

IBM

@server

iSeries

네트워킹 TCP/IP 설정

버전 5 릴리스 3





@server

iSeries

네트워킹 TCP/IP 설정

버전 5 릴리스 3

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 65 페이지의 『주의사항』의 정보를 읽으십시오.

제 7 판(2005년 8월)

| 이 개정판은 개 새정판에 별도로 명시하지 않는 한 Operating System/400®(5722-SS1)의 버전 5, 릴리스 3, 수정 0 및 모든 후속
| 릴리스와 수정에 적용됩니다. 이 버전은 모든 축약 명령어 세트 컴퓨터(RISC) 모델에서 실행되는 것이 아니며 CICS® 모델에서도 실행
| 되지 않습니다.

© Copyright International Business Machines Corporation 1998, 2005. All rights reserved.

목차

제 1 부 TCP/IP 설정	1	제 7 장 iSeries Navigator로 TCP/IP 사용자 정의	39
제 1 장 V5R3의 새로운 사항	3	제 8 장 가상 이더넷을 외부 LAN에 연결하는	
제 2 장 이 주제 인쇄	5	TCP/IP 기술.	43
제 3 장 IPv6(인터넷 프로토콜 버전 6)	7	프록시 ARP 메소드	44
IPv6 정보	7	1단계: 논리 파티션이 가상 이더넷에 참여할 수	
사용할 수 있는 IPv6 기능.	8	있도록 설정	45
시나리오: IPv6	9	2단계: 이더넷 회선 설명 작성	45
IPv6 근거리 통신망(LAN) 작성	9	3단계: IP 데이터그램 이송 켜기	47
IPv4 근거리 통신망(LAN)을 통한 IPv6 패킷 송		4단계: 프록시 ARP를 작동할 수 있게 하는 인터	
신	11	페이스 작성	47
IPv4 광역 네트워크(WAN)를 통한 IPv6 패킷 송		5단계: 파티션 A에 가상 TCP/IP 인터페이스 작성	48
신	13	6단계: 파티션 B에 가상 TCP/IP 인터페이스 작성	48
개념: IPv6	15	7단계: 라우트 작성.	49
IPv6 주소 형식	16	8단계: 네트워크 통신 확인	49
IPv6 주소 유형	17	네트워크 주소 변환 방법	50
IPv6 터널링	18	1단계: 논리 파티션이 가상 이더넷에 참여할 수	
인접 노드 발견	18	있도록 설정	51
상태 없는 주소 자동 구성	19	2단계: 이더넷 회선 설명 작성	51
IPv4와 IPv6 비교	19	3단계: IP 데이터그램 이송 켜기	53
IPv6 문제 해결	26	4단계: 인터페이스 작성	53
IPv6 관련 정보	26	5단계: 네트워크 통신 확인	55
제 4 장 TCP/IP 설정 계획.	27	6단계: 패킷 규칙 작성.	55
TCP/IP 설정 요구사항.	27	7단계: 네트워크 통신 확인	55
TCP/IP 보안 고려사항	28	TCP/IP 라우팅 메소드.	56
제 5 장 TCP/IP 설치	29	1단계: 논리 파티션이 가상 이더넷에 참여할 수	
제 6 장 TCP/IP 구성	31	있도록 설정	57
처음으로 TCP/IP 구성.	31	2단계: 이더넷 회선 설명 작성	57
EZ-Setup 마법사를 사용하여 TCP/IP 구성.	31	3단계: IP 데이터그램 이송 켜기	59
문자 기반의 인터페이스를 사용하여 TCP/IP 구성		4단계: 인터페이스 작성	59
IPv6 구성.	35	가상 이더넷 고려사항	60
설정 요구사항	35	제 9 장 TCP/IP 설정 관련 정보	61
IPv6 구성 마법사를 사용한 IPv6 구성	35	제 2 부 부록	63
오퍼레이팅 시스템이 제한 상태에 있을 때 TCP/IP		부록. 주의사항	65
구성.	36	상표.	66
		서적의 다운로드 및 인쇄 조건	67

제 1 부 TCP/IP 설정

서버를 사용할 준비가 완료되었습니다. 이 주제는 OS/400®에서 TCP/IP 구성에 대한 톨과 프로시듀어를 제공합니다. 예를 들어, 이 정보를 사용하여 회선 설명, TCP/IP 인터페이스 및 라우트를 작성할 수 있습니다. iSeries™ Navigator를 사용하여 TCP/IP 구성을 사용자 정의하는 방법을 찾고, 사용자 네트워크를 들어오고 나가는 자료의 경로를 지정할 수 있는 다양한 TCP/IP 기술에 대해 배우십시오.

이 정보를 사용하여 TCP/IP를 구성하기 전에 하드웨어 설치 및 사용을 참조하여 모든 필요한 하드웨어 구성 요소를 설치했는지 확인하십시오. TCP/IP 구성에 대한 초기 타스크를 완료했으면 TCP/IP 어플리케이션, 프로토콜 및 서비스로 서버의 기능을 확장하여 사용자의 고유한 수요를 충족시킬 준비가 되었습니다.

V5R3의 새로운 사항

새롭게 변경된 TCP/IP 기능을 설명합니다.

이 주제 인쇄

이 주제를 참조하여 TCP/IP 설정 문서의 PDF 버전을 인쇄하거나 다운로드하십시오.

IPv6(인터넷 프로토콜 버전 6)

새로운 인터넷 프로토콜인 IPv6은 인터넷의 미래에 중요한 역할을 하며, iSeries 서버에서 IPv6을 사용할 수 있습니다. 이 주제에서는 IPv6에 대한 일반 정보와 IPv6가 iSeries 서버에서 어떤 식으로 구현되는지에 대해 설명합니다.

TCP/IP 설정 계획

이 주제는 iSeries 서버에 TCP/IP를 설치하고 구성하는 준비를 도와줍니다. TCP/IP 구성을 시작할 때 필요한 모든 정보를 갖추도록 설치 및 구성을 위한 기본 요구사항을 제공합니다. 관련 용어 및 개념을 위한 참조서도 제공됩니다.

TCP/IP 설치

이 주제는 iSeries 서버의 작동을 준비하는 제품 설치 단계를 안내합니다.

TCP/IP 구성

이 주제에서는 iSeries를 사용하고 TCP/IP를 구성하는 방법을 보여줍니다. IPv6 구성을 위한 지침 역시 참조하십시오.

iSeries Navigator로 TCP/IP 사용자 정의

이 주제에서는 iSeries Navigator를 사용할 때의 사용자 정의 옵션을 제공합니다.

가상 이더넷 상의 TCP/IP 기술

OS/400에서 가상 이더넷을 활용하는 방법을 확인하십시오.

TCP/IP 문제 해결

TCP/IP 연결이나 통신에 문제가 발견되면 TCP/IP 문제 해결을 참조하여 솔루션을 찾는데 도움을 받으십시오. 이 문제 해결 안내서는 IPv4 및 IPv6에 관련된 문제점 해결을 돕습니다.

TCP/IP 설정 관련 정보

이 주제는 "이 기능으로 추가로 할 수 있는 일은 무엇일까?"라는 질문에 대한 답으로 생각할 수 있습니다. 서버의 성능을 확장시키는 어플리케이션 및 서비스에 대한 참조서를 찾아보십시오.

제 1 장 V5R3의 새로운 사항



TCP/IP 설정 개선 사항

가상 이더넷을 사용하여 파티션이 서로 통신할 수 있게 하려는 경우, 해당 통신을 외부의 실제 LAN으로 확장해야 할 수 있습니다. 가상 이더넷을 외부 LAN에 연결하는 TCP/IP 기술을 참조하여 가상 이더넷 네트워크를 외부 LAN에 연결하는 방법을 배우십시오. 이 정보를 사용하여 가상 이더넷 네트워크에서 외부 LAN으로 네트워크 통신을 브릿지하기 위한 세 가지 방법을 보여주는 예를 검토하십시오.

이 릴리스에서 새로운 사항이나 변경된 사항에 대한 기타 정보를 찾으려면 사용자 메모를 참조하십시오.

새로운 사항 또는 변경된 사항 참조 방법

기술적인 변경 사항을 표시하기 위해 본 정보는 다음과 같은 이미지를 사용합니다.

-  이미지: 새 정보나 변경된 정보가 시작됨을 표시합니다.
-  이미지: 새 정보나 변경된 정보가 끝남을 표시합니다.


제 2 장 이 주제 인쇄


이 문서의 PDF 버전을 보거나 다운로드하려면 TCP/IP 설정(약 362KB)을 선택하십시오.

기타 정보


다음 PDF도 보거나 인쇄할 수 있습니다.

• 매뉴얼:

– **TCP/IP Configuration and Reference**  (592KB)
이 책에는 TCP/IP를 구성하고 네트워크를 운영 및 관리하는데 대한 정보가 수록되어 있습니다.

– **iSeries 보안을 위한 추가 정보 및 툴**  (1MB)
이 책에는 서버 및 연관된 운영을 보호하기 위해 iSeries의 보안 피처를 사용하는데 대한 기본 권장사항이 수록되어 있습니다.

• 레드북™:

– **TCP/IP Tutorial and Technical Overview**  (7MB)
이 레드북에는 TCP/IP의 기본에 대한 정보가 수록되어 있습니다.


– **TCP/IP for AS/400®: More Cool Things Than Ever**  (9MB)
이 책에는 일반적인 TCP/IP 어플리케이션 및 서비스의 방대한 리스트가 들어 있습니다.

PDF 파일 저장

워크스테이션에 PDF를 저장하려면 다음을 수행하십시오.

1. 브라우저에서 PDF를 마우스 오른쪽 버튼으로 클릭하십시오(위의 링크를 마우스 오른쪽 버튼으로 클릭).
2. Internet Explorer를 사용하는 경우 다른 이름으로 대상 저장...을 클릭하십시오. Netscape Communicator를 사용하는 경우 다른 이름으로 링크 저장...을 클릭하십시오.
3. PDF를 저장할 디렉토리로 가십시오.
4. 저장을 클릭하십시오.

Adobe Acrobat Reader 다운로드

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

제 3 장 IPv6(인터넷 프로토콜 버전 6)

IPv6(인터넷 프로토콜 버전 6)은 인터넷 프로토콜 버전 4(IPv4)의 갱신된 버전이며 인터넷 표준으로서 IPv4를 점진적으로 대체하고 있습니다.

사용자는 IPv6를 사용하여 어떤 식으로 회사의 e-business를 향상시킬 수 있는지 궁금해 할 수도 있고, 회사에서 이러한 향상된 인터넷 프로토콜의 혜택을 누릴 수 있도록 IPv6 어플리케이션을 작성하려는 프로그래머일 수도 있습니다. IPv6에 관한 기본 정보 및 iSeries 서버에서 IPv6을 사용하는 방법에 대해서는 이 주제를 읽으십시오.

IPv6 정보

IPv6이 인터넷 표준으로서 IPv4를 대체하고 있는 이유 및 이를 사용하는 장점에 대해 설명합니다.

사용할 수 있는 IPv6 기능

IPv6이 iSeries 서버에서 현재 어떤 식으로 구현되고 있는지에 대해 설명합니다.

IPv6 시나리오

어떠한 비즈니스 상황에서 IPv6을 사용할 지에 대한 이해를 돕는 예를 제공합니다.

IPv6 개념

기본 IPv6 개념을 설명합니다. IPv4와 IPv6 사이의 차이점을 확실히 모르는 경우에는 IPv4 주소와 IPv6 주소를 서로 비교하는 방법이나 IPv4 패킷 헤더와 IPv6 패킷 헤더를 구분하는 방법과 같은 상세한 비교 정보를 참조하십시오.

IPv6 구성

서버에 IPv6을 구성하기 위한 소프트웨어 요구사항 및 지침을 설명합니다.

IPv6 문제 해결

IPv6 문제점에 대한 솔루션을 설명합니다.

IPv6 관련 정보

IPv6의 이해를 돕는 자원에 대한 링크가 수록되어 있습니다.

IPv6 정보

IPv6(인터넷 프로토콜 버전 6)은 차세대 인터넷 프로토콜입니다. 대부분의 인터넷이 현재 IPv4를 사용하며, 이 프로토콜은 20년 동안 신뢰할 수 있었으며 탄력적이었습니다. 그러나, IPv4에는 인터넷이 확대되면서 많은 문제점을 야기시키는 심각한 제한사항이 있습니다.

특히, 인터넷에 추가되는 모든 새로운 장치에 필요한 IPv4 주소의 부족 현상이 날로 심각해지고 있습니다. IPv6 확장 기능의 핵심은 IP 주소를 32비트에서 128비트로 확장하여 실제로 무한대의 고유한 IP 주소를 가능하게 하는 것입니다. 새로운 IPv6 주소 텍스트 형식은 다음과 같습니다.

```
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
```

여기서 각 x는 4비트를 나타내는 16진수입니다.

IPv6의 확장된 주소지정 기능은 주소 고갈 문제점에 대한 솔루션을 제공합니다. 이는 더 많은 사람들이 모바일 전화 및 핸드헬드 컴퓨터와 같은 모바일 컴퓨터를 사용함에 따라 특히 중요한 사항입니다. 증가하는 무선 사용자의 요구가 IPv4 주소 고갈의 원인이 되었습니다. IPv6의 확장된 IP 주소 기능은 점점 더 늘어나는 무선 장치에 충분한 IP 주소를 제공함으로써 이러한 문제점을 해결합니다.

이러한 주소지정 기능외에, IPv6은 네트워크상의 주소 구성 및 관리 작업을 간단하게 해주는 새로운 기능을 제공합니다. 네트워크를 구성하고 유지보수하는 일은 노동 집약적인 활동입니다. IPv6은 여러가지 네트워크 관리자의 작업을 자동화시켜 일부 작업부하를 줄여줍니다.

IPv6을 사용하는 경우에는 다른 인터넷 서비스 제공자(ISP)로 변경할 때 장치 주소의 번호를 다시 정할 필요가 없습니다. 주소가 전세계적으로 고유하므로 동일한 주소를 따를 수 있습니다.

IPv6 자동 구성 피처는 인터페이스 및 라우터 주소를 자동으로 구성합니다. 상태 없는 자동 구성에서, IPv6은 기계의 MAC 주소와 로컬 노드에서 제공된 네트워크 접두부를 취해 이 두 주소를 결합하여 새로운 고유 IPv6 주소를 작성합니다. 이 피처를 사용하면 DHCP 서버가 필요하지 않으므로 관리자의 시간과 회사의 비용을 절감시켜 줍니다.

IPv6에 관한 정보 소스는 IPv6 관련 정보를 참조하십시오.

iSeries 서버에 특별히 관련된 IPv6 정보는 사용할 수 있는 IPv6 기능을 참조하십시오.

사용할 수 있는 IPv6 기능

IBM®은 몇몇 소프트웨어 릴리스에서 iSeries 서버에 IPv6을 구현하고 있습니다. IPv6은 현재 IPv6 어플리케이션 개발 및 테스트 용도로 어플리케이션 개발 플랫폼에서 구현됩니다. IPv6 기능은 기존 TCP/IP 어플리케이션에 대해 투명하며 IPv4 기능과 공존합니다.

IPv6의 영향을 받는 기본 iSeries 서버 기능은 다음과 같습니다.

- 구성

IPv6의 구성 프로세스가 IPv4의 구성 프로세스와 다르다는 것을 명심하십시오. IPv6 기능을 사용하려면 IPv6용 회선을 구성하여 서버의 TCP/IP 구성을 변경해야 합니다. 이더넷 회선이나 터널 회선에 IPv6을 구성할 수도 있습니다.

IPv6 통신용으로 이더넷 회선을 구성하면 IPv6 네트워크를 통해 IPv6 패킷을 송신합니다. IPv6 근거리 통신망(LAN) 작성에서 IPv6용 이더넷 회선을 구성할 상황에 대해 설명하는 시나리오를 참조하십시오.

터널 회선을 구성하면 기존 IPv4 네트워크를 통해 IPv6 패킷을 송신합니다. IPv4 근거리 통신망(LAN)을 통한 IPv6 패킷 송신 및 IPv4 광역 네트워크(WAN)를 통한 IPv6 패킷 송신에서 IPv6용으로 구성된 터널 회선을 작성하는 두 가지 상황에 대해 설명하는 시나리오를 참조하십시오.

IPv6 구성을 참조하여 IPv6용 네트워크를 구성하십시오.

- **소켓**

IPv6 API 및 툴을 사용하여 소켓 어플리케이션을 개발하고 테스트하십시오. IPv6은 어플리케이션이 새로운 주소 그룹인 AF_INET6을 사용하는 IPv6을 사용할 수 있도록 소켓을 향상시킵니다. 이러한 확장 기능은 기존 IPv4 어플리케이션에 영향을 미치지 않습니다. IPv4와 IPv6 통신을 동시에 지원하거나 IPv6 통신만 지원하는 어플리케이션을 작성할 수도 있습니다. 소켓용 IPv6에 대한 자세한 정보는 AF_INET6 주소 그룹 사용을 참조하십시오.

- **DNS**

정의역명 시스템(DNS)은 AAAA 주소 및 반전 찾아보기를 위한 새로운 도메인인 IP6.ARPA를 지원합니다. DNS가 IPv6 정보를 검색하지만 서버는 IPv4를 사용하여 DNS와 통신해야 합니다.

- **TCP/IP 문제 해결**

IPv6 네트워크 및 터널에 대해 PING, netstat, 라우트 추적 및 통신 추적과 같은 표준 문제 해결 툴을 사용하십시오. 이러한 툴이 이제 IPv6 주소 형식을 지원합니다. IPv4 및 IPv6 네트워크에 대한 문제점 해결에 TCP/IP 문제 해결을 참조하십시오.

IPv6상의 자원에 대해서는 IPv6 관련 정보를 참조하십시오.

시나리오: IPv6

다음 시나리오를 검토하여 IPv6을 구현해야 하는 이유와 각 상황에서 네트워크를 설정하는 방법에 대해 이해하십시오.

- IPv6 근거리 통신망(LAN) 작성
- IPv4 근거리 통신망(LAN)을 통한 IPv6 패킷 송신
- 광역 네트워크(WAN)를 통한 IPv6 패킷 송신

주: 시나리오에서 IP 주소 10.x.x.x는 공용 IP 주소를 나타냅니다. 이 시나리오에서 사용된 모든 주소는 단지 예를 보여주기 위한 것입니다.

IPv6 구성을 참조하여 IPv6용 서버를 구성하십시오.

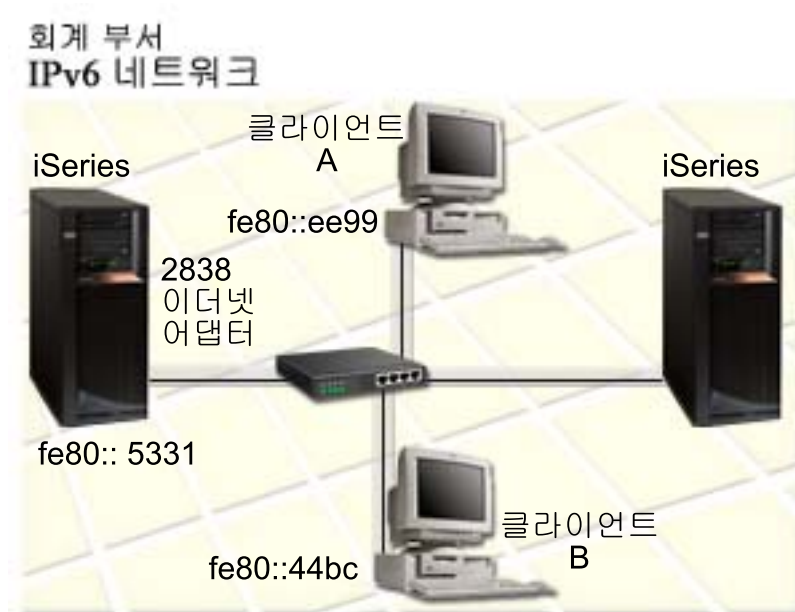
기본 IPv6 개념에 대한 정의는 IPv6 개념을 참조하십시오.

IPv6 근거리 통신망(LAN) 작성

상황

IPv6은 결국 인터넷 표준으로서 IPv4를 대체할 것입니다. 그 결과, 귀사는 재정 운영에 IPv6을 구현하고 연결을 위해 IPv6을 사용하는 새로운 회계 어플리케이션을 구입하기로 결정합니다. 어플리케이션을 사이트 인터넷

근거리 통신망(LAN)에 연결된 다른 서버상에 있는 어플리케이션의 또 다른 인스턴스와 연결해야 합니다. 귀하는 귀사에서 회계 어플리케이션을 시작할 수 있도록 IPv6용으로 서버를 구성해야 합니다. 다음 그림은 이 시나리오의 네트워크 설정을 보여줍니다.



솔루션

IPv6 LAN을 작성하려면 IPv6용 이더넷 회선 설명을 구성해야 합니다. 직원들이 회계 어플리케이션을 사용할 때 iSeries 서버와 네트워크상의 클라이언트들 사이에서 IPv6 패킷이 이동합니다.

설정 요구사항에는 다음과 같은 항목이 포함됩니다.

- OS/400 버전 5 릴리스 2 이상
- 2838 또는 2849 이더넷 어댑터(현재 IPv6용으로 지원되는 유일한 하드웨어 자원 유형)
- Windows®용 iSeries Access 및 iSeries Navigator(iSeries Navigator의 네트워크 구성요소)
- TCP/IP가 서버에서 실행 중이어야 하므로 IPv6용 이더넷 터널 회선을 구성하기 전에 별도의 IPv4 물리적 인터페이스가 구성되어 있어야 합니다. IPv4용 서버를 구성하지 않았으면 IPv6용 회선을 구성하기 전에 처음으로 TCP/IP 구성을 참조하십시오.

구성

IPv6용 이더넷 회선 설명을 구성하려면 iSeries Navigator에서 **IPv6** 구성 마법사를 사용해야 합니다. IPv6은 iSeries Navigator에서만 구성 가능할 것이며, 문자 기반의 인터페이스에서는 구성 가능하지 않을 수도 있습니다.

마법사는 IPv6이 구성될 서버상의 하드웨어 통신 자원의 이름(예를 들어, CMN01)을 필요로 합니다. 이는 현재 IPv4용으로 구성되어 있지 않은 2838 또는 2849 이더넷 어댑터여야 합니다.

