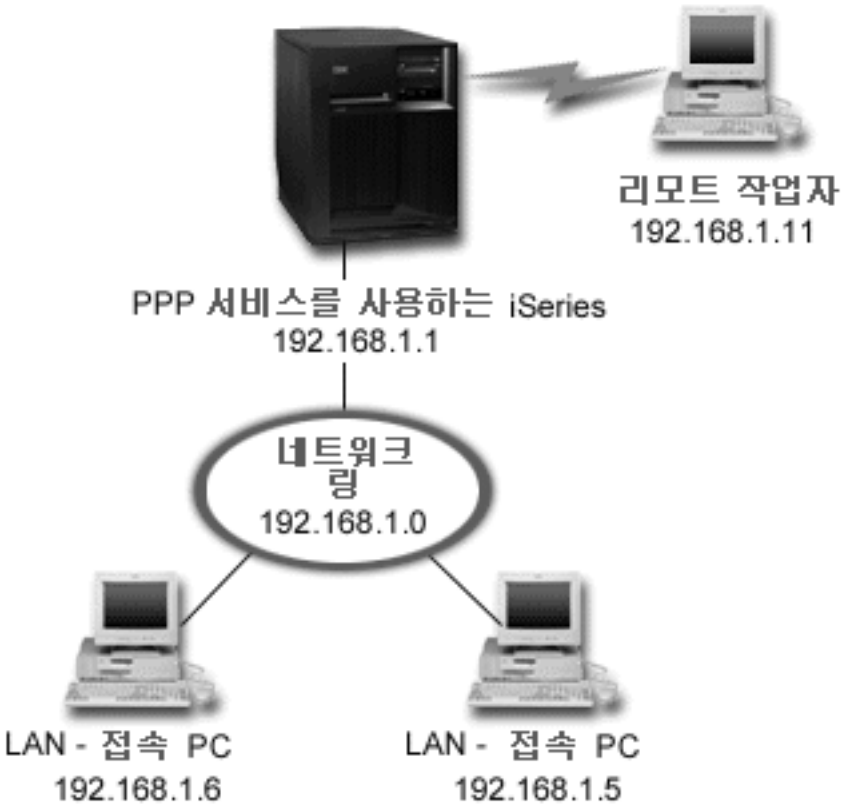


그림 2. 리모트 클라이언트를 iSeries 서버에 연결

솔루션: 모뎀을 사용하여 홈 PC를 iSeries 서버에 연결하는 데 PPP를 사용할 수 있습니다. 이와 같은 유형의 PPP 연결용으로 ECS 모뎀을 사용 중이므로 사용자의 모뎀이 동기 및 비동기 모드의 두 가지 모두로 구성되어 있는지 확인해야 합니다. 위의 그림은 두 대의 PC로 LAN에 연결되어 PPP 서비스를 사용하는 iSeries 서

버를 나타냅니다. 리모트 작업자가 iSeries 서버에 다이얼하여 인증을 받으면 작업 네트워크의 일부가 됩니다 (192.168.1.0). 이 경우, 정적 IP 주소를 다이얼 인 클라이언트로 지정하는 것이 가장 쉽습니다.

리모트 작업자는 iSeries 서버와의 인증에 CHAP-MD5를 사용합니다. iSeries는 MS_CHAP을 사용할 수 없으므로 PPP 클라이언트가 CHAP-MD5를 사용하도록 설정되어 있는지 확인해야 합니다.

리모트 작업자가 위에 나오는 것처럼 회사 네트워크에 액세스할 수 있게 하려면 IP 이송이 PPP 수신자 프로파일과 마찬가지로 TCP/IP 스택에 온으로 설정되어 있어야 하고, IP 라우팅이 바르게 구성되어야 합니다. 또한 리모트 클라이언트가 네트워크에서 취할 수 있는 조치를 제한하거나 보호하려는 경우 IP 패킷을 처리할 때 필터링 규칙을 사용할 수 있습니다.

위의 그림에는 ECS 모뎀이 한번에 하나의 연결만 처리할 수 있으므로 하나의 리모트 다이얼 인 클라이언트만 있습니다. 여러 다이얼 인 클라이언트가 동시에 필요한 경우에는 하드웨어 및 소프트웨어 고려사항에 대한 계획 섹션을 참조하십시오.

샘플 구성:

1. 리모트 PC에서 전화 접속 네트워킹을 구성하고 전화 접속 연결을 작성하십시오.
2. iSeries 서버에서 수신자 연결 프로파일을 구성하십시오.

   다음 정보를 반드시 입력하십시오.

   - **프로토콜 유형**: PPP
   - **연결 유형**: 교환 회선
   - **작동 모드**: 응답
   - **링크 구성**: 사용자 환경에 따라 단일 회선 또는 회선 풀이 될 수 있습니다.
3. 신규 지점 간 프로파일 등록 정보의 **일반** 페이지에서 수신자 프로파일에 대한 이름과 설명을 입력하십시오.
4. **연결** 페이지를 클릭하십시오. 적절한 **회선 이름**을 선택하거나 신규 이름을 입력하고 **신규**를 클릭하여 신규 회선을 작성하십시오.
   a. **일반** 페이지에서, 기존 하드웨어 자원을 강조표시하고 프레임 처리를 **비동기**로 설정하십시오.
   b. **모뎀** 페이지를 클릭하십시오. 이름 선택 리스트에서 **IBM 2772** 모뎀을 선택하십시오.
   c. **확인**을 클릭하여 신규 지점 간 프로파일 등록 정보 페이지로 가십시오.
5. **인증** 페이지를 클릭하십시오.
   a. **iSeries 서버가 리모트 시스템의 ID 확인**을 선택하십시오.
   b. **유효성 검사 리스트를 사용하여 로컬로 인증**을 선택하고 신규 리모트 사용자를 유효성 검사 리스트에 추가하십시오.
   c. **암호 암호화 허용(CHAP-MD5)**을 선택하십시오.
6. **TCP/IP 설정** 페이지를 클릭하십시오.
   a. 192.168.1.1의 로컬 IP 주소를 선택하십시오.
   b. 리모트 주소의 경우 시작 주소가 192.168.1.11인 **고정 IP 주소**를 선택하십시오.

c. **리모트 시스템에 다른 네트워크 액세스 허용**을 선택하십시오.

7. 프로파일을 완료하려면 **확인**을 클릭하십시오.

시나리오: 모뎀을 사용하여 오피스 LAN을 인터넷에 연결

상황: 회사에서 현재 사용하는 기업 어플리케이션이 사용자들의 인터넷 액세스를 요구합니다. 어플리케이션이 많은 양의 자료 교환을 필요로 하지 않으므로 iSeries 서버 및 LAN 접속 PC 클라이언트를 인터넷에 연결할 때 모뎀을 사용할 수 있습니다. 다음 그림은 이러한 상황을 설명한 것입니다.

그림 3. 모뎀을 사용하여 오피스 LAN을 인터넷에 연결

솔루션: ECS 모뎀(또는 다른 호환 모뎀)을 사용하여 iSeries를 인터넷 서비스 제공자(ISP)와 연결할 수 있습니다. ISP에 PPP 연결을 설정하기 위해서는 서버에 PPP 작성자 프로파일을 작성해야 합니다.

iSeries와 PPP 사이에 연결을 작성하면 LAN 접속 PC가 iSeries를 게이트웨이로 사용하여 인터넷과 통신할 수 있습니다. 작성자 프로파일에서 IP 주소를 예약한 LAN 클라이언트가 인터넷과 통신할 수 있도록 주소 숨기기 옵션을 온으로 설정했는지 확인할 수 있습니다.

이제 iSeries와 네트워크가 인터넷에 접속되었으므로 보안 위험 요소에 관한 여러 가지를 알아야 합니다. ISP의 보안 정책을 이해하고 사용자의 서버 및 네트워크를 보호하기 위한 추가 조치를 위해 ISP와 함께 작업하십시오.

이와 같은 유형의 PPP 연결용으로 ECS 모뎀을 사용 중이면 모뎀을 비동기 통신으로 구성하십시오. 인터넷 용도에 따라 대역폭이 문제가 될 수 있습니다. 연결의 대역폭을 증가시키는 방법에 대해 자세히 알려면 계획 섹션을 참조하십시오.

샘플 구성:

1. iSeries 서버에서 개시자 연결 프로파일을 구성하십시오.

   반드시 다음 정보를 선택하십시오.

   - **프로토콜 유형**: PPP
   - **연결 유형**: 교환 회선
   - **작동 모드**: 다이얼
   - **링크 구성**: 사용자 환경에 따라 단일 회선 또는 회선 풀이 될 수 있습니다.
2. 신규 지점 간 프로파일 등록 정보의 **일반** 페이지에서 개시자 프로파일에 대한 이름과 설명을 입력하십시오.
3. **연결** 페이지를 클릭하십시오. 적절한 회선 이름을 선택하거나 신규 이름을 입력하고 **신규**를 클릭하여 신규 회선을 작성하십시오.
   a. 신규 회선 등록 정보의 **일반** 페이지에서 기존 하드웨어 자원을 강조표시하고 프레임 처리를 **비동기**로 설정하십시오.
   b. **모뎀** 페이지를 클릭하십시오. 이름 선택 리스트에서 사용 중인 모뎀을 선택하십시오.
   c. **확인**을 클릭하여 신규 지점 간 프로파일 등록 정보 페이지로 가십시오.
4. **추가**를 클릭한 후 ISP 서버에 다이얼할 전화 번호를 입력하십시오. 필요한 모든 접두부를 포함하고 있는지 확인하십시오.
5. **인증** 페이지를 클릭하고 **리모트 시스템에 이 iSeries 서버의 ID 확인 허용**을 선택하십시오. 인증 프로토콜을 선택한 후 필요한 모든 사용자 이름이나 암호 정보를 입력하십시오.
6. TCP/IP 설정 페이지를 클릭하십시오.
   a. 로컬 및 리모트 IP 주소 모두에 대해 **리모트 시스템이 할당**을 선택하십시오.
   b. **리모트 시스템을 디폴트 라우트로 추가**를 선택하십시오.
   c. 내부 IP 주소가 인터넷에 라우트되지 않도록 **주소 숨기기**를 선택하십시오.
7. **DNS** 페이지를 클릭하고 ISP가 제공한 DNS 서버의 IP 주소를 입력하십시오.
8. 프로파일을 완료하려면 **확인**을 클릭하십시오.

인터넷에 연결하기 위해 연결 프로파일을 사용하려면 Operations Navigator에서 연결 프로파일을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오. 상태가 **활동**으로 바뀌면 연결에 성공한 것입니다. 화면정리를 통해 화면을 갱신하십시오.

주: 네트워크에 있는 다른 시스템에 적절한 라우팅이 정의되어 이들 시스템에서 인터넷 바운드 TCP/IP 통신이 iSeries 서버로 송신되는지도 확인해야 합니다.

시나리오: 모뎀을 사용하여 기업과 리모트 네트워크 연결

상황: 두 곳의 다른 위치에 지사와 본사 네트워크를 가지고 있는 것으로 가정하십시오. 지사에서는 자료 입력 어플리케이션을 위한 데이터베이스 정보를 교환하기 위해 매일 본사와 연결합니다. 교환되는 자료의 양이 물리적 네트워크 연결을 별도로 구매해야 할 정도는 아니므로 모뎀을 사용하여 필요한 두 개의 네트워크를 연결하기로 결정합니다.

그림 4. 모뎀을 사용하여 기업과 리모트 네트워크를 연결

솔루션 PPP는 위의 그림에서와 같이 각 iSeries 서버 간에 연결을 설정하여 두 개의 LAN을 함께 연결할 수 있습니다. 이 경우 지사에서 본사와의 연결을 시작하는 것으로 가정하십시오. 리모트 iSeries에서 개시자 프로파일을 구성하고 본사 서버에서 수신자 프로파일을 구성합니다.

지사 PC가 본사 LAN(192.168.1.0)에 액세스해야 하는 경우 본사 수신자 프로파일에서 IP 이송이 작동(on) 상태이고, IP 주소 라우팅이 PC(192.168.2, 192.168.3, 192.168.1.6 및 이 예에 있는 192.168.1.5)에 대해 사용 가능한 상태이어야 합니다. 또한 TCP/IP 스택에 대한 IP 이송도 활성화되어야 합니다. 이 구성은 LAN 간의 기본 TCP/IP 통신을 가능하게 하는 것입니다. LAN 간의 호스트 이름을 해결하기 위해서는 보안 요소 및 DNS를 고려해야 합니다.

샘플 구성:

1. 리모트 오피스 iSeries 서버에서 개시자 연결 프로파일 구성을 시작하십시오.

   반드시 다음 정보를 선택하십시오.

   - **프로토콜 유형**: PPP
   - **연결 유형**: 교환 회선
   - **작동 모드**: 다이얼
   - **링크 구성**: 사용자 환경에 따라 단일 회선 또는 회선 풀이 될 수 있습니다.
2. 신규 지점 간 프로파일 등록 정보의 **일반** 페이지에서 개시자 프로파일에 대한 이름과 설명을 입력하십시오.
3. **연결** 페이지를 클릭하십시오. 적절한 회선 이름을 선택하거나 신규 이름을 입력하고 **신규**를 클릭하여 신규 회선을 작성하십시오.
   a. 신규 회선 등록 정보의 **일반** 페이지에서 기존 하드웨어 자원을 강조표시하고 프레임 처리를 **비동기**로 설정하십시오.
   b. **모뎀** 페이지를 클릭하십시오. 이름 선택 리스트에서 사용 중인 모뎀을 선택하십시오.
   c. **확인**을 클릭하여 신규 지점 간 프로파일 등록 정보 페이지로 가십시오.
4. **추가**를 클릭한 후 본사 iSeries 서버에 다이얼할 전화 번호를 입력하십시오. 필요한 모든 접두부를 포함하고 있는지 확인하십시오.
5. **인증** 페이지를 클릭하고 **리모트 시스템에 이 iSeries 서버의 ID 확인 허용**을 선택하십시오. **암호 암호화 요구(CHAP-MD5)**를 선택하고, 필요한 사용자 이름 또는 암호 정보를 입력하십시오.
6. **TCP/IP 설정** 페이지를 클릭하십시오.
   a. 로컬 IP 주소에 대해 **고정 IP 주소 사용** 선택 상자에서 리모트 오피스 LAN 인터페이스의 IP 주소(192.168.2.1)를 선택하십시오.
   b. 리모트 IP 주소에 대해, **리모트 시스템이 할당**을 선택하십시오.
   c. 라우팅 섹션에서, **리모트 시스템을 디폴트 라우트로 추가**를 선택하십시오.
   d. 개시자 프로파일을 완료하려면 **확인**을 클릭하십시오.
7. 중앙 오피스의 iSeries 서버에서 **수신자 연결 프로파일**을 구성하십시오.

   반드시 다음 정보를 선택하십시오.

- **프로토콜 유형**: PPP
- **연결 유형**: 교환 회선
- **작동 모드**: 응답
- **링크 구성**: 사용자 환경에 따라 단일 회선 또는 회선 풀이 될 수 있습니다.

8. 신규 지점 간 프로파일 등록 정보의 **일반** 페이지에서, 수신자 프로파일에 대한 이름과 설명을 입력하십시오.
9. **연결** 페이지를 클릭하십시오. 적절한 회선 이름을 선택하거나 신규 이름을 입력하고 **신규**를 클릭하여 신규 회선을 작성하십시오.
   a. **일반** 페이지에서, 기존 하드웨어 자원을 강조표시하고 프레임 처리를 **비동기**로 설정하십시오.
   b. **모뎀** 페이지를 클릭하십시오. 이름 선택 리스트에서 사용 중인 모뎀을 선택하십시오.
   c. **확인**을 클릭하여 신규 지점 간 프로파일 등록 정보 페이지로 가십시오.
10. **인증** 페이지를 클릭하십시오.
    a. **iSeries 서버가 리모트 시스템의 ID 확인**을 선택하십시오.
    b. 신규 리모트 사용자를 유효성 확인 리스트에 추가하십시오.
    c. CHAP-MD5 인증을 선택하십시오.
11. **TCP/IP 설정** 페이지를 클릭하십시오.
    a. 로컬 IP 주소의 경우 선택 상자에서 본사 인터페이스의 IP 주소(192.168.1.1)를 선택하십시오.
    b. 리모트 IP 주소의 경우 **리모트 시스템의 사용자 ID에 따라**를 선택하십시오. 사용자명별 IP 주소 정의 대화 상자가 표시됩니다. **추가**를 클릭하십시오. 호출 사용자 이름, IP 주소 및 서브네트 마스크에 대한 필드를 입력하십시오. 이 시나리오에서는 다음과 같이 입력할 수 있습니다.
       - 호출 사용자 이름: `Remote_site`
       - IP 주소: `192.168.2.1`
       - 서브네트 마스크: `255.255.255.0`

       확인을 클릭한 후 다시 **확인**을 클릭하여 TCP/IP 설정 페이지로 가십시오.
    c. 네트워크에 있는 다른 시스템이 이 iSeries 서버를 게이트웨이로 사용할 수 있도록 하려면 **IP 이송**을 선택하십시오.
12. 수신자 프로파일을 완료하려면 **확인**을 클릭하십시오.

시나리오: RADIUS NAS를 이용한 전화 접속 연결 인증

상황: 회사 네트워크에 분산 전화 접속 네트워킹으로부터 두 개의 iSeries 서버에 연결되는 리모트 사용자가 있습니다. 그리고 인증, 서비스 및 계정을 중앙화하여 하나의 서버에서 사용자 ID 및 암호 유효성 확인에 대한 요청을 처리하고 IP 주소를 판별하게 하려고 합니다.

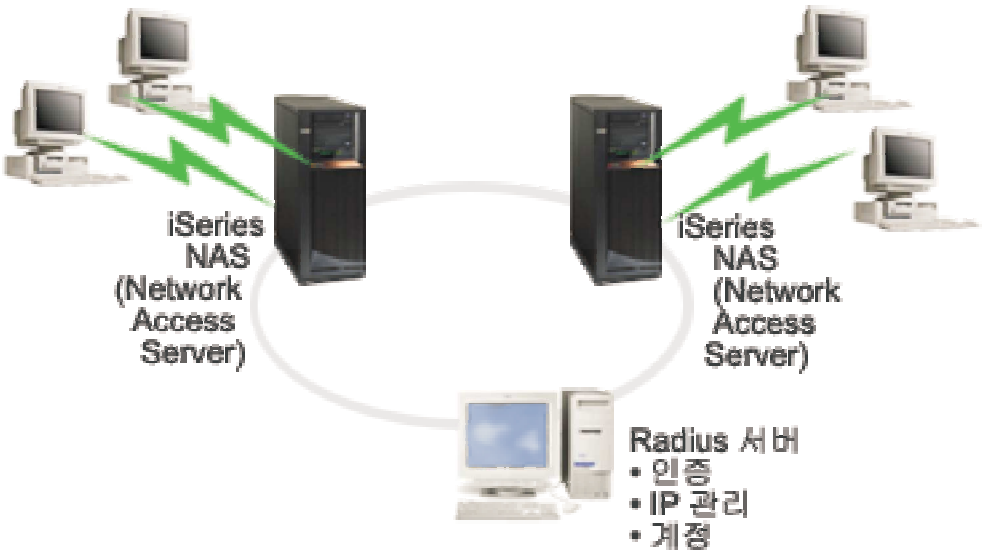


그림 5. RADIUS 서버를 사용하여 전화 접속 연결 인증

솔루션: 연결을 시도할 때 iSeries 서버에서 실행 중인 네트워크 액세스 서버(NAS)가 인증 정보를 네트워크 상의 RADIUS 서버에 전달합니다. 네트워크에 대한 모든 인증 정보를 유지보수하는 RADIUS 서버가 인증 요청과 응답을 처리합니다. 유효한 사용자로 판단되면 RADIUS 서버 또한 피어(peer)의 IP 주소를 할당하도록 구성할 수 있으며 사용자 활동 및 사용을 추적하도록 활성화할 수 있습니다. RADIUS를 지원하려면 iSeries에서 RADIUS NAS 서버를 정의하십시오.

샘플 구성:

1. iSeries Navigator에서 **네트워크**를 펼치고 **리모트 액세스 서비스**를 마우스 오른쪽 버튼으로 클릭한 후 **서비스**를 선택하십시오.
2. **RADIUS** 탭에서 **RADIUS 네트워크 액세스 서버 연결 사용**을 선택하고 **인증을 위해 RADIUS 사용**을 선택하십시오. RADIUS 솔루션에 따라 RADIUS가 연결 계정 및 TCP/IP 주소 구성을 처리하도록 선택할 수 있습니다.
3. **RADIUS NAS 설정** 버튼을 클릭하십시오.
4. **일반** 페이지에서 이 서버에 대한 설명을 입력하십시오.
5. 인증 서버(및 선택적으로 계정 서버) 페이지에서 **추가**를 클릭하고 다음 정보를 입력하십시오.
   a. **로컬 IP 주소** 상자에서 RADIUS 서버에 연결하는 데 필요한 iSeries 인터페이스에 대한 IP 주소를 입력하십시오.
   b. **서버 IP 주소 상자**에서 RADIUS 서버에 대한 IP 주소를 입력하십시오.
   c. **암호** 상자에서 iSeries 서버를 RADIUS 서버로 식별하는 데 사용되는 암호를 입력하십시오.
   d. 포트 상자에서 RADIUS 서버와의 통신에 사용되는 iSeries의 포트를 입력하십시오. 인증 서버에는 1812 포트, 계정 서버에는 1813을 입력하십시오.
6. **확인**을 클릭하십시오.

