

Oracle® Solaris 11.2 시스템을 라우터 또는 로드 밸런서로 구성

ORACLE®

부품 번호: E53807-02
2014년 9월

Copyright © 2011, 2014, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이선스 계약서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이선스 계약서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이선스, 전송, 배포, 진열, 실행, 발행 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주시기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이선스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이선스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사들의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이선스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록 상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제 3자로부터 제공되는 콘텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. Oracle Corporation과 그 자회사는 제 3자의 콘텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제 3자의 콘텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다.

목차

이 설명서 사용	7
1 라우터 및 로드 밸런서 소개	9
라우터 개요	9
경로 지정 프로토콜	9
VRRP 라우터 개요	12
통합된 로드 밸런서 개요	12
ILB의 기능	13
VRRP 라우터 및 로드 밸런서를 사용하는 이유	14
2 시스템을 라우터로 구성	15
IPv4 라우터 구성	15
▼ IPv4 라우터 구성 방법	15
IPv6 라우터 구성	19
in.ripngd 데몬(IPv6 경로 지정용)	20
라우터 알림, 접두어 및 메시지	20
▼ IPv6 지원 라우터를 구성하는 방법	21
3 VRRP(Virtual Router Redundancy Protocol) 사용	23
VRRP 정보	23
VRRP 작동 방식	24
Layer 3 VRRP 기능 정보	26
Layer 2 및 Layer 3 VRRP 비교	26
Layer 2 및 Layer 3 VRRP 제한 사항	28
4 VRRP(Virtual Router Redundancy Protocol) 구성 및 관리	31
VRRP 구성 계획	31
VRRP 설치	31
▼ VRRP를 설치하는 방법	32
VRRP 구성	32

Layer 2 VRRP에 대한 VRRP VNIC 만들기	32
VRRP 라우터 만들기	33
Layer 2 및 Layer 3 VRRP 라우터에 대한 가상 IP 주소 구성	35
VRRP 라우터 사용 및 사용 안함으로 설정	36
VRRP 라우터 수정	37
Layer 2 및 Layer 3 VRRP 라우터 구성 표시	37
VRRP 라우터와 연관된 IP 주소 표시	39
VRRP 라우터 삭제	40
불필요한 ARP 및 NDP 메시지 제어	40
사용 사례: Layer 2 VRRP 라우터 구성	40
5 통합 로드 밸런서 개요	43
ILB 구성 요소	43
ILB 작동 모드	44
DSR(Direct Server Return) 모드	44
NAT(Network Address Translator) 모드	45
ILB 작동 방식	48
6 통합 로드 밸런서 구성 및 관리	51
ILB 설치	51
명령줄 인터페이스를 사용하여 ILB 구성	52
ILB 사용 또는 사용 안함으로 설정	53
▼ ILB를 사용으로 설정하는 방법	53
▼ ILB를 사용 안함으로 설정하는 방법	53
ILB 관리	54
ILB에서 서버 그룹 및 백엔드 서버 정의	54
ILB에서 상태 검사 모니터링	57
ILB 규칙 구성	60
사용 사례: ILB 구성	63
ILB 통계 표시	64
통계 정보 표시	64
NAT 연결 테이블 표시	64
세션 지속성 매핑 테이블 표시	65
구성 가져오기 및 내보내기	66
7 고가용성을 위한 ILB 구성	67
DSR 토폴로지를 사용하여 고가용성 ILB 구성	67
▼ DSR 토폴로지를 사용하여 고가용성 ILB를 구성하는 방법	69
Half-NAT 토폴로지를 사용하여 고가용성 ILB 구성	70

▼ Half-NAT 토폴로지를 사용하여 고가용성 ILB를 구성하는 방법	72
색인	75

이 설명서 사용

- **개요** - Oracle Solaris 11.2를 IPv4 또는 IPv6 라우터의 일부로 구성하는 방법을 설명합니다. VRRP(Virtual Router Redundancy Protocol) 및 ILB(Integrated Load Balancer)에 대한 개요 및 구성 지침을 제공합니다.
- **대상** - 시스템 관리자
- **필요한 지식** - 네트워크 관리와 관련한 기본 기술과 일부 고급 기술

제품 설명서 라이브러리

이 제품에 대한 최신 정보 및 알려진 문제는 설명서 라이브러리(<http://www.oracle.com/pls/topic/lookup?ctx=E36784>)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=info>를 참조하거나, 청각 장애가 있는 경우 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>를 방문하십시오.

피드백

<http://www.oracle.com/goto/docfeedback>에서 이 설명서에 대한 피드백을 보낼 수 있습니다.

라우터 및 로드 밸런서 소개

이 장에서는 라우터 및 로드 밸런서가 Oracle Solaris에서 컴퓨터 네트워크를 연결하고 작업 로드를 분배하는 데 어떻게 사용되는지 설명합니다. 라우터는 RIP(Routing Information Protocol), 차세대 RIP(RIPng), RDISC(Internet Control Message Protocol Router Discovery), OSPF(Open Shortest Path First), BGP(Border Gateway Protocol), IS-IS(Intermediate System to Intermediate System) 및 VRRP(Virtual Router Redundancy Protocol)와 같은 프로토콜을 사용하여 경로 지정 작업을 처리합니다.

로드 밸런서는 네트워크 트래픽을 여러 서버로 분배합니다. 네트워크의 작업 로드 분배는 최적의 리소스 공유를 달성하고 처리량 및 가용성을 높이는 데 도움을 줍니다.

이 장의 내용:

- “라우터 개요” [9]
- “VRRP 라우터 개요” [12]
- “통합된 로드 밸런서 개요” [12]
- “VRRP 라우터 및 로드 밸런서를 사용하는 이유” [14]

라우터 개요

라우터는 컴퓨터 네트워크에서 컴퓨터를 연결하고 네트워크의 컴퓨터 사이에 데이터 패킷을 전송하는 데 사용됩니다. 라우터는 서로 다른 네트워크에서 2개 이상의 연결을 가질 수 있습니다. 라우터는 수신 데이터 패킷에서 주소 정보를 읽어 대상을 결정합니다. 그런 다음 패킷은 라우터의 경로 지정 테이블에 있는 정보를 사용하여 다음 네트워크로 전달됩니다. 라우터의 처리를 지시하는 이 트래픽은 데이터 패킷이 대상 노드에 도달할 때까지 반복됩니다.

경로 지정 프로토콜

경로 지정 프로토콜은 시스템에서 경로 지정 작업을 처리합니다. 라우터는 다른 호스트와 경로 지정 정보를 교환하여 원격 네트워크까지 알려진 경로를 유지합니다. 라우터와 호스트 모두 경로 지정 프로토콜을 실행할 수 있습니다. 호스트의 경로 지정 프로토콜은 다른 라우터 및 호스트의 경로 지정 데몬과 통신합니다. 이러한 프로토콜은 호스트가 패킷 전달 대상을 결

정하는 데 유용합니다. 네트워크 인터페이스가 사용으로 설정되면 시스템이 자동으로 경로 지정 데몬과 통신합니다. 이러한 데몬은 네트워크의 라우터를 모니터링하고 라우터 주소를 로컬 네트워크의 호스트로 알립니다. 일부 경로 지정 프로토콜은 경로 지정 성능을 측정하는 데 사용할 수 있는 통계를 유지 관리하기도 합니다. 패킷 전달과 마찬가지로 Oracle Solaris 시스템에서는 경로 지정을 명시적으로 구성해야 합니다.

RIP 및 RDISC는 표준 TCP/IP 프로토콜입니다. 다음 표에서는 Oracle Solaris에서 지원되는 경로 지정 프로토콜을 설명합니다.

표 1-1 Oracle Solaris 경로 지정 프로토콜

프로토콜	연관된 데몬	설명	지침
RIP	in.routed	IPv4 패킷을 경로 지정하고 경로 지정 테이블을 유지 관리하는 IGP(Interior Gateway Protocol)입니다.	"IPv4 라우터 구성" [15]
RDISC	in.routed	호스트에서 네트워크의 라우터를 검색할 수 있습니다.	"Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리"의 "단일 인터페이스 시스템에 대한 경로 지정 사용"
RIPng	in.ripngd	IPv6 패킷을 경로 지정하고 경로 지정 테이블을 유지 관리하는 IGP입니다.	IPv6 지원 라우터를 구성하는 방법 [21]
NDP(Neighbor Discovery Protocol)		IPv6 라우터의 존재를 알리고 네트워크의 IPv6 호스트를 검색합니다.	"Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리"의 "IPv6에 대해 시스템을 구성하는 방법"

Oracle Solaris의 경로 지정 테이블 및 유형에 대한 자세한 내용은 "Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리"의 "경로 지정 테이블 및 경로 지정 유형"을 참조하십시오.

RIP(Routing Information Protocol)

RIP(Routing Information Protocol)는 거리 벡터 경로 지정 프로토콜입니다. RIP은 홉 카운터를 경로 지정 측정 단위로 사용합니다. 경로 지정 데몬 in.routed로 구현됩니다. 데몬은 시스템이 부트될 때 자동으로 시작됩니다. -s 옵션을 지정하여 라우터에서 실행할 경우 in.routed 데몬은 모든 도달 가능한 네트워크에 대한 경로로 커널 경로 지정 테이블을 채우고 모든 네트워크 인터페이스를 통해 도달 가능성을 알립니다. -q 옵션을 지정하여 호스트에서 실행할 경우 in.routed 데몬은 경로 지정 정보를 추출하지만 도달 가능성을 알리지는 않습니다.

호스트에서 경로 지정 정보는 다음 두 가지 방법으로 추출할 수 있습니다.

- 플래그(대문자 s 또는 공간 절약 모드)를 지정하지 않습니다. in.routed 데몬은 라우터에서 만드는 것과 동일하게 전체 경로 지정 테이블을 만듭니다.
- 플래그를 지정합니다. in.routed 데몬은 각 사용 가능한 라우터에 대해 단일 기본 경로가 포함된 최소 커널 테이블을 만듭니다.

RDISC(ICMP Router Discovery) 프로토콜

호스트는 RDISC(ICMP Router Discovery) 프로토콜을 사용하여 라우터에서 경로 지정 정보를 가져옵니다. 호스트에서 RDISC를 실행하는 경우 라우터 정보를 교환하려면 라우터도 다른 프로토콜(예: RIP)을 실행해야 합니다.

RDISC는 `in.routed` 데몬으로 구현되며, 라우터와 호스트 모두에서 실행되어야 합니다. 호스트에서 `in.routed`는 RDISC를 사용하여 RDISC를 통해 자신을 알리는 라우터에서 기본 경로를 찾습니다. 라우터에서 `in.routed`는 RDISC를 사용하여 직접 연결된 네트워크의 호스트에 기본 경로를 알립니다. 자세한 내용은 [in.routed\(1M\)](#) 매뉴얼 페이지 및 [gateways\(4\)](#) 매뉴얼 페이지를 참조하십시오.

Quagga 경로 지정 프로토콜 모음

Quagga는 Oracle Solaris를 포함한 UNIX 플랫폼용 RIP, RIPng, OSPF(Open Shortest Path First), IS-IS(Intermediate System to Intermediate System) 및 BGP(Border Gateway Protocol) 프로토콜의 구현을 가능하게 하는 경로 지정 소프트웨어 모음입니다.

RIPng는 IPv6에 대한 다양한 개선 기능을 포함하여 IPv6의 지원을 위한 RIP의 확장 기능을 제공합니다. RIPng의 기능은 RIP의 기능과 유사합니다.

OSPF는 대형 자율 시스템 네트워크 내에서 경로 지정 정보를 분배하는 데 사용되는 라우터 프로토콜입니다. OSPF의 최신 버전인 OSPFv3에는 IPv6에 대한 지원이 추가되었습니다.

IS-IS는 대형 서비스 제공업체 네트워크 내에서 경로 지정 정보를 분배하는 데 사용되는 링크 상태 동적 경로 지정 프로토콜입니다.

BGP는 대형 자율 시스템 네트워크 사이에서 경로 및 규칙을 기준으로 경로 지정 결정을 내리기 위해 접두어가 붙은 IP 네트워크 세트를 사용합니다.

다음 표는 Oracle Solaris에서 지원되는 오픈 소스 Quagga 경로 지정 프로토콜을 나열합니다.

표 1-2 Quagga 경로 지정 프로토콜 모음

프로토콜	연관된 데몬	설명
RIP	<code>ripd</code>	IPv4 패킷을 경로 지정하고 주변에 경로 지정 테이블을 알리는 IPv4 거리 벡터링 IGP입니다.
RIPng	<code>ripngd</code>	IPv6 패킷을 경로 지정하고 경로 지정 테이블을 유지 관리하는 IPv6 거리 벡터링 IGP입니다.
OSPF	<code>ospfd</code>	패킷 경로 지정 및 고가용성 네트워킹을 위한 IPv4 링크 상태 IGP입니다.
BGP	<code>bgpd</code>	관리 도메인에 걸쳐 경로 지정을 위한 IPv4 및 IPv6 EGP(Exterior Gateway Protocol)입니다.
IS-IS	<code>isisd</code>	관리 도메인 또는 네트워크 내에서 경로 지정을 위한 IPv4 및 IPv6 링크 상태 IGP입니다.

Quagga 프로토콜에 대한 자세한 내용은 Quagga Routing Suite 웹 사이트(<http://www.nongnu.org/quagga/index.html>)를 참조하십시오.

VRRP(Virtual Router Redundancy Protocol)

VRRP는 라우터 및 로드 밸런서에 주로 사용되는 IP 주소의 고가용성을 제공합니다. VRRP는 RFC 5798, Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6에서 지정된 인터넷 표준 프로토콜입니다. Oracle Solaris에서는 VRRP 서비스를 구성하고 관리하는 관리 도구를 제공합니다.

기존의 표준 Layer 2 VRRP와 함께 Oracle Solaris 11.2에서는 IPMP 및 InfiniBand 인터페이스를 통한 VRRP를 지원하고 영역에서 VRRP에 대한 향상된 지원을 제공하는 독자적인 Layer 3 VRRP를 제공합니다.

VRRP 사용 및 VRRP 라우터 구성에 대한 자세한 내용은 3장. VRRP(Virtual Router Redundancy Protocol) 사용 및 4장. VRRP(Virtual Router Redundancy Protocol) 구성 및 관리를 참조하십시오.

VRRP 라우터 개요

VRRP(Virtual Router Redundancy Protocol) 라우터는 VRRP를 사용하는 하나 이상의 라우터의 작업으로 만들어지는 단일 라우터 이미지입니다. VRRP는 각 VRRP 라우터에서 실행되며 라우터의 상태를 관리합니다. 한 호스트에 여러 개의 VRRP 라우터가 구성될 수 있으며, 각 VRRP 라우터는 서로 다른 가상 라우터에 속합니다.