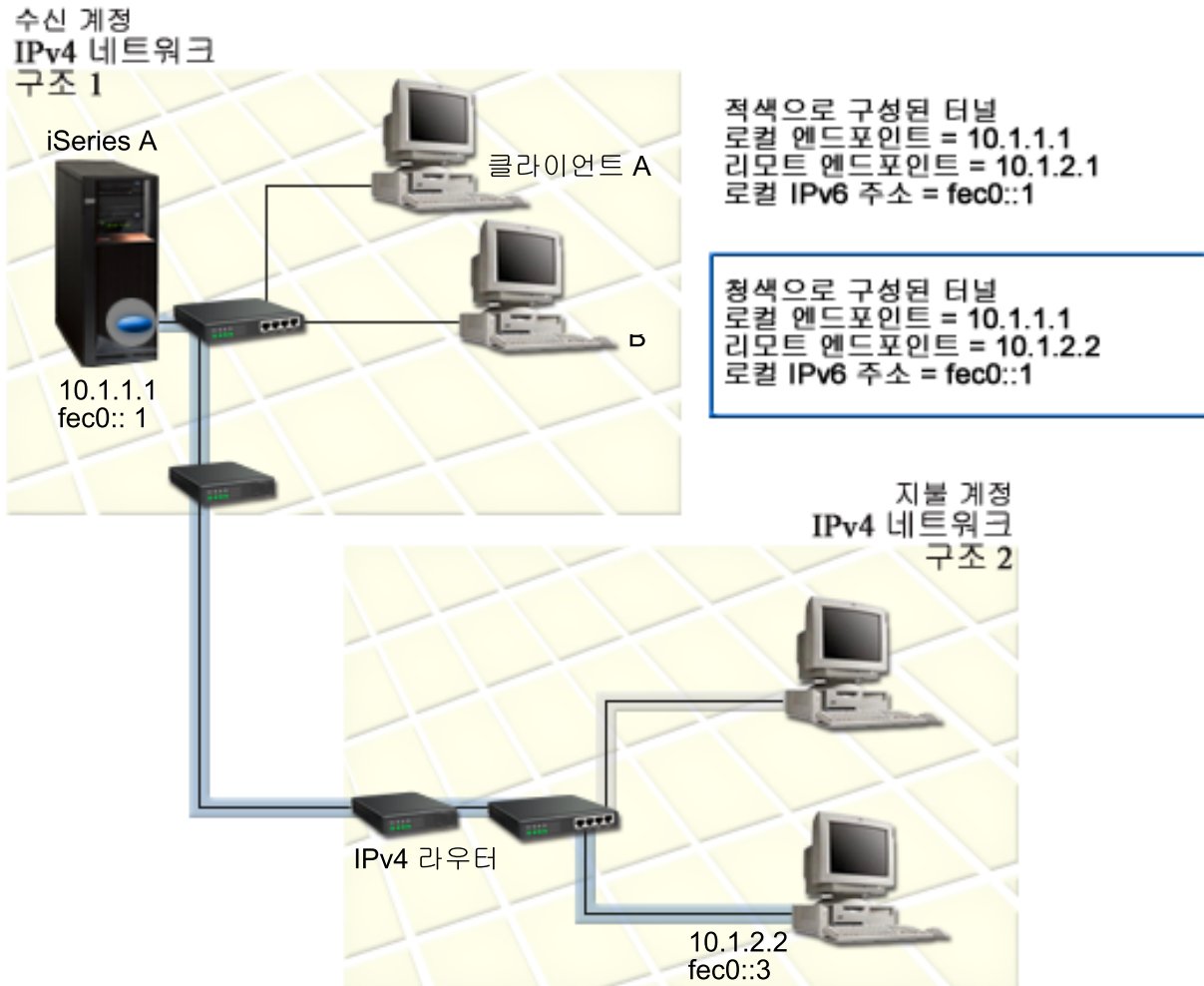
IPv6 구성 마법사를 사용하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> TCP/IP 구성을 선택하십시오.
2. IPv6을 마우스 오른쪽 버튼으로 클릭하고 IPv6 구성을 선택한 후 마법사의 지침에 따라 IPv6용 인터넷 회선을 구성하십시오.

IPv4 근거리 통신망(LAN)을 통한 IPv6 패킷 송신

상황

귀사에서 새로운 IPv6 회계 어플리케이션을 작성했습니다. 이는 로컬에서 사용할 서버 대 클라이언트 어플리케이션입니다. 어플리케이션은 동일한 사이트에 위치하지만 다른 빌딩이나 LAN에 있는 자신의 다른 인스턴스와 통신합니다. 귀사에서 이 어플리케이션에 IPv6을 사용하려 하지만 전체 IPv4 인프라구조를 IPv6으로 변경할 준비가 되어 있지 않습니다. 귀하는 IPv6 패킷이 로컬 IPv4 네트워크를 통해 실행할 수 있도록 IPv6 터널을 구성해야 합니다. 다음 그림은 이 시나리오의 네트워크 설정을 보여줍니다.



솔루션

로컬 IPv4 네트워크를 통해 IPv6을 사용하려면 두 개의 구성된 터널과 여러 개의 연관 라우트를 작성해야 합니다. 예를 보여주기 위해 한 터널은 빨간색으로 그려져 있고 다른 터널은 파란색으로 그려져 있습니다.

먼저, 빨간색 터널을 보십시오.

- 빨간색 터널은 빌딩 1에 있는 iSeries A(로컬 종료점 10.1.1.1)에서 시작하여 빌딩 2에 있는 클라이언트 C(리모트 종료점 10.1.2.1)에서 끝납니다.
- iSeries A는 IPv4 패킷 내에 IPv6 패킷을 캡슐화하여 터널을 통해 클라이언트 C로 IPv4 패킷을 송신하며, 클라이언트 C는 IPv6 패킷을 디캡슐화하여 IPv6 어플리케이션의 또 다른 인스턴스에 연결할 수도 있습니다.

다음에는 파란색 터널을 보십시오.

- 파란색 터널은 빨간색 터널처럼 빌딩 1에 있는 iSeries A(로컬 종료점 10.1.1.1)에서 시작하지만 빌딩 2에 있는 클라이언트 D(리모트 종료점 10.1.2.2)에서 끝납니다.
- iSeries A는 IPv4 패킷 내에 IPv6 패킷을 캡슐화하여 터널을 통해 클라이언트 D로 IPv4 패킷을 송신하며, 클라이언트 D는 IPv6 패킷을 디캡슐화하여 IPv6 어플리케이션의 또 다른 인스턴스에 연결할 수도 있습니다.

각 터널 연결은 지점 간이므로 각 터널에 대한 리모트 종료점을 정의해야 합니다. 이를 위해서는 두 개의 라우트를 작성합니다. 각 라우트는 동일한 터널 회선에 연관되지만 다음 홉(hop)에서 서로 다른 리모트 종료점을 정의합니다. 즉, 라우트를 작성하면서 각 터널의 리모트 종료점을 정의합니다.

터널 종료점을 정의하고 패킷이 빌딩 2에 있는 클라이언트에 도달할 수 있도록 허용하는 초기 라우트를 작성하는 것 외에, 패킷이 빌딩 1에 있는 서버에 리턴할 수 있도록 두 개의 라우트를 더 작성해야 합니다.

설정 요구사항에는 다음과 같은 항목이 포함됩니다.

- OS/400 버전 5 릴리스 2 이상
- Windows용 iSeries Access 및 iSeries Navigator(iSeries Navigator의 네트워크 구성요소)
- 구성된 터널 회선을 작성하기 전에 서버에 TCP/IP(IPv4 사용)를 구성해야 합니다. IPv4용 서버를 구성하지 않았으면 IPv6용 회선을 구성하기 전에 처음으로 TCP/IP 구성을 참조하십시오.

구성

구성된 터널 회선을 작성하려면 iSeries Navigator에서 **IPv6** 구성 마법사 및 새 **IPv6** 라우트 마법사를 사용해야 합니다. IPv6은 iSeries Navigator에서만 구성 가능할 것이며, 문자 기반의 인터페이스에서는 구성 가능하지 않을 수도 있습니다.

IPv6 구성 마법사를 사용하여 빨간색 터널 회선을 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> **TCP/IP** 구성을 선택하십시오.

2. **IPv6**을 마우스 오른쪽 버튼으로 클릭하고 **IPv6** 구성 마법사의 지침에 따라 IPv6용 터널 회선을 구성하십시오. **IPv6** 구성 마법사를 완료하고 나면 구성된 터널 회선에 대한 새 라우트를 구성하라고 프롬프트하며, 새 **IPv6** 라우트 마법사 대화가 나타납니다. IPv6 패킷이 빨간색 터널을 통해 이동할 수 있도록 새 라우트를 작성해야 합니다.
3. 새 **IPv6** 라우트 마법사에서 빨간색 터널에 대한 라우트를 작성하십시오. 다음 홉(hop)으로 리모트 종료점 10.1.2.1을 지정하고 목적지 주소로 fec0::2를 지정하십시오.

새 **IPv6** 라우트 마법사를 다시 사용하여 파란색 터널에 대한 라우트를 작성하십시오. **IPv6** 구성 마법사를 사용하여 파란색 터널을 작성할 필요는 없습니다. 파란색 터널은 새 **IPv6** 라우트 마법사를 사용하여 리모트 종료점을 정의할 때 작성됩니다. 새 **IPv6** 라우트 마법사를 사용하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> TCP/IP 구성 --> **IPv6**을 선택하십시오.
2. 라우트를 마우스 오른쪽 버튼으로 클릭하고 새 라우트를 선택한 후 마법사의 지침에 따라 파란색 터널에 대한 IPv6 라우트를 구성하십시오. 다음 홉(hop)으로 리모트 종료점 10.1.2.2을 지정하고 목적지 주소로 fec0::3을 지정하십시오.

구성된 터널 회선 및 터널 종료점을 정의하는 라우트를 작성한 후에는 클라이언트 C에 라우트를 작성하고 빌딩 1에 있는 서버로 패킷을 다시 이동시키는 라우트를 클라이언트 D에 작성해야 합니다. 이 라우트들 각각에 대해 다음 홉(hop)으로 10.1.1.1을 지정하고 목적지 주소로 fec0::1을 지정해야 합니다.

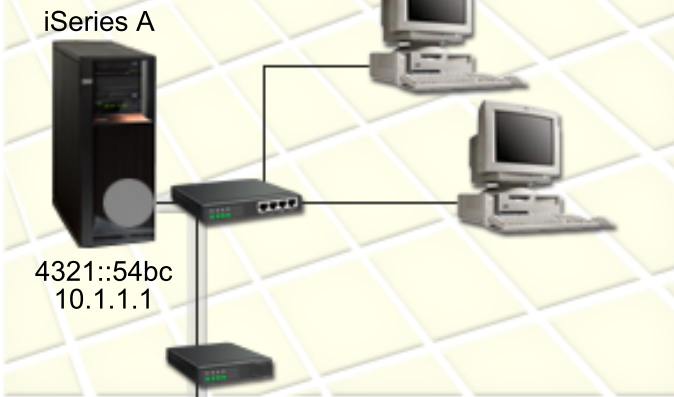
IPv4 광역 네트워크(WAN)를 통한 IPv6 패킷 송신

상황

귀사에서 시카고 오피스의 서버에 미수금 수납용 회계 어플리케이션을 사용합니다. 어플리케이션을 달라스 오피스의 서버에 연결해야 합니다. 이 어플리케이션은 양 쪽 사이트의 서버에서 IPv6 주소지정을 사용합니다. 귀사의 ISP가 두 사이트 사이의 IPv6 라우트를 제공할 수 없으므로 두 서버 사이의 터널을 구성해야 합니다. 어플리케이션 패킷은 두 서버 사이의 IPv4 광역 네트워크를 통해 터널을 통과해 이동합니다. 다음 그림은 이 시나리오의 네트워크 설정을 보여줍니다.

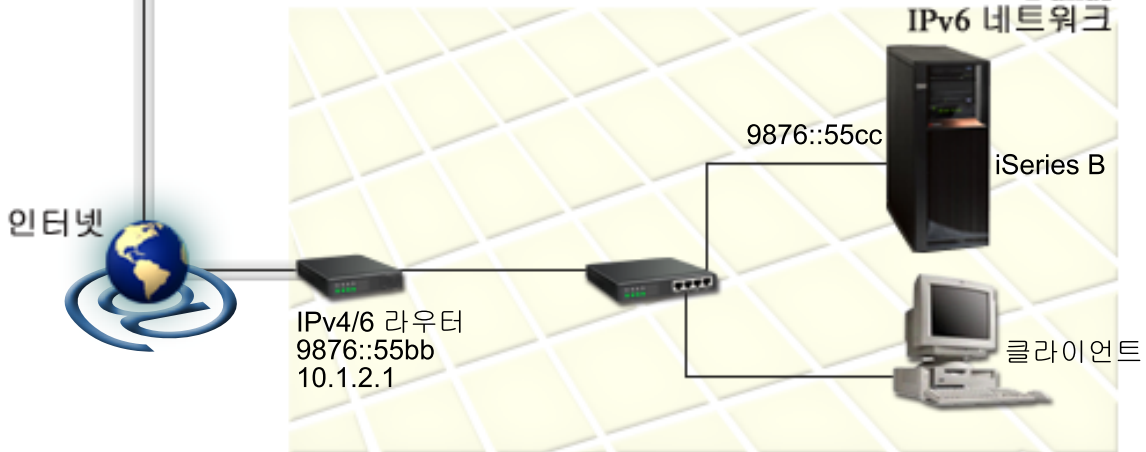
주: 시나리오에서 IP 주소 10.x.x.x는 글로벌로 라우트될 수 있는 공용 IP 주소를 나타냅니다. 사용된 모든 주소는 단지 예를 보여주기 위한 것입니다.

수신 계정
Chicago
IPv4 네트워크



녹색으로 구성된 터널
로컬 엔드포인트 = 10.1.1.1
리모트 엔드포인트 = 10.1.2.1
로컬 IPv6 주소 = 4321::54bc

지불 계정
Dallas
IPv6 네트워크



솔루션

IPv4 인프라구조로 구성된 광역 네트워크를 통해 IPv6을 사용하려면 구성된 터널 회선과 여러 개의 연관 라우트를 작성해야 합니다. 작동 방식은 다음과 같습니다.

- 터널은 시카고에 있는 iSeries A(로컬 종료점 10.1.1.1)에서 시작하여 달라스에 있는 IPv4/6 라우터(리모트 종료점 10.1.2.1)에서 끝납니다.
- iSeries A에 상주하는 어플리케이션은 iSeries B에 상주하는 어플리케이션에 연결되어야 합니다. iSeries A는 IPv4 패킷 내에 IPv6 패킷을 캡슐화하여 터널을 통해 IPv4/6 라우트에 송신합니다. IPv4/6 라우트는 IPv6 패킷을 디캡슐화하여 IPv6 패킷을 iSeries B로 이송합니다.
- 패킷은 역경로를 취하여 시카로로 리턴합니다.

터널 연결은 지점 간이므로 터널의 리모트 종료점을 정의해야 합니다. 이를 위해서는 이 터널 회선과 연관되는 라우트를 작성하십시오. 라우트는 다음 홉(hop)으로 리모트 종료점(10.1.2.1)을 정의합니다. 즉, 라우트를 작성하면서 리모트 종료점을 정의합니다. 또한, 라우트는 목적지 주소를 9876::55cc(iSeries B와 연관된 IPv6 주소)로 정의합니다.

터널 종료점을 정의하고 패킷을 달라스의 iSeries B에 이동시킬 수 있는 초기 라우트를 정의하는 것 외에, 두 개 이상의 라우트를 작성하여 패킷이 시카고의 iSeries A에 리턴되게 해야 합니다.

설정 요구사항에는 다음과 같은 항목이 포함됩니다.

- OS/400 버전 5 릴리스 2 이상
- Windows용 iSeries Access 및 iSeries Navigator(iSeries Navigator의 네트워크 구성요소)
- 구성된 터널 회선을 작성하기 전에 서버에 TCP/IP(IPv4 사용)를 구성해야 합니다. IPv4용 서버를 구성하지 않았으면 IPv6용 회선을 구성하기 전에 처음으로 TCP/IP 구성을 참조하십시오.

구성

구성된 터널 회선을 작성하려면 iSeries Navigator에서 **IPv6** 구성 마법사 및 새 **IPv6** 라우트 마법사를 사용해야 합니다. 구성된 터널은 iSeries Navigator에서만 구성 가능할 것이며, 문자 기반의 인터페이스에서는 구성 가능하지 않을 수도 있습니다.

IPv6 구성 마법사를 사용하여 터널 회선을 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> **TCP/IP** 구성을 선택하십시오.
2. **IPv6**을 마우스 오른쪽 버튼으로 클릭하고 **IPv6** 구성을 선택하여 마법사의 지침에 따라 IPv6용 터널 회선을 구성하십시오. **IPv6** 구성 마법사를 완료하고 나면 구성된 터널 회선에 대한 새 라우트를 구성하라고 프롬프트하며, 새 **IPv6** 라우트 마법사 대화가 나타납니다. IPv6 패킷이 터널을 통해 이동할 수 있도록 새 라우트를 작성해야 합니다.
3. 새 **IPv6** 라우트 마법사에서 터널에 대한 호스트 라우트를 작성하십시오. 다음 홉(hop)으로 리모트 종료점 10.1.2.1을 지정하고 목적지 주소로 9876::55cc를 지정하십시오.

구성된 터널 회선과 터널 종료점을 정의하는 라우트를 작성한 후에는 iSeries B에 라우트를 작성하고 패킷이 시카고에 다시 전달될 수 있도록 하는 라우트를 작성해야 합니다. iSeries B의 라우트에 대해서는 다음 홉(hop)으로 9876::55bb를 지정하고 목적지 주소 주소로 4321::54bc를 지정해야 합니다. IPv4/6 라우터에 있는 라우트의 경우에는 다음 홉(hop)으로 10.1.1.1을 지정하고 목적지 주소로 4321::54bc를 지정해야 합니다.

주: 달라스에 있는 IPv4/6 라우터에 9876::55cc에 대한 직접 라우트가 있어야 하지만, 이 라우트는 자동으로 작성되므로 수동으로 구성할 필요가 없습니다.

개념: IPv6

IPv6 작동 방식을 보다 잘 이해하려면 IPv6 개념에 대한 설명을 읽으십시오.

IPv4와 IPv6 비교

IPv4 속성과 IPv6 속성에 대한 비교 설명을 제공합니다. 이 표를 사용하여 특정 기능을 신속히 찾아보고 각 인터넷 프로토콜에서 이들의 사용법에 대해 비교할 수 있습니다.

IPv6 주소 형식

IPv6 주소의 크기 및 형식에 대해 설명합니다.

IPv6 주소 유형

IPv6 범위 내에서 새로운 주소 유형에 대해 설명합니다.

IPv6 터널링

IPv6 터널링이 어떤 식으로 IPv4 네트워크를 통해 IPv6 패킷이 이동되게 하는지에 대해 설명합니다.

인접 노드 발견

인접 노드 발견이 어떤 식으로 호스트와 라우터가 서로 통신할 수 있게 하는지에 대해 설명합니다.

상태 없는 주소 자동 구성

상태 없는 자동 구성이 어떤 식으로 네트워크 관리자의 일부 작업을 자동화하는지에 대해 설명합니다.

IPv6 주소 형식

IPv6 주소 크기는 128비트입니다. 우선 IPv6 주소 표시는 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx입니다. 여기서 각 x는 4비트를 나타내는 16진수입니다. IPv6 주소의 범위는 0000:0000:0000:0000:0000:0000:0000:0000에서 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff입니다.

이 우선 형식외에, IPv6 주소는 두 개의 단축 형식으로 지정될 수도 있습니다.

- **선행 0 생략**

선행 0은 생략하고 IPv6 주소를 지정하십시오. 예를 들어, IPv6 주소

1050:0000:0000:0000:0005:0600:300c:326b는 1050:0:0:0:5:600:300c:326b라고 씁니다.

- **이중 콜론**

일련의 0 대신 이중 콜론(::)을 사용하여 IPv6 주소를 지정하십시오. 예를 들어, IPv6 주소

ff06:0:0:0:0:0:c3은 ff06::c3이라고 쓸 수 있습니다. IP 주소에서 이중 콜론을 한 번만 사용할 수도 있습니다.

IPv6 주소용 대체 형식은 콜론과 점분리 표기법을 결합하여 IPv4 주소가 IPv6 주소에 내장될 수 있게 합니다. 가장 왼쪽의 96비트에 대해서는 16진 값이 지정되고, 내장 IPv4 주소를 나타내는 가장 오른쪽의 32비트에 대해서는 십진 값이 지정됩니다. 이 형식은 혼성 네트워크 환경에서 작업시 IPv6 노드와 IPv4 노드 사이의 호환성을 보장합니다.

다음 두 가지 유형의 IPv6 주소는 이 대안 형식을 사용합니다.

- **IPv4 맵핑 IPv6 주소**

이 유형의 주소는 IPv4 노드를 IPv6 주소로 나타내는데 사용됩니다. 이를 통해 IPv6 어플리케이션이 IPv4 어플리케이션과 직접 통신할 수 있습니다. 예를 들어, 0:0:0:0:0:ffff:192.1.56.10 및 ::ffff:192.1.56.10/96(단축 형식).

- **IPv4 호환 가능 IPv6 주소**

이 유형의 주소는 터널링에 사용됩니다. 이를 통해 IPv6 노드가 IPv4 인프라구조를 통해 통신할 수 있습니다. 예를 들어, 0:0:0:0:0:0:192.1.56.10 및 ::192.1.56.10/96(단축 형식).

다음 형식 모두 유효한 IPv6 주소 형식입니다. iSeries Navigator에서 다음 IPv6 주소 형식들 중 하나를 지정하십시오.

IPv6 주소 유형

IPv6 주소는 세 가지 기본 유형으로 분류됩니다.

유니캐스트 주소

유니캐스트 주소는 단일 인터페이스를 지정합니다. 유니캐스트 주소 목적지에 송신된 패킷은 한 호스트에서 목적지 호스트로 이동합니다.

세 가지 유형의 유니캐스트 주소는 다음과 같습니다.

링크-로컬 주소

링크-로컬 주소는 단일 로컬 링크(로컬 네트워크)에서 사용하기 위해 설계되었습니다. 링크-로컬 주소는 모든 인터페이스에서 자동으로 구성됩니다. 링크-로컬 주소에 사용되는 접두부는 fe80::/10입니다. 라우터는 링크-로컬 주소가 들어 있는 목적지나 소스 주소가 있는 패킷은 이송하지 않습니다.

사이트-로컬 주소

사이트-로컬 주소는 특정 사이트에서 사용하기 위해 설계되었습니다. 사이트-로컬 주소에 사용된 접두부는 fec0::/10입니다. 라우터는 특정 사이트 밖의 사이트-로컬 주소가 들어 있는 소스 주소가 있는 패킷은 이송하지 않습니다.