7. iSeries Navigator에서 **네트워크 > 리모트 액세스 서비스**를 펼치십시오.
8. 인증을 위해 RADIUS 서버를 사용할 연결 프로파일을 선택하십시오. RADIUS 서비스는 수신자 연결 프로파일에 대해서만 적용할 수 있습니다.
9. 인증 페이지에서 **iSeries 서버가 리모트 시스템의 ID 확인**을 선택하십시오.
10. **RADIUS 서버를 사용하여 리모트로 인증**을 선택하십시오.
11. 인증 프로토콜을 선택하십시오(EAP, PAP 또는 CHAP-MD5). 또한 이 프로토콜을 RADIUS 서버도 사용해야 합니다. 자세한 정보는 시스템 인증을 참조하십시오.
12. **연결 편집 및 계정용으로 RADIUS 사용**을 선택하십시오.
13. **확인**을 클릭하여 연결 프로파일로 변경된 사항을 저장하십시오.

또한 인증 프로토콜, 사용자 자료, 암호 및 계정 정보에 대한 지원을 포함하여 RADIUS 서버를 설정해야 합니다. 자세한 정보는 RADIUS 업체로 문의하십시오.

사용자가 이 연결 프로파일을 사용하여 접속하는 경우 iSeries가 인증 정보를 지정된 RADIUS 서버에 전달합니다. 유효한 사용자로 판별되면 연결이 허용되며 사용자의 정보에 따라 지정된 RADIUS 상의 연결 제한을 적용할 수 있습니다.

시나리오: 그룹 정책 및 IP 필터링을 사용하여 자원에 대한 리모트 사용자 액세스 관리

상황: 네트워크에 몇몇 분산 사용자 그룹이 있으며 각각의 사용자 모두 회사 LAN 상의 다른 자원에 액세스해야 합니다. 자료 입력 그룹의 사용자들은 데이터베이스 및 몇몇 기타 어플리케이션에 대해 액세스를 필요로 하는 반면에 경영 동반자사는 HTTP, FTP 및 텔넷 서비스에 대한 전화 접속 액세스를 필요로 하지만 보안상의 이유로 인해 다른 TCP/IP 서비스나 통신으로의 연결을 허용해서는 안됩니다. 각 사용자에 대한 자세한 연결 속성과 허용을 정의하는 일에는 많은 노력이 필요하며 연결을 사용하는 모든 사용자에 대해 일률적으로 네트워크 제한을 제공하면 충분한 제어가 이루어지지 않습니다. 따라서 반복적으로 서버에 접속하는 몇몇 고유 사용자 그룹에 대해서는 연결 설정 및 권한 정의 방법이 필요합니다.

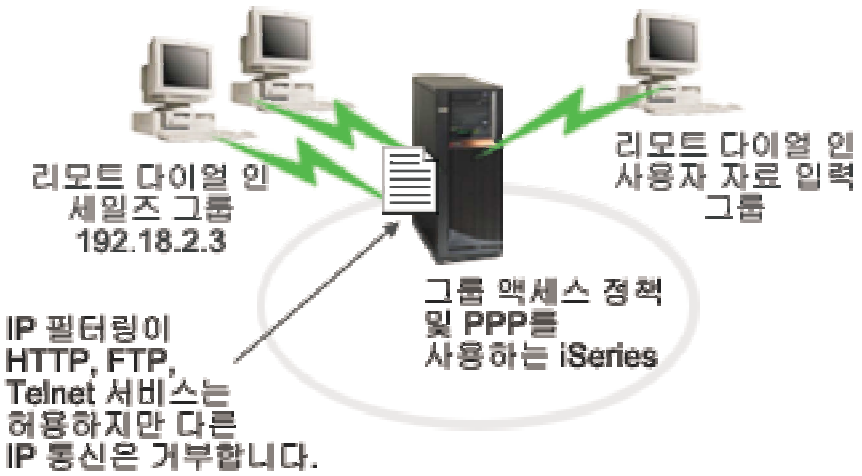


그림 6. 그룹 정책 설정을 기초로 전화 접속 연결에 연결 설정 적용

솔루션: 두 개의 서로 다른 사용자 그룹에 고유한 IP 필터링 제한을 적용하십시오. 따라서 그룹 액세스 정책과 IP 필터링 규칙을 작성해야 합니다. 그룹 액세스 정책은 IP 필터링 규칙을 참조하므로 필터링 규칙을 먼저 작성해야 합니다. 이 예에서는 ″경영 동반자사″ 그룹의 액세스 정책에 대한 IP 필터링 규칙을 포함하는 ppp 필터를 작성해야 합니다. 이러한 필터 규칙은 HTTP, FTP 및 Telnet 서비스를 허용하되 iSeries 서버를 통한 다른 모든 TCP/IP 통신 및 서비스에 대한 액세스는 제한합니다. 이 시나리오에서는 세일즈 그룹에 필요한 필터 규칙만을 보여주지만 ″자료 입력″ 그룹에 대해서도 유사한 필터를 설정할 수 있습니다.

마지막으로 그룹을 정의하기 위한 그룹 액세스 정책(그룹당 하나)을 작성해야 합니다. 그룹 액세스 정책을 통해 사용자 그룹에 공통적인 연결 속성을 정의할 수 있습니다. iSeries 서버 상의 유효성 리스트에 그룹 액세스 정책을 추가하여 이러한 연결 설정을 인증 프로세스에 적용할 수 있습니다. 그룹 액세스 정책은 IP 주소 및 세션에서 사용자의 TCP/IP 서비스 사용 여부를 제한하는 IP 필터링 규칙을 적용하는 속성을 포함하여 세션에 대한 몇 가지 설정을 지정합니다.

샘플 구성:

1. 이 그룹 액세스 정책에 대한 허용 및 제한을 지정하는 PPP 필터 식별자 및 IP 패킷 규칙 필터를 작성하십시오. IP 필터링에 대한 자세한 정보는 IP 패킷 규칙(필터링 및 NAT)을 참조하십시오.
   a. iSeries Navigator에서 **네트워크 > 리모트 액세스 서비스**를 펼치십시오.
   b. **수신자 연결 프로파일**을 클릭하고 이 연결을 위한 연결 프로파일을 마우스 오른쪽 버튼으로 클릭한 후 **등록 정보**를 선택하십시오.
   c. **TCP/IP 설정** 탭을 선택하고 **확장**을 클릭하십시오.
   d. **이 연결에 IP 패킷 규칙 사용**을 선택하고 **규칙 파일 편집**을 클릭하십시오. 이렇게 하면 IP 패킷 규칙 편집기가 시작되어 PPP 필터 패킷 규칙 파일이 열립니다.
   e. **삽입** 메뉴를 열고 **필터**를 선택하여 필터 세트를 추가하십시오. **일반** 탭을 사용하여 필터 세트를 정의하고, **서비스** 탭을 사용하여 사용자가 허용하는 서비스(예: HTTP)를 정의하십시오. 다음 필터는

"services_rules"가 HTTP, FTP 및 Telnet 서비스를 허용하도록 설정합니다. 필터 규칙에는 명시적으로 허용되지 않은 임의의 TCP/IP 서비스 또는 IP 통신을 제한하는 암묵적인 디폴트 거부 명령문이 포함됩니다.

주: 다음 예에 나오는 IP 주소는 전역적으로 라우트시킬 수 있으며 예제용입니다.

```
###The following 2 filters will permit HTTP (Web browser) traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 80 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        80 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = * SRCADDR =  %
        * DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS =  %
        NONE JRN = OFF

###The following 4 filters will permit FTP traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 21 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        21 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 20 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        20 FRAGMENTS = NONE JRN = OFF
###The following 2 filters will permit telnet traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.54.5.1 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.54.5.1 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

f. **삽입** 메뉴를 열고 **필터 인터페이스**를 선택하십시오. 필터 인터페이스를 사용하여 PPP 필터 식별자를 작성하여 직접 정의한 필터 설정을 포함시키십시오.

   1) 일반 탭에서 PPP 필터 ID에 대해

      ```
      permited_services
      ```

      를 입력하십시오.

   2) **필터 세트** 탭에서 **services_rules** 필터 세트를 선택하고 **추가**를 클릭하십시오.

3) 확인을 클릭하십시오. 다음 행이 규칙 파일에 추가됩니다.

```
###The following statement binds (associates) the 'services_rules' filter set with the
PPP filter ID "permitted_services." This PPP filter ID
can then be applied to the physical interface associated with a PPP connection profile
or Group Access Policy.

FILTER_INTERFACE PPP_FILTER_ID = permited_services SET = services_rules
```

g. 변경 사항을 저장한 후 나가십시오. 나중에 이러한 변경 사항을 취소하려면 문자 기반의 인터페이스를 사용하여 명령을 입력하십시오.