Layer 2 VRRP 라우터는 표준 VRRP 프로토콜을 사용하고 고유한 가상 라우터 MAC 주소가 필요합니다. 가상 IP 주소는 항상 동일한 가상 MAC 주소로 분석됩니다. 고유한 가상 라우터 MAC 주소를 얻으려면 VRRP VNIC를 만들어야 합니다. Oracle Solaris에서 독자적인 Layer 3 VRRP 기능은 VRRP 라우터에 대해 고유한 VRRP 가상 MAC 주소를 구성해야 할 필요가 전혀 없도록 해주고 IPMP 및 InfiniBand 인터페이스를 통한 VRRP 지원을 제공합니다.

VRRP 사용 및 VRRP 라우터 구성에 대한 자세한 내용은 3장. VRRP(Virtual Router Redundancy Protocol) 사용 및 4장. VRRP(Virtual Router Redundancy Protocol) 구성 및 관리를 참조하십시오.

통합된 로드 밸런서 개요

Oracle Solaris에서 ILB(Integrated Load Balancer)는 Layer 3 및 Layer 4 로드 균형 조정 기능을 제공합니다. ILB는 SPARC 기반 및 x86 기반 시스템에 설치된 Oracle Solaris 운영

체제에 대해 네트워크(IP) 및 전송(TCP/UDP) 레이어에서 작동합니다. ILB를 사용하여 안정성과 확장성을 향상시키고 네트워크 서비스의 응답 시간을 최소화할 수 있습니다.

ILB는 클라이언트의 수신 요청을 가로채서 로드 균형 조정 규칙을 기반으로 요청을 처리할 백엔드 서버를 결정한 다음 선택한 서버로 요청을 전달합니다. ILB는 백엔드 서버에 대한 라우터로 사용할 수도 있습니다. ILB는 선택적 상태 검사를 수행하고 선택한 서버가 수신 요청을 처리할 수 있는지 여부를 확인할 수 있도록 로드 균형 조정 알고리즘에 대한 데이터를 제공합니다.

ILB의 기능

ILB의 주요 기능은 다음과 같습니다.

- IPv4와 IPv6에 대한 Stateless DSR(Direct Server Return) 및 NAT(네트워크 주소 변환) 작동 모드를 지원합니다.

DSR 및 NAT 작동 모드에 대한 자세한 내용은 [“ILB 작동 모드” \[44\]](#)를 참조하십시오.

- 두 가지 작동 모드에 대한 알고리즘 세트를 사용하여 트래픽/로드 분배 및 서버 선택을 돕습니다.

- CLI(명령줄 인터페이스)를 통해 ILB 관리를 수행할 수 있습니다.

CLI를 사용한 ILB 구성에 대한 자세한 내용은 [“명령줄 인터페이스를 사용하여 ILB 구성” \[52\]](#)을 참조하십시오.

- 상태 검사를 통한 서버 모니터링 기능을 제공합니다.

서버 모니터링 기능에 대한 자세한 내용은 [“ILB에서 상태 검사 모니터링” \[57\]](#)을 참조하십시오.

다음 표에서는 서로 다른 작동 모드에 대해 사용 가능한 ILB의 기능을 나열하고 설명합니다.

표 1-3 ILB 기능

기능	설명	작동 모드
클라이언트가 가상 IP(VIP) 주소에 대해 핑 수행 가능	ILB는 클라이언트에서 VIP 주소로 ICMP echo 요청에 대해 응답합니다.	DSR 및 NAT 모드
서비스 중단 없이 서버 그룹에서 서버 추가 및 제거 가능	ILB는 서버 그룹에서 서버를 동적으로 추가하거나 제거합니다.	NAT 모드
세션 지속성("stickiness") 구성 가능	ILB는 응용 프로그램에 대한 세션 지속성을 구성하여 클라이언트에서 동일한 백엔드 서버로 연결이나 패킷을 보내도록 할 수 있습니다. ILB는 <code>ilbadm create-rule</code> 명령에서 <code>-p</code> 옵션을 사용하고 <code>pmask</code> 옵션을 지정하여 가상 서비스에 대한 세션 지속성(소스 주소 지속성)을 구성할 수 있습니다. 자세한 내용은 “ILB 규칙 만들기” [61] 를 참조하십시오.	DSR 및 NAT 모드
연결 드레이닝 수행 가능	ILB는 새 연결이 사용 안함으로 설정된 서버로 전송되지 않도록 합니다. 이 기능은 활성 연결 또는 세션에 장애를 일으키지 않고 서버를 종료하는 데 유용합니다. 서버에	NAT 모드

기능	설명	작동 모드
	대한 기존 연결은 계속 작동합니다. 해당 서버에 대한 모든 연결이 종료되면 유지 관리 용도로 서버를 종료할 수 있습니다. 서버가 요청을 처리할 준비가 되면 로드 밸런서가 새 연결을 전달할 수 있도록 서버가 사용으로 설정됩니다.	
TCP(Transmission Control Protocol) 및 UDP(User Datagram Protocol) 포트의 로드 균형 조정 가능	ILB는 각 포트에 대한 명시적 규칙이 설정되지 않은 경우에도 다양한 일련의 서버 간에 지정된 IP 주소의 모든 포트에 대한 로드 균형을 조정합니다.	DSR 및 NAT 모드
동일한 서버 그룹 내에서 가상 서비스에 대해 독립적인 포트 지정 가능	ILB는 동일한 서버 그룹의 여러 서버에 대해 서로 다른 대상 포트를 지정할 수 있도록 합니다.	NAT 모드
간단한 포트 범위에 대해 로드 균형 조정 가능	ILB는 지정된 서버 그룹에 대해 VIP의 포트 범위에서 로드 균형을 조정합니다. 다양한 백엔드 서버의 동일한 VIP에서 서로 다른 포트 범위의 로드 균형을 조정하여 편리하게 IP 주소를 절약할 수 있습니다. 또한 NAT 모드에 대해 세션 지속성이 사용으로 설정되어 있는 경우 ILB는 범위 내 여러 포트의 동일한 클라이언트 IP 주소에서 온 요청을 동일한 백엔드 서버로 전송합니다.	DSR 및 NAT 모드
포트 범위 이동 및 축소 가능	포트 범위 이동 및 축소는 로드 균형 조정 규칙의 서버 포트 범위에 따라 달라집니다. 서버 포트 범위가 VIP 포트 범위와 다른 경우 자동으로 포트 이동이 구현됩니다. 서버 포트 범위가 단일 포트인 경우 포트 축소가 구현됩니다.	NAT 모드

ILB 구성 요소, 작동 모드, 알고리즘 및 ILB 작동 방식에 대한 자세한 내용은 [5장. 통합 로드 밸런서 개요](#)를 참조하십시오. ILB 구성 및 관리에 대한 자세한 내용은 [6장. 통합 로드 밸런서 구성 및 관리](#) 및 [7장. 고가용성을 위한 ILB 구성](#)을 참조하십시오.

VRRP 라우터 및 로드 밸런서를 사용하는 이유

LAN과 같은 네트워크를 설정할 때 고가용성 서비스를 제공하는 것이 매우 중요합니다. 고가용성은 장애 발생 시 중복 시스템이 기능을 넘겨 받아 비즈니스 연속성을 유지하는 상태입니다. 고가용성은 과도한 작업 로드가 중복 시스템으로 분배될 때도 관련이 있습니다. 고가용성은 예정 또는 예정되지 않은 작동 중지 시간, 로드 균형 조정 및 재해 복구와 같은 상황에서 중요할 수 있습니다.

네트워크 도메인 내에서 고가용성은 링크, IP 및 라우터와 같은 다양한 레벨에서 구현될 수 있습니다. 로드 밸런서 및 라우터는 고가용성 서비스를 제공하는 데 있어 중요한 역할을 담당합니다. Oracle Solaris에서는 VRRP 라우터 및 ILB가 고가용성을 제공하는 네트워크 레벨 페일오버 및 로드 공유 방식입니다.

VRRP 라우터 작업 및 구성에 대한 자세한 내용은 [3장. VRRP\(Virtual Router Redundancy Protocol\) 사용](#)을 참조하십시오. ILB 작업 및 구성에 대한 자세한 내용은 [5장. 통합 로드 밸런서 개요](#) 및 [6장. 통합 로드 밸런서 구성 및 관리](#)를 참조하십시오.

◆◆◆ 2 장

시스템을 라우터로 구성

라우터는 둘 이상의 네트워크 간 인터페이스를 제공합니다. 라우터의 물리적 네트워크 인터페이스 각각에 고유한 이름과 IP 주소를 지정해야 합니다. 각 라우터에는 기본 네트워크 인터페이스와 연관된 호스트 이름과 IP 주소를 비롯하여 추가 네트워크 인터페이스 각각에 대한 하나 이상의 고유한 이름과 IP 주소가 있는 것입니다. 이 장에서는 Oracle Solaris 시스템을 IPv4 라우터 또는 IPv6 라우터로 구성하는 방법을 설명합니다.

이 장의 내용:

- “IPv4 라우터 구성” [15]
- “IPv6 라우터 구성” [19]

네트워크에서 Oracle Solaris 호스트의 경로 지정 구성에 대한 자세한 내용은 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”의 “단일 인터페이스 시스템에 대한 경로 지정 사용”을 참조하십시오.

경로 지정 프로토콜에 대한 자세한 내용은 “경로 지정 프로토콜” [9] 및 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”의 “IPv6 경로 지정 정보”를 참조하십시오.

IPv4 라우터 구성

다음 절차에 따라 물리적 인터페이스가 하나뿐인 시스템(기본적으로 호스트)을 라우터로 구성할 수 있습니다. “Oracle Solaris 11.2에서 UUCP 및 PPP를 사용하여 직렬 네트워크 관리”의 “다이얼 업 PPP 링크 계획”에 설명된 대로 시스템이 PPP 링크에서 하나의 끝점으로 사용되는 경우 단일 인터페이스 시스템을 라우터로 구성할 수 있습니다.

▼ IPv4 라우터 구성 방법

다음 절차에서는 라우터 설치 후 라우터에 대한 인터페이스를 구성 중인 것으로 간주합니다.

시작하기 전에 라우터가 네트워크에 물리적으로 설치된 후 라우터가 로컬 파일 모드로 작동하도록 구성합니다. 이 구성은 네트워크 구성 서버의 작동이 중지된 경우에도 라우터가 부트되도록 합니다.

1. 관리자로 로그인합니다.

자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “지정된 관리 권한 사용”을 참조하십시오.

2. 시스템의 NIC에 대해 IP 인터페이스를 구성합니다.

```
# ipadm create-ip IP-interface
```

3. 다음 명령 중 하나를 선택하여 유효한 IP 주소로 IP 인터페이스를 구성합니다.

■ 정적 주소를 구성하려면 다음 명령을 입력합니다.

```
# ipadm create-addr -a address [interface | addr-obj]
```

■ 비정적 주소를 구성하려면 다음 명령을 입력합니다.

```
# ipadm create-addr -T address-type [interface | addr-obj]
```

IP 인터페이스를 구성하는 방법에 대한 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.

각 IP 인터페이스는 시스템에서 패킷을 경로 지정해야 하는 네트워크의 IP 주소로 구성되어 있어야 합니다. 따라서 시스템이 192.168.5.0 및 10.0.5.0 네트워크를 제공하는 경우 각 네트워크에 대해 하나의 NIC를 구성해야 합니다.



주의 - DHCP를 사용하도록 IPv4 라우터를 구성하기 전에 DHCP 관리를 철저히 파악하고 있어야 합니다.

4. /etc/inet/hosts 파일에 각 인터페이스의 호스트 이름 및 IP 주소를 추가합니다.

예를 들어, 라우터의 두 인터페이스에 대해 지정된 이름이 각각 krakatoa와 krakatoa-1이라고 가정합니다. /etc/inet/hosts 파일의 항목은 다음과 같습니다.

```
192.168.5.1    krakatoa        #interface for network 192.168.5.0
10.0.5.1     krakatoa-1     #interface for network 10.0.5.0
```

5. “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”의 “로컬 파일 모드에 대한 시스템 구성 방법” 절차를 수행하여 이 라우터가 로컬 파일 모드로 실행되도록 구성합니다.

6. 라우터가 서브넷 네트워크에 연결된 경우 /etc/inet/netmasks 파일에 네트워크 번호 및 넷 마스크를 추가합니다.

예를 들어, IPv4 주소 표기법(예: 192.168.5.0)의 경우 다음과 같이 입력합니다.

```
192.168.5.0    255.255.255.0
```

7. 라우터에서 IPv4 패킷 전달을 사용으로 설정합니다.

```
# ipadm set-prop -p forwarding=on ipv4
```


8. (옵션) 경로 지정 프로토콜을 시작합니다.

다음 명령 중 하나를 사용합니다.

```
# routeadm -e ipv4-routing -u
```

여기서 `-e` 옵션은 IPv4 경로 지정을 사용으로 설정하고 `-u` 옵션은 현재 구성을 실행 중인 시스템에 적용합니다.