글로벌 주소

글로벌 주소는 임의의 네트워크에서 사용하도록 설계되었습니다. 글로벌 주소에 사용된 접두부는 2진 001로 시작합니다.

두 가지 특별한 유형의 유니캐스트 주소는 다음과 같습니다.

미지정 주소

미지정 주소는 0:0:0:0:0:0:0:0이거나 두 개의 콜론(::)으로 단축될 수 있습니다. 미지정 주소는 주소가 없음을 나타내며 절대 호스트에 할당되어서는 안 됩니다. 아직 주소가 할당되지 않은 IPv6 호스트가 이를 사용할 수도 있습니다. 예를 들어, 호스트가 다른 노드로부터 주소를 발견하기 위해 패킷을 송신할 때 소스 주소로서 미지정 주소를 사용합니다.

루프백 주소

루프백 주소는 0:0:0:0:0:0:0:1이거나 ::1로 단축될 수 있습니다. 노드는 자기 자신에게 패킷을 송신하기 위해 루프백 주소를 사용합니다.

애니캐스트 주소

애니캐스트 주소는 서로 다른 위치에서 모두 단일 주소를 공유하는 인터페이스 세트를 지정합니다. 애니캐스트 주소로 송신된 패킷은 가장 인접한 그룹 멤버에게만 갑니다. iSeries 서버는 현재 애니캐스트 주소지정을 지원하지 않습니다.

멀티캐스트 주소

멀티캐스트 주소는 여러 위치에 있는 인터페이스 세트를 지정합니다. 멀티캐스트 주소에 사용되는 접두부

는 ff입니다. 패킷을 멀티캐스트 주소로 송신하면 패킷의 한 사본의 그룹의 각 멤버에게 전달됩니다. iSeries 서버는 현재 기본적인 멀티캐스트 주소지정을 지원합니다. 멀티캐스트 인터페이스 작성 및 어플리케이션 지원은 현재 지원되지 않습니다.

IPv6 터널링

iSeries 서버는 IPv6 터널링을 사용하여 IPv4 도메인을 통해 IPv6 노드(호스트 및 라우터)에 연결할 수 있습니다. 터널링은 분리된 IPv6 노드나 네트워크가 기저의 IPv4 인프라구조 없이 통신할 수 있게 합니다. 터널링을 사용하여 IPv4 및 IPv6 프로토콜이 함께 작동할 수 있으며, 따라서 IPv4 연결을 유지하면서 IPv6을 구현하는 전환 메소드를 제공합니다.

터널은 IPv4 네트워크상에 두 개의 이중 스택(IPv4 및 IPv6)으로 구성됩니다. 이러한 이중 스택 노드는 IPv4와 IPv6 통신을 모두 처리할 수 있습니다. IPv6 인프라구조의 끝에 있는 이중 스택 노드 중 하나는 도착하는 각 IPv6 패킷 앞에 IPv4 헤더를 삽입(캡슐화)하여 이를 마치 정상 IPv4 통신인 것처럼 기존 링크를 통해 송신합니다. IPv4 라우터는 계속해서 이 통신을 이송합니다. 터널의 다른 쪽에서 또 다른 이중 스택 노드가 IPv6 패킷에서 여분의 IP 헤더를 제거(디캡슐화)하여 이를 표준 IPv6을 사용하여 최종 목적지로 라우트합니다.

iSeries 서버용 IPv6 터널링은 가상 회선인 구성된 터널 회선을 통과합니다. 구성된 터널 회선은 IPv6 터널을 지원하는 라우트 가능한 IPv4 주소를 가진 임의의 노드와 통신합니다. 이러한 노드는 로컬 IPv4 정의역이나 리모트 정의역 내에 어디든 존재할 수 있습니다.

구성된 터널 연결은 지점 간입니다. 이런 유형의 터널 회선을 구성하려면 124.10.10.150과 같은 로컬 터널 종료점(IPv4 주소)과 1080:0:0:0:8:800:200c:417a와 같은 로컬 IPv6 주소를 지정해야 합니다. 터널을 통해 통신이 이동할 수 있도록 IPv6 라우트도 작성해야 합니다. 라우트를 작성하면서 터널의 리모트 종료점(IPv4 주소) 중 하나를 라우트의 다음 홉(hop)으로 정의할 것입니다. 무제한 수의 터널에 대한 무제한 수의 종료점을 구성할 수도 있습니다.

IPv6 터널링을 설명하는 시나리오 및 그림은 IPv4 근거리 통신망(LAN)을 통한 IPv6 패킷 송신 및 광역 네트워크(WAN)를 통한 IPv6 패킷 송신을 참조하십시오.

인접 노드 발견

IPv6 노드(호스트나 라우터)는 인접 노드 발견 기능을 사용하여 다른 IPv6 노드의 존재를 발견하고, 노드의 링크층 주소를 판별하고, IPv6 패킷을 이송할 수 있는 라우터를 발견하며, 활동 IPv6 인접 노드의 캐시를 유지보수합니다. IPv6 노드는 다음과 같은 5개의 ICMPv6(Internet Control Message Protocol version 6) 메시지를 사용하여 다른 노드와 통신합니다.

라우터 요청

호스트가 이 메시지를 송신하여 라우터에게 라우터 광고를 생성하도록 요청합니다. 네트워크에서 호스트를 처음으로 사용할 수 있게 될 때 호스트가 초기 라우터 요청을 송신합니다.

라우터 광고

라우터는 주기적으로 또는 라우터 요청에 대한 응답으로 이러한 메시지를 송신합니다. 호스트는 라우터 광

고에서 제공된 정보를 사용하여 자동으로 사이트-로컬 인터페이스, 글로벌 인터페이스 및 연관 라우트를 자동으로 작성합니다. 라우터 광고에는 최대 전송 단위 및 홉(hop) 한계와 같은 호스트에서 사용하는 기타 구성 정보도 들어 있습니다.

인접 노드 요청

노드는 이러한 메시지를 송신하여 인접 노드의 링크층 주소를 판별하거나 인접 노드에 여전히 도달할 수 있는지 확인합니다.

인접 노드 광고

노드는 인접 노드 요청에 대한 응답이나 주소 변경을 발표하기 위한 미요청 메시지로서 이러한 메시지를 송신합니다.

경로 재지정

라우터는 이 메시지를 사용하여 호스트에게 목적지에 대한 더 나은 첫 번째 홉(hop)을 알립니다.

인접 노드 발견 및 라우터 발견에 대한 자세한 정보는 RFC 2461을 참조하십시오. RFC 2461을 보려면 RFC Editor(<http://www.rfc-editor.org/rfcsearch.html>)  를 참조하십시오.

상태 없는 주소 자동 구성

상태 없는 주소 자동 구성은 인터페이스에 대한 IPv6 주소를 자동으로 구성하기 위해 IPv6 노드(호스트나 라우터)가 사용하는 프로세스입니다. 노드는 접두부를 노드의 MAC 주소나 사용자 지정 인터페이스 ID와 결합하여 다양한 IPv6 주소를 빌드합니다. 접두부에는 링크-로컬 접두부(fe80::/10) 및 로컬 IPv6 라우터(있는 경우)가 광고한 길이가 64인 접두부가 포함됩니다. 링크-유형이 멀티캐스트 가능한 경우 상태 없는 주소 자동 구성은 또한 적당한 멀티캐스트 인터페이스를 작성합니다.

노드는 중복 주소 감지를 수행하여 주소를 인터페이스에 할당하기 전에 주소가 고유한지 확인합니다. 노드는 새 주소로 인접 노드 요청 조화를 보내고 응답을 기다립니다. 노드가 응답을 수신하지 않으면 주소가 고유한 걸로 가정합니다. 노드가 인접 노드 광고의 형태로 응답을 수신하면 주소가 이미 사용 중인 것입니다. 노드가 임시 IPv6 주소가 고유하지 않음을 판별하면 자동 구성이 중단되며 인터페이스를 수동 구성해야 합니다.

IPv4와 IPv6 비교

IBM은 몇몇 소프트웨어 릴리스에서 iSeries 서버에 IPv6을 구현하고 있습니다. IPv6은 현재 IPv6 어플리케이션 개발 및 테스트 용도로 어플리케이션 개발 플랫폼에서 구현됩니다.

IPv6의 세부사항이 IPv4와 어떻게 다른지 궁금해하실 수도 있습니다. 이 표를 사용하여 IPv4와 연관된 친숙한 속성을 신속히 살펴보고 IPv6의 유사한 속성과 비교할 수 있습니다. 이 목록에서 속성을 선택하여 표의 비교와 링크하십시오.

- 21 페이지의 『주소』
- 21 페이지의 『주소 할당』
- 21 페이지의 『주소 지속 기간』
- 21 페이지의 『주소 마스크』
- 21 페이지의 『주소 접두부』
- 21 페이지의 『Address Resolution Protocol (ARP)』

- 22 페이지의 『주소 범위』
- 22 페이지의 『주소 유형』
- 22 페이지의 『통신 추적』
- 22 페이지의 『구성』
- 22 페이지의 『DNS(정의역명 시스템)』
- 22 페이지의 『Dynamic DHCP(동적 호스트 구성 프로토콜)』
- 22 페이지의 『FTP(파일 전송 프로토콜)』
- 22 페이지의 『프래그먼트』
- 22 페이지의 『호스트 표』
- 22 페이지의 『인터페이스』
- 22 페이지의 『ICMP(Internet Control Message Protocol)』
- 23 페이지의 『IGMP(Internet Group Management Protocol)』
- 23 페이지의 『IP 헤더』
- 23 페이지의 『IP 헤더 옵션』
- 23 페이지의 『IP 헤더 프로토콜 바이트』
- 23 페이지의 『IP 헤더 서비스 유형(TOS) 바이트』
- 23 페이지의 『iSeries Navigator 지원』
- 23 페이지의 『LAN 연결』
- 23 페이지의 『계층 2 터널 프로토콜(L2TP)』
- 23 페이지의 『루프백 주소』
- 23 페이지의 『MTU(최대 전송 단위)』
- 23 페이지의 『netstat』
- 23 페이지의 『NAT(네트워크 주소 변환)』
- 23 페이지의 『네트워크 표』
- 23 페이지의 『노드 정보 조회』
- 23 페이지의 『패킷 필터링』
- 23 페이지의 『패킷 이송』
- 24 페이지의 『패킷 터널링』
- 24 페이지의 『PING』
- 24 페이지의 『PPP(지점 간 프로토콜)』
- 24 페이지의 『포트 제한사항』
- 24 페이지의 『포트』
- 24 페이지의 『개인 및 공용 주소』
- 24 페이지의 『프로토콜 표』
- 24 페이지의 『QoS(서비스 품질)』
- 24 페이지의 『재번호매김』
- 24 페이지의 『라우트』
- 24 페이지의 『RIP(라우팅 정보 프로토콜)』
- 25 페이지의 『서비스 표』
- 25 페이지의 『SNMP(단순 네트워크 관리 프로토콜)』

- 25 페이지의 『소켓 API』
- 25 페이지의 『소스 주소 선택』
- 25 페이지의 『시작 및 중단』
- 25 페이지의 『Telnet』
- 25 페이지의 『라우트 추적』
- 25 페이지의 『전송층』
- 25 페이지의 『미지정 주소』
- 25 페이지의 『VPN(가상 사설망)』

	IPv4	IPv6
주소	32비트 길이(4바이트). 주소는 주소 클래스에 따라 다른 네트워크 및 호스트 부분으로 구성됩니다. 몇개의 초기 비트에 따라 A, B, C, D 또는 E의 여러가지 주소 클래스가 정의됩니다. 총 IPv4 주소 수는 4 294 967 296개입니다. IPv4 주소의 텍스트 형태는 nnn.nnn.nnn.nnn입니다. 여기서 $0 \leq n \leq 255$ 이며, 각 n은 십진수입니다. 선행 0은 생략할 수도 있습니다. 최대 인쇄 문자 수는 마스 크를 세지 않고 15개입니다.	128비트 길이(16바이트). 기본 구조는 네트워크 번호용으로 64비트와 호스트 번호용으로 64비트입니다. 종종, IPv6 주소의 호스트 부분(또는 그 일부분)은 MAC 주소나 기타 인터페이스 ID입니다. 서브네트 접두부에 따라 IPv6는 IPv4보다 복잡한 구조를 가집니다. IPv6 주소의 수는 IPv4의 수보다 10 ²⁸ (79 228 162 514 264 337 593 543 950 336)배 더 큼니다.IPv6의 텍스트 양식은 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx로, 여기서 각 x는 4비트를 나타내는 16진 숫자입니다. 선행 0은 생략할 수도 있습니다. 임의의 갯수의 0비트를 나타내기 위해 주소의 텍스트 형태에 이중 콜론(::)을 한 번 사용할 수도 있습니다. 예를 들어, ::ffff:10.120.78.40은 IPv6의 IPv4 맵핑 주소입니다. (세부 사항은 RFC 2373을 참조하십시오. 이 RFC를 보려면 RFC Editor(http://www.rfc-editor.org/rfcsearch.html)를 참조하십시오.
주소 할당	원래, 주소는 네트워크 클래스에 의해 할당되었습니다. 주소 공간이 고갈됨에 따라 CIDR(Classless Inter-Domain Routing)을 사용하여 보다 작게 할당했습니다. 기관 및 국가 간에 할당 균형이 이루어지지 않았습니다.	할당은 가장 초기 스테이지에 있습니다. IETF(Internet Engineering Task Force) 및 IAB(Internet Architecture Board)는 모든 조직, 가정 또는 엔터티에 /48 서브네트 접두부 길이가 할당되도록 권장했습니다. 이는 조직에서 서브네팅을 할 수 있도록 16비트를 남겨놓습니다. 주소 공간의 크기가 충분하므로 세계의 모든 사람이 고유한 /48 서브네트 접두부 길이를 가질 수 있습니다.
주소 지속 기간	DHCP를 사용하여 할당된 주소를 제외하고는 일반적으로 해제되는 개념이 아닙니다.	IPv6 주소에는 우선 지속 기간과 유효한 지속 기간의 두 가지 지속 기간이 있습니다. 우선 지속 기간은 항상 유효한 지속 기간보다 작거나 같습니다. 우선 지속 기간이 만기된 후에는 주소가 소스 IP 주소로 사용되지 않습니다. 유효한 지속 기간이 만기된 후에는 주소가 수신 패킷을 위한 유효한 IP 주소로 사용(인식)되지 않습니다. 일부 IPv6 주소는 정의에 의해 무한 우선 지속 기관 및 무한 유효한 지속 기간을 가집니다. 링크 로컬이 그 예입니다(22 페이지의 『주소 범위』 참조).
주소 마스크	호스트 부분으로부터 네트워크를 지정하는데 사용합니다.	미사용(『주소 접두부』 참조).
주소 접두부	종종 호스트 부분으로부터 네트워크를 지정하는데 사용합니다. 주소의 표시 형태에서 종종 /nn 접미부로 씁니다.	주소의 서브네트 접두부를 지정하는데 사용합니다. 인쇄 형태 다음에 /nnn(최대 3자리 십진수, $0 \leq n \leq 128$) 접미부로 씁니다. fe80::982:2a5c/10이 한 예입니다. 여기서 첫 번째 10비트는 서브네트 접두부로 이루어집니다.
ARP(Address Resolution Protocol)	IPv4는 ARP(Address Resolution Protocol)를 사용하여 IPv4 주소와 연관된 MAC 또는 링크 주소와 같은 물리적 주소를 찾습니다.	IPv6는 ICMPv6(Internet Control Message Protocol version 6)을 사용하여 상태 없는 자동 구성 및 인접 노드 발견을 위한 알고리즘의 일부로서 IP 자체 내에 이러한 기능을 내장시킵니다. 따라서, ARP6과 같은 것은 없습니다.

	IPv4	IPv6
주소 범위	유니캐스트 주소의 경우에는 이 개념이 적용되지 않습니다. 지정된 개인 주소 범위 및 루프백이 있습니다. 그 외의 주소는 글로벌로 가정합니다.	IPv6에서 주소 범위는 구조의 일부입니다. 유니캐스트 주소에는 링크-로컬, 사이트-로컬 및 글로벌을 포함하여 3가지의 정의된 범위가 있으며, 멀티캐스트 주소에는 14가지 범위가 있습니다. 소스 및 목적지에 대한 다폴트 주소 선택이 범위를 고려합니다. 범위 좁은 특정 네트워크에서 범위의 인스턴스입니다. 그 결과, IPv6 주소는 존 ID와 함께 입력되고 연관되어야 합니다. 구문은 %zid입니다. 여기서 zid는 번호(보통 작은 번호)나 이름입니다. 존 ID는 주소 뒤와 접두부 앞에 씁니다. 예를 들어, 2ba::1:2:14e:9a9b:c%3/48.
주소 유형	유니캐스트, 멀티캐스트 및 브로드캐스트.	유니캐스트, 멀티캐스트 및 애니캐스트. 설명은 IPv6 주소 유형을 참조하십시오.
통신 추적	iSeries 서버에 들어가고 나오는 TCP/IP (및 기타) 패킷의 자세한 추적을 수집하기 위한 툴.	IPv6에서도 동일하며, IPv4에서 터널된 ICMPv6 및 IPv6 패킷을 포함하여 IPv6이 지원됩니다.
구성	통신하기 전에 새로 설치된 시스템에 구성을 해야 합니다. 즉, IP 주소와 라우트를 할당해야 합니다.	구성은 필요한 기능에 따라 선택적입니다. iSeries Navigator를 사용하여 적당한 이더넷이나 터널 인터페이스를 IPv6으로 지정해야 합니다. 이 작업을 하고 나면 IPv6 인터페이스가 자동으로 구성됩니다. 따라서, 네트워크 유형과 IPv6 라우터 존재 여부에 따라 시스템이 로컬 및 리모트인 다른 IPv6 시스템과 통신할 수 있습니다.
DNS(정의역명 시스템)	어플리케이션은 호스트명을 승인한 후 DNS를 사용하여 소켓 API gethostbyname()를 사용하여 IP 주소를 확보합니다. 어플리케이션은 또한 IP 주소를 승인한 후 DNS를 사용하여 gethostbyaddr()을 사용하여 호스트명을 확보합니다. IPv4의 경우, 반전 찾아보기를 위한 정의역은 in-addr.arpa입니다.	IPv6의 경우와 동일합니다. AAAA(4중 A) 레코드 유형과 반전 찾아보기(IP-to-name)를 사용하여 IPv6에 대한 지원을 합니다. 어플리케이션은 DNS에서 IPv6 주소를 승인할지 여부를 선택한 후 IPv6를 사용하여 통신하거나 하지 않을 수 있습니다. IPv6에 대한 소켓 API gethostbyname()가 변경되지 않았으며 getaddrinfo() API를 사용하여 IPv6만, 혹은 IPv4 및 IPv6 주소를 확보할 수 있습니다(어플리케이션 선택사항). IPv6의 경우, 반전 나블 찾아보기에 사용되는 정의역은 ip6.arpa이며, 이것이 없으면 ip6.int를 사용합니다(API getnameinfo() 참조).
Dynamic DHCP(동적 호스트 구성 프로토콜)	동적으로 IP 주소 및 기타 구성 정보를 확보하는데 사용합니다.	현재, DHCP는 IPv6을 지원하지 않습니다.
FTP(파일 전송 프로토콜)	파일 전송 프로토콜을 사용하여 네트워크 사이에서 파일을 송수신할 수 있습니다.	현재, FTP는 IPv6을 지원하지 않습니다.
프래그먼트	패킷이 이동할 다음 링크에 대해 너무 큰 경우에는 송신자(호스트나 라우터)가 패킷을 프래그먼트화합니다.	IPv6의 경우, 소스 노드에서만 프래그먼트화가 발생하며 리어셀블라는 목적지 노드에서만 수행됩니다. 현재, 프래그먼트화 확장 헤더는 지원되지 않습니다.
호스트 표	iSeries Navigator에서 인터넷 주소를 호스트명과 연관시키는 구성 가능한 표. 예를 들어, 127.0.0.1, loopback. 소켓 이름 분석기는 DNS 찾아보기 전이나 DNS 찾아보기에 실패한 후(호스트명 탐색 우선순위에 의해 결정) 이 표를 사용합니다.	현재, 이 표는 IPv6을 지원하지 않습니다. IPv6 정의역 분석을 위해 고객은 DNS에 AAAA 레코드를 구성해야 합니다. 분석기와 동일한 시스템에 로컬로 DNS를 실행하거나 다른 시스템에서 DNS를 실행할 수도 있습니다.
인터페이스	IPv4 주소로 명명되지 않은 경우, TCP/IP가 패킷을 송수신하기 위해 사용하며 항상 IPv4 주소와 밀접하게 연관되는 개념적이거나 논리적인 엔티티. 논리적 인터페이스라고도 부릅니다. STRTCPIFC 및 ENDTCPIFC 명령을 사용하거나 iSeries Navigator를 사용하여 서로 독립적으로 그리고 TCP/IP와 독립적으로 시작하고 중단할 수 있습니다.	IPv4와 동일한 개념. iSeries Navigator를 사용해서만 서로 독립적으로 그리고 TCP/IP와 독립적으로 시작하고 중단할 수 있습니다.
ICMP(Internet Control Message Protocol)	IPv4는 ICMP를 사용하여 네트워크 정보를 통신합니다.	IPv6에서도 유사하게 사용되나, ICMPv6(Internet Control Message Protocol version 6)은 몇가지 새로운 속성을 제공합니다. 목적지 도달 불가능, 에코우 요청 및 응답과 같은 기본 오류 유형은 똑같이 남아 있습니다. 새로운 유형 및 코드가 인접 노드 발견 및 관련 기능을 지원하기 위해 추가되었습니다.