```
RMVTCPTBL
```

이렇게 하면 서버에서 모든 필터 규칙과 NAT가 제거됩니다.

h. **고급 TCP/IP 설정** 대화 상자에서 **PPP 필터 식별자** 상자를 공백으로 남겨두고 **확인**을 클릭하여 종료하십시오. 그리고 나서 방금 작성한 필터 식별자를 이 연결 프로파일이 아니라 그룹 액세스 정책에 적용하십시오.

2. 이 사용자 그룹에 대한 신규 그룹 액세스 정책을 정의하십시오. 그룹 액세스 정책에 대한 옵션의 자세한 설명은 그룹 액세스 정책 구성을 참조하십시오.

a. iSeries Navigator에서 **네트워크 > 리모트 액세스 서비스 > 수신자 연결 프로파일**을 펼치십시오.

b. 그룹 액세스 정책 아이콘을 마우스 오른쪽 버튼으로 클릭하고 신규 그룹 액세스 정책을 선택하십시오. iSeries Navigator가 신규 그룹 액세스 정책 정의 대화 상자를 표시합니다.

c. 일반 페이지에서 그룹 액세스 정책에 대한 이름 및 설명을 입력하십시오.

d. **TCP/IP 설정** 페이지에서

- **이 연결에 IP 패킷 규칙 사용**을 선택하고 PPP 필터 ID **permitted_services**를 선택하십시오.

e. **확인**을 선택하여 그룹 액세스 정책을 저장하십시오.

3. 그룹 액세스 정책을 이 그룹과 연관된 사용자에 적용하십시오.

a. 이러한 전화 접속 연결을 제어하는 수신자 연결 프로파일을 여십시오.

b. 수신자 연결 프로파일의 **인증** 페이지에서 사용자의 인증 정보가 포함된 유효성 검사 리스트를 선택하고 **열기**를 클릭하십시오.

c. 세일즈 그룹에서 그룹 액세스 정책을 적용할 사용자를 선택한 다음, **열기**를 클릭하십시오.

d. **사용자에 그룹 정책 적용**을 클릭하고 2단계에서 정의한 그룹 액세스 정책을 선택하십시오.

e. 각 세일즈 사용자에 대해 해당 단계를 반복하십시오.

PPP 연결을 통한 사용자 인증에 관해서는 시스템 인증을 참조하십시오.

제 4 장 PPP 개념

PPP를 사용하여 iSeries 서버를 리모트 네트워크, 클라이언트 PC, 기타 iSeries 또는 ISP에 연결할 수 있습니다. 이 프로토콜을 제대로 이용하기 위해서는 이 프로토콜의 기능과 iSeries 지원을 모두 이해해야 합니다. 자세한 정보는 다음 주제를 참조하십시오.

PPP란?
지점 간 프로토콜(PPP)은 하나의 컴퓨터 시스템을 다른 컴퓨터 시스템에 연결하는 데 사용되는 TCP/IP 프로토콜입니다. 자세한 정의는 이 주제를 참조하십시오.

연결 프로파일
지점 간 연결 프로파일이 특정 PPP 연결에 대한 매개변수 및 자원의 세트를 정의합니다. 이러한 매개변수 설정을 사용하는 프로파일을 시작하여 ppp 연결을 다이얼 아웃(시작)하거나 청취(수신)할 수 있습니다.

그룹 액세스 정책
이러한 정책들이 사용자 그룹에 대한 일련의 연결 및 보안 속성을 정의합니다. 시스템에 이러한 사항을 정의하는 것에 관한 정보는 이 주제를 참조하십시오.

PPP란?

컴퓨터는 **PPP** 또는 **지점 간 프로토콜**을 사용하여 전화선을 통해 인터넷에서 통신합니다. PPP 연결은 두 대의 시스템이 전화선을 통해 물리적으로 연결될 때 존재합니다. PPP를 사용하여 한 시스템을 다른 시스템에 연결할 수 있습니다. 예를 들어, 지사와 본사 간에 설정된 PPP 연결은 각 사무소가 네트워크를 통해 다른 사무소로 자료를 전송할 수 있게 해 줍니다.

PPP는 인터넷 표준입니다. 이것은 인터넷 서비스 제공자(ISP) 사이에서 가장 널리 사용되는 연결 프로토콜입니다. PPP를 사용하여 ISP에 연결되면 ISP가 사용자에게 인터넷과의 연결을 제공합니다.

PPP는 서로 다른 제조업체의 리모트 액세스 소프트웨어 간에서 상호운영성을 허용합니다. 또한 여러 네트워크 통신 프로토콜이 같은 물리적 통신 회선을 사용할 수 있게 해 줍니다.

다음 RFC(Request For Comment) 표준이 PPP 프로토콜을 설명합니다. http://www.rfc-editor.org에서 RFC에 관한 자세한 정보를 찾을 수 있습니다.

- RFC1661 지점 간 프로토콜
- HDLC식 프레임 처리에 관한 RFC1662 PPP
- RFC1994 PPP CHAP

연결 프로파일

V5R2는 두 가지 유형의 프로파일을 사용하므로 ppp 연결 또는 연결 집합에 대한 일련의 특성을 정의할 수 있습니다.

- **개시자 연결 프로파일**은 로컬 iSeries 서버에서 시작하여 리모트 시스템에서 수신되는 지점 간 연결입니다. 이 오브젝트를 사용하여 아웃바운드 연결을 구성할 수 있습니다.

- **수신자 연결 프로파일**은 리모트 시스템에서 시작하여 로컬 iSeries 서버에서 수신되는 지점 간 연결입니다. 이 오브젝트를 사용하여 인바운드 연결을 구성할 수 있습니다.

연결 프로파일이 PPP 연결의 작동 방식을 지정합니다. 연결 프로파일의 정보가 다음 질문에 대한 답을 제공합니다.

- 사용할 연결 프로토콜의 유형은? (PPP 또는 SLIP)
- iSeries 서버가 다이얼링을 통해 다른 컴퓨터에 접속하는가(개시자)? iSeries 서버가 다른 시스템으로부터의 호출을 수신하기 위해 대기해야 하는가(수신자)?
- 연결에 사용할 통신 회선은?
- iSeries 서버는 사용할 IP 주소를 어떻게 판별하는가?
- iSeries 서버는 다른 시스템을 어떻게 인증하는가? iSeries 서버는 인증 정보를 어디에 저장하는가?

연결 프로파일은 다음과 같은 연결 세부사항의 논리적 표현입니다.

- 회선 및 프로파일 유형
- 멀티링크 설정
- 리모트 전화 번호 및 다이얼링 옵션
- 인증
- TCP/IP 설정: IP 주소 및 라우팅, IP 필터링
- 작업 관리 및 연결 사용자 정의
- 정의역명 서버

iSeries 서버는 이 구성 정보를 연결 프로파일에 저장합니다. iSeries 서버가 다른 컴퓨터 시스템과 PPP 연결을 설정할 때 필요한 정보를 제공합니다. 연결 프로파일에는 다음과 같은 정보가 들어 있습니다.

- **프로토콜 유형**. PPP와 SLIP 중에서 선택할 수 있습니다. IBM에서는 PPP를 권장합니다.
- **모뎀 선택**. 이 연결 프로파일에 대한 연결 유형 및 작동 모드.

  연결 유형은 연결된 회선의 유형을 지정하고 이 유형이 **다이얼**인지 아니면 **응답**인지를 나타냅니다(개시자 또는 수신자, 각각에 대해). 다음 연결 유형 중에서 선택할 수 있습니다.

  – 교환 회선
  – 전용 회선
  – L2TP(가상 회선)
  – PPPoE(가상 회선)

  PPPoE는 개시자 연결 프로파일에 대해서만 지원됩니다.
- **작동 모드**. 사용할 수 있는 작동 모드는 연결 유형에 따라 다릅니다. 다음 표를 참조하십시오.

개시자 연결 프로파일은 다음 표를 참조하십시오.

표 1. 수신자 연결 프로파일에 대해 사용할 수 있는 작동 모드

연결 유형	사용할 수 있는 작동 모드
교환 회선	– 다이얼 – 요구 시 다이얼(다이얼 전용) – 요구 시 다이얼(전용 피어(peer)에 대해 사용할 수 있는 응답) – 요구 시 다이얼(리모트 피어(peer) 장치 사용 가능)
전용 회선	개시자
L2TP	– 개시자 – 멀티 홉 개시자 – 리모트 다이얼
이더넷을 통한 PPP	개시자

수신자 연결 프로파일은 다음 표를 참조하십시오.

표 2. 개시자(Originator) 연결 프로파일에 대해 사용할 수 있는 작동 모드

연결 유형	사용할 수 있는 작동 모드
교환 회선	응답
전용 회선	종료자
L2TP	종료자(네트워크 서버)

- **링크 구성**. 이 연결이 사용하는 회선 서비스 유형을 지정합니다.

  이 선택사항은 사용자가 선택하는 모드 선택 유형에 따라 다릅니다. 교환 회선 및 전용 회선의 경우 다음 중에서 선택할 수 있습니다.

  – 단일 회선

  – 회선 풀

  – 통합 ISDN 회선

  기타 모든 연결 유형(전용, L2TP, PPPoE)의 경우 회선 서비스 선택에서 단일 회선만 선택할 수 있습니다.

그룹 정책 지원

그룹 정책 지원은 네트워크 관리자가 자원 관리에 도움이 되는 사용자 기본 그룹 정책을 정의할 수 있도록 하고, PPP 또는 L2TP 세션으로 네트워크에 로그인할 때 개별 사용자에게 액세스 제어 정책이 지정될 수 있도록 합니다. 이 개념은 사용자들을 특정 사용자 클래스에 속한 것으로 식별시킬 수 있는 개념으로서 각 클래스에 자체적인 고유 정책이 있다는 것을 의미합니다. 각 고유 그룹 정책을 사용하여 멀티링크 번들에 허용되는 링크 수와 같은 자원 한계, IP 이송과 같은 속성, 그리고 적용할 IP 패킷 필터 규칙 세트의 ID 등을 정의할 수 있습니다. 예를 들어, 네트워크 관리자는 그룹 정책 지원을 사용하여 Vendor_Workers 그룹을 더욱 제한된 서비스 세트로 제한시킬 수 있는 반면에 해당 사용자 클래스가 네트워크에 대해 전체 액세스를 갖는 Work_at_Home 그룹을 정의할 수 있습니다.

예를 보려면, 시나리오: 그룹 액세스 정책 및 IP 주소 필터링을 사용하여 자원에 대한 사용자 액세스 관리를 참조하십시오.

제 5 장 PPP 계획

PPP 연결을 작성하고 관리하기 위해서는 PPP 지원 및 iSeries 서버에서의 다른 연결 방식에 대해 잘 알아야 하며 업무에 필요한 네트워킹 및 보안 계획에 대해서도 이해가 필요합니다. 다음 주제에서는 iSeries PPP 연결에서 사용할 수 있는 옵션과 요구사항에 대해서 설명합니다.

소프트웨어 및 하드웨어 요구사항
iSeries Navigator V4R4 이상은 PPP 연결을 지원합니다. 기타 요구사항 리스트는 이 주제를 참조하십시오.

연결 대안
iSeries는 아날로그 또는 디지털 전화 회선에서부터 전용 또는 부분적인 T1 연결까지 다양한 미디어를 통한 PPP 연결을 지원합니다. 지원되는 연결 옵션에 대한 정보는 이 주제를 참조하십시오.

연결 장비
iSeries 서버는 PPP 연결을 처리하기 위해 모뎀, ISDN 단말기 어댑터, 토큰 링 어댑터, 이더넷 어댑터 또는 CSU/DSU 장치를 사용합니다. 지원되는 하드웨어에 대한 정보는 이 주제를 참조하십시오.

IP 주소 처리
PPP 연결에는 IP 주소 할당 및 연결 시의 IP 패킷 필터링에 사용되는 몇 가지 옵션이 있습니다. 각 옵션에 대한 정보는 이 주제를 참조하십시오.

시스템 인증
iSeries는 유효성 리스트와 암호 교환 또는 RADIUS 서버를 사용하여 전화 접속 연결을 인증할 수 있습니다. 또한 연결되어 있는 시스템에 인증 정보를 제공할 수 있습니다. 인증 옵션에 대한 정보는 이 주제를 참조하십시오.

대역폭 고려사항
iSeries는 PPP 연결을 위해 멀티링크 프로토콜을 지원합니다. 따라서 단일 연결에 대해 여러 개의 아날로그 전화 회선을 사용하여 대역폭을 늘릴 수 있습니다. 이 지원에 대한 개요는 이 주제를 참조하십시오.

소프트웨어 및 하드웨어 요구사항

PPP 환경에는 PPP를 지원하는 컴퓨터가 두 대 이상 필요합니다. 이 컴퓨터 중 하나인 iSeries 서버가 개시자나 수신자로 사용됩니다. 리모트 시스템의 액세스를 위해서는 iSeries 서버에 다음과 같은 전제조건이 필요합니다.

- TCP/IP 지원을 사용하는 **Operations Navigator** 릴리스 4 버전 4(V4R4) 이상
- 다음 연결 프로파일 중 하나:
  - 아웃바운드 PPP 연결을 처리하는 개시자 연결 프로파일
  - 인바운드 PPP 연결을 처리하는 수신자 연결 프로파일
- iSeries Navigator를 사용하는 **Windows용 iSeries Access(95/98/NT/Millenium/2000/XP)**가 설치되어 있는 PC 워크스테이션 콘솔
- 설치 어댑터

  다음 어댑터 중에서 하나를 선택할 수 있습니다.
  - 2699*: 2선 WAN IOA
  - 2720*: PCI WAN/쌍축 IOA
  - 2721*: PCI 2선 WAN IOA

- 2745*: PCI 2선 WAN IOA (IOA 2721 대체)
- 2742*: 2선 IOA(IOA 2745 대체)
- 2750: PCI ISDN V.90 기본율 인터페이스 U IOA(2선 인터페이스)
- 2751: PCI ISDN V.90 기본율 인터페이스 U IOA(4선 인터페이스)
- 2761: 8포트 아날로그 모뎀 IOA
- 2771: 2포트 WAN IOA(포트 1에서 V.90 통합 모뎀을 사용하고 포트 2에서 표준 통신 인터페이스를 사용). 2771 어댑터의 포트 2를 사용하려면 적합한 케이블을 사용하는 외장 모뎀 또는 ISDN 단말기 어댑터가 필요합니다.
- 2772: 2포트 V.90 통합 모뎀 WAN IOA
- 2838: PPPoE 연결용 이더넷 어댑터
- 2793 2포트 WAN IOA(포트 1에서 V.92 통합 모뎀을 사용하고 포트 2에서 표준 통신 인터페이스를 사용). 2793 어댑터의 포트 2를 사용하려면 적합한 케이블을 사용하는 외장 모뎀 또는 ISDN 단말기 어댑터가 필요합니다. 이는 IOA 모델 2771을 대체합니다.
- 2805: 통합된 V.92, 통합된 아날로그 모뎀이 있는 4 포트 WAN IOA. 이 제품이 모델 2761 및 2772를 대체합니다.

  * 이 어댑터에는 외장형 V.90 모뎀(또는 이상)이나 ISDN 단말기 어댑터 및 RS232 또는 해당 케이블이 필요합니다.

- 연결 유형 및 회선에 따라 다음 중 하나를 사용하십시오.
  - 외장형 또는 내장형 모뎀이나 채널 서비스 장치(CSU)/자료 서비스 장치(DSU)
  - 종합 정보 통신망(ISDN) 단말기 어댑터
- 인터넷 연결을 계획 중이면 인터넷 서비스 제공자(ISP)와의 전화 접속 계정을 위한 준비가 필요합니다. 사용자의 ISP로부터 인터넷 연결에 필요한 전화 번호 및 정보를 받아야 합니다.

연결 대안

PPP는 직렬 지점 간 링크를 통해 데이터그램을 전송할 수 있습니다. PPP는 지점 간 통신을 표준화하여 여러 공급업체에서 생산한 장비와 여러 프로토콜의 상호연결을 가능하게 합니다. PPP 자료 연결층은 비동기 및 동기 지점 간 통신 링크 둘 다에서 데이터그램 캡슐화를 위해 HDLC식 프레임 처리를 사용합니다.

PPP가 광범위한 링크 유형을 지원하는 반면 SLIP는 비동기 링크 유형만 지원합니다. SLIP는 일반적으로 아날로그 링크에 대해서만 사용됩니다. 전화 회사에서는 기능과 비용을 고려하여 전통적인 통신 서비스를 제공합니다. 이러한 서비스는 고객과 중앙 오피스 간에 기존 전화 회사 음성 네트워크 설비를 사용합니다.

PPP 링크가 로컬과 리모트 호스트 간의 물리적 접속을 설정합니다. 연결된 링크는 전용 대역폭을 제공합니다. 또한 다양한 자료 전송률과 프로토콜을 나타냅니다. PPP 링크를 사용할 경우 다음 연결 대안 중에서 선택할 수 있습니다.

- 아날로그 전화선
- 디지털 서비스 및 DDS

- 교환-56
- ISDN
- T1/E1 및 보조 T1
- 프레임 릴레이
- PPP 연결용 L2TP(터널링) 지원
- PPP 연결용 PPPoE(DSL) 지원

아날로그 전화선

전용 또는 교환 회선으로 자료를 전송하는 데 모뎀을 사용하는 아날로그 연결은 지점 간 스케일에서 맨 아래에 나옵니다. 전용 회선은 지정된 두 위치 사이의 상시(full-time) 연결로서 교환 회선은 일반적인 음성 전화 회선입니다. 현재 최고속 모뎀은 56Kbps의 비압축 전송률로 작동합니다. 무조건 음성-등급 전화 회로의 신호 대 소음 비율 하에서는 이 비율을 달성하는 것이 어렵습니다.

더 높은 bps(초당 비트 수)라는 모뎀 제조업체들의 주장은 일반적으로 모뎀에서 이용되는 자료 압축(CCITT V.42bis) 알고리즘을 기준으로 한 것입니다. V.42bis가 자료 볼륨을 4분의 1로 감소시킬 수 있는 가능성은 있지만 압축은 자료에 따라 결정되는 것으로서 50%를 달성하는 것조차도 거의 불가능합니다. 이미 압축 또는 암호화시킨 자료의 경우 V.42bis를 적용시킬 때 다시 늘어나는 수도 있습니다. X2나 56Flex는 아날로그 전화선의 경우 bps 전송률을 56k로 확장합니다. 이는 PPP 링크의 한쪽 끝이 아날로그일 때 다른 쪽 끝은 디지털로 사용하도록 요구하는 하이브리드 기술입니다. 또한 56Kbps는 자료를 디지털에서 링크의 아날로그 끝으로 이동할 때만 적용됩니다. 이 기술은 ISP에 있는 링크 및 하드웨어의 디지털 끝으로 연결할 때 적합합니다. 보통은 최대 115.2Kbps 전송률의 비동기 프로토콜을 사용하여 RS232 직렬 인터페이스를 통해 V.24 아날로그 모뎀에 연결할 수 있습니다.

V.90 표준의 경우 한쪽 끝에서 K56flex/x2 호환성 문제가 발생합니다. V.90 표준은 모뎀 업계에서 x2 및 K56flex 캠프를 절충하여 나온 결과입니다. 공용 교환 전화 네트워크를 디지털 네트워크로 볼 때 V.90 기술은 인터넷에서 컴퓨터로 보내는 자료를 최대 56Kbps 속도로 가속화할 수 있습니다. V.90 기술은 기타 표준들과는 다른 것으로서 아날로그 모뎀이 하는 것처럼 자료를 변조하지 않고 디지털식으로 암호화 처리를 합니다. 자료 전송은 비대칭 방법입니다. 따라서 업스트림 전송(대부분 중앙 사이트로 보내는 컴퓨터 키스트로크 및 마우스 명령으로, 대역폭을 덜 요구함)의 경우 계속해서 최대 33.6Kbps의 일반적인 전송률로 흐릅니다. 모뎀에서 송신된 자료는 V.34 표준을 이중복사(mirror)하는 아날로그 전송으로 송신됩니다. 다운스트림 자료 전송만 고속 V.90 전송률을 활용합니다.

V.92 표준은 업스트림 비율을 48Kbps로 올림으로써 V.90을 개선하였습니다. 또한 핸드쉐이킹 프로세스의 개선으로 인해 연결 시간을 줄일 수 있으며 전화 회선에서 들어오는 호출을 허용하거나 호출 대기를 사용하는 중에 ″보유″ 기능을 지원하는 모뎀을 연결 상태로 유지할 수 있습니다.

디지털 서비스 및 DDS

디지털 서비스

디지털 서비스를 사용할 경우 자료가 디지털 형식으로 송신자의 컴퓨터에서 전화 회사의 중앙 오피스, 장거리 제공자, 중앙 오피스, 수신자의 컴퓨터로 순서대로 전달됩니다. 디지털 신호는 아날로그 신호보다 훨씬 더 많은 대역폭과 높은 신뢰성을 제공합니다. 디지털 신호 시스템은 소음, 가변 회선 품질 및 신호 감소와 같이 아날로그 모뎀이 처리해야 하는 많은 문제들을 제거합니다.

DDS

디지털 자료 서비스(DDS)는 가장 기본적인 디지털 서비스입니다. DDS 링크는 최대 56Kbps의 고정 전송률로 처리되는 영구적인 전용 연결입니다. 보통 이 서비스를 DS0라고도 합니다.

아날로그 시나리오에서는 모뎀을 대체하는 채널 서비스 장치/자료 서비스 장치(CSU/DSU)로 DDS에 연결할 수 있습니다. DDS는 기본적으로 CSU/DSU와 전화 회사의 중앙 오피스 간 거리와 관련된 물리적인 제한점을 가집니다. DDS는 거리가 30,000피트 미만일 때 최상으로 작동합니다. 전화 회사는 신호 확장자를 사용하여 더 먼 거리도 수용할 수 있지만 이러한 서비스에는 많은 비용이 듭니다. DDS는 같은 중앙 오피스에서 지원하는 두 지역을 연결할 때 가장 적합합니다. 다른 중앙 오피스로 연결되는 장거리 연결의 경우 마일리지 비용 부과로 인해 DDS가 비실용적일 수 있습니다. 이 경우에는 교환-56이 더 좋은 솔루션일 것입니다. 보통은 최대 56Kbps 전송률의 동기 프로토콜을 사용하여 V.35, RS449 또는 X.21 직렬 인터페이스를 통해 DDS CSU/DSU에 연결할 수 있습니다.