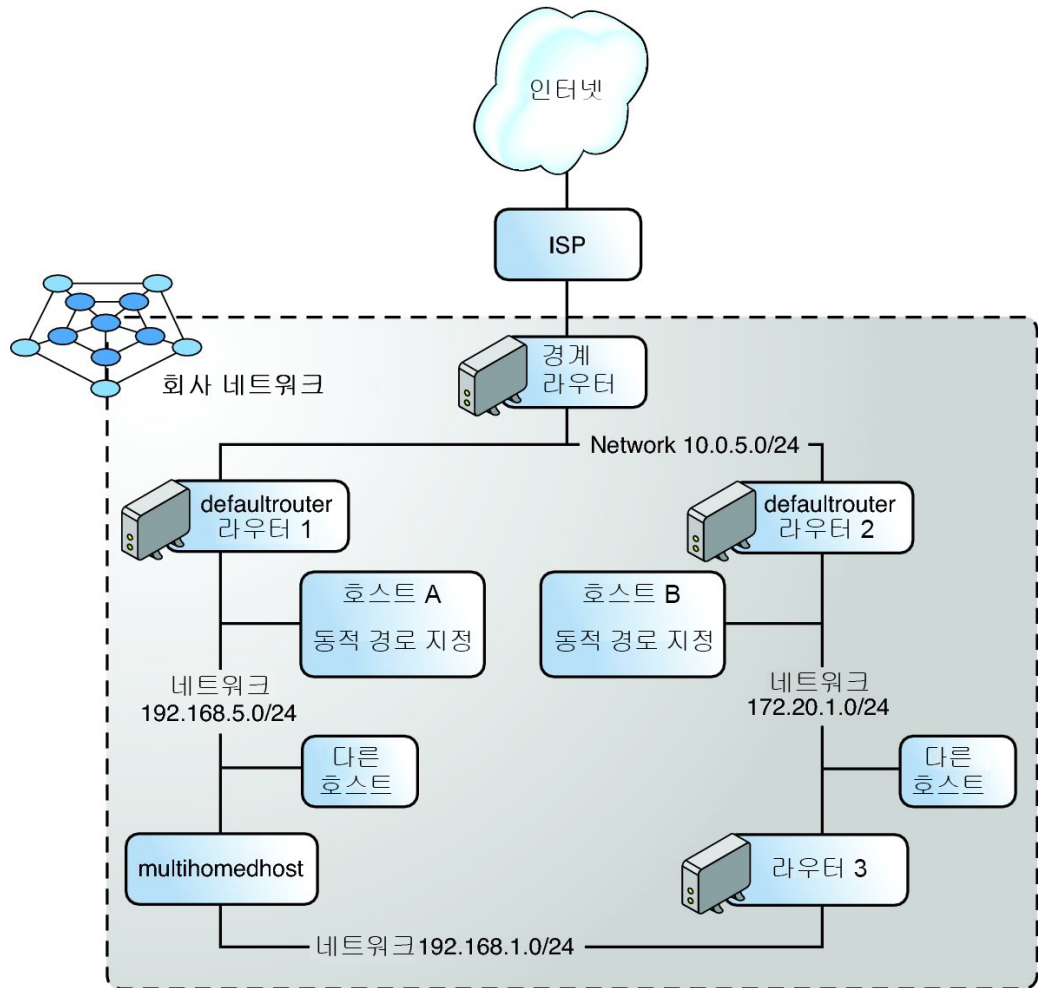
```
# svcadm enable route:default
```

경로 지정 프로토콜을 시작하면 경로 지정 데몬 `/usr/sbin/in.routed`가 자동으로 경로 지정 테이블을 업데이트합니다. 이 프로세스를 동적 경로 지정이라고 합니다. 경로 지정 유형에 대한 자세한 내용은 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”의 “경로 지정 테이블 및 경로 지정 유형”을 참조하십시오. `routeadm` 명령에 대한 자세한 내용은 [routeadm\(1M\)](#) 매뉴얼 페이지, `ipadm` 명령에 대한 자세한 내용은 [ipadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

`in.routed` 데몬과 연관된 SMF(서비스 관리 기능) FMRI(Fault Management Resource Identifier)는 `svc:/network/routing/route`입니다.

예 2-1 시스템을 라우터로 구성

이 예는 다음 그림을 기준으로 합니다.



Router 2에는 두 개의 유선 네트워크 연결(172.20.1.0 네트워크에 대한 연결과 10.0.5.0 네트워크에 대한 연결)이 포함되어 있습니다. 이 예에서는 시스템을 172.20.1.0 네트워크의 라우터(Router 2)로 구성하는 방법을 보여줍니다. 또한 이 예에서는 Router 2가 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”의 “로컬 파일 모드에 대한 시스템 구성 방법”에 설명된 대로 로컬 파일 모드로 작동하도록 구성되었다고 간주합니다.

1. 시스템 인터페이스의 상태를 확인합니다.

```
# dladm show-link
LINK    CLASS    MTU    STATE    BRIDGE    OVER
net0    phys     1500   up       --        --
net1    phys     1500   up       --        --
net2    phys     1500   up       --        --
# ipadm show-addr
```

```

ADDROBJ      TYPE    STATE    ADDR
lo0/v4       static  ok       10.0.0.1/8
net0/v4      static  ok       172.20.1.10/24

```

2. net0만 IP 주소로 구성되었습니다. Router 2를 기본 라우터로 설정하려면 물리적으로 net1 인터페이스를 10.0.5.0 네트워크에 연결합니다.

```

# ipadm create-ip net1
# ipadm create-addr -a 10.0.5.10/24 net1
# ipadm show-addr
ADDROBJ      TYPE    STATE    ADDR
lo0/v4       static  ok       192.168.0.1/8
net0/v4      static  ok       172.20.1.10/24
net1/v4      static  ok       10.0.5.10/24

```

3. 새로 구성된 인터페이스 및 연결된 네트워크에 대한 정보로 다음 네트워크 데이터베이스를 업데이트합니다.

```

# pfedit /etc/inet/hosts
192.168.0.1      localhost
172.20.1.10     router2        #interface for network 172.20.1
10.0.5.10      router2-out   #interface for network 10.0.5
# pfedit /etc/inet/netmasks
172.20.1.0     255.255.255.0
10.0.5.0      255.255.255.0

```

4. 패킷 전달 및 in.routed 경로 지정 데몬을 사용으로 설정합니다.

```

# ipadm set-prop -p forwarding=on ipv4
# svcadm enable route:default

```

그러면 RIP를 통한 IPv4 패킷 전달 및 동적 경로 지정이 Router 2에서 사용으로 설정되었지만, 172.20.1.0 네트워크에 대한 기본 라우터 구성을 완료하려면 다음을 수행해야 합니다.

- 호스트가 새 기본 라우터에서 경로 지정 정보를 가져오도록 172.20.1.0 네트워크에서 각 호스트를 수정합니다. 자세한 내용은 [“Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”](#)의 [“지속\(정적\) 경로 만들기”](#)를 참조하십시오.
- Router 2의 경로 지정 테이블에서 경계 라우터에 대한 정적 경로 지정을 정의합니다. 자세한 내용은 [“Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”](#)의 [“경로 지정 테이블 및 경로 지정 유형”](#)를 참조하십시오. ipadm 명령에 대한 자세한 내용은 [ipadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

IPv6 라우터 구성

이 절에서는 IPv6 라우터를 구성하는 방법에 대해 설명합니다.

in.ripngd 데몬(IPv6 경로 지정용)

in.ripngd 데몬은 IPv6 라우터에 대한 차세대 경로 지정 정보 프로토콜(RIPng)을 구현합니다. RIPng는 IPv6에 해당하는 RIP입니다. routeadm 명령으로 IPv6 라우터를 구성하고 IPv6 경로 지정을 설정하면 in.ripngd 데몬이 라우터에서 RIPng를 구현합니다. RIPng의 지원되는 옵션에 대한 자세한 내용은 [in.ripngd\(1M\)](#)을 참조하십시오.

라우터 알림, 접두어 및 메시지

멀티캐스트 가능 링크 및 지점 간 링크에서 각 라우터는 라우터의 사용 가능성을 알리는 라우터 알림 패킷을 정기적으로 멀티캐스트 그룹에 전송합니다. 호스트는 모든 라우터로부터 라우터 알림을 수신하여 기본 라우터 목록을 작성합니다. 라우터는 몇 초 내에 호스트가 라우터의 존재를 알 수 있도록 자주 라우터 알림을 생성합니다. 그러나 라우터는 알림 부재를 통해 라우터 오류를 감지할 만큼 자주 알림을 전송하지 않습니다. 이웃 연결 불가를 확인하는 별도의 감지 알고리즘을 통해 오류를 감지할 수 있습니다.

라우터 알림에는 호스트가 라우터와 동일한 링크(온 링크)에 있는지 확인하는 데 사용되는 서브넷 접두어 목록이 포함되어 있습니다. 접두어 목록은 자동 주소 구성에도 사용됩니다. 접두어와 연관된 플래그는 특정 접두어의 의도된 사용을 지정합니다. 호스트는 알림의 온 링크 접두어를 사용하여 패킷 대상이 온 링크인 시점 또는 라우터 외부에 있는 시점을 확인하는 데 사용되는 목록을 작성하고 유지 관리합니다. 대상이 알림의 온 링크 접두어에 의해 처리되지 않더라도 대상은 온 링크 상태일 수 있습니다. 이 경우 라우터가 재지정을 전송할 수 있습니다. 재지정은 대상이 이웃임을 발신자에게 알립니다.

라우터는 라우터 알림 및 접두어별 플래그를 사용하여 Stateless 주소 자동 구성을 수행하는 방법을 호스트에 알릴 수 있습니다.

라우터 알림 메시지에는 호스트가 송신 패킷에 사용해야 하는 인터넷 매개변수(예: 홑 한계)가 포함되어 있습니다. 선택적으로 링크 매개변수(예: 링크 MTU)도 포함될 수 있습니다. 이 기능으로 중요한 매개변수를 중앙에서 관리할 수 있습니다. 매개변수는 라우터에 대해 설정될 수 있으며 연결된 모든 호스트에 자동으로 전파됩니다.

노드는 대상 노드에 해당 링크 계층 주소를 반환하도록 요청하는 이웃 요청을 멀티캐스트 그룹에 전송하는 방식으로 주소 결정을 수행합니다. 멀티캐스트 이웃 요청 메시지는 대상 주소의 요청된 노드 멀티캐스트 주소로 전송됩니다. 대상은 유니캐스트 이웃 알림 메시지에 링크 계층 주소를 반환합니다. 패킷의 단일 요청-응답 쌍만으로 개시자와 대상이 서로의 링크 계층 주소를 결정할 수 있습니다. 이웃 요청에는 개시자의 링크 계층 주소가 포함되어 있습니다.

▼ IPv6 지원 라우터를 구성하는 방법

다음 절차에서는 시스템에 이미 IPv6이 구성되었다고 가정합니다. 자세한 절차는 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”의 3 장, “Oracle Solaris에서 IP 인터페이스와 주소 구성 및 관리”를 참조하십시오.

1. 관리자로 로그인합니다.

자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “지정된 관리 권한 사용”을 참조하십시오.

2. 라우터의 모든 인터페이스에서 IPv6 패킷 전달을 구성합니다.

```
# ipadm set-prop -p forwarding=on ipv6
```

3. 경로 지정 데몬을 시작합니다.

in.ripngd 데몬은 IPv6 경로 지정을 처리합니다. 다음 명령 중 하나를 사용하여 IPv6 경로 지정을 사용으로 설정합니다.

- routeadm 명령을 사용합니다.

```
# routeadm -e ipv6-routing -u
```

여기서 -e 옵션은 IPv4 경로 지정을 사용으로 설정하고 -u 옵션은 현재 구성을 실행 중인 시스템에 적용합니다.

- 해당 SMF 명령을 사용합니다.

```
# svcadm enable ripng:default
```

routeadm 명령에 대한 자세한 내용은 [routeadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

4. /etc/inet/ndpd.conf 파일을 만듭니다.

라우터가 알릴 사이트 접두어 및 기타 구성 정보를 /etc/inet/ndpd.conf 파일에 지정합니다. 이 파일은 IPv6 Neighbor Discovery 프로토콜을 구현하는 in.ndpd 데몬이 읽습니다.

변수 및 허용되는 값 목록은 [ndpd.conf\(4\)](#) 매뉴얼 페이지를 참조하십시오.

5. /etc/inet/ndpd.conf 파일에 다음 텍스트를 입력합니다.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

이 텍스트는 IPv6용으로 구성된 라우터의 모든 인터페이스를 통해 라우터 알림을 전송하도록 in.ndpd에 지시합니다.

6. 라우터의 여러 인터페이스에 사이트 접두어를 구성하고 /etc/inet/ndpd.conf 파일에 추가 텍스트를 추가합니다.

텍스트는 다음과 같은 형식으로 추가해야 합니다.

```
prefix global-routing-prefix:subnet ID/64 interface
```

다음 예에서 /etc/inet/ndpd.conf 파일은 net0 및 net1 인터페이스를 통해 사이트 접두어 2001:0db8:3c4d::/48을 알리도록 라우터를 구성합니다.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

```
if net0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 net0
```

```
if net1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 net1
```

7. 시스템을 재부트합니다.

IPv6 라우터가 ndpd.conf 파일에 있는 사이트 접두어를 로컬 사이트에 알립니다.

8. IPv6용으로 구성된 인터페이스를 표시합니다.

```
# ipadm show-addr
ADDROBJ      TYPE      STATE    ADDR
lo0/v4       static    ok       192.68.0.1/8
net0/v4       static    ok       172.16.15.232/24
net1/v4       static    ok       172.16.16.220/24
net0/v6       addrconf ok       fe80::203:baff:fe11:b115/10
lo0/v6       static    ok       ::1/128
net0/v6a     static    ok       2001:db8:3c4d:15:203:baff:fe11:b115/64
net1/v6       addrconf ok       fe80::203:baff:fe11:b116/10
net1/v6a     static    ok       2001:db8:3c4d:16:203:baff:fe11:b116/64
```

출력에서 IPv6용으로 구성된 각 인터페이스가 이제 두 개의 주소를 사용합니다. *interface/v6*과 같은 주소 객체 이름을 포함하는 항목에는 해당 인터페이스에 대한 링크 로컬 주소가 표시됩니다. *interface/v6a*와 같은 주소 객체 이름을 포함하는 항목에는 전역 IPv6 주소가 표시됩니다. 인터페이스 ID 이외에도 이 주소에는 /etc/ndpd.conf 파일에 구성된 사이트 접두어가 포함됩니다. v6a 대상은 무작위로 정의된 문자열입니다. *interface*가 IPv6 주소를 만들려는 인터페이스(예: net0/mystring, net0/ipv6addr)를 나타내는 경우, 다른 문자열을 정의하여 주소 객체 이름의 두번째 부분을 구성할 수 있습니다.

- 참조
- IPv6 네트워크 토폴로지에서 식별한 라우터에서 터널을 구성하는 방법에 대한 자세한 내용은 “Oracle Solaris 11.2의 TCP/IP 네트워크, IPMP 및 IP 터널 관리”의 “IP 터널 관리”를 참조하십시오.
 - 네트워크에서 스위치 및 허브 구성에 대한 자세한 내용은 제조업체의 설명서를 참조하십시오.
 - 서버에서 IPv6 지원을 향상시키는 방법에 대한 자세한 내용은 “Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리”의 “서버에서 IPv6 사용 인터페이스 구성”을 참조하십시오.

◆◆◆ 3 장 3

VRRP(Virtual Router Redundancy Protocol) 사용

네트워크 안정성을 높이는 한 가지 방법은 네트워크의 중요한 구성 요소에 대해 백업을 제공하는 것입니다. Oracle Solaris에서는 고가용성을 제공하기 위해 VRRP(Virtual Router Redundancy Protocol)의 사용을 구성하고 관리하는 관리 도구를 제공합니다. VRRP는 [RFC 5798](http://www.rfc-editor.org/rfc/rfc5798.txt) (<http://www.rfc-editor.org/rfc/rfc5798.txt>)에서 지정된 인터넷 표준 프로토콜입니다.

Oracle Solaris 11.2에서는 IPMP 및 InfiniBand 인터페이스를 통한 VRRP 라우터 만들기를 지원하고 영역에서 VRRP에 대한 기존 지원을 향상시키는 독자적인 Layer 3 VRRP를 제공합니다.

