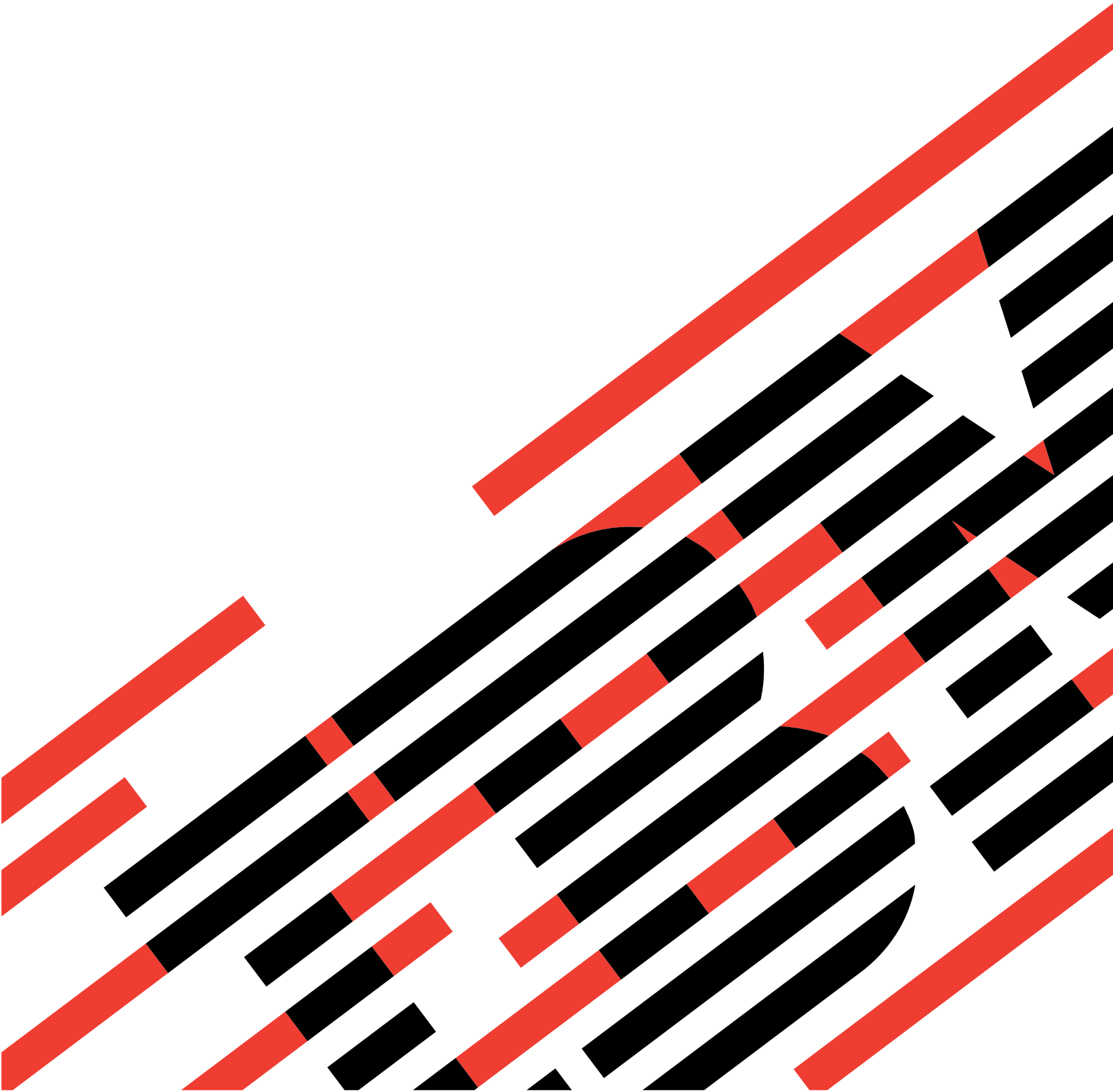
IBM

eserver

iSeries

네트워크 시나리오

버전 5 릴리스 3



IBM

@server

iSeries

네트워크 시나리오

버전 5 릴리스 3

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 55 페이지의 『주의사항』의 정보를 읽으십시오.

제 2 판(2005년 8월)

이 개정판은 새 개정판에서 별도로 명시하지 않는 한 IBM Operating System/400®(제품 번호 5722-SS1)및 후속 릴리스와 수정에 적용됩니다.

목차

제 1 장 네트워크 시나리오

네트워크 주제는 다양한 주제를 포함하고 있습니다. 이 주제의 목적은 기본 네트워킹 정보를 제공하는 것이 아니라 특정 네트워킹 환경에서 사용된 iSeries™ 기술의 예를 제공하기 위한 것입니다. 다음 시나리오에서는 iSeries 서버에서 사용 가능한 네트워킹 서비스와 어플리케이션을 활용하는 방법을 보여줍니다. 일부 기본 고려사항을 읽으려면 네트워크 계획 작업 용지를 참조하십시오.

이 주제 인쇄
이 페이지는 이 정보의 PDF 버전을 다운로드하고 인쇄하는 방법에 대한 지침을 제공합니다.

시나리오: LAN과 통신하기 위해 iSeries 서버 설정
사용자는 네트워크 관리자로서 근거리 통신망(LAN)에 새 iSeries 서버를 추가하려고 합니다. 이 시나리오에서는 네트워크 관리자에게 전제조건 정보뿐만 아니라 LAN과 통신하기 위해 iSeries 서버를 설정하는 방법에 대한 지침을 제공합니다.

시나리오: 리모트 연결 사용
회사에는 지점 영업소가 있으며, 이 곳의 몇몇 영업 담당자는 사용자의 iSeries 서버에 연결해야 합니다. 또한 다른 지역에 소재한 본사에도 연결해야 합니다. 본사와 지점 영업소 간에 전송되는 정보는 매우 중요하므로 사용자에게는 인터넷을 통해 정보를 전송할 때 이를 보호하는 문제가 관건입니다. 이 시나리오를 사용하여 리모트 클라이언트와 서버에 대한 연결을 구성하십시오.

시나리오: 파티션 간 통신을 위한 가상 이더넷 작성
사용자는 규모가 작은 회사의 시스템 관리자입니다. 네 개의 논리 파티션으로 나누어진 서버를 사용하고 있습니다. 사용자는 네 개의 논리 파티션 모두의 통신을 허용해야 합니다. 사용자는 IT 부서의 자금과 공간이 제한되어 있기 때문에 과도한 이더넷 카드와 케이블 구매를 피하고 싶어합니다.

시나리오: L2TP를 사용하여 논리 파티션 간 모뎀 공유
네 개의 논리 파티션에 걸쳐 설정된 가상 이더넷이 있습니다. 이 시나리오를 사용하여 선택한 논리 파티션이 모뎀을 공유하도록 할 수 있습니다. 이러한 논리 파티션은 외부 LAN에 액세스하기 위해 공유된 모뎀을 사용합니다.

제 2 장 V5R3의 새로운 사항

네트워크 시나리오는 자신이 관리하는 네트워크에서 공통 TCP/IP 기술을 사용하는 데 관심 있는 네트워크 관리자를 위한 시작 지점을 제공합니다. 각 시나리오는 전체 타스크를 제공하며, Information Center 내의 추가 정보와 자원을 가리킵니다. 다음 시나리오는 네트워크 환경에서 유사한 네트워크 토폴로지를 설계하고 구현하는 데 도움을 줄 수 있습니다.

새 네트워크 시나리오

- 시나리오: LAN과 통신하기 위해 iSeries 서버 설정
- 시나리오: 리모트 연결 사용
- 시나리오: 파티션 간 통신을 위한 가상 이더넷 작성
- 시나리오: L2TP를 사용하여 논리 파티션에 걸쳐 모뎀 공유

이 릴리스의 새로운 사항이나 변경된 사항에 대한 다른 정보를 찾으려면 사용자 메모를 참조하십시오.

제 3 장 이 주제 인쇄

이 문서의 PDF 버전을 보거나 다운로드하려면 네트워크 시나리오(약 242KB)를 선택하십시오.

다음과 같은 관련 주제를 보거나 다운로드할 수 있습니다.

- TCP/IP 설정(45KB)에는 다음 주제가 들어 있습니다.
  - Internet Protocol 버전 6(IPv6)
  - TCP/IP 설정 계획
  - TCP/IP 설치
  - TCP/IP 구성
  - TCP/IP 사용자 정의
  - 가상 이더넷상의 TCP/IP 기술
- 리모트 액세스 서비스(277KB)에는 다음 주제가 들어 있습니다.
  - PPP 시나리오
  - PPP 개념
  - PPP 계획
  - PPP 구성
  - PPP 관리
  - PPP 문제 해결
- VPN(가상 사설망)(509KB)에는 다음 주제가 들어 있습니다.
  - VPN 시나리오
  - VPN 개념
  - VPN 계획
  - VPN 구성
  - VPN 관리
  - VPN 문제 해결
- TCP/IP 문제 해결(235KB)에는 다음 정보가 들어 있습니다.
  - 대화식 문제 해결사
  - 도구 및 기술 문제 해결
  - 특정 어플리케이션과 관련된 문제 해결

PDF 파일 저장

보거나 인쇄를 위해 워크스테이션에 PDF를 저장하려면 다음을 수행하십시오.

- 브라우저에서 PDF를 마우스 오른쪽 버튼으로 클릭하십시오(위의 링크를 마우스 오른쪽 버튼으로 클릭).
- Internet Explorer를 사용하는 경우에는 **다른 이름으로 대상 저장...**을 클릭하십시오. Netscape Communicator를 사용하는 경우에는 **다른 이름으로 링크 저장...**을 클릭하십시오.
- PDF를 저장할 디렉토리로 이동하십시오.
- **저장**을 클릭하십시오.

Adobe Acrobat Reader 다운로드

이러한 PDF를 보거나 인쇄하려면 Adobe Acrobat Reader가 필요합니다. Adobe 웹 사이트 (www.adobe.com/products/acrobat/readstep.html)  에서 사본을 다운로드할 수 있습니다.

제 4 장 네트워크 계획 작업

이 작업 용지를 네트워크 계획 연구의 보충 자료로 사용하십시오. 각 시나리오에는 네트워크 환경에 대해 작성된 전제조건과 가정이 표시된 표와 유사한 정보를 포함하고 있습니다. 아래 표는 모든 환경에 대한 전체 네트워크 설계를 다루지는 않지만 사용자 고유의 환경에 대해 고려할 수 있는 기초를 제공합니다. 예를 들어, 이러한 시나리오를 사용하기 전에 사용자는 서버 가용성, 성능, 기능 등에 대해 계획해야 합니다.

보다 자세한 고려사항을 검토하려면 하드웨어 및 소프트웨어 계획: 전체 계획 체크 리스트 보기를 참조하십시오회사에서 필요로 하는 어플리케이션과 네트워킹 솔루션은 비즈니스 목적에 따라 다를 수 있습니다.

서버 작업	회사 응답
서버 모델을 기록하십시오.	
오퍼레이팅 시스템 버전을 기록하십시오.	
논리 파티션 환경을 이해하고 문서화하십시오.	
iSeries 서버에 연결해야 하는 클라이언트를 판별합니다.	
설치된 통신 어댑터 유형을 기록하십시오. 이더넷, 토큰링 등에 대한 자세한 정보는 네트워크 통신을 참조하십시오.	
통신 자원명을 기록하십시오.	
iSeries 서버의 IP 주소를 기록하십시오.	
iSeries 서버의 서브네트 마스크를 기록하십시오.	
게이트웨이 주소를 기록하십시오.	
호스트명과 정의역명을 기록하십시오.	
정의역명 서버의 IP 주소를 기록하십시오.	

네트워크 작업	회사 응답
명확한 네트워크 목표를 수립하십시오.	
사용자는 누구이며 요구사항은 무엇입니까?	
이러한 요구사항을 지원하는 어플리케이션은 무엇입니까?	
어플리케이션의 예상 성능은 무엇입니까?	
필요한 프로토콜은 무엇입니까? 상호운영성을 고려하십시오. 대부분의 네트워크는 TCP/IP를 사용하지만 또 다른 대안도 있습니다. 자세한 내용은 네트워크 통신을 참조하십시오.	
일부 어플리케이션의 경우 다른 어플리케이션보다 상위 우선순위가 필요합니까?	
어플리케이션이 지연이나 패킷 유실에 민감합니까?	
특정 보안 요구사항이 있는 어플리케이션은 무엇입니까? 보안 계획은 네트워크 계획과 통합되어야 합니다. 네트워크 보안 계획에 대한 자원은 eServer security planner를 참조하십시오.	
네트워크의 성장 가능성 및 발전 속도에 대해 고려하였습니까? 기본 네트워크 구조에서 반드시 보안을 고려해야 합니다.	
LAN에 사용되어야 하는 기술은 무엇입니까?	
네트워크에 연결되는 기타 장치에는 무엇이 있습니까?	
네트워크의 구조를 계획해보십시오.	

제 5 장 시나리오: LAN과 통신하기 위해 iSeries 설정

상황

사용자는 Sampson Organic Produce라는 작은 도매 회사의 네트워크 관리자입니다. 이 회사의 고객은 유기 농법으로 지은 고품질 농산물을 원하는 지역 식품점과 개별 가정입니다. 비즈니스는 나날이 성장하고 있으며 최근에는 재고 관리를 효율적으로 하기 위해 새 iSeries 서버를 구입했습니다. 과거에는 자원과 키 비즈니스 어플리케이션을 개별 워크스테이션에 저장했습니다. 하지만, 비즈니스가 변화함에 따라 이러한 어플리케이션에 있는 데이터를 보다 쉽게 공유해야 할 필요가 생겨났습니다. 예를 들어, 전화 주문을 받은 직원은 제품 가용성을 판별하기 위해 보다 빠르게 재고를 확인해야 합니다. 과거에는 고객이 기다리는 동안 재고 데이터베이스에 액세스할 수 있는 권한이 있는 직원이 재고를 확인했습니다.

이제는 이러한 키 비즈니스 어플리케이션을 새 서버에 모두 통합할 계획입니다. 이미 새 서버에 필요한 하드웨어 계획과 설정 타스크를 모두 완료했습니다. 통신 및 네트워킹을 조사했고 이더넷 근거리 통신망(LAN)을 사용하기로 결정했습니다.

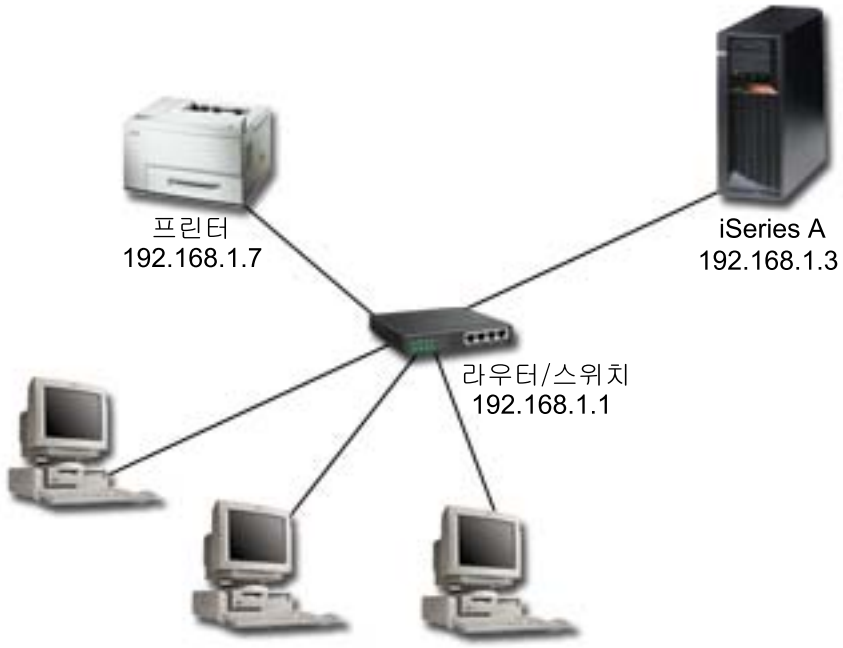
목적

LAN에 서버를 추가한 후 다음 사항을 완료하려고 합니다.

- LAN 사용을 위한 iSeries 설정.
- LAN에 있는 프린터 설정.
- 서버에 저장된 데이터의 보호 보장.
- 다른 호스트와 통신하기 위해 TCP/IP 서비스 찾기.

세부사항

다음 그림은 라우터에 연결된 iSeries 서버를 보여 줍니다. Sampson Organic Produce라는 소규모의 가상 회사의 네트워크를 묘사하고 있는 이 그림에서 세 개의 워크스테이션과 프린터가 라우터에 연결되어 있습니다.



