Oracle® Solaris 11.2의 네트워크 배치 계획

부품 번호: E53782
2014년 7월

ORACLE®

목차

이 설명서 사용

- **개요** - IPv4 및 IPv6 네트워크 배치 계획을 지원하는 기본 항목과 작업이 포함되어 있습니다.
- **대상** - 시스템 관리자
- **필요한 지식** - 네트워크 관리 개념 및 방법의 기본 사항 파악

제품 설명서 라이브러리

이 제품에 대한 최신 정보 및 알려진 문제는 설명서 라이브러리(http://www.oracle.com/pls/topic/lookup?ctx=E56343)에서 확인할 수 있습니다.

Oracle 지원 액세스

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

피드백

http://www.oracle.com/goto/docfeedback에서 이 설명서에 대한 피드백을 보낼 수 있습니다.

♦ ♦ ♦ 1 장

1 네트워크 배치 계획

이 장에서는 TCP/IP 네트워크의 배치를 계획할 때 고려해야 할 몇 가지 사항에 대해 설명합니다. 설명하는 계획 작업은 체계적이고 비용 효과적인 방식으로 네트워크를 배치하는 데 도움이 될 수 있습니다. 네트워크 계획에 대한 자세한 내용은 본 설명서에서 다루지 않습니다. 여기서는 일반적인 지침만 제공합니다. 또한 본 설명서에서는 사용자가 기본적인 네트워킹 개념 및 용어를 알고 있다고 가정합니다.

Oracle Solaris에서 TCP/IP가 구현된 방식에 대한 설명과 이 릴리스의 네트워크 관리 개요는 "Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리 "의 1 장, "Oracle Solaris의 네트워크 관리 정보"를 참조하십시오.

사이트의 전체 네트워킹 체계 계획에 대한 자세한 내용은 "Oracle Solaris 11.2의 네트워크 관리 전략 "의 1 장, "Oracle Solaris 네트워크 관리 요약"에 설명된 네트워킹 전략을 참조하십시오.

이 장의 내용:

네트워크 하드웨어 결정

지원해야 할 시스템 수에 따라 네트워크 구성 방식이 달라집니다. 한 건물의 한 층에 수십 대의 독립형 시스템이 배치되는 작은 규모의 네트워크가 조직에 필요할 수도 있고, 또는 여러 건물에 1,000대 이상의 시스템이 배치되는 네트워크를 설정해야 할 수도 있습니다. 이 설정에 따라 서브넷이라는 세분화로 네트워크를 추가로 구분해야 할 수 있습니다.

하드웨어에 대해 결정해야 할 몇 가지 계획 요소는 다음과 같습니다.

- 네트워크 토폴로지, 레이아웃 및 네트워크 하드웨어 연결

- 서버에 필요한 가상 시스템을 포함하여 네트워크가 지원할 수 있는 호스트 시스템 유형 및 개수
- 이러한 시스템에 설치할 네트워크 장치
- 사용할 네트워크 매체의 유형(예: 이더넷 등)
- 브리지, 라우터 및 방화벽을 사용하여 네트워크 매체를 확장하거나 로컬 네트워크를 외부 네트워크에 연결

  브리지 작동 방식에 대한 자세한 내용은 "Oracle Solaris 11.2의 네트워크 데이터 링크 관리 "의 "브리지된 네트워크 개요"를 참조하십시오.

  라우터 작동 방법에 대한 설명은 "네트워크의 라우터 계획" [12]을 참조하십시오.

  방화벽에 대한 자세한 내용은 "Oracle Solaris 11.2의 네트워크 보안 "의 4 장, "Oracle Solaris의 IP 필터 정보"를 참조하십시오.

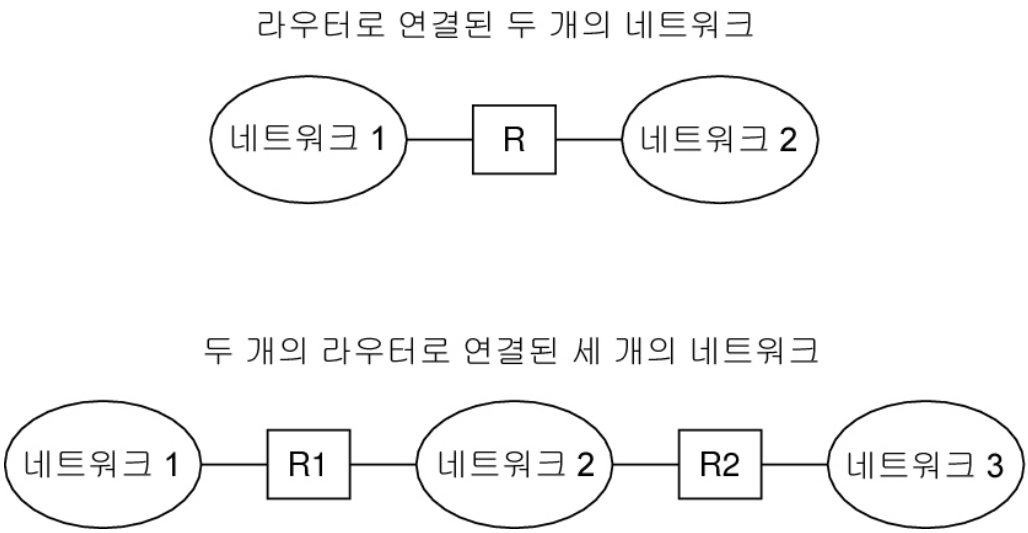
네트워크 토폴로지 개요

네트워크 토폴로지는 네트워크의 연결 방식을 기술합니다. 라우터는 네트워크를 서로 연결해주는 엔티티입니다. 라우터는 두 개 이상의 네트워크 인터페이스를 포함하고 IP 전달을 구현하는 시스템입니다. 하지만 시스템은 "Oracle Solaris 11.2 시스템을 라우터 또는 로드 밸런서로 구성 "의 2 장, "시스템을 라우터로 구성"의 설명에 따라 제대로 구성되기 전까지 라우터로 작동할 수 없습니다.

라우터는 두 개 이상의 네트워크를 연결하여 보다 큰 인터네트워크를 형성합니다. 두 개의 인접한 네트워크 간에 패킷을 전달하도록 라우터를 구성해야 합니다. 또한 라우터는 인접한 네트워크에 연결된 다른 라우터에 전달하여 인접한 네트워크 외부에 있는 네트워크에 패킷을 전달할 수 있어야 합니다.

다음 그림에서는 네트워크 토폴로지의 기본 요소를 보여줍니다. 그림의 위쪽 부분은 단일 라우터로 연결된 네트워크 2개의 간단한 구성을 보여 줍니다. 그림의 아래쪽 부분은 라우터 2개로 연결된 네트워크 3개의 구성을 보여 줍니다. 첫번째 예제에서 라우터 R은 네트워크 1 및 네트워크 2를 보다 큰 인터네트워크로 결합합니다. 두번째 예제에서 라우터 R1은 네트워크 1과 2를 연결합니다. 라우터 R2는 네트워크 2와 3을 연결합니다. 이러한 연결로 네트워크 1, 2, 3이 포함된 네트워크가 형성됩니다.

