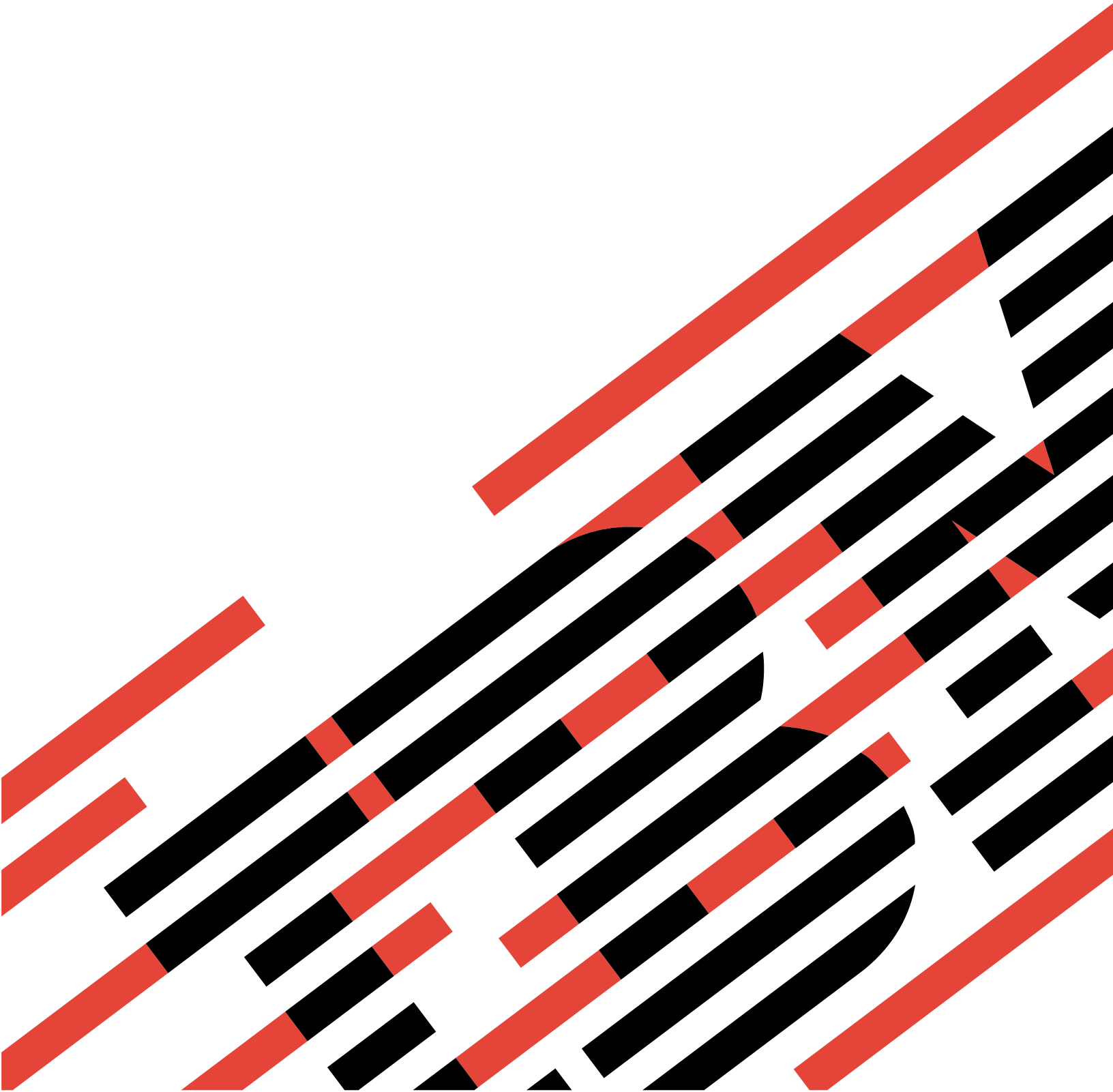
IBM

eserver

iSeries

TCP/IP 라우팅 및 로드 균형 조절



IBM

@server

iSeries

TCP/IP 라우팅 및 로드 균형 조절

목차

TCP/IP 라우팅 및 로드 균형 조절

iSeries 서버의 TCP/IP 통신량을 라우트하고 균형 조절을 위한 더 좋은 방법을 찾고 계십니까? iSeries 서버를 많은 일에 사용할 수 있으나 TCP/IP 네트워크와의 연결로 인해 그 통합 라우팅 기능이 외부 라우터의 필요성을 제거시킬 수 있다는 점을 알아야 합니다.

백그라운드 정보와 더불어 라우팅 및 로드 균형 조절을 통해 iSeries 서버에서 사용할 수 있는 옵션들을 이해할 수 있을 것입니다. 그림을 사용하여 각 방법을 설명하므로 연결이 이루어지는 방법을 알 수 있습니다. 이 방법에는 라우팅 기법을 구성하는 것에 관한 설명은 없습니다. 이 페이지에서는 iSeries 서버를 더 잘 활용하기 위해 사용자가 알아야 할 라우팅 원칙 및 개념에 초점을 맞추었습니다.

이 방법들이 중요한 이유

이 방법에 나오는 기법들은 더 적은 수의 외부 라우터와 서버를 사용할 수 있기 때문에 전체적인 연결 비용을 절감시킬 수 있습니다. 이 라우팅 방법들을 사용할 경우 더 효율적으로 IP 주소를 관리하는 방법을 배우게 되므로 IP 주소를 자유롭게 사용할 수 있습니다. 로드 균형 조절 방법을 숙지함으로써 시스템에서 통신 로드의 균형을 조절하여 iSeries 서버 성능을 전반적으로 향상시킬 수 있습니다.

이 페이지를 인쇄하는 방법

이 주제를 쉽게 인쇄하여 하나의 문서로 읽을 수 있습니다. 이 주제 인쇄에 나오는 지침을 따르십시오.

시작하기 전에

iSeries 400 서버에서 라우팅과 로드 균형 조절을 처음 접하는 경우 방법을 살펴보기 전에 이 페이지들을 볼 수 있습니다.

릴리스별 TCP/IP 라우팅 기능에는 iSeries 서버의 각 버전과 릴리스에서 사용할 수 있는 라우팅 기능에 관한 정보가 들어 있으므로 사용할 수 있는 기능에 어떤 것이 있는지 알 수 있습니다.

패킷 처리에서는 iSeries 서버가 정보 패킷을 처리하는 방식을 보여줍니다.

공통 라우팅 규칙에서는 iSeries 서버 라우팅에 대한 기본 규칙을 설명합니다. 라우팅 방법을 읽을 때 다음 규칙들을 고려하십시오.

사용할 방법을 찾기 위한 방법

서로 다른 많은 방법을 사용할 수 있습니다. 스스로 결정하여 이 방법들을 사용자의 네트워크 환경에 적용할 수 있습니다.

TCP/IP 라우팅 연결 방법에서는 iSeries 서버가 자료를 라우팅하는 방법에 대해 설명합니다.

TCP/IP 로드 균형 조절 방법에서는 iSeries 서버의 통신 로드의 균형을 조절하는 데 사용할 수 있는 여러 가지 TCP/IP 기법을 설명합니다.

iSeries 서버 TCP/IP 라우팅에 대한 추가 정보

TCP/IP 라우팅 및 로드 균형 조절에 관한 기타 정보에는 TCP/IP 라우팅 및 로드 균형 조절과 관련된 추가 참조 정보가 들어 있습니다.

이 주제 인쇄

보기 또는 인쇄를 위해 이 문서의 PDF 버전을 보거나 다운로드할 수 있습니다. PDF 파일을 보려면 Adobe(R) Acrobat(R) Reader를 설치하십시오. Adobe(R) Acrobat(R) 웹 사이트에서 사본을 다운로드 받을 수 있습니다.

PDF 버전을 보거나 다운로드하려면 라우팅 및 로드 균형 조절

(약 1.8MB 또는 36 페이지)을 선택하십시오.

보기 또는 인쇄를 위해 워크스테이션에 PDF를 저장하려면 다음과 같이 하십시오.

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

릴리스별 TCP/IP 라우팅 기능

다음 리스트에는 iSeries 서버에서 릴리스별로 지원되는 기능이 나옵니다. 기능 사용을 계획하기 전에 리스트를 확인하여 수행하려는 기능을 지원하는 올바른 릴리스가 시스템에 있는지 알아보십시오. 그러나 어떤 경우에는 다른 접근 방식으로 같은 결과를 얻을 수 있습니다.

V3R1: 정적 라우트 기반의 패킷 전송이 도입되었습니다.

V3R7/V3R2: 직렬 회선 인터넷 프로토콜(SLIP), 프록시 ARP(Address Resolution Protocol) 라우팅, 번호를 지정하지 않은 연결 네트워크 지원이 도입되었습니다.

V4R1: 동적 라우팅 정보 프로토콜 버전 1(RIPv1)이 도입되었습니다.

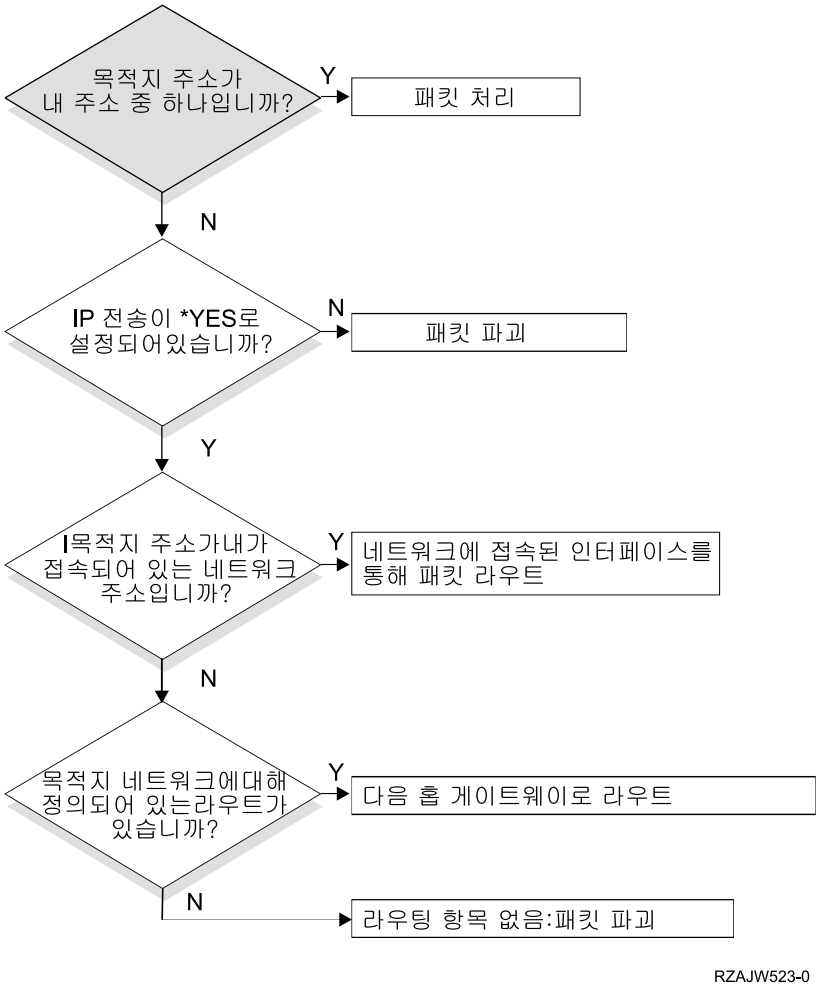
V4R2: 동적 라우팅 정보 프로토콜 버전 2(RIPv2), 투명한 서브네트화, 중복 라우트 기반의 로드 균형 조절이 도입되었습니다.

V4R3: 가상 IP 주소, IP 주소 가장, 네트워크 주소 변환(NAT), CIDR(Classless Inter-Domain Routing)이 도입되었습니다.

V4R4: OptiConnect상의 IP가 도입되었습니다.

패킷 처리

패킷 프로세스를 잘 이해하면 라우팅 기능의 구현 방법을 결정할 때 도움이 됩니다. 아래에 나오는 단순화시킨 흐름 도표에서 IP 패킷(데이터그램)이 iSeries 서버에 도달할 때 발생하는 논리 프로세스를 볼 수 있습니다. 실제 흐름은 다를 수 있지만 결과는 같습니다. 다음 논리는 디폴트 패킷 처리 시나리오만 설명합니다. 확장 라우팅 기법을 사용할 경우 패킷 처리가 약간 다를 수 있습니다.



먼저 IP 헤더의 목적지 주소를 시스템에 정의된 모든 주소와 비교합니다. 패킷이 사용자 시스템을 목표로 하는 것으로 판별되면 TCP와 같은 상위 레벨 소프트웨어에 대한 IP 스택으로 패킷을 전달한 후 목적지 포트에서 청취하고 있는 어플리케이션으로 다시 전달합니다.

패킷을 로컬로 허용할 수 없으면 IP 전송 속성에 대해 검사합니다. IP 전송이 *YES로 설정되어 있으면 라우터처럼 패킷을 전송하도록 시스템을 구성합니다. 속성이 TCP/IP 속성이나 PPP 프로파일에 *NO로 설정되어 있으면 패킷이 파괴됩니다.

패킷의 목적지 주소를 시스템에서 알고 있는 모든 *DIRECT 라우트와 비교합니다. 이것은 패킷의 목적지가 이 시스템에 직접 연결된 네트워크인지를 알아보기 위해 패킷의 목적지 주소를 정의된 인터페이스의 *DIRECT 라우팅 항목에 지정된 서브네트 마스크에 포함시킴으로써 이루어집니다. 검사는 가장 특정한 라우트로부터 이루어집니다.