	IPv4	IPv6
IGMP(Internet Group Management Protocol)	IPv4 라우터는 IGMP를 사용하여 특정 멀티캐스트 그룹에 대한 통신을 원하는 호스트를 찾으며, IPv4 호스트는 IGMP를 사용하여 IPv4 라우터에게 기존 멀티캐스트 그룹 리스너(호스트상)를 알려줍니다.	IPv6의 경우에는 MLD(multicast listener discovery) 프로토콜로 대체되었습니다. IPv4에서 IGMP가 하는 것과 근본적으로 동일한 기능을 하나, 몇가지 MLD 고유의 ICMPv6 유형 값을 추가하여 ICMPv6을 사용합니다.
IP 헤더	현재의 IP 옵션에 따라 20-60바이트의 가변 길이.	40바이트의 고정 길이. IP 헤더 옵션이 없습니다. 일반적으로, IPv6 헤더는 IPv4 헤더보다 간단합니다.
IP 헤더 옵션	(전송 헤더 앞에) IP 헤더에 덧붙이는 여러가지 옵션.	IPv6 헤더에는 옵션이 없습니다. 대신, IPv6은 추가(선택적) 확장 헤더를 추가합니다. 확장 헤더는 AH 및 ESP(IPv4에서 변경되지 않았음), 홉(hop)별, 라우팅, 프래그먼트 및 목적지입니다. 현재, IPv6은 확장 헤더를 지원하지 않습니다.
IP 헤더 프로토콜 바이트	전송층이나 패킷 페이로드의 프로토콜 코드. 예를 들어, ICMP.	IPv6 헤더 바로 다음에 오는 헤더 유형. IPv4 프로토콜 필드와 동일한 값을 사용합니다. 그러나 구조상의 효과는 현재 정의된 다음 헤더 범위를 허용하는 것이며, 쉽게 확장됩니다. 다음 헤더는, 전송 헤더, 확장 헤더 또는 ICMPv6입니다.
IP 헤더 서비스 유형(TOS) 바이트	QoS 및 차별 서비스에서 통신 클래스를 지정하기 위해 사용됩니다.	IPv4와 유사하게 IPv6 통신 클래스를 지정합니다. 서로 다른 코드를 사용합니다. 현재, IPv6은 TOS를 지원하지 않습니다.
iSeries Navigator 지원	iSeries Navigator는 TCP/IP에 대한 완전한 구성 정보를 제공합니다.	IPv6 구성 마법사를 포함하여 IPv6에 대한 선택적 구성이 iSeries Navigator에서 완전히 제공됩니다.
LAN 연결	IP 인터페이스에서 물리적 네트워크에 도달하기 위해 사용합니다. 예를 들어, 토르넷, 이더넷 및 PPP와 같이 많은 유형이 있습니다. 물리적 인터페이스, 링크 또는 회선이라도 포함합니다.	IPv6에서도 동일한 개념을 가집니다. 현재, 2838 및 2849 이더넷 카드 및 터널 회선만 지원됩니다.
계층 2 터널 프로토콜(L2TP)	L2TP는 가상 PPP로 여겨질 수 있으며 지원되는 모든 회선 유형에서 작동합니다.	현재, L2TP는 IPv6을 지원하지 않습니다.
루프백 주소	노드가 자기 자신에게 패킷을 송신하는데에만 사용될 수 있는 127.*.*.*(보통 127.0.0.1)의 주소를 가진 인터페이스. 물리적 인터페이스(회선 설명)는 *LOOPBACK으로 명명됩니다.	개념은 IPv4에서와 동일하며 단일 루프백 주소는 0000:0000:0000:0000:0000:0000:0000:0001 또는 ::1(단축 버전)입니다. 가상 물리적 인터페이스는 *LOOPBACK6으로 명명됩니다.
MTU(최대 전송 단위)	링크의 최대 전송 단위는 이더넷이나 모뎀과 같은 특정 링크 유형이 지원하는 최대 바이트 수입니다. IPv4의 경우, 일반적인 최소값은 576입니다.	IPv6에는 1280바이트의 MTU상에 설계된 하한 바운드가 있습니다. 즉, IPv6은 이 한계 아래에서 패킷을 프래그먼트하지 않습니다. 1280 MTU 미만의 링크를 통해 IPv6을 송신하기 위해서는 링크층이 IPv6 패킷을 투명하게 프래그먼트하고 디프래그먼트해야 합니다.
netstat	TCP/IP 연결, 인터페이스 또는 라우트의 상태를 보기 위한 툴. iSeries Navigator 및 5250에서 사용할 수 있습니다.	IPv6에서도 동일하며, IPv6은 5250 및 iSeries Navigator에 대해 지원됩니다.
NAT(네트워크 주소 변환)	TCP/IP에 통합된 기본 방화벽 기능으로, iSeries Navigator를 사용하여 구성됩니다.	현재, NAT는 IPv6을 지원하지 않습니다. 보다 일반적으로 말하면, IPv6은 NAT를 필요로 하지 않습니다. IPv6의 확장된 주소 공간은 주소 부족 문제점을 없애며 번호 매김을 더 쉽게 해줍니다.
네트워크 표	iSeries Navigator에서 네트워크 이름을 마스크 없이 IP 주소와 연관시키는 구성 가능한 표. 예를 들면 host Network14와 IP address 1.2.3.4.입니다.	현재, IPv6용으로 이 표에 변경된 사항은 없습니다.
노드 정보 조회	존재하지 않습니다.	내용이 있는 것을 제외하고 ping처럼 작동해야 하는 간단하고 편리한 네트워크 툴. IPv6 노드는 또 다른 IPv6 노드에서 목표의 DNS명, IPv6 유니캐스트 주소 또는 IPv4 주소를 조회할 수도 있습니다. 현재, 지원되지 않습니다.
패킷 필터링	TCP/IP에 통합된 기본 방화벽 기능으로, iSeries Navigator를 사용하여 구성됩니다.	현재, 패킷 필터링은 IPv6을 지원하지 않습니다. 그러나, IPv4 필터링을 터널된 IPv6 통신에 적용할 수 있습니다.
패킷 이송	로컬이 아닌 IP 주소에 대해 수신하는 IP 패킷을 이송하도록 iSeries 서버를 구성할 수 있습니다. 보통, 인바운드 인터페이스와 아웃바운드 인터페이스는 서로 다른 LAN에 연결됩니다.	현재, IPv6 패킷은 이송되지 않습니다.

	IPv4	IPv6
패킷 터널링	IPv4에서는, 터널-모드 VPN 연결에 대한 VPN(IPv4에서 터널된 IPv4) 및 L2TP에서 터널링이 발생합니다.	IPv6의 경우, IPv4 패킷에서의 터널링은 IPv6의 전개에 있어 주요 부분이 될것로 기대됩니다. 현재, 최소한 5개의 서로 다른 유형의 6-in-4 터널링이 IETF에 의해 정의되며, 각각 서로 다른 속성 및 장점을 가집니다. IPv6 노드가 기존 IPv4 인터넷을 통해 통신할 수 있도록 기본 및 유연한 유형의 IPv6-in-IPv4 터널링이 지원됩니다. 구성된 터널링이라고도 하며, 두 개의 IPv6 노드 사이에서 가상 지점 간 링크를 제공하며 *TNLCFG64라는 새로운 유형의 터널 회선을 사용합니다.
PING	도달 가능성을 테스트하는 기본 TCP/IP 툴. iSeries Navigator 및 5250에서 사용할 수 있습니다.	IPv6에서도 동일하며, IPv6은 5250 및 iSeries Navigator에 대해 지원됩니다.
PPP(지점 간 프로토콜)	PPP는 다양한 모뎀 및 회선 유형을 통한 전화 접속 인터넷을 지원합니다.	현재, PPP는 IPv6을 지원하지 않습니다.
포트 제한사항	고객은 이러한 iSeries 패널을 사용하여 TCP나 UDP에 대해 선택된 포트 번호나 포트 번호 범위를 특정 프로파일에만 사용할 수 있도록 구성할 수 있습니다.	IPv6에서는 지원되지 않습니다. 구성된 제한사항은 IPv4에만 적용됩니다.
포트	TCP와 UDP에는 각각 1-65535 범위의 포트 번호로 식별되는 별도의 포트 공간이 있습니다.	IPv6의 경우, 포트는 IPv4와 동일하게 작동합니다. 새 주소 그룹이 있으므로 이제 네 개의 별도 포트 공간이 있습니다. 예를 들어, 어플리케이션이 바인딩할 수 있는 두 개의 TCP 포트 80 공간(하나는 AF_INET에, 다른 하나는 AF_INET6에)이 있습니다.
개인 및 공용 주소	IETF RFC 1918에 의해 개인용으로 지정된 세 가지 주소 범위 즉, 10.*.*.* (10/8), 172.16.0.0에서 172.31.255.255 (172.16/12) 및 192.168.*.* (192.168/16)을 제외한 모든 IPv4 주소가 공용입니다. 개인 주소 정의역은 일반적으로 조직 내에서 사용됩니다. 개인 주소는 인터넷을 통해 라우트될 수 없습니다.	IPv6에도 유사한 개념이 있으나, 중요한 차이점이 있습니다. 주소는 공용 주소이거나 이전에는 anonymous라는 용어를 사용했던 임시 주소입니다. RFC 3041을 참조하십시오. IPv4 개인 주소와는 달리, 임시 주소는 글로벌로 라우트될 수 있습니다. 동기 역시 다릅니다. IPv6 임시 주소는 통신을 시작할 때 클라이언트의 신원을 보호하기 위한 것입니다(개인 보호에 대한 배려). 임시 주소의 지속 기간은 제한되어 있으며, 링크(MAC) 주소인 인터페이스 ID를 포함하지 않습니다. 일반적으로 공용 주소와 구분이 가능하지 않습니다. IPv6은 설계되어 있는 범위 지정을 사용하여 제한된 주소 범위를 표기합니다(22 페이지의 『주소 범위』 참조).
프로토콜 표	iSeries Navigator에서 프로토콜 이름을 프로토콜 번호와 연관시키는 구성 가능한 표. 예를 들어, UDP, 17. 시스템은 IP, TCP, UDP, ICMP의 몇 가지 항목과 함께 제공됩니다.	표는 변경 없이 IPv6을 지원합니다.
QoS(서비스 품질)	서비스 품질을 사용하여 TCP/IP 어플리케이션을 위한 패킷 우선순위 및 대역폭을 요청할 수 있습니다.	현재, QoS는 IPv6을 지원하지 않습니다. 그러나, IPv6이 IPv4에서 터널링되면 기존 iSeries QoS 설비가 IPv4 통신에 적용된 후 투명하게 IPv6 페이로드를 처리할 수 있습니다.
재번호매김	수동 재구성을 통해 수행됩니다. DHCP에서는 예외일 수도 있습니다. 일반적으로, 사이트나 조직에서 가능하면 피해야 할 어렵고 문제가 많은 프로세스입니다.	IPv6의 중요한 구조상의 요소로, 특히 /48 접두부 내에서 대개 자동이어야 합니다.
라우트	논리적으로, IP 주소(1만 포함할 수도 있음)를 물리적 인터페이스 및 하나의 다음 홉(hop) IP 주소에 맵핑시키는 것. 목적지 주소가 세트의 일부로서 정의되는 IP 패킷은 회선을 사용해 다음 홉(hop)으로 이동됩니다. IPv4 라우트는 IPv4 인터페이스와 연관되므로, IPv4 주소와 연관됩니다. 다폴트 라우트는 *DFROUTE입니다.	개념적으로, IPv4와 동일합니다. 한 가지 중요한 차이점은 IPv6 라우트는 인터페이스가 아니라 물리적 인터페이스(*TNLCFG64 또는 ETH03과 같은 링크)와 연관(바인드)된다는 것입니다. 여기에는 여러가지 이유가 있습니다. 한 가지 이유는 IPv6에 대한 스스 주소 선택 기능이 IPv4와 다르다는 것입니다. 25 페이지의 『주소 선택』 내용을 참조하십시오. 견고성을 향상시키기 위해 중복 라우트가 허용되지만, 라우트 찾기 동안에는 무시됩니다.
RIP(라우팅 정보 프로토콜)	RIP는 routed 디면에서 지원되는 라우팅 프로토콜입니다.	현재, RIP는 IPv6을 지원하지 않습니다. IPv6 라우팅은 정적 라우트를 사용합니다.

	IPv4	IPv6
서비스 표	iSeries 서버에서 예를 들어, 서비스 이름 FTP-제어, 포트 21, TCP 및 UDP와 같은 포트 및 프로토콜과 서비스 이름을 연관시키는 구성 가능한 표. 많은 수의 잘 알려진 서비스가 서비스 표에 나열됩니다. 많은 어플리케이션이 이 표를 사용하여 어느 포트를 사용할지 판별합니다.	IPv6용으로 이 표에 변경된 사항은 없습니다.
SNMP(단순 네트워크 관리 프로토콜)	SNMP는 시스템 관리를 위한 프로토콜입니다.	현재, SNMP는 IPv6을 지원하지 않습니다. IPv6 라우팅은 정적 라우트를 사용합니다.
소켓 API	어플리케이션은 이러한 API를 통해 TCP/IP를 사용합니다. IPv6을 필요로 하지 않는 어플리케이션은 IPv6을 지원하기 위한 소켓 변경에 영향을 받지 않습니다.	IPv6은 어플리케이션이 이제 새로운 주소 그룹인 AF_INET6을 통해 IPv6을 사용할 수 있도록 소켓을 향상시킵니다. 기존 IPv4 어플리케이션이 IPv6 및 API 변경의 영향을 전혀 받지 않도록 확장 기능이 설계되었습니다. IPv4와 IPv6 동시 통신 또는 IPv6 전용 통신을 지원하려는 어플리케이션은 ::ffff:a.b.c.d 형태의 IPv4 맵핑 IPv6 주소를 사용하여 쉽게 조정될 수 있습니다. 여기서 a.b.c.d는 클라이언트의 IPv4 주소입니다. 새 API에는 텍스트에서 2진수로, 2진수에서 텍스트로의 IPv6 주소 변환 지원도 포함되어 있습니다. IPv6용 소켓 확장 기능에 대한 자세한 정보는 AF_INET6 주소 그룹 사용을 참조하십시오.
소스 주소 선택	어플리케이션이 소스 IP를 지정할 수도 있습니다(보통, bind()를 사용하여). INADDR_ANY에 바인드하는 경우에는 라우트를 기반으로 소스 IP에 바인드합니다.	IPv4에서는, 어플리케이션이 bind()를 사용하여 소스 IPv6 주소를 지정할 수도 있습니다. IPv4와 마찬가지로, in6addr_any를 사용하여 시스템이 IPv6 소스 주소를 선택하게 할 수도 있습니다. 그러나 IPv6 회선에 많은 IPv6 주소가 있으므로 소스 IP를 선택하는 내부 메소드가 다릅니다.
시작 및 중단	STRTCP와 ENDTCP를 사용하여 TCP/IP를 시작하고 종료하십시오.	IPv4와 동일합니다. IPv4 및 IPv6은 서로 독립적으로 또는 TCP/IP와 독립적으로 시작되거나 중단될 수 없습니다. 즉, IPv4 또는 IPv6만이 아니라 모든 TCP/IP를 시작하고 중단해야 합니다. AUTOSTART 매개변수 = *YES인 경우(디폴트)에는 모든 IPv6 인터페이스가 자동으로 시작됩니다. IPv6은 IPv4 없이 사용되거나 구성될 수 없으며, IPv6에는 IPv6 루프백이 구성되어 있어야 합니다(::1).
Telnet	Telnet을 사용하여 마치 리모트 컴퓨터에 직접 연결되어 있는 것처럼 로그온하여 사용할 수 있습니다.	현재, Telnet은 IPv6을 지원하지 않습니다.
라우트 추적	경로를 판별하는 기본 TCP/IP 툴, iSeries Navigator 및 5250에서 사용할 수 있습니다.	IPv6에서도 동일하며, IPv6은 5250 및 iSeries Navigator에 대해 지원됩니다.
전송층	TCP, UDP, RAW. 새로운 전송인 SCTP(스트림 제어 전송 프로토콜)는 TCP와 UDP의 최고 피쳐 즉, 보장된 무접속 통신을 제공하기 위한 것입니다. SCTP는 가장 초기 스테이지에 있으며, iSeries에서 지원되지 않습니다.	동일한 세 개의 전송이 존재하며 기능적으로 IPv6용으로 변경된 사항은 없습니다.
미지정 주소	명확히 지정되지 않은 것. 소켓 프로그래밍은 INADDR_ANY로 0.0.0.0을 사용합니다.	::/128(128개의 0비트)로 정의됩니다. 일부 인접 노드 발견 패킷 및 소켓과 같은 여러가지 다른 문맥에서 소스 IP로 사용됩니다. 소켓 프로그래밍은 in6addr_any로 ::/128을 사용합니다.
VPN(가상 사설망)	VPN(IPsec 사용)을 사용하여 기존 공용 네트워크를 통해 보안이 된 사설망을 확장할 수 있습니다.	현재, VPN은 IPv6을 지원하지 않습니다. 그러나, IPv6이 IPv4에서 터널링되면 기존 iSeries VPN 설비가 IPv4 통신에 적용된 후 투명하게 IPv6 패킷로드를 처리할 수 있습니다.


IPv6 문제 해결

서버에 IPv6을 구성했으면 IPv4에서와 동일한 몇가지 문제 해결 툴을 사용할 수도 있습니다. 예를 들어, 라우트 추적 및 PING과 같은 툴은 IPv4 및 IPv6 주소 형식을 모두 승인하므로 두 유형의 네트워크 모두에 대한 연결 및 라우트를 테스트하는데 사용할 수 있습니다. 또한, 통신 추적 기능을 사용하여 IPv4 및 IPv6 통신 회선에서 자료를 추적할 수도 있습니다.

IPv4 및 IPv6에 관련된 문제점을 해결하는 기술을 제공하는 일반 문제 해결 안내서는 TCP/IP 문제 해결을 참조하십시오.

IPv6 관련 정보

IPv6에 대한 자세한 정보는 다음 정보 소스를 참조하십시오.

IETF(Internet Engineering Task Force)(<http://www.ietf.cnri.reston.va.us/>) 
IPv6을 포함하여 인터넷 프로토콜을 개발하는 그룹에 대해 배울 수 있습니다.

IP Version 6(IPv6)(<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 
현재 IPv6 스펙 및 IPv6에 대한 여러가지 소스 참조가 나와 있습니다.

IPv6 Forum(<http://www.ipv6forum.com/>) 
최근의 IPv6 개발에 대해 알리는 소식지 및 이벤트에 대해 나와 있습니다.

제 4 장 TCP/IP 설정 계획

iSeries 서버의 설치 및 구성을 시작하기 전에 잠시 운영 계획을 세우십시오. 다음 주제에서 계획 지침을 참조할 수 있습니다. 이러한 계획 지침은 IPv4를 사용한 기본 TCP/IP 설정에 관한 것입니다. IPv6을 구성하려면 IPv6 구성에서 설정 요구사항 및 구성 지침을 참조하십시오.

TCP/IP 설정 요구사항

TCP/IP 설정시 필요한 기본 구성 정보를 수집하고 기록하십시오.

TCP/IP 보안 고려사항

네트워크의 새로운 멤버로서 보안 요구를 고려하십시오.

TCP/IP 설정 요구사항

이 페이지를 인쇄하여 사용자 서버와 그 서버가 연결되어 있는 TCP/IP 네트워크에 관한 구성 정보를 기록하십시오. 나중에 TCP/IP를 구성할 때 이 정보를 참조해야 합니다. 표 아래 나오는 지침을 따라 처음 두 행의 값을 판별할 수 있습니다. 이들 용어 중에 모르는 용어가 있을 경우 IBM 레드북 TCP/IP for AS/400: More

Cool Things Than Ever  의 제 2 장, "TCP/IP: Basic Installation and Configuration"을 참조하십시오.

필수 정보	시스템	예
시스템에 설치된 통신 어댑터의 유형(아래의 지침 참조)		이더넷
자원명		CMN01
iSeries 서버의 IP 주소		199.5.83.158
iSeries 서버의 서브네트 마스크		255.255.255.0
게이트웨이 주소		199.5.83.129
사용자 시스템의 호스트명 및 정의역명		sys400.xyz.company.com
정의역명 서버의 IP 주소		199.4.191.76

통신 어댑터 정보를 찾으려면 다음 단계를 따르십시오.

1. 서버 명령행에서 go hardware를 입력하고 **Enter**를 누르십시오.
2. 통신 자원에 대한 작업(옵션 1)을 선택하려면 1을 입력한 후 **Enter**를 누르십시오.

통신 자원은 자원 이름별로 나옵니다. 자원에 대한 작업을 하거나 추가 정보를 보려면 화면에 나오는 지침을 따르십시오.

다음에 수행할 작업:

TCP/IP 설치

TCP/IP 보안 고려사항

TCP/IP 구성을 계획할 때는 항상 보안 요구를 고려해야 합니다. 다음과 같은 보안 전략을 이용하여 TCP/IP가 노출되는 것을 제한할 수 있습니다.

- **필요한 TCP/IP 어플리케이션만 시작합니다.**

TCP/IP 어플리케이션마다 자체적인 고유 보안 노출을 가지고 있습니다. 특정 어플리케이션에 대한 요구를 거부하는 데 있어서 라우터의 영향을 받지 않습니다. 2차적인 보안 수단으로서 필요 없는 어플리케이션은 그 자동시작 값을 NO로 설정하십시오.

- **TCP/IP 어플리케이션이 실행되는 시간을 제한합니다.**

서버 실행 시간을 줄임으로써 노출을 제한하십시오. 가능하다면 업무 시간 이외에는 FTP 및 Telnet 등의 TCP/IP 서버를 중단시키십시오.

- **TCP/IP 어플리케이션을 시작하고 변경할 수 있는 사용자를 제어합니다.**


TCP/IP 구성 설정을 변경하기 위해서는 디폴트로 *IOSYSCFG 권한이 필요합니다. *IOSYSCFG 권한이 없는 사용자의 경우 *ALLOBJ 권한 또는 TCP/IP 시작 명령에 대한 명시적 권한이 필요합니다. 사용자에게 특수 권한을 부여하는 것은 곧 보안 노출을 의미합니다. 각 사용자에게 특수 권한을 부여할 필요가 있는지를 평가하고 특수 권한을 최소 범위로 유지하십시오. 또한 특수 권한을 가지고 있는 사용자를 계속 추적하고 그 권한에 대한 요구도 정기적으로 검토하십시오. 이렇게 하면 업무 시간 이외에 발생할 가능성이 있는 서버 액세스도 제한할 수 있습니다.

- **TCP/IP 라우팅을 제어합니다.**

- IP 이송을 허용하지 않음으로써 해커가 다른 보안 시스템을 공격하기 위해 웹 서버를 사용할 수 없게 합니다.
- 공용 웹 서버에 대한 라우트(인터넷 서비스 제공자에 대한 디폴트 라우트)를 하나만 정의합니다.
- 웹 서버의 TCP/IP 호스트 표에 내부 보안 시스템의 호스트명 및 IP 주소를 구성하지 않습니다. 이 표에는 연결할 필요가 있는 기타 공용 서버의 이름만 넣으십시오.

- **리모트, 대화식 사인 온을 위해 설계된 TCP/IP 서버를 제어합니다.**

FTP 및 Telnet 등의 어플리케이션은 외부 공격에 매우 취약합니다. 노출을 제어하는 방법에 대한 세부사항

은 iSeries 보안을 위한 추가 정보 및 툴  에서 대화식 사인 온을 제어하는 추가 정보에 관한 장을 참조하십시오.