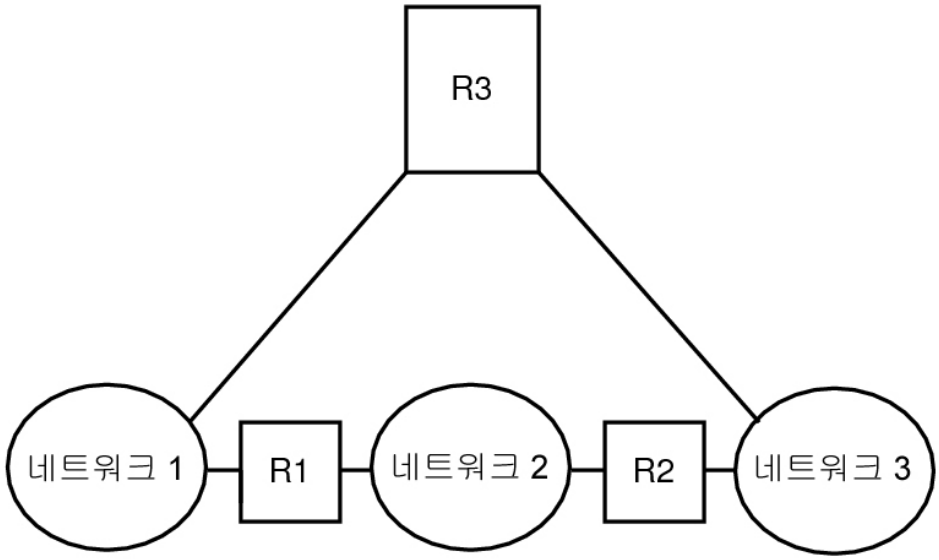
그림 1-1 기본 네트워크 토폴로지



네트워크를 인터네트워크로 연결하는 것 외에도 라우터는 대상 네트워크의 주소에 따라 네트워크 사이에 패킷 경로를 지정합니다. 인터네트워크가 점점 더 복잡해짐에 따라 각 라우터는 패킷 대상에 대해 더 많은 항목을 결정해야 합니다.

다음 그림은 보다 복잡한 경우를 보여 줍니다. 라우터 R3은 네트워크 1과 3을 연결합니다. 중복성은 신뢰성을 향상해 줍니다. 네트워크 2가 작동 중지되면 라우터 R3이 네트워크 1과 3 사이의 경로를 제공할 수 있습니다. 여러 네트워크를 상호 연결시킬 수 있습니다. 하지만 네트워크는 동일한 네트워크 토폴로지를 사용해야 합니다.

그림 1-2 네트워크 사이에 추가 경로를 제공하는 네트워크 토폴로지



라우터는 “네트워크의 라우터 계획” [12]에서 자세히 설명합니다.

네트워크에서 서브넷 사용

서브넷 사용은 크기 및 제어 문제를 해결하기 위해 관리 세분화를 사용해야 하는 것과 관련이 있습니다. 네트워크에 있는 호스트 및 서버가 많을수록 관리 작업이 복잡해집니다. 관리 세분화를 만들고 서브넷을 사용하면 복잡한 네트워크 관리가 더 쉬워집니다.

네트워크에 대한 관리 세분화를 설정하는 것은 다음 요소에 따라 결정됩니다.

- **네트워크 크기**

  서브넷은 광대한 지역에 세분화가 배치된 비교적 작은 네트워크에서도 유용합니다.
- **사용자 그룹의 공통 요구 사항**

  예를 들어, 한 건물에 국한되며 비교적 적은 수의 시스템을 지원하는 네트워크가 있을 수 있습니다. 이러한 시스템은 여러 하위 네트워크로 구분됩니다. 각 하위 네트워크는 요구

사항이 다른 사용자 그룹을 지원합니다. 이 예에서는 각 서브넷에 대해 관리 세분화를 사용할 수 있습니다.

- **보안**

  핵심 서버, 데스크탑 시스템 및 인터넷 연결 웹 서버를 개별 서브넷으로 분리하고 서브넷 사이에 방화벽을 설정하는 것이 좋습니다.

IPv4 자율 시스템 토폴로지

일반적으로 라우터와 네트워크가 여러 개인 사이트에서는 네트워크 토폴로지를 단일 경로 지정 도메인 또는 AS(자율 시스템)로 관리합니다. 그림 1-3. “IPv4 라우터가 여러 개인 자율 시스템”은 3개의 로컬 네트워크(`10.0.5.0`, `172.20.1.0` 및 `192.168.5.0`)로 구분된 AS를 보여 줍니다.

네트워크는 다음 유형의 시스템으로 구성됩니다.

- 라우터

  라우터는 경로 지정 프로토콜을 사용하여 네트워크 패킷이 소스에서 로컬 네트워크 내의 대상 또는 외부 네트워크로 지정되거나 경로 지정되는 방식을 관리합니다. Oracle Solaris에서 지원되는 경로 지정 프로토콜에 대한 자세한 내용과 라우터로 시스템을 구성하는 방법에 대한 지침은 “Oracle Solaris 11.2 시스템을 라우터 또는 로드 밸런서로 구성 ”의 “경로 지정 프로토콜”을 참조하십시오.

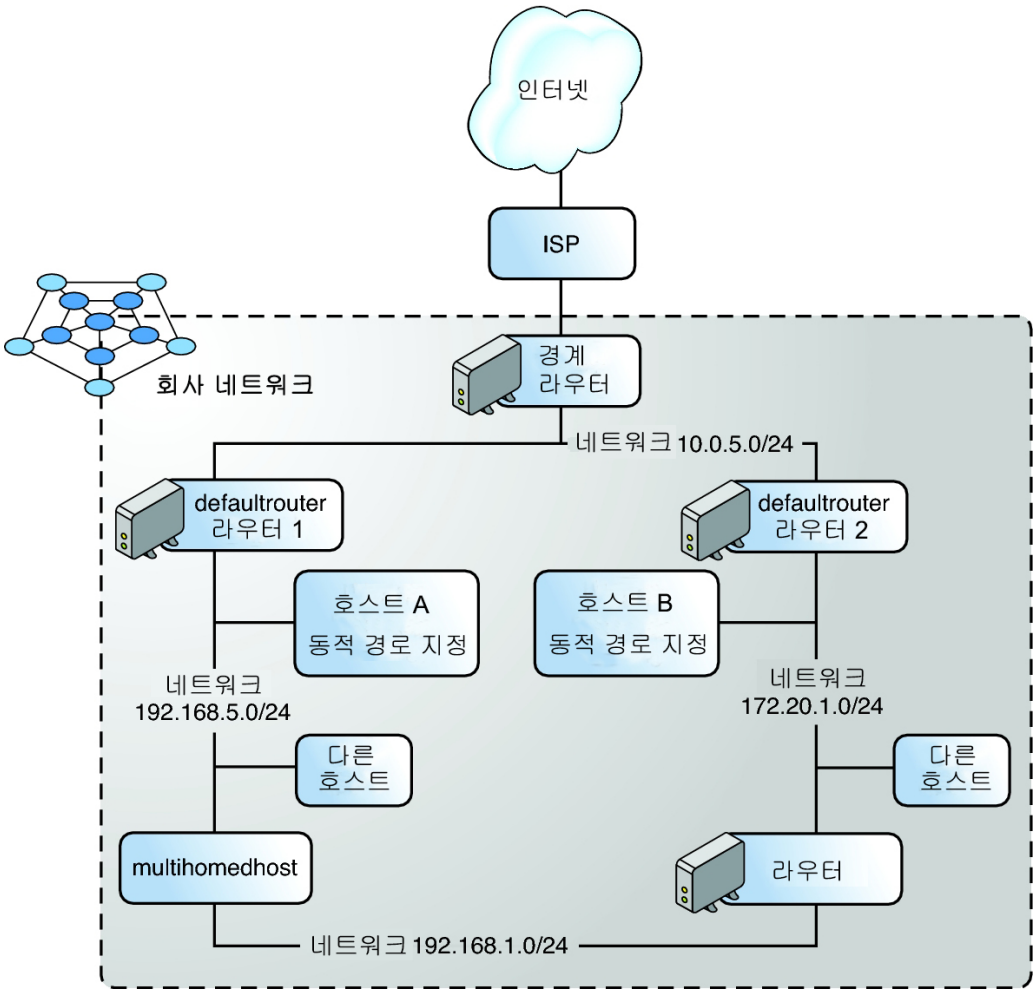
  라우터 유형에는 다음이 포함됩니다.