참고 - 이 장에서 L2 VRRP(Layer 2 VRRP) 용어에 대한 모든 언급은 구체적으로 인터넷 표준 VRRP를 가리키고, L3 VRRP(Layer 3 VRRP) 용어에 대한 모든 언급은 독자적인 Oracle Solaris Layer 3 VRRP를 가리킵니다.

이 장에서는 Layer 2 VRRP 및 Oracle Solaris의 독자적인 Layer 3 VRRP에 대한 개요를 제공합니다.

이 장의 내용:

- “VRRP 정보” [23]
- “VRRP 작동 방식” [24]
- “Layer 3 VRRP 기능 정보” [26]
- “Layer 2 및 Layer 3 VRRP 비교” [26]
- “Layer 2 및 Layer 3 VRRP 제한 사항” [28]

VRRP 정보

VRRP는 라우터 또는 로드 밸런서에 주로 사용되는 IP 주소의 고가용성을 제공합니다. 서비스에서 로드 균형 조정과 같이 경로 지정 이외의 기능을 제공하더라도 VRRP를 사용하는 서

비스는 VRRP 라우터라고도 합니다. VRRP가 고가용성을 위해 로드 밸런서와 함께 어떻게 사용되는지에 대한 자세한 내용은 [7장. 고가용성을 위한 ILB 구성](#)을 참조하십시오.

VRRP 라우터는 VRRP를 실행 중인 라우터입니다. VRRP는 각 VRRP 라우터에서 실행되며 라우터의 상태를 관리합니다. 한 호스트에 VRRP가 구성된 여러 라우터가 있을 수 있으며, 각 라우터는 서로 다른 가상 라우터에 속합니다. VRRP를 사용하면 LAN에서 가상 라우터를 사용할 수 있으므로 라우터에 대한 오류 복구가 가능합니다.

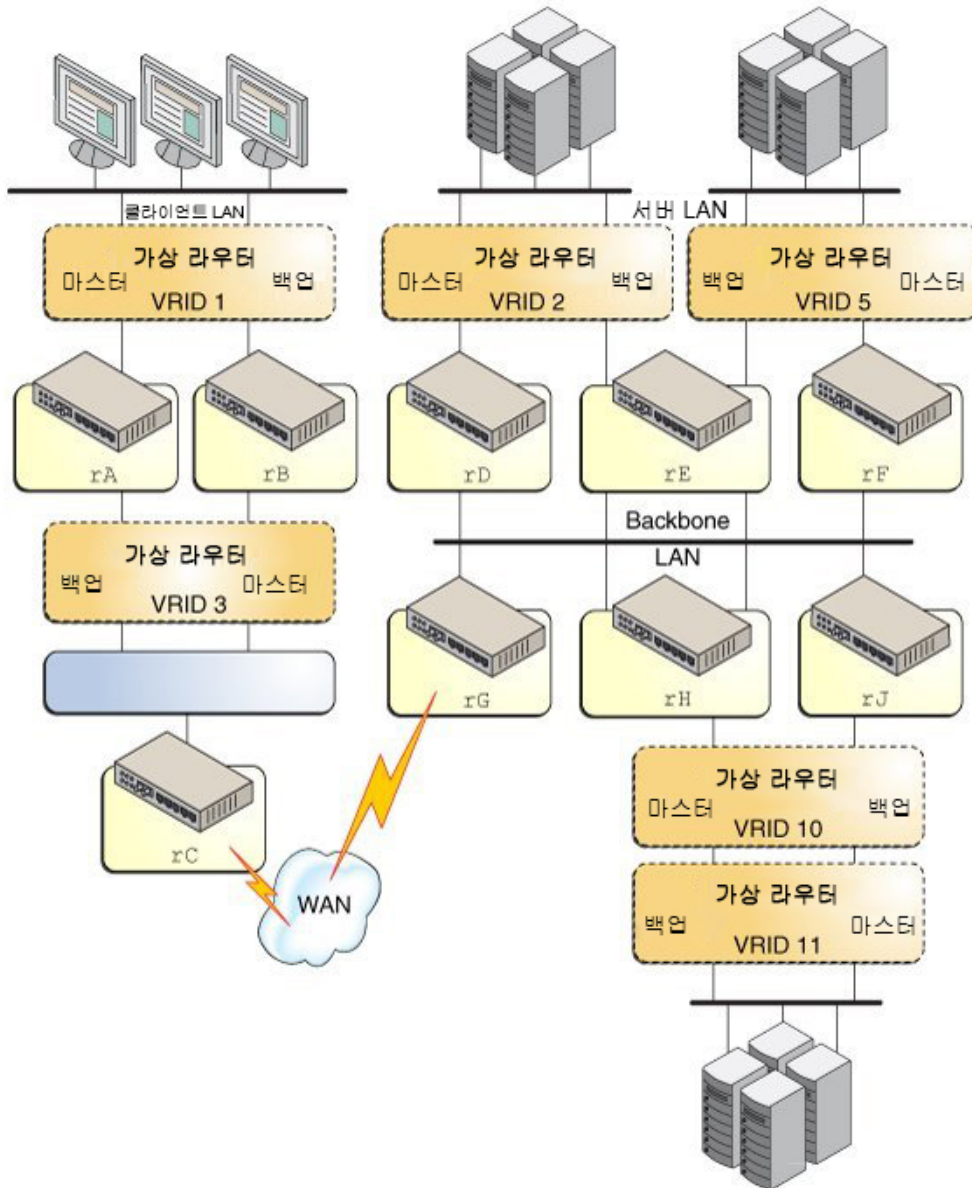
VRRP 작동 방식

다음 VRRP 라우터 용어를 알아 두십시오.

- 라우터 이름 - 시스템 전체 고유 식별자.
- VRID(가상 라우터 ID) - 지정된 네트워크 세그먼트에서 가상 라우터를 식별하는 데 사용되는 고유한 숫자입니다. VRID는 LAN 내에서 가상 라우터를 식별합니다.
- 기본 IP 주소 - VRRP 공개의 소스 IP 주소입니다.
- VRIP(가상 IP 주소) - 다른 호스트가 네트워크 서비스를 가져오는 VRID와 연결된 IP 주소입니다. VRIP는 VRID에 속한 VRRP 인스턴스에 의해 관리됩니다.
- 마스터 라우터 - 제공된 시간에 가상 라우터에 대한 경로 지정 기능을 수행하는 VRRP 인스턴스입니다. 지정된 VRID에 대한 마스터 라우터는 한 번에 하나만 활성 상태일 수 있습니다. 마스터 라우터는 가상 라우터와 연관된 IPv4 또는 IPv6 주소를 제어합니다. 가상 라우터는 마스터 라우터의 IP 주소로 전송된 패킷을 전달합니다.
- 백업 라우터 - 활성이지만 마스터 상태가 아닌 VRID에 대한 VRRP 인스턴스를 백업 라우터라고 합니다. VRID에 대해 여러 개의 백업 라우터가 존재할 수 있습니다. 현재 마스터 라우터에서 오류가 발생할 경우 백업 라우터가 마스터 라우터 역할을 맡습니다.
- VRRP 매개변수 - 우선 순위, 공개 간격, 선취 모드 및 승인 모드를 포함합니다.
- VRRP 상태 정보 및 통계.

다음 VRRP 로드 공유 구성 그림은 하나의 라우터 인터페이스에 여러 개의 VRID가 있을 수 있음을 보여줍니다. 부연 텍스트는 그림에 사용된 VRRP 구성 요소에 대한 설명입니다. 이러한 VRRP 로드 공유 구성은 여러 VRID가 하나의 라우터 인터페이스에 있을 수 있음을 나타냅니다.

그림 3-1 LAN에서 VRRP의 로드 공유 구성



- 라우터 rA는 가상 라우터 VRID 1의 마스터 라우터이며 VRID 3의 백업 라우터입니다. 라우터 rA는 VRID 1의 가상 IP(VIP) 주소에 지정된 패킷의 경로 지정을 처리하며 VRID 3에 대해 경로 지정 역할을 맡습니다.
- 라우터 rB는 가상 라우터 VRID 3의 마스터 라우터이며 VRID 1의 백업 라우터입니다. 라우터 rB는 VRID 3의 VIP로 주소가 지정된 패킷의 경로 지정을 처리하고 VRID 1의 경로 지정 역할을 맡을 준비가 되어 있습니다.
- 라우터 rC에는 VRRP 기능이 없으나 VRID 3의 VIP를 사용하여 클라이언트 LAN 서브넷에 접속합니다.
- 라우터 rD는 VRID 2의 마스터 라우터입니다. 라우터 rF는 VRID 5의 마스터 라우터입니다. 라우터 rE는 이러한 두 VRID의 백업 라우터입니다. rD 또는 rF에서 오류가 발생하면 rE는 해당 VRID의 마스터 라우터가 됩니다. rD 및 rF 둘 다 동시에 실패할 수 있습니다. VRRP 라우터는 하나 이상의 VRID에 대한 마스터 라우터가 될 수 있습니다.
- 라우터 rG는 중추 LAN의 WAN(원거리 통신망) 게이트웨이입니다. 중추에 연결된 모든 라우터는 OSPF와 같은 동적 경로 지정 프로토콜을 사용하여 WAN에 있는 라우터와 경로 지정 정보를 공유합니다. 라우터 rC에서 클라이언트 LAN 서브넷에 대한 경로가 VRID 3의 VIP를 경유한다고 공개하는 경우에도 VRRP는 이 작업에 관련되지 않습니다.
- 라우터 rH는 VRID 10의 마스터 라우터이며 VRID 11의 백업 라우터입니다. 마찬가지로 라우터 rJ는 VRID 11의 마스터 라우터이며 VRID 10의 백업 라우터입니다.

Layer 3 VRRP 기능 정보

Oracle Solaris에서 독자적인 L3 VRRP(Layer 3 Virtual Router Redundancy Protocol) 기능은 VRRP 라우터에 대해 고유한 VRRP 가상 MAC 주소를 구성해야 할 필요가 전혀 없도록 해주고 IPMP 및 InfiniBand 인터페이스를 통한 더 향상된 VRRP 지원과 영역에서 VRRP 지원을 제공합니다. L3 VRRP 프로토콜은 표준 VRRP 사양을 준수하지 않습니다. 동일한 가상 라우터에 있는 VRRP 라우터 사이에서 고유한 가상 MAC 주소를 사용하는 대신 L3 VRRP 구현에서는 불필요한 ARP(Address Resolution Protocol) 메시지 및 NDP(Neighbor Discovery Protocol) 메시지를 사용하여 현재 마스터 VRRP 라우터의 가상 IP 주소와 MAC 주소간 매핑을 새로 고칩니다.

Layer 3 VRRP는 IPMP 및 InfiniBand 인터페이스를 통한 VRRP 지원과 영역에서 더 향상된 지원을 제공하고, VRRP VNIC를 만들어야 하는 필요도 없습니다.

Layer 2 및 Layer 3 VRRP 비교

다음 표에서는 Layer 2 및 Layer 3 VRRP에 대한 비교를 제공합니다.

표 3-1 Layer 2 및 Layer 3 VRRP 비교

기능	Layer 2 VRRP	Layer 3 VRRP
VRRP VNIC 만들기	VRRP VNIC를 만들어야 합니다.	VRRP VNIC에서 제공하는 가상 VRRP MAC 주소가 필요하지 않으므로 VRRP VNIC를 만들 필요가 없습니다.
IPMP 지원	지원되지 않습니다.	지원됩니다. Layer 3 VRRP 라우터가 IPMP 그룹 인터페이스를 통해 만들어진 경우, 마스터 라우터의 각 가상 IP 주소는 기존 IPMP 정책에 따라 활성 IPMP 기본 인터페이스의 MAC 주소와 연관됩니다. IPMP 그룹에서 페일오버가 발생하는 경우 불필요한 ARP 또는 NDP 메시지를 사용하여 L2 또는 L3 매핑이 알려집니다.
영역 지원	서로 다른 영역에서 동일한 가상 라우터에 속하는 여러 VRRP 라우터를 실행하는 문제입니다. 동일한 VRRP 가상 MAC 주소를 공유하는 둘 이상의 VRRP 라우터가 있는 시스템에서는 내장된 가상 스위치가 VRRP 라우터로 VRRP 알림 패킷의 정상적인 플로우를 방해합니다. 자세한 내용은 "Layer 2 및 Layer 3 VRRP 제한 사항" [28] 을 참조하십시오.	지원됩니다.
Infini Band 지원	지원되지 않습니다.	지원됩니다.
고유한 가상 라우터 MAC 주소	고유한 가상 라우터 MAC 주소가 필요합니다. 가상 IP 주소는 항상 동일한 가상 MAC 주소로 분석됩니다.	필요하지 않습니다. VRRP 라우터가 만들어진 MAC 주소를 사용합니다. MAC 주소는 동일한 가상 라우터에 있는 모든 VRRP 라우터마다 서로 다릅니다. 동일한 MAC 주소는 이 L3 VRRP 라우터로 보호되는 가상 IP 주소와 연관됩니다.
VRRP 가상 IP 주소 구성	구성해야 합니다.	구성해야 합니다.
ICMP(Internet Control Message Protocol) 재지정	L2 VRRP가 라우터 그룹 사이에서 실행 중일 때 사용될 수 있습니다. L2 VRRP 라우터가 ICMP 재지정을 사용해야 하는 경우 재지정해야 하는 패킷의 대상 MAC 주소(VRRP 가상 MAC 주소)를 확인합니다. 대상 MAC 주소를 사용함으로써 L2 VRRP 라우터는 패킷을 처음에 보낸 가상 라우터를 확인합니다. 이에 따라 L2 VRRP 라우터는 소스 주소를 선택하고 ICMP 재지정 메시지를 소스에 보낼 수 있습니다.	ICMP 재지정을 사용 안함으로 설정해야 합니다. 여러 VRRP 라우터가 동일한 인터페이스를 통해 만들어진다면 동일한 MAC 주소를 공유합니다. 따라서 L3 VRRP는 대상 MAC 주소를 확인할 수 없습니다.
마스터 라우터 선택	마스터 라우터 선택이 호스트에 투명하게 이루어 집니다. 마스터 라우터가 변경될 경우 호스트와 라우터 사이에 존재하는 스위치가 MAC 학습 기능을 사용하여 트래픽을 보낼 새로운 포트를 식별합니다.	마스터 라우터를 선택하면 가상 IP 주소의 Layer 2 매핑이 변경되고 새로운 매핑을 불필요한 ARP 또는 NDP 메시지로 알려야 합니다.
페일오버 시간	보통입니다.	마스터 라우터 선택이 바뀌면 불필요한 ARP 또는 NDP 메시지의 추가 요구 사항으로 인해 더 길어질 수 있습니다.