보안 및 사용할 수 있는 옵션에 대한 자세한 정보는 iSeries와 인터넷 보안을 참조하십시오.

제 5 장 TCP/IP 설치

OS/400과 함께 기본 TCP/IP 지원이 제공되어 iSeries 서버를 네트워크에 연결할 수 있게 합니다. 그러나 Telnet, FTP 및 SMTP와 같은 TCP/IP 어플리케이션을 사용하려는 경우 TCP/IP 연결 유틸리티를 설치해야 합니다. 오퍼레이팅 시스템에 포함되어 있는 이 유틸리티는 별도로 설치가 가능한 사용권 프로그램입니다.

iSeries 서버에 TCP/IP 연결 유틸리티를 설치하려면 다음 단계를 따르십시오.

1. TCP/IP 설치 매체를 서버에 넣으십시오. 설치 매체가 CD-ROM이면 CD-ROM을 광 장치에 넣으십시오. 설치 매체가 테이프이면 테이프 드라이브에 넣으십시오.
2. 명령행에서 GO LICPGM을 입력한 후 **Enter**를 눌러 사용권 프로그램에 대한 작업 화면에 액세스하십시오.
3. 사용권 프로그램에 대한 작업 화면에서 옵션 **11**(사용권 프로그램 설치)을 선택하여 사용권 프로그램 및 사용권 프로그램의 선택적 파트 리스트를 보십시오.
4. 57xxTC1(iSeries용 TCP/IP 연결 유틸리티) 옆의 옵션 열에 **1**(설치)을 입력하십시오. **Enter**를 누르십시오. 설치할 사용권 프로그램 확인 화면에 설치를 위해 선택한 사용권 프로그램이 나옵니다. **Enter**를 누르고 확인하십시오.
5. 옵션 설치 표시 화면에 다음 선택사항을 채우십시오.

설치 장치	CD-ROM 장치에서 설치하면 Q0PT를 입력하십시오. 테이프 드라이브에서 설치하면 TAP01을 입력하십시오.
설치할 오브젝트	이 옵션으로는 프로그램과 언어 오브젝트 모두 설치, 프로그램만 설치 또는 언어 오브젝트만 설치를 수행할 수 있습니다.
자동 재시작	이 옵션은 설치 프로세스가 성공적으로 완료되었을 때 시스템이 자동으로 시작하는지 판별합니다.

TCP/IP 연결 유틸리티가 성공적으로 설치되면 사용권 프로그램에 대한 작업 메뉴 또는 사인 온 화면이 나옵니다.

6. 옵션 **50**(메세지 기록부 표시)을 선택하고 사용권 프로그램이 성공적으로 설치되었는지 확인하십시오.

설치 중 오류가 발생하면 사용권 프로그램에 대한 작업 화면 맨 아래에 사용권 프로그램에 대한 작업이 완료되지 않았습니까?라는 메세지가 나옵니다. 문제가 발생하더라도 TCP/IP 연결 유틸리티 설치를 재시도하십시오. 문제를 해결할 수 없으면 지원을 요청하십시오.

주:

다음과 같은 기타 사용권 프로그램들을 설치할 수 있습니다.

- Windows 95/NT용 iSeries Access(5769-XD1 V3R1M3 또는 그 이상)은 일부 TCP/IP 구성요소를 구성하는 데 사용되는 iSeries Navigator 지원을 제공합니다.
- iSeries용 IBM HTTP Server(57xx-DG1)는 웹 서버 지원을 제공합니다.

- TCP/IP 어플리케이션 중 일부의 경우 추가 사용권 프로그램을 설치해야 사용할 수 있습니다. 필요한 프로그램을 알아보려면 원하는 특정 어플리케이션의 설정 지침을 검토하십시오.

제 6 장 TCP/IP 구성

처음으로 TCP/IP를 구성하거나, IPv6 기능을 사용하도록 기존 구성을 변경할 수 있습니다. 이 주제에서는 이들 각 상황에서 TCP/IP를 구성하는 지침을 제공합니다. 서버에 TCP/IP를 구성하는 방법에 대한 지침은 아래 옵션을 참조하십시오.

처음으로 TCP/IP 구성

새로운 서버를 설정하는 경우 이 지침을 사용하십시오. 처음으로 연결을 설정하고 TCP/IP를 구성할 것입니다.

IPv6 구성

이 지침을 사용하여 IPv6 기능용으로 서버를 구성하십시오. 이 인터넷 프로토콜의 향상된 주소지정 기능과 견고한 피처의 혜택을 누릴 것입니다. IPv6에 대해 잘 모르겠으면 IPv6(인터넷 프로토콜 버전 6)에서 개요를 보십시오. IPv6을 구성하기 전에 서버에 TCP/IP가 구성되어 있어야 합니다.

오퍼레이팅 시스템이 제한 상태에 있을 때 TCP/IP 구성

오퍼레이팅 시스템이 제한 상태일 때 TCP/IP를 실행해야 하는 경우 이 방법을 사용하십시오.

처음으로 TCP/IP 구성

새로운 서버에 TCP/IP를 설정하는 다음 메소드들 중 하나를 선택하십시오.

EZ-Setup 마법사를 사용하여 TCP/IP 구성

PC에서 EZ-Setup 마법사를 사용할 수 있는 경우 이 우선 메소드를 사용하십시오. EZ-Setup 마법사는 iSeries 서버와 함께 패키징되어 있습니다.

문자 기반의 인터페이스를 사용하여 TCP/IP 구성

EZ-Setup 마법사를 사용할 수 없는 경우 이 메소드를 사용하십시오. 예를 들어, iSeries Navigator를 실행하기 전에 기본 TCP/IP 구성을 필요로 하는 PC에서 iSeries Navigator를 사용하려면 문자 기반의 인터페이스를 사용하여 기본 구성을 수행해야 합니다.

EZ-Setup 마법사를 사용하여 TCP/IP 구성

iSeries Navigator는 TCP/IP를 구성하기 위한 간결한 대화 상자 및 마법사를 제공하는 그래픽 사용자 인터페이스입니다. 초기 설정의 경우, iSeries Navigator의 EZ-Setup 마법사를 사용하여 연결을 설정하고 최초로 TCP/IP를 구성하십시오. 인터페이스가 사용하기 쉬우므로 서버와 작업하기 위한 우선 메소드입니다. EZ-Setup 마법사가 들어 있는 CD-ROM은 iSeries 서버에 패키징되어 있습니다.

서버를 구성하려면 다음 단계를 따르십시오.

1. EZ-Setup 마법사를 사용하십시오. 서버와 함께 패키징된 CD-ROM에서 마법사를 액세스하십시오. 마법사의 지침에 따라 TCP/IP를 구성하십시오.

2. TCP/IP 시작


- a. iSeries Navigator에서 서버 -> 네트워크를 확장하십시오.
- b. **TCP/IP** 구성을 마우스 오른쪽 버튼으로 클릭하여 시작을 선택하십시오. TCP/IP가 시작할 때 자동으로 시작하도록 설정한 모든 인터페이스와 서버가 시작됩니다.

서버에 TCP/IP 구성을 완료했습니다. 네트워킹 요구사항이 변경됨에 따라 iSeries Navigator를 사용하여 구성을 수정하십시오. iSeries Navigator로 TCP/IP 사용자 정의를 참조하여 라우트 및 인터페이스를 추가하거나 IPv6 구성을 참조하여 네트워크에서 인터넷 프로토콜 버전 6을 사용하십시오.

문자 기반의 인터페이스를 사용하여 TCP/IP 구성

iSeries Navigator의 EZ-Setup 마법사를 사용할 수 없으면 문자 기반의 인터페이스를 대신 사용하십시오. 예를 들어, iSeries Navigator를 실행하기 전에 기본 TCP/IP 구성을 필요로 하는 PC에서 iSeries Navigator를 사용하려면 문자 기반의 인터페이스를 사용하여 기본 구성을 수행해야 합니다.

이 섹션에서 설명된 구성 단계를 수행하기 위해서는 사용자 프로파일에 *IOSYSCFG 특수 권한이 필요합니다.

이 유형의 권한에 대한 자세한 정보는 iSeries 보안 참조서  에서 사용자 프로파일에 관한 장을 참조하십시오.

문자 기반의 인터페이스를 사용하여 TCP/IP를 구성하려면 다음 단계를 따르십시오.

1. 명령행에서 GO TCPADM을 입력하여 TCP/IP 관리 메뉴를 표시한 후 Enter를 누르십시오.
2. 옵션 1(TCP/IP 구성)을 지정하여 TCP/IP 메뉴 구성(CFGTCP)을 표시한 후 Enter를 누르십시오. 이 메뉴를 사용하여 구성 타스크를 선택하십시오. 서버 구성을 시작하기 전에 메뉴를 검토하십시오.

다음 단계를 수행하여 서버에 TCP/IP를 구성하십시오.

1. 회선 설명 구성
2. IP 데이터그램 이송 켜기
3. 인터페이스 구성
4. 라우트 구성
5. 로컬 정의역 및 호스트명 정의
6. 호스트 표 정의
7. TCP/IP 시작

회선 설명 구성(이더넷)

이 지침은 이더넷 통신 어댑터를 통해 TCP/IP를 구성하는데 관한 것입니다. 그러나, 토큰링과 같은 다른 유형의 어댑터를 사용하는 경우에는 TCP/IP Configuration and Reference의 Appendix A에서 어댑터 고유의 명령을 참조하십시오.

회선 설명을 구성하려면 다음 단계를 따르십시오.

1. 명령행에서 CRTLINETH를 입력하여 회선 설명 작성(이더넷) (CRTLINETH) 메뉴를 액세스하고 Enter를 누르십시오.
2. 회선 설명을 지정하고 Enter를 누르십시오. (임의의 이름을 사용하십시오.)
3. 자원명을 지정하고 Enter를 누르십시오.

다음에 수행할 작업:

IP 데이터그램 이송 켜기

IP 데이터그램 이송 켜기

패킷이 서로 다른 서브네트로 이송될 수 있도록 IP 데이터그램 이송을 켜십시오.

IP 데이터그램 이송을 켜려면 다음 단계를 따르십시오.

1. 명령행에 CHGTCPA를 입력하고 F4를 누르십시오.
2. IP 데이터그램 이송 프롬프트에 대해 *YES를 입력하십시오.

다음에 수행할 작업:

인터페이스 구성

인터페이스 구성

인터페이스를 구성하려면 다음 단계를 따르십시오.

1. 명령행에서 CFGTCP를 입력하여 TCP/IP 구성 메뉴를 액세스하고 Enter를 누르십시오.
2. TCP/IP 구성 메뉴에서 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
3. 옵션 1(추가)을 지정하여 TCP/IP 인터페이스 추가 표시 화면을 표시하고 Enter를 누르십시오.
4. iSeries 서버를 표시하려는 주소 값, 서브네트 마스크 주소 및 이전에 정의한 회선 설명 이름을 지정한 후 Enter를 누르십시오.

인터페이스를 시작하려면 구성된 인터페이스에 대해 옵션 9(시작)를 지정하고 Enter를 누르십시오.

다음에 수행할 작업:

라우트 구성

라우트 구성

리모트 네트워크에 도달하기 위해서는 최소한 하나의 라우팅 항목이 필요합니다. 수동으로 추가한 라우팅 항목이 없는 경우에는 서버가 접속되어 있는 네트워크와 동일한 네트워크에 있지 않은 시스템에 도달할 수 없습니다. 리모트 네트워크에서 서버에 도달하려 하는 TCP/IP 클라이언트가 제대로 기능하기 위해서는 라우팅 항목도 추가해야 합니다.

항상 최소한 하나의 디폴트 라우트(*DFTRROUTE)에 대한 항목을 갖도록 라우팅 표가 정의되게 계획해야 합니다. 라우팅 표의 어느 항목에도 일치되는 것이 없는 경우에는 첫 번째로 사용할 수 있는 디폴트 라우트 항목에 지정된 IP 라우터로 자료가 송신됩니다.

디폴트 라우트를 구성하려면 다음 단계를 따르십시오.

1. TCP/IP 구성 메뉴에서 옵션 2(TCP/IP 라우트에 대한 작업)를 선택하고 Enter를 누르십시오.
2. 옵션 1(추가)을 지정하여 TCP/IP 라우트 추가(ADDTCPRTE) 표시 화면으로 찾아 가서 Enter를 누르십시오.
3. 라우트 목적지에는 *DFTRROUTE를, 서브네트 마스크에는 *NONE을, 다음 홉(hop)에는 IP 주소를 지정하고 Enter를 누르십시오.

다음에 수행할 작업:

로컬 정의역 및 호스트명 정의

로컬 정의역 및 호스트명 정의

로컬 정의역 및 호스트명을 정의하려면 다음 단계를 따르십시오.

1. TCP/IP 구성 메뉴에서 옵션 12(TCP/IP 도메인 변경)를 선택하고 Enter를 누르십시오.
2. 선택한 이름이 로컬 호스트명 및 정의역명이 되도록 지정하고 다른 매개변수는 디폴트 값으로 두고 Enter를 누르십시오.

다음에 수행할 작업:

호스트 표 정의

호스트 표 정의

호스트 표를 정의하려면 다음 단계를 따르십시오.

1. TCP/IP 구성 메뉴에서 옵션 10(TCP/IP 호스트 표에 대한 작업)을 선택하고 Enter를 누르십시오.
2. 옵션 1(추가)을 지정하여 TCP/IP 호스트 표 항목 추가 표시 화면으로 찾아 가서 Enter를 누르십시오.
3. IP 주소, 연관 로컬 호스트명 및 완전 규정 호스트명을 지정한 후 Enter를 누르십시오.
4. 필요하면 더하기 부호(+)를 지정하여 둘 이상의 호스트명에 대한 공간을 사용할 수 있도록 하십시오.
5. 이름으로 통신하려는 네트워크상의 각 호스트에 대해 이 단계들을 반복하고 각각에 대한 항목을 추가하십시오.

다음에 수행할 작업:

TCP/IP 시작

TCP/IP 시작

TCP/IP를 시작하기 전에는 TCP/IP 서비스를 사용할 수 없습니다.

TCP/IP를 시작하려면 명령행에서 STRTCP를 입력하십시오.

TCP/IP 시작(STRTCP) 명령은 TCP/IP 처리를 초기화하고 활성화하며, TCP/IP 인터페이스를 시작하고, 서버 작업을 시작합니다. STRTCP 명령은 AUTOSTART *YES인 TCP/IP 인터페이스 및 서버만 시작합니다.

서버에 TCP/IP 구성을 완료했습니다. 네트워킹 요구사항이 변경됨에 따라 iSeries Navigator를 사용하여 구성을 수정하십시오. iSeries Navigator로 TCP/IP 사용자 정의를 참조하여 라우트 및 인터페이스를 추가하거나 IPv6 구성을 참조하여 네트워크에서 인터넷 프로토콜 버전 6을 사용하십시오.

IPv6 구성

네트워크에서 IPv6을 사용하여 차세대 인터넷의 장점을 누릴 수 있습니다. IPv6 기능을 사용하려면 IPv6 전용 회선을 구성하여 TCP/IP 구성을 변경해야 합니다. 2838이나 2849 이더넷 어댑터 또는 구성된 터널 회선(가상 회선)에 회선을 구성해야 합니다. IPv6 구성에 대한 지침은 다음 주제들을 읽으십시오.

설정 요구사항

이 주제는 IPv6용 서버를 구성하기 위한 하드웨어 및 소프트웨어 요구사항을 나열합니다.

IPv6 구성 마법사를 사용한 IPv6 구성

IPv6 구성 마법사 사용에 관한 지침을 참조하여 서버에 IPv6을 구성하십시오.

설정 요구사항

다음 두 가지 유형의 IPv6 구성 중 어느 것이 해당 상황에 적당한지 판별하십시오. 어느 유형을 선택할지 확실하지 않은 경우에는 IPv6 시나리오에서 예를 참조하십시오.

다음과 같은 요구사항을 만족시켜 IPv6이 서버에서 기능할 수 있도록 하십시오.

IPv6용 이더넷 회선 구성:

- OS/400 버전 5 릴리스 2 이상
- Windows용 iSeries Access 및 iSeries Navigator
 - iSeries Navigator의 네트워크 구성요소
- IPv6 전용 2838 또는 2849 이더넷 어댑터.
- 인접한 LAN 밖에 있는 IPv6 통신을 송신하려는 경우에만 IPv6 가능 라우터가 필요합니다.
- 서버에서 TCP/IP가 실행 중이어야 하므로 별도의 물리적 어댑터에 TCP/IP(IPv4 사용)를 구성해야 합니다. IPv4용 서버를 구성하지 않았으면 IPv4용 회선을 구성하기 전에 처음으로 TCP/IP 구성을 참조하십시오.

구성된 터널 회선 작성(TNLCFG64):

- OS/400 버전 5 릴리스 2 이상
- Windows용 iSeries Access 및 iSeries Navigator
 - iSeries Navigator의 네트워크 구성요소
- IPv6용 터널 회선을 구성하기 전에 서버에 TCP/IP(IPv4 사용)를 구성해야 합니다. IPv4용 서버를 구성하지 않았으면 처음으로 TCP/IP 구성을 참조하십시오.

마법사를 액세스하는데 대한 지침을 보려면 IPv6 구성 마법사를 사용한 IPv6 구성으로 찾아 가십시오.

IPv6 구성 마법사를 사용한 IPv6 구성

서버에 IPv6을 구성하려면 iSeries Navigator에서 IPv6 구성 마법사를 사용하여 서버의 구성을 변경해야 합니다. IPv6은 iSeries Navigator에서만 구성 가능할 것이며, 문자 기반의 인터페이스에서는 구성 가능하지 않을 수도 있습니다.

주: 문자 기반의 인터페이스에서 회선 설명 작성(이더넷) CRTLINETH 명령을 사용하여 IPv6 이더넷 회선 설명을 구성할 수도 있습니다. 그러나, 16진 멀터캐스트 그룹 주소인 333300000001을 지정해야 합니다. 그런 후, **IPv6 Configuration** 마법사를 사용하여 IPv6 구성을 완료해야 합니다.

마법사는 다음과 같은 입력을 필요로 합니다.

IPv6용 이더넷 회선 구성:

이 구성으로 IPv6 근거리 통신망(LAN)을 통해 IPv6 패킷을 송신할 수 있습니다. 마법사는 IPv6이 구성 될 서버상의 하드웨어 통신 자원의 이름(예를 들어, CMN01)을 필요로 합니다. 이는 현재 IPv4용으로 구성되어 있지 않은 2838 또는 2849 이더넷 어댑터여야 합니다. IPv6 근거리 통신망(LAN) 작성에서 IPv6 용 이더넷 회선을 구성할 상황을 보여주는 시나리오를 참조하십시오.

구성된 터널 회선 작성(TNLCFG64):

이 구성으로 IPv4 네트워크를 통해 IPv6 패킷을 송신할 수 있습니다. 마법사는 로컬 종료점에 대한 IPv4 주소 및 터널과 연관된 로컬 인터페이스에 대한 IPv6 주소를 필요로 합니다. IPv4 근거리 통신망(LAN)을 통한 IPv6 패킷 송신 및 IPv4 광역 네트워크(WAN)를 통한 IPv6 패킷 송신에서 IPv6용으로 구성된 터널 회선을 작성하는 두 가지 상황을 보여주는 시나리오를 참조하십시오.

IPv6 구성 마법사를 사용하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> **TCP/IP** 구성을 확장하십시오.
2. **IPv6**을 마우스 오른쪽 버튼으로 클릭하고 **IPv6** 구성을 선택하십시오.
3. 마법사의 지침에 따라 서버에 IPv6을 구성하십시오.

오퍼레이팅 시스템이 제한 상태에 있을 때 TCP/IP 구성

상황

네트워크 관리자는 서버에 대한 백업 상태 보고서를 확보해야 합니다. 백업 프로시저를 실행 중일 때 사용자가 구성을 변경하지 못하도록 오퍼레이팅 시스템은 제한 상태에 있어야 합니다. 관리자는 리모트 상태이므로 PDA 장치(또는 임의의 TCP/IP 네트워킹 장치)를 사용하여 상태 보고서에 액세스합니다. PDA는 서버와 통신하기 위해 사용할 수 있는 활동 TCP/IP 인터페이스가 필요한 소켓 사용 어플리케이션을 사용합니다. 이 통신을 허용하려면 먼저 특수 매개변수를 사용하여 TCP/IP를 시작해야 합니다. TCP/IP를 시작한 후, 시스템에 대한 액세스를 허용하기 위해 특정 TCP/IP 인터페이스를 시작해야 합니다. 아래 정보가 추가 정보를 제공합니다.

전제조건

iSeries 서버가 OS/400(R) V5R2 또는 그 이상을 실행 중입니다.

제한사항

오퍼레이팅 시스템이 제한 상태에서 실행 중일 때 다음 제한이 적용됩니다.

- TCP/IP 서버(STRTCPSPRV CL 명령)에는 사용 중인 서브시스템이 필요하므로 이 서버를 시작할 수 없습니다.

- 네트워크 서버 설명(NWSD) 또는 네트워크 인터페이스 설명(NWID)에 접속되지 않는 특정 회선(이더넷, 토큰링 또는 DDI)에 대해 한 인터페이스만을 시작할 수 있습니다.

구성 단계

1. 특수 매개변수를 사용하여 TCP/IP 시작

iSeries 시스템이 제한 상태에 있을 때, 명령행 인터페이스에서 STRTCP STRSVR(*NO) STRIFC(*NO) 명령을 처리하십시오. 이들이 오퍼레이팅 시스템이 제한 상태에 있을 때 승인되는 유일한 매개변수입니다. 위의 명령은 TCP/IP를 시작하지만, TCP/IP 어플리케이션 서버나 IP 인터페이스를 시작하지 않으며 시작할 수 없습니다.

2. 특정 TCP/IP 인터페이스 시작

제한 상태에서 TCP/IP를 시작한 후, 소켓 사용 어플리케이션에 필요한 특정 인터페이스를 시작할 수 있습니다.

- a. 시작하려는 인터페이스가 *ELAN, *TRLAN 또는 *DDI의 회선 설명을 사용하는지 확인하십시오.

인터페이스에 대한 회선 유형을 보려면, 명령행 인터페이스에서 CFGTCP를 입력하고 옵션 1(TCP/IP 인터페이스에 대한 작업)을 입력하십시오.

- b. 인터페이스가 NWID 또는 NWSD에 접속되지 않는지 확인하십시오. 다른 모든 시도는 오류 메시지를 표시합니다.