  - 경계 라우터 - 로컬 네트워크(예: `10.0.5.0`)를 외부 서비스 공급자에 연결합니다.
  - 기본 라우터 - 여러 로컬 네트워크를 자체적으로 포함할 수 있는 로컬 네트워크에서 패킷 경로 지정을 관리합니다. 예를 들어, 그림 1-3. “IPv4 라우터가 여러 개인 자율 시스템”에서 Router 1은 `192.168.5`에 대한 기본 라우터로 사용됩니다. 동시에 Router 1은 `10.0.5.0` 내부 네트워크에도 연결됩니다. Router 2의 인터페이스는 `10.0.5.0` 및 `172.20.1.0` 내부 네트워크에 연결됩니다.
  - 패킷 전달 라우터 - 내부 네트워크 간에 패킷을 전달하지만 경로 지정 프로토콜을 실행하지 않습니다. 그림 1-3. “IPv4 라우터가 여러 개인 자율 시스템”에서 Router 3은 `172.20.1` 및 `192.168.5` 네트워크에 연결된 패킷 전달 라우터입니다.
- 클라이언트 시스템
  - 멀티홈 시스템 또는 NIC가 여러 개인 시스템입니다. Oracle Solaris에서 이러한 시스템은 기본적으로 패킷을 동일한 네트워크 세그먼트 내의 다른 시스템에 전달할 수 있습니다.
  - 단일 인터페이스 시스템은 패킷 전달 및 수신 구성 정보에 로컬 라우터를 사용합니다.

작업과 관련된 자세한 내용은 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리 ”의 3 장, “Oracle Solaris에서 IP 인터페이스와 주소 구성 및 관리”를 참조하십시오.

추가 네트워크 구성 요소를 구성하는 경우 다음 그림을 참조로 사용하십시오.

그림 1-3 IPv4 라우터가 여러 개인 자율 시스템



네트워크의 라우터 계획

TCP/IP에서는 호스트 및 라우터라는 두 가지 유형의 엔티티가 네트워크에 존재합니다. 모든 네트워크에는 호스트가 있어야 하며, 라우터는 네트워크에 따라 필요합니다. 네트워크의 물리적 토폴로지에 따라 라우터가 필요한지 여부가 결정됩니다. 이 절에서는 네트워크 토폴로지 및 경로 지정의 개념에 대해 소개합니다. 이러한 개념은 기존 네트워크 환경에 다른 네트워크를 추가하려는 경우에 중요합니다.

참고 - IPv4 및 IPv6 네트워크의 라우터 구성에 대한 자세한 내용과 작업은 “Oracle Solaris 11.2 시스템을 라우터 또는 로드 밸런서로 구성 ”의 2 장, “시스템을 라우터로 구성”을 참조하십시오.

라우터가 패킷을 전송하는 방법

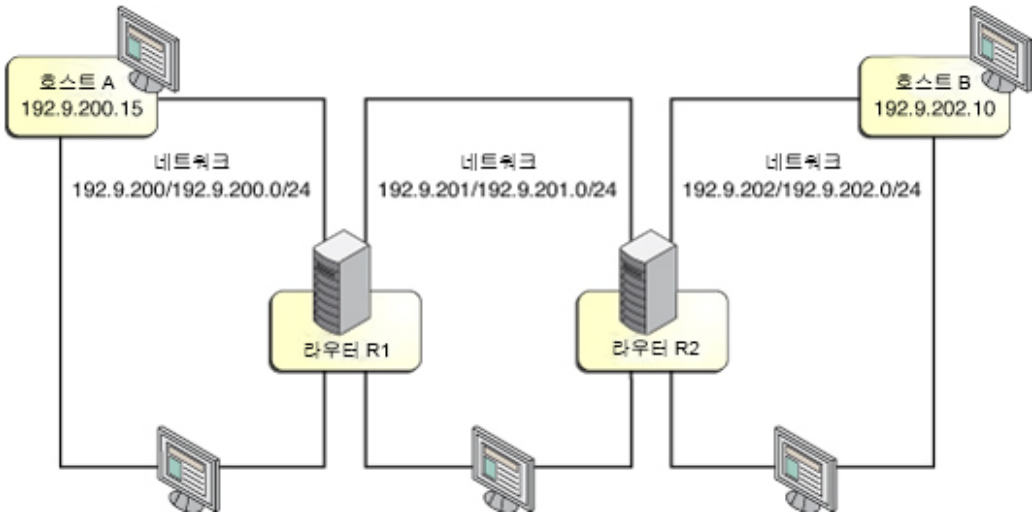
라우터는 다음과 같은 방식으로 패킷을 전송합니다.

- IP 네트워크의 모든 노드가 경로 지정 테이블에 경로 지정 정보를 유지 관리합니다. 이러한 테이블에는 로컬 및 원격 네트워크 둘 다에 연결된 시스템에 접근하는 방법에 대한 정보가 들어 있습니다. 경로 지정 테이블은 로컬 구성 정보 및 이웃 시스템과 교환되는 경로 지정 프로토콜 메시지에서 생성됩니다.
- 호스트 시스템은 패킷을 처음 보낼 때 경로 지정 테이블에서 패킷의 대상을 조회하여 대상이 로컬 네트워크에 있는지 확인합니다. 있을 경우 패킷이 해당 IP 주소를 가진 호스트로 직접 전달됩니다. 없을 경우 패킷이 로컬 네트워크의 라우터로 전달됩니다.
- 라우터가 패킷을 수신하면 경로 지정 테이블을 검사하여 대상 주소가 연결된 네트워크 중 하나의 시스템 주소인지 또는 다른 라우터를 통해 메시지를 전달해야 하는지 확인합니다. 그런 다음 대상 경로에서 다음 시스템으로 메시지를 전송합니다.
- 메시지가 대상 시스템에 도착할 때까지 메시지를 수신하는 각 라우터에서 이 프로세스가 반복됩니다.

“Oracle Solaris 11.2 시스템을 라우터 또는 로드 밸런서로 구성 ”의 2 장, “시스템을 라우터로 구성”을 참조하십시오.

다음 그림에서는 두 라우터로 연결된 세 네트워크의 네트워크 토폴로지를 보여줍니다.

그림 1-4 상호 연결된 세 네트워크의 네트워크 토폴로지



라우터 R1은 네트워크 192.9.200.0/24 및 192.9.201.0/24를 연결합니다. 라우터 R2는 네트워크 192.9.201.0/24 및 192.9.202.0/24를 연결합니다.

네트워크 192.9.200.0/24의 호스트 A가 네트워크 192.9.202의 호스트 B에 메시지를 전송하면 다음과 같은 이벤트가 발생합니다.

1. 호스트 A가 경로 지정 테이블에서 192.9.202.10 경로를 확인합니다. 로컬 네트워크 주소 범위에는 이 주소가 포함되지 않지만 이전에 학습된 라우터 R1을 통한 기본 경로에 이 주소가 포함됩니다. 따라서 호스트 A가 라우터 R1에 패킷을 전송합니다.
2. 라우터 R1은 해당 경로 지정 테이블을 검사합니다. 로컬 네트워크 주소 범위에는 대상 주소가 포함되지 않지만 라우터 R2를 통한 알려진 네트워크 192.9.202.0/24 경로에 이 주소가 포함되므로 라우터 R1이 라우터 R2에 패킷을 전송합니다.
3. 라우터 R2는 네트워크 192.9.202.0/24에 직접 연결되어 있습니다. 경로 지정 테이블 조회를 통해 192.9.202.10이 연결된 네트워크에 있는 것이 확인됩니다. 라우터 R2가 호스트 B에 직접 패킷을 전송합니다.