Layer 2 및 Layer 3 VRRP 제한 사항

Layer 2 및 Layer 3 VRRP에는 모두 Layer 2 및 Layer 3 VRRP 가상 IP 주소를 정적으로 구성해야 한다는 공통적인 제한 사항이 있습니다. IP 주소에 대한 두 개의 기존 자동 구성 도구인 `in.ndpd`(IPv6 자동 구성의 경우) 및 `dhcpagent`(DHCP(Dynamic Host Configuration Protocol) 구성의 경우)를 사용하여 VRRP 가상 IP 주소를 자동으로 구성할 수 없습니다. 또한 Layer 2 및 Layer 3 VRRP에는 특정 제한 사항이 있습니다.

Layer 2 VRRP 기능에는 다음과 같은 제한 사항이 있습니다.

■ 배타적 IP 영역 지원

VRRP 라우터가 배타적 IP 영역에서 만들어지면 VRRP 서비스 `svc:/network/vrrp/default`가 자동으로 사용으로 설정됩니다. VRRP 서비스는 이러한 특정 영역에 대한 VRRP 라우터를 관리합니다. 그러나 배타적 IP 영역에 대한 지원은 다음과 같이 제한됩니다.

- VNIC(Virtual Network Interface Card)는 비전역 영역 내부에 만들 수 없으므로 먼저 전역 영역에 VRRP VNIC를 만들어야 합니다. 그런 다음 VRRP 라우터가 상주하는 비전역 영역에 VNIC를 지정합니다. 그러면 `vrrpadm` 명령을 사용하여 비전역 영역에서 VRRP 라우터를 만들 수 있습니다.
- 단일 Oracle Solaris 시스템에서 동일한 가상 라우터에 참가할 두 개의 VRRP 라우터를 서로 다른 영역에 만들 수 없습니다. Oracle Solaris에서는 동일한 MAC(media access control) 주소를 가지는 두 개의 VNIC를 만들도록 허용하지 않습니다.

■ 다른 네트워크 기능과의 상호 작업

- L2 VRRP 서비스는 IPMP(IP Network Multipathing) 인터페이스에서 작동할 수 없습니다. VRRP에는 특정 VRRP MAC 주소가 필요하지만 IPMP는 IP 층에서 완전하게 작동합니다. IPMP에 대한 자세한 내용은 [“Oracle Solaris 11.2의 TCP/IP 네트워크, IPMP 및 IP 터널 관리”의 2 장](#), [“IPMP 관리 정보”](#)를 참조하십시오.

VRRP는 트렁크의 링크 통합 또는 DLMP 통합 모드에서 사용할 수 있습니다. 통합에 대한 자세한 내용은 [“Oracle Solaris 11.2의 네트워크 데이터 링크 관리”의 2 장](#), [“링크 집계를 사용하여고가용성 구성”](#)을 참조하십시오.

- L2 VRRP 서비스는 IPoIB(IP over Infiniband) 인터페이스에서 작동할 수 없습니다.

■ EoIB(Ethernet Over InfiniBand) 지원

L2 VRRP는 EoIB(Ethernet Over InfiniBand) 인터페이스를 지원하지 않습니다. 모든 L2 VRRP 라우터는 고유한 가상 MAC 주소와 연관되므로 동일한 가상 라우터에 참가하는 VRRP 라우터는 동일한 가상 MAC 주소를 동시에 사용해야 하는데, 이것이 EoIB 인터페이스에서 지원되지 않습니다. L3 VRRP는 동일한 가상 라우터에 존재하는 모든 VRRP 라우터 사이에서 서로 다른 MAC 주소를 사용함으로써 이 제한 사항을 극복합니다.

Layer 3 VRRP 기능에는 다음과 같은 제한 사항이 있습니다.

- 불필요한 ARP 또는 NDP 메시지를 사용하면 마스터 라우터 선택 중 페일오버 시간이 더 길어질 수 있습니다.

마스터 라우터 선택이 바뀔 경우 L3 VRRP는 불필요한 ARP 또는 NDP 메시지를 사용하여 새로운 L2 또는 L3 매핑을 알립니다. 불필요한 ARP 또는 NDP 메시지를 사용해야 하

는 추가 요구 사항으로 인해 페일오버 시간이 더 길어질 수 있습니다. 경우에 따라 모든 알려진 불필요한 ARP 또는 NDP 메시지가 손실된 경우 호스트가 새로 고쳐진 ARP 또는 NDP 항목을 검색하려면 더 많은 시간이 소요될 수 있습니다. 따라서 새 마스터 라우터로 패킷 전송이 지연될 수 있습니다.

- ICMP 재지정을 사용하는 경우 동일한 대상 MAC 주소가 여러 라우터에서 공유되므로 대상 MAC 주소를 확인할 수 없습니다.

대칭이 아닌 네트워크 토폴로지의 라우터 그룹 사이에서 VRRP를 사용하는 경우 ICMP 재지정을 사용할 수 있습니다. ICMPv4 재지정 또는 ICMPv6 재지정의 IPv4 또는 IPv6 소스 주소는 다음 홉 경로 지정 결정을 내릴 때 마지막 호스트에서 사용한 주소여야 합니다.

L3 VRRP 라우터가 ICMP 재지정을 사용해야 하는 경우 L3 VRRP 라우터가 재지정해야 하는 패킷의 대상 MAC 주소(VRRP 가상 MAC 주소)를 확인합니다. 동일한 인터페이스를 통해 만들어진 여러 라우터에서 동일한 대상 MAC 주소가 공유되므로 L3 VRRP 라우터가 대상 MAC 주소를 확인할 수 없습니다. 따라서 L3 VRRP 라우터를 사용할 때는 ICMP 재지정을 사용 안함으로 설정하는 것이 좋습니다. `send_redirects` 공용 IPv4 및 IPv6 프로토콜 등록 정보를 다음과 같이 사용하여 ICMP 재지정을 사용 안함으로 설정할 수 있습니다.

```
# ipadm set-prop -m ipv4 -p send_redirects=off
```

- VRRP 가상 IP 주소는 `in.ndpd` 또는 DHCP로 자동으로 구성할 수 없습니다.

◆◆◆ 4 장

VRRP(Virtual Router Redundancy Protocol) 구성 및 관리

이 장에서는 Layer 2 및 Layer 3 VRRP 구성 작업을 설명합니다.

이 장의 내용:

- “VRRP 구성 계획” [31]
- “VRRP 설치” [31]
- “VRRP 구성” [32]
- “사용 사례: Layer 2 VRRP 라우터 구성” [40]

VRRP 구성 계획

Layer 2 또는 Layer 3 VRRP 구성 계획에는 다음 단계가 포함됩니다.

1. L2 VRRP 또는 L3 VRRP 라우터를 구성할지 결정합니다.
2. (L2 VRRP 라우터만 해당) VRRP VNIC를 만듭니다. 자세한 내용은 “Layer 2 VRRP에 대한 VRRP VNIC 만들기” [32]를 참조하십시오.
L2 VRRP 라우터를 만들 때 `vrrpadm` 명령의 `-f` 옵션을 사용하면 VRRP VNIC를 자동으로 만들 수 있습니다.
3. VRRP 라우터를 만듭니다. 자세한 내용은 “VRRP 라우터 만들기” [33]를 참조하십시오.
4. VRRP 라우터에 대한 가상 IP 주소를 구성합니다. 자세한 내용은 “Layer 2 및 Layer 3 VRRP 라우터에 대한 가상 IP 주소 구성” [35]을 참조하십시오.
`vrrpadm` 명령의 `-a` 옵션을 사용하여 가상 IP 주소를 구성할 수 있습니다. 자세한 내용은 “VRRP 라우터 만들기” [33]를 참조하십시오.

VRRP 설치

시스템에서 VRRP를 사용하려면 VRRP를 설치해야 합니다.

▼ VRRP를 설치하는 방법

1. 관리자로 로그인합니다.
자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “지정된 관리 권한 사용”을 참조하십시오.
2. VRRP 패키지가 설치되었는지 확인합니다.

```
# pkg info vrrp
```
3. 설치되지 않은 경우 VRRP 패키지를 설치합니다.

```
# pkg install vrrp
```

VRRP 구성

vrrpadm 명령을 사용하여 VRRP 라우터를 구성할 수 있습니다. vrrpadm show-router 명령을 제외한 vrrpadm 명령의 모든 하위 명령 결과는 보존됩니다. 예를 들어, vrrpadm create-router 명령으로 만들어진 VRRP 라우터는 재부트 이후에도 지속됩니다. 자세한 내용은 [vrrpadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

VRRP 라우터를 구성하려면 Network Management 프로파일의 일부인 solaris.network.vrrp 권한 부여가 필요합니다.

참고 - vrrpadm show-router 명령으로 시작된 읽기 전용 작업에는 solaris.network.vrrp 권한 부여가 필요하지 않습니다.



주의 - Oracle Solaris 번들 IP 필터와 함께 VRRP를 사용하는 경우 ipfstat -io 명령을 사용하여 표준 VRRP 멀티캐스트 주소 224.0.0.18/32에 대해 들어오거나 나가는 IP 트래픽이 허용되는지 여부를 확인해야 합니다. 트래픽이 허용되지 않는 경우 마스터 및 백업 VRRP 라우터는 둘 다 MASTER 상태가 됩니다. 따라서 각 VRRP 라우터에 대한 IP 필터 구성에 해당하는 규칙을 추가해야 합니다. 자세한 내용은 “Oracle Solaris 11.2의 네트워크 관리 문제 해결”의 “VRRP 및 Oracle Solaris에 번들된 IP 필터 관련 문제 해결”을 참조하십시오.

Layer 2 VRRP에 대한 VRRP VNIC 만들기

VNIC는 시스템의 물리적 네트워크 어댑터 위에 구성된 가상 네트워크 인터페이스이며 네트워크 가상화의 필수 구성 요소입니다. 물리적 인터페이스에는 VNIC가 여러 개 있을 수 있습니다.

니다. VNIC에 대한 자세한 내용은 [“Oracle Solaris 11.2의 네트워크 가상화 및 네트워크 리소스 관리”](#)를 참조하십시오.

각 Layer 2 VRRP 라우터에는 특수한 VRRP VNIC가 필요합니다. 다음 명령 구문을 사용하십시오.

```
# dladm create-vnic [-t] [-R root-dir] -l link [-m vrrp -V VRID -A \
{inet | inet6}] [-v VLAN-ID] [-p prop=value[,...]] VNIC
```

이 명령은 VRRP 사양으로 정의된 가상 라우터 MAC 주소로 VNIC를 만듭니다. VNIC 주소 유형 `vrrp`를 사용하여 VRID 및 주소 그룹을 지정합니다. 주소 그룹은 IPv4 또는 IPv6 주소를 가리키는 `inet` 또는 `inet6`입니다. 예:

```
# dladm create-vnic -m vrrp -V 21 -A inet6 -l net0 vnic0
```

자세한 내용은 [dladm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

참고 - `vrrpadm` 명령과 함께 `-f` 옵션을 사용하여 VRRP VNIC를 만들 수도 있습니다. 자세한 내용은 [“VRRP 라우터 만들기” \[33\]](#)를 참조하십시오.

VRRP 라우터 만들기

`vrrpadm create-router` 명령은 지정된 VRID 및 주소 그룹을 다른 지정된 매개변수와 함께 사용하여 Layer 2 또는 Layer 3 VRRP 라우터를 만듭니다. 자세한 내용은 [vrrpadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

VRRP 라우터를 만들려면 다음 구문을 사용합니다.

```
# vrrpadm create-router [-T {l2 | l3}] [-f] -v VRID -I ifname \
-A [inet | inet6] [-a assoc-IPaddress] [-P primary-IPaddress] \
[-p priority] [-i adv-interval] [-o flags] router-name
```

`-T l2 | l3` 라우터의 유형을 지정합니다. 유형을 다음 값 중 하나로 설정할 수 있습니다. 기본값은 `l2`입니다.

- `l2` - L2 유형 VRRP 라우터
- `l3` - L3 유형 VRRP 라우터

`-f` (L2 VRRP만 해당) L2 VRRP 라우터와 함께 VRRP VNIC 만들기를 지정합니다. `-f` 옵션을 지정할 경우 `vrrpadm` 명령은 지정된 VRID 및 주소 그룹으로 VRRP VNIC가 존재하는지 여부를 확인합니다. VRRP VNIC가 존재하지 않을 경우에만 만들어집니다. 시스템은 이름 지정 규칙 `vrrp-VRID_ifname_v4 | 6`을 사용하여 VRRP VNIC의 이름을 생성합니다. Layer 3 VRRP 라우터를 만들 경우에는 `-f` 옵션은 소용이 없습니다.

-v VRID	주소 그룹과 연관된 경우 VLAN을 정의하는 가상 라우터 식별자입니다.
-I ifname	VRRP 라우터가 구성되는 인터페이스입니다. Layer 2 VRRP의 경우, 인터페이스는 물리적 링크, VLAN 또는 통합이 될 수 있습니다. Layer 3 VRRP의 경우, 인터페이스에는 IPMP 인터페이스, DHCP 관리 인터페이스 및 InfiniBand 인터페이스도 포함될 수 있습니다. 이 링크는 이 VRRP 라우터가 실행 중인 LAN을 결정합니다.
-A [inet inet6]	IPv4 또는 IPv6 주소를 가리키는 inet 또는 inet6 주소 그룹입니다.
-a assoc-IPaddress	<p>심표로 구분된 IP 주소 목록을 지정합니다. IP 주소는 다음 형식으로 지정할 수 있습니다.</p> <ul style="list-style-type: none"> ■ IP-address[/prefix-length] ■ hostname[/prefix-length] ■ linklocal <p>linklocal을 지정할 경우, IPv6 link-local vrrp 주소가 연관된 가상 라우터의 VRID를 기준으로 구성됩니다. linklocal 형식은 IPv6 VRRP 라우터에만 적용됩니다. -a 옵션과 -f 옵션을 함께 사용하면 VNIC가 자동으로 만들어지고 연결되도록 할 수 있습니다.</p>
-p primary-IPaddress	VRRP 알림을 보내는 데 사용되는 VRRP 기본 IP 주소를 지정합니다.
-p priority	마스터 선택을 위해 사용되는 지정된 VRRP 라우터의 우선 순위입니다. 기본값은 255입니다. 우선 순위 값이 가장 높은 라우터가 마스터 라우터로 선택됩니다.
-i adv-interval	알림 간격(밀리초)입니다. 기본값은 1000입니다.
-o flags	VRRP 라우터의 선취 및 승인 모드입니다. 값은 preempt 또는 un_preempt, 또는 accept 또는 no_accept일 수 있습니다. 기본적으로 선취 및 승인 모드는 각각 preempt 및 accept로 설정됩니다.
router-name	router-name 은 이 VRRP 라우터의 고유한 식별자입니다. 라우터 이름에 허용되는 문자는 영숫자(a-z, A-Z, 0-9) 및 밑줄('_')입니다. 라우터 이름의 최대 길이는 31자입니다.