- iSeries A는 OS/400® 버전 5 릴리스 2(V5R2)에서 실행되며 모든 관련 비즈니스 어플리케이션을 포함합니다.
- iSeries A IP: 192.168.1.3
- iSeries A 서브네트 마스크: 255.255.255.128
- 워크스테이션 1 IP: 192.168.1.4
- 워크스테이션 2 IP: 192.168.1.5
- 워크스테이션 3 IP: 192.168.1.6
- 프린터 IP: 192.168.1.7
- 라우터 IP: 192.168.1.1

주: 외부 네트워크 연결 계획이 없는 경우에는 라우터/스위치 대신에 허브를 사용할 수 있습니다.

전제조건 및 가정

이 시나리오는 이 네트워크 환경에서 다음 전제조건이 충족되었다고 가정합니다.

- 네트워크에서 모든 케이블 연결 및 하드웨어 설치가 완료되었습니다.
- 라우터를 사용하는 경우 라우터가 구성되었습니다. 허브나 스위치는 구성할 수 없습니다.

구성 단계

다음 타스크를 완료하십시오. 각 단계를 마치면 다음 타스크로 연결되는 링크가 있습니다.

1. 계획 작업 용지 검토
2. TCP/IP 설정

3. TCP/IP 테스트
4. LAN에서 프린터 구성(선택사항)
5. 네트워크 연결 테스트
6. 시스템 보안 권장사항 구현
7. TCP/IP 어플리케이션, 프로토콜 및 서비스 탐색

시나리오 세부사항: LAN과 통신하기 위해 iSeries 설정

다음 단계는 네트워크 관리자가 가상 회사 Sampson Organic Produce의 기존 LAN과 통신하기 위해 iSeries 서버를 구성하는 방법을 보여 줍니다. 이러한 타스크를 완료하기 전에 네트워크 관리자는 필요한 전제조건을 완료해야 합니다.

1단계: 계획 작업 용지 검토

계획을 세운 후에 네트워크 관리자는 이 시나리오에서 제시된 타스크에 직접 영향을 미치는 다음 질문에 대답했습니다. 사용자 고유의 작업 용지를 작성하기 위한 공백 표의 경우 네트워크 계획 작업 용지를 검토하십시오.

서버 작업	회사 응답
서버 용량을 기록하십시오.	모델 820
오퍼레이팅 시스템 또는 시스템들을 기록하십시오.	OS/400
현재 논리 파티션 환경을 이해하고 문서화하십시오.	논리 파티션 없음
iSeries에 연결해야 하는 클라이언트를 판별합니다.	iSeries Navigator를 포함하고 있는 IBM @server, iSeries Access for Windows®
설치된 통신 어댑터 유형을 기록하십시오.	이더넷
통신 자원명을 기록하십시오.	cmn01
iSeries 서버의 IP 주소를 기록하십시오.	192.168.1.3
iSeries 서버의 서브네트 마스크를 기록하십시오.	255.255.255.128
게이트웨이 주소를 기록하십시오.	192.168.1.1
호스트명과 정의역명을 기록하십시오.	iseriesa.sampson.com
정의역명 서버의 IP 주소를 기록하십시오.	LAN이 다른 네트워크에 연결되지 않았기 때문에 DNS는 필요하지 않습니다. 회사는 네트워크상의 모든 시스템에 호스트 테이블 항목을 추가했습니다.

네트워크 가정	회사 결정
사용자는 누구이며 요구사항은 무엇입니까?	고객의 주문을 접수하는 세 개의 영역.
이러한 요구사항을 지원하는 어플리케이션은 무엇입니까?	웹 기반이 아닌 사내 주문 어플리케이션.

네트워크 가정	회사 결정
필요한 프로토콜은 무엇입니까? 상호운영성을 고려하십시오.	TCP/IP
어플리케이션이 지연이나 패킷 유실에 민감합니까?	아니오
어플리케이션에 특정 보안 고려사항이 필요합니까?	기본 시스템 보안. 세부사항은 시나리오에 통합되어 있습니다.
네트워크의 성장 가능성 및 발전 속도에 대해 고려하였습니까? 기본 네트워크 구조에서 반드시 보안을 고려해야 합니다.	예. 잘 모름.
네트워크에 연결되는 다른 장치는 무엇입니까?	프린터--IBM Infoprint® 40
네트워크의 구조를 계획해보십시오.	시나리오 다이어그램을 참조하십시오.

2단계: TCP/IP 설정

네트워크 계획 작업을 완료한 후에는 iSeries 시스템에서 TCP/IP를 설정해야 합니다.

네트워크에서 TCP/IP를 설정하려면 다음 단계를 수행하십시오.

1. **TCP/IP 연결 및 유틸리티 사용권 프로그램 설치**
   a. TCP/IP의 설치 매체를 서버에 삽입하십시오. 서버는 설치 매체로 CD-ROM 장치를 사용합니다.
   b. 명령행에서 GO LICPGM을 입력하고 Enter를 눌러 사용권 프로그램에 대한 작업 표시 화면에 액세스하십시오.
   c. 사용권 프로그램에 대한 작업 표시 화면에서 옵션 11(사용권 프로그램 설치)을 선택하여 사용권 프로그램의 목록과 사용권 프로그램의 선택 기능에 대해 보십시오.
   d. 57xxTC1(iSeries용 TCP/IP 연결 유틸리티)과 57xxCM1(통신 유틸리티) 및 57xxXE1(Windows용 iSeries Access) 다음에 있는 옵션 컬럼에 1(설치)을 입력하십시오. Enter를 누르십시오. 설치할 사용권 프로그램 확인 표시 화면에 설치를 위해 선택한 사용권 프로그램이 표시됩니다.
   e. Enter를 눌러 확인하십시오.
   f. 네트워크 관리자는 선택한 설치 옵션이 표시됩니다.
      - 설치 장치: QOPT (CD-ROM 장치에서 설치할 때 사용합니다.)
      - 설치할 오브젝트: 프로그램과 언어 오브젝트 모두 설치합니다.
      - 자동 재시작: 예(설치를 완료한 후 시스템이 자동으로 재시작하도록 할지 여부를 판별합니다.)

      TCP/IP 연결 유틸리티가 제대로 설치되면 사용권 프로그램에 대한 작업 메뉴나 사인 온 표시 화면이 나타납니다.
   g. 사용권 프로그램이 제대로 설치되었는지 확인하려면 옵션 50(메세지의 기록부 표시)을 선택하십시오.
2. **TCP/IP 구성**
   a. 명령행에서 WRKHDWRSC *CMN을 입력하여 통신 자원에 대한 작업 메뉴를 표시하십시오.
   b. 이더넷 포트의 통신 자원 옆에 5를 입력하고 Enter를 누르십시오.
   c. 통신 설명에 대한 작업 메뉴에서 1을 입력하고 Enter를 누르십시오.
   d. 회선 설명 작성(이더넷) (CRTLINETH) 메뉴가 나타납니다.

e. 회선 설명 필드에 회선 설명을 입력하십시오. 이 예에서 네트워크 관리자는 Eth01을 선택했습니다.

f. 회선 속도와 양방향 전송 필드에 정확한 정보를 입력하십시오. 이러한 값은 iSeries에 연결하는 스위치 상의 포트와 일치해야 합니다. 이 예제에서는, 100M 및 *HALF를 각각 입력했습니다. Enter를 누르십시오.

g. F10을 눌러 추가 매개변수를 보십시오. 매개변수를 보려면 PaDn을 누르십시오.

h. 링크 속도 필드가 이전에 입력한 회선 속도와 일치하도록 변경하십시오(예: 100M).

i. 다른 디폴트 값을 모두 승인하고 Enter를 누르십시오.

j. F3을 눌러 통신 자원에 대한 작업 메뉴로 돌아가십시오.

k. F3을 다시 한 번 눌러 명령 입력 메뉴로 돌아가십시오.

l. 명령행에서 CFGTCP를 입력하여 TCP/IP 구성 메뉴를 표시하십시오.

m. TCP/IP 구성 메뉴에서 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하십시오.

n. 옵션 1(추가)를 선택하여 TCP/IP 인터페이스 추가 표시 화면을 표시하고 Enter를 누르십시오.

o. 다음 값을 입력하여 새 TCP/IP 인터페이스를 작성하고 Enter를 누르십시오.

   - 인터넷 주소: 192.168.1.3
   - 회선 설명: Eth01
   - 서브네트 마스크: 255.255.255.128

   주: 이러한 주소는 예제 목적으로만 사용됩니다. 사용자는 사용자 고유의 네트워크와 관련된 값을 입력해야 합니다.

p. F3을 눌러 TCP/IP 구성 메뉴로 돌아가십시오.

q. TCP/IP 구성 메뉴에서 옵션 2(TCP/IP 라우트에 대한 작업)를 선택하십시오.

r. 옵션 1(추가)을 선택하여 TCP/IP 라우트 추가(ADDTCPRTE) 표시 화면으로 이동하고 Enter를 누르십시오.

s. 다음 값을 입력하여 라우트를 작성하고 Enter를 누르십시오.

   - 라우트 목적지: *DFTROUTE
   - 서브네트 마스크: *NONE
   - 다음 홉(hop): 192.168.1.1

   주: 다른 네트워크에 연결되지 않은 경우에는 이 라우트는 필요하지 않습니다. 여기에서는 회사가 추후 인터넷에 연결할 계획을 가정하여 추가되었습니다.

t. TCP/IP 구성 메뉴에서 옵션 10(TCP/IP 호스트 표 항목에 대한 작업)을 선택하고 Enter를 누르십시오.

u. 옵션 1(추가)을 선택하여 TCP/IP 호스트 표 항목 추가 표시 화면으로 이동하고 Enter를 누르십시오.

v. 다음 값을 입력하여 새 호스트 표 항목을 추가하고 Enter를 누르십시오.

   - IP 주소: 192.168.1.3
   - 호스트명: iseriesa.sampson.com
   - 이름: iseriesa

w. 네트워크상의 각 시스템에 대해 위의 단계를 반복하십시오. 정의역명 서버(DNS)에서 서버가 구성되지 않았으므로 각 시스템에는 호스트 표 항목이 있어야 합니다. 예를 들어, iSeries A가 워크스테이션 1(192.168.1.4/wstn1)과 통신할 수 있으려면 **IP 주소**: 192.168.1.4, **호스트명**: wstn1.sampson.com 및 **이름**: wstn1과 같은 추가 호스트 표 항목을 추가하십시오. 이것이 네트워크 환경의 현실에 맞지 않으면 DNS 구성에 대한 정보는 Information Center의 DNS 주제를 참조하십시오.

x. 명령행에서 STRTCP를 입력하여 TCP/IP를 시작하십시오. 그러면 인터페이스와 회선도 함께 시작됩니다.

3단계: TCP/IP 테스트

TCP/IP 연결 및 유틸리티 사용권 프로그램을 설치하고 iSeries 시스템에 TCP/IP를 구성한 후에는 TCP/IP 연결을 테스트해야 합니다.

네트워크에서 TCP/IP 연결을 테스트하려면 다음을 수행하십시오.

1. TCP/IP 통신이 구성되었고 각 워크스테이션에서 시작되었는지 확인하십시오. 워크스테이션 공급자가 제공한 문서를 사용하십시오.
2. 워크스테이션 1에서 명령 프롬트를 열고 PING 192.168.1.3을 입력하십시오. 패킷이 iSeries A에 송신되었음을 확인하는 메세지를 수신합니다. 이는 워크스테이션이 서버에 액세스할 수 있음을 의미합니다.

4단계: 사용자 워크스테이션에서 Windows용 iSeries Access 설치 및 구성

사용권 프로그램(LP)을 설치하는 동안 Sampson Organic Produce는 서버에 Windows용 iSeries Access의 LP를 설치했습니다. iSeries Navigator(Windows용 iSeries Access의 구성요소)를 사용하려면 또한 PC에 클라이언트를 설치해야 합니다. 자세한 내용은 Windows용 iSeries Access 지침을 참조하십시오. iSeries Navigator가 작동 중이면 7단계를 수행할 수 있습니다.

5단계: LAN에서 프린터 구성

또한 사용자가 오피스 LAN에 연결된 공통 프린터를 공유할 수 있도록 허용하여 인쇄 서비스를 제공해야 합니다. 네트워크에 있는 프린터는 SNMP(Simple Network Management Protocol)와 호환 가능합니다. iSeries 시스템을 인쇄 서버로 사용하여 인쇄 작업을 관리하고 이를 LAN에 있는 이 프린터로 송신합니다. 이 프린터는 네트워크 어댑터로 LAN에 연결되어 있습니다.

주: 이 단계는 선택적 단계로 사용자 고유의 네트워크 설정에는 적합하지 않을 수 있습니다.

iSeries 서버를 인쇄 작업을 관리하는 인쇄 서버로 설정하려면 다음 단계를 수행하십시오.

1. **프린터 구성**
   a. 모든 케이블 연결이 완료되었는지 확인하십시오.
   b. 프린터의 지침 매뉴얼을 사용하여 프린터가 설치되었는지 확인하십시오.
   c. 프린터의 제어판에서 포트 시간종료를 300(5분)으로 설정하십시오. 이 타이머는 프린터가 페이지 인쇄 명령으로 종료되지 않는 마지막 페이지를 인쇄하기 전에 대기하는 시간을 초 단위로(5-300) 제어합니다.

2. **프린터 장치 설명 작성**

   a. 문자 기반 인터페이스에서 CRTDEVPRT를 입력하여 프린터 장치 설명을 작성하십시오. 프린터 장치 설명은 프린터가 LAN에 직접 연결될 때 작성되어야 합니다.

   b. 장치 설명 작성(프린터) 표시 화면에서 다음을 입력하십시오.

      주: 모든 매개변수를 보려면 F10 및 Enter를 눌러야 합니다. 아래에 나열되지 않은 표시 화면에 표시된 모든 매개변수의 디폴트 값을 승인할 수 있습니다. 각 매개변수의 자세한 설명은 iSeries Information Center에서 CL command finder를 참조하십시오. CRTDEVPRT 명령을 이름으로 검색하고 장치 설명 작성(프린터) 명령을 선택하십시오. 이러한 설명을 사용하면 특정 상황에서 최선의 선택을 할 수 있습니다.

      1) 장치 설명: PRINTER1
      2) 장치 클래스: *LAN
      3) 장치 유형: 3812
      4) 장치 모델: 1
      5) LAN 연결: *IP
      6) 포트 번호: 2501
      7) 용지 넘김: *AUTOCUT
      8) 프린터 오류 메세지: *INFO
      9) 제조업체 유형 및 모델: *IBM4340
      10) 용지 소스 1: *LETTER
      11) 용지 소스 2: *LETTER
      12) 봉투 소스: *NONE
      13) 이름 또는 주소: 192.168.1.7
      14) 사용자 정의 옵션: *IBMSHRCNN
      15) 시스템 드라이버 프로그램: *IBMSNMPDRV
      16) 텍스트 설명: IBM IP40의 *LAN 3812 SNMP 장치 설명

   c. 이러한 필드를 완료한 후 Enter를 누르십시오.

   d. 명령행에서 VRYCFG를 입력하여 PRINTER1의 구성을 연결변환하십시오.

   e. 구성 변환(VRYCFG) 표시 화면에서 다음을 입력하십시오.

      1) 구성 오브젝트: PRINTER1
      2) 유형: *DEV
      3) 상태: *ON

   f. 이러한 필드를 완료한 후 Enter를 누르십시오.

   g. 명령행에서 STRPRTWTR를 입력하여 프린터 출력기를 시작하십시오.

h. 프린터 출력기 시작(STRPRTWTR) 표시 화면에서 프린터 필드에 PRINTER1을 입력하십시오. Enter를 누르십시오.

3. **프린터 연결 테스트**
   a. 프린터가 켜져 있고 준비 상태인지 확인하십시오.
   b. WRKWTR(모든 프린터 명령 작동)을 입력하여 프린터 장치 상태가 STR인지 확인하십시오.
   c. PING "192.168.1.7"을 입력하여 iSeries A가 프린터와 통신할 수 있는지 확인하십시오. 시스템이 프린터에 연결되었음이 표시됩니다.

6단계: 네트워크 연결 테스트

네트워크의 프린터 구성을 완료한 후에는 네트워크의 모든 연결을 테스트해야 합니다.

네트워크에서 모든 연결을 테스트하려면 다음을 완료하십시오.

1. 명령행에서 Ping "xx.xx.xx.xx"를 입력하십시오. 여기서 *xx.xx.xx.xx*는 각 워크스테이션과 프린터의 IP 주소입니다.
2. 각 워크스테이션의 명령 프롬트에 Ping "xx.xx.xx.xx"를 입력하십시오. 여기서 *xx.xx.xx.xx*는 iSeries 서버와 프린터의 IP 주소입니다.
   주: 각 워크스테이션에서 새 프린터를 구성하고 각 호스트 표에 프린터 IP 주소를 추가해야 합니다.

테스트 페이지를 인쇄하려면 다음 지침을 사용하여 iSeries A의 작업 기록부를 인쇄하십시오.