그리고 나서 iSeries 서버가 리모트 호스트와 직접 연결되어 있지 않으면 라우팅 표를 탐색합니다. 다시 한 번 가장 특정한 호스트(서브네트 마스크 255.255.255.255)로부터 다른 라우트(서브네트 마스크 0.0.0.0)로 탐색합니다. 라우트를 찾으면 그 다음 홉 게이트웨이로 패킷을 전송합니다.

흐름 도표에서의 마지막 점은 일치하는 라우팅 항목이 없으면 패킷이 파괴됨을 보여줍니다.

공통 라우팅 규칙

이 규칙은 TCP/IP 전반에 걸쳐 그리고 iSeries 서버 상의 TCP/IP에 적용되는 기본 규칙의 일부입니다. iSeries 서버에 라우팅 기능을 구현할 때 이 규칙을 고려해야 합니다. 이 규칙은 시스템의 패킷에서 발생하는 일과 패킷이 갈 수 있는 곳을 판별하는 데 도움이 됩니다. 대부분의 규칙과 마찬가지로, 예외가 있습니다.

1. 사용자 시스템은 IP 주소를 갖지 않으며, 인터페이스만이 IP 주소를 갖습니다.

   이 규칙에 대한 예외는 가상 IP(무연결) 주소이며, 이 주소는 시스템에 할당됩니다. 가상 IP는 V4R3부터 사용할 수 있습니다.

2. 일반적으로 목적지 IP 주소가 사용자 시스템에 정의되는 경우, 시스템은 패킷이 오는 인터페이스에 상관없이 IP 주소를 처리합니다.

   이 경우의 예외는 주소가 번호를 지정하지 않은 인터페이스와 연관되는 경우 또는 IP NAT나 필터링이 사용 중인 경우, 패킷이 전송되거나 삭제될 수 있다는 점입니다.

3. IP 주소와 마스크가 연결된 네트워크의 주소를 정의합니다.

4. 시스템의 라우트 아웃은 인터페이스에 연결된 네트워크 주소에 기초하여 선택됩니다. 선택된 라우트는 다음 항목에 기초한 것입니다.
   - 라우트 그룹 탐색 순서: 직접 라우트, 서브네트워크 라우트, 그 다음 디폴트 라우트.
   - 그룹내에서 가장 특정한 서브네트 마스크를 갖는 라우트가 선택됩니다.
   - 특정 라우트는 동등하게 리스트 순서나 로드 균형 조절 기법에 따릅니다.
   - 라우트는 시스템에 의해 수동으로 또는 동적으로 추가될 수 있습니다.

라우팅 연결 방법

라우팅은 네트워크 통신이 출발지에서 목적지로 흐르는 경로와 경로가 연결되는 방법에 관여합니다. 이 페이지에서는 iSeries 서버를 사용하는 경우에 고려해야 할 라우팅 방법에 관한 개념 정보로의 링크를 제공합니다.

- 지점 간 연결을 사용한 라우팅
  지점 간 연결을 사용하여 로컬 시스템에서 리모트 시스템으로 또는 로컬 네트워크에서 리모트 네트워크로 자료를 보낼 수 있습니다. 여기에서는 지점 간 연결에 대한 IP 주소 구성에 사용되는 두 개념을 설명합니다.
- 프록시 ARP 라우팅
  프록시 ARP(Address Resolution Protocol)는 신규 논리 네트워크를 작성하거나 라우팅 표를 갱신할 필요 없이 실제로 분리되어 있는 네트워크간의 연결을 제공합니다. 또한 프록시 ARP 라우팅 기법의 확장으로서 투명한 서브네트의 설명도 포함하고 있습니다.
- 동적 라우팅
  동적 라우팅은 네트워크가 변경할 때 라우팅 표를 자동으로 재구성하는 유지보수가 적은 방법입니다.
- 라우트 바인딩
  라우트 바인딩은 정보의 응답 패킷을 내보내기 위해 사용해야 할 인터페이스를 제어합니다.
- CIDR(Classless Inter-Domain Routing)
  CIDR은 라우팅 표의 크기를 줄이고 더 많은 IP 주소를 업무 범위내에서 사용할 수 있게 해 줍니다.
- 가상 IP를 사용한 라우팅
  가상 IP는 실제 인터페이스에 주소를 바인드할 필요 없이 시스템에 하나 이상의 주소를 할당하는 방법을 제공합니다. 다른 주소에 바인드시킨 도미노 웹(Domino Web) 서버의 복수 발생이나 디폴트 포트에 바인드시켜야 하는 다른 서비스를 실행하려는 경우에 이 기능을 사용할 수 있습니다.
- 결함 허용 한계
  결함 허용 한계는 고장 이후 라우트를 회복시킬 수 있는 여러 가지의 방법을 보여줍니다.
- NAT(네트워크 주소 변환)를 사용한 라우팅
  NAT를 사용한 라우팅으로 사설망에서 사용되는 IP 주소를 마스크하여 사설망을 보호하면서 인터넷과 같은 리모트 네트워크에 액세스하게 해 줍니다. 이 페이지에서는 iSeries 서버가 지원하는 NAT의 종류와 이것을 사용하는 이유에 대하여 설명합니다.
- OptiConnect 및 논리 파티션을 사용한 라우팅
  OptiConnect는 고속 광섬유 버스를 사용하여 여러 iSeries 서버를 연결시킵니다. 이 정보는 논리 파티션을 갖는 OptiConnect의 사용법과 및 사용 시의 장점을 다룹니다.

지점 간 연결을 사용한 라우팅

지점 간 연결은 일반적으로 광역 네트워크(WAN)를 통해 두 시스템을 연결하는 데 사용됩니다. 지점 간 연결을 사용하면 로컬 시스템에서 리모트 시스템으로 또는 로컬 네트워크에서 리모트 네트워크로 자료를 보낼 수 있습니다. 지점 간 연결을 지점 간 프로토콜과 혼동하지 마십시오. 지점 간 프로토콜(PPP)은 컴퓨터를 인터넷에 연결하기 위해 일반적으로 사용되는 지점 간 연결의 한 가지 유형입니다. PPP 연결을 설정하고 관리하는 방법에 대한 자세한 내용은 PPP 연결을 참조하십시오.

전화접속 회선, 전용 회선, 프레임 릴레이와 같은 기타 유형의 네트워크에서 지점 간 연결을 사용할 수 있습니다. 지점 간 연결에 대해 IP 주소를 구성할 수 있는 방법에는 번호를 지정한 연결과 번호를 지정하지 않은 연결이 있습니다. 이름에서 알 수 있드시 번호를 지정한 연결은 각 인터페이스에 대해 고유한 IP 주소를 갖습니다. 번호를 지정하지 않은 연결은 연결을 위해 추가 IP 주소를 사용하지 않습니다.

번호를 지정한 네트워크 연결:

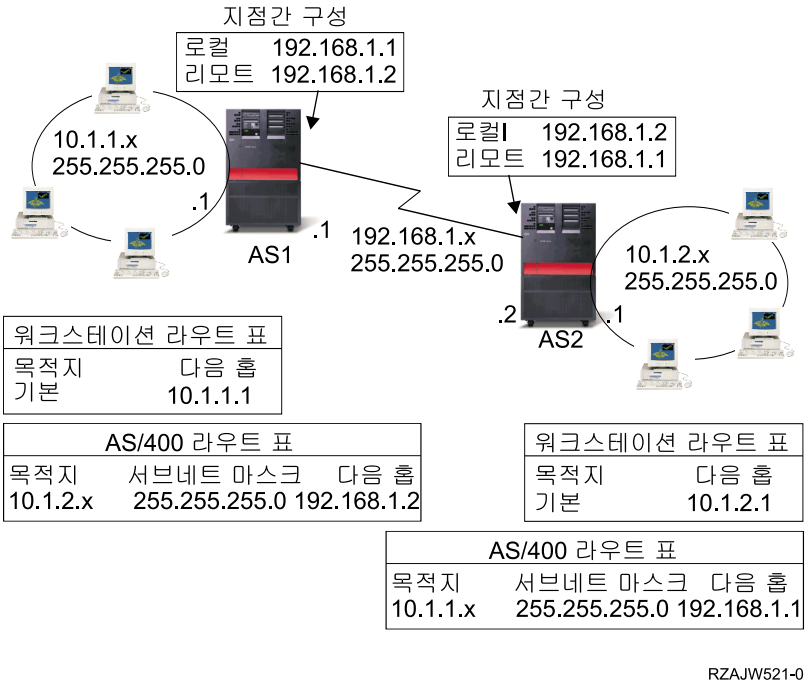
표면적으로는 지점 간 연결을 구성하는 가장 간단한 방법이 번호를 지정한 연결을 사용하는 것으로 보입니다. 번호를 지정한 연결은 연결의 각 끝에 대해 고유한 IP 주소를 정의한 지점 간 연결 정의입니다.

다음은 번호를 지정한 지점 간 연결을 고려할 때 유념해야 할 몇 가지 사항입니다.

- 연결의 각 끝이 고유한 IP 주소를 갖습니다.
- 리모트 시스템으로 통신이 흐를 수 있도록 라우팅 명령문을 사용자 시스템에 추가해야 합니다.
- 네트워크 관리자가 지점 간 링크의 주소를 관리해야 합니다.
- 두 시스템을 연결하는 데에만 주소가 모두 사용됩니다.

지점 간 연결을 iSeries 서버에 정의하면 연결의 다른 쪽 끝에서 임의의 네트워크로 연결하는 방법을 설명하기 위해 각 끝에 라우팅 항목을 작성해야 합니다. iSeries 서버에서의 라우팅 선택 프로세스는 각 인터페이스에 대하여 IP 주소를 갖는 것에 따라 달라집니다. 네트워크 관리자가 이들 주소와 라우트를 관리해야 합니다. 작은 네트워크에서는 이 주소들을 추적하는 것이 쉬우며 추가로 많은 주소들을 사용하지 않습니다. 그러나 큰 네트워크에서는 단지 각 끝에 인터페이스를 정의하기 위해 전체 주소 서브네트를 사용할 경우가 있습니다.

아래 그림은 두 대의 iSeries 서버에 있어서 번호를 지정한 네트워크 연결을 보여줍니다. 단지 AS1에서 AS2로의 통신만을 원하면 라우팅 항목이 필요 없습니다. 리모트 네트워크(10.1.2.x)의 시스템들과 통신할 경우에는 그림에 포함된 라우팅 항목을 각 시스템에 추가해야 합니다. 이것은 리모트 네트워크 10.1.2.x가 192.168.1.x 연결의 일부이기 때문입니다.



RZAJW521-0

번호를 지정하지 않은 네트워크 연결:

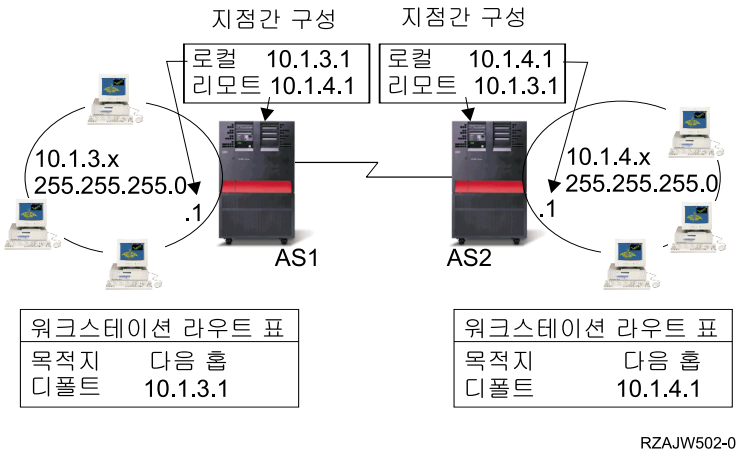
번호를 지정하지 않은 연결은 번호를 지정한 연결보다 더 복잡한 지점 간 연결 정의 방법입니다. 그러나 네트워크 관리를 위해서는 번호를 지정하지 않은 연결이 더 간단하고 좋은 방법인 것을 알 수 있습니다.

iSeries 서버에서의 라우팅 선택 프로세스는 인터페이스에 대하여 IP 주소를 갖는 것에 따라 달라집니다. 번호를 지정하지 않은 연결에서는 지점 간 인터페이스가 고유한 주소를 갖지 않습니다. 번호를 지정하지 않은 연결에서는 iSeries 서버 인터페이스의 IP 주소가 실제 리모트 시스템의 IP 주소입니다.

번호를 지정하지 않은 연결을 고려할 때 주의해야 할 사항:

- 지점 간 인터페이스가 리모트 네트워크에 있는 것으로 표시되는 주소를 갖습니다.
- 라우팅 명령문이 시스템에 필요하지 않습니다.
- 링크에 대해 IP 주소를 사용하지 않으므로 네트워크 관리를 단순화할 수 있습니다.

다음 예에서는 AS1이 10.1.4.x 네트워크에 인터페이스를 갖는 것으로 나오며 AS2는 10.1.3.x 네트워크에 인터페이스를 갖는 것으로 나옵니다. AS1은 주소 10.1.3.1로 LAN 네트워크 10.1.3.x에 연결됩니다. 이것은 AS1이 10.1.3.x 네트워크의 모든 시스템과 직접 통신할 수 있게 해 줍니다.