교환-56

상시 연결이 필요하지 않은 경우 일반적으로 교환-56(SW56)이라고 하는 교환 디지털 서비스를 사용하여 비용을 절감할 수 있습니다. SW56 링크는 DTE가 CSU/DSU 방식으로 디지털 서비스에 연결하는 DDS 설정과 유사합니다. 그러나 SW56 CSU/DSU에는 리모트 호스트의 전화 번호를 입력하는 다이얼 패드가 포함되어 있습니다. SW56은 국내 또는 전세계의 서로 다른 SW56 가입자들에게 전화 접속 디지털 연결을 제공합니다. SW56 호출은 숫자화된 음성 전화처럼 장거리 디지털 네트워크를 통해 전달됩니다. SW56은 로컬 전화 시스템과 같은 전화 번호를 사용하고 사용료는 업무용 음성 전화와 동일합니다. SW56은 북미 네트워크에서만 사용되는 것으로 자료 전달을 위한 단일 채널로만 제한됩니다. SW56은 ISDN을 사용할 수 없는 지역에 대한 대안입니다. 일반적으로, 최대 56Kbps 전송률의 동기 프로토콜을 사용하여 V.35 또는 RS 449 직렬 인터페이스를 통해 SW56 CSU/DSU에 연결할 수 있습니다. V.25bis 호출/응답 장치를 사용할 경우 자료 및 호출이 단일 직렬 인터페이스를 통해 흐름을 제어합니다.

ISDN

교환-56처럼 ISDN도 교환 끝 대 끝(end-to-end) 디지털 연결을 제공합니다. 그러나 다른 서비스와는 달리 ISDN은 같은 연결을 통해 음성과 자료를 모두 전달합니다. ISDN 서비스의 유형에는 여러 가지가 있으며 기본율 인터페이스(BRI)가 가장 일반적입니다. BRI는 고객 자료를 전달하는 두 개의 64Kbps B 채널과 신호 자료를 전달하는 D 채널로 이루어집니다. 두 개의 B 채널은 함께 링크되어 128Kbps(결합된)의 기본율을 제공할 수 있습니다. 일부 지역의 경우 전화 회사가 각각의 B 채널을 56Kbps 또는 112Kbps(결합된)로 제한할 수 있습니다. 고객 지역이 중앙 오피스 스위치의 18,000피트 내에 있어야 하는 물리적인 제한사항도 있습니다. 이 거

리는 반복기(repeater)를 통해 확장시킬 수 있습니다. ISDN에 연결할 때는 단말기 어댑터라는 장치를 사용할 수 있습니다. 대부분의 단말기 어댑터에는 전화 잭에 직접 연결할 수 있는 통합 네트워크 단말 장치(NT1)가 있습니다. 일반적으로 단말기 어댑터는 비동기 RS232 링크를 통해 컴퓨터에 연결하고 전통적인 아날로그 모뎀처럼 설정 및 제어를 위해 AT 명령 세트를 사용합니다. 각 브랜드별로 ISDN에 고유한 매개변수를 설정하기 위한 자체 AT 명령 확장자가 있습니다. 과거에는 서로 다른 브랜드의 ISDN 단말기 어댑터 간에 상호운영성 문제가 많이 발생했습니다. 이와 같은 문제점들은 주로 두 개의 B 채널에 대한 접속 구조 뿐만 아니라 V.110 및 V.120에서 있던 다양한 전송률 적용 프로토콜에 의한 것이었습니다.

현재는 업계에서 두 개의 B 채널을 링크하기 위한 PPP 멀티링크를 비동기 PPP 프로토콜로 한데 모아서 공급하고 있습니다. 또한 일부 단말기 어댑터 제조업체에서는 V.34(아날로그 모뎀) 기능을 자신의 단말기 어댑터에 통합시켰습니다. 이것은 단일 ISDN 회선을 사용하는 고객들이 ISDN 서비스의 동시 음성/자료 기능의 장점을 이용하여 ISDN 또는 전통적 아날로그 전화를 처리할 수 있게 해 줍니다. 또한 이러한 신 기술을 통해 단말기 어댑터를 56K(X2/56Flex) 클라이언트용 디지털 서버로 작동시킬 수 있게 되었습니다.

일반적으로 사용자들은 최대 230.4Kbps 비율의 비동기 프로토콜을 사용하는 RS232 직렬 인터페이스를 통해 ISDN 단말기 어댑터를 연결하려고 합니다. 그러나 RS232를 통한 비동기용 최대 iSeries 서버 보오율은 115.2Kbps입니다. 불행하게도 이것은 최대 바이트 전송율을 11.5k 바이트/초로 제한합니다. 그러나 멀티링크를 사용하는 단말기 어댑터는 압축되지 않은 14/16k 바이트를 처리할 수 있습니다. 일부 단말기 어댑터는 RS232를 통한 비동기를 128Kbps로 지원하지만 RS232를 통한 비동기용 iSeries 서버 최대 보오율은 64Kbps입니다.

iSeries 서버는 V.35를 통한 비동기 처리를 최대 230.4Kbps 비율로 실행할 수 있지만 단말기 어댑터 제조업체는 일반적으로 이러한 구성을 제공하지 않습니다. RS232를 V.35 인터페이스로 변환시키는 인터페이스 변환기가 이 문제에 대한 적절한 솔루션이 될 수 있지만 iSeries 서버에 대해서 올바른 평가가 이루어지지 않았습니다. 또 다른 대안은 128Kbps 비율의 V.35 인터페이스 비동기 프로토콜을 사용하는 단말기 어댑터입니다. 그러나 이러한 단말기 어댑터가 있더라도 대다수가 동기 멀티링크 PPP를 제공하지 않습니다.

T1/E1 및 보조 T1

T1/E1

T1 연결은 4선 동선 회로에서 24개 64Kbps(DS0) TDM(time division multiplexed) 채널을 함께 번들로 제공합니다. 이는 총 1.544Mbps의 대역폭을 생성합니다. 유럽이나 다른 일부 지역에서 E1 회로는 총 2.048Mbps를 위해 32개의 64Kbps 채널을 함께 번들로 제공합니다. TDM은 여러 사용자들이 사전 할당된 타임 슬롯을 사용하여 디지털 전송 매체를 공유할 수 있도록 합니다. 복수 디지털 PBX는 T1 서비스의 장점을 이용하여 PBX와 전화 회사 간에 24선 쌍을 라우트하는 대신 한 개의 T1 회선을 통해 복수 호출 회로를 가져옵니다. 음성과 자료에서 T1을 공유한다는 점은 매우 중요합니다. 예를 들어, 전화 서비스가 나머지 채널을 인터넷 연결용으로 남겨 놓은 채 T1 링크 중 24 채널의 서브세트로 나올 수 있습니다. T1 멀티플렉서 장치는 T1 트렁크를 여러 서비스에서 공유할 때 24 DS0 채널을 관리하기 위해 필요한 것입니다. 단일 자료 전용 연결의 경우 채널화되지 않은 상태로 이 회로를 실행시킬 수 있습니다(신호에서 TDM이 수행되지 않음). 결과적으로 더욱 간단한 CSU/DSU 장치를 사용할 수 있습니다. 일반적으로 복수의 64Kbps에서 1.544Mbps 또는 2.048Mbps

전송률의 동기 프로토콜을 사용하여 V.35 또는 RS 449 직렬 인터페이스를 통해 T1/E1 CSU/DSU 또는 멀티플렉서에 연결할 수 있습니다. CSU/DSU 또는 멀티플렉서가 네트워크에서 시간 재기 기능을 제공합니다.

보조 T1

보조 T1(FT1)의 경우 고객이 64Kbps 서브멀티 T1 회선을 전용하여 사용할 수 있습니다. FT1은 전용 T1의 비용으로 인해 고객이 사용하는 실제 대역폭을 처리할 수 없을 때 유용합니다. FT1을 사용하면 필요한 때에만 지불하면 되기 때문입니다. 또한 FT1에는 전화 회사의 중앙 오피스에 있는 멀티플렉싱(Multiplexing) DS0 채널과 같이 전체 T1 회로에서 사용할 수 없는 기능이 있습니다. FT1 회로의 리모트 끝은 전화 회사에서 유지보수하는 디지털 액세스 상호-연결 스위치에 있습니다. 같은 디지털 스위치를 공유하는 시스템들은 DS0 채널을 교환할 수 있습니다. 이러한 구조는 보통 자신의 위치에서 전화 회사의 디지털 스위치에 단일 T1 트렁크를 사용하는 ISP들이 사용합니다. 이 경우에는 여러 클라이언트들이 FT1 서비스를 제공받을 수 있습니다. 일반적으로 64Kbps의 배수로 동기 프로토콜을 사용하는 V 3.5 또는 RS 449 직렬 인터페이스를 통해 T1/E1 CSU/DSU 또는 멀티플렉서에 연결할 수 있습니다. FT1을 사용하면 24개 채널의 서브세트가 사전에 지정됩니다. T1 멀티플렉서는 사용자 서비스용으로 지정된 타임 슬롯을 위해서만 구성하십시오.

프레임 릴레이

프레임 릴레이는 프레임의 주소 필드(자료 링크 연결 식별자)에 기초하고 있는 네트워크를 통해 프레임을 라우트하고, 라우트 또는 가상 연결을 관리하기 위한 프로토콜입니다.

미국 내에서는 프레임 릴레이 네트워크가 T-1(1.544Mbps) 및 T-3(45Mbps) 속도의 자료 전송률을 지원합니다. 프레임 릴레이를 서비스 제공자가 소유하는 기존의 T-1 및 T-3 회선을 활용하기 위한 하나의 방법으로 생각할 수 있습니다. 이제는 대부분의 전화 회사들이 56Kbps에서 T-1 속도로 연결을 원하는 고객들에게 프레임 릴레이 서비스를 제공합니다. (유럽의 경우 프레임 릴레이의 속도가 64Kbps에서 2Mbps까지 다양하며, 미국의 경우 프레임 릴레이가 비교적 저렴한 편이므로 널리 사용되고 있습니다.) 그러나 일부 지역에서는 ATM과 같은 더 빠른 기술로 대체되는 중입니다.

PPP 연결용 L2TP(터널링) 지원

L2TP(계층 2 터널링 프로토콜)는 요구하는 L2TP 클라이언트(L2TP 액세스 집중기 또는 LAC)와 목표 L2TP 서버 종료점(L2TP 네트워크 서버 또는 LNS) 사이의 링크 계층 터널을 지원하기 위해 PPP를 확장하는 터널링 프로토콜입니다. L2TP 터널을 사용하면 전화 접속 프로토콜이 종료하는 위치와 네트워크에 대한 액세스가 제공되는 위치를 분리할 수 있는데 이것이 바로 L2TP를 가상 PPP로 부르는 이유입니다. L2TP 프로토콜은 RFC 표준 RFC2661으로 문서화되어 있습니다. RFC에 대한 자세한 정보는 http://www.rfc-editor.org를 참조하십시오. L2TP 터널은 전체 PPP 세션에 걸쳐 확장시키거나 두 세그먼트 세션 중 한 세그먼트에 대해서만 확장시킬 수 있습니다. 이것은 다음의 네 가지 터널링 모델로 정리할 수 있습니다.

- 자발적 터널
- 강제적 터널-들어오는 호출
- 강제적 터널-리모트 다이얼
- L2TP 멀티 홉 연결

자발적 터널

임시 터널 모델에서 터널은 사용자, 일반적으로 L2TP가 작동되는 클라이언트 사용에 의해 작성됩니다. 결과적으로 사용자가 L2TP 패킷을 인터넷 서비스 제공자(ISP)에게 송신하고 ISP가 이 패킷을 LNS로 전송합니다. 자발적 터널링에서 ISP는 L2TP를 지원할 필요가 없으며 L2TP 터널 개시자는 실제로 리모트 클라이언트와 같은 시스템에 상주합니다. 이 모델에서 터널은 L2TP 클라이언트에서 LNA로 전체 PPP 세션에 걸쳐 확장됩니다.

강제적 터널 모델 - 들어오는 호출

강제적 터널 모델-들어오는 호출에서 터널은 사용자의 조치나 사용자에게 어떤 선택사항도 허용하지 않는 상태에서 작성됩니다. 결과적으로, 사용자가 PPP 패킷을 ISP(LAC)로 송신하고 ISP가 이 패킷을 L2TP에 캡슐화하여 LNS로 터널을 통과시킵니다. 강제적 터널링의 경우 ISP에 반드시 L2TP 기능이 있어야 합니다. 이 모델에서 터널은 단지 ISP와 LNS 사이에서 PPP 세션의 세그먼트에 확장됩니다.

강제적 터널 모델 - 리모트 다이얼

강제적 터널 모델-리모트 다이얼에서 홈 게이트웨이(LNS)는 ISP(LAC)에 대해 터널을 시작하고 ISP에게 PPP 응답 클라이언트에 로컬 호출을 처리할 것을 지시합니다. 이 모델은 리모트 PPP 응답 클라이언트가 ISP와 영구 설정된 전화 번호를 가지고 있는 경우를 위한 것입니다. 이 모델은 인터넷에 등록된 회사가 전화 접속 링크를 필요로 하는 리모트 오피스에 연결을 설정해야 할 때 사용됩니다. 이 모델에서 터널은 LNS와 ISP 사이에서 PPP 세션의 세그먼트에만 확장됩니다.

L2TP 멀티 홉 연결

L2TP 멀티 홉 연결은 클라이언트 LAC 및 LNS를 위하여 L2TP 통신을 다시 지정하는 방법입니다. 멀티 홉 연결은 L2TP 멀티 홉 게이트웨이(L2TP 단말기와 개시자 프로파일을 함께 링크하는 시스템)를 사용하여 설정됩니다. 멀티 홉 연결을 설정하기 위해 L2TP 멀티 홉 게이트웨이는 일련의 LAC에 대한 LNS로 작용하는 동시에 지정 LNS에 대한 LAC로 작용합니다. 클라이언트 LAC에서 L2TP 멀티 홉 게이트웨이로 터널을 설정하면 그 다음에 L2TP 멀티 홉 게이트웨이와 목표 LNS 사이에 다른 터널이 설정됩니다. 그리고 나서 클라이언트 LAC에서 나온 L2TP 통신이 L2TP 멀티 홉 게이트웨이에 의해 목표 LNS로 다시 지정되고 목표 LNS의 통신은 클라이언트 LAC로 다시 지정됩니다.

PPP 연결용 PPPoE(DSL) 지원

DSL은 고객의 구내 및 ISP 제공자 사이에서 실행될 수 있는 기존의 전화 회선(구리선)을 통해 보다 많은 대역폭을 얻는 데 필요한 기술을 말합니다. 따라서 쌍축 전화선(구리선)을 통해 동시 음성 및 고속 자료 서비스를 사용할 수 있습니다. 모뎀 속도는 다양한 압축 및 기타 기술을 사용하여 점진적으로 증가하였으나 오늘날의 최고 속도(초속 56kbit)는 거의 이 기술의 한계점에 도달한 것 같습니다. DSL 기술을 사용하면 꼬인 쌍축 회선을 통해 본사로부터 가정, 학교 또는 업무 장소로 보다 빠른 속도가 사용됩니다. 일부 영역에서는 초당 2 메가바이트에 이르는 속도가 측정되었는데 이것은 현재 가장 빠른 모뎀보다 30배 이상 빠른 속도입니다. PPPoE는 Point to Point Protocol over Ethernet의 약자입니다. PPP는 일반적으로 전화 접속 모뎀 연결과 같은 일련의 통신에 사용됩니다. 현재 많은 DSL 인터넷 서비스 제공자들이 추가된 로그인 및 보안 기능으로 인해 이더넷을 통해 PPP를 사용하고 있습니다. 그러면 DSL 모뎀은 무엇입니까? DSL ″모뎀″은 전화선(구리선)의 어느 한 쪽 끝에 있는 장치로서 컴퓨터 또는 LAN이 DSL 연결을 통해 인터넷에 연결할 수 있도록 해 줍니다. 전화 접속 연결과 달리 일반적으로 전용 전화선(회선을 동시에 공유할 수 있도록 해 주는 POTS 분리

기 상자)이 필요하지 않습니다. DSL은 모뎀 기술의 차세대 기술로 인정받고 있습니다. DSL 모뎀은 전통적인 아날로그 모뎀과의 유사성에도 불구하고 더 높은 수준의 처리량을 제공합니다.

연결 장비

다음은 PPP 환경에서 사용할 수 있는 세 종류의 통신 장비입니다.

- 모뎀
- CSU/DSU
- ISDN 단말기 어댑터
- 2838 유형 이더넷 어댑터(PPPoE 연결용)

모뎀

PPP 연결용으로 외장 및 내장 모뎀 둘 다 사용됩니다. 모뎀에 사용되는 명령 세트는 일반적으로 모뎀 문서에 그 설명이 나옵니다. 이 명령은 모뎀을 재설정하고 초기화하는 데 사용되며, 리모트 시스템의 전화 번호를 다이얼하도록 모뎀으로 알릴 때 사용됩니다. 모뎀 모델별로 서로 다른 초기화 명령 스트링이 있으므로 PPP 연결 프로파일과 함께 사용하기 전에 모델을 정의해야 합니다. 내장형 모뎀의 경우 모뎀 스트링이 용도에 맞게 이미 정의되어 있습니다.

iSeries 서버에는 여러 가지 모델의 모뎀이 사전정의되어 있지만 신규 모델의 경우 Operations Navigator을 통해 정의할 수 있습니다. 기존 정의는 신규 유형을 정의하기 위한 기초로 사용할 수 있습니다. 모뎀이 어떤 명령을 사용하는지 알 수 없거나 모뎀 문서에 액세스할 수 없으면 Generic Hays 모뎀 정의에서 시작하십시오. 사전정의되어 공급된 정의는 변경할 수 없습니다. 단, 기존 초기화 명령이나 다이얼 스트링에 추가 명령을 추가할 수 있습니다.

PPP 연결을 설정하기 위해 iSeries 서버와 함께 제공되는 전자 고객 지원(ECS) 모뎀을 사용할 수 있습니다. 이전 시스템에서는 ECS 모뎀이 IBM 7852-400 외장 모뎀이었습니다. 신규 시스템에서는 2771 또는 2772 내장 모뎀을 ECS 모뎀으로 사용할 수 있습니다.

CSU/DSU

채널 서비스 장치(CSU)는 단말기를 디지털 회선으로 연결하는 장치입니다. 자료 서비스 장치(DSU)는 통신 회선의 보호 및 진단 기능을 수행하는 장치입니다. 일반적으로 이 두 장치가 하나의 장치 즉, CSU/DSU로 패키징되어 있습니다.

CSU/DSU를 그 기능은 매우 강력하지만 비용이 높은 제품으로 생각할 수도 있습니다. 그러나 T-1이나 T-3 연결의 양 끝에는 반드시 이러한 제품이 필요하며 양 끝에 있는 장치로 같은 제조업체의 제품을 사용해야 합니다.

ISDN 단말기 어댑터

ISDN은 서로 다른 멀티미디어 어플리케이션 사이에서 음성, 자료 및 비디오로 통신할 수 있게 해 주는 디지털 연결을 제공합니다.

단말기 어댑터가 iSeries 서버에 사용할 수 있는 것인지 확인하십시오.

- ISDN 단말기 어댑터 권장사항은 사용에 가장 적합한 단말기 어댑터를 알려줍니다.
- ISDN 단말기 어댑터 제한사항은 iSeries 서버에서 테스트가 이루어진 여러 ISDN 단말기 어댑터에 대한 정보 및 간략한 평가 내용을 제공합니다.

단말기 어댑터를 구성하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 서버를 선택하고 **네트워크 -> 리모트 액세스 서비스**를 선택하십시오.
2. **모뎀**을 마우스 오른쪽 버튼으로 클릭한 후 **신규 모뎀**을 선택하십시오.
3. 신규 모뎀 등록 정보 대화상자에서 일반 탭의 모든 필드 상자에 올바른 값을 입력하십시오. ISDN 단말기 어댑터를 통신 장치로 지정했는지 확인하십시오.
4. **ISDN 매개변수** 탭을 선택하십시오.
5. **ISDN 매개변수** 탭에 있는 ISDN 등록 정보를 단말기 어댑터에 필요한 등록 정보와 일치하도록 추가 또는 변경하십시오.

Operations Navigator를 사용하는 샘플 프로시듀어에 대해서는 ISDN 단말기 어댑터 구성 예를 검토하십시오.

ISDN 단말기 어댑터 권장사항

권장되는 외장 ISDN 단말기 어댑터나 ISDN 모뎀은 **3Com/U.S. Robotics Courier I ISDN V.Everything** 입니다. 이 모뎀은 iSeries 서버의 시작 및 응답 모드에서 ISDN을 통한 V.34 아날로그 모뎀 연결, V.90(X2), V.92 및 멀티링크 PPP를 지원합니다. 또한 ISDN PPP 연결을 통한 CHAP(Challenge Handshake Authentication Protocol)을 자동으로 지원합니다. Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA 및 ADtran ISU 2x64 Dual Port와 같은 ISDN 단말기 어댑터도 사용할 수 있습니다.

- **iSeries 서버에서 시작하는 연결** 수신측에서 시작된 CHAP 챌린지는 iSeries 서버와 암호 인증 프로토콜(PAP) 인증을 협상하는 동안 Curier I 단말기 어댑터에 의해 응답이 이루어집니다. PAP 응답은 ISDN 연결에 나오지 않습니다.
- **iSeries 서버가 응답하는 연결** Courier I는 iSeries 서버 응답 구성이 iSeries 서버로 하여금 CHAP 챌린지를 사용하여 인증을 열도록 되어 있는 경우 호출측에 의한 CHAP 인증을 요구합니다. iSeries 서버가 PAP로 인증을 열면 Courier I 단말기 어댑터가 PAP를 사용하여 인증합니다.

1999년 이전형 Courier I 모뎀을 사용 중인 경우 ISDN 연결에서 최대 성능을 얻으려면 Courier I 모뎀이 V.35 케이블로 iSeries 서버에 연결되어 있는지 확인하십시오. RS-232 대 V.35 모뎀 케이블이 Courier I 모뎀과 함께 제공됩니다. 하지만 이 케이블의 이전 버전에 있는 V.35 커넥터는 암수(gender)가 틀립니다. 교체하려면 3Com/US Robotics 고객 지원부로 연락하십시오.