인터페이스가 NWID 또는 NWSD에 접속되지 않았음을 확인하려면, 명령행 인터페이스에서 DSPLIND abc를 입력하십시오(여기서 abc는 회선 설명의 이름입니다). 자원명이 *NWID 또는 *NWSD가 아닌지 확인하십시오.

주: 인터페이스가 NWID 또는 NWSD에 접속되어 있는 경우, 다른 인터페이스를 선택할 것을 권장합니다.

- c. 마지막으로, 인터페이스를 시작하십시오. 명령행 인터페이스에서 STRTCPIFC INTNETADR('a.b.c.d')를 입력하십시오. a.b.c.d를 인터페이스 IP 주소로 대체하십시오.

주: STRTCPIFC INTNETADR(*AUTOSTART)가 지정되지 않도록 해야 합니다.

3. 인터페이스가 사용 중인지 확인하십시오.

어플리케이션에 대한 특정 인터페이스를 핑(Ping)하십시오. 제한 상태에서 동작할 TCP/IP 관련 유틸리티는 매우 적습니다. 그러나 Ping 및 Netstat를 사용할 수 있습니다. Ping 및 netstat 명령 사용에 대한 자세한 정보는 TCP/IP 문제 해결 안에 있는 네트워크 구조를 확인하는 툴을 검토하십시오.

제 7 장 iSeries Navigator로 TCP/IP 사용자 정의

TCP/IP를 구성했으면 사용자 구성을 사용자 정의하는지 결정할 수 있습니다. 네트워크가 커짐에 따라 등록 정보를 변경하고, 인터페이스를 추가하고, 서버에 라우트를 추가해야 할 수도 있습니다. IPv6 어플리케이션을 사용하도록 IPv6(인터넷 프로토콜 버전 6)용으로 서버를 구성해야 할 수도 있습니다. iSeries Navigator에서 방법을 사용하여 이러한 작업을 신속히 수행하십시오.

아래 주제 중에서 선택하여 iSeries Navigator를 사용하여 구성을 사용자 정의하십시오. 이러한 주제는 iSeries Navigator로 TCP/IP 구성을 관리하기 위한 시작점을 제공합니다.

TCP/IP 설정 변경

IPv6 구성

IPv4 인터페이스 추가

IPv6 인터페이스 추가

IPv4 라우트 추가

IPv6 라우트 추가

TCP/IP 설정 변경

iSeries Navigator를 사용하여 TCP/IP 설정을 보고 변경할 수 있습니다. 예를 들어, 호스트 또는 정의역명, 이름 서버, 호스트 표 항목, 시스템 속성, 포트 제한사항, 서버 또는 클라이언트 연결에 대한 등록 정보를 변경할 수 있습니다. 일반 등록 정보나 전송과 같이 IPv4나 IPv6에 고유한 등록 정보를 변경할 수도 있습니다.

일반 TCP/IP 등록 정보 페이지를 액세스하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크를 선택하십시오.
2. TCP/IP 구성을 마우스 오른쪽 버튼으로 클릭하고 등록 정보를 선택하여 TCP/IP 등록 정보 대화를 여십시오.
3. 대화 맨 위에 있는 탭을 선택하여 TCP/IP 정보를 보거나 편집할 수 있습니다.

호스트 표 항목을 추가 및 변경하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크를 선택하십시오.
2. TCP/IP 구성을 마우스 오른쪽 버튼으로 클릭하고 호스트 표를 선택하여 호스트 표 대화를 여십시오.
3. 호스트 표 대화를 사용하여 호스트 표 항목을 추가, 편집 또는 제거하십시오.

IPv4 고유의 등록 정보 페이지를 액세스하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크를 선택하십시오.
2. IPv4를 마우스 오른쪽 버튼으로 클릭하고 등록 정보를 선택하여 IPv4 등록 정보 대화를 여십시오.
3. 대화 맨 위에 있는 탭을 선택하여 IPv4 등록 정보 설정을 보고 편집하십시오.

IPv6 고유의 등록 정보 페이지를 액세스하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크를 선택하십시오.
2. **IPv6**을 마우스 오른쪽 버튼으로 클릭하고 등록 정보를 선택하여 **IPv6 등록 정보** 대화를 여십시오.
3. 대화 맨 위에 있는 탭을 선택하여 IPv6 등록 정보 설정을 보고 편집하십시오.

IPv6 구성

IPv6에 대해 잘 모르겠으면 IPv6(인터넷 프로토콜 버전 6)에서 개요를 보십시오.

IPv6을 구성하려면 **IPv6 구성** 마법사를 사용하여 서버의 구성을 변경해야 합니다. 마법사를 사용하기 전에 IPv6 구성에서 지침 및 특별 요구사항을 참조하십시오.

IPv4 인터페이스 추가

새 IPv4 인터페이스를 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> **TCP/IP 구성** --> **IPv4**를 선택하십시오.
2. 인터페이스를 마우스 오른쪽 버튼으로 클릭하여 새 인터페이스를 선택하고, 근거리 통신망(LAN), 광역 네트워크(WAN) 또는 가상 IP를 선택하여 적당한 유형의 IPv4 인터페이스를 작성하십시오.
3. 마법사의 지침에 따라 새 IPv4 인터페이스를 작성하십시오.

IPv6 인터페이스 추가

새 IPv6 인터페이스를 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> **TCP/IP 구성** --> **IPv6**을 선택하십시오.
2. 인터페이스를 마우스 오른쪽 버튼으로 클릭하고 새 인터페이스를 선택하십시오.
3. 마법사의 지침에 따라 새 IPv6 인터페이스를 작성하십시오.

IPv4 라우트 추가

라우트 정보를 변경할 때 변경 정보는 즉시 유효합니다.

새 IPv4 라우트를 구성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> **TCP/IP 구성** --> **IPv4**를 선택하십시오.
2. 라우트를 마우스 오른쪽 버튼으로 클릭하고 새 라우트를 선택하십시오.
3. 마법사의 지침에 따라 새 IPv4 라우트를 구성하십시오.

IPv6 라우트 추가

라우트 정보를 변경할 때 변경 정보는 즉시 유효합니다.

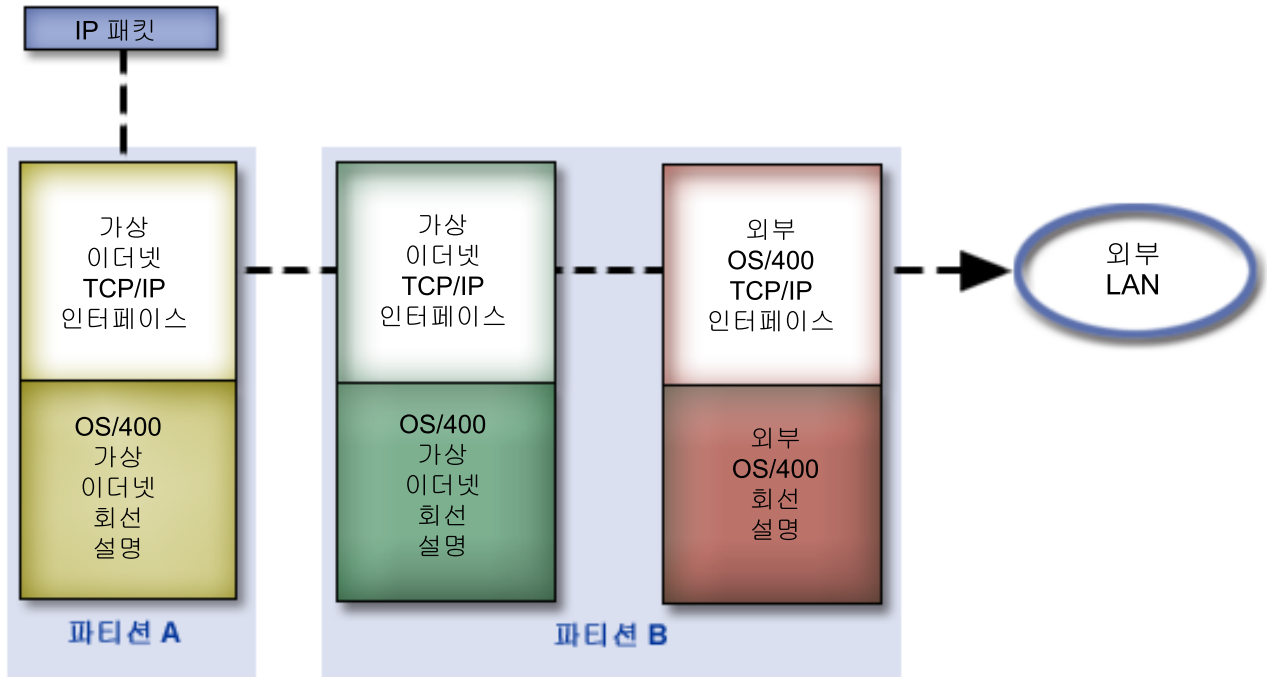
새 IPv6 라우트를 구성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> 네트워크 --> **TCP/IP 구성** --> **IPv6**을 선택하십시오.

2. 라우트를 마우스 오른쪽 버튼으로 클릭하고 새 라우트를 선택하십시오.
3. 마법사의 지침에 따라 새 IPv6 라우트를 구성하십시오.

제 8 장 가상 이더넷을 외부 LAN에 연결하는 TCP/IP 기술

▶ 파티션간 통신에 가상 이더넷 네트워크를 사용 중인 경우, 이들 파티션이 실제 외부 LAN과 통신할 수 있어야 합니다. 다양한 TCP/IP 기술을 사용하여 가상 이더넷 네트워크를 외부 LAN에 연결하는 여러 가지 방법이 있습니다. TCP/IP 통신이 가상 이더넷 네트워크와 외부 LAN 사이에 흐를 수 있게 해야 합니다. 이 그림은 IP 패킷의 논리적 흐름을 보여줍니다.



파티션 A에 의해 시작된 IP 통신은 가상 이더넷에서 파티션 B의 가상 이더넷 인터페이스로 이동합니다. 아래에 설명된 세 가지 TCP/IP 기술 중 하나를 구현하여 IP 패킷이 외부 인터페이스에서 계속적으로 목적지로 향하도록 할 수 있습니다.

가상 이더넷과 외부 LAN을 연결하는 세 가지 방법이 있습니다. 각 방법은 TCP/IP 및 사용자 환경의 지식에 따라 실행 가능성에 약간의 차이가 있습니다. 다음 방법 중 하나를 선택하십시오.

- **프록시 ARP**

이 방법은 투명한 서브네팅을 사용하여 파티션의 가상 인터페이스를 외부 인터페이스와 연관시킵니다. 프록시 ARP 기능은 TCP/IP 스택에 빌드됩니다. 필요한 IP 주소가 있을 경우, 이 접근방식이 권장됩니다.

- **네트워크 주소 변환**


OS/400 패킷 필터를 사용하면 파티션과 외부 파티션 사이의 통신량을 라우트할 수 있습니다.

- **TCP/IP 라우팅**

표준 TCP/IP 라우팅이 임의의 다른 LAN에 대한 라우팅을 정의하는 것과 같은 방식으로 가상 이더넷에 대한 통신을 라우트하는 데 사용됩니다. 이것은 네트워크 전체의 라우팅 정보를 갱신하도록 요구합니다.

프록시 ARP 메소드

프록시 ARP 메소드는 일반적으로 투명한 서브네팅이라고 부르는 기술을 사용합니다. 투명한 서브네팅에 대한 자세한 정보를 배울 수 있습니다.

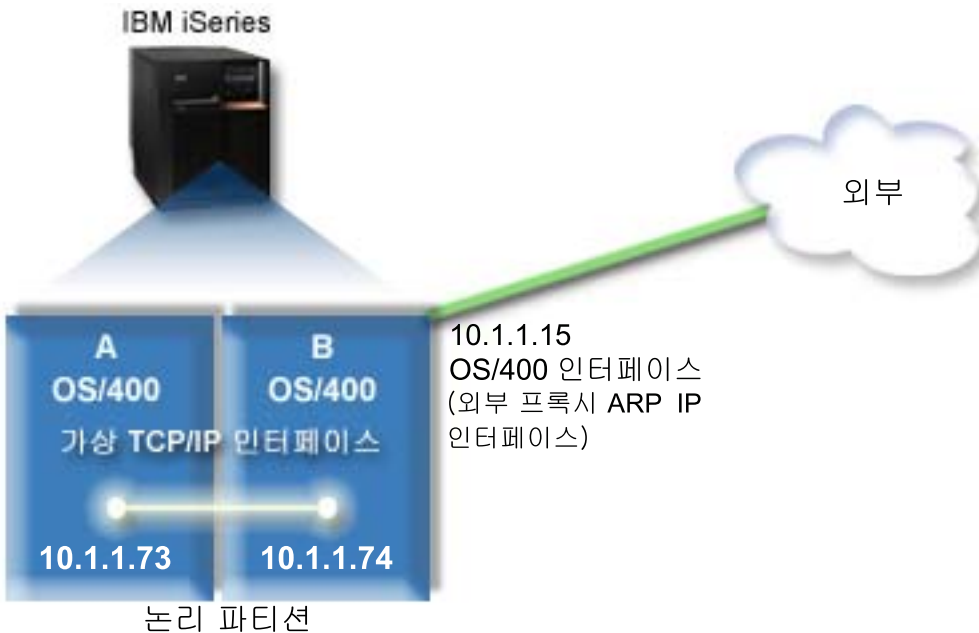
- V4 TCP/IP for AS/400: More Cool Things Than Ever 

이 레드북은 예제 구성을 사용한 일반적인 솔루션을 보여주는 샘플 시나리오를 제공합니다. 또한 iSeries 서버에서 TCP/IP를 계획, 설치, 조정, 구성 및 문제 해결하는 데 도움을 줍니다.

- TCP/IP 라우팅 작업부하 균형 조절

이 주제는 라우팅 및 작업부하 균형 조절에 대한 기술과 지침을 제공합니다.

프록시 ARP 메소드를 사용할 것을 선택하는 경우, 서브네트와 TCP/IP에 대해 이해해야 합니다. 사용자 네트워크가 라우트할 수 있는 IP 주소의 연속적인 블록을 확보해야 합니다. 이 IP 주소 블록을 서브네팅합니다. 이 예에서는 연속적인 네 개의 IP 주소 블록(10.1.1.72부터 10.1.1.75까지)이 사용됩니다. 네 개의 IP 주소 블록이므로 이들 주소에 대한 서브네트 마스크는 255.255.255.252입니다. 이 그림에 표시되는 것처럼 파티션의 가상 TCP/IP 인터페이스에 하나를 지정합니다.



이 예에서, 파티션 A의 TCP/IP 통신량은 가상 이더넷을 지나 파티션 B의 10.1.1.74 인터페이스로 진행합니다. 10.1.1.74가 외부 프록시 ARP 인터페이스 10.1.1.15와 연관되므로, 패킷은 프록시 ARP 인터페이스를 사용하여 가상 이더넷의 밖에서도 계속됩니다.

프록시 ARP 연결 메소드를 사용하도록 가상 이더넷을 구성하려면 다음 구성 작업을 완료하십시오.

1. 논리 파티션이 가상 이더넷에 참여할 수 있도록 설정
2. 이더넷 회선 설명 작성
3. IP 데이터그램 이송 켜기
4. 프록시 ARP를 작동가능하게 하는 인터페이스 작성

- | 5. 파티션 A에 가상 TCP/IP 인터페이스 작성
- | 6. 파티션 B에 가상 TCP/IP 인터페이스 작성
- | 7. 라우트 작성
- | 8. 네트워크 통신 확인

| 1단계: 논리 파티션이 가상 이더넷에 참여할 수 있도록 설정

| 주: 270 및 8xx 모델 서버 이외의 서버를 사용할 경우, 1차 파티션 대신 eServer™용 하드웨어 관리 콘솔(HMC)을 사용하여 이 단계를 수행해야 합니다. 세부사항에 대해서는 가상 이더넷을 참조하십시오.

| 가상 이더넷을 작동할 수 있게 하려면 다음 단계를 따르십시오.

- | 1. 1차 파티션(파티션 A)의 명령행에서 STRSST를 입력하고 Enter를 누르십시오.
- | 2. 서비스 툴 사용자 ID와 암호를 입력하십시오.
- | 3. SST(시스템 서비스 툴) 화면에서 옵션 5(시스템 파티션에 대한 작업)를 선택하십시오.
- | 4. 시스템 파티션에 대한 작업 화면에서 옵션 3(파티션 구성에 대한 작업)을 선택하십시오.
- | 5. F10(가상 이더넷에 대한 작업)을 누르십시오.
- | 6. 파티션 A와 파티션 B에 대한 적합한 열에 1을 입력하여 파티션이 가상 이더넷을 통해 서로 통신할 수 있게 하십시오.
- | 7. 시스템 서비스 툴(SST)을 나가서 명령행으로 리턴하십시오.

| 다음 수행 작업

| 이더넷 회선 설명 작성

| 2단계: 이더넷 회선 설명 작성

| 사용 중인 서버 모델에 따라서 두 가지 방법 중 하나로 이 단계를 수행해야 합니다. 특정 서버 모델을 기반으로 회선 설명 작성을 위한 방법 중 하나를 선택하십시오.

- | • 270 및 8xx 모델 서버에 이더넷 회선 설명 작성
- | • 270 및 8xx 모델 서버 이외의 모든 서버에 이더넷 회선 설명 작성

| 270 및 8xx 모델 서버에 이더넷 회선 설명 작성

| 가상 이더넷을 지원하는 새로운 이더넷 회선 설명을 구성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 WRKHDWRSC *CMN을 입력하고 Enter를 누르십시오.
- | 2. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 7(자원 상세 표시)을 선택하십시오.
| 268C로 식별되는 이더넷 포트가 가상 이더넷 자원입니다. 각 가상 이더넷에 대해 논리 파티션에 연결되는 하나가 있습니다.
- | 3. 자원 상세 표시 화면에서 아래로 화면이동하여 포트 주소를 찾으십시오. 포트 주소는 논리 파티션의 구성 중에 사용자가 선택한 가상 이더넷과 각각 대응합니다.

- | 4. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 5(구성 설명에 대한 작업)를 선택하고 Enter를 누르십시오.
- | 5. 구성 설명에 대한 작업 화면에서 옵션 1(작성)을 선택하고 Enter를 눌러서 회선 설명 이더넷 작성 (CRTLINETH) 화면을 표시하십시오.
 - | a. 회선 설명 프롬프트에 대해 VETH0를 입력하십시오. 이름 VETH0는 임의이지만 논리 파티션이 통신할 수 있게 한 가상 이더넷 페이지의 번호 지정된 열에 해당합니다. 회선 설명과 연관된 가상 이더넷에 대해 동일한 이름을 사용하는 경우, 가상 이더넷 구성을 쉽게 추적할 수 있습니다.
 - | b. 회선 속도 프롬프트에 대해 1G를 입력하십시오.
 - | c. 양방향 전송 프롬프트에 대해 *FULL을 입력하고 Enter를 누르십시오.
 - | d. 최대 프레임 크기 프롬프트에 대해 8996을 입력하고 Enter를 누르십시오. 프레임 크기를 8996으로 변경하면, 가상 이더넷을 통한 자료 전송이 개선됩니다.

| 회선 설명이 작성되었음을 표시하는 메시지가 표시됩니다.

- | 6. 회선 설명을 연결변환하십시오. WRKCFGSTS *LIN을 입력하고 VETH0에 대해 옵션 1(연결변환)을 선택하십시오.
- | 7. 1 - 6단계를 반복하되, 파티션 B의 명령행에서 단계를 수행하여 파티션 B에 대한 이더넷 회선 설명을 작성하십시오.

| 회선 설명의 이름이 임의적이긴 하지만, 가상 이더넷과 연관된 모든 회선 설명에 대해 동일한 이름을 사용하는 것이 좋습니다. 이 시나리오에서 모든 회선 설명은 VETH0로 명명됩니다.

| 다음 수행 작업

| IP 데이터그램 이송 크기

| 270 및 8xx 모델 서버 이외의 서버에서 이더넷 회선 설명 작성

| 가상 이더넷을 지원하는 새로운 이더넷 회선 설명을 구성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 WRKHDWRSC *CMN을 입력하고 Enter를 누르십시오.
- | 2. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 7(자원 상세 표시)을 선택하십시오.

| 268C로 식별되는 이더넷 포트는 가상 이더넷 자원입니다. 각 가상 이더넷 어댑터에 대해 하나가 있습니다. 268C로 식별되는 각 포트는 HMC를 사용하여 가상 이더넷을 작성할 때(1단계) 작성되는 연관된 위치 코드를 갖습니다.
- | 3. 자원 상세 표시 화면에서 아래로 화면이동하여 이 가상 이더넷에 대해 작성된 특정 위치 코드와 연관되는 268C 자원을 찾으십시오.
- | 4. 통신 자원에 대한 작업 화면에서, 적당한 가상 이더넷 자원의 옆의 옵션 5(구성 설명에 대한 작업)를 선택하고 Enter를 누르십시오.
- | 5. 구성 설명에 대한 작업 화면에서 옵션 1(작성)을 선택하고 Enter를 눌러서 회선 설명 이더넷 작성 (CRTLINETH) 화면을 표시하십시오.

- | a. 회선 설명 프롬프트에 대해 VETH0를 입력하십시오. 회선 설명 및 연관된 가상 이더넷에 대해 VETH0 같은 동일한 이름을 사용하는 경우, 가상 이더넷 구성을 쉽게 추적할 수 있습니다.
- | b. 회선 속도 프롬프트에 대해 1G를 입력하십시오.
- | c. 양방향 전송 프롬프트에 대해 *FULL을 입력하고 Enter를 누르십시오.
- | d. 최대 프레임 크기 프롬프트에 대해 8996을 입력하고 Enter를 누르십시오. 프레임 크기를 8996으로 변경하면, 가상 이더넷을 통한 자료 전송이 개선됩니다.

| 회선 설명이 작성되었음을 표시하는 메시지가 표시됩니다.