1. iSeries Navigator에서 **기본 조작 -> 프린터 출력**을 선택하십시오.
2. 오른쪽 분할 창에서 출력명을 마우스 오른쪽 버튼으로 클릭하고 **열기**를 선택하여 출력을 보십시오.
3. 표시기에서 **파일 --> 인쇄**를 선택하십시오.
4. 인쇄 옵션을 선택하고 **인쇄**를 클릭하십시오. 이 페이지는 프린터로 송신되어야 합니다.

이러한 연결이 작동하지 않으면 Sampson Organic의 네트워크 관리자는 문제를 찾기 위해 TCP/IP 문제 해결을 사용하게 됩니다.

7단계: 시스템 보안 권장사항 구현

iSeries 서버에 저장된 자산을 보호하기 위해, Sampson Organic Produce는 시스템 환경을 기반으로 권장사항의 동적 세트를 작성하는 대화식 계획 도구인 IBM® @server Security Planner를 사용했습니다. 이 도구에 액세스하려면 IBM @server Security Planner를 참조하십시오.Sampson Organic Produce의 관리자가 Security Planner에서 보안 설정 구현을 위해 예로 생성했던 보안 권장사항을 사용할 수 있습니다.

iSeries A에서 보안을 구현하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries A**를 차례로 선택하십시오. **보안**을 마우스 오른쪽 버튼으로 클릭한 다음 **구성**을 선택하십시오.
2. **시작** 페이지에서 **다음**을 클릭하십시오.
3. 일반 보안 정책을 설명하려면 **평균**을 선택하십시오. **다음**을 클릭하십시오.

4. 서버를 사용할 방법을 설명하려면 **비즈니스 어플리케이션 실행**을 선택하십시오. **다음**을 클릭하십시오.
5. **아니오**를 선택하고 **다음**을 클릭하십시오.
6. APPC 사용에 대해 **아니오**를 선택하고 **다음**을 클릭하십시오.
7. TCP/IP를 사용 중임을 나타내려면 **예**를 선택하고 **다음**을 클릭하십시오.
8. 인터넷에 연결되지 않았음을 나타내려면 **예**를 선택하고 **다음**을 클릭하십시오.
9. **아니오**를 선택하고 **다음**을 클릭하십시오.
10. IBM iSeries NetServer를 사용 중이 아님을 나타내려면 **아니오**를 선택하십시오. **다음**을 클릭하십시오.
11. **아니오**를 선택하고 **다음**을 클릭하십시오.
12. **아니오**를 선택하고 **다음**을 클릭하십시오.
13. 서버에서 보안 관련 조치를 감사하려면 **예**를 선택하십시오. **다음**을 클릭하십시오.
14. 시스템에서 보안을 모니터하기 위해 보고서를 예약하려면 **예**를 선택하십시오. **다음**을 클릭하십시오.
15. 이러한 보고서를 예약하려면 **한 달에 한 번**을 선택하십시오. **다음**을 클릭하십시오.
16. 보안 권장사항을 검토하려면 **세부사항...**을 클릭하십시오. 해당 보안 제어를 선택 취소하여 보안 값을 변경할 수 있습니다. **확인**을 클릭하십시오. **다음**을 클릭하십시오.
17. 관리자와 사용자 정보 보고서를 저장할 디렉토리를 지정하십시오. **다음**을 클릭하십시오. 이러한 각 보고서를 검토할 수 있습니다.
18. **다음**을 다시 클릭하십시오.
19. **예, 지금 변경합니다.**를 선택하고 **완료**를 클릭하십시오. 이제 iSeries A에서 보안 구성을 완료했습니다.

8단계: TCP/IP 서비스, 어플리케이션 및 프로토콜 탐색

Sampson Organic Produce가 미래에 구현할 수 있는 다른 TCP/IP 서비스가 많이 있습니다. 가장 일반적인 유틸리티는 텔넷 및 FTP입니다. 또한, 더 많은 정보를 인쇄하려고 할 수 있습니다. TCP/IP 어플리케이션, 프로토콜 및 서비스에 대해 추가로 탐색하려면 다음 링크를 사용하십시오.

- TCP/IP 어플리케이션, 프로토콜 및 서비스
- 인쇄

주: iSeries Navigator의 추가 기능을 탐색할 수도 있습니다.

보안 권장사항

다음 권장사항은 Sampson Organic Produce Company의 IBM @server Security Planner로 생성되었습니다. 이러한 세부사항을 검토하려면 IBM @server Security Planner를 완료하십시오.

주: 다음 권장사항은 보안 값의 전체 설명과 이러한 시스템 값의 작동 고려사항을 포함하지 않습니다. 보안 참조 매뉴얼의 제 3장, "보안 시스템 값"이나 Information Center의 OS/400 시스템 값 파인더를 사용하여 특정 시스템 값과 그 옵션에 대한 자세한 내용을 볼 수 있습니다.

표 1. 일반 보안 권장사항

시스템 값	권장 값
QSECURITY	40
QINACTITV	60
QINACTMSGQ	*DSCJOB
QDSCJOBITV	240
QSHRMEMCTL	1 (Yes)
QRETSVRSEC	1 (Yes)
QRMTSRVATR	0(아니오)
QRMTIPL	*NONE

표 2. 암호 정책 권장사항

시스템 값	권장 값
QPWDLVL	0
QPWDEXPITV	90
QPWDMINLEN	8
QPWDRQDDIF	8
QPWDLMTCHR	*NONE
QPWDLMTAJC	0(허용)
QPWDLMTREP	0(문자 반복 가능)
QPWDPOSDIF	0(아니오)
QPWDRQDDGT	1 (Yes)
QPWDVLDPGM	*NONE

표 3. 사인 온 정책 권장사항

시스템 값	권장 값
QDSPSGNINF	1 (Yes)
QLMTDEVSSN	0(아니오)
QLMTSECOFR	1(예)
QMAXSIGN	3
QMAXSGNACN	2(사용자 프로파일 작동 불가능)
QRMTSIGN	*FRCSIGNON(항상 사인 온 표시)

표 4. 복원 정책 권장사항

시스템 값	권장 값
QALWOBJRST	*ALWPTF
QVFYOBJRST	3
QFRCCVNRST	3

표 5. 감사 정책 권장사항

시스템 값	권장 값
QAUDCTL	*AUDLVL,*OBJAUD, *NOQTEMP

표 5. 감사 정책 권장사항 (계속)

QAUDCTL	*NONE
주: 보고서 감사는 월별로 스케줄됩니다.	

제 6 장 시나리오: 리모트 연결 사용 가능

상황

사용자는 여러 모바일 영업 사원을 관리하는 지점 영업소의 네트워크 관리자입니다. 또한 다른 지역에 소재한 본사와도 함께 일합니다. 리모트 영업 담당자와 본사는 모두 사용자의 내부 네트워크에 액세스해야 합니다. 그러나 정보가 인터넷을 통해 전송될 때 보호하는 문제에 대해 염려하고 있습니다

본사에서는 고객 계정과 청구서와 같은 민감한 정보에 액세스해야 합니다. 모바일 영업 사원은 지점 영업소 간 프로토콜(PPP)을 통해 ISP에 전화 접속하여 지점 영업소에 정보를 전송합니다. 이들은 민감한 정보도 함께 전송하므로 이러한 통신에서 자료 무결성과 프라이버시를 보장해야 합니다. 민감한 신용 카드 번호와 고객 문의처 정보가 공용 인터넷에 노출되기를 바라지 않습니다. 두 사용자 그룹을 위한 옵션을 조사한 후에 리모트 직원을 위해 VPN(가상 사설망)을 사용하여 본사와의 연결을 보호하고 VPN으로 보호된 L2TP(Layer Two Tunnel Protocol)를 사용하도록 결정했습니다.

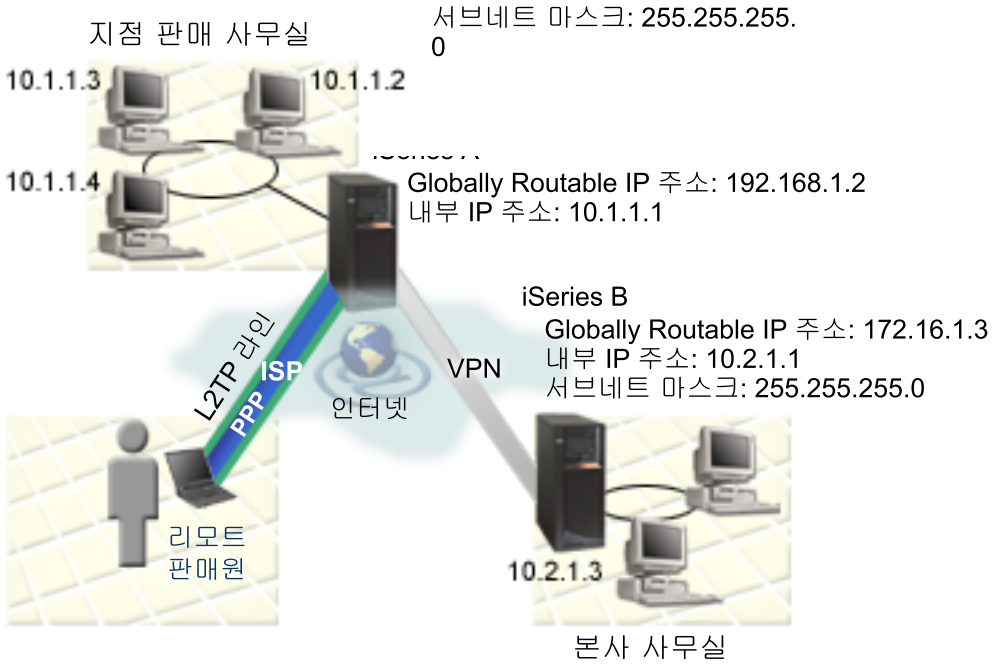
목적

MyCo, Inc의 관리자는 이 시나리오에서 다음과 같은 목적이 있습니다.

- 리모트 영업 사원과 본사에게 액세스 제공
- 이러한 목표를 지원하기 위해 기존 iSeries 서버 사용
- 리모트 영업 사원과 본사가 지점 영업소 네트워크에 액세스할 수 있도록 허용

세부사항

다음 네트워크 토폴로지는 지점 영업소와 본사 및 리모트 영업 담당자와의 연결을 보여 줍니다. 지점 영업소에 대한 연결은 VPN으로 보호되어 있습니다. 이 네트워크의 각 파트에 대한 다음 설명은 이러한 구성에 대한 세부사항을 제공합니다.



지점 영업소

- iSeries A는 OS/400 버전 5 릴리스 2(V5R2)에서 실행되며 모든 관련 비즈니스 어플리케이션을 포함합니다.
- iSeries A는 지점 영업소와의 VPN 연결을 위한 게이트웨이로 작동합니다.
- iSeries A의 IP 주소는 192.168.1.2이며 전체적으로 라우팅 가능합니다.

  주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
- 서브네트 마스크는 255.255.255.0입니다.
- iSeries A는 IP 주소 10.1.1.1을 사용하여 서브네트에 연결합니다.
- 지점 영업소의 내부 네트워크 내에서 모든 PC는 iSeries A를 가리키는 디폴트 라우트를 사용하여 구성되었습니다.
- iSeries A의 완전 규정 호스트명은 iseriesa.myco.min.com입니다.
- iSeries A 및 B 모두 연결을 시작할 수 있습니다.
- 리모트 직원은 범위가 10.1.1.100 - 10.1.1.150 사이인 IP 주소의 풀(pool)을 사용합니다.

본사

- iSeries B는 OS/400 버전 5 릴리스 2(V5R2)에서 실행되며 모든 관련 비즈니스 어플리케이션을 포함합니다.
- iSeries B는 본사와의 VPN 연결을 위한 게이트웨이로 작동합니다.
- iSeries B의 IP 주소는 172.16.1.3이며 전체적으로 라우팅 가능합니다.

주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.

- 서브네트 마스크는 255.255.255.0입니다.
- iSeries B는 IP 주소 10.2.1.1을 사용하여 서브네트에 연결합니다.
- 본사의 내부 네트워크 내에서 모든 PC는 iSeries B를 가리키는 디폴트 라우트를 사용하여 구성되었습니다.
- iSeries B의 완전 규정 호스트명은 iseriesb.myco.wis.com입니다.

리모트 영업 담당자

- Windows XP 오퍼레이팅 시스템이 있는 랩탑
- 리모트 직원은 범위가 10.1.1.100 - 10.1.1.150 사이인 IP 주소의 풀(pool)을 사용합니다.

전제조건 및 가정

이 시나리오는 지점 영업소와 본사 간의 VPN 구성의 예를 제공합니다. 또한 이동하는 영업 사원이 지점 영업소에 연결하기 위해 리모트 액세스를 구성하는 방법에 대한 지침을 제공합니다. 이 시나리오는 여러 전제조건 단계가 완료 및 테스트되었고 이러한 구성 단계를 시작하기 전에 작동가능한 것으로 가정합니다. 이 시나리오에서는 이러한 전제조건이 완료된 것으로 가정합니다.

1. 다음 사용권 프로그램이 설치되었는지 확인하십시오.
   - OS/400 버전 5 릴리스 2(5722-SS1)
   - 디지털 임증 관리자(5722-SS1 옵션 34)

     주: 이 시나리오는 DCM이 두 시스템 모두에 설치되었지만 둘 중 하나의 시스템에서는 아직 구성되지 않은 것으로 가정합니다.
   - 암호 액세스 제공자(5722-AC3)
   - OS/400용 TCP/IP 연결 유틸리티(5722-TC1)
   - iSeries용 IBM HTTP Server(5722-DG1)
   - Windows용 IBM @server iSeries Access(5722-XE1) 및 iSeries Navigator
   - IBM Developer Kit for Java™(5722-JV1)
   - 시스템에 최신 PTF가 설치되었는지 확인하십시오.
2. 다음 서버 설정이 완료되었는지 확인하십시오.
   - IP 인터페이스, 라우트, 로컬 호스트명 및 로컬 정의역명을 포함하여 TCP/IP를 구성해야 합니다.
   - 기본 시스템 보안이 구성 및 테스트되었습니다.
   - iSeries Navigator의 네트워크 구성요소가 설치되었습니다.
   - 보유 서버 보안 자료(QRETSVRSEC *SEC) 시스템 값이 1로 설정되었습니다.
   - 공유 메모리(QSHRMEMCTL) 시스템 값이 1로 설정되었습니다.
   - 필요한 엔드포인트 간에 정상 TCP/IP 통신이 설정되었습니다.

3. 리모트 직원이 사용하는 PC가 다음 요구사항을 충족하는지 확인하십시오.
   - Windows 32비트 오퍼레이팅 시스템이 있는 Windows XP 클라이언트가 iSeries 서버에 제대로 연결되어 있고 TCP/IP가 구성되어 있습니다.
   - 233Mhz 처리 장치.
   - Windows XP 클라이언트에는 64MB RAM이 있어야 합니다.
   - Windows용 iSeries Access 및 iSeries Navigator가 클라이언트 PC에 설치되었습니다.
   - 소프트웨어는 IP 보안(IPSec) 프로토콜을 지원해야 합니다.
   - 소프트웨어는 L2TP(Layer 2 Tunneling Protocol)를 지원해야 합니다.
   - ISP에 대한 연결이 설정되었습니다.

이러한 전제조건에 추가로, 두 네트워크가 모두 각 네트워크에 필터 규칙을 설정 및 활성화했고 라우팅을 구성했으며 IP 주소지정 체계를 설정한 것으로 가정합니다. 이러한 타스크를 완료하지 않은 경우 다음 주제를 참조하십시오.

- IP 필터링 및 네트워크 주소 변환(NAT)
- TCP/IP 라우팅 및 작업부하 균형

주: 이 시나리오는 인터넷에 직접 연결된 iSeries 보안 게이트웨이를 보여 줍니다. 방화벽이 없는 것은 시나리오를 단순화하기 위해서 입니다. 방화벽을 사용할 필요가 없음을 암시하는 것은 아닙니다. 실제로, 인터넷에 연결할 때 보안 관련 문제를 고려해야 합니다. 이러한 위험을 줄이는 여러 방법에 대한 자세한 설명은 이 레드북, AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00  를 참조하십시오.

구성 타스크

MyCo, Inc 지점 영업소에 대한 리모크 연결을 사용하려면 다음 타스크를 완료하십시오.