예 4-1 Layer 2 VRRP 라우터 만들기

다음 예에서는 데이터 링크 net0을 통해 라우터를 만드는 방법을 보여줍니다.

```
# dladm create-vnic -m vrrp -V 12 -A inet -l net0 vnic1
# vrrpadm create-router -V 12 -A inet -p 100 -I net0 l2router1
# vrrpadm show-router l2router1
```

```
NAME      VRID  TYPE  IFNAME AF   PRIO ADV_INTV MODE  STATE  VNIC
l2router1 12   L2    net0  IPv4 100  1000   e-pa- BACK  vnic1
```

L2 VRRP 라우터 l2router1은 IPv4 주소 그룹 및 VRID 12를 사용하여 데이터 링크 net0을 통해 만들어집니다. vrrpadm show-router 명령에 대한 자세한 내용은 “[Layer 2 및 Layer 3 VRRP 라우터 구성 표시](#)” [37]를 참조하십시오.

예 4-2 Layer 3 VRRP 라우터 만들기

다음 예에서는 ipmp0이라는 IPMP 인터페이스를 통해 L3 VRRP 라우터를 만드는 방법을 보여줍니다.

```
# vrrpadm create-router -V 6 -I ipmp0 -A inet -T l3 l3router1
# vrrpadm show-router
NAME      VRID  TYPE  IFNAME AF   PRIO ADV_INTV MODE  STATE  VNIC
l3router1 6     L3    ipmp0 IPv4 255  1000   eopa- INIT  --
```

L3 VRRP 라우터 l3router1은 IPv4 주소 그룹 및 VRID 6을 사용하여 IPMP 인터페이스 ipmp0을 통해 만들어집니다. vrrpadm show-router 명령에 대한 자세한 내용은 “[Layer 2 및 Layer 3 VRRP 라우터 구성 표시](#)” [37]를 참조하십시오.

Layer 2 및 Layer 3 VRRP 라우터에 대한 가상 IP 주소 구성

L2 VRRP 라우터에 대한 IP 주소를 구성하려면 연관된 VRRP VNIC를 통해 vrrp 유형의 가상 IP 주소를 구성해야 합니다.

L3 VRRP 라우터에 대한 가상 IP 주소를 구성하려면 L3 VRRP 라우터가 구성된 동일한 IP 인터페이스에서 vrrp 유형의 IP 주소를 사용해야 합니다.

참고 - IPv6 주소를 구성하려면 VRRP VNIC 또는 L3 VRRP 라우터의 주소 그룹을 inet6로 지정하여 라우터를 만들었어야 합니다.

VRRP 라우터에 대한 가상 IP 주소를 구성하려면 다음 구문을 사용합니다.

```
# ipadm create-addr [-t] -T vrrp [-a local=addr[/prefix-length]] \
  [-n router-name].... addr-obj | interface
```

-t 구성된 주소가 임시이며 활성 구성에만 변경 사항이 적용되도록 지정합니다.

-T vrrp 구성된 주소가 vrrp 유형이 되도록 지정합니다.

`-n router-name` VRRP 라우터 이름은 IP 주소가 구성된 VRRP VNIC 인터페이스에서 파생될 수 있으므로 `-n router-name` 옵션은 L2 VRRP 라우터에 대해 선택 사항입니다.

자세한 내용은 [ipadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

참고 - `vrrpadm` 명령과 함께 `-a` 옵션을 사용하여 가상 IP 주소를 구성할 수도 있습니다. 자세한 내용은 “[VRRP 라우터 만들기](#)” [33]를 참조하십시오.

예 4-3 L2 VRRP 라우터에 대한 가상 IP 주소 구성

`vrrp` 유형 IP 주소를 사용하여 L2 VRRP 라우터에 대한 가상 IP 주소를 구성할 수 있습니다. 다음 예에서는 `l2router1`에 대한 가상 IP 주소를 만드는 방법을 보여줍니다.

```
# ipadm create-ip vrrp_vnic1
# ipadm create-addr -T vrrp -n l2router1 -a 192.168.82.8/24 vrrp_vnic1/vaddr1
```

다음 예에서는 `V6vrrp_vnic1/vaddr1`에 대한 IPv6 link-local `vrrp` IP 주소를 만드는 방법을 보여줍니다.

```
# ipadm create-ip V6vrrp_vnic1
# ipadm create-addr -T vrrp V6vrrp_vnic1/vaddr1
```

VRRP 라우터에 대한 IPv6 link-local `vrrp` 유형 IP 주소를 구성하려면 로컬 주소를 지정할 필요가 없습니다. IPv6 link-local `vrrp` 유형 IP 주소는 연관된 VRRP 라우터의 VRID를 기준으로 만들어집니다.

예 4-4 L3 VRRP 라우터에 대한 가상 IP 주소 구성

다음 예에서는 `l3router1`에 대한 가상 IP 주소를 구성하는 방법을 보여줍니다.

```
# ipadm create-ip ipmp0
# ipadm create-addr -T vrrp -n l3router1 -a 172.16.82.8/24 ipmp0/vaddr1
```

다음 예에서는 L3 VRRP 라우터 `l3V6router1`에 대한 IPv6 link-local `vrrp` 유형 IP 주소를 구성하는 방법을 보여줍니다.

```
# ipadm create-ip ipmp1
# ipadm create-addr -T vrrp -n l3V6router1 ipmp1/vaddr0
```

VRRP 라우터 사용 및 사용 안함으로 설정

VRRP 라우터는 처음 만들 때 기본적으로 사용으로 설정됩니다. VRRP 라우터를 사용 안함으로 설정하고 다시 사용으로 설정할 수 있습니다. 라우터를 사용으로 설정하는 경우 VRRP 라

우터가 만들어진 인터페이스(vrrpadm create-router로 라우터를 만들 때 -I 옵션을 사용하여 지정됨)가 존재해야 합니다. 그렇지 않으면 사용으로 설정 작업이 실패합니다. L2 VRRP 라우터의 경우, 라우터의 VRRP VNIC가 존재하지 않으면 라우터는 소용이 없습니다. 구문은 다음과 같습니다.

```
# vrrpadm enable-router router-name
```

때로는 구성 변경을 위해 일시적으로 VRRP 라우터를 사용 안함으로 설정한 다음 라우터를 다시 사용으로 설정해야 할 수 있습니다. 라우터를 사용 안함으로 설정하기 위한 구문은 다음과 같습니다.

```
# vrrpadm disable-router router-name
```

VRRP 라우터 수정

vrrpadm modify-router 명령은 지정된 VRRP 라우터의 구성을 변경합니다. 라우터의 우선 순위, 알림 간격, 선취 모드 및 승인 모드를 수정할 수 있습니다. 구문은 다음과 같습니다.

```
# vrrpadm modify-router [-p priority] [-i adv-interval] [-o flags] router-name
```

Layer 2 및 Layer 3 VRRP 라우터 구성 표시

vrrpadm show-router 명령은 지정된 VRRP 라우터의 구성 및 상태를 표시합니다. 자세한 내용은 [vrrpadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오. 구문은 다음과 같습니다.

```
# vrrpadm show-router [-P | -x] [-p] [-o field[,...]] [router-name]
```

예 4-5 Layer 2 VRRP 라우터 구성 표시

다음 예에서는 vrrpadm show-router 명령 출력을 보여줍니다.

```
# vrrpadm show-router vrrp1
NAME VRID TYPE IFNAME AF PRIO ADV_INTV MODE STATE VNIC
vrrp1 1 L2 net1 IPv4 100 1000 e-pa- BACK vnic1
```

NAME VRRP 라우터의 이름입니다.

VRID VRRP 라우터의 VRID입니다.

TYPE VRRP 라우터의 유형(L2 또는 L3)입니다.

IFNAME VRRP 라우터가 구성되는 인터페이스입니다. L2 VRRP 라우터의 경우, 인터페이스는 물리적 이더넷 인터페이스, VLAN 또는 통합이 될 수 있습니다.

AF	VRRP 라우터의 주소 그룹입니다. IPv4 또는 IPv6일 수 있습니다.
PRIO	마스터 선택을 위해 사용되는 VRRP 라우터의 우선 순위입니다.
ADV_INTV	표시되는 알림 간격(밀리초)입니다.
MODE	VRRP 라우터와 연관된 플래그 세트이며 다음과 같은 값이 포함될 수 있습니다. <ul style="list-style-type: none"> ■ e - 라우터가 사용으로 설정되도록 지정합니다. ■ p - 모드가 preempt가 되도록 지정합니다. ■ a - 모드가 accept가 되도록 지정합니다. ■ o - 라우터가 가상 주소 소유자가 되도록 지정합니다.
STATE	VRRP 라우터의 현재 상태입니다. 가능한 값은 INIT(초기화), BACK(백업) 및 MAST(마스터)입니다.

이 예에서는 지정된 VRRP 라우터 vrrp1에 대한 정보가 표시됩니다.

```
# vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 BACK MAST 1m17s vnic1 10.0.0.100 10.0.0.1
```

PRV_STAT	VRRP 라우터의 이전 상태입니다.
STAT_LAST	마지막 상태 전환 이후 경과 시간입니다.
PRIMARY_IP	VRRP 라우터가 선택한 기본 IP 주소입니다.
VIRTUAL_IPS	VRRP 라우터에서 구성된 가상 IP 주소입니다.

이 예에서는 VRRP 라우터가 선택한 기본 IP 주소, VRRP 라우터에서 구성된 가상 IP 주소 및 VRRP 라우터의 이전 상태와 같은 라우터에 대한 추가 정보가 표시됩니다.

```
# vrrpadm show-router -P vrrp1
NAME PEER P_PRIO P_INTV P_ADV_LAST M_DOWN_INTV
vrrp1 10.0.0.123 120 1000 0.313s 3609
```

PEER	피어 VRRP 라우터의 기본 IP 주소입니다.
P_PRIO	피어 VRRP 라우터의 우선 순위이며, 피어로부터 수신된 알림의 일부입니다.
P_INTV	알림 간격(밀리초)이며, 피어로부터 수신된 알림의 일부입니다.
P_ADV_LAST	피어로부터 수신된 마지막 알림 이후 경과 시간입니다.
M_DOWN_INTV	마스터 라우터가 작동 중지로 선언된 이후 시간 간격(밀리초)입니다.

-P 옵션은 VRRP 라우터가 백업 상태일 때만 사용됩니다.

예 4-6 시스템에 L3 VRRP 라우터 표시

```
# vrrpadm show-router
NAME VRID TYPE IFNAME AF PRIO ADV_INTV MODE STATE VNIC
l3vr1 12 L3 net1 IPv6 255 1000 eopa- INIT -
```

이 예에서는 L3 VRRP 라우터 l3vr1이 net1 인터페이스를 통해 구성되었습니다.

VRRP 라우터와 연관된 IP 주소 표시

ipadm show-addr 명령을 사용하여 VRRP 라우터와 연관된 IP 주소를 표시할 수 있습니다. ipadm show-addr 명령 출력에서 ROUTER 필드에는 특정 vrrp 유형 IP 주소와 연관된 VRRP 라우터의 이름이 표시됩니다.

L2 VRRP의 vrrp 유형 IP 주소의 경우, VRRP 라우터의 이름은 IP 주소가 구성된 VRRP VNIC에서 파생됩니다. VRRP VNIC에 대한 L2 라우터를 만들기 전에 ipadm show-addr 명령을 실행할 경우 ROUTER 필드에는 ?가 표시됩니다. L3 VRRP의 vrrp 유형 IP 주소의 경우, ROUTER 필드에는 항상 지정된 라우터 이름이 표시됩니다. 기타 유형의 IP 주소의 경우, ROUTER 필드는 해당 사항이 없으며 --가 표시됩니다.

예 4-7 VRRP 라우터와 연관된 IP 주소 표시

```
# ipadm show-addr -o addrobj,type,vrrp-router,addr
ADDROBJ TYPE VRRP-ROUTER ADDR
lo0/v4 static -- 127.0.0.1/8
net1/p1 static -- 192.168.11.10/24
net1/v1 vrrp l3router1 192.168.81.8/24
vrrp_vnic1/vaddr1 vrrp l2router1 192.168.82.8/24
lo0/v6 static -- ::1/128
```

이 예에서는 l3router1이 vrrp 유형 IP 주소 192.168.81.8/24와 연관되고, l2router1이 vrrp 유형 IP 주소 192.168.82.8/24와 연관되었습니다.

출력에는 다음 정보가 표시됩니다.

ADDROBJ 주소 객체의 이름입니다.

TYPE 주소 객체의 유형이며, 다음 중 하나가 될 수 있습니다.

- from-gz
- static
- dhcp

- addrconf
- vrrp

VRRP-ROUTER VRRP 라우터의 이름입니다.

ADDR 숫자 IPv4 또는 IPv6 주소입니다.

VRRP 라우터 삭제

vrrpadm delete-router 명령은 지정된 VRRP 라우터를 삭제합니다. 구문은 다음과 같습니다.

```
# vrrpadm delete-router router-name
```

참고 - vrrpadm create-router 명령의 -f, -a, -P 옵션을 사용하여 각각 만들어진 VRRP VNIC, vrrp 유형 IP 주소 및 기본 IP 주소는 vrrpadm delete-router 명령의 결과로 삭제되지 않습니다. 해당하는 ipadm 및 dladm 명령을 사용하여 명시적으로 삭제해야 합니다.

불필요한 ARP 및 NDP 메시지 제어

백업 라우터가 마스터 VRRP 라우터가 되면 VRRP는 마스터 라우터와 연관된 모든 가상 IP 주소에 대해 플래그를 설정하여 가상 IP 주소를 보호합니다. 가상 IP 주소에 대한 충돌이 없을 경우 가상 IP 주소와 새로운 마스터의 MAC 주소 사이의 새로운 매핑을 알리기 위해 여러 불필요한 ARP 및 인접 알림 메시지가 보내집니다.

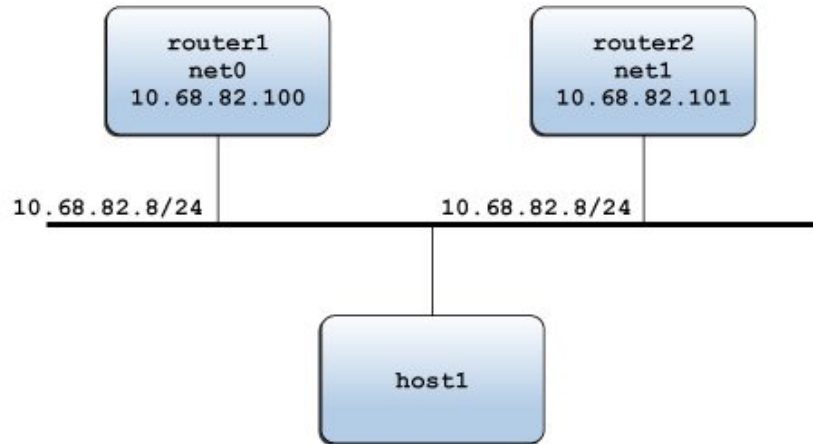
보내지는 메시지 수 및 메시지의 알림 간격을 제어하기 위해 다음과 같은 IP 프로토콜 등록 정보를 사용할 수 있습니다.