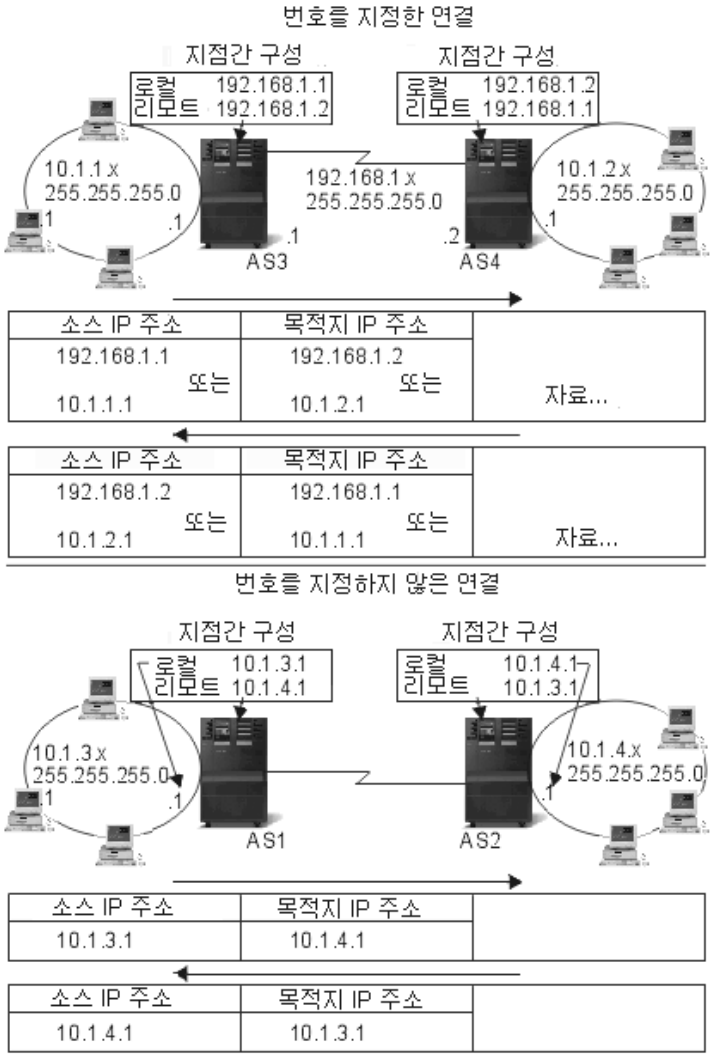
또한 예에서 AS2도 볼 수 있습니다. AS2는 주소 10.1.4.1로 LAN 네트워크 10.1.4.x에 연결됩니다. 이것은 AS2가 10.1.4.x 네트워크의 모든 시스템과 직접 통신할 수 있게 해 줍니다. 각 시스템(AS1과 AS2)은 리모트 주소를 자신의 라우팅 표에 로컬 인터페이스로서 추가합니다. 주소는 해당 주소로 향하는 패킷이 로컬로 처리되지 않도록 특별하게 취급됩니다. 리모트 주소에 대한 패킷은 인터페이스에 배치되고 연결의 다른 끝으로 전송됩니다. 패킷이 연결의 다른 끝에 도착할 때 정상적인 패킷 처리가 사용됩니다.

이제 AS1을 10.1.4.x 네트워크에 연결하고 AS2를 10.1.3.x 네트워크에 연결해야 합니다. 이 두 시스템이 같은 장소에 있다면 LAN 어댑터를 간단하게 각 시스템에 추가하고 새 인터페이스의 플러그를 올바른 LAN에 끼울 수 있습니다. 이렇게 하면 AS1과 AS2에 어떠한 라우팅 항목도 추가할 필요가 없습니다. 그러나 이 예에서는 시스템이 서로 다른 도시에 있으므로 지점 간 연결을 사용해야 합니다. 지점 간 연결을 사용하더라도 여전히 라우팅 항목을 추가하는 것을 피하고 싶을 것입니다. 이 경우 지점 간 프로토콜(PPP) 연결을 번호를 지

정하지 않은 연결로 정의하면 iSeries 서버에 라우팅 항목을 추가하지 않고 LAN 어댑터를 사용한 것과 같은 결과를 얻을 수 있습니다. 이를 위해 각 시스템은 라우트 해석에 사용할 리모트 시스템의 IP 주소를 빌려옵니다.

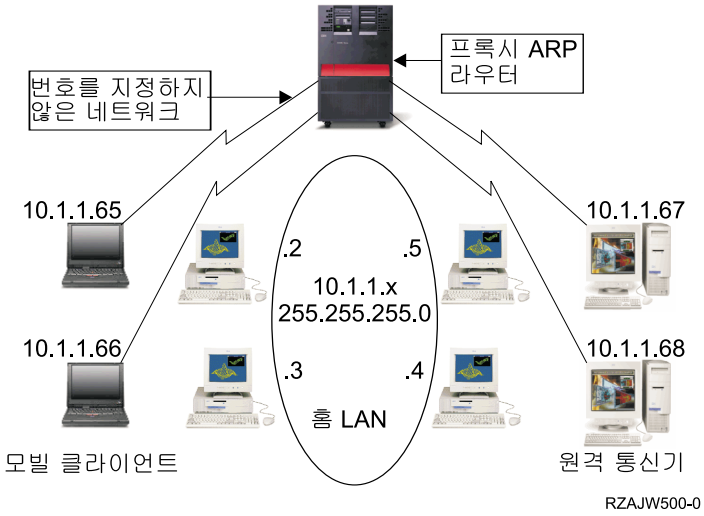
번호를 지정하지 않은 연결 대 번호를 지정한 연결의 자료 흐름:

다음 그림은 번호를 지정한 연결과 번호를 지정하지 않은 지점 간 연결에서 사용되는 주소를 보여줍니다. 그림 맨 위의 절반은 번호를 지정한 연결로서 리모트 시스템 주소 192.168.1.2 또는 10.1.2.1이 리모트 시스템에 도달할 때 사용됩니다. 이것은 10.1.2.1에 대한 패킷이 다음 홉으로서 192.168.1.2를 향하게 하는 라우팅 항목이 AS3에 들어 있기 때문입니다. 리턴 패킷에 사용되는 주소는 수신 패킷에 기초를 두고 있습니다. 그림 맨 아래에서 번호를 지정하지 않은 연결에 사용되는 주소를 볼 수 있습니다. 아웃바운드 패킷에는 10.1.3.1의 소스와 10.1.4.1의 목적지를 갖습니다. 시스템이 지점 간 연결의 리모트 시스템 주소를 사용하여 리모트 시스템에 대해 직접 인터페이스를 갖기 때문에 어느 쪽 시스템에도 라우팅 항목이 필요하지 않습니다.



프록시 ARP(Address Resolution Protocol) 라우팅

프록시 ARP(Address Resolution Protocol) 라우팅을 사용하면 물리적으로 구별되는 별개의 네트워크가 하나의 논리 네트워크에 있는 것처럼 만들 수 있습니다. 프록시 ARP는 신규 논리 네트워크를 작성하거나 라우팅 표를 갱신할 필요 없이 물리적으로 별개의 네트워크 사이에서 연결을 제공합니다. 프록시 ARP를 사용하면 시스템들이 LAN에 직접 연결되어 있지 않더라도 LAN의 다른 시스템에 연결되어 있는 것처럼 나타날 수 있습니다. 이것은 다이얼 인 인터페이스로부터 전체 네트워크로의 연결을 제공하기 위한 전화접속 시나리오에서 유용합니다. 다음 그림은 발생할 가능성이 있는 하나의 시나리오를 보여줍니다. 10.1.1.x는 사용자의 홈 LAN이고 10.1.1.65부터 10.1.1.68까지는 리모트 시스템입니다.

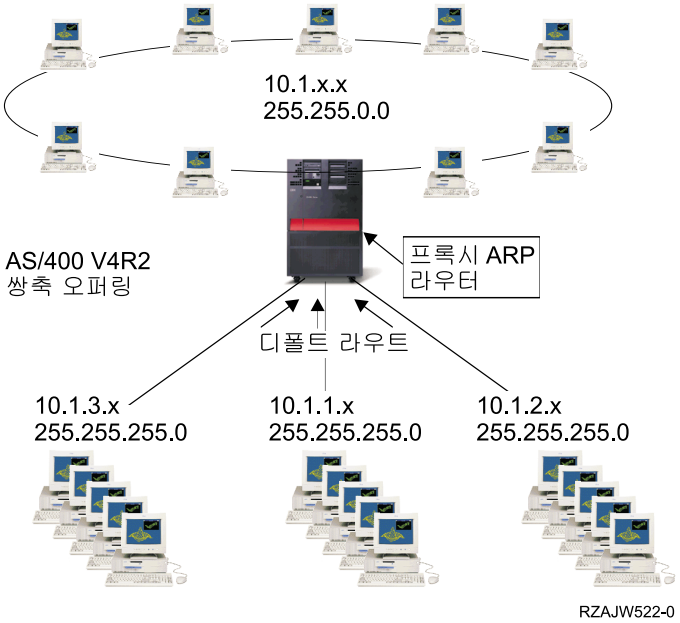


홈 LAN(10.1.1.x)의 시스템은 리모트 시스템 중 하나로 자료를 송신할 때 맨 먼저 ARP 요구를 수행합니다. 이것은 목표 시스템의 주소를 요구하기 위해 LAN 세그먼트에 연결되어 있는 모든 시스템으로 가는 브로드캐스트입니다. 그러나, 리모트로 연결된 시스템은 브로드캐스트를 알지 못합니다. 이 시스템이 프록시 ARP가 들어오는 시스템입니다. iSeries 서버는 어떤 시스템이 리모트로 연결되어 있는지 알고 있습니다. iSeries 서버가 리모트로 연결된 기계 중 하나에 대한 ARP 요구를 알게 되면 해당 주소를 사용하여 ARP 요구에 응답합니다. 또한 iSeries 서버는 자료를 받아 다시 리모트 시스템으로 전송합니다. 전송이 발생하기 위해서는 IP 전송을 *yes로 설정해야 합니다. 리모트 시스템이 연결되어 있지 않으면 iSeries 서버가 ARP 요구에 응답하지 않고 요구한 시스템이 자료를 송신하지 않습니다.

전체 서브네트 또는 일정 범위의 호스트에 대한 프록시로서 투명한 서브네트를 사용할 수 있습니다. 투명한 서브네트화는 스터브 네트워크가 1차 네트워크 주소 공간 밖의 주소를 할당받게 해 줍니다.

투명한 서브네트

프록시 ARP 개념을 확장하는 한 방법으로 투명한 서브네트를 사용할 수 있습니다. 투명한 서브네트는 단일 호스트에 대해 작업하므로 전체 서브네트나 일정 범위의 호스트에 연결할 수 있습니다. 아래 그림에서 스터브 네트워크(10.1.1.x부터 10.1.3.x까지)에는 1차 네트워크 주소 공간(10.1.x.x) 범위 밖의 주소가 할당되어 있음을 볼 수 있습니다.



쌍축 LAN은 실제 LAN 주소 범위 안에 있는 주소 범위에 정의됩니다. V4R2 이전에는 TCP/IP 라우트 추가 및 TCP/IP 인터페이스 추가에 대한 편집에서 이것을 허용하지 않았습니다. V4R2에서는 편집이 편리해졌습니다. 투명한 서브네트를 사용하여 다른 세그먼트의 두 인터페이스가 동일한 세그먼트에 있는 것처럼 보이는 주소를 가질 수 있습니다. 이 경우 iSeries 400 서버가 쌍축 제어기 뒤에 연결되어 있는 어떤 시스템에 대해서나 자동으로 프록시 ARP를 수행합니다. 이로 인해 10.1.x.x 네트워크의 모든 시스템이 10.1.x.x 네트워크의 시스템으로 변경하지 않고 모든 서브네트 시스템과 통신할 수 있습니다.

WAN상의 투명한 서브네트화:

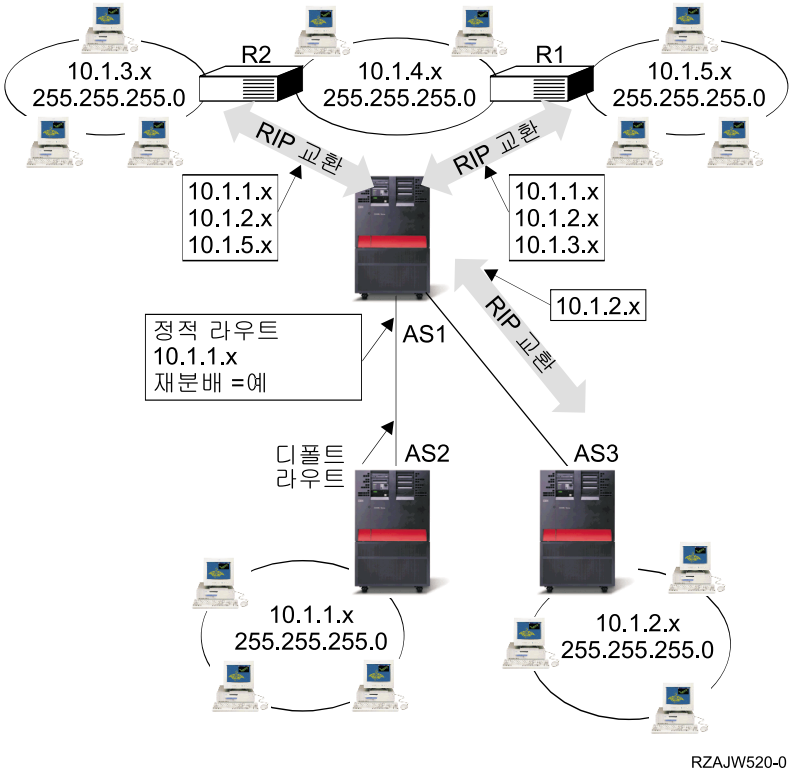
투명한 서브네트 기능은 리모트 위치에 놓인 실제 LAN을 처리할 수 있도록 더욱 확장시킬 수 있습니다. WAN상의 투명한 서브네트화는 리모트 네트워크가 홈 네트워크에 연결되어 있는 것처럼 보이게 합니다. 위의 그림에는 세 개의 네트워크가 iSeries 서버를 통해 홈 10.1.x.x 네트워크에 연결되어 있습니다. 이 네트워크들은 홈 네트워크에 대해 리모트 네트워크를 투명하게 만드는 서브네트 마스크를 사용하여 모두 정의되어 있습니다. 프록시 ARP가 10.1.1.x, 10.1.2.x, 10.1.3.x 서브네트에 있는 시스템의 홈 네트워크에 대한 모든 ARP 요구에 응답합니다. 이로 인해 홈 네트워크에 대한 통신이 홈 네트워크의 iSeries 서버로 자동으로 라우트됩니다. 그리고 나서 iSeries 서버가 차례로 해당 자료를 올바른 리모트 iSeries 서버로 라우트합니다. 이때 리모트 iSeries 서버에서는 이 자료를 처리하거나 리모트 LAN상의 올바른 시스템으로 자료를 다시 전송합니다. 리모트 LAN의 워크스테이션은 네트워크 안의 리모트 iSeries 서버를 첫 번째 홉 게이트웨이로 가리키는 디폴트 라우트를 가지고 있어야 합니다. 홈 LAN 안의 워크스테이션들은 신규 논리 네트워크가 작성되지 않기 때문에 추가로 라우팅 항목이 필요 없습니다.