1. **디지털 인증 관리자를 사용하여 인증 기관(CA) 설정**
   a. DCM의 계획 작업 용지 완료
   b. iSeries A에서 iSeries용 IBM HTTP Server 시작
   c. iSeries A를 인증 기관(CA)으로 구성
   d. iSeries B에 대한 서버 인증서 작성
   e. iSeries B에서 .KDB 및 .RDB 이름 변경
   f. iSeries B에서 *SYSTEM 인증서 저장소 암호 변경
   g. iSeries B에서 OS/400 VPN 키 관리자에 대한 CA 신뢰 정의
2. **지점 영업소와 본사 간 VPN 연결 구성**
   a. 지점 영업소와 본사 간 VPN 연결을 위한 계획 작업 용지 완료
   b. iSeries A에서 VPN 구성
   c. iSeries B에서 VPN 구성

d. 두 서버 모두에서 필터 규칙 활성화

e. VPN 연결 시작

f. 엔드포인트 간 VPN 연결 테스트

3. **리모트 사용자에 대한 VPN 연결 구성**

a. 지점 영업소에서 리모트 영업 사원으로 VPN 연결을 위한 계획 작업 용지 완료

b. iSeries A에서 L2TP 종료 프로그램 구성

c. 리시버 연결 프로파일 시작

d. 리모트 클라이언트의 iSeries A에서 VPN 연결 구성

e. Windows XP 클라이언트에서 리모트 연결을 위한 VPN 정책 갱신

f. 필터 규칙 활성화

g. Windows XP 클라이언트에서 VPN 구성

h. 엔드포인트 간 연결 테스트

이 시나리오에 외에, 리모트 연결 설정을 위해 여러 개의 다른 시나리오도 사용할 수 있습니다. 이러한 기술 사용의 예를 추가로 보려면 Information Center의 다음 주제를 참조하십시오.

- DCM 시나리오
- VPN 시나리오
- PPP 시나리오

시나리오 세부사항: 리모트 연결 사용 가능

MyCo, Inc 회사는 지점 영업소와 본사 및 리모트 영업 담당자 간 데이터 전송을 보호하기 위해 VPN 연결을 사용하려고 합니다.

철저한 계획을 세운 후에, 지점 영업소의 관리자는 다음 타스크를 완료하여 본사와 리모트 직원 간 보안 연결을 설정했습니다. 적절한 설정을 위해 몇몇 계획 타스크는 반드시 완료해야 합니다. 이러한 타스크를 완료하기 전에 이 시나리오의 모든 전제조건이 완료되었는지 확인하십시오.

1. 디지털 인증 관리자(DCM)를 사용하여 인증 기관(CA) 설정
2. 지점 영업소와 본사 간 VPN 연결 구성
3. 리모트 사용자에 대한 VPN 연결 구성

디지털 인증 관리자를 사용하여 인증 기관(CA) 설정

인증 기관(CA)을 설정하기 전에 지점 영업소의 관리자는 여러 계획 타스크가 완료되었는지 확인해야 합니다. 이러한 타스크를 완료하기 전에 이 시나리오의 모든 전제조건이 완료되었는지 확인하십시오.

1단계: DCM의 계획 작업 용지 완료

철저한 계획을 세운 후에, MyCo, Inc는 비즈니스 파트너에서 발행할 디지털 인증서를 설정하기 위해 다음 작업에 대한 계획을 완료했습니다.

표 6. 디지털 인증 관리자(DCM)를 사용하여 인증 기관(CA)을 작성하기 위한 계획 작업 용지

질문	응답
인증서의 공용 및 개인용 키를 생성하기 위해 사용할 키 크기는 무엇입니까?	1024
인증서 저장소 암호는 무엇입니까?	secret **주:** 이 시나리오에서 사용된 모든 암호는 예제 목적으로만 사용됩니다. 이러한 암호를 실제 구성에서 사용하지 마십시오.
인증 기관 이름은 무엇입니까?	mycoca
조직 이름은 무엇입니까?	myco
인증의 유효 기간은 무엇입니까?	1095(3년)
사용하는 브라우저는 무엇입니까?	Windows용 Internet Explorer 버전 6.0
이 인증서를 네트워크상의 사용자에게 발행하겠습니까?	아니오

표 7. iSeries A의 서버 인증을 위한 계획 작업 용지

질문	응답
인증서의 공용 및 개인용 키를 생성하기 위해 사용할 키 크기는 무엇입니까?	1024
인증서 저장소 암호는 무엇입니까?	secret **주:** 이 시나리오에서 사용된 모든 암호는 예제 목적으로만 사용됩니다. 이러한 암호를 실제 구성에서 사용하지 마십시오.
인증서 레이블 이름은 무엇입니까?	mycocert
인증서의 공통 이름은 무엇입니까?	mycocert
조직 이름은 무엇입니까?	MyCo, Inc
iSeries 서버의 IP 주소는 무엇입니까?	192.168.1.2 **주:** 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
iSeries 서버의 완전 규정 호스트명은 무엇입니까?	iseriesa.myco.min.com

표 8. iSeries B의 서버 인증을 위한 계획 작업 용지

질문	응답
인증서의 공용 및 개인용 키를 생성하기 위해 사용할 키 크기는 무엇입니까?	1024
인증서 레이블 이름은 무엇입니까?	corporatecert
인증서의 공통 이름은 무엇입니까?	corporatecert
인증서 저장소 경로와 파일명은 무엇입니까?	/tmp/iseriesb.kdb

표 8. iSeries B의 서버 인증을 위한 계획 작업 용지 (계속)

질문	응답
인증서 저장소 암호는 무엇입니까?	secret2 **주:** 이 시나리오에서 사용된 모든 암호는 예제 목적으로만 사용됩니다. 이러한 암호를 실제 구성에서 사용하지 마십시오.
서버 인증서의 공통 이름은 무엇입니까?	corporatecert
이 인증서를 보유하는 조직명은 무엇입니까?	MyCo, Inc
iSeries 서버의 IP 주소는 무엇입니까?	172.16.1.3 **주:** 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
iSeries 서버의 완전 규정 호스트명은 무엇입니까?	iseriesb.myco.wis.com

2단계: iSeries A에서 iSeries용 IBM HTTP Server 시작

디지털 인증 관리자(DCM) 인터페이스에 액세스하려면 다음 타스크를 완료하여 HTTP Server의 관리 인스턴스를 시작해야 합니다.

1. iSeries A에서 문자 기반 인터페이스에 사인 온하십시오.
2. 명령 프롬트에서 `strtcpsvr server(*HTTP) httpsvr(*admin)`를 입력하십시오. HTTP Server의 관리 서버가 시작됩니다.

3단계: iSeries A를 인증 기관(CA)으로 구성

1. 웹 브라우저에서 `http://iseriesa:2001`을 입력하면 iSeries 타스크 페이지가 표시되어 디지털 인증 관리자(DCM) 인터페이스에 액세스할 수 있습니다.
2. 사용자의 iSeries A 사용자 프로파일명과 암호를 사용하여 로그 온하십시오.
3. **디지털 인증 관리자**를 클릭하십시오.
4. 왼쪽 탐색 분할 창에서 **인증 기관(CA) 작성**을 선택하십시오.
5. **인증 기관(CA) 작성** 페이지에서, 다음 필수 필드를 DCM 계획 작업 용지에 있는 정보로 채우십시오.
   - **키 크기:** 1024
   - **인증서 저장소 암호:** secret
   - **암호 확인:** secret

     주: 이 시나리오에서 사용된 모든 암호는 예제 목적으로만 사용됩니다. 이러한 암호를 실제 구성에서 사용하지 마십시오.
   - **인증 기관(CA) 이름:** mycoca

- **조직명:** MyCo, Inc
- **시/도:** min
- **시/군/구:** us
- **인증 기관(CA)의 유효 기간(2-7300):** 1095

6. **계속**을 클릭하십시오.
7. **로컬 CA(인증 권한) 설치** 페이지에서 **계속**을 클릭하십시오.
8. **인증 기관(CA) 정책 자료** 페이지에서 다음 옵션을 선택하십시오.
   - **사용자 인증서 작성 허용:** 예
   - **이 인증 기관(CA)에서 발행한 인증서의 유효 기간(1-2000):** 365
9. **승인된 정책 자료** 페이지에서 표시된 메세지를 읽고 **계속**을 클릭하여 디폴트 서버 인증서 저장소(*SYSTEM) 사용자의 인증 기관(CA)이 서명한 서버 인증서를 작성하십시오. 확인 메세지를 읽고 **계속**을 클릭하십시오.
10. **서버 또는 클라이언트 인증서 작성** 페이지에서 다음 정보를 입력하십시오.
    - **키 크기:** 1024
    - **인증서 레이블:** mycocert
    - **인증서 저장소 암호:** secret
    - **암호 확인:** secret

      주: 이 시나리오에서 사용된 모든 암호는 예제 목적으로만 사용됩니다. 이러한 암호를 실제 구성에서 사용하지 마십시오.
    - **공통 이름:** mycocert
    - **조직명:** myco
    - **시/도:** min
    - **시/군/구:** us
    - **IP 버전 4 주소:** 192.168.1.2

      주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
    - **완전 규정 정의역명:** iseriesa.myco.min.com
    - **전자 우편 주소:** adminstrator@myco.min.com
11. **계속**을 클릭하십시오.
12. **어플리케이션 선택** 페이지에서 **계속**을 클릭하십시오.

주: VPN 새 연결 마법사는 사용자가 방금 작성한 인증서를 OS/400 VPN 키 관리자 어플리케이션에 자동으로 지정합니다. 이 인증서를 사용하는 다른 어플리케이션이 있으면 이 페이지에서 선택할 수 있습니다. 이 시나리오는 VPN 연결을 위한 인증서만을 사용하므로 추가 어플리케이션을 선택할 필요가 없습니다.

13. **어플리케이션 상태** 페이지에서 표시된 메세지를 읽고 **취소**를 클릭하십시오. 그러면 변경한 사항이 승인됩니다.

    주: 오브젝트 서명에 사용되는 인증서가 들어 있는 인증서 저장소를 작성하려면 **계속**을 클릭하십시오.
14. DCM 인터페이스가 화면정리되면 **인증서 저장소 선택**을 선택하십시오.
15. **인증서 저장소 선택** 페이지에서 ***SYSTEM**을 선택하십시오. **계속**을 클릭하십시오.
16. **인증서 저장소 및 암호** 페이지에서 secret를 입력하십시오. **계속**을 클릭하십시오.
17. 왼쪽 탐색 프레임에서 **어플리케이션 관리**를 선택하십시오.
18. **어플리케이션 관리** 페이지에서 **CA 신뢰 목록 정의**를 선택하십시오. **계속**을 클릭하십시오.
19. **CA 신뢰 리스트 정의** 페이지에서 **서버**를 선택하십시오. **계속**을 클릭하십시오.
20. **OS/400 VPN 키 관리자**를 선택하십시오. **CA 신뢰 리스트 정의**를 클릭하십시오.
21. **CA 신뢰 리스트 정의** 페이지에서 **LOCAL_CERTIFICATE_AUTHORITY**를 선택하십시오. **확인**을 클릭하십시오.

4단계: iSeries B에 대한 서버 인증서 작성

1. 왼쪽 탐색 분할 창에서 **인증서 작성**을 클릭하고 **또 다른 iSeries를 위한 서버 또는 클라이언트 인증서**를 선택하십시오.
2. **계속**을 클릭하십시오.
3. **또 다른 iSeries를 위한 서버 또는 클라이언트 인증서 작성** 페이지에서, **V5R2**를 선택하십시오. 이는 iSeries B의 릴리스 레벨입니다. **계속**을 클릭하십시오.
4. **서버 또는 클라이언트 인증서 작성** 페이지에서 다음 정보를 입력하십시오.
   - **키 크기:** 1024
   - **인증서 레이블:** corporatecert
   - **인증서 저장소 경로 및 파일명:**/tmp/iseriesb.kdb
   - **인증서 저장소 암호:** secret
   - **암호 확인:** secret2

     주: 이 시나리오에서 사용된 모든 암호는 예제 목적으로만 사용됩니다. 이러한 암호를 실제 구성에서 사용하지 마십시오.
   - **공통 이름:** corporatecert
   - **조직명:** MyCo, Inc
   - **시/도:** wis
   - **시/군/구:** us

- **IP 버전 4 주소:** 172.16.1.3

  주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
- **완전 규정 호스트명:** iseriesb.myco.wis.com
- **전자 우편 주소:** adminstrator@myco.wis.com

5. **계속**을 클릭하십시오.그러면 사용자는 서버 인증서가 iSeries B용 iSeries A에 작성되었음을 확인하는 확인 메시지를 수신하게 됩니다. 지점 영업소의 네트워크 관리자로서 사용자는 이러한 파일을 암호화된 전자 우편을 통해 본사의 관리자에게 송신합니다. 본사의 관리자는 이제 인증서 저장소(.KDB) 파일 및 요구(.RDB) 파일을 iSeries B로 이동하고 이름을 변경해야 합니다. 본사의 관리자는 이러한 파일을 2진 FTP를 사용하여 통합 파일 시스템(IFS)의 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리로 이동해야 합니다. 이 과정이 완료되면 관리자는 해당 디렉토리에서 이러한 파일의 이름을 변경해야 합니다.

5단계: iSeries B에서 .KDB 및 .RDB 이름 변경

*SYSTEM 인증서 저장소가 iSeries B에 존재하지 않기 때문에, 네트워크 관리자는 iseriesb.kdb 및 iseriesb.RDB 파일을 DEFAULT.KDB 및 DEFAULT.RDB로 이름을 변경해야 합니다. 그리고 전송된 파일을 iSeries B에서 *SYSTEM 인증서 저장소로 사용합니다.

1. iSeries Navigator에서 **iSeries B** -> **파일 시스템** -> **통합 파일 시스템** -> **Qibm** -> **UserData** -> **ICSS** -> **Cert** -> **Server**를 차례로 선택하여, 파일 iseriesb.kdb 및 iseriesb.RDB가 이 디렉토리에 나열되는지 확인하십시오.
2. 명령행에서 `wrklnk('/qibm/userdata/icss/cert/server')`를 입력하십시오.
3. **링크 오브젝트에 대한 작업** 페이지에서 7을 선택하여 iseriesb.kdb 파일의 이름을 변경하십시오. Enter를 누르십시오.
4. **오브젝트 이름 변경** 페이지에서 **새 오브젝트** 필드에 `DEFAULT.KDB`를 입력하십시오. Enter를 누르십시오.
5. 3단계 및 4단계를 반복하여 iseriesb.RDB 파일의 이름을 DEFAULT.RDB로 변경하십시오.
6. iSeries Navigator를 화면정리하고 **iSeries B** -> **파일 시스템** -> **통합 파일 시스템** -> **Qibm** -> **UserData** -> **ICSS** -> **Cert** -> **Server**를 차례로 선택하여 이러한 파일이 변경되었는지 확인하십시오. DEFAULT.KDB 및 DEFAULT.RDB가 디렉토리에 나열되어 있어야 합니다.

6단계: iSeries B에서 인증서 저장소 암호 변경

이제 네트워크 관리자는 DEFAULT.KDB 및 DEFAULT.RDB 파일이 작성되었을 때 입력된 *SYSTEM 인증서 저장소의 암호를 변경해야 합니다.

주: *SYSTEM 인증서 저장소 암호를 변경해야 합니다. 암호를 변경하면 암호는 어플리케이션이 암호를 자동으로 회복하고 인증서에 액세스하기 위해 인증서 저장소를 열 수 있도록 은닉됩니다.

1. 브라우저에서 `http://iseriesb:2001`을 입력하십시오. **인증서 저장소 선택**을 클릭하십시오.

2. ***SYSTEM 인증서 저장소**를 선택하고 암호로 secret2를 입력하십시오. 이것은 iSeries B의 서버 인증서를 작성할 때 지점 영업소 관리자가 지정한 암호입니다. **계속**을 클릭하십시오.
3. 왼쪽 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 **암호 변경**을 선택한 후 **계속**을 클릭하십시오.
4. **인증서 저장소 암호 변경** 페이지에서 **새 암호** 및 **암호 확인** 필드에 coporatepwd를 입력하십시오.
5. 만기 정책에 대해 **암호가 만기되지 않음**을 선택하십시오. **계속**을 클릭하십시오.확인 페이지가 로드됩니다. **확인**을 클릭하십시오.
6. **인증서 저장소 암호 변경** 확인 페이지에서 표시된 메세지를 읽고 **확인**을 클릭하십시오.
7. 다시 로드되는 **인증서 저장소 및 암호** 페이지에서 **인증서 저장소 암호** 필드에 coporatepwd를 입력하십시오. **계속**을 클릭하십시오.

7단계: iSeries B에서 OS/400 VPN 키 관리자에 대한 CA 신뢰 정의

1. 왼쪽 탐색 프레임에서 **어플리케이션 관리**를 선택하십시오.
2. **어플리케이션 관리** 페이지에서 **CA 신뢰 목록 정의**를 선택하십시오. **계속**을 클릭하십시오.
3. **CA 신뢰 리스트 정의** 페이지에서 **서버**를 선택하십시오. **계속**을 클릭하십시오.
4. **OS/400 VPN 키 관리자**를 선택하십시오. **CA 신뢰 리스트 정의**를 클릭하십시오.
5. **CA 신뢰 리스트 정의** 페이지에서 **LOCAL_CERTIFICATE_AUTHORITY**를 선택하십시오. **확인**을 클릭하십시오.

이제 지점 영업소와 본사의 관리자는 VPN 구성을 시작할 수 있습니다.

지점 영업소와 본사 간 VPN 연결 구성

다음 단계는 지점 영업소의 관리자가 VN 연결을 구성하는 방법을 보여 줍니다.