네트워크에 대한 IP 주소 지정 형식 결정

네트워크 주소 지정 체계를 계획할 때는 다음 요소를 고려하십시오.

- 사용할 IP 주소의 유형(IPv4 또는 IPv6)
- 네트워크의 잠재적 시스템 수

- 각각 개별 IP 주소와 함께 여러 NIC(네트워크 인터페이스 카드)를 필요로 하는 멀티홈 또는 라우터 시스템 수
- 네트워크에서 개인 주소를 사용할지 여부
- IP 주소 풀을 관리하는 DHCP 서버를 사용할지 여부

IPv4 주소

TCP/IP 네트워크에 사용되는 원래 주소 형식입니다. IPv4 주소는 32비트 길이입니다. IPv4 주소는 원래 연속 블록 16777216(클래스 A), 65536(클래스 B) 또는 256(클래스 C) 주소로 다양한 조직에 할당되었습니다. 주소 블록을 요청한 각 조직은 고정된 주소 접두어 및 암시적 접두어 마스크를 받았으며, 둘 다 점으로 구분된 10진수 표기법으로 지정되었습니다. 예를 들어, IANA(Internet Assigned Numbers Authority)는 클래스 A 주소 블록 `156.0.0.0` 넷마스크 `255.0.0.0`을 ARIN(American Registry for Internet Numbers)에 할당했습니다. 첫번째 바이트가 156인 모든 주소는 이 주소 블록 내에 있습니다. ARIN은 해당 클래스 A 블록에서 클래스 B 주소 블록 `156.151.0.0` 넷마스크 `255.255.0.0`을 Sun Microsystems(현재 Oracle)에 하위 할당했습니다.

이후에 IETF(Internet Engineering Task Force)는 IPv4 주소 부족 및 전역 인터넷 경로 지정 테이블의 제한적인 용량에 대한 임시 해결책으로 CIDR(*Classless Inter-Domain Routing*) 주소를 개발했습니다. CIDR 주소 할당은 조직의 요구 사항에 가장 적합한 비트 경계에 따라 세분화됩니다. 주소 블록은 점으로 구분된 10진수 IPv4 주소, 슬래시 및 주소 접두어 길이(비트)로 지정됩니다.

자세한 내용은 다음 자료를 참조하십시오.

- Internet Protocol DARPA Internet Program Protocol Specification (http://tools.ietf.org/html/rfc791)
- Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan (http://tools.ietf.org/html/rfc4632)

다음 표에서는 CIDR 표기법 및 점으로 구분된 10진수 형식 둘 다의 서브넷 길이 지정 예와 해당 접두어 길이의 네트워크에서 가능한 총 호스트 수를 제공합니다.

표 1-1 CIDR 접두어 및 이와 동등한 십진수

CIDR 네트워크 접두어 길이	해당 점으로 구분된 10진수 서브넷 마스크	사용 가능한 IP 주소
/19	255.255.224.0	8,192
/20	255.255.240.0	4,096
/21	255.255.248.0	2,048
/22	255.255.252.0	1,024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64

CIDR 네트워크 접두어 길이	해당 점으로 구분된 10진수 서브넷 마스크	사용 가능한 IP 주소
/27	255.255.255.224	32

개인 주소

IANA는 IPv4 주소 블록을 예약했습니다. 이러한 개인 주소는 개인 네트워크 내의 네트워크 트래픽에 사용되며, 인터넷 서비스 공급자로부터 IPv4 주소 블록을 요청하는 조직은 대체로 각 시스템에 고유한 주소를 사용할 만큼 충분한 할당을 받지 못합니다. 일반적으로 조직은 내부 네트워크의 시스템에 개인 주소를 지정합니다. 시스템은 NAT(Network Address Translator) 및 응용 프로그램 프록시 서버를 통해 인터넷의 다른 사이트와 통신하여 ISP(인터넷 서비스 공급자)가 제공한 주소를 효과적으로 공유할 수 있습니다.

다음 표에서는 IPv4 주소 범위와 해당 넷마스크를 나열합니다.

네트워크 접두어/길이	IPv4 주소 범위
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/125	172.16.0.0 - 172.31.255.25
192.168.0.0/16	192.168.0.0 - 192.168.255.255

DHCP 주소

DHCP(Dynamic Host Configuration Protocol) 프로토콜을 통해 시스템은 부트 프로세스의 일부로 DHCP 서버로부터 IP 주소 등의 구성 정보를 수신할 수 있습니다. DHCP 서버는 DHCP 클라이언트에 주소를 지정할 IP 주소 풀을 유지 관리합니다. DHCP를 사용하는 사이트는 클라이언트가 계속 연결되어 있지 않은 경우 각 클라이언트에 영구적 IP 주소를 지정할 때 필요한 IP 주소 수보다 작은 IP 주소 풀을 사용할 수 있습니다. 이 경우 클라이언트 간에 주소를 공유하여 필요한 총 IP 주소 수를 줄일 수 있습니다. 그러나 클라이언트 추가와 제거가 많지 않을 경우 궁극적으로 동일한 개수의 IP 주소가 필요합니다. DHCP 주소 사용 시의 보다 일반적인 이점은 구성 세부 사항으로 DHCP 서버를 설정하기 때문에 개별 호스트 구성을 많이 수행할 필요가 없다는 것입니다. 이 경우 호스트에 필요한 구성이 최소화되거나 수동 구성이 필요하지 않습니다. DHCP 서비스를 설정하여 사이트의 IP 주소 또는 주소 일부를 관리할 수 있습니다. 자세한 내용은 “Oracle Solaris 11.2의 DHCP 작업 ”을 참조하십시오.

IPv6 주소

이러한 128비트 IPv6 주소는 IPv4에서 사용할 수 있는 것보다 큰 주소 공간을 제공합니다. IPv6 주소는 16진수 4개로 구성된 그룹 8개로 제공되며, 각 그룹이 콜론으로 구분됩니다. 각 그룹의 선행 0을 표시하지 않을 수 있습니다. 0만 포함된 하나 이상의 연속 그룹은 다음 예와 같이 이중 콜론으로 대체할 수 있습니다.

```
2001:db8:2f32:27:214:4fff:fe4a:9926
```

CIDR 형식의 IPv4 주소와 마찬가지로 IPv6 주소는 클래스가 없으며, 다음 예와 같이 접두어를 사용하여 사이트의 네트워크를 정의하는 주소 일부를 지정합니다.

```
2001:db8:2f32::/48
```

IPv6 주소 지정에 대한 자세한 내용은 IP Version 6 Addressing Architecture (http://tools.ietf.org/html/rfc4291)를 참조하십시오.

설명서 접두어

IPv6 주소의 경우 접두어 `2001:db8::/32`는 설명서 예에서 특별히 사용되는 특수한 IPv6 접두어입니다. 본 설명서의 예에서는 개인 IPv4 주소와 예약된 IPv6 설명서 접두어를 사용합니다.

네트워크의 IP 번호 얻기

IPv4 네트워크는 IPv4 네트워크 번호와 네트워크 마스크(넷마스크)의 조합으로 정의됩니다. IPv6 네트워크는 사이트 접두어 및 서브넷 접두어(서브넷이 사용되는 경우)로 정의됩니다.

개인 네트워크가 인터넷의 외부 네트워크와 통신할 수 있도록 하려면 해당 조직으로부터 네트워크에 대해 등록된 IP 번호를 얻어야 합니다. 이 주소가 IPv4 주소 지정 체계에 대한 네트워크 번호 또는 IPv6 주소 지정 체계에 대한 사이트 접두어로 사용됩니다.