- arp_publish_count
- arp_publish_interval
- ndp_unsolicit_count
- ndp_unsolicit_interval

IP 프로토콜 등록 정보에 대한 자세한 내용은 [“Oracle Solaris 11.2 조정 가능 매개변수 참조 설명서”](#)의 [“중복 주소 검색과 관련된 IP 조정 가능 매개변수”](#)를 참조하십시오.

사용 사례: Layer 2 VRRP 라우터 구성

다음 그림은 일반 VRRP 구성을 보여줍니다.



이 예에서 IP 주소 10.68.82.8은 host1의 기본 게이트웨이로 구성됩니다. 이 IP 주소는 두 개의 VRRP 라우터(router1 및 router2)로 구성된 가상 라우터가 보호하는 가상 IP 주소입니다. 특정 시점에 두 라우터 중 하나만 가상 라우터의 책임을 맡고 host1에서 오는 패킷을 전달하는 마스터 라우터로 작동합니다.

가상 라우터의 VRID는 12라고 가정합니다. 다음 예는 router1 및 router2에서 VRRP 구성 예를 구성하는 데 사용되는 명령을 보여줍니다. router1은 가상 IP 주소 10.68.82.8의 소유자이며, 우선 순위는 기본값(255)입니다. router2는 우선 순위가 100인 대기 라우터입니다.

VRRP 구성에 사용되는 명령에 대한 자세한 내용은 [vrrpadm\(1M\)](#), [dladm\(1M\)](#), [ipadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

router1의 경우:

1. VRRP 패키지를 설치합니다.

```
# pkg install vrrp
```

2. VRID 값을 12로 사용하여 net0을 통해 VNIC vnic0을 만듭니다.

```
# dladm create-vnic -m vrrp -V 12 -A inet -l net0 vnic0
```

3. net0을 통해 VRRP 라우터 vrrp1을 만듭니다.

```
# vrrpadm create-router -V 12 -A inet -I net0 vrrp1
```

4. IP 인터페이스 vnic0 및 net0을 구성합니다.

```
# ipadm create-ip vnic0
```

```
# ipadm create-addr -T vrrp -a 10.68.82.8/24 vnic0/router1
```

```
# ipadm create-ip net0
```

```
# ipadm create-addr -T static -a 10.68.82.100/24 net0/router1
```

5. vrrp1에 대한 라우터 정보를 표시합니다.

```
# vrrpadm show-router -x vrrp1
```

```
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 MASTER INIT 14.444s vnic0 10.68.82.100 10.68.82.8
```

마찬가지로 router2의 경우:

1. VRID 값을 12로 사용하여 net1을 통해 VNIC vnic1을 만듭니다.

```
# dladm create-vnic -m vrrp -V 12 -A inet -l net1 vnic1
```

2. net1을 통해 VRRP 라우터 vrrp2를 만듭니다.

```
# vrrpadm create-router -V 12 -A inet -I net1 -p 100 vrrp2
```

3. vnic1 및 net1에 IP 인터페이스를 구성합니다.

```
# ipadm create-ip vnic1
```

```
# ipadm create-addr -T vrrp -a 10.68.82.8/24 vnic1/router2
```

```
# ipadm create-ip net1
```

```
# ipadm create-addr -T static -a 10.68.82.101/24 net1/router2
```

4. vrrp2에 대한 라우터 정보를 표시합니다.

```
# vrrpadm show-router -x vrrp2
```

```
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp2 BACKUP INIT 2m32s vnic1 10.68.82.101 10.68.82.8
```

router1의 구성을 예로 사용하여 net0을 통해 하나 이상의 IP 주소를 구성해야 합니다. router1의 이 IP 주소는 기본 IP 주소로, VRRP 알림 패킷을 전송하는 데 사용됩니다.

```
# vrrpadm show-router -x vrrp1
```

```
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 MASTER INIT 14.444s vnic1 10.68.82.100 10.68.82.8
```

◆◆◆ 5 장

통합 로드 밸런서 개요

이 장에서는 ILB 구성 요소의 구성 요소 및 ILB가 작동하는 모드(예: DSR(Direct Server Return) 모드 및 NAT(Network Address Translator) 모드)에 대해 설명합니다.

이 장의 내용:

- “ILB 구성 요소” [43]
- “ILB 작동 모드” [44]
- “ILB 작동 방식” [48]

ILB에 대한 자세한 내용은 “통합된 로드 밸런서 개요” [12]를 참조하십시오.

ILB 구성 요소

ILB는 SMF(서비스 관리 기능) 서비스 `svc:/network/loadbalancer/ilb:default`를 통해 관리됩니다. SMF에 대한 자세한 내용은 “Oracle Solaris 11.2의 시스템 서비스 관리”를 참조하십시오. ILB의 세 가지 주요 구성 요소는 다음과 같습니다.

- `ilbadm` 명령줄 인터페이스(CLI) - CLI를 사용하여 로드 균형 조정 규칙을 구성하고 선택적 상태 검사를 수행하고 통계를 볼 수 있습니다.
- `libilb` 구성 라이브러리 - `ilbadm` 및 타사 응용 프로그램에서 ILB 관리를 위해 `libilb`에 구현된 기능을 사용할 수 있습니다.
- `ilbd` 데몬 - 이 데몬은 다음 작업을 수행합니다.
 - 재부트 및 패키지 업데이트에서 지속 구성을 관리합니다
 - 구성 정보를 처리하고 실행을 위해 ILB 커널 모듈로 전송하여 ILB 커널 모듈에 대한 순차적 액세스를 제공합니다.
 - 로드 분배가 제대로 조정되도록 상태 검사를 수행하고 결과를 ILB 커널 모듈로 전송합니다.

ILB 작동 모드

ILB는 단일 각 및 이중 각 토폴로지에서 IPv4와 IPv6에 대해 Stateless DSR 및 NAT 작동 모드를 지원합니다.

DSR(Direct Server Return) 모드

DSR 모드에서 ILB는 백엔드 서버에 대한 수신 요청의 로드 균형을 조정하지만 서버에서 클라이언트로의 반환 트래픽이 로드 균형 조정을 무시할 수 있도록 합니다. 하지만 ILB가 백엔드 서버의 라우터로 사용되도록 설정할 경우 백엔드 서버가 클라이언트로 보낸 응답이 ILB를 실행하는 시스템을 통해 경로 지정됩니다. DSR의 현재 ILB 구현에서는 TCP 연결 추적을 제공하지 않아 Stateless가 됩니다. Stateless DSR을 사용할 경우 ILB는 기본 통계를 제외하고 처리된 패킷에 대한 상태 정보를 저장하지 않습니다. Stateless이므로 성능은 일반적인 IP 전달 성능과 유사합니다. DSR 모드는 비연결 프로토콜에 가장 적합합니다.

장점:

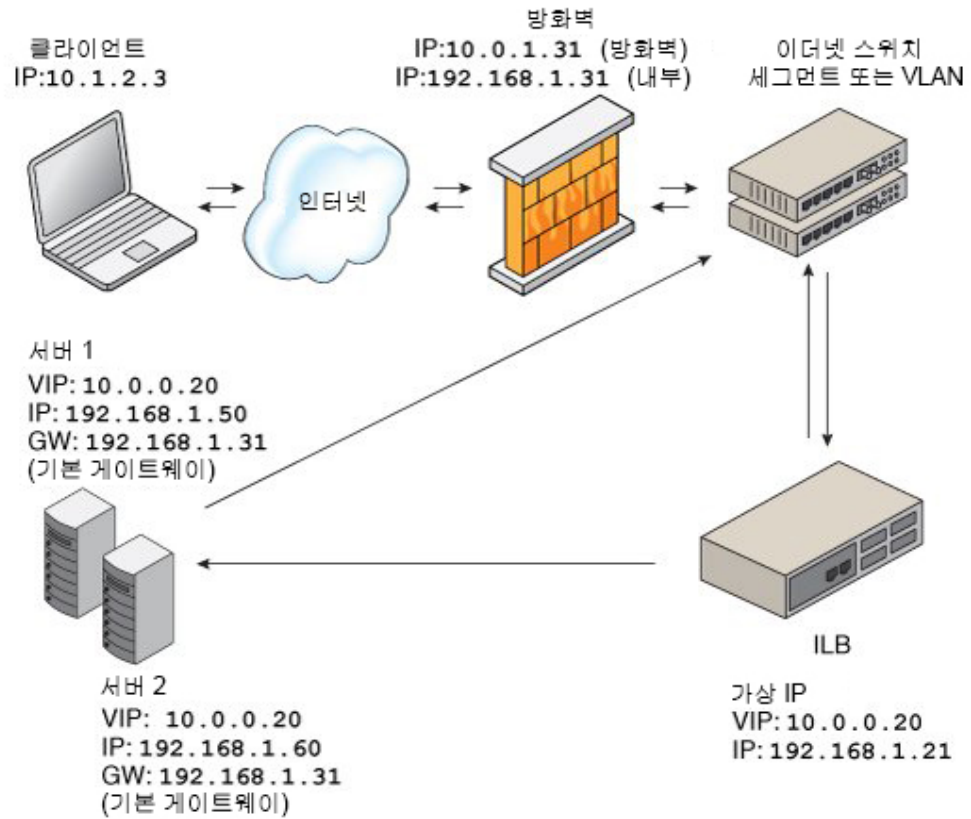
- 패킷의 대상 MAC 주소만 변경되고 서버가 직접 클라이언트에 응답하므로 DSR은 NAT 보다 성능이 뛰어납니다.
- 서버 및 클라이언트 간 투명성이 완전합니다. 서버가 클라이언트 IP 주소에서 직접 연결을 확인하고 기본 게이트웨이를 통해 클라이언트에 응답합니다.

단점:

- 백엔드 서버가 고유 IP 주소(상태 검사용)와 가상 IP 주소(로드 균형이 조정된 트래픽용)에 모두 응답해야 합니다.
- Stateless이므로 서버를 추가하거나 제거하면 연결 장애가 발생합니다.

다음 그림은 DSR 모드로 ILB 구현을 보여줍니다.

그림 5-1 DSR(Direct Server Return) 토폴로지



이 그림에서 두 백엔드 서버 모두 동일한 서브넷(192.168.1.0/24)에 ILB 상자로 있습니다. 서버는 라우터에도 연결되어 있으므로 ILB 상자에서 전달한 요청을 수신한 후 클라이언트에 직접 응답할 수 있습니다.

NAT(Network Address Translator) 모드

ILB는 로드 균형 조정 기능에 대해서만 독립형 모드로 NAT를 사용합니다. 이 모드에서 ILB는 헤더 정보를 재작성하고 수신 및 송신 트래픽을 처리합니다. ILB는 Half-NAT 및 Full-NAT 모드 모두로 작동합니다. 그러나 Full-NAT는 소스 IP 주소도 재작성하여 모든 연결이 로드 밸런서에서 시작되는 것으로 서버에 표시되도록 합니다. NAT는 TCP 연결 추적을 제공합니다(Statefulness을 의미함). NAT 모드는 추가 보안을 제공하므로 HTTP(Hypertext Transfer Protocol) 또는 SSL(Secure Sockets Layer) 트래픽에 가장 적합합니다.

장점:

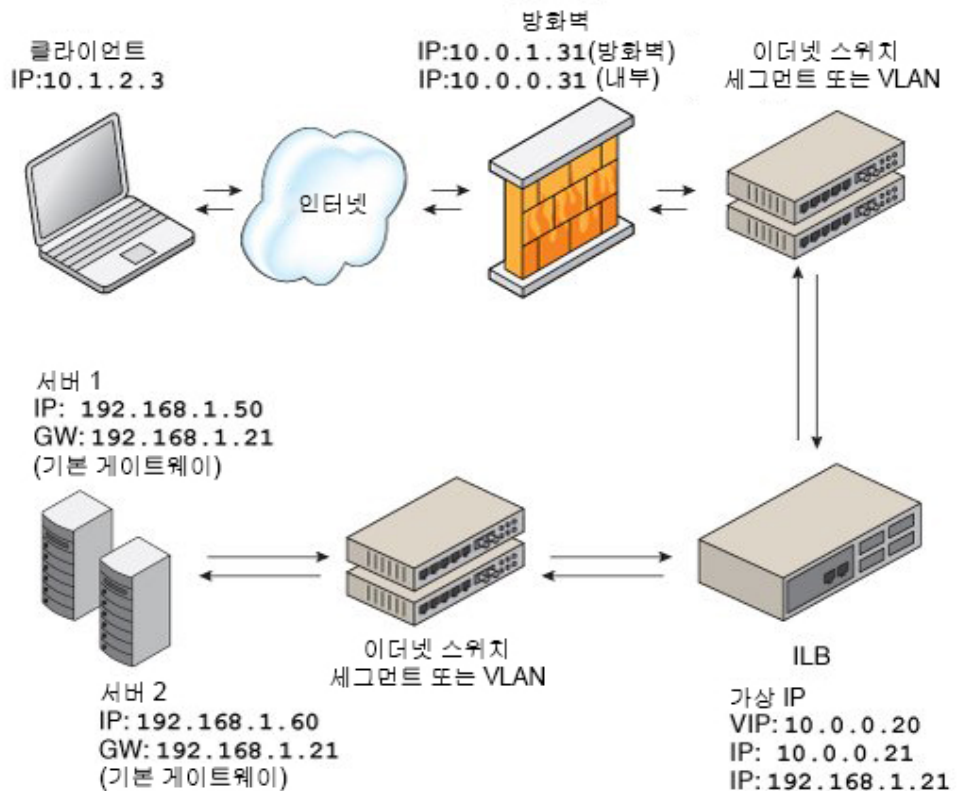
- 기본 게이트웨이가 로드 밸런서를 가리키도록 변경하여 모든 백엔드 서버에서 작동합니다
- 로드 밸런서가 연결 상태를 유지 관리하므로 연결 장애 없이 서버를 추가하거나 제거할 수 있습니다.

단점:

- 처리 시 IP 헤더가 조작되고 서버가 로드 밸런서로 응답을 보내므로 DSR에 비해 성능이 떨어집니다
- 모든 백엔드 서버에서 로드 밸런서를 기본 게이트웨이로 사용해야 합니다

일반적인 NAT 모드 구현은 다음 그림에 나타난 것과 같습니다.