동적 라우팅

동적 라우팅은 라우팅 인터넷 프로토콜(RIP)과 같은 내부 게이트웨이 프로토콜(IGP)에서 제공합니다. RIP를 사용하면 RIP 네트워크의 일부로 호스트를 구성할 수 있습니다. 이와 같은 유형의 라우팅에는 유지보수가 거

의 필요 없으며 네트워크가 변경되거나 붕괴될 때 라우팅 표를 자동으로 재구성합니다. RIPv2가 iSeries 서버에 추가되었으므로 RIP 패킷을 송수신하여 네트워크 전체에서 라우트를 갱신할 수 있습니다.

아래 그림에서는 AS2를 통한 네트워크 10.1.1.x와의 연결을 설명하는 중앙 시스템(AS1)에 정적 라우트가 추가됩니다. 이것은 라우트 재분배를 예(yes)로 설정한 정적 라우트(네트워크 관리자가 추가함)입니다. 이렇게 설정하면 다른 라우터 및 시스템들이 이 라우터를 공유하며 10.1.1.x에 대한 통신량이 있을 때 그 통신량을 중앙의 iSeries 서버(AS1)로 라우트합니다. AS2가 라우트된 서버를 시작시킨 후 RIP 정보를 송수신합니다. 이 예에서는 AS1이 AS2가 10.1.2.x에 직접 연결되어 있다는 메세지를 송신하는 중입니다.



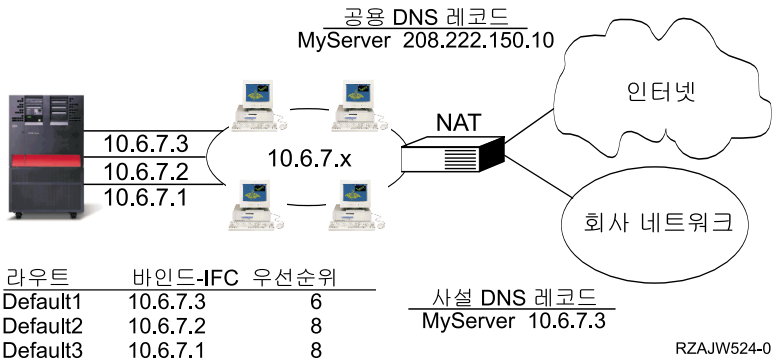
이 예에서 발생하는 문제

- AS1은 AS2로부터 이 RIP 패킷을 수신하고 처리합니다. AS1에 10.1.2.x에 대한 라우트가 없으면 이 라우트를 저장합니다. AS1에 10.1.2.x에 대한 경로가 있으면(같은 홉 수 또는 더 작은 홉 수를 가진) 이 신규 라우트 정보를 삭제합니다. 이 예에서는 AS1이 라우트 자료를 보유합니다.
- AS1이 10.1.5.x에 대한 라우트 정보를 가진 R1으로부터 정보를 수신하여 이 라우트 정보를 보유합니다.
- AS1이 10.1.3.x에 대한 라우트 정보를 가진 R2로부터 정보를 수신하여 이 라우트 정보를 보유합니다.
- 다음에 AS1이 RIP 메세지를 송신할 때 AS1은 자신은 알고 있지만 R1이 모를 수도 있는 모든 연결을 설명하는 정보를 R1에 송신합니다. AS1이 10.1.1.x, 10.1.2.x, 10.1.3.x에 관한 라우트 정보를 송신합니다. AS1은 R1이 10.1.4.x에 연결되어 있고 라우트가 필요 없다는 것을 알기 때문에 10.1.4.x에 대한 정보를 R1에 송신하지 않습니다. 비슷한 정보가 R2와 AS3에 송신됩니다.

라우트 바인딩

우선 라우트 바인딩을 진행하기 전에 정보의 응답 패킷을 내보내기 위해 사용했던 인터페이스에 대해 사용자가 완전한 제어를 가지고 있지 않습니다. 라우트 추가 기능에 추가시킨 우선 라우트 바인딩 인터페이스는 사용자가 라우트를 인터페이스에 명시적으로 바인드할 수 있게 함으로써 패킷을 송신할 때 사용되는 인터페이스에 대해 제어를 더욱 강화시킵니다.

다음 그림에는 동일한 네트워크에 연결된 세 개의 인터페이스가 나옵니다. 인바운드 요구를 수신하는 인터페이스에 관계없이 응답을 동일한 인터페이스에 송신할 수 있도록 해야 합니다. 이와 같이 하려면 각 인터페이스에 "복제" 라우트를 추가하십시오. 이 예에서는 서로 다른 인터페이스에 명시적으로 바인드시킨 세 개의 디폴트 라우트를 추가합니다. 이 바인딩은 인터페이스가 시작하거나 종료하는 순서와 관계 없이 변경되지 않습니다.



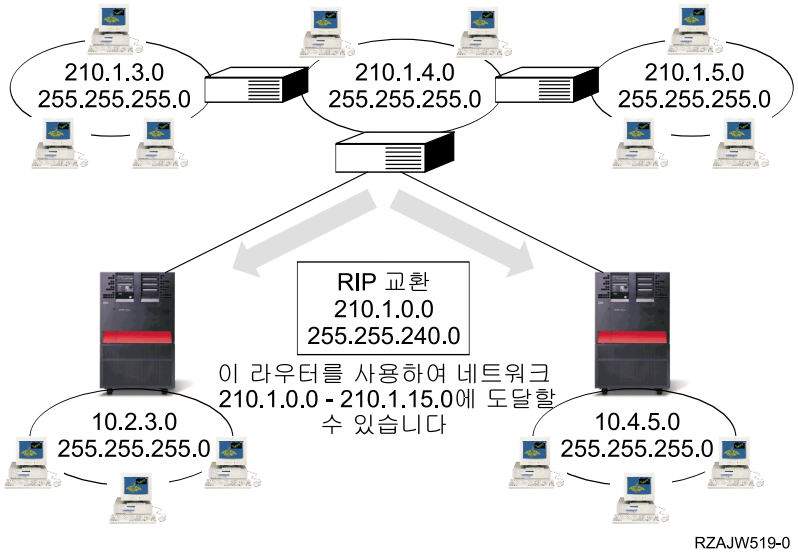
라우트	바인드-IFC	우선순위
Default1	10.6.7.3	6
Default2	10.6.7.2	8
Default3	10.6.7.1	8

CIDR(Classless Inter-Domain Routing)

CIDR(무 클래스 도메인간 라우팅) 또는 수퍼네팅(supernetting)은 여러 개의 C 클래스 주소 범위를 하나의 네트워크나 라우트에 결합시키기 위한 하나의 방법입니다. 이 라우팅 방법은 C 클래스 인터넷 프로토콜(IP) 주소를 추가합니다. 이 주소는 고객이 사용할 수 있도록 인터넷 서비스 제공자(ISP)가 제공한 것입니다. CIDR 주소는 라우팅 표의 크기를 줄이고 더 많은 IP 주소를 사용할 수 있게 해 줍니다.

과거에는 네트워크 클래스에 필요한 마스크 이상으로 서브네트 마스크가 필요했습니다. C 클래스 주소의 경우 이것은 255.255.255.0이 사용자가 지정할 수 있는 가장 큰(253 호스트) 서브네트였습니다. 회사들이 네트워크에 253개 이상의 호스트를 필요로 할 때 IP 주소를 보존하기 위해서는 인터넷이 여러 개의 C 클래스 주소를 발행해야 했습니다. 이로 인해 라우트 구성 및 기타 어려운 문제가 발생했습니다.

이제 CIDR을 통해 이와 같은 인접한 C 클래스 주소들을 서브네트 마스크로 하나의 네트워크 주소 범위에 결합시킬 수 있습니다. 예를 들어, 4개의 C 클래스 주소(서브네트 마스크 255.255.255.0을 이용하는 208.222.148.0, 208.222.149.0, 208.222.150.0, 208.222.151.0)를 제공하려는 경우 ISP에게 서브네트 마스크 255.255.252.0을 사용하여 각 주소를 슈퍼네트로 만들어 줄 것을 요청할 수 있습니다. 이 마스크가 라우팅을 위해 4개의 네트워크를 하나로 결합시킵니다. CIDR은 불필요하게 할당되어 있는 IP 주소의 수를 줄여 주기 때문에 유익합니다.

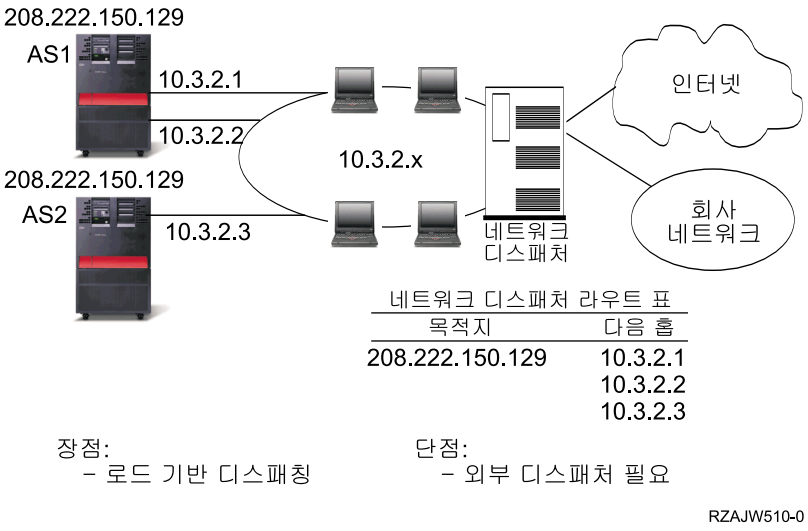


이 예에서는 라우터가 네트워크 주소 210.1.0.0과 서브네트 마스크 255.255.240.0을 이용하는 하나의 RIP 메세지를 송신하도록 설정됩니다. 이것은 시스템이 이 라우터를 통해 210.1.0.0부터 210.1.15.0까지의 네트워크에 대한 RIP 메세지를 수신하도록 지시합니다. CIDR을 사용할 수 없으면 16개의 메세지 대신에 같은 정보를 담고 있는 하나의 메세지를 송신합니다.

가상 IP를 사용한 라우팅

무회로 또는 루프백 인터페이스라고도 부르는 가상 IP는 여러 가지의 다른 용도로 사용할 수 있는 강력한 기능입니다. 가상 IP는 실제 인터페이스에 주소를 바인드할 필요 없이 하나 이상의 주소를 시스템에 할당하는 방법을 제공합니다. 서로 다른 주소에 바인드된 도미노 웹 서버의 복수 발생을 실행하거나 디폴트 포트에 바인드해야 하는 기타 서비스를 실행하려는 경우에 이 기능을 사용할 수 있습니다.

가상 IP를 사용할 대부분의 환경은 로드 균형 조절 및 결함 허용 한계와 같이 로컬 게이트웨이와 iSeries 서버 사이에 복수의 경로를 제공하려는 경우입니다. 이러한 관점에서는 각 '경로'는 추가적인 인터페이스를 의미하며 결과적으로 iSeries 서버에서의 가상 IP 주소가 아닌 추가 IP 주소를 의미합니다. 이러한 복수 인터페이스는 로컬 네트워크에서만 볼 수 있어야 합니다. 리모트 클라이언트들이 iSeries 서버의 여러 IP 주소들을 알 필요가 없습니다. 즉 리모트 클라이언트들이 iSeries 서버를 하나의 IP 주소로 간주하는 것이 이상적입니다. 인바운드 패킷이 게이트웨이를 통해 로컬 네트워크를 지나 iSeries 서버에 도달하는 방식이 리모트 클라이언트에게는 보이지 않아야 합니다. 이것을 수행하는 방법은 가상 IP를 사용하는 것입니다. 리모트 클라이언트가 가상 IP 인터페이스만을 보는 반면 로컬 클라이언트는 실제 IP 주소 중 하나를 사용하여 iSeries와 통신해야 합니다.