ISP는 다양한 서비스 레벨을 기반으로 하는 가격에 따라 네트워크에 대한 IP 주소를 제공합니다. 여러 ISP를 조사하여 네트워크에 가장 적합한 서비스를 제공하는 ISP를 결정하십시오. 일반적으로 ISP는 기업에 동적으로 할당되는 주소 또는 정적 IP 주소를 제공합니다. IPv4 주소와 IPv6 주소를 모두 제공하는 ISP도 있습니다.

사이트가 ISP인 경우 로케일에 적합한 인터넷 레지스트리(IR)로부터 고객의 IP 주소 블록을 얻습니다. 궁극적으로 IANA에서 등록된 IP 주소를 전 세계의 IR에 위임합니다. 각 IR에는 IR이 제공하는 로케일에 적합한 템플리트와 등록 정보가 있습니다. IANA 및 IR에 대한 자세한 내용은 IANA's IP Address Service 페이지 (http://www.iana.org/ipaddress/ip-addresses.htm)를 참조하십시오.

네트워크에서 이름 지정 엔티티 사용

TCP/IP 프로토콜은 IP 주소를 사용하여 네트워크에서 시스템을 찾습니다. 하지만 호스트 이름을 사용하면 IP 주소보다 간편하게 시스템을 식별할 수 있습니다.

TCP/IP 관점에서 네트워크는 일련의 이름이 지정된 엔티티입니다. 호스트는 이름이 있는 엔티티입니다. 라우터도 이름이 있는 엔티티이며, 네트워크도 이름이 있는 엔티티입니다. 네트

워크가 설치된 그룹 또는 부서가 사업부, 지역 또는 회사일 수 있으므로 해당 그룹 또는 부서에도 이름이 지정될 수 있습니다. 이론상 네트워크 식별에 사용될 수 있는 이름의 계층은 거의 제한이 없습니다.

도메인 이름

여러 네트워크는 호스트 및 라우터를 관리 도메인의 계층으로 구성합니다. NIS(Network Information Service) 또는 DNS(Domain Name System) 이름 지정 서비스를 사용 중인 경우 조직에 대해 전 세계에서 고유한 도메인 이름을 선택해야 합니다. 도메인 이름이 고유하게 하려면 *InterNIC*에 도메인 이름을 등록해야 합니다. 인터넷의 다른 사이트가 DNS를 통해 시스템을 찾을 수 있게 하려는 경우 고유한 도메인 이름이 필요합니다.

다른 도메인 아래에 있는 도메인 이름을 하위 도메인이라고도 합니다. 도메인 이름 구조는 계층 구조입니다. 일반적으로 새 도메인은 기존의 관련 도메인 아래에 배치됩니다. 예를 들어, 자회사의 도메인 이름은 모회사의 도메인 아래에 배치될 수 있습니다. 도메인 이름에 다른 관계가 없을 경우 조직에서는 기존의 최상위 레벨 도메인(예: `.com`, `.org`, `.edu`, `.gov` 등) 중 하나의 바로 아래에 도메인 이름을 배치할 수 있습니다.

이름 지정 서비스 및 디렉토리 서비스 선택

Oracle Solaris에서는 3가지 유형의 이름 지정 서비스(로컬 파일, NIS 및 DNS) 중에서 선택할 수 있습니다. 이름 지정 서비스는 네트워크의 시스템에 대한 중요한 정보(예: 호스트 이름, IP 주소 등)를 유지 관리합니다. 이름 지정 서비스와 함께, 또는 이름 지정 서비스 대신 LDAP 디렉토리 서비스를 사용할 수도 있습니다. LDAP은 분산 이름 지정과 기타 디렉토리 서비스를 위해 디렉토리 서버에 액세스하는 데 사용되는 보안 네트워크 프로토콜입니다. 이 표준 기반 프로토콜은 계층적 데이터베이스 구조를 지원합니다. 동일한 프로토콜을 사용하여 UNIX 및 다중 플랫폼 환경에서 이름 지정 서비스를 제공할 수 있습니다. Oracle Solaris의 이름 지정 서비스 소개는 "Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: DNS 및 NIS "의 1 장, "이름 지정 및 디렉토리 서비스 정보"를 참조하십시오.

네트워크 데이터베이스의 구성은 중요합니다. 따라서 네트워크 계획 프로세스의 일부로 사용할 이름 지정 또는 디렉토리 서비스를 결정해야 합니다. 또한 이름 지정 서비스 사용 결정에 따라 조직에서 네트워크를 관리 도메인으로 구성할지 여부가 달라집니다.

이름 지정 또는 디렉토리 서비스의 경우 다음 중에서 선택할 수 있습니다.

- NIS 또는 DNS - NIS 및 DNS 이름 지정 서비스는 네트워크의 여러 서버에서 네트워크 데이터베이스를 유지 관리합니다. "Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: DNS 및 NIS "에서는 이러한 이름 지정 서비스 및 데이터베이스 구성 방법을 설명합니다. 이름 공간 및 관리 도메인 개념에 대해서도 자세히 설명합니다.
- LDAP - 이름 지정 서비스와 함께, 또는 이름 지정 서비스 대신 LDAP 디렉토리 서비스를 사용할 수도 있습니다. LDAP은 분산 이름 지정과 기타 디렉토리 서비스를 위해 디렉토리 서버에 액세스하는 데 사용되는 보안 네트워크 프로토콜입니다.

- 로컬 파일 - NIS, DNS 또는 LDAP을 구현하지 않을 경우 네트워크는 로컬 파일을 사용하여 이름 지정 서비스를 제공합니다. “로컬 파일”이라는 용어는 네트워크 데이터베이스에 사용되는 `/etc` 디렉토리의 일련의 파일을 의미합니다. 본 설명서의 절차에서는 별도로 지정되지 않은 경우 로컬 파일을 이름 지정 서비스로 사용 중이라고 가정합니다.

참고 - 네트워크에 대한 이름 지정 서비스로 로컬 파일을 사용하기로 결정할 경우 나중에 다른 이름 지정 서비스를 설정할 수 있습니다.

호스트 이름 관리

네트워크를 구성할 시스템에 대한 이름 지정 체계를 계획합니다. 네트워크의 각 시스템에 기본 네트워크 인터페이스의 IP 주소에 해당하는 TCP/IP 호스트 이름이 있어야 합니다. 호스트 이름은 시스템의 하위 도메인 내에서 고유해야 합니다. 물리적 시스템과 마찬가지로 가상 시스템에도 고유한 IP 주소와 호스트 이름이 있어야 합니다.

시스템에는 다음이 포함될 수 있습니다.

- 시스템의 IP 주소에 매핑되는 여러 호스트 이름. 예를 들어, `systema.mycompany.com`은 `www.mycompany.com`으로 알려질 수도 있습니다.
- IPv4 및 IPv6 주소 둘 다에 사용되는 동일한 호스트 이름.
- 네트워크 번호 재지정을 지원하기 위해 일정 기간 동안 동일한 호스트 이름으로 구성되는 새 IP 주소 및 더 이상 사용되지 않는 이전 IP 주소.
- 각각 고유한 IP 주소와 호스트 이름을 가지며 서로 다른 서브넷에 있는 여러 네트워크 인터페이스.

네트워크를 계획할 때는 설정 프로세스 중 간편하게 액세스할 수 있도록 IP 주소 및 연관된 호스트 이름 목록을 만드십시오. 이 목록을 통해 모든 호스트 이름이 고유한지 확인할 수 있습니다.

참고 - 기본 인터페이스의 TCP/IP 호스트 이름은 `hostname` 명령으로 설정하는 시스템 호스트 이름과 다른 엔티티입니다. Oracle Solaris에서 필수는 아니지만 일반적으로 동일한 이름이 둘 다에 사용됩니다. 일부 네트워크 응용 프로그램은 이 규약에 종속됩니다. 자세한 내용은 `hostname(1)` 매뉴얼 페이지를 참조하십시오.