- | 6. 회선 설명을 연결변환하십시오. WRKCFGSTS *LIN을 입력하고 VETH0에 대해 옵션 1(연결변환)을 선택하십시오.
- | 7. 1 - 6단계를 반복하되, 파티션 B의 명령행에서 단계를 수행하여 파티션 B에 대한 이더넷 회선 설명을 작성하십시오.

| 회선 설명의 이름이 임의적이긴 하지만, 가상 이더넷과 연관된 모든 회선 설명에 대해 동일한 이름을 사용하는 것이 좋습니다. 이 시나리오에서 모든 회선 설명은 VETH0로 명명됩니다.

| 다음 수행 작업

| IP 데이터그램 이송 크기

| 3단계: IP 데이터그램 이송 크기

- | 패킷이 서로 다른 서브네트로 이송될 수 있도록 IP 데이터그램 이송을 켜십시오.
- | IP 데이터그램 이송을 켜려면 다음 단계를 따르십시오.
- | 1. 파티션 A의 명령행에서 CHGTCPA를 입력하고 F4를 누르십시오.
- | 2. IP 데이터그램 이송 프롬프트에 대해 *YES를 입력하십시오.

| 다음 수행 작업

| 프록시 ARP를 작동가능하게 하는 인터페이스 작성

| 4단계: 프록시 ARP를 작동할 수 있게 하는 인터페이스 작성

- | 프록시 ARP를 작동할 수 있게 하는 TCP/IP 인터페이스를 작성하려면 다음 단계를 완료하십시오.
 - | 1. 사용자 네트워크가 라우트할 수 있는 IP 주소의 연속적인 블록을 확보하십시오.
- | 이 가상 이더넷에 두 개의 파티션이 있으므로 4개 주소의 블록이 필요합니다. 블록에 있는 첫 번째 IP 주소의 네 번째 세그먼트는 반드시 4로 나누어져야 합니다. 이 블록의 첫 번째와 마지막 IP 주소는 서브네트 및 브로드캐스트 IP 주소이며 사용하지 않을 수 있습니다. 두 번째 및 세 번째 IP 주소는 파티션 A와 파티션 B의 가상 이더넷에 대한 TCP/IP 인터페이스에 사용할 수 있습니다. 이 프로시저의 경우, IP 주소 블록은 255.255.255.252의 서브네트 마스크를 갖는 10.1.1.72부터 10.1.1.75까지입니다.

| 또한 외부 TCP/IP 주소에 대한 하나의 IP 주소가 필요합니다. 이 IP 주소는 연속적인 주소의 블록에 속할
| 필요는 없지만, 255.255.255.0의 동일한 원본 서브네트 마스크 안에 있어야 합니다. 이 프로시듀어에서 외
| 부 IP 주소는 10.1.1.15입니다.

| 2. 파티션 B에 대한 OS/400 TCP/IP 인터페이스를 작성하십시오. 이 인터페이스를 외부, 프록시 ARP IP 주
| 소라고 합니다. 이 인터페이스를 작성하려면 다음 단계를 완료하십시오.

- | a. 파티션 B의 명령행에서, CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
- | b. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
- | c. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.
- | d. 인터넷 주소 프롬프트에 대해 '10.1.1.15'를 입력하십시오.
- | e. 회선 설명 프롬프트에 대해 ETHLINE 같은 회선 설명의 이름을 입력하십시오.
- | f. 서브네트 마스크 프롬프트에 대해 '255.255.255.0'을 입력하십시오.

| 3. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선
| 택하십시오.

| 다음 수행 작업

| 파티션 A에 가상 TCP/IP 인터페이스 작성

| 5단계: 파티션 A에 가상 TCP/IP 인터페이스 작성

| 가상 인터페이스를 작성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
- | 2. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
- | 3. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.
- | 4. 인터넷 주소 프롬프트에 '10.1.1.73'을 입력하십시오.
- | 5. 회선 설명 프롬프트에 대해 ETHLINE 같은 회선 설명의 이름을 입력하십시오.
- | 6. 서브네트 마스크 프롬프트에 '255.255.255.252'를 입력하십시오.
- | 7. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선
| 택하십시오.

| 다음 수행 작업

| 파티션 B에 가상 TCP/IP 인터페이스 작성

| 6단계: 파티션 B에 가상 TCP/IP 인터페이스 작성

| 가상 인터페이스를 작성하려면 다음 단계를 따르십시오.

- | 1. 파티션 B의 명령행에서, CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
- | 2. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
- | 3. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.

- | 4. 인터넷 주소 프롬프트에 '10.1.1.74'를 입력하십시오.
- | 5. 회선 설명 프롬프트에 대해 ETHLINE 같은 회선 설명의 이름을 입력하십시오.
- | 6. 서브넷 마스크 프롬프트에 '255.255.255.252'를 입력하십시오.
- | 7. 연관된 로컬 인터페이스 프롬프트에 '10.1.1.15'를 입력하십시오. 이것은 가상 인터페이스를 외부 인터페이스에 연관시키고 프록시 ARP가 가상 인터페이스 10.1.1.74와 외부 인터페이스 10.1.1.15 사이에 패킷을 이송할 수 있게 합니다.
- | 8. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선택하십시오.

| 다음 수행 작업

| 라우트 작성

| **7단계: 라우트 작성**

| 패킷이 가상 이더넷 네트워크를 나갈 수 있도록 하는 디폴트 라우트를 작성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 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 프롬프트에 *DFTRROUTE를 입력하십시오.
- | 5. 서브넷 마스크 프롬프트에 *NONE을 입력하십시오.
- | 6. 다음 홉(hop) 프롬프트에 '10.1.1.74'를 입력하십시오.

| 파티션 A의 패킷은 이 디폴트 라우트를 사용하여 가상 이더넷을 통해 10.1.1.74 인터페이스로 이동합니다. 10.1.1.74가 외부 프록시 ARP 인터페이스 10.1.1.15와 연관되므로, 패킷은 프록시 ARP 인터페이스를 사용하여 가상 이더넷 외부까지 계속됩니다.

| 다음 수행 작업

| 네트워크 통신 확인

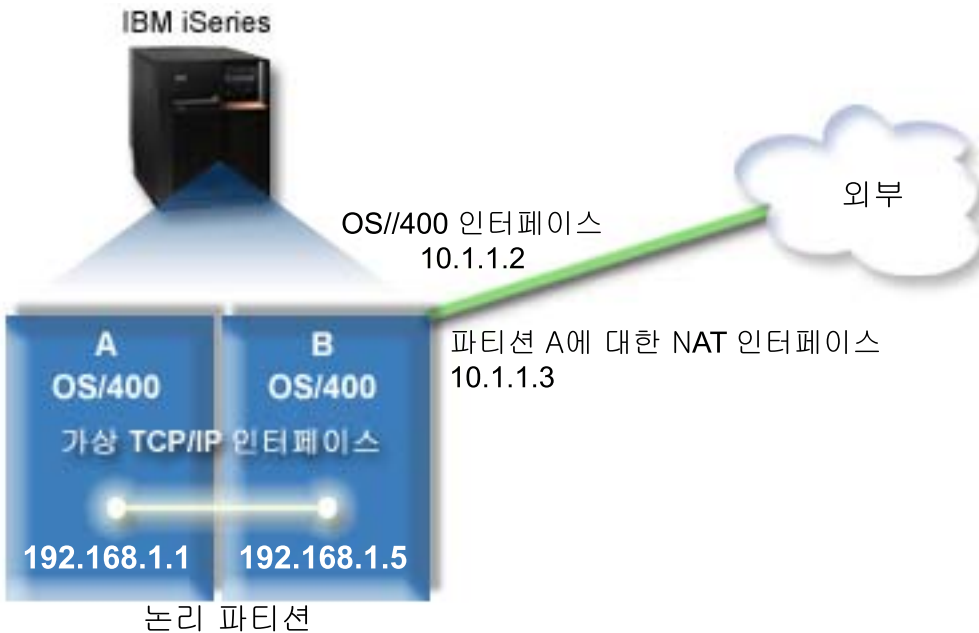
| **8단계: 네트워크 통신 확인**

- | Ping 명령을 사용하여 네트워크 통신을 확인하십시오.
- | • 파티션 A에서, 가상 이더넷 인터페이스 10.1.1.74 및 외부 호스트를 ping하십시오.
- | • 외부 OS/400 호스트에서, 가상 이더넷 인터페이스 10.1.1.73과 10.1.1.74를 ping하십시오.

네트워크 주소 변환 방법

네트워크 주소 변환(NAT)은 사용자의 가상 이더넷 네트워크와 외부 네트워크 사이에서 통신을 라우트할 수 있습니다. NAT의 이 특정한 형태를 정적 NAT라고 부르며, 가상 이더넷 네트워크로 들어오고 나가는 인바운드 및 아웃바운드 IP 통신을 허용합니다. 사용자의 가상 이더넷 네트워크가 외부 클라이언트가 시작하는 통신을 수신할 필요가 없는 경우에는 가변 NAT 같은 NAT의 다른 형태도 작동합니다. TCP/IP 라우팅 및 프록시 ARP 메소드와 마찬가지로, 기존 OS/400 네트워크 연결을 활용할 수 있습니다. IP 패킷 규칙을 사용할 것으로, iSeries Navigator를 사용하여 사용자 자신의 규칙을 작성하고 적용해야 합니다.

다음 그림은 NAT를 사용하여 가상 이더넷 네트워크를 외부 네트워크에 연결하는 예입니다. 10.1.1.x 네트워크는 외부 네트워크를 표시하는 반면, 192.168.1.x 네트워크는 가상 이더넷 네트워크를 표시합니다.



이 예에서 서버에 대한 모든 기존 TCP/IP 통신은 10.1.1.2 인터페이스를 통해 실행됩니다. 이것이 정적 맵 시나리오이므로, 인바운드 통신은 10.1.1.3 인터페이스에서 192.168.1.5 인터페이스로 변환됩니다. 아웃바운드 통신은 192.168.1.5 인터페이스에서 외부 10.1.1.3 인터페이스로 변환됩니다. 파티션 A와 파티션 B는 각각 가상 인터페이스 192.168.1.1과 192.168.1.5를 사용하여 서로 통신합니다.

정적 NAT가 작동하게 하려면 먼저 OS/400 및 TCP/IP 통신을 설정해야 합니다. 그런 다음 일부 IP 패킷 규칙을 작성하고 적용합니다. NAT 메소드를 사용하도록 가상 이더넷을 구성하려면 다음 구성 작업을 완료하십시오.

1. 논리 파티션이 가상 이더넷에 참여할 수 있도록 설정
2. 이더넷 회선 설명 작성
3. IP 데이터그램 이송 켜기
4. 인터페이스 작성
5. 네트워크 통신 확인

- | 6. 패킷 규칙 작성
- | 7. 네트워크 통신 확인

| **1단계: 논리 파티션이 가상 이더넷에 참여할 수 있도록 설정**

| 주: 270 및 8xx 모델 서버 이외의 서버를 사용할 경우, 1차 파티션 대신 eServer용 하드웨어 관리 콘솔(HMC)을 사용하여 이 단계를 수행해야 합니다. 세부사항에 대해서는 가상 이더넷을 참조하십시오.

| 가상 이더넷을 작동할 수 있게 하려면 다음 단계를 따르십시오.

- | 1. 1차 파티션(파티션 A)의 명령행에서 STRSST를 입력하고 Enter를 누르십시오.
- | 2. 서비스 툴 사용자 ID와 암호를 입력하십시오.
- | 3. SST(시스템 서비스 툴) 화면에서 옵션 5(시스템 파티션에 대한 작업)를 선택하십시오.
- | 4. 시스템 파티션에 대한 작업 화면에서 옵션 3(파티션 구성에 대한 작업)을 선택하십시오.
- | 5. F10(가상 이더넷에 대한 작업)을 누르십시오.
- | 6. 파티션 A와 파티션 B에 대한 적합한 열에 1을 입력하여 파티션이 가상 이더넷을 통해 서로 통신할 수 있게 하십시오.
- | 7. 시스템 서비스 툴(SST)을 나가서 명령행으로 리턴하십시오.

| **다음 수행 작업**

| 이더넷 회선 설명 작성

| **2단계: 이더넷 회선 설명 작성**

| 사용 중인 서버 모델에 따라서 두 가지 방법 중 하나로 이 단계를 수행해야 합니다. 특정 서버 모델을 기반으로 회선 설명 작성을 위한 방법 중 하나를 선택하십시오.

- | • 270 및 8xx 모델 서버에 이더넷 회선 설명 작성
- | • 270 및 8xx 모델 서버 이외의 모든 서버에서 이더넷 회선 설명 작성

| **270 및 8xx 모델 서버에 이더넷 회선 설명 작성**

| 가상 이더넷을 지원하는 새로운 이더넷 회선 설명을 구성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 WRKHDWRSC *CMN을 입력하고 Enter를 누르십시오.
- | 2. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 7(자원 상세 표시)을 선택하십시오.
| 268C로 식별되는 이더넷 포트가 가상 이더넷 자원입니다. 각 가상 이더넷에 대해 논리 파티션에 연결되는 하나가 있습니다.
- | 3. 자원 상세 표시 화면에서 아래로 화면이동하여 포트 주소를 찾으십시오. 포트 주소는 논리 파티션의 구성 중에 사용자가 선택한 가상 이더넷과 각각 대응합니다.
- | 4. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 5(구성 설명에 대한 작업)를 선택하고 Enter를 누르십시오.

- | 5. 구성 설명에 대한 작업 화면에서 옵션 1(작성)을 선택하고 Enter를 눌러서 회선 설명 이더넷 작성 (CRTLINETH) 화면을 표시하십시오.
- | a. 회선 설명 프롬프트에 대해 VETH0를 입력하십시오. 이름 VETH0는 임의이지만 논리 파티션이 통신할 수 있게 한 가상 이더넷 페이지의 번호 지정된 열에 해당합니다. 회선 설명과 연관된 가상 이더넷에 대해 동일한 이름을 사용하는 경우, 가상 이더넷 구성을 쉽게 추적할 수 있습니다.
- | b. 회선 속도 프롬프트에 대해 1G를 입력하십시오.
- | c. 양방향 전송 프롬프트에 대해 *FULL을 입력하고 Enter를 누르십시오.
- | d. 최대 프레임 크기 프롬프트에 대해 8996을 입력하고 Enter를 누르십시오. 프레임 크기를 8996으로 변경 하면, 가상 이더넷을 통한 자료 전송이 개선됩니다.
- | 회선 설명이 작성되었음을 표시하는 메시지가 표시됩니다.
- | 6. 회선 설명을 연결변환하십시오. WRKCFGSTS *LIN을 입력하고 VETH0에 대해 옵션 1(연결변환)을 선택하십시오.
- | 7. 1 - 6단계를 반복하되, 파티션 B의 명령행에서 단계를 수행하여 파티션 B에 대한 이더넷 회선 설명을 작성하십시오.
- | 회선 설명의 이름이 임의적이긴 하지만, 가상 이더넷과 연관된 모든 회선 설명에 대해 동일한 이름을 사용하는 것이 좋습니다. 이 시나리오에서 모든 회선 설명은 VETH0로 명명됩니다.

| 다음 수행 작업

| IP 데이터그램 이송 켜기

| **270 및 8xx 모델 서버 이외의 서버에서 이더넷 회선 설명 작성**

| 가상 이더넷을 지원하는 새로운 이더넷 회선 설명을 구성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 WRKHDWRSC *CMN을 입력하고 Enter를 누르십시오.
- | 2. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 7(자원 상세 표시)을 선택하십시오.
- | 268C로 식별되는 이더넷 포트는 가상 이더넷 자원입니다. 각 가상 이더넷 어댑터에 대해 하나가 있습니다. 268C로 식별되는 각 포트는 HMC를 사용하여 가상 이더넷을 작성할 때(1단계) 작성되는 연관된 위치 코드를 갖습니다.
- | 3. 자원 상세 표시 화면에서 아래로 화면이동하여 이 가상 이더넷에 대해 작성된 특정 위치 코드와 연관되는 268C 자원을 찾으십시오.
- | 4. 통신 자원에 대한 작업 화면에서, 적당한 가상 이더넷 자원의 옆의 옵션 5(구성 설명에 대한 작업)를 선택하고 Enter를 누르십시오.
- | 5. 구성 설명에 대한 작업 화면에서 옵션 1(작성)을 선택하고 Enter를 눌러서 회선 설명 이더넷 작성 (CRTLINETH) 화면을 표시하십시오.
- | a. 회선 설명 프롬프트에 대해 VETH0를 입력하십시오. 회선 설명 및 연관된 가상 이더넷에 대해 VETH0 같은 동일한 이름을 사용하는 경우, 가상 이더넷 구성을 쉽게 추적할 수 있습니다.
- | b. 회선 속도 프롬프트에 대해 1G를 입력하십시오.

- | c. 양방향 전송 프롬프트에 대해 *FULL을 입력하고 Enter를 누르십시오.
- | d. 최대 프레임 크기 프롬프트에 대해 8996을 입력하고 Enter를 누르십시오. 프레임 크기를 8996으로 변경하면, 가상 이더넷을 통한 자료 전송이 개선됩니다.

| 회선 설명이 작성되었음을 표시하는 메시지가 표시됩니다.

| 6. 회선 설명을 연결변환하십시오. WRKCFGSTS *LIN을 입력하고 VETH0에 대해 옵션 1(연결변환)을 선택하십시오.

| 7. 1 - 6단계를 반복하되, 파티션 B의 명령행에서 단계를 수행하여 파티션 B에 대한 이더넷 회선 설명을 작성하십시오.

| 회선 설명의 이름이 임의적이긴 하지만, 가상 이더넷과 연관된 모든 회선 설명에 대해 동일한 이름을 사용하는 것이 좋습니다. 이 시나리오에서 모든 회선 설명은 VETH0로 명명됩니다.

| 다음 수행 작업

| IP 데이터그램 이송 켜기

| 3단계: IP 데이터그램 이송 켜기

| 패킷이 서로 다른 서브네트로 이송될 수 있도록 IP 데이터그램 이송을 켜십시오.

| IP 데이터그램 이송을 켜려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 CHGTCPA를 입력하고 F4를 누르십시오.
- | 2. IP 데이터그램 이송 프롬프트에 대해 *YES를 입력하십시오.

| 다음 수행 작업

| 인터페이스 작성

| 4단계: 인터페이스 작성

| TCP/IP 인터페이스를 작성하려면 다음 단계를 따르십시오.

- | 1. 파티션 B에 서버와의 일반 통신을 위한 OS/400 TCP/IP 인터페이스를 작성하고 시작하십시오. 이 인터페이스를 작성하려면 다음 단계를 완료하십시오.
 - | a. 파티션 B의 명령행에서, CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
 - | b. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
 - | c. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.
 - | d. 인터넷 주소 프롬프트에 '10.1.1.2'를 입력하십시오.
 - | e. 회선 설명 프롬프트에 ETHLINE를 입력하십시오.
 - | f. 서브네트 마스크 프롬프트에 대해 '255.255.255.0'을 입력하십시오.
 - | g. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선택하십시오.

2. 외부 네트워크에 연결하는 다른 TCP/IP 인터페이스를 작성하고 시작하십시오. 기존의 외부 TCP/IP 인터페이스와 동일한 회선 설명을 사용해야 합니다. 이 인터페이스가 결국에는 파티션에 대한 주소 변환을 수행합니다. 이 인터페이스를 작성하려면 다음 단계를 완료하십시오.
 - a. 파티션 B의 명령행에서, CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
 - b. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
 - c. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.
 - d. 인터넷 주소 프롬프트에 '10.1.1.3'을 입력하십시오.
 - e. 회선 설명 프롬프트에 ETHLINE를 입력하십시오.
 - f. 서브네트 마스크 프롬프트에 대해 '255.255.255.0'을 입력하십시오.
 - g. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선택하십시오.
3. 파티션 A에 가상 이더넷을 위한 OS/400 TCP/IP 인터페이스를 작성하고 시작하십시오. 이 인터페이스를 작성하려면 다음 단계를 완료하십시오.
 - a. 파티션 A의 명령행에서 CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
 - b. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
 - c. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.
 - d. 인터넷 주소 프롬프트에 '192.168.1.1'을 입력하십시오.
 - e. 회선 설명 프롬프트에 VETH0를 입력하십시오.
 - f. 서브네트 마스크 프롬프트에 대해 '255.255.255.0'을 입력하십시오.
 - g. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선택하십시오.
4. 파티션 B에 가상 이더넷을 위한 OS/400 TCP/IP 인터페이스를 작성하고 시작하십시오. 이 인터페이스를 작성하려면 다음 단계를 완료하십시오.
 - a. 파티션 B의 명령행에서, CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
 - b. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
 - c. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.
 - d. 인터넷 주소 프롬프트에 '192.168.1.5'를 입력하십시오.
 - e. 회선 설명 프롬프트에 VETH0를 입력하십시오.
 - f. 서브네트 마스크 프롬프트에 대해 '255.255.255.0'을 입력하십시오.
 - g. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선택하십시오.