주: 3Com/US Robotics에 따르면 이 단말기 어댑터의 V.35 버전을 제 3의 공급자로부터 일부 구할 수는 있으나 더 이상 제공하지 않는 것으로 되어 있습니다. RS-232 버전은 RS-232 연결이 115.2Kb로 제한되기 때문에 iSeries에서 성능이 다소 떨어지는 경향이 있으나 여전히 사용이 권장됩니다.

또한 Black Box Corporation에서 V.35 to RS-232 어댑터를 구할 수 있습니다. 부품 번호는 FA-058입니다.

iSeries 서버에서는 V.35 회선 속도를 반드시 230.4Kbps로 설정하십시오.

ISDN 단말기 어댑터 제한사항

다음에 나오는 단말기 어댑터에 대해 평가가 이루어졌습니다. 이 단말기들은 iSeries 서버로부터 ISDN 리모트 연결을 시작할 경우에만 권장됩니다.

3Com Impact IQ ISDN:

이 단말기 어댑터는 다음과 같은 이유로 인해 iSeries 서버용으로 권장되지 않습니다.

- 단말기 어댑터가 V.34 아날로그 모뎀 연결을 지원하지 않습니다. 단, 외장 RJ-11 연결을 사용하여 V.34 아날로그 모뎀 연결을 지원할 수 있습니다.
- 단말기 어댑터가 현재 V.90 연결을 지원하지 않습니다.
- 115,200bps를 초과하는 속도로 단말기 어댑터를 iSeries 서버에 연결할 수 없습니다.
- 단말기 어댑터가 CHAP(Challenge Handshake Authertication Protocol)를 자동으로 지원하지 않습니다. 단, S84=0을 설정하여 iSeries 서버 CHAP 인증을 수행시킬 수 있습니다.
- iSeries 서버가 단말기 어댑터에서 자료 세트 준비(DSR) 신호를 모니터할 때 연결이 종료되는 시기를 판별할 수 없습니다. 이로 인해 결국 잠재적인 시스템 보안 노출의 결과를 초래할 수 있습니다.

Motorola BitSurfr Pro ISDN:

이 단말기 어댑터는 다음과 같은 이유로 인해 iSeries 서버용으로 권장되지 않습니다.

- 단말기 어댑터가 V.34 아날로그 모뎀 연결을 지원하지 않습니다. 단, 외장 RJ-11 연결을 사용하여 V.34 아날로그 모뎀 연결을 지원할 수 있습니다.
- 단말기 어댑터가 현재 V.90 연결을 지원하지 않습니다.
- 115,200bps를 초과하는 속도로 단말기 어댑터를 iSeries 서버에 연결할 수 없습니다.
- 단말기 어댑터가 CHAP 인증을 자동으로 지원하지 않습니다. 그러나, @M2=C를 설정하여 iSeries 서버 CHAP 인증을 수행시킬 수 있습니다.
- 단말기 어댑터는 단일 링크 및 복수 링크 PPP 호출 모두에 대한 응답을 자동으로 허용하지 않습니다. 리모트로부터 시작하는 단말기 어댑터는 응답 단말기 어댑터와 같은 프로토콜(단일 링크 또는 복수 링크)로 설정해야 합니다.
- iSeries 서버 하드웨어 흐름 제어 메카니즘은 이 단말기 어댑터와 제대로 작동하지 않습니다. 결과적으로, iSeries 서버가 멀티링크 PPP 연결에서 자료를 송신할 때 성능이 떨어지게 됩니다.

IP 주소 처리

PPP 연결에서는 PPP 연결에 필요한 IP 주소를 관리할 수 있도록 해 주는 연결 프로파일의 유형에 따라 IP 주소를 관리하기 위한 다양한 여러 옵션 집합이 기존 네트워크 구조와 유기적으로 작업할 수 있습니다. 네트워크의 IP 주소 구조 정의에 대한 정보는 다음 주제를 참조하십시오.

- DHCP

DHCP는 네트워크의 IP 주소 지정을 중앙에서 관리할 수 있습니다. 네트워크를 위한 DHCP 서비스 설정과 관리 방법을 알 수 있습니다.

- DNS

  DNS를 사용하면 호스트명과 관련 IP 주소 관리를 보다 쉽게 처리할 수 있습니다. 네트워크를 위한 DNS 서비스 설정과 관리 방법을 알 수 있습니다.

- BOOTP

  BOOTP는 클라이언트 워크스테이션과 iSeries 서버를 연결하고 IP 주소를 할당하기 위해 사용됩니다. 네트워크를 위한 BOOTP 서비스 설정과 관리 방법을 알 수 있습니다.

- IP 패킷 필터링

  IP 필터 규칙 파일을 작성하여 특정 IP 주소에 대한 사용자 및 그룹 액세스를 제한합니다. IP 필터링 지원을 포함하여 네트워크에서 이 옵션을 구현하는 방법을 알 수 있습니다.

PPP 연결 프로파일을 구성하기 위해서는 먼저 네트워크 IP 주소 관리 전략에 대해 잘 알아야 합니다. 이 전략은 인증 전략, 보안 관련 문제 및 TCP/IP 설정을 포함하여 구성 프로세스 전체에 결쳐 여러 결정사항에 영향을 미칩니다.

개시자 연결 프로파일:

일반적으로 개시자에 대해 정의된 로컬 및 리모트 IP 주소는 **리모트 시스템이 할당**하는 것으로 정의됩니다. 이것은 리모트 시스템에 있는 관리자가 연결에 사용될 IP 주소를 제어할 수 있게 해 줍니다. 많은 ISP들이 추가 요금을 위해 고정 IP 주소를 제공하더라도 인터넷 서비스 제공자(ISP)에 대한 대부분의 연결은 거의 이와 같은 방식으로 정의됩니다.

로컬 또는 리모트 IP 주소에 대해 고정 IP 주소를 정의하는 경우 리모트 시스템이 사용자가 정의한 주소를 승인하도록 정의되어 있는지 확인해야 합니다. 하나의 대표적인 어플리케이션을 사용자의 로컬 주소로서 고정 IP 주소로 정의하고 리모트 주소는 리모트 시스템이 할당하도록 정의합니다. 사용자가 연결하는 시스템도 같은 방식으로 정의할 수 있으며 사용자가 연결할 때 두 시스템에서는 리모트 시스템의 주소를 알기 위한 방법으로 서로 주소를 교환합니다. 이 방법은 한 사무소가 임시 연결을 위해 다른 사무소를 호출할 때 유용합니다.

또 다른 고려사항은 IP 주소 변조(Masquerading)를 작동시키는가 하는 것입니다. 예를 들어, iSeries 서버가 ISP를 통해 인터넷과 연결되는 경우 이것은 iSeries 서버 뒤에서 접속 네트워크가 인터넷에 액세스할 수 있게 해 줍니다. 기본적으로 iSeries 서버는 네트워크에 있는 시스템의 IP 주소를 ISP가 할당한 로컬 IP 주소 뒤에 ″숨깁니다″. 따라서 모든 IP 통신이 iSeries 서버에서 나온 것처럼 만듭니다. ‘리모트 시스템을 디폴트 라우트로 추가’ 상자를 작동시켜야 하는 iSeries 서버 뿐만 아니라 LAN에 있는 두 대의 시스템에 대해서도 추가적인 라우팅 고려사항이 있습니다(인터넷 통신이 iSeries 서버로 송신되는지 확인하기 위해).

수신자 연결 프로파일:

수신자 연결 프로파일에는 개시자 연결 프로파일보다 더 많은 IP 주소 고려사항과 옵션이 있습니다. IP 주소 구성 방법은 네트워크를 위한 IP 주소 관리 계획, 해당 연결의 특정 기능 및 기능 요구사항을 포함하여 보안 계획에 의해 결정됩니다.

로컬 IP 주소

단일 수신자 프로파일의 경우 고유 IP 주소를 정의하거나 iSeries 서버에 있는 기존 로컬 IP 주소를 사용할 수 있습니다. 이 주소가 PPP 연결에서 iSeries 서버 끝을 식별하는 주소가 됩니다. 동시에 여러 연결을 지원하도록 정의된 수신자 프로파일의 경우 기존 로컬 IP 주소를 사용해야 합니다. 이전의 기존 로컬 IP 주소가 없으면 가상 IP 주소를 작성할 수 있습니다.

리모트 IP 주소

PPP 연결에 리모트 IP 주소를 할당하는 데 사용되는 많은 옵션이 있습니다. 다음 옵션은 수신자 연결 프로파일의 **TCP/IP** 페이지에서 지정할 수 있습니다.

주: 리모트 시스템을 LAN의 일부로 사용하려면 IP 주소 라우팅을 구성하고 LAN 접속 시스템에 대한 주소 범위 내에서 IP 주소를 지정하고, 이 연결 프로파일과 iSeries 시스템 모두에 대해 IP 이송을 사용할 수 있는지 확인해야 합니다.

표 3. 수신자 프로파일 연결용 IP 주소 지정 옵션

옵션	설명
고정 IP 주소	리모트 사용자들이 다이얼 인 할 때 이들에게 부여할 단일 IP 주소를 정의합니다. 이 주소는 호스트 전용 IP 주소(서브네트 마스크는 255.255.255.255)로서 단일 연결 수신자 프로파일에만 있습니다.
주소 풀(pool)	시작 IP 주소를 정의하고 나서 정의할 추가 IP 주소 수의 범위를 정의합니다. 그리고 나면 연결하는 각 사용자들이 정의된 범위 내에서 고유 주소를 부여받습니다. 이 주소는 호스트 전용 IP 주소(서브네트 마스크는 255.255.255.255)로서 복수 연결 수신자 프로파일에만 있습니다.
RADIUS	Radius 서버가 리모트 IP 주소 및 그 서브네트 마스크를 판별합니다. 이것은 다음을 정의한 경우에만 있습니다. • 리모트 액세스 서버 서비스 구성에서 인증 및 IP 주소지정에 대해 Radius 지원을 작동 가능으로 설정한 경우 • 수신자 연결 프로파일에 대해 인증이 작동하며 Radius에 의해 리모트로 인증이 이루어지도록 정의한 경우
DHCP	DHCP 릴레이가 리모트 IP 주소를 판별합니다. 이것은 리모트 액세스 서버 서비스 구성에서 DHCP 지원을 작동 가능으로 설정한 경우에만 있습니다. 이 주소가 호스트 전용 IP 주소(서브네트 마스크는 255.255.255.255)입니다.
리모트 시스템의 사용자 ID를 기본으로 주소 정의	리모트 IP 주소는 인증 시 리모트 시스템에 대해 정의된 사용자 ID로 판별됩니다. 이것은 관리자로 하여금 다이얼 인하는 사용자에게 다른 리모트 IP 주소(및 연관된 서브네트 마스크)를 할당할 수 있게 해 줍니다. 또한 알려진 리모트 사용자들이 스스로 환경을 정의할 수 있도록 이 사용자 ID 각각에 대해 추가 라우트를 정의할 수 있게 해 줍니다. 이 기능이 제대로 작동하기 위해서는 인증을 작동 가능으로 설정해야 합니다.
리모트 시스템의 사용자 ID를 기본으로 추가 IP 주소 정의	이 옵션은 리모트 시스템의 사용자 ID를 기본으로 주소를 정의할 수 있도록 합니다. 이 옵션은 리모트 IP 주소 지정 방법이 **리모트 시스템의 사용자 ID를 기본으로 주소 정의**로 정의된 경우 자동으로 선택됩니다. (그리고 반드시 사용되어야 합니다.) 이 옵션은 고정 IP 주소 및 주소 풀의 주소 지정 방법에 대해서도 사용할 수 있습니다. 리모트 사용자가 iSeries 서버에 연결할 때 리모트 IP 주소가 이 사용자에 대해 특별히 정의된 것인지를 판별하기 위한 탐색이 이루어집니다. 이 경우 그 주소, 마스크, 가능한 라우트 세트가 연결에 사용됩니다. 그러나 사용자가 정의되어 있지 않으면 주소에 디폴트로 정의되어 있는 고정 IP 주소나 그 다음에 있는 주소 풀 IP 주소를 사용합니다.

표 3. 수신자 프로파일 연결용 IP 주소 지정 옵션 (계속)

옵션	설명
리모트 시스템에 자신의 IP 주소 정의 허용	이 옵션은 리모트 사용자가 협상을 통해 자신의 IP 주소를 정의하는 것을 허용합니다. 리모트 사용자가 자신의 주소를 사용하기 위해 협상하지 않으면 정의된 리모트 IP 주소 지정 방법에 의해 리모트 IP 주소가 판별됩니다. 초기에는 이 옵션이 작동 불가능으로 설정되어 있으며 작동 가능으로 설정할 때는 먼저 신중한 고려가 필요합니다.
IP 주소 라우팅	전화 접속 클라이언트 및 iSeries는 클라이언트가 iSeries가 속한 LAN 상의 임의의 IP 주소에 대한 액세스를 요청하는 경우 반드시 적절히 구성된 IP 주소 라우팅이 있어야 합니다.

IP 패킷 필터링

IP 패킷 필터링은 네트워크에 로그인할 때 개별 사용자에게 서비스를 제한하는 메카니즘입니다. 패킷 필터링은 목적지 IP 주소 및/또는 포트에 따라 액세스를 ″허용″하거나 ″거부″할 수 있습니다. 여러 정책들은 각각 자체적인 고유 PPP 필터 식별자로 여러 세트의 패킷 필터 규칙을 정의하는 식으로 강제 적용됩니다. 패킷 필터 규칙을 특정 수신자 연결 프로파일에 대해 지정하거나 해당 범주의 사용자에 대한 필터 규칙을 적용하는 그룹 정책을 사용하여 지정할 수 있습니다. 패킷 필터 규칙 자체가 PPP에 정의되지는 않지만 iSeries Navigator의 IP 패킷 규칙 아래에 정의됩니다. 자세한 정보는 IP 패킷 규칙 Information Center 주제를 참조하십시오.

L2TP 연결의 경우, 반드시 IP SEc 필터링이 있는 VPN을 사용하여 네트워크 통신을 보호해야 합니다. 자세한 정보는 VPN Information Center 주제를 참조하십시오.

시스템 인증

iSeries 서버가 사용하는 PPP 연결은 iSeries에 대한 리모트 클라이언트 다이얼 인과 iSeries가 다이얼링하는 ISP 또는 기타 서버에 대한 연결 모두를 인증하는 데 필요한 몇 가지 옵션을 지원합니다. iSeries는 인증 정보, 권한이 있는 사용자 및 연관 암호의 리스트를 포함하여 iSeries 상의 유효성 리스트 범위를 유지보수하기 위한 여러 가지 방법을 지원하며 이를 통해 네트워크 사용자의 상세한 인증 정보를 유지보수하는 RADIUS 서버를 지원합니다. iSeries 또한 사용자 ID와 암호 정보 암호화 및 단순한 암호 교환에서부터 CHAP-MD5를 사용한 maceration 지원에 이르기까지 여러 옵션을 지원합니다. iSeries Navigator 연결 프로파일의 **인증** 탭에서 다이얼 아웃 시 iSeries 유효성 확인에 사용되는 사용자 ID 및 암호를 포함하여 시스템 인증에 대한 기본설정을 지정할 수 있습니다.

유효성 검사 유지보수 및 인증 정보에 대한 자세한 정보는 다음을 참조하십시오.

- 리모트 인증 다이얼 인 사용자 서비스(RADIUS)
- 유효성 리스트

지원되는 암호 인증 프로토콜에 대한 제세한 정보는 다음을 참조하십시오.

- 챌린지 핸드쉐이크 인증 프로토콜(CHAP-MD5)
- 암호 인증 프로토콜(PAP)
- 확장 인증 프로토콜(EAP)

CHAP-MD5

챌린지 핸드쉐이크 인증 프로토콜(CHAP-MD5)은 인증 시스템과 리모트 장치에만 알려진 값을 연산하는 알고리즘(MD-5)을 사용합니다. CHAP를 사용하면 사용자 ID와 암호가 항상 암호화되므로 PAP보다 안전한 프로토콜입니다. 이 프로토콜은 플레이백 및 시행 착오 액세스 시도에 있어서 효과적입니다. CHAP 인증은 연결 중에 한번 이상 발생할 수 있습니다.

인증 시스템은 네트워크에 연결을 시도하는 리모트 장치로 챌린지를 송신합니다. 그리고 리모트 장치는 두 장치가 모두 사용하는 공통 알고리즘(MD-5)으로 연산되는 값을 사용하여 응답합니다. 인증 시스템은 고유 연산과 비교하여 응답을 확인합니다. 값이 일치하면 인증을 승인하고 값이 일치하지 않으면 연결을 종료합니다.

EAP

확장 인증 프로토콜(EAP)은 제 3자 인증 모듈이 PPP 구현과 대화할 수 있도록 합니다. EAP는 토큰(스마트) 카드, Kerberos, 공용 키 및 S/키와 같은 인증 스키마를 위한 표준 지원 메카니즘을 제공함으로써 PPP를 확장합니다. EAP는 제 3자 보안 장치로 인해 RAS 인증을 증가시키는 늘어나는 요구에 부응하기 위한 것입니다. EAP는 사전 공격 및 암호 추측을 사용하는 해커로부터 VPN을 보호합니다. EAP는 PAP와 CHAP를 상당 부분 향상시킨 것입니다.

EAP를 사용하면 인증 정보가 정보에 포함되어 있는 것이 아니라 정보와 별도로 존재합니다. 이를 통해 리모트 서버가 정보를 수신하거나 전달하기 전에 필요한 인증을 협상할 수 있습니다.

현재 iSeries 서버는 기본적으로 CHAP-MD5와 동등한 EAP 버전만 지원합니다. 그러나 위에 설명한 일부 추가 인증 스키마를 지원할 수 있는 RADIUS 서버를 사용하여 리모트 인증을 사용할 수 있습니다.

PAP

암호 인증 프로토콜(PAP)은 피어(peer) 시스템으로 ID를 설정하는 간단한 방법을 제공하기 위한 양방향 핸드쉐이크를 사용합니다. 링크가 이루어질 때 핸드쉐이크가 수행됩니다. 링크가 이루어지면 제거 장치가 사용자 ID/암호 쌍을 인증 시스템으로 송신합니다. 쌍의 정확성에 따라 인증 시스템이 연결을 계속하거나 종료합니다.

PAP 인증은 리모트 시스템에 송신할 사용자 이름과 암호를 분명한 텍스트 형식으로 요구합니다. PAP에서는 사용자 ID와 암호가 암호화되지 않으므로 이를 추적할 수 있으며 해커의 침범에 대해 무방비로 노출될 수 있습니다. 그러므로 가능하면 항상 CHAP를 사용하십시오.

RADIUS 개요

RADIUS(리모트 인증 다이얼 인 사용자 서비스(Remote Authentication Dial In User Service))는 분산 전화 접속 네트워크에 있는 리모트 액세스 사용자를 위해 중앙 인증, 계정 및 IP 관리 서비스를 제공하는 인터넷 표준 프로토콜입니다.

RADIUS 클라이언트 서버 모델에는 RADIUS 서버에 대한 클라이언트의 역할을 하는 네트워크 액세스 서버(NAS)가 있습니다. NAS 역할을 하는 iSeries 서버가 RFC 2865에 정의된 RADIUS 표준 프로토콜을 사용하여 지정된 RADIUS 서버에 사용자 및 연결 정보를 송신합니다.

RADIUS 서버는 사용자를 인증함으로써 수신 사용자 연결 요청에 대해 작업한 후 필요한 모든 구성 정보를 NAS로 보내고 NAS(iSeries 서버)가 인증된 다이얼 인 사용자에게 인증된 서비스를 전달할 수 있도록 합니다.

RADIUS 서버에 도달할 수 없으면 iSeries 서버가 인증 요구를 대체 서버로 라우트할 수 있습니다. 이것은 현재 사용 중인 액세스점과 관계 없이 전사적으로 액세스를 위한 고유 로그인 사용자 ID와 함께 다이얼 인 서비스를 사용자들에게 제공할 수 있게 해 줍니다.

RADIUS 서버가 인증 요구를 수신하여 이 요구를 유효화시키면 RADIUS 서버가 자료 패킷을 해독하여 사용자 이름 및 암호 정보에 액세스합니다. 그리고 나서 이 정보를 지원 중인 해당 보안 시스템으로 전달합니다. 이것은 UNIX 암호 파일, Kerberos, 범용 보안 시스템 또는 고객이 개발한 보안 시스템이 될 수 있습니다. RADIUS 서버는 인증된 사용자들에게 허용된 IP 주소 등의 모든 서비스를 iSeries 서버로 다시 송신합니다. RADIUS 계정 요청도 유사한 방법으로 처리됩니다. 리모트 사용자의 계정 정보는 지정 RADIUS 계정 서버로 송신시킬 수 있습니다. RADIUS 계정 표준 프로토콜은 RFC 2866에 정의되어 있습니다. RADIUS 계정 서버는 RADIUS 계정 요구에서 나온 정보를 기록함으로써 수신된 계정 요구에 대해 작업합니다. 예로 제공되는 RADIUS 구성에서는 RADIUS 서버를 사용하여 전화 접속 사용자 인증 시나리오를 참조하십시오.

유효성 리스트

유효성 리스트는 리모트 사용자의 사용자 ID 및 암호 정보를 저장하기 위해 사용됩니다. 기존 유효성 리스트를 사용하거나 수신자 연결 프로파일 인증 페이지에서 새로 작성할 수 있습니다. 유효성 검사 리스트 항목에서도 사용자 ID와 암호를 연관시키기 위한 인증 프로토콜 유형을 요구합니다. **암호화 - CHAP-MD5/EAP** 또는 **비암호화 - PAP**가 바로 그것입니다.

자세한 정보는 온라인 도움말을 참조하십시오.

대역폭 고려사항 - 멀티링크

특정 타스크를 완료하기 위해 추가 대역폭이 필요한 경우도 있으나 항상 필요한 것은 아닙니다. 이 경우 전문 하드웨어와 비싼 통신 회선을 구입하는 것이 타당한 해결책은 아닙니다. PPP 멀티링크 프로토콜(MP)은 여러 PPP 링크를 함께 그룹화하여 하나의 가상 링크 또는 ″번들″을 형성합니다. 여러 링크를 하나로 모음으로써 표준 모뎀과 전화선을 사용하여 두 시스템 간에서 총 대역폭을 증가시킬 수 있습니다. 하나의 MP 번들에 여섯 개까지 링크를 포함시킬 수 있습니다. 멀티링크 연결을 설정하려면 PPP 링크의 양 끝에서 멀티링크 프로토콜을 지원해야 합니다. 멀티링크 프로토콜은 RFC(Request For Comment) 표준 RFC1990으로 문서화되어 있습니다. RFC에 대한 자세한 정보는 http://www.rfc-editor.org를 참조하십시오.