♦ ♦ ♦ 2 장

2 IPv6 주소 사용 계획

이 장에서는 1장. 네트워크 배치 계획의 내용을 보완하기 위해 네트워크에서 IPv6 주소를 사용하기로 결정할 경우 추가로 고려해야 할 사항에 대해 설명합니다.

IPv4 주소와 IPv6 주소를 모두 사용하도록 계획한 경우 현재 ISP가 두 주소 유형을 모두 지원하는지 확인합니다.

IPv6 개념에 대한 소개는 Internet Protocol, Version 6 (IPv6) Specification (http://www.ietf.org/rfc/rfc2460.txt)을 참조하십시오.

IPv6 구성 작업은 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리 ”의 “IPv6 인터페이스 구성”을 참조하십시오.

IPv6 네트워크 문제 해결에 대한 자세한 내용은 “Oracle Solaris 11.2의 네트워크 관리 문제 해결 ”의 “IPv6 배치 관련 문제 해결”을 참조하십시오.

이 장의 내용:

IPv6 계획 작업

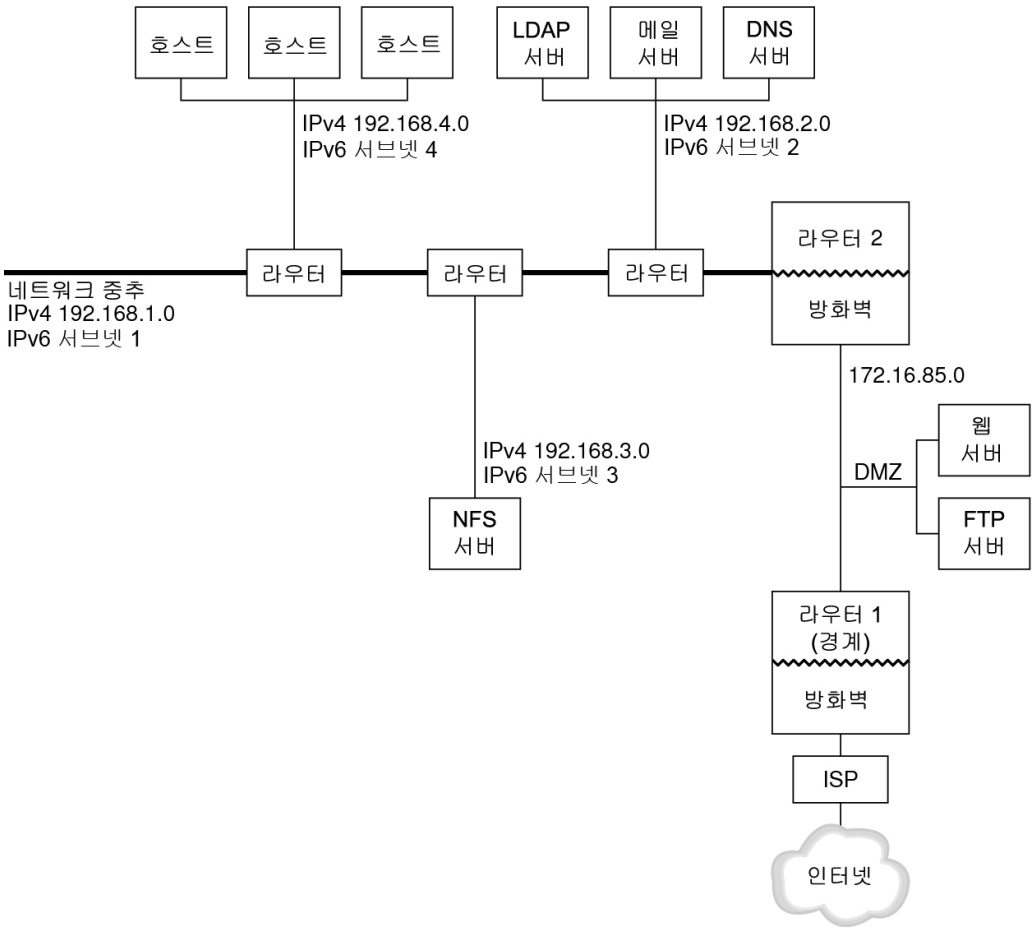
다음 표는 네트워크에서 IPv6을 구현하려고 계획한 경우 고려해야 할 사항에 대해 설명합니다. 기존 IPv4 네트워크에서 IPv6 네트워크로 마이그레이션하는 경우 추가 지침은 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리 ”의 “IPv4 네트워크에서 IPv6 네트워크로 마이그레이션”을 참조하십시오.

작업	설명	지침
IPv6을 지원하도록 하드웨어 준비	하드웨어를 IPv6으로 업그레이드할 수 있는지 확인합니다.	“IPv6에 대한 하드웨어 지원 확인” [24]
IPv6에서 응용 프로그램을 사용할 수 있는지 확인	IPv6 환경에서 응용 프로그램을 실행할 수 있는지 확인합니다.	“IPv6을 지원하도록 네트워크 서비스 구성” [26]
터널 사용 계획 설계	다른 서브넷 또는 외부 네트워크에 대한 터널을 실행할 라우터를 결정합니다.	“네트워크에서 터널 사용 계획” [28]
네트워크 보안을 설정하고 IPv6 보안 정책을 개발하는 방법 계획	보안을 위해 IPv6을 구성하기 전에 DMZ 및 해당 엔티티에 대한 주소 지정 계획이 필요합니다. 이 릴리스의 IP 필터, IP 보안 아키텍처(IPsec), IKE(Internet Key Exchange) 및 기타 보안 기능 사용과 같은 보안 구현 방식을 결정합니다.	“IPv6 구현에 대한 보안 고려 사항” [28] “Oracle Solaris 11.2의 네트워크 보안 ”
네트워크 시스템에 대한 주소 지정 계획 만들기	IPv6을 구성하기 전에 서버, 라우터 및 호스트에 대한 계획을 세워야 합니다. 이 단계에는 네트워크에 대한 사이트 접두어 얻기 및 IPv6 서브넷 계획(필요한 경우) 작업이 포함됩니다.	“노드에 대한 IPv6 주소 지정 계획 만들기” [25]

IPv6 네트워크 토폴로지 개요

일반적으로 IPv6은 다음 그림에 표시된 것과 같이 IPv4도 사용하는 혼합 네트워크 토폴로지에 사용됩니다. 다음 그림은 이 장에 설명된 IPv6 구성 작업에 대한 설명에서 참조로 사용됩니다.

그림 2-1 IPv6 네트워크 토폴로지 시나리오



그림에 설명된 엔터프라이즈 네트워크 시나리오는 기존 IPv4 주소를 포함하는 5개 서브넷으로 구성됩니다. 네트워크 링크는 관리 서브넷과 직접적으로 일치합니다. 네 개의 내부 네트워크는 RFC 1918 스타일의 개인 IPv4 주소로 표시되는데, 이는 IPv4 주소가 없는 경우의 일반적인 솔루션입니다.

이러한 내부 네트워크는 다음과 같은 주소 체계를 사용합니다.

- 서브넷 1은 내부 네트워크 중추 `192.168.1`입니다.
- 서브넷 2는 LDAP `sendmail` 및 DNS 서버를 포함하는 내부 네트워크 `192.168.2`입니다.
- 서브넷 3은 엔터프라이즈의 NFS 서버를 포함하는 내부 네트워크 `192.168.3`입니다.
- 서브넷 4는 엔터프라이즈 직원에 대한 호스트를 포함하는 내부 네트워크 `192.168.4`입니다.