다음 수행 작업

네트워크 통신 확인

| 5단계: 네트워크 통신 확인

| Ping 명령을 사용하여 네트워크 통신을 확인하십시오.

| • 파티션 A에서, 가상 이더넷 인터페이스 192.168.1.5 및 외부 호스트를 ping하십시오.

| • 외부 OS/400 호스트에서 가상 이더넷 인터페이스 192.168.1.1 및 192.168.1.5의 각각을 ping하십시오.

| 다음 수행 작업

| 패킷 규칙 작성

| 6단계: 패킷 규칙 작성

| 파티션 A의 개인용 주소를 파티션 B의 공용 주소에 맵핑하는 패킷 규칙을 작성하려면 iSeries Navigator의 주소 변환 마법사를 사용하십시오.

| 패킷 규칙을 작성하려면 다음 단계를 따르십시오.

| 1. iSeries Navigator에서, **iSeries 서버 -> 네트워크-> IP 정책**을 차례로 선택하십시오.

| 2. 패킷 규칙을 오른쪽 마우스 버튼으로 클릭하고 규칙 편집기를 선택하십시오.

| 3. 마법사 메뉴에서 주소 변환을 선택하십시오.

| 4. 마법사의 지시에 따라서 패킷 규칙을 작성하십시오. 이 프로시듀어는 다음 선택을 사용합니다.

| • 주소 변환 맵핑 선택

| • 개인용 IP 주소 192.168.1.1 입력

| • 공용 IP 주소 10.1.1.3 입력

| • ETHLINE 같이 인터페이스가 구성되는 회선 선택

| 5. 파일 메뉴에서 규칙 활성화를 선택하십시오.

| 다음에 수행할 작업

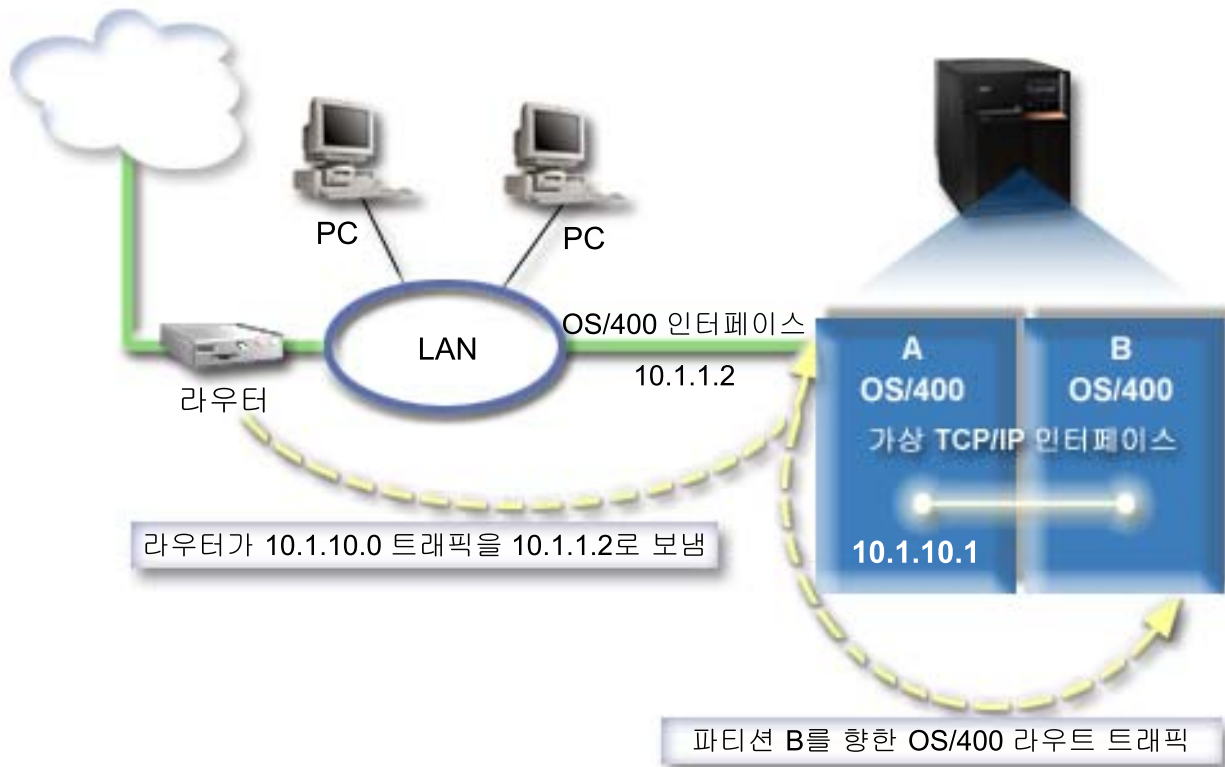
| 네트워크 통신 확인

| 7단계: 네트워크 통신 확인

| 패킷 규칙을 작성한 후 네트워크 통신을 확인해야 합니다. 아웃바운드 통신을 테스트하려면 파티션 A에서 외부 호스트를 ping하십시오. 그런 다음 해당 외부 호스트에서 파티션 A를 ping하여 인바운드 통신을 테스트하십시오.

TCP/IP 라우팅 메소드

또한 다양한 라우팅 기술을 사용하여 iSeries 서버를 통한 파티션에 대한 통신량을 라우트할 수 있습니다. 이 솔루션은 서버에서 구성하는 것이 어렵지는 않지만, 네트워크의 토폴로지에 따라서는 구현하는 것이 쉽지 않을 수도 있습니다. 다음 그림을 고려하십시오.



기존의 TCP/IP 인터페이스(10.1.1.2)는 LAN에 연결됩니다. LAN은 라우터를 통해 리모트 네트워크에 연결됩니다. 파티션 B의 가상 TCP/IP 인터페이스는 10.1.10.2로 주소지정되고 파티션 A의 가상 TCP/IP 인터페이스는 10.1.10.1로 주소지정됩니다. OS/400에서, IP 데이터그램 이송을 켜면 OS/400은 IP 패킷을 파티션 B로 및 파티션 B로부터 라우트합니다. 파티션 B에 대한 TCP/IP 연결을 정의할 때, 라우트 주소는 10.1.10.1이어야 합니다.

이 유형의 라우팅의 어려움은 IP 패킷을 iSeries로 이송하는 것입니다. 이 시나리오에서, 10.1.10.0 네트워크로 목적지가 지정되는 패킷을 10.1.1.2 인터페이스로 전달하도록 라우터에서 라우트를 정의할 수 있습니다. 이것은 리모트 네트워크 클라이언트에 대해 작동합니다. 또한 동일한 라우터를 다음 홉(hop)으로 인식하는 경우 로컬 LAN 클라이언트(iSeries와 동일한 LAN에 연결되는 클라이언트)에 대해서도 작동합니다. 그렇지 않으면, 각 클라이언트가 10.1.10.0 통신량을 OS/400 10.1.1.2 인터페이스로 보내는 라우트를 가져야 합니다. 따라서 이 방법은 실행 불가능합니다. 많은 LAN 클라이언트가 있으면 많은 라우트를 정의해야 합니다.

TCP/IP 라우팅 메소드를 사용하도록 가상 이더넷을 구성하려면 다음 지침을 사용하십시오.

1. 논리 파티션이 가상 이더넷에 참여할 수 있도록 설정
2. 이더넷 회선 설명 작성

- | 3. IP 데이터그램 이송 켜기
- | 4. 인터페이스 작성

| **1단계: 논리 파티션이 가상 이더넷에 참여할 수 있도록 설정**

| 주: 270 및 8xx 모델 서버 이외의 서버를 사용할 경우, 1차 파티션 대신 eServer용 하드웨어 관리 콘솔(HMC)을 사용하여 이 단계를 수행해야 합니다. 세부사항에 대해서는 가상 이더넷을 참조하십시오.

| 가상 이더넷을 작동할 수 있게 하려면 다음 단계를 따르십시오.

- | 1. 1차 파티션(파티션 A)의 명령행에서 STRSST를 입력하고 Enter를 누르십시오.
- | 2. 서비스 툴 사용자 ID와 암호를 입력하십시오.
- | 3. SST(시스템 서비스 툴) 화면에서 옵션 5(시스템 파티션에 대한 작업)를 선택하십시오.
- | 4. 시스템 파티션에 대한 작업 화면에서 옵션 3(파티션 구성에 대한 작업)을 선택하십시오.
- | 5. F10(가상 이더넷에 대한 작업)을 누르십시오.
- | 6. 파티션 A와 파티션 B에 대한 적합한 열에 1을 입력하여 파티션이 가상 이더넷을 통해 서로 통신할 수 있게 하십시오.
- | 7. 시스템 서비스 툴(SST)을 나가서 명령행으로 리턴하십시오.

| 다음에 수행할 작업

| 이더넷 회선 설명 작성

| **2단계: 이더넷 회선 설명 작성**

| 사용 중인 서버 모델에 따라서 두 가지 방법 중 하나로 이 단계를 수행해야 합니다. 특정 서버 모델을 기반으로 회선 설명 작성을 위한 방법 중 하나를 선택하십시오.

- | • 270 및 8xx 모델 서버에 이더넷 회선 설명 작성
- | • 270 및 8xx 모델 서버 이외의 모든 서버에서 이더넷 회선 설명 작성

| **270 및 8xx 모델 서버에 이더넷 회선 설명 작성**

| 가상 이더넷을 지원하는 새로운 이더넷 회선 설명을 구성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 WRKHDWRSC *CMN을 입력하고 Enter를 누르십시오.
- | 2. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 7(자원 상세 표시)을 선택하십시오.
| 268C로 식별되는 이더넷 포트가 가상 이더넷 자원입니다. 각 가상 이더넷에 대해 논리 파티션에 연결되는 하나가 있습니다.
- | 3. 자원 상세 표시 화면에서 아래로 화면이동하여 포트 주소를 찾으십시오. 포트 주소는 논리 파티션의 구성 중에 사용자가 선택한 가상 이더넷과 각각 대응합니다.
- | 4. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 5(구성 설명에 대한 작업)를 선택하고 Enter를 누르십시오.

- | 5. 구성 설명에 대한 작업 화면에서 옵션 1(작성)을 선택하고 Enter를 눌러서 회선 설명 이더넷 작성 (CRTLINETH) 화면을 표시하십시오.
- | a. 회선 설명 프롬프트에 대해 VETH0를 입력하십시오. 이름 VETH0는 임의이지만 논리 파티션이 통신할 수 있게 한 가상 이더넷 페이지의 번호 지정된 열에 해당합니다. 회선 설명과 연관된 가상 이더넷에 대해 동일한 이름을 사용하는 경우, 가상 이더넷 구성을 쉽게 추적할 수 있습니다.
- | b. 회선 속도 프롬프트에 대해 1G를 입력하십시오.
- | c. 양방향 전송 프롬프트에 대해 *FULL을 입력하고 Enter를 누르십시오.
- | d. 최대 프레임 크기 프롬프트에 대해 8996을 입력하고 Enter를 누르십시오. 프레임 크기를 8996으로 변경 하면, 가상 이더넷을 통한 자료 전송이 개선됩니다.

| 회선 설명이 작성되었음을 표시하는 메시지가 표시될 것입니다.

- | 6. 회선 설명을 연결변환하십시오. WRKCFGSTS *LIN을 입력하고 VETH0에 대해 옵션 1(연결변환)을 선택하십시오.
- | 7. 1 - 6단계를 반복하지만, 파티션 B의 명령행에서 단계를 수행하여 파티션 B에 대한 이더넷 회선 설명을 작성하십시오.

| 회선 설명의 이름이 임의적이긴 하지만, 가상 이더넷과 연관된 모든 회선 설명에 대해 동일한 이름을 사용하는 것이 좋습니다. 이 시나리오에서 모든 회선 설명은 VETH0로 명명됩니다.

| 다음에 수행할 작업

| IP 데이터그램 이송 켜기

| 270 및 8xx 모델 서버 이외의 서버에서 이더넷 회선 설명 작성

| 가상 이더넷을 지원하는 새로운 이더넷 회선 설명을 구성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 WRKHDWRSC *CMN을 입력하고 Enter를 누르십시오.
- | 2. 통신 자원에 대한 작업 화면에서 적당한 가상 이더넷 포트 옆의 옵션 7(자원 상세 표시)을 선택하십시오.
| 268C로 식별되는 이더넷 포트는 가상 이더넷 자원입니다. 각 가상 이더넷 어댑터에 대해 하나가 있습니다. 268C로 식별되는 각 포트는 HMC를 사용하여 가상 이더넷을 작성할 때(1단계) 작성되는 연관된 위치 코드를 갖습니다.
- | 3. 자원 상세 표시 화면에서 아래로 화면이동하여 이 가상 이더넷에 대해 작성된 특정 위치 코드와 연관되는 268C 자원을 찾으십시오.
- | 4. 통신 자원에 대한 작업 화면에서, 적당한 가상 이더넷 자원의 옆의 옵션 5(구성 설명에 대한 작업)를 선택하고 Enter를 누르십시오.
- | 5. 구성 설명에 대한 작업 화면에서 옵션 1(작성)을 선택하고 Enter를 눌러서 회선 설명 이더넷 작성 (CRTLINETH) 화면을 표시하십시오.
 - | a. 회선 설명 프롬프트에 대해 VETH0를 입력하십시오. 회선 설명 및 연관된 가상 이더넷에 대해 VETH0 같은 동일한 이름을 사용하는 경우, 가상 이더넷 구성을 쉽게 추적할 수 있습니다.
 - | b. 회선 속도 프롬프트에 대해 1G를 입력하십시오.

- | c. 양방향 전송 프롬프트에 대해 *FULL을 입력하고 Enter를 누르십시오.
- | d. 최대 프레임 크기 프롬프트에 대해 8996을 입력하고 Enter를 누르십시오. 프레임 크기를 8996으로 변경하면, 가상 이더넷을 통한 자료 전송이 개선됩니다.

| 회선 설명이 작성되었음을 표시하는 메시지가 표시될 것입니다.

- | 6. 회선 설명을 연결변환하십시오. WRKCFGSTS *LIN을 입력하고 VETH0에 대해 옵션 1(연결변환)을 선택하십시오.

- | 7. 1 - 6단계를 반복하지만, 파티션 B의 명령행에서 단계를 수행하여 파티션 B에 대한 이더넷 회선 설명을 작성하십시오.

| 회선 설명의 이름이 임의적이긴 하지만, 가상 이더넷과 연관된 모든 회선 설명에 대해 동일한 이름을 사용하는 것이 좋습니다. 이 시나리오에서 모든 회선 설명은 VETH0로 명명됩니다.

| 다음에 수행할 작업

| IP 데이터그램 이송 켜기

| 3단계: IP 데이터그램 이송 켜기

| 패킷이 서로 다른 서브네트로 이송될 수 있도록 IP 데이터그램 이송을 켜십시오.

| IP 데이터그램 이송을 켜려면 다음 단계를 따르십시오.

- | 1. 파티션 A의 명령행에서 CHGTCPA를 입력하고 F4를 누르십시오.
- | 2. IP 데이터그램 이송 프롬프트에 대해 *YES를 입력하십시오.

| 다음에 수행할 작업

| 인터페이스 작성

| 4단계: 인터페이스 작성

| TCP/IP 인터페이스를 작성하려면 다음 단계를 따르십시오.

- | 1. 파티션 A에 OS/400 TCP/IP 인터페이스를 작성하십시오. 인터페이스를 작성하려면 다음 단계를 따르십시오.
 - | a. 파티션 A의 명령행에서 CFGTCP를 입력하고 Enter를 눌러서 TCP/IP 구성 화면을 표시하십시오.
 - | b. 옵션 1(TCP/IP 인터페이스에 대한 작업)을 선택하고 Enter를 누르십시오.
 - | c. 옵션 1(추가)을 선택하고 Enter를 눌러서 ADDTCPIFC(TCP/IP 인터페이스 추가) 화면을 보십시오.
 - | d. 인터넷 주소 프롬프트에 '10.1.1.2'를 입력하십시오.
 - | e. 회선 설명 프롬프트에 대해 ETHLINE 같은 회선 설명의 이름을 입력하십시오.
 - | f. 서브네트 마스크 프롬프트에 대해 '255.255.255.0'을 입력하십시오.
- | 2. 인터페이스를 시작하십시오. TCP/IP 인터페이스에 대한 작업 화면에서 인터페이스별로 옵션 9(시작)를 선택하십시오.

- | 3. 2와 3단계를 반복하여 파티션 A와 파티션 B에서 TCP/IP 인터페이스를 작성하고 시작하십시오.
- | 이들 인터페이스는 가상 이더넷에 사용됩니다. 이들 인터페이스에 대해 IP 주소 10.1.10.1 및 10.1.10.2와
- | 서브네트 마스크 255.255.255.0을 사용하십시오.

| 가상 이더넷 고려사항

| 파티션간 통신을 위해 네트워크 카드를 사용하는 것의 대안으로 가상 이더넷을 사용할 수 있습니다. 그러면 추
| 가 하드웨어를 구매하지 않고 논리 파티션 사이의 고속 통신을 설정할 수 있습니다. 작동할 수 있는 16 포트
| 의 각각에 대해 시스템이 자원 유형 268C를 갖는 CMNxx 같은 가상 이더넷 통신 포트를 작성합니다. 그러면
| 동일한 근거리 통신망(LAN)에 할당되는 논리 파티션은 해당 링크를 통해 통신할 수 있게 됩니다. 실제 시스
| 템에서는 최대 16개의 상이한 가상 근거리 통신망(LAN)을 구성할 수 있습니다. 가상 이더넷은 1Gb 이더넷
| 어댑터를 사용하는 것과 동일한 기능을 제공합니다. 토큰링 또는 이더넷 10Mbps 및 100Mbps 근거리 통신망
| (LAN)은 가상 이더넷이 지원되지 않습니다.

| 가상 이더넷은 실질적인 이점을 제공하는 경제적인 네트워킹 솔루션입니다.



- | • 경제적: 잠재적으로 여러분의 네트워킹 하드웨어가 필요없습니다. 여러분의 물리적 LAN 카드를 설치하지 않고
| 도 서버에 파티션을 추가하여 외부 LAN과 통신할 수 있습니다. 현재 서버가 추가 LAN 카드를 설치할 사
| 용할 수 있는 카드 슬롯을 제한한 경우, 가상 이더넷 사용은 서버를 업그레이드하기 위한 요구사항 없이 LAN
| 으로 접속된 파티션을 동작하는 기능을 제공합니다.
- | • 유연성: 파티션 사이의 선택적인 통신 경로 구성을 가능케 하는 최대 16개의 개별 연결을 구성할 수 있습니
| 다. 추가된 유연성을 위해 구성 모델은 논리 파티션이 가상 이더넷과 실제 LAN 연결을 구현할 수 있도록
| 허용합니다. 이것은 방화벽 어플리케이션을 호스트하기 위해 Linux 파티션을 사용할 때 바람직한 피처입니
| 다.
- | • 고속: 가상 이더넷은 1GB 이더넷 연결을 에뮬레이트하고 파티션 사이의 빠르고 편리한 통신 방법을 제공합
| 니다. 이것은 상이한 논리 파티션에서 실행하는 여러 어플리케이션을 통합할 기회를 향상시킵니다.
- | • 융통성: 파티션이 OS/400 또는 Linux에서 실행 중인지와 관계없이, 모두가 동일한 가상 이더넷에 연결될
| 수 있습니다.
- | • 축소된 경합: 파티션간 통신에 가상 이더넷을 사용함으로써, 외부 LAN에서 통신량이 줄어듭니다. 충돌 기
| 반 표준인 이더넷의 경우, 이것이 특히 다른 LAN 사용자를 위한 서비스 저하를 막는 데 도움이 됩니다.





제 9 장 TCP/IP 설정 관련 정보

이제 서버가 시작되어 실행 중이므로 "서버로 어떤 작업을 더 할 수 있을까?"라고 자신에게 물어볼 수 있습니다. TCP/IP 설정 주제에 관련된 매뉴얼 및 IBM 레드북(PDF 형식)과 Information Center 주제가 아래 나열되어 있습니다. PDF를 보거나 인쇄할 수 있습니다. 다음 참조서를 통해 iSeries 서버를 최대한 활용하십시오.




매뉴얼

- **TCP/IP Configuration and Reference**  (592KB)
이 책에는 TCP/IP를 구성하고 네트워크를 운영 및 관리하는데 대한 정보가 수록되어 있습니다.
- **iSeries 보안을 위한 추가 정보 및 툴**  (1MB)
이 책에는 서버 및 연관된 운영을 보호하기 위해 iSeries의 보안 피처를 사용하는데 대한 기본 권장사항이 수록되어 있습니다.

레드북

- **TCP/IP Tutorial and Technical Overview**  (7MB)
이 레드북에는 TCP/IP의 기본에 대한 정보가 수록되어 있습니다.
- **TCP/IP for AS/400: More Cool Things Than Ever**  (9MB)
이 책에는 일반적인 TCP/IP 어플리케이션 및 서비스의 방대한 리스트가 들어 있습니다.

IPv6

- **IETF(Internet Engineering Task Force)** (<http://www.ietf.cnri.reston.va.us/>) 
IPv6을 포함하여 인터넷 프로토콜을 개발하는 그룹에 대해 배울 수 있습니다.
- **IP Version 6(IPv6)** (<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 
현재 IPv6 스펙 및 IPv6에 대한 여러가지 소스 참조가 나와 있습니다.
- **IPv6 Forum** (<http://www.ipv6forum.com/>) 
최근의 IPv6 개발에 대해 알리는 소식지 및 이벤트에 대해 나와 있습니다.


기타 정보

- **TCP/IP**
이 주제에는 구성 범위 그 이상의 TCP/IP 어플리케이션 및 서비스에 대한 정보가 들어 있습니다.

워크스테이션에 PDF를 저장하려면 다음을 수행하십시오.

1. 브라우저에서 PDF를 마우스 오른쪽 버튼으로 클릭하십시오(위의 링크를 마우스 오른쪽 버튼으로 클릭).

2. 다른 이름으로 대상 저장...을 클릭하십시오.
3. PDF를 저장할 디렉토리로 가십시오.
4. 저장을 클릭하십시오.

PDF를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요한 경우에는 Adobe 웹 사이트 (www.adobe.com/prodindex/acrobat/readstep.html)  에서 사본을 다운로드할 수 있습니다.

제 2 부 부록

부록. 주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 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 재산을 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 라이선스까지 부여하는 것은 아닙니다. 라이선스에 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 라이선스 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, 이 변경사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및(또는) 프로그램을 사전 통지없이 언제든지 개선 및(또는) 변경할 수 있습니다.

이 정보에서 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 사용
- | 하거나 배포할 수 있습니다.

(1) 독립적으로 생성된 프로그램이나 기타 프로그램(본 프로그램 포함)간의 정보 교환 및 (2) 교환된 정보의 상호 이용을 목적으로 정보를 원하는 프로그램 라이선스 사용자는 다음 주소로 문의하십시오.

135-270

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

이러한 정보는 해당 조항 및 조건에 따라(예를 들면, 사용료 지불 포함) 사용할 수 있습니다.

- | 이 정보에 기술된 라이선스가 있는 프로그램 및 이 프로그램에 대해 사용 가능한 모든 라이선스가 있는 자료
- | 는 IBM이 IBM 기본 계약, IBM 국제 프로그램 라이선스 계약(IPLA), 기계 코드에 대한 IBM 라이선스 계
- | 약, 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 문서의 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.

IBM의 향후 방향 또는 의도에 관한 언급은 별도의 통지 없이 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 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 소프트웨어로 보는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 등록상표입니다.

AS/400

e(로고)server

eServer

IBM

iSeries
OS/400
Redbooks

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

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

서적의 다운로드 및 인쇄 조건

- | 귀하가 다운로드하려는 정보를 사용하는 데에는 다음의 조건이 적용되며 귀하가 이를 승인하는 경우에 해당
- | 서적을 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 귀하는 이들 정보를 귀하 사업장 내에서만 복제, 배포
- | 및 전시할 수 있습니다. 귀하는 IBM의 명시적인 동의없이 귀하의 사업장 이외에서 해당 정보의 2차적 저작물
- | 을 작성할 수 없으며 이들 정보 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

- | 본 계약에서 명시하지 않는 한, 본 정보 또는 데이터, 소프트웨어 또는 기타 지적 재산권에 대하여 다른 허가
- | 나 라이선스 또는 권리가 부여되지 않습니다.

- | 해당 정보의 사용이 IBM에게 손해를 가져오거나, 상기 지시사항이 적절하게 준수되지 않을 것으로 판단한 경
- | 우, IBM은 본 계약에서 부여한 서적에 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 이 정보의 내용과 관련하여 어떠한 보증도 하지
- | 않습니다. 본 정보는 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음)
- | 묵시적이든 명시적이든 일체의 보증없이 "현상태대로" 제공됩니다.

All material copyrighted by IBM Corporation.

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

IBM