요구 시 대역폭

물리적 링크를 동적으로 추가하고 제거하는 기능을 통해 시스템이 필요할 때만 대역폭을 제공하도록 구성할 수 있습니다. 이와 같은 접근방식을 보통 ″요구 시 대역폭″이라고 하며 실제로 대역폭을 사용할 때 추가 대역폭에 대해서만 사용료를 부담하면 됩니다. ″요구 시 대역폭″의 이점을 활용하기 위해서는 최소한 하나의 피어(peer) 시스템이 MP 번들에서 현재 제공하는 총 사용 대역폭을 모니터할 수 있어야 합니다. 그러면 사용 대역폭이 구성에 정의된 값을 초과할 때 링크를 번들에 추가시키거나 제거시킬 수 있습니다. 대역폭 지정 프로토콜은 피

어(peer) 시스템이 MP 번들에(서) 링크를 추가하거나 제거하는 것을 협상할 수 있게 해 줍니다. RFC2125에 PPP 대역폭 지정 프로토콜(BAP)와 대역폭 지정 제어 프로토콜(BACP) 모두 문서화되어 있습니다.

제 6 장 PPP 구성

지점 간 연결을 설정하기 위해 PPP를 사용하려면 먼저 PPP 환경을 구성해야 합니다. 다음은 PPP 환경의 구성 정보를 제공하는 섹션들입니다.

- 연결 프로파일 작성
- 모뎀 구성
- 리모트 PC 구성
- AT&T 글로벌 네트워크를 통해 인터넷 액세스 구성
- 연결 마법사
- 그룹 액세스 정책 구성
- PPP 연결을 위한 IP 패킷 필터링 규칙 적용
- PPP 수신자 연결 프로파일에 대한 RADIUS 및 DHCP 서비스 작동 가능

연결 프로파일 작성

시스템 간에 PPP 연결을 구성하는 데 있어서 첫 번째 단계는 iSeries 서버에 연결 프로파일을 작성하는 일입니다. 연결 프로파일은 다음과 같은 연결 세부사항의 논리적 표현입니다.

- 회선 및 프로파일 유형
- 멀티링크 설정
- 리모트 전화 번호 및 다이얼링 옵션
- 인증
- TCP/IP 설정: IP 주소 및 라우팅
- 작업 관리 및 연결 사용자 정의
- 정의역명 서버

네트워크 디렉토리 밑에 있는 **리모트 액세스 서비스**에 다음 오브젝트들이 나옵니다.

- **개시자 연결 프로파일**은 iSeries 서버(로컬 시스템)에서 시작하는 아웃바운드 지점 간 연결입니다. 이것은 리모트 시스템이 수신하는 PPP 연결입니다.
- **수신자 연결 프로파일**은 리모트 시스템에서 시작하는 인바운드 지점 간 연결입니다. 이것은 iSeries 서버(로컬 시스템)가 수신하는 PPP 연결입니다.
- **모뎀**

연결 프로파일을 작성하려면 다음 단계과 같이 하십시오.

1. iSeries Navigator에서 시스템을 선택하고 **네트워크 -> 리모트 액세스 서비스**를 펼치십시오.
2. 다음 옵션 중 하나를 선택하십시오.

- iSeries 서버를 해당 초기 연결용 서버로 설정하려면 마우스 오른쪽 버튼으로 **개시자 연결 프로파일**을 클릭하십시오.
- iSeries 서버를 리모트 시스템과 사용자로부터 들어오는 연결을 허용하는 서버로 설정하려면 마우스 오른쪽 버튼으로 **수신자 연결 프로파일**을 클릭하십시오.

3. **신규 프로파일**을 선택하십시오.
4. **신규 지점 간 연결 프로파일 설정** 페이지에서 프로토콜 유형을 선택하십시오.
5. 모뎀 선택을 지정하십시오.
6. 링크 구성을 선택하십시오.
7. **확인**을 클릭하십시오.

   신규 지점 간 프로파일 등록 정보 페이지가 표시됩니다. 네트워크에 고유한 나머지 값을 설정할 수 있습니다. 자세한 정보는 온라인 도움말을 참조하십시오.

프로토콜 유형: PPP 또는 SLIP

지점 간 연결을 작성하기 위해 어느 프로토콜 유형을 선택합니까?

PPP는 표준 인터넷 연결입니다. PPP는 서로 다른 제조업체의 리모트 액세스 소프트웨어 간에서 상호운영성을 허용합니다. 또한 여러 네트워크 통신 프로토콜이 동일한 물리적 통신 회선을 사용할 수 있도록 합니다.

PPP는 SLIP를 지점 간 연결을 위한 선택 프로토콜을 대체합니다. SLIP RFC(Request for Comment)는 다음과 같은 문제로 인해 인터넷 표준이 될 수 없습니다.

- SLIP에는 두 호스트 간에서 IP 주소지정을 정의하기 위한 표준 방법이 없습니다. 이것은 번호를 지정하지 않은 통신망은 사용할 수 없음을 나타냅니다.
- SLIP는 오류 감지나 오류 압축에 대한 지원을 하지 않습니다. 오류 발견이나 오류 압축은 PPP에서 지원합니다.
- SLIP는 시스템 인증을 지원하지 않은 반면에 PPP는 양방향 인증을 지원합니다.

현재까지도 SLIP가 계속 사용되고 있으며 iSeries 서버에서 지원됩니다. 그러나 IBM에서는 지점 간 연결을 설정할 때 PPP를 사용할 것을 권장합니다. SLIP는 멀티링크 연결에 대한 지원을 하지 않습니다. SLIP에 비해 PPP가 더 나은 인증 지원을 제공합니다. 이것은 PPP가 가지고 있는 자체적인 압축 기능 때문입니다.

주: 이 릴리스에서는 ASYNC 회선 유형으로 정의된 SLIP 연결 프로파일을 더 이상 지원하지 않습니다. 이 연결 파일을 사용하는 경우 연결 프로파일을 SLIP 프로파일 또는 PPP 회선 유형을 사용하는 PPP 프로파일로 마이그레이트해야 합니다.

모드 선택

PPP 연결 프로파일의 모드 선택에는 **연결 유형** 및 **작동 모드**에 대한 선택이 포함됩니다. 선택한 모드를 통해 서버가 신규 PPP 연결을 어떻게 사용하는 지가 결정됩니다.

모드 선택을 지정하려면 다음과 같이 하십시오.

1. 다음 연결 유형 중에서 하나를 선택하십시오.

- 교환 회선
- 전용 회선
- L2TP(가상 회선)
- PPPoE 회선

2. 신규 PPP 연결에 적합한 작동 모드를 선택하십시오.
3. 선택한 연결 유형과 작동 모드를 기록하십시오. PPP 연결 구성을 시작할 때 이 정보가 필요합니다.

교환 회선

전화선을 통해 연결하기 위해 다음 중 하나를 사용할 경우 이 연결 유형을 선택하십시오.

- 모뎀(내장 또는 외장)
- 내부 ISDN 기본율 인터페이스 어댑터
- 외부 ISDN 단말기 어댑터

교환 회선 연결 유형에는 다음과 같은 작동 모드가 있습니다.

- **응답**

  이 작동 모드 유형을 선택하면 리모트 시스템이 iSeries 서버에 다이얼할 수 있습니다.

- **다이얼**

  이 작동 모드를 선택하면 iSeries 서버가 리모트 시스템에 다이얼할 수 있습니다.

- **요구 시 다이얼(다이얼 전용)**

  이 작동 모드를 선택하면 시스템에서 TCP/IP 통신이 감지될 때 iSeries 서버가 자동으로 리모트 시스템에 다이얼할 수 있습니다. 이 연결은 자료 전송이 완료될 때 그리고 특정 기간 동안 TCP/IP 통신이 발생하지 않을 때 종료합니다.

- **요구 시 다이얼(응답 가능 전용 피어(peer) 장치)**

  이 작동 모드를 선택하면 iSeries 서버가 전용 리모트 시스템의 호출에 응답할 수 있습니다. 또한 리모트 시스템에 대한 TCP/IP 통신이 감지될 때 iSeries 서버가 리모트 시스템을 호출할 수 있습니다. 두 시스템 모두 iSeries 서버이면서 둘 다 이 작동 모드를 사용할 경우 TCP/IP 통신은 영구 실제 연결을 수행할 필요 없이 요구가 있으면 두 시스템 사이를 이동합니다. 이 작동 모드에는 전용 자원이 필요합니다. 이 작동 모드가 제대로 기능하기 위해서는 반드시 리모트 피어(peer) 장치가 다이얼 인해야 합니다.

- **요구 시 다이얼(리모트 피어(peer) 장치 작동 가능)**

  이 작동 모드를 선택하면 리모트 시스템이 다이얼하거나 응답할 수 있습니다. 들어오는 호출을 처리하기 위해서는 이 작동 모드를 지정하는 PPP 연결 프로파일에서 기존 응답 프로파일을 참조해야 합니다. 이렇게 하면 하나의 응답 프로파일이 하나 이상의 피어(peer) 장치에서 보낸 모든 들어오는 호출 및 각 발신 호출에 대한 별도의 요구 시 다이얼 프로파일을 처리할 수 있습니다. 이 작동 모드에는 리모트 피어(peer) 장치에서 보낸 들어오는 호출을 처리하기 위한 전용 자원이 필요 없습니다.

전용 회선

로컬 iSeries 서버 및 리모트 시스템 사이에 전용 회선을 설치한 경우에는 이 연결 유형을 선택하십시오. 전용 회선을 사용하면 두 시스템을 연결하는 데 모뎀이나 ISDN 단말기 어댑터가 필요하지 않습니다.

두 시스템 간의 전용 회선 연결은 영구 또는 전용 회선으로 간주합니다. 전용 회선은 항상 열려 있습니다. 전용 회선 연결의 한쪽 끝은 개시자로 구성되고 다른 쪽 끝은 종료자로 구성됩니다.

전용 회선 연결 유형에는 다음과 같은 작동 모드가 있습니다.

- **종료자**

  이 작동 모드를 선택하면 리모트 시스템이 전용 회선을 통해 iSeries 서버에 액세스할 수 있습니다. 이 작동 모드는 전용 회선 응답 프로파일을 참조합니다.

- **개시자**

  이 작동 모드를 선택하면 iSeries 서버가 전용 회선을 통해 리모트 시스템에 액세스할 수 있습니다. 이 작동 모드는 전용 회선 다이얼 프로파일을 참조합니다.

L2TP(가상 회선)

L2TP(Layer Two Tunneling Protocol)를 사용하는 시스템 간의 연결을 제공하려면 이 연결 유형을 선택하십시오.

L2TP 터널이 완료되면 iSeries 서버와 리모트 시스템 사이에 가상 PPP 연결이 이루어집니다. IP 보안(IP-SEC)과 함께 L2TP 터널링을 사용하여 인터넷을 통해 보안 자료를 송신, 라우트 및 수신할 수 있습니다.

L2TP(가상 회선) 연결 유형에는 다음과 같은 작동 모드가 있습니다.

- **종료자**

  이 작동 모드를 선택하면 리모트 시스템이 L2TP 터널을 통해 iSeries 서버에 연결할 수 있습니다.

- **개시자**

  이 작동 모드를 선택하면 iSeries 서버가 L2TP 터널을 통해 리모트 시스템에 연결할 수 있습니다.

- **리모트 다이얼**

  이 작동 모드를 선택하면 iSeries 서버가 L2TP 터널을 통해 ISP에 연결하고 ISP에게 리모트 클라이언트로 다이얼하도록 지시할 수 있습니다.

- **멀티 홉 개시자**

  이 작동 모드를 선택하면 iSeries 서버가 멀티 홉 연결을 설정할 수 있습니다.

  주: 이 멀티 홉 개시자가 연관되어 있는 L2TP 종료자 프로파일의 경우 ″멀티 홉 연결 허용″ 상자가 선택되어야 하며 PPP 사용자 이름을 멀티 홉 개시자 프로파일에 링크하는 PPP 유효성 리스트 항목이 필요합니다.

계층 2 터널링 프로토콜(L2TP): L2TP는 요구하는 L2TP 클라이언트와 목표 L2TP 서버 종료점 사이의 링크 계층 터널을 지원하기 위해 PPP를 확장한 것입니다. L2TP 터널을 사용하면 전화 접속 프로토콜이 종료하는 위치와 네트워크에 대한 액세스가 제공되는 위치를 분리할 수 있습니다.

인터넷 서비스 제공자(ISP)는 가상 회선 모드를 사용하여 가상 사설망(VPN)을 작동시킵니다. VPN이 L2TP와 작업하는 방식에 관한 자세한 정보는 VPN에 의해 보호된 L2TP 연결 구성을 참조하십시오.

다음 그림은 세 가지의 서로 다른 L2TP 터널링 구현을 보여줍니다.

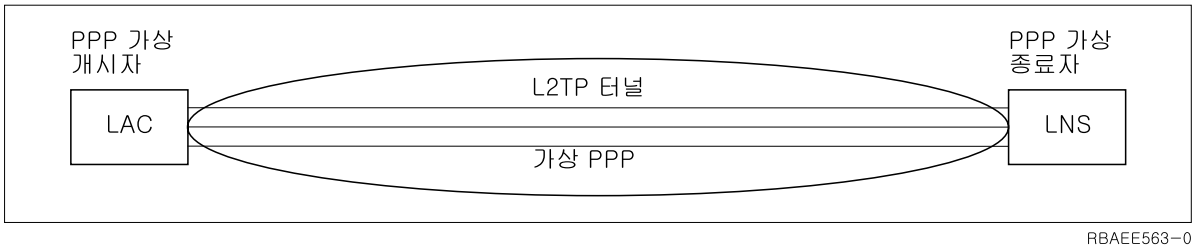


그림 7. PPP 가상 개시자 또는 PPP 가상 종료자

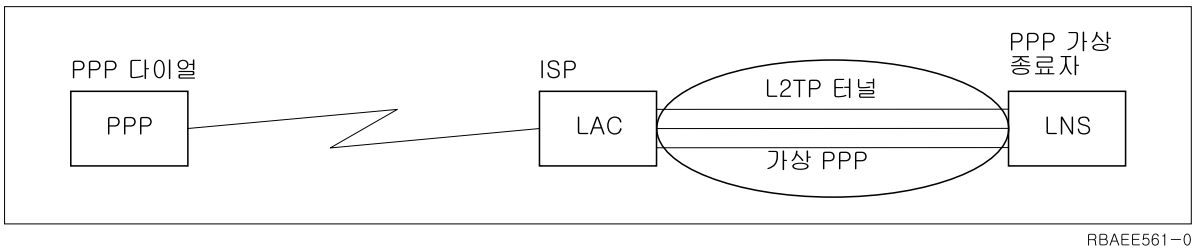


그림 8. PPP 다이얼 개시자 또는 PPP 가상 종료자

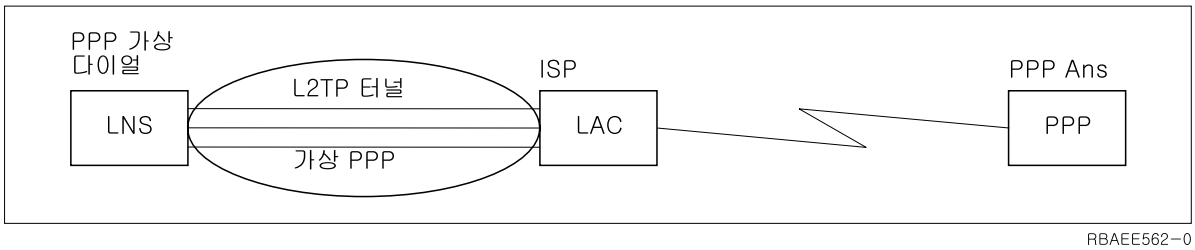


그림 9. PPP 가상 다이얼 또는 PPP 가상 응답

PPPoE 회선

PPPoE 연결은 가상 회선을 사용하여 2838 유형의 이더넷 어댑터를 통해 PPP 데이터를 DSL 모뎀(이더넷 기반의 LAN에 연결된 ISP가 제공)에 의해에 전달합니다. 따라서 LAN 사용자들이 iSeries 서버를 통해 PPP 세션을 경유하여 빠른 속도의 인터넷 액세스를 사용할 수 있습니다. 일단 iSeries와 ISP 간의 연결이 시작되면 LAN 상의 개별 사용자가 PPPoE를 통해 ISP와 고유한 세션을 시작할 수 있습니다.

PPPoE 연결은 개시자(Originator) 연결 프로파일만이 사용하며 개시자 작동 모드를 암시하는 것으로 단일 회선만을 사용합니다.

링크 구성

링크 구성은 PPP 연결 프로파일이 연결을 설정하기 위해 사용하는 회선 서비스의 유형을 정의합니다. 회선 서비스의 유형은 사용자가 지정하는 연결 유형에 따라 다릅니다.

- 단일 회선
- 회선 풀
- 통합 ISDN 회선

단일 회선

아날로그 모뎀과 연결된 PPP 회선을 정의하려면 이 회선 서비스를 선택하십시오. 모뎀이 필요하지 않은 전용 회선에서도 이 옵션이 사용됩니다. PPP 연결 프로파일은 항상 동일한 iSeries 서버 통신 포트 자원을 사용합니다.

필요한 경우 아날로그 단일 회선을 응답 프로파일과 다이얼 프로파일 간에 '공유'되도록 구성할 수 있습니다. 동적 자원 공유는 자원 활용을 향상시키기 위해 설계된 새로운 기능입니다. V5R2가 발표되기 전까지는 프로파일이 모뎀 자원을 사용하는 즉시 시작된 것으로 확약되었습니다. 이러한 방식은 자원이 수동적인 대기 상태에 있더라도 사용자가 세션 당 하나의 자원만 사용하는 것으로 제한시켰습니다. 이제는 특정 자원에 액세스할 때 새로운 공유 규칙이 적용됩니다. 즉, 다이얼 프로파일이 응답 프로파일 전에 시작되는 경우와 응답 프로파일이 다이얼 프로파일 전에 시작되는 경우의 두 가지입니다. 이것은 자원 공유가 가능한 것을 전제로 한 것입니다. 첫 번째 경우에서는 시작된 다이얼 프로파일이 성공적으로 연결됩니다. 그리고 두 번째로 시작된 응답 프로파일은 회선을 사용할 수 있기까지 대기합니다. 일단 다이얼 연결이 종료되면 응답 프로파일이 회선을 요청하고 시작됩니다. 두 번째 경우에서는 시작된 응답 프로파일이 들어오는 연결을 기다립니다. 들어오는 연결을 성공적으로 처리할 수 없으면 두 번째로 시작된 다이얼 프로파일이 회선을 '빌려주는' 응답 프로파일로부터 회선을 '빌려옵니다'. 그리고 나면 나가는 연결이 설정됩니다. 일단 연결이 종료되면 다이얼 프로파일이 들어오는 연결을 수용할 준비가 된 응답 프로파일에 회선을 리턴합니다. 공유 기능을 설정하려면 교환 회선 설명을 위한 모뎀 탭을 클릭하고 '동적 자원 공유 사용'을 선택하십시오.

단일 회선 서비스는 L2TP(가상 회선) 및 PPPoE(가상 회선) 연결 유형에도 사용됩니다. L2TP(가상 회선) 연결 유형의 경우 단일 회선에서 사용되는 하드웨어 통신 포트 자원이 없습니다. L2TP 연결에 사용되는 단일 회선은 터널을 설정하는 데 필요한 물리적 PPP 하드웨어가 없는 *가상* 회선입니다. PPPoE 연결과 함께 사용되는 단일 회선 또한 가상 회선으로서 마치 리모트 연결을 지원하는 PPP 회선처럼 물리적인 이더넷 회선을 처리하는 데 필요한 메카니즘을 제공합니다. PPPoE 가상 회선은 물리적 이더넷 회선에 바인드되어 DSL 모뎀에 대한 이더넷 LAN 연결을 통해 PPP 프로토콜 자료 전송을 지원하는 데 사용됩니다.

회선 풀

회선 풀의 회선을 사용하기 위해 PPP 연결을 설정하려면 이 회선 서비스를 선택하십시오. PPP 연결이 시작할 때 iSeries 서버가 회선 풀에서 사용되지 않는 회선을 선택합니다. 요구 시 다이얼 프로파일의 경우 서버는 리모트 시스템에 대한 TCP/IP 통신을 감지할 때까지 회선을 선택하지 않습니다.

연결 프로파일에 대한 특정 회선 설명을 정의하는 대신 회선 풀을 사용할 수 있습니다. 하나의 회선 풀에 여러 개의 회선 설명을 지정할 수 있습니다.

회선 풀은 또한 단일 연결 프로파일이 복수 수신 아날로그 호출을 처리하거나 단일 발신 아날로그 호출을 처리할 수 있게 해 줍니다. PPP 연결이 종료할 때 이 회선이 회선 풀로 리턴합니다.

여러 개의 수신 아날로그 호출을 동시에 처리하기 위해 회선 풀을 사용하는 경우 들어오는 최대 연결 수를 지정해야 합니다. 연결 프로파일을 구성할 때 **신규 지점 간 프로파일 등록 정보** 대화 상자의 연결 탭에서 이 값을 설정할 수 있습니다. 늘어난 대역폭의 단일 연결을 위해 회선 풀을 사용하려면 멀티링크 설정을 사용하십시오.

회선 풀 사용의 장점

- PPP 연결이 시작될 때까지 PPP 연결에 대한 회선 자원을 확약하지 않습니다.

  특정 회선을 사용하는 PPP 연결에서 동적 자원 공유가 가능하지 않은 한 회선을 사용할 수 없으면 이 연결이 종료합니다. 회선 풀을 사용하는 연결의 경우 프로파일이 시작할 때 사용할 수 있는 회선이 최소한 하나는 회선 풀에 있어야 합니다.

  또한 자원이 공유되도록 구성된 경우, 즉 동적 자원 공유가 가능하면 특히 나가는 연결에 있어서 추가적인 자원 가용성이 제공됩니다.
- 회선 풀과 함께 요구 시 다이얼 프로파일을 사용하여 자원을 보다 효율적으로 사용할 수 있습니다.

  iSeries 서버는 요구 시 다이얼 연결을 사용할 경우에만 회선 풀에서 회선을 선택합니다. 다른 연결의 경우에는 다른 시간에 같은 회선을 사용할 수 있습니다.
- 보다 적은 지원 자원으로 더 많은 PPP 연결을 시작할 수 있습니다.

  예를 들어, 사용자 환경에 네 개의 고유 연결 유형이 필요하지만 지정 시간에 두 개의 회선만 필요한 경우 이러한 환경을 위해 회선 풀을 사용할 수 있습니다. 네 개의 요구 시 다이얼 연결 프로파일을 작성하고 각 프로파일이 두 개의 회선 설명을 포함하는 회선 풀을 참조하도록 만들 수 있습니다. 각각의 회선을 네 개의 연결 프로파일이 사용할 수 있으므로 항상 두 개의 연결은 활성화되어 있습니다. 회선 풀을 사용하면 네 개의 회선을 각각 설치할 필요가 없습니다.

  또한 PPP 연결과 PPP 서버의 조합 환경에서는 회선이 '단일 회선'인지 아니면 '회선 풀(pool)'에 있는 것인지에 관계 없이 회선을 공유할 수 있습니다. 먼저 시작된 프로파일은 연결이 활성화될 때까지 자원을 확약하지 않습니다. 예를 들어, PPP 서버가 시작되었으며 들어오는 연결을 청취 중이면 시작된 PPP 클라이언트에 사용 회선을 '빌려주고' PPP 서버에서 공유 회선을 '빌려옵니다'.

복수 연결 프로파일 지원

복수 연결을 지원하는 지점 간 연결 프로파일을 사용하면 하나의 연결 프로파일로 많은 디지털, 아날로그 또는 L2TP 호출을 처리할 수 있습니다. 이 방법은 여러 사용자를 iSeries 서버에 연결하지만 각각의 PPP 회선을 처리하기 위해 별도의 지점 간 연결 프로파일을 지정하지 않을 때 유용합니다. 이 피처는 하나의 어댑터 또는 2750 및 2751 어댑터(8개의 별도 ISDN B 채널 연결을 지원하는)에서 나온 네 개의 사용 회선을 가지고 있는 4 포트 2805 통합 모뎀에 특히 유용합니다.

복수 연결 프로파일을 지원하는 아날로그 회선의 경우에는 지정된 회선 풀의 모든 회선을 최대 연결 수까지 사용합니다. 기본적으로, 회선 풀에 정의된 각 회선에 대해 별도의 연결 프로파일 작업이 시작됩니다. 모든 연결 프로파일 작업은 각 회선에서 들어오는 호출을 기다립니다.

복수 연결 프로파일에 대한 로컬 IP 주소