1단계: 지점 영업소와 본사 간 VPN 연결을 위한 계획 작업 용지

지점 영업소의 관리자는 지점 영업소와 본사 간 VPN 연결을 구성하기 위해 동적 계획 작업 용지를 작성하기 위해 VPN planning advisor를 사용했습니다. VPN planning advisor는 사용자의 VPN 요구에 대한 특정 질문을 하는 대화식 도구입니다. 사용자의 응답에 따라 어드바이저는 VPN 연결을 구성할 때 사용될 환경에 맞는 사용자 정의된 계획 작업 용지를 생성합니다. 이 작업 용지를 iSeries 서버에서 VPN을 구성할 때 사용할 수 있습니다. VPN Advisor를 사용하여 다음 각 계획 작업 용지가 생성되고 iSeries Navigator에서 VPN 새 연결 마법사를 사용하여 VPN을 구성할 때 사용됩니다. VPN Advisor를 사용하려면 VPN(가상 사설망) Information Center 주제에 있는 VPN Planning Advisor를 참조하십시오.

표 9. 지점 영업소와 본사 간 VPN 연결을 위한 계획 작업 용지

VPN 마법사의 질문:	**VPN Advisor의 권장사항**
연결 그룹의 이름은 무엇입니까?	SalestoCorporate
작성하려는 연결 그룹 유형은 무엇입니까?	**게이트웨이를 다른 게이트웨이로 연결**을 선택하십시오.

표 9. 지점 영업소와 본사 간 VPN 연결을 위한 계획 작업 용지 (계속)

VPN 마법사의 질문:	**VPN Advisor의 권장사항**
키를 보호하기 위해 사용할 인터넷 키 교환 정책은 무엇입니까?	**새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오.
인증서를 사용 중입니까?	**예**를 선택하고 인증서로 mycocert를 선택하십시오. **주:** 이 인증서는 iSeries A에서 인증 기관 구성 단계에서 작성되었습니다.
로컬 연결 엔드포인트를 표현할 ID를 선택하십시오.	선택한 인증서에 정의된 ID 유형 및 ID 리스트에서 ID 유형 **IP 버전 4 주소** 및 ID **192.168.1.2**를 선택하십시오. **주:** 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
연결하려는 키 서버의 ID는 무엇입니까?	ID 유형: **IP 버전 4자리 주소** 및 ID **172.16.1.3**을 선택하십시오. **주:** 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
이 연결이 보호할 자료의 로컬 엔드포인트은 무엇입니까?	**ID 유형:** IP 버전 4 서브네트 **ID:** 10.1.1.0 **마스크:** 255.255.255.0
이 연결이 보호할 자료의 리모트 엔드포인트는 무엇입니까?	**ID 유형:** IP 버전 4 서브네트 **ID:** 10.2.1.0**마스크:** 255.255.255.0
이 연결이 보호할 자료의 포트 및 프로토콜은 무엇입니까?	**로컬 포트:** 모든 포트 **리모트 포트:** 모든 포트 **프로토콜:** 모든 프로토콜
자료를 보호하기 위해 사용할 자료 정책은 무엇입니까?	**새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오.
이 연결이 적용될 로컬 시스템의 인터페이스를 확인하십시오.	• ETHLINE(지점 영업소) • ELINE(본사)

2단계: iSeries A에서 VPN 구성

VPN 연결 계획을 완료한 후에는 iSeries A를 구성하여 VPN으로 두 네트워크 간 자료 전송을 보호할 수 있습니다.

주: VPN 새 연결 마법사를 실행할 때 VPN 서버가 이미 시작되었다면 마법사는 인증서 저장소나 방금 작성한 인증서를 자동으로 찾지 않습니다. VPN 서버가 실행 중이면 VPN 새 연결 마법사를 실행하기 전에 이를 iSeries Navigator에서 재시작해야 합니다.

MyCo, Inc의 관리자는 iSeries A에서 VPN을 구성하기 위해 VPN planning advisor에서 생성한 계획 작업 용지를 사용했습니다.

1. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **IP 정책**을 차례로 선택하십시오.
2. **VPN(가상 사설망)**을 마우스 오른쪽 버튼으로 클릭하고 **새 연결**을 선택하여 연결 마법사를 시작하십시오. 마법사가 작성한 오브젝트에 대한 정보는 시작 페이지를 검토하십시오.
3. **연결명** 페이지에서 **이름** 필드에 SalestoCorporate를 입력하십시오. (선택적)이 연결 그룹의 설명을 지정하십시오. **다음**을 클릭하십시오.
4. **연결 시나리오** 페이지에서 **게이트웨이를 다른 게이트웨이로 연결**을 선택하십시오. **다음**을 클릭하십시오.
5. **인터넷 키 교환 정책** 페이지에서 **새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오. **다음**을 클릭하십시오.
6. **로컬 연결 엔드포인트에 대한 인증서** 페이지에서 **예**를 선택하고 인증서 리스트에서 **mycocert**를 선택하십시오. **다음**을 클릭하십시오.
7. **로컬 연결 엔드포인트 ID** 페이지에서 ID 유형으로 **버전 4 IP 주소**를 선택하십시오. 연관된 IP 주소는 192.168.1.2이어야 합니다. 이 정보 또한 DCM에서 사용자가 작성한 인증서에 정의됩니다.

   주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.

   다음을 클릭하십시오.
8. **리모트 키 서버** 페이지에서 ID 유형 필드에서 **버전 4 IP 주소**를 선택하십시오. **ID** 필드에 172.16.1.3을 입력하십시오. 이것은 본사의 네트워크에 있는 iSeries B의 IP 주소입니다. **다음**을 클릭하십시오.

   주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
9. **로컬 자료 엔드포인트** 페이지에서 ID 유형으로 **IP 버전 4 서브네트**를 선택하고 ID에는 **10.1.1.0**을, 마스크에는 **255.255.255.0**을 입력하십시오.
10. **리모트 자료 엔드포인트** 페이지에서 ID 유형으로 **IP 버전 4 서브네트**를 선택하고 ID에는 **10.2.1.0**을, 마스크에는 **255.255.255.0**을 입력하십시오.
11. **자료 서비스** 페이지에서 로컬 포트와 리모트 포트에 대해 각각 **모든 포트**와 **모든 포트**를 선택하고, 프로토콜에는 **모든 프로토콜**을 선택하십시오. **다음**을 클릭하십시오.
12. **자료 정책** 페이지에서 **새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오. **다음**을 클릭하십시오.

13. **어플리케이션 인터페이스** 페이지에서 **ETHLINE**를 선택하십시오. 다음을 클릭하십시오.
14. **요약** 페이지에서 마법사가 작성할 오브젝트를 검토하여 올바른지 확인하십시오.
15. **완료**를 클릭하여 구성을 완료하십시오. **정책 필터 활성화** 대화 상자가 나타나면 **아니오, 패킷 규칙을 나중에 활성화합니다**를 선택한 다음 **확인**을 클릭하십시오.

3단계: iSeries B에서 VPN 구성

본사의 관리자는 지점 영업소의 관리자가 iSeries A를 구성할 때 사용했던 것과 같은 단계를 사용하며, 필요하면 IP 주소를 반전합니다. 계획 작업 용지를 지침으로 사용하십시오. 이 관리자가 iSeries B 구성을 완료한 후에 두 관리자는 모두 두 서버 모두에서 필터 규칙을 활성화할 수 있습니다.

4단계: 두 서버 모두에서 필터 규칙 활성화

마법사는 이 연결이 제대로 작동하기 위해 필요한 패킷 규칙을 자동으로 작성합니다. 그러나 VPN 연결을 시작하기 전에 두 서버 모두에서 이를 활성화해야 합니다. iSeries A에서 이를 수행하려면 다음 단계를 수행하십시오.

주: 필터 규칙을 활성화한 후 iSeries에 대한 연결이 끊기면 현재 서버에서 활동 중인 모든 필터 규칙을 삭제해야 합니다. 이를 수행하려면 문자 기반 인터페이스에서 RMVTCPTBL (*ALL) 명령을 사용하십시오.

1. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **IP 정책**을 차례로 선택하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **규칙 활성화**를 선택하십시오.
3. **패킷 규칙 활성화** 페이지에서 **VPN이 생성한 규칙만 활성화**를 선택하고 이러한 필터 규칙을 활성화할 인터페이스로 **ETHLINE**를 선택하십시오. **확인**을 클릭하십시오.
4. 인터페이스로 ETHLINE 대신 ELINE를 사용하고 이러한 단계를 반복하여 iSeries B에서 패킷 규칙을 활성화하십시오.

5단계: VPN 연결 시작

다음 단계를 수행하여 iSeries A에서 SalestoCorporate 연결을 시작하십시오.

1. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **IP 정책**을 차례로 선택하십시오.
2. **VPN(가상 사설망)**을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오. 그러면 VPN 서버가 시작됩니다.
3. **VPN(가상 사설망)** --> **보안 연결**을 차례로 선택하십시오. 오른쪽 분할 창에 연결 리스트를 표시하려면 **모든 연결**을 클릭하십시오. **SalestoCorporate**를 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오.
4. **보기** 메뉴에서 **화면정리**를 선택하십시오. 연결이 시작되면 상태는 유휴에서 사용 가능으로 변경됩니다. 연결을 시작하는 데 몇 분이 소요될 수 있으므로 상태가 사용 가능으로 변경될 때까지 주기적으로 화면정리하십시오.
5. iSeries B에서 이러한 단계를 반복하십시오.

6단계: 엔드포인트 간 VPN 연결 테스트

두 서버 모두 구성을 마치고 연결을 시작한 후에는 리모트 호스트가 서로 통신할 수 있는지 확인하기 위해 연결성을 테스트해야 합니다.

주: 리모트 네트워크의 목적지에 통신량이 많은 경우, 로컬 클라이언트의 라우트가 적절히 구성되었는지 확인하십시오.

분점 영업소에 있는 Windows XP 워크스테이션에서 네트워크 관리자는 다음 단계를 완료했습니다.

1. 명령 프롬트에 `ping 10.2.1.3`을 입력하십시오. 이것은 본사의 네트워크에 있는 워크스테이션 중 하나의 IP 주소입니다.

   주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
2. 이러한 단계를 반복하십시오. 이번에는 본사와 지점 간의 연결성을 테스트합니다.

이제 관리자는 리모트 사용자에 대한 VPN 연결을 구성할 수 있습니다.

리모트 사용자에 대한 VPN 연결 구성

지점 영업소와 본사 간 VPN 연결을 구성한 후 지점 영업소의 관리자는 리모트 영업 사원에 대한 보안 연결을 설정하려고 합니다.

1단계: 지점 영업소에서 리모트 영업 사원으로 VPN 연결을 위한 계획 작업 용지 완료

지점 영업소의 관리자는 서버와 리모트 워크스테이션에서 VPN을 구성하기 위해 동적 계획 작업 용지를 작성하기 위해 VPN planning advisor를 사용했습니다. VPN planning advisor는 사용자의 VPN 요구에 대한 특정 질문을 하는 대화식 도구입니다. 사용자의 응답에 따라 어드바이저는 VPN 연결을 구성할 때 사용될 환경에 맞는 사용자 정의된 계획 작업 용지를 생성합니다. 이 작업 용지를 iSeries 서버에서 VPN을 구성할 때 사용할 수 있습니다. iSeries Navigator의 VPN 마법사에서 사용될 VPN Advisor를 사용하여 다음 각 계획 작업 용지가 생성되었습니다. VPN Advisor를 사용하려면 VPN(가상 사설망) 주제에 있는 VPN Planning Advisor를 참조하십시오.

표 10. 지점 영업소와 리모트 영업 사원 간 VPN 연결을 위한 계획 작업 용지

VPN 마법사의 질문:	**VPN Advisor의 권장사항**
연결 그룹의 이름은 무엇입니까?	SalestoRemote
작성하려는 연결 그룹 유형은 무엇입니까?	**호스트를 다른 호스트로 연결**을 선택하십시오.
키를 보호하기 위해 사용할 인터넷 키 교환 정책은 무엇입니까?	**새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오.
인증서를 사용 중입니까?	**아니오**를 선택하십시오.

표 10. 지점 영업소와 리모트 영업 사원 간 VPN 연결을 위한 계획 작업 용지 (계속)

VPN 마법사의 질문:	**VPN Advisor의 권장사항**
이 연결의 로컬 키 서버를 표현할 ID를 입력하십시오.	ID 유형:**IP 버전 4 주소** IP 주소 :**192.168.1.2** **주:** 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
연결하려는 키 서버의 ID는 무엇입니까?	ID 유형: **모든 IP 주소 사전 공유 키**: mycokey **주:** 사전 공유 키는 OS/400 VPN이 연결을 인증하고 사용자의 자료를 보호하는 키를 설정하기 위해 사용하는 32문자 텍스트 스트링입니다. 일반적으로, 사전 공유 키는 암호를 다루는 방식과 유사하게 다루어야 합니다.
이 연결이 보호할 자료의 포트 및 프로토콜은 무엇입니까?	**로컬 포트**: 1701 **리모트 포트**: 모든 **포트프로토콜**: UDP
자료를 보호하기 위해 사용할 자료 정책은 무엇입니까?	**새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오.
이 연결이 적용될 로컬 시스템의 인터페이스를 확인하십시오.	ETHLINE(지점 영업소)

2단계: iSeries A에서 L2TP 종료 프로그램 구성

리모트 워크스테이션에 대한 리모트 연결을 구성하려고 합니다. 이러한 클라이언트로부터 인바운드 연결을 승인하려면 iSeries A를 설정해야 합니다. iSeries A의 L2TP 종료 프로그램 프로파일을 구성하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **리모트 액세스 서비스**를 차례로 선택하십시오.
2. **리시버 연결 프로파일**을 마우스 오른쪽 버튼으로 클릭하고 iSeries A를 리모트 사용자로부터 들어오는 연결을 허용하는 서버로 설정하고 **새 프로파일**을 선택하십시오.
3. **새 지점 간 연결 프로파일 설정** 페이지에서, 다음 옵션을 선택하십시오.
   - **프로토콜 유형:** PPP
   - **연결 유형:** L2TP(가상 회선)

     주: 작동 모드 필드는 자동으로 **종료 프로그램(네트워크 서버)**을 표시해야 합니다.
   - **회선 서비스 유형**: 단일 회선
4. **확인**을 클릭하십시오. 그러면 **새 지점 간 프로파일 등록 정보** 페이지가 실행됩니다.

5. **새 지점 간 프로파일 등록 정보** 페이지에서, **이름** 필드에 MYCOL2TP를 입력하십시오. **확인**을 클릭하십시오.
6. **연결** 탭에서 **로컬 터널 엔드포인트 IP 주소**로 **192.168.1.2**를 선택하십시오.

   주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
7. **MYCOL2TP**를 **가상 회선명**으로 선택하십시오. **확인**을 클릭하십시오. 그러면 **새 L2TP 등록 정보** 페이지가 실행됩니다.
8. **인증** 페이지에서 호스트명으로 iseriesa를 입력하십시오. **확인**을 클릭하십시오. 그러면 **연결** 페이지로 되돌아갑니다.
9. **연결** 페이지에서 다음 옵션을 선택하고, **최대 연결 횟수**로 25를 입력하십시오.
10. **인증** 탭에서 **리모트 시스템의 ID를 확인하기 위해 이 iSeries 서버 필요**를 선택하십시오.
11. **유효성 리스트를 사용하여 로컬에서 인증**을 선택하십시오.
12. **유효성 리스트명** 필드에 QL2TP를 입력하고, **신규**를 클릭하십시오.
13. **유효성 리스트** 페이지에서 **추가**를 선택하십시오.
14. 각 리모트 직원의 사용자 이름과 암호를 추가하십시오. **확인**을 클릭하십시오.
15. 암호 확인 페이지에서 각 리모트 직원의 암호를 재입력하십시오. **확인**을 클릭하십시오.
16. **TCP/IP 설정** 페이지에서 **로컬 IP 주소**로 10.1.1.1을 선택하십시오.
17. **IP 주소 지정 메소드** 필드에서 **주소 풀(pool)**을 선택하십시오.
18. **시작 IP 주소** 필드에 10.1.1.100을, **주소 개수**에 49를 입력하십시오.
19. **리모트 시스템이 다른 네트워크에 액세스할 수 있도록 허용(IP 이송)**을 선택하십시오. **확인**을 클릭하십시오.

3단계: 리시버 연결 프로파일 시작

iSeries A에 대한 L2TP 리시버 연결 프로파일을 구성한 후 관리자는 이 연결이 리모트 클라이언트로부터 들어오는 요구를 청취할 수 있도록 이 연결을 시작해야 합니다.

주: QSYSWRK 서브시스템이 시작하지 않은 리시버 연결 프로파일을 시작하려고 시도하면 오류 메세지를 수신할 수 있습니다. QUSRWRK 서브시스템을 시작하려면 다음 타스크를 완료하십시오.