외부 공개 네트워크 172.16.85는 회사의 DMZ처럼 작동합니다. 이 네트워크에는 웹 서버, 익명 FTP 서버 및 엔터프라이즈가 외부에 제공하는 기타 리소스가 포함되어 있습니다. 라우터 2는 내부 중추와 구분된 공개 네트워크 172.16.85 및 방화벽을 실행합니다. DMZ(비무장 지대)의 다른 쪽 끝에 있는 라우터 1은 방화벽을 실행하며 엔터프라이즈의 경계 서버로 사용됩니다.

그림 2-1. "IPv6 네트워크 토폴로지 시나리오"에서 공개 DMZ의 RFC 1918 전용 주소는 172.16.85입니다. 실제로 공개 DMZ에는 등록된 IPv4 주소가 있습니다. 대부분의 IPv4 사이트는 공개 주소 및 RFC 1918 개인 주소를 결합하여 사용합니다. 그러나 IPv6을 사용할 경우 공개 주소 및 개인 주소의 개념이 달라집니다. IPv6의 주소 공간은 훨씬 더 크므로 개인 네트워크 및 공개 네트워크 모두에서 공개 IPv6 주소를 사용하십시오.

Oracle Solaris 듀얼 프로토콜 스택은 동시 IPv4 및 IPv6 작업을 지원합니다. 네트워크에 IPv6을 배치하는 중과 배치 후에도 IPv4 관련 작업을 성공적으로 실행할 수 있습니다. 이미 IPv4를 사용 중인 작동 중인 네트워크에 IPv6을 배치할 경우 진행 중인 작업이 중단되지 않습니다.

IPv6에 대한 하드웨어 지원 확인

하드웨어의 다음 클래스와 관련하여 IPv6이 사용 가능한지 제조업체의 설명서를 확인하십시오.

- 라우터
- 방화벽
- 서버
- 스위치

참고 - 이 설명서의 모든 절차에서는 장비, 특히 라우터를 IPv6으로 업그레이드할 수 있다고 가정합니다. 그러나 일부 라우터 모델은 IPv6으로 업그레이드할 수 없습니다. 자세한 내용과 임시해결책은 "Oracle Solaris 11.2의 네트워크 관리 문제 해결 "의 "IPv4 라우터를 IPv6으로 업그레이드할 수 없음"을 참조하십시오.

IPv6 주소 지정 계획 준비

IPv4에서 IPv6으로의 주요 전환에는 다음과 같은 준비가 필요한 주소 지정 계획 개발이 포함됩니다.

- "사이트 접두어 획득" [25]
- "IPv6 번호 지정 체계 만들기" [25]

실제 마이그레이션 작업은 "Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리 "의 "IPv4 네트워크에서 IPv6 네트워크로 마이그레이션"을 참조하십시오.

사이트 접두어 획득

IPv6을 구성하기 전에 사이트 접두어를 획득해야 합니다. 사이트 접두어는 IPv6 구현에서 모든 노드에 대한 IPv6 주소를 파생시키는 데 사용됩니다.

IPv6을 지원하는 ISP는 48비트 IPv6 사이트 접두어를 조직에 제공합니다. 현재 ISP가 IPv4만 지원할 경우 IPv4 지원을 위한 현재 ISP를 유지하면서 IPv6 지원을 위한 다른 ISP를 사용할 수 있습니다. 이 경우 여러 임시해결책 중 하나를 사용할 수 있습니다. 자세한 내용은 "Oracle Solaris 11.2의 네트워크 관리 문제 해결 "의 "현재 ISP가 IPv6을 지원하지 않음"을 참조하십시오.

소속된 조직이 ISP일 경우 적합한 인터넷 레지스트리에서 고객의 사이트 접두어를 획득합니다. 자세한 내용은 Internet Assigned Numbers Authority (IANA) (http://www.iana.org)를 참조하십시오.

IPv6 번호 지정 체계 만들기

제안된 IPv6 네트워크가 완전히 새로운 네트워크가 아니라면 기존 IPv4 토폴로지를 기반으로 IPv6 번호 지정 체계를 만드십시오.

노드에 대한 IPv6 주소 지정 계획 만들기

대부분의 호스트에서는 인터페이스에 대한 IPv6 주소의 Stateless 자동 구성이 적합한 시간 절약 전략입니다. 호스트가 가장 가까운 라우터로부터 사이트 접두어를 받으면 Neighbor Discovery가 호스트에 있는 각 인터페이스에 대한 IPv6 주소를 자동으로 생성합니다.

서버는 정적 IPv6 주소를 사용해야 합니다. 서버의 IPv6 주소를 수동으로 구성하지 않은 경우, 서버에서 NIC 카드가 교체될 때마다 새 IPv6 주소가 자동 구성됩니다.

서버 주소를 만들 때 다음 사항에 유의하십시오.

- 서버에 의미 있고 안정적인 인터페이스 ID를 제공합니다. 한 가지 전략은 인터페이스 ID에 순차적 번호 지정 체계를 사용하는 것입니다. 예를 들어, 그림 2-1. "IPv6 네트워크 토폴로지 시나리오"에 표시된 LDAP 서버의 내부 인터페이스는 `2001:db8:3c4d:2::2`가 될 수 있습니다.
- IPv4 네트워크의 번호를 정기적으로 재지정하지 않는 경우, 라우터 및 서버의 기존 IPv4 주소를 인터페이스 ID로 사용합니다. 그림 2-1. "IPv6 네트워크 토폴로지 시나리오"에서 DMZ에 대한 라우터 1 인터페이스의 IPv4 주소는 `192.168/16`이라고 가정합니다. IPv4 주소를 16진수로 변환한 다음 그 결과를 인터페이스 ID로 사용할 수 있습니다. 새 인터페이스 ID는 `::7bc8:156F`입니다.

  ISP로부터 주소를 받은 것이 아니라 등록된 IPv4 주소를 소유한 경우에만 이 방법을 사용하십시오. ISP가 제공한 IPv4 주소를 사용하는 경우 종속성이 생기는데, 이 종속성으로 인해 ISP를 변경하면 문제가 발생할 수 있습니다.

사용 가능한 IPv4 주소의 개수에는 제한이 있으므로 과거에는 네트워크 설계자가 등록된 전역 주소 및 개인 RFC 1918 주소를 사용할 위치를 고려해야 했습니다. 그러나 IPv6 주소에는 전역 및 개인 IPv4 주소의 개념이 적용되지 않습니다. 공개 DMZ를 비롯한 모든 네트워크 링크에서 사이트 접두어를 포함하는 전역 유니캐스트 주소를 사용할 수 있습니다.

서브넷 번호 지정 체계 만들기

기존 IPv4 서브넷을 해당 IPv6 서브넷에 매핑하여 번호 지정 체계를 시작하십시오. 예를 들어, 그림 2-1. “IPv6 네트워크 토폴로지 시나리오”에 표시된 서브넷을 고려해 보십시오. 서브넷 1-4은 주소의 처음 16비트에 대해 RFC 1918 IPv4 개인 주소 지정을 사용합니다. 숫자 1-4는 서브넷을 나타냅니다. 설명을 위해 IPv6 접두어 refix `2001:db8:3c4d/48`가 사이트에 지정되었습니다.

다음 표는 개인 IPv4 접두어가 IPv6 접두어에 매핑되는 방식을 보여줍니다.

IPv4 서브넷 접두어	해당 IPv6 서브넷 접두어
`192.168.1.0/24`	`2001:db8:3c4d:1::/64`
`192.168.2.0/24`	`2001:db8:3c4d:2::/64`
`192.168.3.0/24`	`2001:db8:3c4d:3::/64`
`192.168.4.0/24`	`2001:db8:3c4d:4::/64`

IPv6을 지원하도록 네트워크 서비스 구성

다음과 같은 일반 IPv4 네트워크 서비스도 IPv6에서 사용할 수 있습니다.

- DNS
- HTTP(Apache 2 릴리스 또는 Orion)
- LDAP
- NFS
- `sendmail`

IMAP 메일 서버는 IPv4에서만 사용 가능합니다.