복수 연결 프로파일의 로컬 IP 주소를 사용할 수 있지만 로컬 IP 주소는 iSeries 서버에 정의된 기존의 IP 주소여야 합니다. 로컬 IP 주소 풀다운 리스트를 사용하여 기존의 주소를 선택할 수 있습니다. 로컬 iSeries 서버 IP 주소를 PPP 프로파일에 대한 로컬 IP 주소로 선택하면 리모트 사용자들이 로컬 네트워크의 자원에 액세스할 수 있습니다. 또한 리모트 IP 주소 풀에 있는 IP 주소가 로컬 IP 주소와 동일한 네트워크에 놓이도록 정의해야 합니다.

로컬 iSeries 서버 IP 주소가 없거나 리모트 사용자가 LAN에 액세스하지 못하게 하려면 iSeries 서버에 대한 가상 IP 주소를 정의해야 합니다. 가상 IP 주소를 무회로 인터페이스라고도 합니다. 지점 간 프로파일은 이 IP 주소를 로컬 IP 주소로 사용할 수 있습니다. 이 주소는 실제 네트워크에 연결된 것이 아니므로 iSeries 서버에 접속된 다른 네트워크로 통신을 자동 전송하지 않습니다.

가상 IP 주소를 작성하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 서버를 펼치고 **네트워크 -> TCP/IP 구성 -> IPV4 -> 인터페이스**에 액세스하십시오.
2. **인터페이스**를 마우스 오른쪽 버튼으로 클릭하고 **신규 인터페이스 -> 가상 IP**를 선택하십시오.
3. 인터페이스 마법사의 안내에 따라 가상 IP 인터페이스를 작성하십시오. 지점 간 연결 프로파일이 작성되면 가상 IP 주소를 사용할 수 있습니다. TCP/IP 설정 페이지에 있는 로컬 IP 주소 필드의 풀다운 리스트를 사용하여 프로파일과 함께 주소를 사용할 수 있습니다.

   주: 복수 연결 프로파일을 시작하기 전에 가상 IP 주소를 활성화시켜야 합니다. 그렇지 않으면 프로파일이 시작되지 않습니다. 인터페이스를 작성한 후 주소를 활성화하려면 인터페이스 마법사를 사용할 때 주소를 시작하는 옵션을 선택하십시오.

복수 연결 프로파일에 대한 리모트 IP 주소 풀

복수 연결 프로파일의 리모트 IP 주소 풀을 사용할 수도 있습니다. 일반적인 단일 연결 지점 간 프로파일을 사용하면 하나의 리모트 IP 주소(연결이 구축될 때 호출 시스템에 제공되는)만 지정할 수 있습니다. 이제는 여러 호출자들을 동시에 연결할 수 있으므로 리모트 IP 주소의 시작 뿐만 아니라 호출 시스템에 제공되는 추가 IP 주소 범위를 정의할 경우에도 리모트 IP 주소 풀을 사용할 수 있습니다.

회선 풀 제한사항

이 제한사항은 복수 연결을 위해 회선 풀을 사용할 때 적용됩니다.

- 특정 회선은 한 번에 하나의 회선 풀에만 있을 수 있습니다. 회선 풀에서 회선을 제거할 경우 제거된 회선을 다른 회선 풀에 사용할 수 있습니다.
- 회선 풀을 사용하는 복수 연결 프로파일을 시작할 때 회선 풀에 있는 모든 회선이 프로파일에 있는 최대 연결 수만큼 사용됩니다. 회선이 없을 경우에는 모든 신규 연결이 실패합니다. 또한 회선 풀에 회선이 없는 상태에서 다른 프로파일을 시작하면 이 프로파일이 종료합니다.
- 회선 풀이 있는 단일 연결 프로파일을 시작할 때 시스템은 회선 풀에 있는 하나의 회선만 사용합니다. 같은 회선 풀을 사용하는 복수 연결 프로파일을 시작하면 회선 풀에 남아 있는 모든 회선을 사용합니다.

리모트 IP 주소 풀: 리모트 IP 주소 풀은 여러 개의 들어오는 연결과 함께 사용되는 지점 간 연결 프로파일에 응답하거나 종료할 때 사용할 수 있습니다. 여기에는 L2TP, 고유 ISDN 및 둘 이상의 최대 연결 수를 지닌 회선 풀이 포함됩니다. 이 기능은 시스템이 고유의 리모트 IP 주소를 들어오는 각 연결에 할당할 수 있게 해 줍니다.

연결할 1차 시스템이 시작 IP 주소 필드에 정의된 IP 주소를 수신합니다. 주소가 이미 사용 중인 경우에는 주소 수 범위 내에서 그 다음 IP 주소가 할당됩니다. 예를 들어, 시작 IP 주소가 10.1.1.1이고 주소 수가 5로 정의되어 있으면 리모트 IP 주소 풀 내에서 그 주소는 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 및 10.1.1.5입니다. 리모트 IP 주소 풀 주소에 정의되는 서브네트 마스크는 항상 255.255.255.255입니다.

다음은 리모트 IP 주소 풀을 사용할 때 적용되는 제한사항들입니다.

- 둘 이상의 연결 프로파일이 동일한 주소 풀을 지정할 수 있습니다. 그러나 풀의 모든 주소가 사용되면 다른 연결이 종료되어 주소를 사용할 수 있을 때까지 모든 후속 연결 요구가 거부됩니다.
- 기타 수신 시스템이 풀의 주소를 사용하는 동안 특정 주소를 일부 리모트 시스템에 할당하려면 다음과 같이 하십시오.
  1. **인증** 탭에서 리모트 시스템 인증을 사용할 수 있으면 리모트 시스템의 사용자 이름을 알 수 있습니다.
  2. 특정 IP 주소가 필요 없는 들어오는 모든 연결 요구에 대해 리모트 IP 주소 풀을 정의하십시오.
  3. **리모트 시스템 사용자 ID를 기준으로 추가 IP 주소 정의**를 확인한 후 **사용자명으로 IP 주소 정의**를 클릭하여 특정 사용자에 대한 리모트 IP 주소를 정의하십시오.

  리모트 사용자가 연결될 때 iSeries 서버가 이 사용자에 대해 특정 IP 주소가 정의되어 있는지 판별합니다. 정의되어 있으면 리모트 시스템에 IP 주소가 제공됩니다. 그렇지 않으면, 리모트 IP 주소 풀에서 주소를 리턴합니다.

ISDN

ISDN 네트워크 연결과 연관된 PPP 회선을 정의하려면 이 회선 서비스를 선택하십시오.

ISDN 사용의 장점

- ISDN은 보다 빠른 속도로 깨끗한 통신을 제공합니다.
- ISDN의 목적은 모든 유형의 자료를 전송하기 위해 단일 인터페이스와 고속 디지털 네트워크를 사용하여 범용 연결성을 제공하는 것입니다.
- ISDN은 또한 교환 연결을 위한 빠른 연결 성능을 제공합니다. 아날로그 모뎀은 연결하는 데 최고 30초 이상 걸리지만 ISDN은 몇 초만에 연결됩니다.

PPP에 대한 모뎀 구성

아날로그 PPP 연결의 경우 외장 모뎀, 내장 모뎀 또는 ISDN 단말기 어댑터를 사용할 수 있습니다. 모뎀은 아날로그 연결 기능(전용 회선 및 교환 회선)을 제공합니다. iSeries 서버에는 가장 일반적인 모뎀의 모뎀 설명이 정의되어 있습니다.

다음 모뎀 구성 타스크를 완료할 수 있습니다.

- 신규 모뎀 구성
- 모뎀을 회선 설명과 연관
- 모뎀 명령 스트링 설정

신규 모뎀 구성

1. iSeries Navigator에서 서버를 선택하고 **네트워크 -> 리모트 액세스 서비스**를 펼치십시오.
2. **모뎀**을 마우스 오른쪽 버튼으로 클릭한 후 **신규 모뎀**을 선택하십시오.
3. 일반 탭에서 모든 필드 상자에 올바른 값을 입력하십시오.
4. **선택적:** 모뎀에 필요한 모든 초기화 명령을 추가하려면 추가 매개변수 탭을 클릭하십시오.
5. **확인**을 클릭하여 항목을 저장하고 신규 모뎀 등록 정보 페이지를 닫으십시오.

기존 모뎀 설명을 사용할 수 있는지 판별하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 서버를 선택하고 **네트워크 -> 리모트 액세스 서비스**를 펼치십시오.
2. **모뎀**을 선택하십시오.
3. 모뎀 리스트를 검토하여 제조업체 이름, 모뎀 및 모뎀 형식을 찾으십시오.

   주: 모뎀이 디폴트 리스트에 나오면 다음 단계를 수행할 필요가 없습니다.
4. 사용자의 모뎀과 거의 일치하는 모뎀 설명을 마우스 오른쪽 버튼으로 클릭한 후 **등록 정보**를 선택하여 명령 스트링을 검토하십시오.
5. 모뎀 문서를 참조하여 모뎀별로 명령 스트링을 알아보십시오.

   명령 스트링이 모뎀 요구사항과 일치하면 디폴트 모뎀 등록 정보를 사용하십시오. 그렇지 않으면, 모뎀에 대한 모뎀 설명 작성 후 모뎀 리스트에 추가하십시오.

모뎀 설명을 작성하려면 다음과 같이 하십시오.

1. Operations Navigator에서, 서버를 선택하고, **네트워크 -> 리모트 액세스 서비스**를 펼치십시오.
2. **모뎀**을 선택하십시오.
3. 모뎀 리스트에서 마우스 오른쪽 버튼으로 **$generic hayes**를 클릭하고 **신규 모뎀 기본 파일**을 선택하십시오.
4. **신규 모뎀** 대화 상자에서 모뎀에 필요한 정보와 일치하도록 명령 스트링을 변경하십시오.

모뎀 명령 스트링 설정

아래 표에는 iSeries 서버에 정의되어 있는 모뎀에서 사용되는 최소한의 명령 스트링 세트가 나옵니다. 모뎀에 대한 사용자 매뉴얼에서 각각에 해당하는 명령 스트링을 찾을 수 있습니다. 제조업체의 권장 설정을 모뎀 설명에 사용하십시오.

모뎀 등록 정보	대부분의 모뎀에 맞는 명령 스트링
제품 출하 시 디폴트로 모뎀 재설정	AT&F 또는 AT&Z
모뎀 초기화:	

명령 결과 코드 표시	Q0 및 V1
정상 CD 및 DTR 모드	&C1 및 &D2
에코 모드 작동 중지	E0
캐리어 감지를 따르는 자료 세트 준비(DSR)	&S1
하드웨어 흐름 제어 작동가능(RTS/CTS)	
오류 정정 및 압축(선택적) 작동가능(V.42/V.42 bis)	
DTE-DCE 회선 속도가 고정 115.2Kbps(또는 모뎀에서 허용되는 최대 속도)로 실행 가능한 것이어야 함.	
(선택적) 모뎀이 이 기능을 지원하는 경우 비활동 시간 작동가능	
모뎀 응답 모드:	
n 번 울린 후 응답	S0=*n*(n = 1 또는 2)
*m*초 후 캐리어(연결)가 없는 경우 단절	S7=*m*
모뎀 다이얼 유형	톤 다이얼링의 경우 ATDT 또는 펄스 다이얼링의 경우 ATDP

예: ISDN 단말기 어댑터 구성

1. Operations Navigator에서, 서버를 선택하고, **네트워크 -> 리모트 액세스 서비스**를 펼치십시오.
2. **모뎀**을 마우스 오른쪽 버튼으로 클릭한 후 **신규 모뎀**을 선택하십시오.
3. 일반 탭에서 모든 필드 상자에 올바른 값을 입력하십시오.
4. **선택적:** ISDN 매개변수 탭을 클릭하여 모뎀에 필요한 모든 초기화 명령을 추가하십시오.

   ISDN 단말기 어댑터의 경우 이 리스트의 명령 및 매개변수가 다음과 같은 조건에 한해 단말기 어댑터로 송신됩니다.

   - 리스트의 명령 또는 매개변수가 변경되거나 추가될 경우
   - iSeries 서버가 수행할 수 있는 특정 오류 회복 조치의 결과로서

   결과적으로 이 명령이 다음과 같이 제한됩니다.

   - 현지 전화 회사가 제공하는 ISDN 스위치 유형 및 버전 설정
   - 현지 전화 회사가 제공하는 디렉토리 번호 및 서비스 프로파일 ID(SPID) 설정
   - 현지 전화 회사가 제공하는 단말기 항목 ID(TEI) 설정
   - B 채널 프로토콜(비동기 대 동기 PPP) 설정
   - 매개변수 길이를 표시하기 위해 캐리지 리턴을 필요로 하는 가변 길이를 가진 기타 모뎀 설정
   - 설정값 재설정 또는 시스템 전원 차단 후 설정값 복원을 위해 신규 설정 저장 및 활성화
   - *U* 인터페이스 활동 상태 탐색침 명령(ATD*x*). iSeries 서버가 ISDN 중앙 오피스 스위치와의 동기화가 완료된 시기를 판별할 수 있도록 합니다. *x*에는 # 및 *를 포함하여 전화 번호에 사용되는 숫자 중 하나를 사용할 수 있습니다.
5. 추가 모뎀 명령에 **추가**를 클릭하십시오. 연관된 매개변수 및 명령 리스트에 대한 간략한 설명이 있을 수도 있고 없을 수도 있습니다. 모뎀이 회선 설명과 연관되어 있으면 연관된 매개변수 없이 지정한 모든 명령을 매개변수로 할당할 수 있습니다.

6. **확인**을 클릭하여 각 항목을 저장하고 신규 모뎀 등록 정보 페이지를 닫으십시오.

모뎀을 회선 설명과 연관

1. iSeries Navigator에서 서버를 선택하고 **네트워크 -> 리모트 액세스 서비스 -> 개시자 연결 프로파일** 또는 **수신자 연결 프로파일**을 펼치십시오.
2. 다음 옵션 중 하나를 선택하십시오.
   - 기존 연결 프로파일에 대해 작업하려면 연결 프로파일을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
   - 신규 연결 프로파일에 대해 작업하려면 신규 프로파일을 작성하십시오.
3. 신규 지점 간 프로파일 등록 정보 페이지에서 **연결** 탭을 선택한 후 **신규**를 클릭하십시오.
   - 링크 구성에 대한 이름을 입력하십시오.
   - **신규**를 클릭하고 신규 회선 등록 정보 대화 상자를 여십시오.
4. 신규 회선 등록 정보 대화 상자에서 **모뎀** 탭을 클릭한 후 리스트에서 모뎀을 선택하십시오. 선택한 모뎀이 이 회선 설명과 연관됩니다. 내부 모뎀의 경우 적합한 모뎀 정의를 이미 선택했어야 합니다. 자세한 정보는 온라인 도움말을 참조하십시오.

V5R2의 경우에는 들어오는 호출을 기다리는 중인 수신자 연결 프로파일에 할당된 ppp 회선과 모뎀을 ″빌려 올 수(borrow)″ 있도록 개시자(Originator) 연결 프로파일을 구성할 수 있습니다. 연결이 끝나면 시작한 연결이 PPP 회선과 모뎀을 수신자 연결 프로파일에 ″리턴″합니다. 이러한 새로운 기능을 작동할 수 있게 하려면 ppp 회선 구성 대화 상자의 모뎀 탭에서 **동적 자원 공유 사용** 옵션을 선택하십시오. 그러면 수신자 및 개시자(Originator) 연결 프로파일의 연결 탭에서 PPP 회선을 구성할 수 있습니다.

리모트 PC 구성

Windows 32비트 오퍼레이팅 시스템을 실행하는 PC에서 iSeries 서버로 연결하려면 모뎀을 적절히 설치하고 구성했는지 그리고 PC에 TCP/IP 및 전화 접속 네트워크를 설치했는지 확인하십시오.

PC에서 전화 접속 네트워킹 구성에 관한 정보는 Microsoft Windows 문서를 참조하십시오. 반드시 다음 정보를 지정하거나 입력하십시오.

- 전화 접속 연결 유형에는 **PPP**를 사용하십시오.
- 암호화된 암호를 사용하는 경우 MD-5 CHAP를 사용하는지 확인하십시오. (MS-CHAP는 iSeries 서버에서 지원되지 않습니다.) 일부 Windows 버전은 MD-5 CHAP를 직접 지원하지 않지만 Microsoft로부터 추가 도움을 받아 구성할 수 있습니다.
- 암호화되지 않은(또는 비보호) 암호를 사용하는 경우 PAP가 자동으로 사용됩니다. 다른 모든 비보호 프로토콜 유형은 iSeries 서버에서 지원하지 않습니다.
- 일반적으로 IP 주소지정은 리모트 시스템이 정의하거나 이 경우 iSeries 서버가 정의합니다. 대체 IP 주소지정 방법을 사용하는 경우(사용자 자신의 IP 주소를 정의하는 것처럼) iSeries 서버가 사용자의 주소지정 방법을 승인하도록 구성되어 있는지 확인하십시오.
- 사용자 환경에 적합할 경우 DNS IP 주소를 추가하십시오.

AT&T 글로벌 네트워크를 통해 인터넷 액세스 구성

IBM은 IBM AT&T 글로벌 네트워크를 통해 인터넷 액세스를 제공합니다. 이 서비스에 액세스하는 경우 AT&T 글로벌 네트워크에 다이얼하기 위한 교환 다이얼 PPP 연결 프로파일을 구성하는 데 도움을 주는 AT&T 글로벌 네트워크 다이얼 연결 마법사를 사용할 수 있습니다. 마법사는 8개 패널을 약 10분 간에 걸쳐 처리합니다. 언제든지 마법사를 취소할 수 있으며 기존 자료는 저장되지 않습니다.

두 가지 어플리케이션 유형이 AT&T 글로벌 네트워크 연결을 사용할 수 있습니다.

- **메일 교환**: 단일 AT&T 글로벌 네트워크 계정에서 메일을 정기적으로 검색하여 이를 Lotus Mail 사용자 또는 SMTP(Simple Mail Transfer Protocol) 사용자에게 분배하기 위해 iSeries 서버에 송신할 수 있게 해 줍니다.
- **전화 접속 네트워킹**: 표준 인터넷 액세스처럼 AT&T 글로벌 네트워크에서 기타 전화 접속 네트워킹 어플리케이션을 사용합니다.

다른 PPP 연결 프로파일과 마찬가지로 사용자들이 AT&T 글로벌 네트워크 연결 프로파일을 유지보수합니다.

AT&T 글로벌 네트워크 다이얼 연결 마법사를 사용하려면 다음 어댑터 중 하나가 필요합니다.

- 2699: 2회선 WAN IOA
- 2720: PCI WAN/쌍축 IOA
- 2721: PCI 2회선 WAN IOA
- 2745: PCI 2회선 WAN IOA(IOA 2721 대체)
- 2761: 8포트 아날로그 모뎀 IOA
- 2771: 2포트 WAN IOA(포트 1에서 V.90 통합 모뎀을 사용하고 포트 2에서 표준 통신 인터페이스를 사용). 2771 어댑터의 포트 2를 사용하려면 적합한 케이블을 사용하는 외장 모뎀 또는 ISDN 단말기 어댑터가 필요합니다.
- 2772: 2포트 V.90 통합 모뎀 WAN IOA
- 2793 2포트 WAN IOA(포트 1에서 V.92 통합 모뎀을 사용하고 포트 2에서 표준 통신 인터페이스를 사용). 이 제품이 모델 2771을 대체합니다.
- 2805: 통합된 V.92, 통합된 모뎀이 있는 4 포트 WAN IOA. 이 제품이 모델 2761 및 2772를 대체합니다.

AT&T 글로벌 네트워크 다이얼 연결 마법사를 시작하기 전에 먼저 환경에 대해 다음과 같은 정보를 수집해야 합니다.

- 메일 교환 어플리케이션 또는 전화 접속 네트워킹 어플리케이션에 대한 AT&T 글로벌 네트워크 계정 정보(계정 번호, 사용자 ID 및 암호)
- 메일 교환 어플리케이션에 대한 메일 서버 및 정의역명 서버의 IP 주소
- 단일 회선 연결에 사용되는 모뎀 이름

AT&T 글로벌 네트워크 다이얼 연결 마법사를 시작하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 서버를 펼치고 **네트워크 -> 리모트 액세스 서비스**에 액세스하십시오.

2. **개시자 연결 프로파일**을 마우스 오른쪽 버튼으로 클릭하고 **신규 AT&T 글로벌 네트워크 다이얼 연결**을 선택하십시오.
3. AT&T 글로벌 네트워크 다이얼 연결 마법사가 시작할 때 패널을 완료하기 위한 정보가 필요하면 **도움말**을 클릭하십시오.

연결 마법사

신규 다이얼 연결 마법사

이 마법사는 인터넷 서비스 제공자(ISP) 또는 인트라넷에 액세스하기 위한 전화 접속 연결 프로파일을 구성하는 단계로 안내합니다. 마법사를 완료하기 위해서는 네트워크 관리자나 인터넷 서비스 제공자(ISP)로부터 몇 가지 정보를 받아야 할 수 있습니다. 이 마법사를 완료하는 데 관한 자세한 정보는 온라인 도움말을 참조하십시오.

범용 연결 마법사

이 마법사는 IBM에 연결하기 위한 전자 고객 지원 소프트웨어에 사용할 프로파일을 구성하는 단계로 안내합니다. 전자 서비스 지원은 고유 iSeries 서버 시스템 환경을 모니터하여 시스템 및 상황별로 수정 프로그램 권장사항을 제공합니다. 이 마법사를 완료하는 데 관한 자세한 정보는 온라인 도움말을 참조하십시오.

그룹 액세스 정책 구성

수신자 연결 프로파일 아래에 나오는 **그룹 액세스 정책**이 리모트 사용자 그룹에 적용되는 지점 간 연결 매개변수를 구성하기 위한 옵션을 제공합니다. 이 옵션은 리모트 시스템에서 시작하여 로컬 시스템에서 수신되는 지점 간 연결에 대해서만 적용됩니다.

신규 그룹 액세스 정책을 구성하려면 다음과 같이 하십시오.

1. Operations Navigator에서 서버를 선택하고 **네트워크 -> 리모트 액세스 서비스 -> 수신자 연결 프로파일**을 펼치십시오.