가상 IP 환경은 리모트로 연결되어 있는 클라이언트용 서버로 작동하는 iSeries 서버를 위한 것입니다. 실제 인터페이스보다 더 중요한 것은 가상 IP 주소가 다른 서브네트에 있다는 것입니다. 또한 가상 IP 주소를 사용할 경우 iSeries 서버가 큰 네트워크나 서브네트워크에 연결된 것이 아닌 단일 호스트로 보이게 됩니다. 그러므로 가상 IP 인터페이스에 대한 서브네트 마스크를 255.255.255.255로 설정하는 것이 좋습니다.

가상 IP 주소가 하나의 실제 인터페이스에 바인드된 것이 아니기 때문에 iSeries 서버는 가상 IP 주소에 대한 ARP(Address Resolution Protocol) 요구에 절대 응답하지 않습니다. 다시 말해서 가상 IP 주소에 직접 전달할 수 없습니다. 다른 시스템이 가상 IP 주소에 도달하기 위해서는 해당 주소에 도달하도록 정의된 라우트가 있어야 합니다. 이것이 가상 IP가 주로 리모트로 연결된 클라이언트용으로 설계되는 이유입니다. 다음 예에서 워크스테이션들은 모두 다음 홉 게이트웨이로 iSeries 서버에 있는 10.3.2 인터페이스 중 하나를 가리킵니다. 패킷이 iSeries 서버에 도착하면 패킷 처리 과정을 거치게 됩니다. 목적지 주소가 시스템에 정의된 주소(가상 IP 주소 포함) 중 하나와 일치하면 시스템이 해당 패킷을 처리합니다.

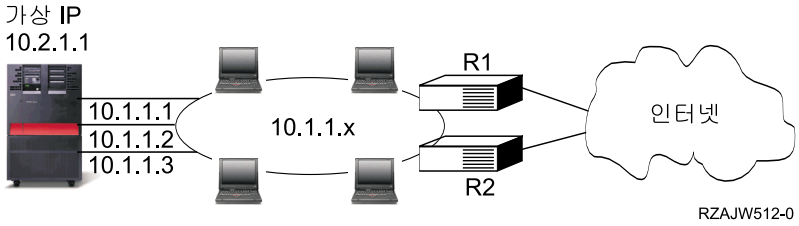
DNS 서버는 요구 받은 서버의 주소를 사용합니다. 이 경우 모든 주소가 같은 시스템을 나타냅니다. 가상 IP 기능은 여러 시스템을 하나의 큰 시스템으로 통합할 때 사용할 수 있습니다.

결함 허용 한계

가상 IP 주소의 또 다른 사용법은 라우트 결함 허용 한계에 대해 보호하는 것입니다.

이 예는 정전 이후에 라우트를 회복시킬 수 있는 여러 가지 방법을 보여줍니다. 가장 신뢰할 수 있는 연결은 가상 IP 주소를 시스템에 정의한 경우입니다. 가상 IP 지원을 사용하면 인터페이스가 실패하더라도 그 세션이 다른 인터페이스를 사용하여 계속 대화할 수 있습니다.

네트워크 장애: 라우트와 연결이 대체 경로로 다시 바운드 됨



라우터 R1이 실패하는 경우 발생하는 사항

- R1을 통한 연결이 R2를 통해 다시 전달됩니다.
- 실패한 게이트웨이는 R1이 회복되었음을 감지하지만 활동 중인 연결은 R2를 통해 계속 실행합니다.

인터페이스 10.1.1.1이 실패하는 경우 발생하는 사항

- 활동 중인 10.1.1.1에 대한 연결은 없어지지만 기타 10.1.1.2, 10.1.1.3, 10.2.1.1에 대한 연결은 남습니다.
- 라우트 리바인드:
  - V4R2 이전: 간접 라우트를 10.1.1.2 또는 10.1.1.3에 리바인드시킵니다.
  - V4R2: 우선 바인딩 인터페이스를 NONE으로 설정하는 경우에만 라우트를 리바인드시킵니다.
  - V4R3 이상: 10.2.1.1을 가상 IP 주소 및 1차 시스템 주소로 정의해야 합니다.
    - 시스템의 1차 IP 주소는 계속해서 활동 상태로 있습니다.
    - 최소한 하나의 실제 인터페이스가 활동 상태로 있을 동안에는 시스템이 액세스 가능 상태를 유지합니다.

네트워크 주소 변환과 함께 라우팅

NAT(네트워크 주소 변환)는 방화벽 내부에서 사용되는 IP 주소를 마스킹함으로써 사설망을 보호하면서 리모트 네트워크(보통 인터넷)에 대해 액세스를 제공합니다. iSeries 서버 라우팅을 위해 이러한 유형의 NAT를 사용할 수 있습니다.

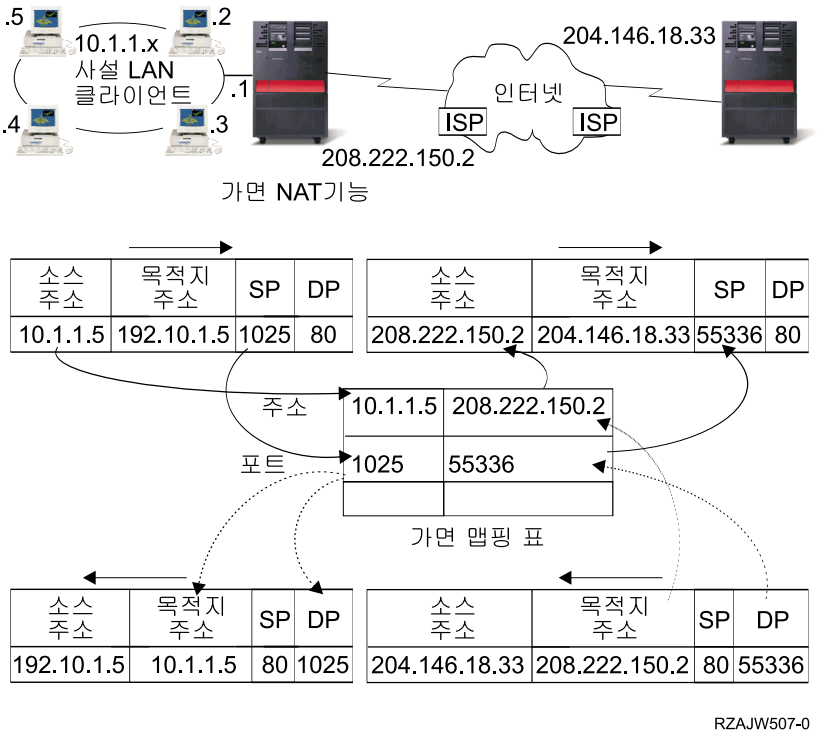
- 가면 NAT
  가면 NAT를 사용하면 사설망을 공용 인터페이스에 바인드한 주소 뒤에 숨겨서 표시할 수 있습니다.
- 동적 NAT
  동적 NAT는 사설망내에서 공용 네트워크와의 연결을 구축합니다. 차이점은 공용 주소의 풀(pool)이 아웃바운드가 연결될 때 유지보수되고 사용된다는 점입니다.
- 정적 NAT
  정적 NAT는 공용 네트워크에서 사설망으로 이루어지는 인바운드 연결을 지원합니다.

가면 NAT(Masguerade NAT)

가면 NAT는 사설망을 공용 인터페이스로 바인드시킨 주소로 표현할 뿐 아니라 주소 뒤에 숨기기 위해 사용됩니다. 많은 경우에 있어서 이것은 인터넷 서비스 제공자(ISP)가 할당하는 주소로서 지점 간 프로토콜(PPP) 연

결의 경우 동적일 수 있습니다. 이와 같은 유형의 변환은 외부 공용 네트워크로 지정된 사설망내에서 시작하는 연결에 대해서만 사용할 수 있습니다. 각 아웃바운드 연결은 서로 다른 소스 IP 포트 번호를 사용하여 유지보수됩니다.

가면 NAT를 사용하면 개인용 IP 주소를 갖는 워크스테이션이 iSeries 서버를 사용하는 인터넷상의 호스트와 통신할 수 있습니다. iSeries 서버에는 인터넷 게이트웨이로서 로컬 ISP가 할당한 IP 주소가 있습니다. 로컬로 연결된 기계라는 용어는 연결 방법(LAN 또는 WAN)이나 연결 거리에 상관없이 내부 네트워크의 모든 기계를 지칭하는 데 사용됩니다. 외부 기계라는 용어는 인터넷에 있는 기계를 의미하는 데 사용됩니다. 다음 그림은 가면 NAT의 작동 방식을 나타낸 것입니다.



인터넷 쪽에서는 모든 워크스테이션이 iSeries 400 서버에 포함된 것으로 보입니다. 즉 하나의 IP 주소만 iSeries 400 서버와 워크스테이션 모두에 연관됩니다. 라우터가 워크스테이션용 패킷을 수신할 때 라우터는 패킷을 수신할 내부 LAN의 주소를 판별하고 해당 주소로 패킷을 송신합니다.

iSeries 서버가 게이트웨이인 동시에 디폴트 목적지가 될 수 있도록 각 워크스테이션을 설정해야 합니다. 워크스테이션 중 하나가 인터넷으로 보낼 패킷을 iSeries 서버로 보낼 경우 특정 통신 연결(포트)과 워크스테이션간의 통신이 설정됩니다. 가면 NAT 기능은 포트 번호를 저장하여 그 연결을 통해 워크스테이션의 패킷에 대한 응답을 수신할 때 응답을 올바른 워크스테이션으로 송신할 수 있게 해 줍니다.

활동 포트 연결 그리고 연결의 양 끝이 마지막으로 액세스한 시간에 대한 레코드가 작성되고 가면 NAT가 그 레코드를 유지보수합니다. 이 레코드는 유휴 링크를 더 이상 사용하지 않는다는 가정하에 사전에 결정된 시간을 근거로 유휴 상태의 모든 연결에서 주기적으로 제거됩니다.

워크스테이션과 인터넷 사이의 모든 통신은 반드시 로컬로 연결된 기계로 시작해야 합니다. 이것은 효과적인 보안 방화벽으로서 인터넷이 사용자 워크스테이션의 존재를 알 수 없으므로 워크스테이션 주소를 인터넷에 브로드캐스트할 수 없습니다.

가면 NAT 구현의 핵심은 여러 통신 스트림간의 구별을 위해 가면 NAT가 발행한 논리 포트를 사용하는 것입니다. TCP에 소스 및 목적지 포트 번호가 들어 있습니다. NAT가 이 목적지에 논리 포트 번호를 추가합니다.

아웃바운드 가면 NAT 처리:

위의 그림에서 아웃바운드 메세지는 개인용 LAN에서 인터넷으로 가는 패킷입니다. 아웃바운드 메세지(로컬에서 외부로)에는 시작한 워크스테이션이 사용하는 소스 포트가 들어 있습니다. NAT가 이 번호를 저장하고 전송 헤더에서 고유한 논리 포트 번호로 대체합니다. 아웃바운드 데이터그램에서는 소스 포트 번호가 로컬 포트 번호입니다.

1. 아웃바운드 가면 NAT 처리는 수신되는 모든 IP 패킷이 외부 IP 주소에 바인드된다는 가정하에 패킷을 로컬로 라우트시켜야 하는지를 검사하지 않습니다.

2. 논리 포트 번호 세트가 소스 IP 주소와 소스 포트뿐 아니라 전송층에 일치하는 포트가 있는지를 탐색합니다. 일치하는 포트 번호를 발견하면 해당 논리 포트 번호를 소스 포트로 대체시킵니다. 일치하는 포트 번호를 발견하지 못하면 새 번호를 작성하고 새 논리 포트 번호를 선택하여 소스 포트를 대체시킵니다.

3. 소스 IP 주소를 변환시킵니다.

4. 그런 다음 IP가 평소와 같이 패킷을 처리하여 올바른 외부 시스템으로 송신합니다.

인바운드 가면 NAT 처리(응답 및 기타):

위의 그림에서 인바운드 메세지는 인터넷에서 개인용 LAN으로 가는 패킷입니다. 인바운드 데이터그램에서는 목적지 포트 번호가 로컬 포트 번호입니다(인바운드 메세지에서는 소스 포트 번호가 외부 포트 번호입니다. 아웃바운드 메세지에서는 목적지 포트 번호가 외부 포트 번호입니다).

로컬로 연결된 기계에 바인드시킨 인터넷으로부터 리턴되는 응답 메세지는 전송층 헤더에서 목적지 포트 번호로서 가면이 할당된 논리 포트 번호를 갖습니다. 가면 NAT 인바운드 처리 단계는 다음과 같습니다.

1. 가면 NAT는 데이터베이스에서 이 논리 포트 번호(소스 포트)를 탐색합니다. 논리 포트 번호를 발견하지 못하면 그 패킷을 필요 없는 패킷으로 가정하여 그대로 호출자에게 리턴시킵니다. 그런 다음 정상적인 알 수 없는 목적지로 처리합니다.