1. 문자 기반 인터페이스에서 strsbs를 입력하십시오.
2. 서브시스템 시작 표시 화면에서 **서브시스템 설명** 필드에 QUSRWRK를 입력하십시오.

리모트 클라이언트에 대해 VPN을 구성하려면 다음 타스크를 완료하십시오.

1. iSeries Navigator에서 **보기** 메뉴에서 **화면정리**를 선택하십시오. 그러면 iSeries Navigator의 인스턴스가 화면정리됩니다.
2. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **리모트 액세스 서비스**를 차례로 선택하십시오.

3. **리시버 연결 프로파일**을 두 번 클릭하고 **MYCOL2TP**를 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오.
4. **상태** 필드는 **연결 요청을 기다리는 중**을 표시합니다.

4단계: 리모트 클라이언트의 iSeries A에서 VPN 연결 구성

iSeries A에 대한 L2TP 리시버 연결 프로파일을 구성 및 시작한 후 관리자는 리모트 클라이언트와 지점 영업소의 네트워크 간 연결을 보호하기 위해 VPN을 구성해야 합니다. 리모트 클라이언트에 대해 VPN을 구성하려면 다음 타스크를 완료하십시오.

1. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **IP 정책**을 차례로 선택하십시오.
2. **VPN(가상 사설망)**을 마우스 오른쪽 버튼으로 클릭하고 **새 연결**을 선택하여 VPN 새 연결 마법사를 시작하십시오. 마법사가 작성한 오브젝트에 대한 정보는 **시작** 페이지를 검토하십시오.
3. **다음**을 클릭하여 **연결명** 페이지로 가십시오.
4. **이름** 필드에 SalestoRemote를 입력하십시오.
5. (선택적)이 연결 그룹의 설명을 지정하십시오. **다음**을 클릭하십시오.
6. **연결 시나리오** 페이지에서 **호스트를 다른 호스트로 연결**을 선택하십시오. **다음**을 클릭하십시오.
7. **인터넷 키 교환 정책** 페이지에서 **새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오. **다음**을 클릭하십시오.
8. **로컬 연결 엔드포인트에 대한 인증서** 페이지에서 **아니오**를 선택하십시오. **다음**을 클릭하십시오.
9. **로컬 키 서버** 페이지에서 ID 유형으로 **버전 4 IP 주소**를 선택하십시오. 연관된 IP 주소는 192.168.1.2이어야 합니다. **다음**을 클릭하십시오.

   주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
10. **리모트 키 서버** 페이지에서 ID 유형 필드에서 **모든 IP 주소**를 선택하십시오. **사전 공유 키** 필드에 mycokey를 입력하십시오. **다음**을 클릭하십시오.
11. **자료 서비스** 페이지에서 로컬 포트에 대해 1701을 입력하고 리모트 포트로는 1701을, 프로토콜로는 UDP를 선택하십시오. **다음**을 클릭하십시오.
12. **자료 정책** 페이지에서 **새 정책 작성**을 선택한 다음 **가장 높은 보안, 가장 낮은 성능**을 선택하십시오. **다음**을 클릭하십시오.
13. **어플리케이션 인터페이스** 페이지에서 **ETHLINE**를 선택하십시오. **다음**을 클릭하십시오.
14. **요약** 페이지에서 마법사가 작성할 오브젝트를 검토하여 올바른지 확인하십시오.
15. **완료**를 클릭하여 구성을 완료하십시오. **정책 필터 활성화** 대화 상자가 나타나면**아니오, 패킷 규칙을 나중에 활성화합니다**를 선택하고 **확인**을 클릭하십시오.

5단계: Windows XP 클라이언트에서 리모트 연결을 위한 VPN 정책 갱신

마법사는 대부분의 VPN 구성에서 사용될 수 있는 표준 연결을 작성하므로 Windows XP 클라이언트와의 상호운영성을 보장하기 위해 이 마법사에서 생성된 정책을 갱신해야 합니다. 이러한 VPN 정책을 갱신하려면 다음 타스크를 완료하십시오.

1. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **IP 정책** --> **VPN(가상 사설망)** --> **IP 보안 정책**을 차례로 선택하십시오.
2. **인터넷 키 교환 정책**을 두 번 클릭하고 **모든 IP 주소**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **변형** 페이지에서 **추가**를 클릭하십시오.
4. **인터넷 키 교환 변형 추가** 페이지에서 다음 옵션을 선택하고 **확인**을 클릭하십시오.
   - **인증 메소드:** 사전 공유 키
   - **해시 알고리즘:** MD5
   - **암호화 알고리즘:** DES-CBC
5. **확인**을 클릭하십시오.
6. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **IP 정책** --> **VPN(가상 사설망)** --> **IP 보안 정책**을 차례로 선택하십시오.
7. **데이터 정책**을 두 번 클릭하고 **SalestoRemote**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
8. **일반** 페이지에서 **Diffie-Hellman PFS(Perfect Forward Secrecy) 사용**을 선택취소하십시오.
9. **제안** 페이지에서 **추가**를 클릭하십시오.
10. **새 자료 정책 제안** 페이지에서 다음 옵션을 선택하십시오.
    - **캡슐화 모드:** 전송
    - **키 만기:** 15분
    - **만기 시 크기 한계:** 100000
11. **변형** 페이지에서 **추가**를 클릭하십시오.
12. **자료 정책 변형 추가** 페이지에서 다음 옵션을 선택하고 **확인**을 클릭하십시오.
    - **프로토콜:** ESP(Encapsulating Security Payload)
    - **인증 알고리즘:** MD5
    - **암호화 알고리즘:** DES-CBC
13. **확인**을 클릭하십시오.

6단계: 필터 규칙 활성화

마법사는 이 연결이 제대로 작동하기 위해 필요한 패킷 규칙을 자동으로 작성합니다. 그러나 VPN 연결을 시작하기 전에 두 서버 모두에서 이를 활성화해야 합니다. iSeries A에서 이를 수행하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 **iSeries A** --> **네트워크** --> **IP 정책**을 차례로 선택하십시오.

2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **규칙 활성화**를 선택하십시오.
3. **패킷 규칙 활성화** 페이지에서 **VPN이 생성한 규칙만 활성화**를 선택하고 이러한 필터 규칙을 활성화할 인터페이스로 **ETHLINE**를 선택하십시오. **확인**을 클릭하십시오.

리모트 사용자가 각자의 Windows XP 워크스테이션을 구성할 수 있으려면 관리자는 사용자가 직접 사용자측 연결을 설정할 수 있도록 다음 정보를 제공해야 합니다. 각 리모트 사용자에게 다음 정보를 제공하십시오.

- 사전 공유 키명: `mycokey`
- iSeries A의 IP 주소: 192.168.1.2

  주: 이 시나리오에서 사용된 IP 주소는 예제 목적으로만 사용됩니다. IP 주소지정 체계를 반영한 것이 아니며 실제 구성에서 사용되어서도 안 됩니다. 이러한 타스크를 완료할 때 사용자 고유의 IP 주소를 사용해야 합니다.
- 연결에 대한 사용자명 및 암호

  주: 관리자가 L2TP 종료 프로그램 프로파일 구성 시 유효성 리스트에 사용자명과 암호를 추가할 때 작성되었습니다.

7단계: Windows XP 클라이언트에서 VPN 구성

MyCo, Inc의 리모트 사용자는 다음 단계를 완료하여 각자의 리모트 Windows XP 클라이언트를 설정해야 합니다.

1. Windows XP **시작** 메뉴에서 **프로그램 --> 보조 프로그램 --> 통신 --> 새 연결 마법사**를 차례로 선택하십시오.
2. **시작** 페이지에서 개요 정보를 읽으십시오. **다음**을 클릭하십시오.
3. **네트워크 연결 유형** 페이지에서 **내 작업 공간에서 네트워크에 연결**을 선택하십시오. **다음**을 클릭하십시오.
4. **네트워크 연결** 페이지에서 **VPN(가상 사설망) 연결**을 선택하십시오. **다음**을 클릭하십시오.
5. **연결명** 페이지에서 **회사명** 필드에 `Connection to Branch office`를 입력하십시오. **다음**을 클릭하십시오.
6. **공용 네트워크** 페이지에서 **초기 연결을 다이얼하지 않음**을 선택하십시오. **다음**을 클릭하십시오.
7. **VPN 서버 선택** 페이지에서 **호스트명 또는 IP 주소** 필드에 `192.168.1.2`를 입력하십시오. **다음**을 클릭하십시오.
8. **요약** 페이지에서 **이 연결에 대한 단축키를 바탕화면에 추가**를 클릭하십시오. **완료**를 클릭하십시오.
9. 바탕화면에 작성된 **MyCo에 연결** 아이콘을 클릭하십시오.
10. **MyCo에 연결** 페이지에서 관리자가 제공한 사용자명과 암호를 입력하십시오.
11. **다음 사용자를 위해 이 사용자명과 암호 저장** 및 **나만 사용**을 선택하십시오. **등록 정보**를 클릭하십시오.
12. **보안** 페이지에서 다음 **보안 옵션**이 선택되었는지 확인하십시오.
    - **일반**
    - **보안 암호 필요**
    - **자료 암호화 필요**

Click **IPSec 설정**.

13. **IPSec 설정** 페이지에서 **인증에 사전 공유 키 사용**을 선택하고 사전 공유 키 필드에 mycokey를 입력하십시오. **확인**을 클릭하십시오.
14. **네트워킹** 페이지에서 **L2TP IPSec VPN**을 **VPN 유형**으로 선택하십시오. **확인**을 클릭하십시오.
15. 사용자명과 암호로 사인 온하고 **연결**을 클릭하십시오.

클라이언트 측에서 VPN 연결을 시작하려면 연결 마법사를 완료한 후 데스크탑에 나타나는 아이콘을 클릭하십시오.

8단계: 엔드포인트 간 VPN 연결 테스트

iSeries A와 리모트 사용자 간 연결 구성을 마치고 연결을 시작한 후에는 리모트 호스트가 서로 통신할 수 있는지 확인하기 위해 연결성을 테스트해야 합니다. 이를 수행하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 **iSeries A** --> **네트워크**를 차례로 선택하십시오.
2. **TCP/IP 구성**을 마우스 오른쪽으로 클릭하고 **유틸리티**를 선택한 다음 **핑**을 선택하십시오.
3. **핑 시작** 대화 상자에서 **핑** 필드에 10.1.1.101을 입력하십시오.

   주: 10.1.1.101은 iSeries A의 L2TP 종료 프로그램 프로파일에 지정된 주소 풀(pool)로부터 리모트 영업 클라이언트에게 동적으로 지정된 IP 주소를 표현합니다.
4. **지금 핑**을 클릭하여 iSeries에서 리모트 워크스테이션으로의 연결성을 확인하십시오. **확인**을 클릭하십시오.

리모트 클라이언트로부터 연결을 테스트하려면 리모트 직원은 Windows XP 워크스테이션에서 이러한 단계를 완료해야 합니다.

1. 명령 프롬트에 ping 10.1.1.2를 입력하십시오. 이것은 본사의 네트워크에 있는 워크스테이션 중 하나의 IP 주소입니다.
2. 이러한 단계를 반복하십시오. 이번에는 본사와 지점 간의 연결성을 테스트합니다.

제 7 장 시나리오: 파티션 간 통신을 위한 가상 이더넷 작성

상황

사용자는 규모가 작은 회사의 시스템 관리자입니다. 네 개의 논리 파티션으로 나누어진 서버를 사용하고 있습니다. 사용자는 네 개의 논리 파티션 모두 사이에서 고속 통신을 허용해야 하며 이 통신을 외부 LAN으로 확장해야 합니다. 사용자의 하드웨어는 LAN 카드를 꽂을 수 있는 카드 슬롯 수가 제한되어 있습니다. 그러므로 추가 LAN 카드가 필요하지 않는 솔루션을 찾아야 합니다.

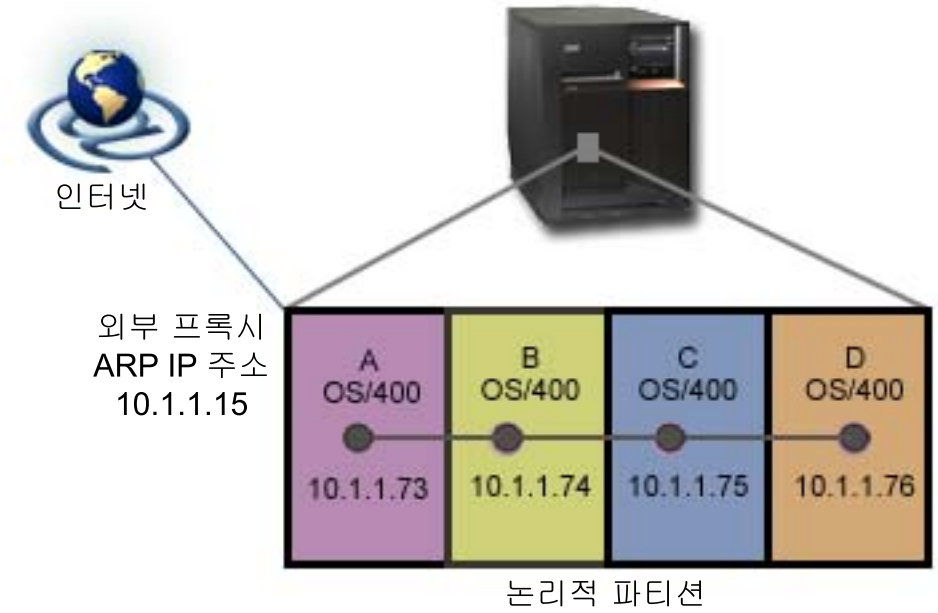
목적

이 시나리오의 목적은 다음과 같습니다.

- 논리 파티션 간 통신을 허용하기 위해 가상 이더넷 네트워크 작성.
- 프록시 ARP가 가상 이더넷 네트워크를 외부 LAN에 연결할 수 있도록 만들기.
- 필요한 회선, 인터페이스 및 라우트 구성.

세부사항

이 그림은 네 개의 논리 파티션 간 통신을 가능하게 해주고 프록시 ARP를 사용하여 데이터가 가상 이더넷과 외부 LAN 간을 흐를 수 있도록 해주는 가상 이더넷을 보여 줍니다.



- iSeries 서버에 네 개의 논리 파티션이 작성되었습니다.
- 각 파티션은 OS/400 버전 5 릴리스 3에서 실행됩니다.
- 각 파티션에 구성된 가상 TCP/IP 인터페이스는 다음 IP 주소를 사용합니다.

  - 파티션 A IP: 10.1.1.73
  - 파티션 B IP: 10.1.1.74
  - 파티션 C IP: 10.1.1.75
  - 파티션 D IP: 10.1.1.76
- 외부 프록시 ARP 인터페이스는 IP 주소 10.1.1.15를 사용하여 파티션 A에 구성되어 있습니다.

전제조건 및 가정

설치 요구사항은 다음과 같습니다.

- 기본 논리 파티션에 설치된 OS/400 버전 5 릴리스 3 이상
- IBM 270 및 8xx 모델 서버
- 이 경우에는 서버 상의 네 개의 논리 파티션(LPAR). 기본 논리 파티션에는 OS/400 버전 5 릴리스 3 이상이 설치되어 있어야 합니다. 다른 논리 파티션에는 OS/400 V5R3 또는 Linux를 설치할 수 있습니다.

  이 시나리오에서 모든 논리 파티션은 OS/400을 사용합니다.

구성 단계

다음 구성 타스크를 완료하십시오.

1. 논리 파티션이 가상 이더넷에 참여할 수 있도록 만들기
2. 이더넷 회선 설명 작성
3. IP 데이터그램 이송 켜기
4. 프록시 ARP를 사용할 수 있도록 인터페이스 작성
5. 파티션 A에서 가상 이더넷 인터페이스 작성
6. 파티션 B에서 가상 이더넷 인터페이스 작성
7. 파티션 C에서 가상 이더넷 인터페이스 작성
8. 파티션 D에서 가상 이더넷 인터페이스 작성
9. 라우트 작성
10. 네트워크 통신 확인

시나리오 세부사항: 파티션 간 통신을 위한 가상 이더넷 작성

다음 타스크는 네트워크 관리자가 가상 이더넷 네트워크를 작성하는 방법과 네트워크가 프록시 ARP를 사용하여 외부 LAN과 통신할 수 있도록 만드는 방법을 보여 줍니다.

1단계: 논리 파티션이 가상 이더넷에 참여할 수 있도록 만들기

가상 이더넷을 사용할 수 있으려면 다음 단계를 수행하십시오.

1. 1차 파티션(파티션 A)의 명령행에서 STRSST를 입력하고 Enter를 누르십시오.