2. **그룹 액세스 정책**을 마우스 오른쪽 버튼으로 클릭하고 **신규 그룹 액세스 정책**을 선택하십시오.
3. **일반** 탭에서 신규 그룹 액세스 정책에 대한 이름과 설명을 입력하십시오.
4. **멀티링크** 탭을 클릭하고 멀티링크 구성을 설정하십시오.

   멀티링크 구성은 여러 개의 실제 회선을 하나의 번들로 함께 결합하는 것을 나타냅니다. 번들당 최대 링크 수는 1-16입니다. 연결이 작성될 때까지 회선 유형 설정을 알 수 없으므로 디폴트 값은 항상 1입니다. 그룹 정책은 특정 사용자에 대해 멀티링크 프로토콜의 기능을 확장하거나 제한하는 데 사용할 수 있습니다.

   - **번들당 최대 링크**는 하나의 논리 회선으로 가능한 최대 링크 수(또는 회선)를 나타냅니다. 최대 회선 수가 이 그룹 정책을 PPP 프로파일 세션에 적용할 때 사용할 수 있는 회선 수를 초과해서는 안됩니다.
   - 리모트 시스템이 대역폭 할당 프로토콜(BACP)을 지원할 때만 연결이 설정되도록 지정하려면 **대역폭 할당 프로토콜 요구**를 확인하십시오. BACP를 협상할 수 없으면 단일 링크가 허용됩니다.
5. 다음 중 하나를 작동가능하게 하려면 **TCP/IP 설정** 탭을 클릭하십시오.

- 리모트 시스템의 다른 네트워크 액세스 허용(IP 이송).

  이 옵션은 사용자가 IP 이송을 원하는지 여부를 지정합니다. 이 옵션을 선택하면 기본적으로 iSeries 서버가 이 연결에 대해 라우터로 작용할 수 있습니다. 이것은 이 iSeries 서버로 지정되지 않은 인터넷 프로토콜(IP) 데이터그램이 이 시스템을 통해 연결된 네트워크로 갈 수 있게 해 줍니다. 이것을 공백 상태로 남겨두면 인터넷 프로토콜(IP)이 데이터그램을 리모트 시스템에서 삭제합니다(iSeries 서버에 대해 로컬인 모든 주소로 지정되지 않은).

  보안 상의 이유로 사용자가 IP 이송을 허용하지 않을 수 있습니다. 그러나 이와는 대조적으로 인터넷 서비스 제공자(ISP)의 경우 일반적으로 IP 이송을 제공합니다. 이것은 시스템 전반의 IP 데이터그램 이송이 작동 가능한 경우에만 효과가 있으며 그렇지 않은 경우에는 표시가 되어 있더라도 무시됩니다. 시스템 전반의 IP 데이터그램 이송은 TCP/IP 등록 정보 페이지의 설정 탭에서 표시될 수 있습니다.

- TCP/IP 헤더 압축(VJ) 요구

  이 옵션은 사용자가 인터넷 프로토콜(IP)이 연결을 설정한 후 헤더 정보를 압축하게 할 것인지 여부를 지정합니다. 압축할 경우 일반적으로 성능이 높아지는데 특히 대화식 통신이나 느린 직렬 회선에서 특히 그렇습니다. 헤더 압축은 RFC 1332에 정의된 Van Jacobson(VJ) 방식을 따릅니다. PPP의 경우 연결이 설정되었을 때 압축에 협상이 이루어집니다. 연결의 다른 쪽 끝이 VJ 압축을 지원하지 않으면 iSeries 서버가 압축을 사용하지 않는 연결을 설정합니다.

- 이 연결에 대해서 IP 패킷 규칙 사용

  이 옵션은 사용자가 이 그룹 정책에 대해 필터 규칙을 적용하는지 여부를 지정합니다. 필터 규칙을 통해 네트워크에서 허용하는 IP 통신을 제어할 수 있습니다. 그리고 이 IP 패킷 필터링 구성요소를 사용하여 시스템을 보호할 수 있습니다. IP 패킷 필터링 구성요소는 사용자가 지정하는 규칙에 따라 패킷을 필터링하여 시스템을 보호합니다. 이 규칙은 패킷 헤더 정보에 기초한 것입니다.

  IP 패킷 규칙에 관한 자세한 정보는 Information Center에서 IP 패킷 필터링 및 NAT 주제를 참조하십시오.

예를 들어, 그룹 액세스 정책 및 IP 주소 필터링을 사용하여 자원에 대한 사용자 액세스 관리를 참조할 수 있습니다.

리모트 액세스 사용자에 대해 그룹 정책 적용:

신규 **수신자 연결 프로파일**에 대한 지점 간 등록 정보를 완료했으면 리모트 액세스 사용자에 대해 그룹 정책을 적용할 수 있습니다.

리모트 액세스 사용자에 대해 그룹 정책을 적용하려면 다음과 같이 하십시오.

1. **인증** 페이지를 클릭하십시오.
2. **iSeries 서버가 리모트 시스템의 ID 확인**을 선택하십시오.
3. **유효성 리스트를 사용하여 로컬로 인증**을 선택하십시오.
4. 기존의 유효성 확인 리스트가 있으면 풀다운 리스트에서 선택하여 **열기**를 클릭하십시오. 유효성 확인 리스트를 처음 작성하는 경우 신규 유효성 확인 리스트에 대한 이름을 입력한 후 **신규**를 클릭하십시오.
5. 신규 사용자를 유효성 리스트에 추가하려면 **추가**를 클릭하십시오.

6. 사용자 추가 대화 상자에서 다음을 완료하십시오.
   - 사용자명이 정의되어 있는 인증 프로토콜을 선택하십시오.
   - 사용자명과 암호를 입력하십시오.

     주: 보안을 위해 챌린지 핸드쉐이크 인증 프로토콜22314(CHAP), 확장 인증 프로토콜(EAP) 및 암호 인증 프로토콜(PAP) 사용자 정의에 같은 암호를 사용하지 않는 것이 좋습니다.
   - **사용자에 대해 그룹 정책 적용**을 선택하고 풀다운 리스트에서 그룹 정책을 선택한 후 **열기**를 클릭하십시오.

     그룹 정책 등록 정보를 수정하거나 기존 설정에 대해 작업할 수 있습니다. 구성을 완료하고 지점 간 등록 정보 페이지로 가려면 **확인**을 클릭하십시오.

IP 패킷 필터링 규칙을 PPP 연결에 적용

Information Center의 IP 패킷 필터링 및 NAT 규칙 주제에 PPP 연결 프로파일에 대해 참조할 수 있는 IP 패킷 규칙의 작성 방법이 나옵니다. 패킷 규칙 파일을 사용하여 네트워크 상의 IP 주소에 대한 그룹 액세스를 제한할 수 있습니다. PPP 연결과 함께 필터 규칙 파일을 사용하는 예에 관해서는 시나리오: 그룹 정책 및 IP 필터링을 사용하여 자원에 대한 리모트 사용자 액세스 관리를 참조하십시오.

다음과 같이 두 가지 방법으로 기존 IP 패킷 필터링 규칙을 참조할 수 있습니다.

- 연결 프로파일 레벨
  1. **수신자 연결 프로파일**에 대한 **지점 간 등록 정보**를 완료한 후 TCP/IP 설정 페이지를 선택하고 **확장**을 클릭하십시오.
  2. **이 연결에 IP 패킷 규칙 사용**을 선택하고 풀다운 리스트에서 PPP 필터 식별자를 선택하십시오.
  3. **확인**을 클릭하고 PPP 필터를 연결 프로파일에 적용하십시오.
- 사용자 레벨
  1. 기존 그룹 액세스 정책을 열거나 신규 그룹 액세스 정책을 작성하십시오.
  2. TCP/IP 설정 페이지를 클릭하십시오.
  3. **이 연결에 IP 패킷 규칙 사용**을 선택하고 풀다운 리스트에서 PPP 필터 식별자를 선택하십시오.
  4. **확인**을 클릭하고 PPP 필터를 적용하십시오.

연결 프로파일에 대한 RADIUS 및 DHCP 서비스 작동 가능

PPP 수신자 연결 프로파일에 대한 RADIUS 및 DHCP 서비스를 작동 가능하게 하려면 다음과 같이 하십시오.

1. Operations Navigator에서, 서버를 선택하고, **네트워크 -> 리모트 액세스 서비스**를 펼치십시오.
2. **리모트 액세스 서비스**를 마우스 오른쪽 버튼으로 클릭하고, **서비스**를 선택하십시오.
3. **DHCP-WAN** 탭을 클릭하십시오. 이렇게 함으로써 자동으로 DHCP를 사용할 수 있으며 시스템 상에서 실행되는 DHCP 서버 및 릴레이 에이전트를 감지할 수 있습니다.

4. RADIUS 서비스를 작동 가능하게 하려면 **RADIUS** 탭을 클릭하십시오.
   a. **RADIUS 네트워크 액세스 서버 연결 작동 가능**을 선택하십시오.
   b. **인증을 위해 RADIUS 사용**을 선택하십시오.
   c. RADIUS 솔루션에 따라 RADIUS가 연결 계정 및 TCP/IP 주소 구성을 사용할 수 있습니다.
5. **RADIUS NAS 설정** 버튼을 클릭하여 연결을 RADIUS 서버로 구성하십시오.
6. 확인을 클릭하여 iSeries Navigator로 가십시오.

예로 든 RADIUS 구성에서는 RADIUS 서버를 사용하여 전화 접속 사용자 인증 시나리오를 참조하십시오.

제 7 장 PPP 관리

다음은 iSeries 서버에서 수행할 수 있는 PPP 관리 타스크입니다.

- 연결 프로파일에 대한 등록 정보 설정
- PPP 활동 모니터링

PPP 연결 프로파일에 대한 등록 정보 설정

연결 프로파일을 작성할 때 일반적으로 지점 간 연결 프로파일 설정 대화 상자에서 신규 연결 프로파일에 대한 프로토콜, 연결 유형 및 작동 모드를 선택합니다. 이 대화 상자에서 선택사항을 입력하면 연결 프로파일 등록 정보 양식이 나옵니다. 지점 간 연결 프로파일 설정 대화 상자에서 지정한 선택사항이 연결 프로파일 등록 정보 양식의 페이지 내용과 탭 순서를 결정합니다. 등록 정보 양식은 개시자 연결 프로파일과 수신자 연결 프로파일에서 서로 다릅니다.

신규 지점 간 프로파일 등록 정보 대화 상자의 각 페이지를 완료할 때 이 지침을 사용할 수 있습니다. 각 페이지에서 선택하는 설정은 사용자 환경 및 구성한 연결 유형에 따라 다릅니다. iSeries Navigator 온라인 도움말을 통해 이 대화 상자에 나오는 각 옵션의 설명을 볼 수 있습니다. 자세한 정보는 PPP 예와 프로시듀어를 참조하십시오.

PPP 활동 모니터링

이 페이지에서는 Operations Navigator를 사용하여 연결 프로파일 및 세션 기록부를 보는 방법에 관해 설명합니다.

PPP 연결 작업에 대한 정보

- 각 PPP 연결 작업을 관리하기 위해 두 가지 PPP 제어 작업이 사용됩니다. 이 작업들은 QSYSWRK 서브시스템에서 실행됩니다.
  - QTPPPCTL - 기본 PPP 제어 작업. 이 작업이 각 PPP 연결 작업을 관리합니다.
  - QTPPPL2TP - L2TP 서버. 이 작업이 L2TP 터널 설정을 관리하며 L2TP 프로파일이 현재 실행되는 경우에만 실행됩니다.
- PPP 연결 작업은 QTCP 사용자 프로파일 하에서 실행되며 각 PPP 연결을 처리하는 데 사용됩니다. 이 작업들은 디폴트로 QUSRWRK 서브시스템에서 실행되며 다른 서브시스템에서 실행되도록 구성할 수도 있습니다. 다음과 같이 두 가지 PPP 연결 작업 이름을 사용할 수 있습니다.
  - QTPPPSSN - 이 작업은 L2TP PPP 이외의 모든 연결을 처리하는 데 사용됩니다.
  - QTPPPL2SSN - 이 작업은 QTPPPL2TP 작업이 L2TP 터널을 협상한 후 가상 PPP 자료를 처리하는 데 사용됩니다.
- SLIP 연결 작업은 QTCP 사용자명 아래 QSYSWRK 서브시스템에서 실행됩니다. 다음은 두 가지 유형의 SLIP 작업명입니다.

- QTPPDIAL*nn*은 다이얼 아웃 작업입니다. 여기서 *nn*은 1과 99 사이의 숫자입니다.
- QTPPANS*nn*은 다이얼 인 작업입니다. 여기서 *nn*은 1과 99 사이의 숫자입니다.

연결 프로파일에 대한 작업

1. iSeries Navigator에서 서버를 펼치고 **네트워크 -> 리모트 액세스 서비스**에 액세스하십시오. **개시자 연결 프로파일** 또는 **수신자 연결 프로파일**을 선택하십시오.
2. 프로파일 열에서 연결 프로파일 이름을 마우스 오른쪽 버튼으로 클릭한 후 다음 옵션 중 하나를 선택하십시오.
   - **작업**을 선택하면 QTPP*xxx* 작업에 대한 작업 기록부가 열립니다.
   - **연결**을 선택하면 이 프로파일과 연관된 모든 연결에 대한 정보를 표시하는 대화 상자가 열립니다. 이 정보에 현재 연결, 이전 연결 또는 두 가지 모두를 위한 연결 자료가 포함되어 있습니다. 각 연결에 대한 작업 출력 또는 연결 세부사항을 보기 위해 옵션을 사용할 수 있습니다.
   - **등록 정보**를 선택하면 연결에 대한 현재의 등록 정보를 표시하는 등록 정보 페이지가 열립니다.

연결 정보 보기:

1. iSeries Navigator에서 서버를 펼치고 **네트워크 -> 리모트 액세스 서비스**에 액세스하십시오. **개시자 연결 프로파일** 또는 **수신자 연결 프로파일**을 선택하십시오.
2. 프로파일 열에서 활성 상태의 연결 프로파일을 마우스 오른쪽 버튼으로 클릭한 후 **연결**을 선택하여 연결 정보를 보십시오.

   이 프로파일에 대한 각 연결이 표시됩니다(현재 및 이전). 상태 필드는 연결의 현재 상태를 나타냅니다. 각 PPP 작업의 상태에 따라 연결된 사용자의 ID, 리모트 IP 주소 및 PPP 작업 이름과 같은 추가 정보가 표시될 수 있습니다.
3. 연결에 대한 작업 출력이나 세부사항을 보려면, 마우스 오른쪽 버튼으로 연결을 클릭하십시오. 버튼이 작동 가능 상태로 됩니다.
4. 작업 출력을 보려면 **작업**을 클릭하십시오. 작업 기록부에서 마우스 오른쪽 버튼으로 작업명을 클릭한 후 **프린터 출력**을 선택하십시오. 연결 세션 기록부 및 작업 기록부(종료된 세션에 대한)의 내용이 표시될 수 있습니다.
5. 연결 세부사항을 보려면 **세부사항**을 클릭하십시오. 세부사항은 현재 활동하는 연결에 대해서만 표시될 수 있습니다. 세부사항 대화 상자에서 특정 연결에 대한 추가 연결 정보를 볼 수 있습니다.

iSeries 서버에서 PPP 출력에 대한 작업

PPP 출력에 대해 작업하려면 iSeries 서버 명령행에서 WRKTCPPTP를 입력하십시오.

- 활동 중인 모든 PPP 작업(QTPPPCTL 및 QTPPPL2TP 포함)에 대해 작업하려면 **F14**(활동 작업에 대한 작업)를 누르십시오.
- 특정 연결 프로파일에 대한 모든 출력에 대해 작업하려면 해당 프로파일에 대해 **옵션 8**(출력에 대한 작업)을 선택하십시오.
- PPP 프로파일 구성을 인쇄하려면 해당 프로파일에 대해 **옵션 6**(인쇄)을 선택하십시오. WRKSPLF 명령을 사용하여 인쇄 출력에 액세스할 수 있습니다.

연결 상태:

연결 프로파일 상태는 개시자 또는 수신자 프로파일 중 하나를 선택한 후 **네트워크 > 리모트 액세스 서비스** 아래 연결 프로파일 리스트에서 각 프로파일에 대한 **상태** 필드에 표시됩니다. 각 연결에 대한 상태는 연결 대화 상자를 통해 표시됩니다.

1차 상태 설명	**원인**
연결 요구 대기 중	수신자 프로파일이 연결 준비를 완료함
들어오는 호출 대기 중	서버가 연결 준비를 완료함
연결 중	리모트 시스템과의 연결을 처리하는 중
활동/활동 연결	연결이 이루어지고 작업을 실행하는 중
비활동	이 연결 프로파일에 대해 현재 실행되는 작업이 없음
종료됨	정보를 사용할 수 있음
멀티홉 종료자가 멀티홉 개시자를 시작하는 중	멀티홉 진행 중
멀티홉 연결이 활동 중	멀티홉이 성공적으로 연결됨

2차 상태 설명	**원인**
모뎀 초기화 중	전화 접속 연결 시작 시 모뎀을 초기화하는 중
모뎀 연결 대기 중	PPP 서버가 청취 상태임
DIALING xxx-xxxx	전화 접속 클라이언트에 의해 다이얼된 번호
들어오는 호출이 감지됨	PPP 서버가 들어오는 모뎀 호출을 감지함
모뎀이 연결됨	PPP 핸드쉐이크가 성공적으로 완료됨
선택적	PPP 연결이 활동하는 중
링크가 종료됨	피어(peer)에 의해 연결이 종료됨
중단됨	프로파일 또는 작업이 종료됨
인증 실패	인증 실패로 인해 PPP 연결이 설정되지 못함
연결 비활동 시간종료	비활동 시간종료로 PPP 연결이 설정되지 못함
IP 주소 협상	IP 협상 문제로 인해 PPP 연결이 종료됨
리모트 모뎀이 응답하지 않음	다른 쪽에서 응답이 없음으로 PPP 연결이 설정되지 못함
프로토콜 거부	NCP 협상 실패로 인해 PPP 연결이 설정되지 못함
재시도 실패	재시도 횟수를 초과하여 PPP 연결이 설정되지 못함
피어(peer)로부터 PPPoE 세션 확약을 수신함	PPPoE 협상이 성공적으로 완료됨
L2TP 호출이 설정됨	L2TP 터널 설정 메세지

제 8 장 PPP 문제 해결

프로그램 임시 수정(PTF) 및 문제 해결에 대한 최신 정보는 iSeries server TCP/IP 홈 페이지의 에 정리되어 있습니다. 이 링크를 통해 이 주제와 관련된 보충 정보 및 최신 정보를 제공받을 수 있습니다.

PPP 연결 문제가 발생하면 이 체크 리스트를 사용하여 오류 정보를 수집할 수 있습니다. 오류 현상을 식별하거나 PPP 연결 문제를 분석할 때 이 체크 리스트를 참조하십시오.

1. 필수 지원 정보:
   - 리모트 호스트 유형, 오퍼레이팅 시스템 및 레벨
   - iSeries 서버 호스트 오퍼레이팅 시스템 레벨
   - 실패 세션의 작업 기록부 및 연결 대화 파일

     V5R1에서는 작업 기록부 및 연결 대화 출력이 프로파일과 같은 이름으로 OUTQ에 저장되었습니다.
   - 사용자의 환경에서 사용된 경우에 연결 스크립트
   - 연결 실패 전후의 연결 프로파일 상태
2. 권장 지원 정보:
   - 회선 설명
   - 연결 프로파일

     WRKTCPPTP의 옵션 6이 프로파일 설정을 인쇄합니다.
   - 모뎀 유형 및 모델
   - 모뎀 명령 스트링
   - 통신 추적

ITSO 레드북 TCP/IP for iSeries server: More Cool Things Than Ever(SG24-5190) 에서 다음과 같은 PPP 문제점에 관해 광범위하게 설명합니다. 또한 자세한 문제점 해결 정보를 제공합니다.

문제점	솔루션
모뎀 하드웨어 구성 dip-스위치 및 기타 하드웨어 설정의 틀린 구성	모뎀이 올바른 프레임 처리 유형으로 구성되어 있는지 확인하십시오. *비동기* 또는 *동기* 상태일 수 있습니다. 자세한 정보는 모뎀 매뉴얼을 참조하십시오.
모뎀 AT 명령 사용하려는 모뎀이 Operations Navigator의 사전정의된 모뎀 리스트에 없습니다.	신규 모뎀 작성.
PPP 사용자 및 암호 PPP 연결을 시도할 때 사용자명 및 암호 오류가 발생합니다.	• 사용자 ID 및 암호의 대소문자를 확인하십시오. • 피어(peer) 시스템이 사용하는 인증 프로토콜이 같은 것인지 확인하십시오. • 다른 피어(peer) 시스템이 CHAP로 구성되어 있으면 한 피어(peer) 시스템에서 PAP를 사용하지 마십시오.

문제점	솔루션
연결 프로파일을 시작하기 위한 PPP 회선 식별된 PPP 회선들은 모두 같은 하드웨어 자원에서 사용합니다.	같은 하드웨어 자원을 사용하는 다른 회선들은 단절변환시켜야 합니다.
PPP 프로토콜 틀린 PPP 프로토콜 구성으로 인해 연결 오류가 발생할 수 있습니다.	구성 오류 때문에 피어(peer)가 서로 통신할 수 없는 상황에서는 하위 레벨의 PPP 프로토콜을 조사해야 할 수 있습니다. PPP 기록부나 PPP 작업의 작업 기록부에 이 문제가 표시되지 않은 경우 통신 추적 기능을 사용하여 문제를 조사할 수 있습니다.

제 9 장 PPP에 대한 기타 정보

PPP에 대한 기타 정보 소스:

- 최신 프로그램 임시 수정(PTF)을 포함하여 PPP 및 L2TP의 최신 구성 정보에 관해 iSeries server TCP/IP 홈 페이지에서 PPP 링크를 통해 알 수 있습니다. 이 링크에서 **리모트 액세스 서비스: PPP 연결** 주제에 포함되어 있는 정보를 보충하고 대체하는 최신 정보를 제공합니다.
- ITSO 레드북 TCP/IP for iSeries server: More Cool Things Than Ever(SG24-5190) 에서 TCP/IP 서비스와 어플리케이션에 관한 광범위한 설명을 제공합니다.

Printed in U.S.A