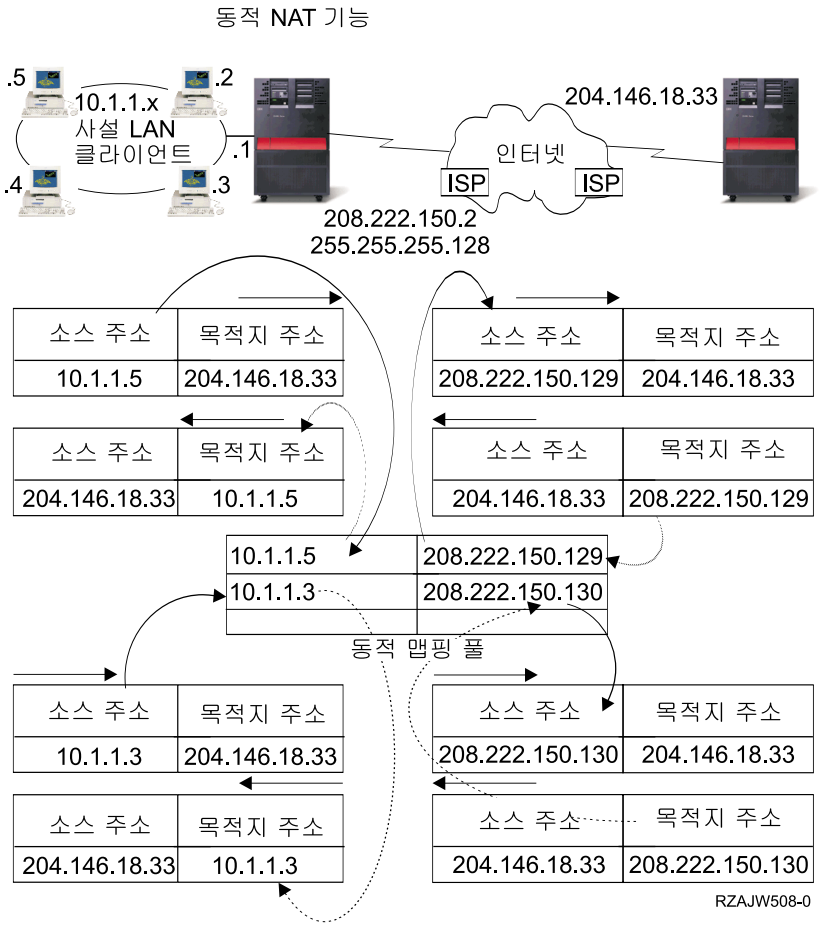
2. 일치하는 논리 포트 번호가 있으면 소스 IP 주소가 기존 논리 포트 번호 표 항목의 목적지 IP 주소와 일치하는지 판별하기 위해 추가로 검사합니다. 일치하면 원래 로컬 기계의 포트 번호로 IP 헤더의 소스 포트를 대체시킵니다. 검사에 실패하면 패킷을 그대로 리턴합니다.

3. 로컬 일치 IP 주소를 패킷 IP 목적지에 배치합니다.

4. IP나 TCP가 평소와 같이 패킷을 처리한 다음 올바르게 로컬로 연결된 기계에서 끝냅니다. 올바른 소스 및 목적지 포트 주소를 판별하기 위해서는 가면 NAT에 논리 포트 번호가 필요하므로 가면 NAT가 인터넷으로부터 필요없는 데이터그램을 처리하는 것은 불가능합니다.

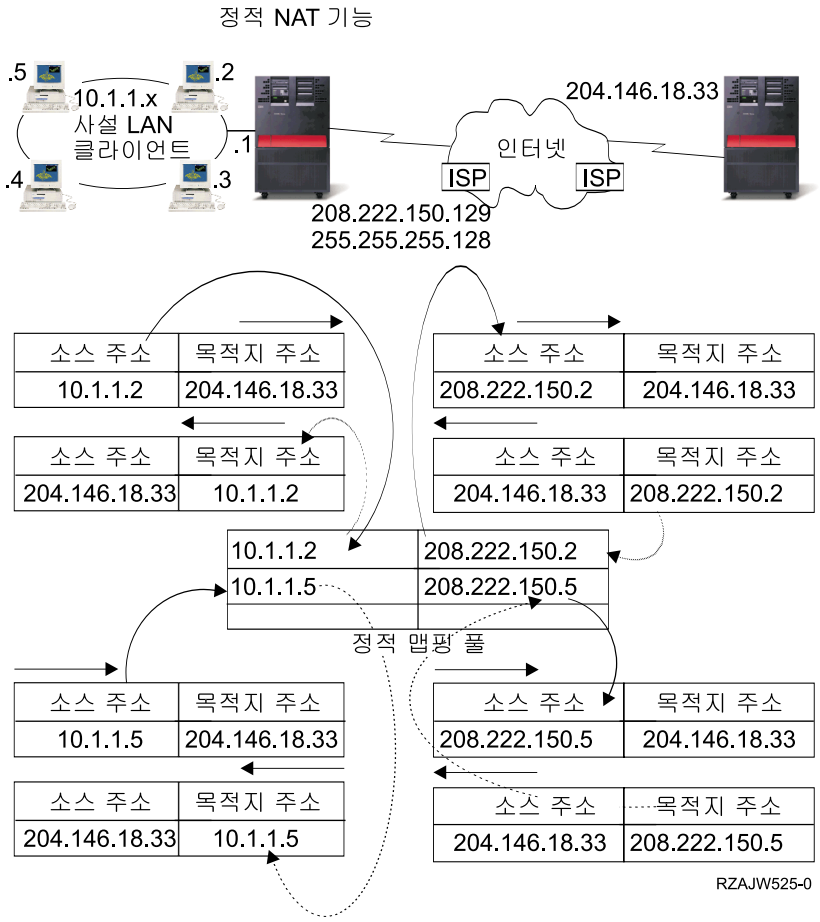
동적 NAT

동적 NAT는 사설망 안으로부터 공용 네트워크로 연결을 설정하기 위해서만 사용할 수 있습니다. 네트워크 주소의 풀(pool)은 아웃바운드 연결이 이루어질 때 유지보수되고 사용됩니다. 각 연결에 고유한 공용 주소가 할당됩니다. 최대 동시 연결 수는 풀(pool)에 있는 공용 주소의 수와 같습니다. 이것은 주소 사이의 일대일 대응과 유사합니다. 동적 NAT는 동적 NAT 주소를 통해 인터넷과 통신할 수 있게 해 줍니다. 아래 그림은 동적 NAT를 보여줍니다.



정적 NAT

정적 NAT는 개인용 및 공용 주소의 단순한 일대일 맵핑입니다. 정적 NAT는 공용 네트워크에서 사설망으로의 인바운드 연결을 지원하는 데 필요합니다. 정의된 각 로컬 주소에 대해 글로벌하게 고유하고 연관된 주소가 있어야 합니다.



OptiConnect 및 논리 파티션을 사용한 라우팅

OptiConnect와 논리 파티션은 사용자가 프록시 ARP, 지점 간 연결, 가상 IP 인터페이스의 기본 라우팅 방법을 사용하기 위한 기타 환경을 제공합니다. 다음은 기본 방법과 다른 몇 가지의 방법입니다.

- TCP/IP 및 OptiConnect
  OptiConnect를 사용하면 OptiConnect 버스를 통해 TCP/IP 연결을 정의할 수 있습니다. 이 페이지에는 이 피처와 그 사용 방법이 나옵니다.
- 논리 파티션을 갖는 가상 OptiConnect
  가상 OptiConnect TCP/IP 인터페이스는 파티션 간 통신 경로로 사용됩니다. 단일 iSeries 서버는 복수의 가상 기계로 논리적으로 파티션되어 있습니다. 각 파티션에는 고유한 주소 공간이 있습니다. TCP/IP의 관점에서는 각 파티션이 독립된 iSeries 서버로 보입니다. 이 페이지에는 이 피처를 사용할 때의 장점이 나옵니다.

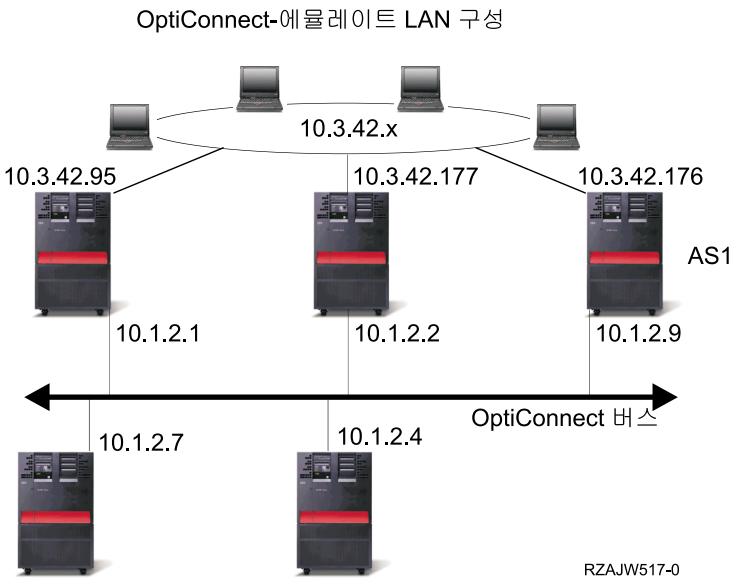
TCP/IP 및 OptiConnect

OptiConnect를 사용하면 OptiConnect 버스상에 TCP/IP 연결을 정의할 수 있습니다. OptiConnect상의 TCP/IP는 프록시 ARP, 번호를 지정하지 않은 지점 간 네트워크, 가상 IP 인터페이스와 같은 라우팅 빌딩 블록을 위한 또 다른 방법을 제공합니다. OptiConnect 에뮬레이트 LAN 구성과 OptiConnect 지점 간 구성으로 이것을 구성할 수 있습니다.

OptiConnect 에뮬레이트 LAN 구성을 사용하면 OptiConnect 버스가 TCP/IP에 대한 LAN으로 나타납니다. 이것은 구성하기가 간단하지만 LAN OptiConnect 연결은 RIP(라우팅 정보 프로토콜) 또는 정적 라우트를 필요로 하기 때문에 자동으로 이루어집니다.

OptiConnect 지점 간 구성은 OptiConnect 호스트의 각 쌍에 대해 구성되는 번호를 지정하지 않은 지점 간 인터페이스를 사용합니다. 신규 네트워크가 작성되지 않으므로 LAN OptiConnect 연결이 자동으로 이루어집니다. 이 구성의 장점 중 하나는 추가 라우트 정의가 필요없다는 점입니다. 하나의 네트워크에 있는 호스트와 다른 네트워크에 있는 호스트간의 연결은 자동으로 이루어집니다. 또 다른 장점은 두 네트워크가 모두 활동하는 경우에는 iSeries 서버간에서 OptiConnect 버스를 통해 자료 전송이 이루어지는데 이것은 이 라우트들이 가장 특정한 서브네트 마스크를 갖고 있기 때문입니다. OptiConnect 버스가 다운되면 토큰링 LAN으로 통신이 자동 전환됩니다.

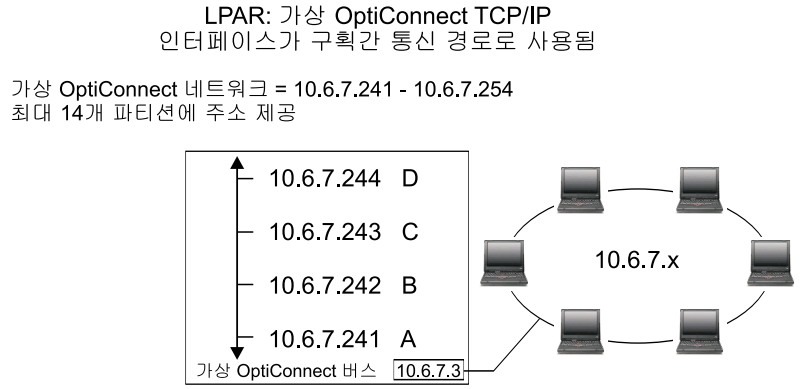
가상 IP를 사용한 OptiConnect 지점 간 구성은 번호를 지정하지 않은 지점 간 구성을 변형시킨 것입니다.번호를 지정하지 않은 지점 간 인터페이스를 사용할 때마다 연관된 로컬 인터페이스를 각 인터페이스에 지정해야 한다는 점을 기억하십시오. 이것은 지점 간 링크의 리모트 끝에 있는 시스템이 로컬 iSeries 서버를 알 수 있는 IP 주소입니다. 아래에서와 같이 연관된 로컬 인터페이스가 iSeries 서버의 1차 LAN 인터페이스일 수 있습니다. 또는 연관된 로컬 인터페이스로서 가상 IP 인터페이스를 사용할 수 있습니다. 이 구성에서는 OptiConnect 버스를 지점 간 연결의 콜렉션으로 사용합니다. 그리고 각 호스트 쌍에 대해 번호를 지정하지 않은 연결을 정의합니다. 이전 구성과 마찬가지로 추가 라우트 정의가 필요없으며 하나의 네트워크에 있는 호스트와 다른 네트워크에 있는 호스트 사이의 연결은 자동으로 이루어집니다. 이 구성의 장점은 두 네트워크 중 어느 하나만 활동하는 경우에도 임의의 iSeries 서버에 도달할 수 있는 경로가 존재한다는 점입니다.



가상 OptiConnect 및 논리 파티션을 사용한 라우팅

논리 파티션을 사용하여 하나의 iSeries 서버가 복수의 가상 기계로 논리적으로 파티션됩니다. 가상 OptiConnect TCP/IP 인터페이스는 파티션 간 통신 경로로 사용됩니다. 각 파티션에는 고유한 주소 공간과 고유한 TCP/IP 인스턴스가 있으며 고유한 전용 I/O 어댑터를 가질 수 있습니다. TCP/IP의 관점에서는 각 파티션이 독립된

iSeries 서버로 보입니다. 서로 다른 파티션 간의 TCP/IP 통신은 가상 OptiConnect 버스를 사용하여 이루어집니다. TCP/IP 라우팅 코드는 실제 OptiConnect 버스로 연결시킨 또 다른 시스템에 대한 경로와 다르지 않은 또 하나의 파티션에 대한 경로를 사용합니다.