2. 서비스 도구 사용자 ID와 암호를 입력하십시오.
3. 시스템 서비스 툴(SST) 표시 화면에서 옵션 5(시스템 파티션에 대한 작업)를 선택하십시오.
4. 시스템 파티션에 대한 작업 표시 화면에서 옵션 3(파티션 구성에 대한 작업)을 선택하십시오.
5. F10(가상 이더넷에 대한 작업)을 누르십시오.
6. 1차 파티션 및 2차 파티션의 해당 열에서 1을 입력하여 파티션이 가상 이더넷을 통해 서로 통신할 수 있도록 하십시오.
7. 시스템 서비스 툴(SST)을 종료하여 명령행으로 되돌아가십시오.

2단계: 이더넷 회선 설명 작성

가상 이더넷을 지원하기 위해 새 이더넷 회선 설명을 구성하려면 다음 단계를 수행하십시오.

1. 논리 파티션 A의 명령행에서, WRKHDWRSC *CMN을 입력하고 Enter를 누르십시오.
2. 통신 자원에 대한 작업 표시 화면에서 해당 가상 이더넷 포트 옆에 있는 옵션 7(자원 세부사항 표시)을 선택하십시오.

   268C로 식별된 이더넷 포트가 가상 이더넷 자원입니다. 논리 파티션에 연결된 각 가상 이더넷마다 하나의 자원이 있습니다.
3. 자원 세부사항 표시 표시 화면에서 아래로 스크롤하여 포트 주소를 찾으십시오.

   포트 주소는 논리 파티션 구성 시 선택한 가상 이더넷에 해당합니다.
4. 통신 자원에 대한 작업 표시 화면에서 해당 가상 이더넷 포트 옆에 있는 옵션 5(구성 설명에 대한 작업)를 선택하고 Enter를 누르십시오.
5. 구성 설명에 대한 작업 표시 화면에서 옵션 1(작성)을 선택하고 Enter를 눌러 CRTLINETH(회선 설명 이더넷 작성) 표시 화면을 보십시오.
   a. *회선 설명* 프롬트에 VETH0를 입력하십시오. 이름 VETH0는 모호하기는 하지만 사용자가 논리 파티션이 통신이 가능하도록 만든 가상 이더넷 페이지의 번호 지정된 열에 해당합니다. 회선 설명과 각 연관된 가상 이더넷에 같은 이름을 사용하면 가상 이더넷 구성을 쉽게 추적할 수 있습니다.
   b. *회선 속도* 프롬트에 1G를 입력하십시오.
   c. *양방향 전송* 프롬트에 *FULL을 입력하고 Enter를 누르십시오.
   d. *최대 프레임 크기* 프롬트에 8996을 입력하고 Enter를 누르십시오.

      프레임 크기를 8996으로 변경하면 가상 이더넷을 통과하는 자료 전송이 향상됩니다.

      회선 설명이 작성되었음을 알리는 메세지가 표시됩니다.
6. 회선 설명을 연결변환하십시오. WRKCFGSTS *LIN을 입력하고 VETH0에 대해 옵션 1(연결변환)을 선택하십시오.
7. 1부터 6단계까지를 반복하되 논리 파티션 B, C 및 D의 명령행에서 단계를 수행하여 각 논리 파티션에 대한 이더넷 회선 설명을 작성하십시오.

회선 설명의 이름은 모호하지만 가상 이더넷과 연관된 모든 회선 설명에 같은 이름을 사용하는 것이 좋습니다. 이 시나리오에서는 모든 회선 설명의 이름은 VETH0입니다.

3단계: IP 데이터그램 이송 켜기

가상 이더넷을 외부 LAN으로 연결하는 파티션에서 IP 데이터그램 이송을 켜야 합니다. IP 데이터그램 이송을 사용하면 IP 패킷이 서로 다른 서브네트 사이에서 이송될 수 있습니다. 이 시나리오의 경우 파티션 A에서 IP 데이터그램 이송을 켜야 합니다.

IP 데이터그램 이송을 켜려면 다음 단계를 수행하십시오.

1. 논리 파티션 A의 명령행에서, CHGTCPA를 입력하고 F4를 누르십시오.
2. *IP 데이터그램 이송* 프롬트에 *YES를 입력하십시오.

4단계: 프록시 ARP를 사용할 수 있도록 인터페이스 작성

TCP/IP 인터페이스를 작성하기 전에 가상 이더넷이 실제 LAN에 연결될 방법을 결정해야 합니다. 논리 파티션이 외부 LAN상의 시스템과 통신할 수 있도록 하려면 TCP/IP 통신이 가상 이더넷과 외부 LAN 간을 이동할 수 있도록 해야 합니다. 가상 및 외부 네트워크를 연결하는 데에는 프록시 ARP, 네트워크 주소 변환(NAT) 및 TCP/IP 라우팅 등의 세 가지 메소드가 있습니다. 이 시나리오는 프록시 ARP 메소드를 사용합니다. 이 네트워크 통신을 연결하는 세 가지 방법 모두에 대한 자세한 내용은 가상 이더넷을 외부 LAN에 연결하는 TCP/IP 기술을 참조하십시오.

프록시 ARP를 사용하기 위해 TCP/IP 인터페이스를 작성하려면 다음 단계를 완료하십시오.

1. 네트워크가 라우팅 가능한 IP 주소의 연속적인 블록을 구하십시오.

   이 가상 이더넷에 총 네 개의 논리 파티션이 있기 때문에 여덟 개의 주소 블록이 필요합니다. 블록에서 첫 번째 IP 주소의 네 번째 세그먼트는 8로 나눌 수 있어야 합니다. 이 블록의 첫 번째 및 마지막 IP 주소는 IP 주소의 서브네트이자 브로드케스트이며 사용할 수 없습니다. 두 번째 주소는 논리 파티션에서 가상 TCP/IP 인터페이스에 사용될 수 있으며 세 번째, 네 번째 및 다섯 번째 주소는 다른 논리 파티션에서 TCP/IP 연결에 사용될 수 있습니다. 이 시나리오의 경우 IP 주소 블록은 10.1.1.72 ~ 10.1.1.79이며 서브네트 마스크는 255.255.255.248입니다.

   또한 외부 TCP/IP 주소의 단일 IP 주소가 필요합니다. 이 IP 주소는 연속 주소 블록에 속하면 안되며 동일한 원래 서브네트 마스크 255.255.255.0 내에 있어야 합니다.
2. 논리 파티션 A에 대해 OS/400 TCP/IP 인터페이스를 작성하십시오. 이 인터페이스는 외부, 프록시 ARP IP 인터페이스로 알려져 있습니다.

   인터페이스를 작성하려면 다음 단계를 따르십시오.

   a. 파티션 A의 명령행에서, CFGTCP를 입력하고 Enter를 눌러 TCP/IP 구성 화면 표시를 보십시오.
   b. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
   c. 옵션 1(추가)를 선택하고 Enter를 눌러 TCP/IP 인터페이스 추가(ADDTCPIFC) 표시 화면을 보십시오.

d. *인터넷 주소* 프롬트에 '10.1.1.15'를 입력하십시오.

e. *회선 설명* 프롬트에 ETHLINE과 같은 회선 설명 이름을 입력하십시오.

f. *서브네트 마스크* 프롬트에 '255.255.255.0'을 입력하십시오.

3. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 표시 화면에서 시작할 인터페이스에 대해 옵션 9(시작)를 선택하십시오.

5단계: 파티션 A에서 가상 이더넷 인터페이스 작성

1. 파티션 A의 명령행에서, CFGTCP를 입력하고 Enter를 눌러 TCP/IP 구성 화면 표시를 보십시오.
2. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
3. 옵션 1(추가)를 선택하고 Enter를 눌러 TCP/IP 인터페이스 추가(ADDTCPIFC) 표시 화면을 보십시오.
4. *인터넷 주소* 프롬트에 '10.1.1.73'을 입력하십시오.
5. *회선 설명* 프롬트에 VETH0를 입력하십시오.
6. *서브네트 마스크* 프롬트에 '255.255.255.248'을 입력하십시오.
7. *연관된 인터넷 주소* 프롬트에 '10.1.1.15'를 입력하십시오. 그러면 가상 이더넷 인터페이스가 외부 인터페이스에 연관되고 프록시 ARP가 가상 이더넷 인터페이스 10.1.1.73과 외부 인터페이스 10.1.1.15 간에 패킷을 이송할 수 있습니다.
8. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 표시 화면에서 시작할 인터페이스에 대해 옵션 9(시작)를 선택하십시오.

6단계: 파티션 B에서 가상 이더넷 인터페이스 작성

1. 파티션 B의 명령행에서, CFGTCP를 입력하고 Enter를 눌러 TCP/IP 구성 화면 표시를 보십시오.
2. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
3. 옵션 1(추가)를 선택하고 Enter를 눌러 TCP/IP 인터페이스 추가(ADDTCPIFC) 표시 화면을 보십시오.
4. *인터넷 주소* 프롬트에 '10.1.1.74'를 입력하십시오.
5. *회선 설명* 프롬트에 VETH0를 입력하십시오.
6. *서브네트 마스크* 프롬트에 '255.255.255.248'을 입력하십시오.
7. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 표시 화면에서 시작할 인터페이스에 대해 옵션 9(시작)를 선택하십시오.

7단계: 파티션 C에서 가상 이더넷 인터페이스 작성

1. 파티션 C의 명령행에서, CFGTCP를 입력하고 Enter를 눌러 TCP/IP 구성 화면 표시를 보십시오.
2. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
3. 옵션 1(추가)를 선택하고 Enter를 눌러 TCP/IP 인터페이스 추가(ADDTCPIFC) 표시 화면을 보십시오.
4. *인터넷 주소* 프롬트에 '10.1.1.75'를 입력하십시오.
5. *회선 설명* 프롬트에 VETH0를 입력하십시오.
6. *서브네트 마스크* 프롬트에 '255.255.255.248'을 입력하십시오.

7. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 표시 화면에서 시작할 인터페이스에 대해 옵션 9(시작)를 선택하십시오.

8단계: 파티션 D에서 가상 이더넷 인터페이스 작성

1. 파티션 D의 명령행에서, CFGTCP를 입력하고 Enter를 눌러 TCP/IP 구성 화면 표시를 보십시오.
2. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
3. 옵션 1(추가)를 선택하고 Enter를 눌러 TCP/IP 인터페이스 추가(ADDTCPIFC) 표시 화면을 보십시오.
4. *인터넷 주소* 프롬트에 '10.1.1.76'을 입력하십시오.
5. *회선 설명* 프롬트에 VETH0를 입력하십시오.
6. *서브네트 마스크* 프롬트에 '255.255.255.248'을 입력하십시오.
7. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 표시 화면에서 시작할 인터페이스에 대해 옵션 9(시작)를 선택하십시오.

9단계: 라우트 작성

패킷이 가상 이더넷을 종료할 수 있도록 디폴트 라우트를 작성하려면 다음 단계를 수행하십시오.

1. 파티션 B의 명령행에서, CFGTCP를 입력하고 Enter를 누르십시오.
2. 옵션 2(TCP/IP 라우트에 대한 작업)를 선택하고 Enter를 누르십시오.
3. 옵션 1(추가)을 선택하고 Enter를 누르십시오.
4. *라우트 목적지* 프롬트에 *DFTROUTE를 입력하십시오.
5. *서브네트 마스크* 프롬트에 *NONE'을 입력하십시오.
6. *다음 홉(hop)* 프롬트에 '10.1.1.73'을 입력하십시오.
7. 파티션 C와 D에 대해 1부터 6단계까지를 반복하여 이러한 각 논리 파티션에서 디폴트 라우트를 작성하십시오. 각 경우에 다음 홉(hop) 주소로 10.1.1.73을 지정하십시오.

   이러한 각 논리 파티션의 패킷은 이러한 디폴트 라우트를 사용하여 가상 이더넷을 통해 10.1.1.73 인터페이스로 이동합니다. 10.1.1.73이 외부 프록시 ARP 인터페이스 10.1.1.15와 연관되어 있으므로 패킷은 프록시 ARP 인터페이스를 사용하여 가상 이더넷으로부터 계속 이동합니다.

10단계: 네트워크 통신 확인

Ping 명령을 사용하여 네트워크 통신을 확인하십시오.

- 파티션 B, C 및 D에서 가상 이더넷 인터페이스 10.1.1.73 및 외부 호스트를 ping하십시오.
- 외부 OS/400 호스트에서 각 가상 이더넷 인터페이스 10.1.1.73, 10.1.1.74, 10.1.1.75 및 10.1.1.76을 ping하십시오.

제 8 장 시나리오: L2TP를 사용한 논리 파티션간 모뎀 공유

상황

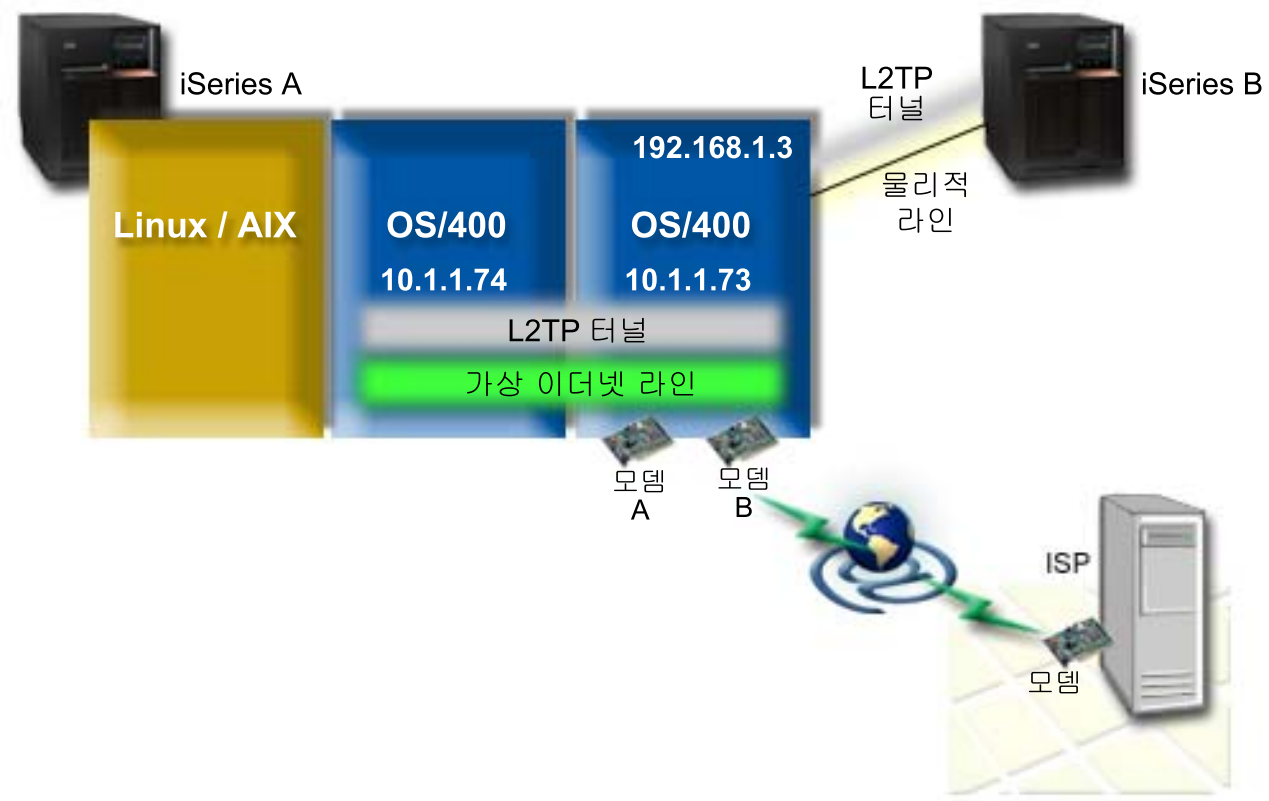
당신은 중간급 회사의 시스템 관리자입니다. 현재 회사의 컴퓨터 장비를 갱신할 시기이지만, 그보다 하드웨어를 능률화하고자 합니다. 우선 세 대의 이전 서버를 새로운 하나의 iSeries 서버로 통합하여 처리를 시작합니다. iSeries 서버에 세 개의 논리 파티션을 작성합니다. 새로운 iSeries 서버에는 2793 내장 모뎀이 있습니다. 이는 PPP를 지원하는 유일한 입/출력 프로세서(IOP)입니다. 이전의 7852-400 전자 고객 지원(ECS) 모뎀도 있습니다.

상황

각 시스템이나 파티션이 자체 모뎀 없이, 복수 시스템과 파티션이 동일한 모뎀을 공유하여 전화 접속 연결을 할 수 있습니다. 이를 위해서는 송신 호출을 허용하는 L2TP 프로파일을 구성하고 L2TP 터널을 사용해야 합니다. 네트워크에서 터널은 가상 이더넷 네트워크 및 물리적 네트워크를 연결합니다. 물리적 회선은 네트워크의 다른 서버에 연결하며 모뎀을 공유하기도 합니다.

세부사항

다음 그림은 이 시나리오의 네트워크 특성을 보여 줍니다.



전제조건 및 가정

iSeries-A의 설치 요구사항은 다음과 같습니다.