IPv6용으로 구성된 노드는 IPv4 서비스를 실행할 수 있습니다. IPv6을 설정할 경우 모든 서비스가 IPv6 연결을 수락하는 것은 아닙니다. IPv6으로 이식된 서비스만 연결을 수락합니다. IPv6으로 이식되지 않은 서비스는 계속 프로토콜 스택의 IPv4 부분에서 작동합니다.

서비스를 IPv6으로 업그레이드한 후 문제가 발생할 수 있습니다. 자세한 내용은 “Oracle Solaris 11.2의 네트워크 관리 문제 해결 ”의 “IPv6을 지원하도록 서비스를 업그레이드할 때 발생하는 문제”를 참조하십시오.

▼ IPv6을 지원하도록 네트워크 서비스를 준비하는 방법

1. **IPv6을 지원하도록 다음 네트워크 서비스를 업데이트합니다.**

   - 메일 서버
   - NIS 서버
   - NFS

   참고 - LDAP은 IPv6 관련 구성 작업 없이 IPv6을 지원합니다.

2. **IPv6에서 방화벽 하드웨어를 사용할 수 있는지 확인합니다.**
   지침은 해당 방화벽 관련 설명서를 참조하십시오.

3. **네트워크에 있는 다른 서비스가 IPv6으로 이식되었는지 확인합니다.**
   자세한 내용은 소프트웨어의 마케팅 보조 자료 및 관련 설명서를 참조하십시오.

4. **사이트에서 다음 서비스를 배치하는 경우 이러한 서비스에 대해 적절한 조치를 취했는지 확인합니다.**

   - **방화벽** - IPv4에서 IPv6을 지원하기 위해 적용된 정책을 강화합니다. 보다 자세한 보안 고려 사항은 "IPv6 구현에 대한 보안 고려 사항" [28]을 참조하십시오.
   - **메일** - DNS에 대한 MX 레코드(메일 교환기 레코드)에 메일 서버의 IPv6 주소를 추가합니다.
   - **DNS** - DNS 관련 고려 사항은 IPv6을 지원하도록 DNS를 준비하는 방법 [27]을 참조하십시오.
   - **IPQoS** - IPv4에 사용된 것과 동일한 *Diffserv* 정책을 호스트에 대해 사용합니다.

5. **해당 노드를 IPv6으로 변환하기 전에 노드에서 제공하는 네트워크 서비스를 감사합니다.**

▼ IPv6을 지원하도록 DNS를 준비하는 방법

Oracle Solaris는 클라이언트측과 서버측 둘 다에 대한 DNS 분석을 지원합니다. IPv6을 위해 DNS 서비스를 준비하려면 다음 절차를 따르십시오.

IPv6에 대한 DNS 지원과 관련된 자세한 내용은 "Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: DNS 및 NIS "을 참조하십시오.

1. **순환 이름 분석을 수행하는 DNS 서버가 듀얼 스택(IPv4 및 IPv6)인지 아니면 IPv4 전용인지 확인합니다.**

2. **DNS 서버에서 DNS 데이터베이스를 정방향 영역의 관련 IPv6 데이터베이스 AAAA 레코드로 채웁니다.**

   참고 - 중요한 서비스를 여러 개 실행하는 서버의 경우 특별한 주의가 필요합니다. 네트워크가 제대로 작동하는지 확인하십시오. 또한 중요한 서비스가 모두 IPv6으로 이식되었는지도 확인하십시오. 그런 다음 서버의 IPv6 주소를 DNS 데이터베이스에 추가하십시오.

3. **AAAA 레코드의 연관된 PTR 레코드를 역방향 영역에 추가합니다.**

4. **영역에 대해 설명하는 NS 레코드에 IPv4 전용 데이터 또는 IPv6 및 IPv4 데이터를 추가합니다.**

네트워크에서 터널 사용 계획

사용자의 네트워크가 IPv4 및 IPv6으로 마이그레이션되므로 IPv6 구현은 전환 방식으로 사용될 여러 터널 구성을 지원합니다. 터널을 통해 분리된 IPv6 네트워크가 통신할 수 있게 됩니다. 대부분의 인터넷은 IPv4를 실행하므로, 사용자 사이트의 IPv6 패킷은 인터넷에서 터널을 통과하여 대상 Pv6 네트워크로 이동합니다.

다음은 IPv6 네트워크 토폴로지에서 터널을 사용하기 위한 몇 가지 주요 시나리오입니다.

- IPv6 서비스를 구매한 ISP는 사이트의 경계 라우터에서 ISP 네트워크로 연결되는 터널을 만들 수 있도록 해줍니다. 그림 2-1. “IPv6 네트워크 토폴로지 시나리오”는 이러한 터널을 보여줍니다. 이 경우 IPv4 터널을 통해 수동 IPv6을 실행합니다.
- IPv4 연결로 분산된 대형 네트워크를 관리합니다. IPv6을 사용하는 분산된 사이트를 연결하려면 각 서브넷의 에지 라우터에서 자동 6to4 터널을 실행하면 됩니다.
- 기반구조의 라우터를 IPv6으로 업그레이드할 수 없는 경우도 있습니다. 이 경우 두 개의 IPv6 라우터를 끝점으로 사용하여 IPv4 라우터를 통과하는 수동 터널을 만들 수 있습니다.

터널 구성 절차는 “Oracle Solaris 11.2의 TCP/IP 네트워크, IPMP 및 IP 터널 관리 ”의 5 장, “IP 터널 관리”를 참조하십시오. 터널 관련 개념 정보는 “Oracle Solaris 11.2의 TCP/IP 네트워크, IPMP 및 IP 터널 관리 ”의 “IP 터널 기능 요약”을 참조하십시오.

IPv6 구현에 대한 보안 고려 사항

IPv6을 기존 네트워크에 사용할 경우 사이트의 보안이 손상되지 않도록 유의해야 합니다.

IPv6 구현을 도입할 때 다음 보안 문제에 유의하십시오.

- IPv6 패킷과 IPv4 패킷 모두에 대해 동일한 양의 필터링이 필요합니다.

- IPv6 패킷은 대개 방화벽을 통해 터널링됩니다.

  따라서 다음 시나리오 중 하나로 구현해야 합니다.

  - 방화벽이 터널 내에서 컨텐츠 검사를 수행하도록 합니다.
  - 반대쪽 터널 끝점에 동일한 규칙을 사용하는 IPv6 방화벽을 배치합니다.
- IPv6 - UDP(사용자 데이터그램 프로토콜) - IPv4 터널을 사용하는 전환 방식이 존재합니다. 이러한 방식은 방화벽을 방해하므로 문제가 될 수 있습니다.
- IPv6 노드는 엔터프라이즈 네트워크 외부에서 전역적으로 연결할 수 있습니다. 보안 정책이 공개 액세스를 금지하는 경우 방화벽에 대해 보다 엄격한 규칙을 설정해야 합니다. 예를 들어, *Stateful* 방화벽 구성을 고려해 보십시오.

이 설명서에는 IPv6 구현에서 사용될 수 있는 다음과 같은 보안 기능에 대한 정보가 포함되어 있습니다.

- IP 보안 아키텍처(IPsec) 기능을 통해 IPv6 패킷에 대한 암호화된 보호를 제공할 수 있습니다. 자세한 내용은 “Oracle Solaris 11.2의 네트워크 보안 ”의 6 장, “IP Security Architecture 정보”를 참조하십시오.
- IKE(Internet Key Exchange) 기능은 IPsec에 대한 키 관리를 자동화합니다. 자세한 내용은 “Oracle Solaris 11.2의 네트워크 보안 ”의 8 장, “IKE(Internet Key Exchange)”를 참조하십시오.

색인