구획	인터페이스	라인	서브넷 마스크	MTU	
D	10.6.7.244	*OPC	255.255.255.240	4096	
C	10.6.7.243	*OPC	255.255.255.240	4096	
B	10.6.7.242	*OPC	255.255.255.240	4096	
A	10.6.7.241	*OPC	255.255.255.240	4096	(연관된 로컬
A	10.6.7.3	TRNLINE	255.255.255.0	4096	인터페이스 = 10.6.7.3)

RZAJW515-0

이 예에는 하나의 LAN 어댑터만 시스템에 설치되어 있습니다. 이 어댑터는 파티션 A에 할당되어 있습니다. LAN에 있는 클라이언트들은 시스템에 정의된 다른 파티션과 통신해야 합니다. 이를 위해서 가상 OptiConnect 버스에 투명한 서브네트를 정의합니다. LAN에는 네트워크 주소 10.6.7.x가 있습니다. 추가 파티션을 계획할 경우 IP 주소가 필요합니다. 12개의 주소를 확보하기 위해서는 255.255.255.240의 서브네트 마스크를 사용해야 합니다. 이로 인해 10.6.7.241에서 10.6.7.254까지 총 14개의 사용할 수 있는 주소를 확보할 수 있습니다. 이 주소를 LAN에서 이미 사용하고 있지는 않은지 확인하십시오. 주소를 확보했으면 각 파티션마다 주소를 할당하십시오. 각 파티션에 인터페이스를 추가하고 가상 OptiConnect 버스에 그 주소를 정의하십시오.

투명한 서브네트화는 다음 사항이 참일 때 자동으로 작동 가능하게 됩니다. 첫째, 가상 OptiConnect 버스가 실제 LAN 인터페이스의 MTU 크기보다 작거나 같습니다. 두 번째, OptiConnect 버스 서브네트가 LAN 네트워크 주소의 서브네트입니다. 두 가지 사항이 모두 참이면 투명한 서브네트화가 자동으로 작동 가능하게 됩니다. 인터페이스 10.6.7.3은 파티션에 정의된 모든 인터페이스에 대해 프록시를 수행합니다. 이것은 LAN에 있는 클라이언트들을 파티션과 연결시킬 수 있게 해 줍니다.

TCP/IP 로드 균형 조절 방법

로드 균형 조절은 복수 프로세서, 복수 인터페이스 어댑터, 복수 호스트 서버에 걸쳐서 대량으로 액세스되는 기계의 네트워크 통신량과 로드를 재분배하는 것입니다. iSeries 서버에서 최고의 성능을 얻으려면 서버의 여러 부분에 통신 로드를 분산시켜야 합니다.

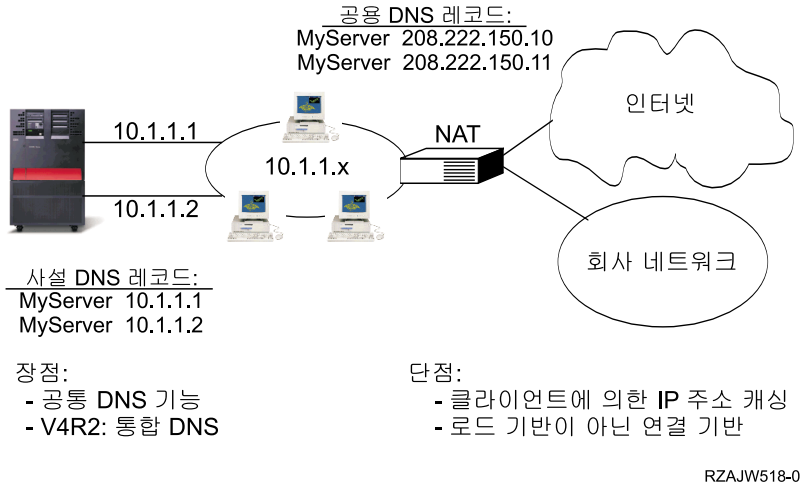
iSeries 서버의 로드를 조절하기 위해 여러 가지 다양한 TCP/IP 라우팅 메소드를 사용할 수 있습니다.

- DNS 기반의 로드 균형 조절
  인바운드 로드에 대해 DNS 기반의 로드 균형 조절을 사용할 수 있습니다. 로컬 클라이언트에 로드 균형 조절이 필요하면 DNS 로드 균형 조절을 사용해야 합니다.
- 중복 라우트 기반의 로드 균형 조절
  여기에서 복수 인터페이스에 걸쳐서 이루어지는 아웃바운드 로드 균형 조절에 대해 배울 수 있습니다. 이것은 DNS 기반의 로드 균형 조절보다 더 많은 융통성을 제공하되 로컬 클라이언트에 대해서는 활동하지 않는 연결 기반의 솔루션입니다.
- 가상 IP를 사용한 로드 균형 조절
  이 솔루션을 위해서는 사용자에게 IBM eNetwork Dispatcher와 같은 외부 로드 균형 조절 기계가 있어야 합니다. 가상 IP 주소를 사용하면 특정 인터페이스가 아닌 시스템에 주소를 할당할 수 있습니다. 여러 서버에 같은 주소를 정의할 수 있으므로 로드 균형 조절을 위한 많은 새로운 옵션들을 사용할 수 있습니다.

DNS 기반의 로드 균형 조절

DNS 기반의 로드 균형 조절은 인바운드 로드 균형 조절에 사용됩니다. 단일 호스트 서버명에 대해 여러 개의 복수 호스트 IP 주소가 구성됩니다. DNS는 리턴되는 호스트 IP 주소를 후속 클라이언트 호스트명 분석 요구로 대체합니다. 이와 같은 로드 균형 조절 유형의 장점은 이것이 공통 DNS 기능이라는 점입니다. 이 솔루션의 단점은 IP 주소가 클라이언트에 의해 캐시될 수 있으며 로드 기반의 솔루션이 아닌 연결 기반의 솔루션이라는 점입니다.

로드 균형 조절을 위한 첫 번째 방법은 DNS 기능을 사용하여 같은 시스템명에 대해 여러 개의 주소를 전달하는 것입니다. DNS는 사용하는 시스템명을 위한 주소 레코드에 대해 요구가 있을 때마다 다른 IP 주소를 제공합니다. 아래 예에서 각 주소는 서로 다른 시스템과 대응합니다. 이것은 사용자가 서로 분리되어 있는 두 대의 시스템에 걸쳐서 로드 균형 조절을 제공할 수 있게 해 줍니다. 사설망의 클라이언트에서는 클라이언트들이 각 요구에 대해 서로 다른 주소를 수신합니다. 이것이 공통 DNS 기능입니다. 공용 DNS 또한 두 개의 주소 항목을 갖는다는 점에 유의하십시오. 이 주소들은 정적 NAT를 사용하여 변환되므로 사용자가 인터넷상에 있으면 두 시스템에 도달할 수 있습니다.



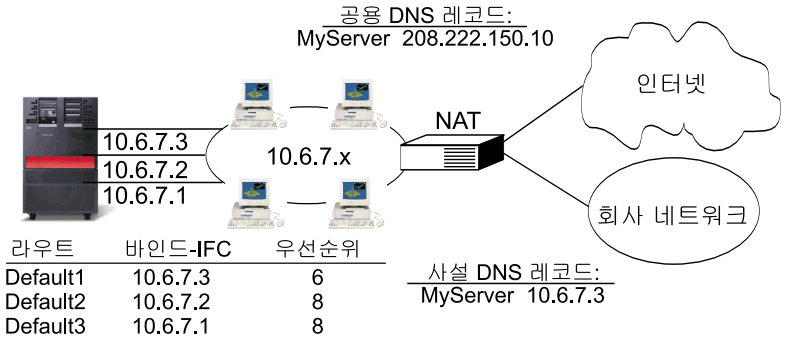
사용자 프로그램이 특정 시스템에 도달하거나 초기 연결 후에 같은 시스템으로 리턴하는 것에 달려 있으면 첫 번째 연결이 이루어진 후 다른 시스템명을 송신하도록 웹 페이지와 사이트를 코딩해야 합니다. MyServer1 208.222.150.10과 MyServer2 208.222.150.11에 대해서 DNS 항목을 더 추가할 수 있습니다. 이 경우, 한 예로 첫 번째 연결이 이루어지고 나면 웹 사이트가 MyServer2를 가리킬 수 있습니다. 이와 같은 유형의 로드 균형 조절은 연결 요구별 균형 조절을 제공합니다. 대부분의 경우 주소를 일단 분석했으면 클라이언트가 주소를 캐시하여 다시 요청하지 않습니다. 이와 같은 유형의 로드 균형 조절은 각 시스템으로 가는 통신량을 고려하지 않습니다. 이와 같은 유형의 로드 균형 조절은 인바운드 통신량만 고려하며 두 시스템에 하나의 어댑터를 가지는 것이 아니라 한 시스템에 두 개의 어댑터를 가질 수 있다는 점에 유의하십시오.

중복 라우트 기반의 로드 균형 조절

여러 인터페이스간의 아웃바운드 로드 균형 조절을 위해 중복 라우트 기반의 로드 균형 조절을 사용할 수 있습니다. 이것은 DNS 기반의 로드 균형 조절에 비해 더 많은 융통성을 갖고 있지만 로컬 클라이언트에 대해서는 활동하지 않는 연결 기반의 솔루션입니다. 이와 같은 유형의 로드 균형 조절을 사용할 때의 장점은 이것이

전반적인 iSeries 서버 솔루션이라는 것과 DNS에 비해 더 많은 융통성을 가지며 HTTP나 Telnet과 같이 대부분의 통신이 아웃바운드인 어플리케이션에 적합하다는 점입니다. 단점은 로컬 클라이언트에 대해서는 활동하지 않는 연결 기반의 솔루션이며(로드 기반의 솔루션이 아님) 인바운드 요구에는 유효하지 않다는 점입니다.

아래 예에서는 사용 중인 시스템의 세 어댑터가 모두 같은 LAN 세그먼트에 연결되어 있습니다. 어댑터 중 하나를 인바운드 회선 전용으로 설정하고 나머지 두 어댑터를 아웃바운드로 설정합니다. 로컬 클라이언트는 이전과 같은 방법으로 계속 작업합니다. 다시 말해서, 아웃바운드 인터페이스는 인바운드 인터페이스와 같다고 할 수 있습니다. 로컬 클라이언트는 시스템에 도달하기 위해 라우터가 필요 없는 시스템이라는 점을 기억하십시오. 라우터 대신에 스위치를 사용하면 로컬 클라이언트가 매우 큰 네트워크가 될 수 있습니다.



중복, 간접 라우트, 우선순위 **>(5)**의 경우 라우트 우선순위에 따라 라우트 로빈 방식으로 선택

장점:
- 총체적 AS/400 솔루션
- DNS보다 유연성이 큼
- HTTP, Telnet에 적합

단점:
- 로드 기반이 아닌 연결 기반
- 로컬 클라이언트에는 활성화 되지 않음
- 인바운드 요구에는 유효하지 않음

RZAJW511-0

구성 방법

TCP/IP 라우트 추가 명령행과 iSeries Navigator 인터페이스에 이것을 구성할 수 있습니다. 하나를 중복 라우트 우선순위라고 부르고 다른 하나를 우선 바인딩 인터페이스라고 부릅니다. 중복 라우트 우선순위 값을 디폴트 값인 5 그대로 사용하면 아무 일도 발생하지 않습니다. 5보다 큰 값을 설정하면 동일한 우선순위의 연결 간에 각 연결을 분산시킵니다. 우선 바인딩 인터페이스는 시스템이 알고 있는 첫 번째 IP 주소가 아닌 다른 IP 주소가 라우터를 특정 인터페이스에 바인드시킬 때 사용합니다.

위의 예에는 중복 라우트 우선순위가 6인 "인바운드" 어댑터(10.6.7.3)가 나옵니다. 다른 두 개의 어댑터에는 중복 우선순위가 8로 구성되어 있습니다. 한 어댑터의 중복 라우트 우선순위가 6이므로 모든 단일 라우트 우선순위가 8인 인터페이스가 다운되지 않는 한 아웃바운드 연결에 선택되지 않습니다.

모든 아웃바운드 인터페이스를 같은 우선순위에 넣어야 합니다. 일부를 한 값에 넣고 나머지를 다른 값에 넣으면 가장 높은 인터페이스 값만 사용됩니다.

DNS는 10.6.7.3 인터페이스를 가리키며 그 인터페이스를 인바운드 인터페이스로 만든다는 점을 유의하십시오. 중복 라우트 우선순위를 사용하지 않더라도 우선 바인딩 인터페이스 매개변수를 사용하여 항상 각 인터페이스에 있는 시스템으로부터 디폴트 라우트를 정의해야 합니다.

가상 IP 및 프록시 ARP를 사용한 어댑터 실패 시 전환

상황

사용자의 iSeries는 리모트와 LAN 클라이언트로부터 받은 데이터 항목을 처리합니다. 여기에는 회사의 중요한 어플리케이션도 들어 있습니다. 회사가 성장함에 따라 iSeries 및 네트워크에 대한 요구도 늘어났습니다. 이러한 성장으로 인해 예고없이 다운되는 경우가 발생하지 않고 네트워크에서 iSeries를 사용할 수 있도록 하는 것이 매우 중요해졌습니다. 어떤 이유에서든 네트워크 어댑터를 사용할 수 없는 경우, iSeries의 다른 네트워크 어댑터가 이를 대신하여 네트워크 클라이언트가 어떠한 장애도 알지 못하도록 해야 합니다.