- 비동기 통신이 가능한 모뎀이 있는 파티션에 설치된 OS/400 버전 5 릴리스 3 이상
- 파티션이 가능한 하드웨어
- Windows용 iSeries Access 및 iSeries Navigator(iSeries Navigator의 구성 및 서비스 구성요소), 버전 5 릴리스 3 이상
- 서버에 최소 두 개의 논리 파티션(LPAR)을 작성했습니다. 모뎀이 있는 파티션에는 OS/400 버전 5 릴리스 3 이상이 설치되어 있어야 합니다. 다른 파티션에는 OS/400 V5R2나 V5R3, Linux 또는 AIX가 설치되어 있어야 합니다. 이 시나리오에서는 파티션이 OS/400 또는 Linux 오퍼레이팅 시스템을 사용하고 있습니다.
- 파티션간에 통신하도록 작성된 가상 이더넷이 있습니다. 다음 시나리오인 파티션간 통신을 위한 가상 이더넷 네트워크 작성을 참조하십시오.

iSeries-B의 설치 요구사항은 다음과 같습니다.

- Windows용 iSeries Access 및 iSeries Navigator(iSeries Navigator의 구성 및 서비스 구성요소), 버전 5 릴리스 2 이상

구성 단계

다음 구성 타스크를 완료하십시오.

1. 모뎀이 있는 파티션의 인터페이스에 대한 L2TP 종료자 프로파일 작성

2. 10.1.1.74에서 L2TP 리모트 다이얼 프로파일 작성
3. 192.168.1.2에서 L2TP 리모트 다이얼 프로파일 작성
4. 연결 테스트

시나리오 세부사항: L2TP를 사용한 논리 파티션간 모뎀 공유

전제조건을 완료하면 L2TP 프로파일을 구성할 준비가 된 것입니다.

1단계: 모뎀이 있는 파티션의 인터페이스에 대한 L2TP 종료자 프로파일을 구성하십시오.

다음 단계를 따라 인터페이스의 종료자 프로파일을 작성하십시오.

1. iSeries Navigator에서 서버 --> **네트워크** --> **리모트 액세스 서비스**를 차례로 선택하십시오.
2. **수신자 연결 프로파일**을 마우스 오른쪽 버튼으로 클릭하고 **신규 프로파일**을 선택하십시오.
3. 설정 페이지에서 다음 옵션을 선택하고 **확인**을 클릭하십시오.
   - **프로토콜 유형**: PPP
   - **연결 유형**: L2TP(가상 회선)
   - **조작 모드**: 종료자(네트워크 서버)
   - **회선 서비스 유형**: 단일 회선
4. **신규 프로파일 -- 일반** 탭에서 다음 필드를 완료하십시오.
   - **이름**: toExternal
   - **설명**: 전화 걸기할 수신자 연결
   - **TCP로 프로파일 시작**을 선택하십시오.
5. **신규 프로파일 -- 연결** 탭에서 다음 필드를 완료하십시오.
   - **로컬 터널 종료점 IP 주소**: 모두
   - **가상 회선명**: toExternal.
     이 회선에는 연관된 물리적 인터페이스가 없습니다. 가상 회선은 이 PPP 프로파일의 다양한 특성에 대해 설명합니다. L2TP 회선 등록 정보 대화상자가 열립니다. 인증 탭을 클릭하고 서버의 호스트명을 입력하십시오. **확인**을 클릭하여 신규 PPP 프로파일 등록 정보 창의 연결 탭으로 돌아가십시오.
6. **나가는 호출 설정 허용**을 클릭하십시오. **나가는 호출 다이얼 등록 정보** 대화상자가 나타납니다.
7. **나가는 호출 다이얼 등록 정보** 페이지에서 회선 서비스 유형을 선택하십시오.
   - **회선 서비스 유형**: 회선 풀(pool)
   - **이름**: dialOut
   - **신규**를 클릭하십시오. 신규 회선 풀(pooll) 등록 정보 대화상자가 나타납니다.
8. 신규 회선 풀 등록 정보 대화상자에서, 나가는 호출에 허용할 회선과 모뎀을 선택하고 **추가**를 클릭하십시오. 이들 회선을 정의할 필요가 있으면 **신규 회선**을 선택하십시오. 이들 모뎀이 있는 파티션의 인터페이스는 이 회선 풀로부터 열려 있는 회선을 사용하려 시도합니다. 신규 회선 등록 정보 창이 나타납니다.
9. **신규 회선 프로파일 -- 일반** 탭에서 다음 필드에 정보를 입력하십시오.

- **이름**: line1
- **설명**: 라인 풀(pool)에 대한 첫 번째 회선 및 첫 번째 모뎀(2793 내장 모뎀)
- **하드웨어 자원**: cmn03(통신 포트)

10. 다른 모든 탭의 디폴트를 승인하고 **확인**을 클릭하여 신규 회선 등록 정보 창으로 돌아가십시오.
11. 신규 회선 풀 등록 정보 대화상자에서, 나가는 호출에 허용할 회선과 모뎀을 선택하고 **추가**를 클릭하십시오. 풀(pool)에 2793 모뎀이 선택되어 있는지 확인하십시오.
12. **신규 회선**을 다시 선택하여 7852-400 ECS 모뎀을 추가하십시오. 신규 회선 등록 정보 창이 나타납니다.
13. **신규 회선 프로파일 -- 일반** 탭에서 다음 필드에 정보를 입력하십시오.
    - **이름**: line2
    - **설명**: 라인 풀(pool)에 대한 두 번째 회선 및 두 번째 모뎀(7852-400 외장 ECS 모뎀)
    - **하드웨어 자원**: cmn04(V.24포트)
    - **프레이밍**: 비동기
14. **신규 회선 등록 정보 --모뎀** 탭에서, 외부 모뎀(7852-400)을 선택하고 **확인**을 클릭하여 신규 회선 등록 정보 창으로 돌아가십시오.
15. 회선 풀(poo)에 추가할 수 있는 다른 회선을 선택하고 **추가**를 클릭하십시오. 이 예에서는 위에서 추가한 두 개의 신규 모뎀이 *풀의 선택한 회선* 필드 아래에 나열되는지 확인하고 **확인**을 클릭하여 나가는 호출 다이얼 등록 정보 창으로 돌아가십시오.
16. 나가는 호출 다이얼 등록 정보 창에서 **디폴트 다이얼 번호**를 입력하고 확인을 클릭하여 신규 PPP 프로파일 등록 정보 창으로 돌아가십시오.

    주: 이러한 번호는 이들 모뎀을 사용하는 다른 시스템이 자주 호출하게 될 ISP와 같은 것일 수 있습니다. 다른 시스템이 *PRIMARY 또는 *BACKUP과 같은 전화 번호를 지정하는 경우, 다이얼한 실제 번호는 여기에 지정된 것입니다. 다른 시스템이 실제 전화 번호를 지정하면 이 전화 번호가 대신 사용됩니다.
17. **TCP/IP 설정** 탭에서 다음 값을 선택하십시오.
    - **로컬 IP 주소**: 없음
    - **리모트 IP 주소**: 없음

    주: L2TP 세션을 종료하기 위해 프로파일도 사용하고 있는 경우에는 iSeries 서버를 나타내는 로컬 IP 주소를 선택해야 합니다. 리모트 IP 주소의 경우, 서버와 동일한 서브네트에 있는 주소 풀(pool)을 선택할 수 있습니다. 모든 L2TP 세션은 이 풀(pool)에서 IP 주소를 확보합니다. 다른 고려사항은 다중 연결 프로파일 지원을 참조하십시오.
18. **인증** 탭에서 모든 디폴트 값을 채택하십시오.

이제 모뎀이 있는 파티션에서 L2TP 종료자 프로파일의 구성을 마쳤습니다. 다음 단계는 L2TP 리모트 다이얼 -- 10.1.1.74에 대한 발신자 프로파일을 구성하는 것입니다.

2단계: 10.1.1.74에서 L2TP 발신자 프로파일 구성

L2TP 발신자 프로파일을 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 10.1.1.74 --> **네트워크 --> 리모트 액세스 서비스**를 차례로 선택하십시오.
2. **발신자 연결 프로파일**을 마우스 오른쪽 버튼으로 클릭하고 **신규 프로파일**을 선택하십시오.
3. 설정 페이지에서 다음 옵션을 선택하고 **확인**을 클릭하십시오.
   - **프로토콜 유형**: PPP
   - **연결 유형**: L2TP(가상 회선)
   - **조작 모드**: 리모트 다이얼
   - **회선 서비스 유형**: 단일 회선
4. **일반** 탭에서 다음 필드를 완료하십시오.
   - **이름**: toModem
   - **설명**: 모뎀을 파티션할 발신자 연결
5. **연결** 탭에서 다음 필드를 완료하십시오.

   가상 회선명: toModem
   이 회선에는 연관된 물리적 인터페이스가 없습니다. 가상 회선은 이 PPP 프로파일의 다양한 특성에 대해 설명합니다. L2TP 회선 등록 정보 대화상자가 열립니다.
6. **일반** 탭에서 가상 회선에 대한 설명을 입력하십시오.
7. **인증** 탭에서 파티션의 로컬 호스트명을 입력하고 **확인**을 클릭하여 **연결** 페이지로 돌아가십시오.
8. **리모트 전화 번호** 필드에 *PRIMARY 및 *BACKUP을 추가하십시오. 그러면 모뎀이 있는 파티션의 종료자 프로파일과 동일한 전화 번호를 프로파일에서 사용할 수 있습니다.
9. **리모트 터널 종료점 호스트명 또는 IP 주소** 필드에 리모트 터널 종료점 주소(10.1.1.73)를 입력하십시오.
10. **인증** 탭에서 **리모트 시스템에 이 iSeries 서버의 ID 확인 허용**을 선택하십시오.
11. 사용할 인증 프로토콜 아래에서 **필수 암호화 암호(CHAP-MD5)**를 선택하십시오. 디폴트로 **확장 가능한 인증 프로토콜 허용**도 선택됩니다.

    주: 프로토콜은 다이얼링하고 있는 서버에서도 사용하는 프로토콜과 일치해야 합니다.
12. 사용자명과 암호를 입력하십시오.

    주: 사용자명과 암호는 다이얼링하고 있는 서버에 유효한 사용자명 및 암호와 일치해야 합니다.
13. **TCP/IP 설정** 탭으로 이동하여 필요한 필드를 확인하십시오.
    - **로컬 IP 주소**: 리모트 시스템에서 할당함
    - **리모트 IP 주소**: 리모트 시스템에서 할당함
    - **라우팅**: 추가 라우팅이 필요없음
14. **확인**을 클릭하여 PPP 프로파일을 저장하십시오.

3단계: 192.168.1.2에 대한 L2TP 리모트 다이얼 프로파일 구성

2단계를 반복하십시오. 그러나 리모트 터널 종료점 주소를 192.168.1.3(iSeries B가 연결하는 실제 인터페이스)으로 변경하십시오.

주: 이들은 가상 IP 주소로서 예시용으로만 사용됩니다.

4단계: 연결 테스트

두 서버 모두의 구성을 완료한 후, 연결을 테스트하여 시스템이 모뎀을 공유해서 외부 네트워크에 도달하는지 확인해야 합니다. 이를 위해 다음 단계를 따르십시오.

1. L2TP 종료자 프로파일이 사용 중인지 확인하십시오.
   a. iSeries Navigator에서 10.1.1.73 --> **네트워크 --> 리모트 액세스 서비스** --> **수신자 연결 프로파일**을 차례로 선택하십시오.
   b. 오른편 분할 창에서, 원하는 프로파일(toExternal)을 찾은 다음 **상태** 필드가 *사용 중*인지 확인하십시오. 그렇지 않은 경우, 프로파일을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오.
2. 10.1.1.74에서 리모트 다이얼 프로파일을 시작하십시오.
   a. iSeries Navigator에서 10.1.1.74 --> **네트워크 --> 리모트 액세스 서비스** --> **발신자 연결 프로파일**을 차례로 선택하십시오.
   b. 오른편 분할 창에서, 원하는 프로파일(toModem)을 찾은 다음 **상태** 필드가 *사용 중*인지 확인하십시오. 그렇지 않은 경우, 프로파일을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오.
3. iSeries B에서 리모트 다이얼 프로파일을 시작하십시오.
   a. iSeries Navigator에서 192.168.1.2 --> **네트워크 --> 리모트 액세스 서비스** --> **발신자 연결 프로파일**을 차례로 선택하십시오.
   b. 오른편 분할 창에서, 작성한 프로파일을 찾은 다음 **상태** 필드가 *사용 중*인지 확인하십시오. 그렇지 않은 경우, 프로파일을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오.
4. 가능하면 다이얼한 ISP 또는 다른 목적지를 핑하여 두 프로파일이 모두 사용 중인지 확인하십시오. 10.1.1.74 및 192.168.1.2 모두에서 핑을 시도합니다.
5. 다른 방법으로, 연결 상태를 검사할 수도 있습니다.
   a. iSeries Navigator에서 원하는 서버(예를 들어, 10.1.1.73) --> **네트워크 --> 리모트 액세스 서비스** --> **발신자 연결 프로파일**을 차례로 선택하십시오.
   b. 오른편 분할 창에서 작성한 프로파일을 마우스 오른쪽 버튼으로 클릭하고 **연결**을 선택하십시오. 연결 상태 창에서 어느 프로파일이 활동, 비활동, 연결 중 등의 상태를 볼 수 있습니다.

부록. 주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서는 이 자료에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급하는 것이 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

2바이트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM 고객만족센터에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다. IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 일체의 보증없이 이 책을『현상태대로』제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 언제든지 이 책에서 설명한 제품 및/또는 프로그램을 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이센스 사용자는 다음 주소로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

이러한 정보는 해당 조건(예를 들어, 사용료 지불 등)에 따라 사용될 수 있습니다.

이 정보에 기술된 라이센스가 있는 프로그램 및 이 프로그램에 대해 사용 가능한 모든 라이센스가 있는 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA), 기계 코드에 대한 IBM 라이센스 계약 또는 이와 동등한 계약에 따라 제공한 것입니다.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 레벨 상태의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한, 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 사용자의 특정 환경에서 검증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 다른 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 비IBM 제품을 테스트하지 않았으므로, 이들 제품과 관련된 성능의 정확성, 호환성 또는 기타 주장에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지없이 변경될 수 있습니다.

표시된 모든 IBM 제품 가격은 IBM에서 제안한 현재 소매 가격이며 통지없이 변경될 수 있습니다. 실제 판매가는 다를 수 있습니다.

이 정보는 계획 수립 목적으로만 사용됩니다. 이 정보는 기술된 제품이 GA(General Availability)되기 전에 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이 예제에는 가능한 완벽하게 개념을 설명하기 위해 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

이 정보를 소프트카피로 확인하는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 상표입니다.

e(로고)Server
IBM
iSeries
Operating System/400
OS/400
400

Microsoft®, Windows, Windows NT®, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

Java 및 모든 java 기반 상표는 미국 또는 기타 국가에서 사용되는 Sun Microsystems, inc.의 상표입니다.

기타 회사, 제품, 서비스 이름은 해당 회사의 상표 또는 서비스표입니다.

서적 다운로드 및 인쇄 조건

귀하가 다운로드하려는 정보를 사용하는 데에는 다음의 조건이 적용되며 귀하가 이를 승인하는 경우에 해당 정보를 사용할 수 있습니다.

개인적인 사용: 일체의 소유권 표시를 하는 경우에 한하여 귀하는 이들 정보를 개인적이며 비상업적인 용도로 복제할 수 있습니다. 귀하는 IBM의 명시적인 동의없이 해당 정보에 대한 2차적 저작물 또는 그 일부를 배포, 전시 또는 작성할 수 없습니다..

상업적 사용: 일체의 소유권 표시를 하는 경우에 한하여 이러한 정보를 사업장 내에서만 복제, 배포 및 전시할 수 있습니다. 귀하는 IBM의 명시적인 동의없이 귀하의 사업장 이외에서 해당 정보의 2차적 저작물을 작성할 수 없으며 이들 정보 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

본 계약에서 명시하지 않는 한, 정보 또는 모든 데이터, 소프트웨어 또는 기타 지적 재산권에 대하여 다른 허가나 라이센스 또는 권리가 부여되지 않습니다.

해당 정보의 사용이 IBM에게 손해를 가져오거나, 상기 지시사항이 적절하게 준수되지 않은 것으로 판단한 경우, IBM은 본 계약에서 부여한 정보에 대해 허가를 취소할 권리가 있습니다.

귀하는 미국 수출법 및 관련 규정을 포함하여 모든 적용 가능한 법률 및 규정을 철저히 준수하지 않는 경우 본 정보를 다운로드, 송신 또는 재송신할 수 없습니다. IBM은 이들 정보의 내용과 관련하여 어떠한 보증도 하지 않습니다. 본 서적은 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 일체의 보증없이 ″현상태대로″ 제공됩니다.

귀하는 본 사이트로부터 정보를 다운로드하거나 인쇄함으로써 본 조건에 동의한 것으로 간주됩니다.