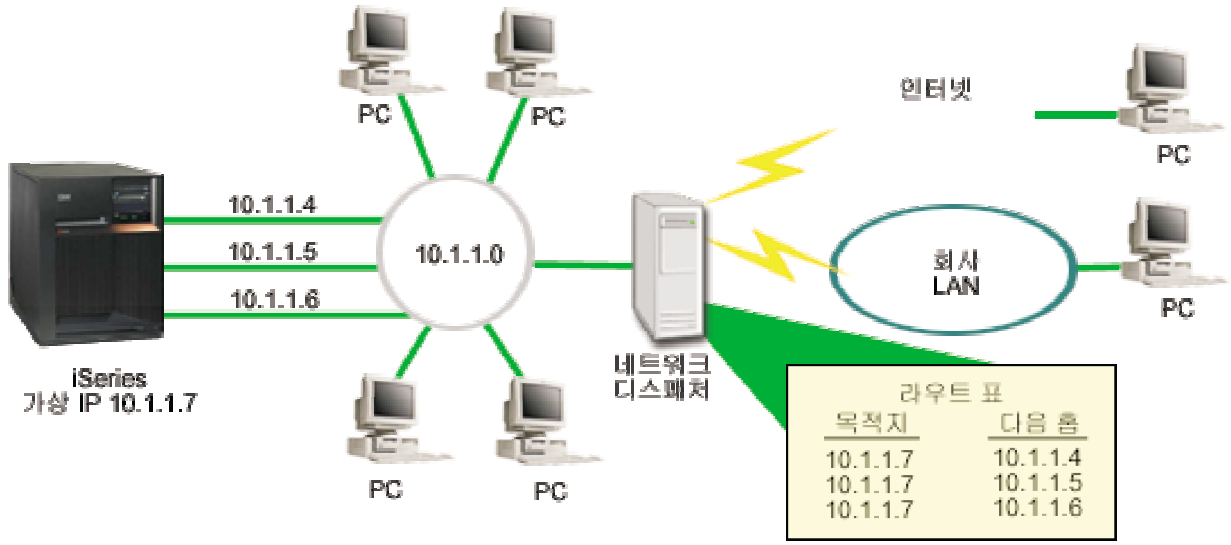
목적

가용성의 개념에는 실패한 구성요소에 대한 중복 및 백업이라는 여러 다른 측면이 포함됩니다. 이 시나리오에서 목표는 어댑터에 장애가 발생한 경우 iSeries에 대한 네트워크 가용성을 제공하는 것입니다.

세부사항

위 시나리오를 처리하는 한 가지 방법은 iSeries에서 LAN으로 실제 여러 개의 접속을 설정하는 것입니다. 다음 그림을 살펴 보십시오.

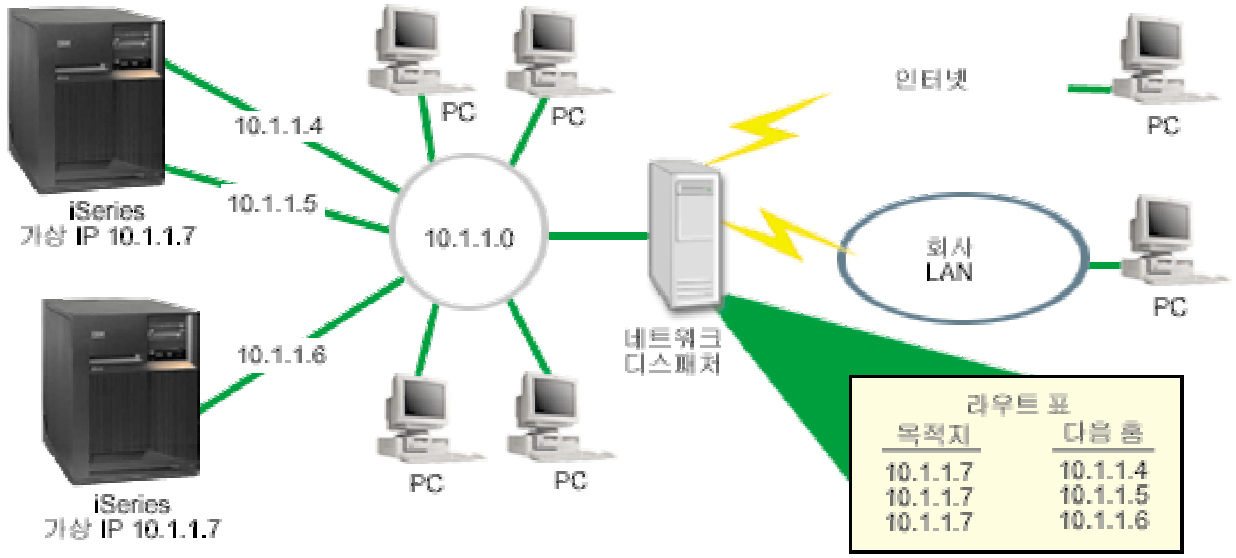
그림 1. 로컬 클라이언트가 없는 어댑터 실패 시 전환



각각의 실제 접속에는 서로 다른 IP 주소가 있습니다. 그리고 나서 시스템에 가상 IP 주소를 지정할 수 있습니다. 이 가상 IP 주소로 클라이언트는 시스템을 인식합니다. 모든 리모트 클라이언트(실제 iSeries와 같은 LAN에 접속되어 있지 않은 클라이언트)는 네트워크 디스패처와 같은 외부 로드 균형 조절 서버를 통해 iSeries와 통신합니다. 리모트 클라이언트로부터 수신한 IP 요구가 네트워크 디스패처를 통해 들어갈 때 네트워크 디스패처는 가상 IP 주소를 iSeries의 네트워크 어댑터 중 하나로 라우트합니다.

iSeries가 연결되어 있는 LAN에 클라이언트가 있는 경우 이 클라이언트는 이 네트워크 디스패처를 사용하여 로컬로 바인드시킨 통신의 방향을 지정하지 않는데, 이는 네트워크 디스패처에 필요 이상의 과부하가 발생하기 때문입니다. 네트워크 디스패처의 라우트 테이블과 유사한 라우트 항목을 각 클라이언트에 작성할 수도 있었지만, 클라이언트의 수가 많다면 이것은 실제로 그리 유용하지 않은 방법입니다. 이 상황은 다음 표에서 설명됩니다.

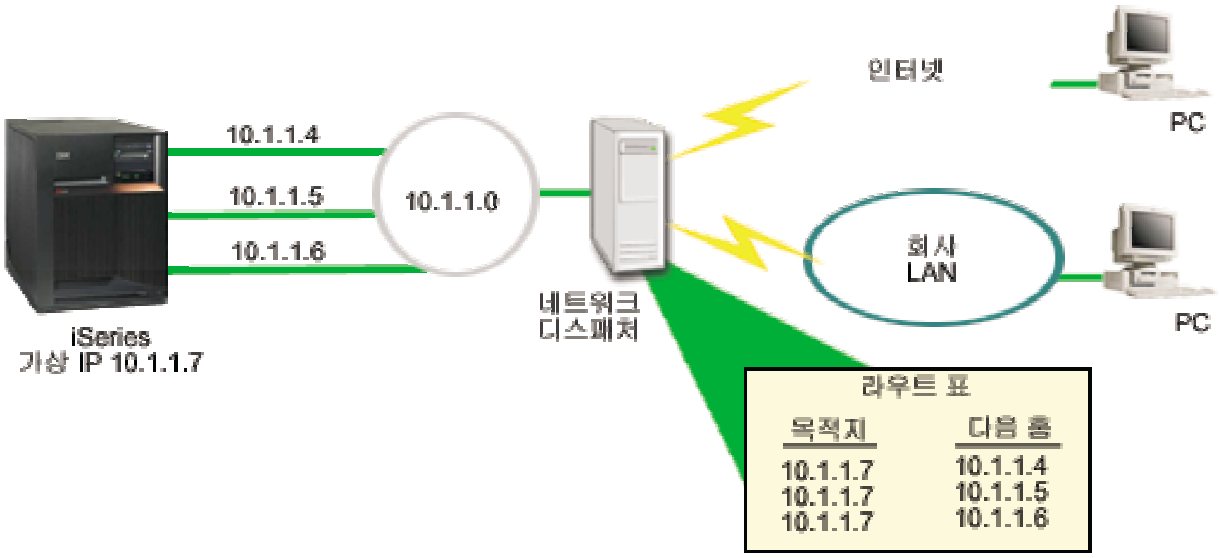
그림 2. 로컬 클라이언트가 있는 어댑터 실패 시 전환



OS/400 V5R2부터는 로컬 클라이언트(iSeries와 같은 LAN에 접속되어 있는 클라이언트)가 ARP를 통해 iSeries 가상 IP 주소에 연결될 수 있습니다. 이를 통해 로컬 클라이언트가 어댑터 실패 시 전환 솔루션도 가질 수 있습니다.

이 솔루션에서는 서로 지원하기 위한 두 개 이상의 iSeries 서버가 있을 수 있습니다. iSeries 시스템 중 어느 하나를 사용할 수 없게 되면 두 번째 시스템이 실패 시 전환 시스템으로 작동할 수 있습니다. 다음 그림에서는 두 개의 iSeries 서버를 사용한 동일한 설정을 보여줍니다.

그림 3. 복수의 iSeries 및 로컬 클라이언트가 있는 어댑터 실패 시 전환



패킷 라우팅은 단일 iSeries 및 리모트 클라이언트의 라우팅과 동일합니다. 그러나 로컬 클라이언트의 경우 차이가 있습니다. 동일한 가상 IP 주소를 사용하는 여러 iSeries를 가지고 있는 경우 iSeries 중 하나에 대해서만 프록시할 수 있습니다. 이 경우 프록시로 작동하는 두 개의 LAN 연결을 갖는 iSeries를 갖게 됩니다.

구성 단계

가상 IP 및 프록시 arp를 사용하는 로드 균형 조절 구성은 표준 TCP/IP 구성과 매우 유사하며 여기에 가상 TCP/IP 인터페이스를 추가합니다. 위의 로컬 클라이언트가 있는 어댑터 실패 시 전환(26 페이지 참조)의 경우 일반 구성 단계는 다음과 같습니다.

1. **가상 TCP/IP 인터페이스를 구성하십시오.**

   iSeries Navigator를 사용하여 가상 TCP/IP 인터페이스를 작성하십시오. 새로운 가상 IP 인터페이스 마법사를 **네트워크** -> **TCP/IP 구성** -> **IPv4** -> **인터페이스**에서 찾을 수 있습니다. 그러면 오른쪽 마우스 버튼으로 **인터페이스**를 클릭하고 **새 인터페이스** -> **가상 IP**를 선택하십시오.

   이 예에서는 서브네트 마스크가 255.255.255.255인 IP 주소 10.1.1.7을 입력합니다. 가상 인터페이스를 작성했으면 그 인터페이스를 오른쪽 마우스 버튼으로 클릭하고 **등록 정보**를 선택하십시오. **고급** 탭을 클릭하고 **프록시 ARP 작동** 선택란을 체크하십시오.

2. **모든 실제 LAN 연결에 대하여 TCP/IP 인터페이스를 작성하십시오.**

   TCP/IP 인터페이스 작성 마법사를 사용하여 TCP/IP 인터페이스를 작성하십시오. 마법사는 iSeries Navigator에 있으며 **네트워크** -> **TCP/IP 구성** -> **IPv4** -> **인터페이스**에서 찾을 수 있습니다. 그런 다음 오른쪽 **인터페이스**를 클릭하고 **새 인터페이스** -> **근거리 통신망(LAN)**을 선택하십시오. 각 LAN 연결에 대한 마법사를 완료하십시오.

이 예에서는 서브네트 마스크가 255.255.255.0인 IP 주소 10.1.1.4, 10.1.1.5 및 10.1.1.6을 입력하여 마법사를 세 번 실행시킵니다. 각 인터페이스를 완료한 후 해당 인터페이스를 오른쪽 마우스 버튼으로 클릭하고 **등록 정보**를 선택하십시오. **고급** 탭에서 해당 인터페이스를 1단계에서 작성한 가상 IP 인터페이스와 연관시키십시오. **연관된 로컬 인터페이스** 선택 상자를 사용하여 인터페이스를 연관시킬 수 있습니다.

TCP/IP 라우팅 및 로드 균형 조절에 관한 기타 정보

DNS는 TCP/IP 네트워크에서 인터넷 프로토콜(IP) 주소와 연관된 호스트명을 관리하기 위한 첨단 시스템입니다. 여기에서는 DNS를 구성하고 관리하기 위해 알아야 할 기본 개념과 프로시듀어를 설명합니다.

논리 파티션은 추가 백그라운드 정보와 세부사항을 제공합니다.

NAT 및 IP 필터 관리는 필터 규칙을 관리할 때 참조할 수 있습니다. 일부 기능에는 주석 추가, 편집 및 보기가 포함되어 있습니다.

OptiConnect

에서는 OptiConnect 라우팅에 대한 정보를 제공합니다. 이것은 *OptiConnect for OS/400 V4R4*라고 하는 iSeries 서버 온라인 책입니다.

지점 간 프로토콜은 일반적으로 컴퓨터를 인터넷에 연결할 때 사용됩니다. PPP는 인터넷 표준으로서 인터넷 서비스 제공자(ISP) 사이에서 가장 광범위하게 사용되는 연결 프로토콜입니다.

Printed in U.S.A