그림 5-2 NAT(Network Address Translation) 토폴로지



이 경우 VIP에 대한 모든 요청이 ILB를 경유하여 백엔드 서버로 전달됩니다. NAT의 경우 백엔드 서버의 모든 응답이 ILB를 경유합니다.



주의 - ILB에서 구현된 NAT 코드 경로는 Oracle Solaris의 IP 필터 기능에서 구현된 코드 경로와 다릅니다. 이러한 코드 경로를 동시에 사용하지 마십시오.

Half-NAT 로드 균형 조정 모드

Half-NAT 모드의 ILB 작동에서는 ILB가 패킷의 헤더에 대상 IP 주소만 다시 씁니다. Half-NAT 구현을 사용하는 경우 서버가 상주하는 동일한 서브넷에서 서비스의 VIP 주소에 연결할 수 없습니다. 다음 표는 클라이언트와 ILB 사이 그리고 ILB와 백엔드 서버 사이를 이동하는 패킷의 IP 주소를 보여줍니다.

표 5-1 서버 및 클라이언트가 다른 네트워크에 있는 경우 Half-NAT 구현의 요청 플로우와 응답 플로우

요청 플로우	소스 IP 주소	대상 IP 주소
1. 클라이언트 -> ILB	클라이언트	ILB의 VIP
2. ILB -> 서버	클라이언트	서버
응답 플로우		
3. 서버 -> ILB	서버	클라이언트
4. ILB -> 클라이언트	ILB의 VIP	클라이언트

클라이언트 시스템을 서버와 동일한 네트워크에 연결하면 의도한 서버가 클라이언트에 직접 응답하며, 테이블의 4번째 단계는 발생하지 않습니다. 따라서 클라이언트에 대한 서버 응답의 소스 IP 주소가 잘못되었습니다. 클라이언트가 로드 밸런서로 연결 요청을 전송하면 의도한 서버에서 응답이 발생합니다. 이 시점 이후부터 클라이언트의 IP 스택이 정확하게 모든 응답을 삭제합니다. 이 시나리오의 경우 요청 플로우와 응답 플로우는 다음 표에 나타난 대로 진행됩니다.

표 5-2 서버 및 클라이언트가 동일한 네트워크에 있는 경우 Half-NAT 구현의 요청 플로우와 응답 플로우

요청 플로우	소스 IP 주소	대상 IP 주소
1. 클라이언트 -> ILB	클라이언트	ILB의 VIP
2. ILB -> 서버	클라이언트	서버
응답 플로우		
3. 서버 -> 클라이언트	서버	클라이언트

Full-NAT 로드 균형 조정 모드

Full-NAT 구현의 ILB 작동에서는 트래픽이 로드 밸런서를 양방향으로 통과하도록 소스 및 대상 IP 주소가 재작성됩니다. Full-NAT 모드에서는 서버가 상주하는 서브넷과 동일한 서브넷에서 VIP에 연결할 수 있습니다.

다음 표는 Full-NAT 모드를 사용하여 클라이언트와 ILB 사이 그리고 ILB와 백엔드 서버 사이를 이동하는 패킷의 IP 주소를 보여줍니다. ILB 상자를 사용하는 특별한 기본 경로가 서버에서 필요하지 않습니다. Full-NAT 모드에서는 관리자가 ILB에서 백엔드 서버와 통신하는 데 소스 주소로 사용할 하나의 IP 주소 또는 IP 주소 범위를 마련해 두어야 합니다. 사용되는 주소가 서브넷 C에 속한다고 가정하겠습니다. 이 시나리오에서는 ILB가 프록시로 작동합니다.

표 5-3 Full-NAT 구현의 요청 플로우와 응답 플로우

요청 플로우	소스 IP 주소	대상 IP 주소
1. 클라이언트 -> ILB	클라이언트	ILB의 VIP
2. ILB -> 서버	로드 밸런서의 인터페이스 주소(서브넷 C)	서버
응답 플로우		
3. 서버 -> ILB	서버	ILB의 인터페이스 주소(서브넷 C)
4. ILB -> 클라이언트	ILB의 VIP	클라이언트

ILB 작동 방식

이 절에서는 ILB의 프로세스에 대해 설명하며, 여기에는 클라이언트에서 VIP로 요청 처리, 백엔드 서버로 요청 전달 및 응답 처리가 포함됩니다.

클라이언트-서버 패킷 처리에는 다음 단계가 포함됩니다.

1. ILB에서 클라이언트가 VIP 주소로 보낸 수신 요청을 받아 로드 균형 조정 규칙과 요청을 일치시킵니다.
2. ILB에서 일치하는 로드 균형 조정 규칙을 찾을 경우 로드 균형 조정 알고리즘을 사용하여 작동 모드에 따라 요청을 백엔드 서버로 전달합니다.
 - DSR 모드에서는 ILB가 수신 요청의 MAC 헤더를 선택된 백엔드 서버의 MAC 헤더로 바꿉니다.
 - Half-NAT 모드에서는 ILB가 수신 요청의 대상 IP 주소 및 전송 프로토콜 포트 번호를 선택된 백엔드 서버의 대상 IP 주소 및 전송 프로토콜 포트 번호로 바꿉니다.
 - Full-NAT 모드에서는 ILB가 수신 요청의 소스 IP 주소 및 전송 프로토콜 포트 번호를 로드 균형 조정 규칙의 NAT 소스 주소로 바꿉니다. ILB는 또한 수신 요청의 대상 IP 주소 및 전송 프로토콜 포트 번호를 선택된 백엔드 서버의 대상 IP 주소 및 전송 프로토콜 포트 번호로 바꿉니다.

3. ILB는 수정된 수신 요청을 선택된 백엔드 서버로 전달합니다.

서버-클라이언트 패킷 처리에는 다음 단계가 포함됩니다.

1. 백엔드 서버가 클라이언트의 수신 요청에 대한 응답으로 ILB에 응답을 보냅니다.
2. 백엔드 서버로부터 응답을 받은 후 ILB의 작업은 작동 모드를 기반으로 합니다.
 - DSR 모드에서는 백엔드 서버의 응답이 ILB를 무시하고 클라이언트로 직접 전송됩니다. 하지만 ILB가 백엔드 서버의 라우터로도 사용되는 경우에는 백엔드 서버가 클라이언트로 보낸 응답이 ILB를 실행하는 시스템을 통해 경로 지정됩니다.
 - Half-NAT 및 Full-NAT 모드에서는 ILB가 백엔드 서버의 응답을 수신 요청과 일치시키고 변경된 IP 주소 및 전송 프로토콜 포트 번호를 원래 수신 요청의 IP 주소 및 전송 프로토콜 포트 번호로 바꿉니다. 그런 다음 ILB는 응답을 클라이언트로 전달합니다.

◆◆◆ 6 장

통합 로드 밸런서 구성 및 관리

ILB는 네트워크 프로토콜 스택의 L3 및 L4 층에서 구성됩니다. 이 장에서는 `ilbadm` 명령을 사용하여 ILB 설치, ILB 사용/사용 안함으로 설정, ILB에서 서버 그룹 및 백엔드 서버 정의, 그리고 ILB 구성 내보내기/가져오기 작업을 설명합니다. 자세한 내용은 [ilbadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오. 고가용성을 위한 ILB 구성에 대한 자세한 내용은 [7장. 고가용성을 위한 ILB 구성](#)을 참조하십시오.

Oracle Solaris 통합 로드 밸런서를 배치하는 방법에 대한 자세한 내용은 [Deploying the Oracle Solaris Integrated Load Balancer in 60 Minutes \(http://www.oracle.com/technetwork/systems/hands-on-labs/hol-deploy-ilb-60mmin-2137812.html\)](http://www.oracle.com/technetwork/systems/hands-on-labs/hol-deploy-ilb-60mmin-2137812.html)를 참조하십시오. Oracle Solaris에서 Oracle Solaris 영역 및 ILB를 사용하여 응용 프로그램에 고가용성을 추가하는 방법에 대한 자세한 내용은 [How to Set Up a Load-Balanced Application Across Two Oracle Solaris Zones \(http://www.oracle.com/technetwork/articles/servers-storage-admin/loadbalancedapp-1653020.html\)](http://www.oracle.com/technetwork/articles/servers-storage-admin/loadbalancedapp-1653020.html)을 참조하십시오.

이 장의 내용:

- “ILB 설치” [51]
- “명령줄 인터페이스를 사용하여 ILB 구성” [52]
- “ILB 사용 또는 사용 안함으로 설정” [53]
- “ILB 관리” [54]
- “사용 사례: ILB 구성” [63]
- “ILB 통계 표시” [64]
- “구성 가져오기 및 내보내기” [66]

ILB 설치

ILB에는 커널 및 userland 설치가 있습니다. ILB 커널 설치는 Oracle Solaris 설치의 일부로 자동으로 수행됩니다. 하지만 ILB userland 설치는 다음 명령을 사용하여 수행해야 합니다.

```
# pkg install ilb
```

명령줄 인터페이스를 사용하여 ILB 구성

ILB CLI는 `/usr/sbin/ilbadm` 디렉토리에 있습니다. CLI에는 로드 균형 조정 규칙, 서버 그룹 및 상태 검사를 구성하기 위한 하위 명령이 포함되어 있습니다. 통계를 표시하고 구성 상세 정보를 보기 위한 하위 명령도 포함되어 있습니다. `ilbadm show-rule`, `ilbadm show-server` 및 `ilbadm show-healthcheck`와 같은 보기 하위 명령을 제외하고 ILB 구성 하위 명령에 대한 사용자 권한 부여를 설정해야 합니다. ILB 구성 하위 명령을 실행하려면 `solaris.network.ilb.config` RBAC 권한 부여가 있어야 합니다.

- 기존 사용자에게 권한 부여를 지정하는 방법에 대한 자세한 내용은 [“Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 3 장](#), [“Oracle Solaris에서 권한 지정”](#)을 참조하십시오.
- 또한 시스템에 새 사용자 계정을 만들 때 권한 부여를 제공할 수 있습니다.

다음 예에서는 그룹 ID 10, 사용자 ID 1210 그리고 시스템에서 ILB를 관리하기 위한 권한 부여를 사용하여 `ilbadm` 사용자를 만듭니다.

```
# useradd -g 10 -u 1210 -A solaris.network.ilb.config ilbadm
```

`useradd` 명령은 `/etc/passwd`, `/etc/shadow` 및 `/etc/user_attr` 파일에 새 사용자를 추가합니다. `-A` 옵션을 사용하면 사용자에게 권한을 지정합니다.

하위 명령은 다음 두 가지 범주로 구분될 수 있습니다.

- **구성 하위 명령** - 이러한 하위 명령을 통해 다음 작업을 수행할 수 있습니다.
 - 로드 균형 조정 규칙 생성 및 삭제
 - 로드 균형 조정 규칙 사용 및 사용 안함으로 설정
 - 서버 그룹 생성 및 삭제
 - 서버 그룹에서 서버 추가 및 제거
 - 백엔드 서버를 사용 및 사용 안함으로 설정
 - 로드 균형 조정 규칙 내 서버 그룹에 대한 서버 상태 검사 생성 및 삭제

참고 - 구성 하위 명령을 관리하려면 권한이 필요합니다. 알맞은 역할을 만들고 사용자에게 역할을 지정하려면 [“Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “역할 만들기”](#)를 참조하십시오.

- **보기 하위 명령** - 이러한 하위 명령을 통해 다음 작업을 수행할 수 있습니다.
 - 구성된 로드 균형 조정 규칙, 서버 그룹 및 상태 검사 보기
 - 패킷 전달 통계 보기
 - NAT 연결 테이블 보기
 - 상태 검사 결과 보기
 - 세션 지속성 매핑 테이블 보기

참고 - 보기 하위 명령을 관리하는 데는 권한이 필요하지 않습니다.

ilbadm 하위 명령에 대한 자세한 내용은 [ilbadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

ILB 사용 또는 사용 안함으로 설정

이 절에서는 ILB가 설치된 후 ILB를 사용으로 설정하거나 ILB 서비스가 필요하지 않은 경우 ILB를 사용 안함으로 설정하는 방법을 설명합니다.

▼ ILB를 사용으로 설정하는 방법

1. 관리자로 로그인합니다.
자세한 내용은 “[Oracle Solaris 11.2의 사용자 및 프로세스 보안](#)”의 “[지정된 관리 권한 사용](#)”을 참조하십시오.
2. IPv4 또는 IPv6 중에서(또는 둘 다) 적절한 전달 서비스를 사용으로 설정합니다.
성공하는 경우 이 명령은 출력을 생성하지 않습니다.

```
# ipadm set-prop -p forwarding=on ipv4
# ipadm set-prop -p forwarding=on ipv6
```
3. ILB 서비스를 사용으로 설정합니다.

```
# svcadm enable ilb
```
4. ILB 서비스가 사용으로 설정되었는지 확인합니다.

```
# svcs ilb
```


이 명령은 서비스 구성 저장소에 기록된 대로 서비스 인스턴스에 대한 정보를 표시합니다.

▼ ILB를 사용 안함으로 설정하는 방법

ILB 서비스가 필요하지 않은 경우 ILB를 사용 안함으로 설정할 수 있습니다.

1. 관리자로 로그인합니다.

자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “지정된 관리 권한 사용”을 참조하십시오.

2. ILB 서비스를 사용 안함으로 설정합니다.

```
# svcadm disable ilb
```

3. ILB 서비스가 사용 안함으로 설정되었는지 확인합니다.

```
# svcs ilb
```

이 명령은 서비스 구성 저장소에 기록된 대로 서비스 인스턴스에 대한 정보를 표시합니다.

다음 순서 ILB 서비스가 사용 안함으로 설정된 후 IP 전달을 사용 안함으로 설정해야 합니다(필요하지 않은 경우).

ILB 관리

ILB를 사용으로 설정한 후 서버 그룹 정의, ILB의 상태 검사 모니터링 및 ILB 규칙 만들기를 통해 ILB를 설정할 수 있습니다.

이 절에서는 다음 항목을 다룹니다.

- “ILB에서 서버 그룹 및 백엔드 서버 정의” [54]
- “ILB에서 상태 검사 모니터링” [57]
- “ILB 규칙 구성” [60]

ILB에서 서버 그룹 및 백엔드 서버 정의

이 절에서는 ILB 서버 그룹을 만들고 백엔드 서버를 서버 그룹에 추가하는 방법을 설명합니다. 서버가 `create-servergroup` 또는 `add-server` 하위 명령을 사용하여 추가된 경우 서버 ID가 시스템에서 생성됩니다. 서버 ID는 서버 그룹 내에서 고유합니다. `ilbadm` 하위 명령에 대한 자세한 내용은 `ilbadm(1M)` 매뉴얼 페이지를 참조하십시오.

ILB 서버 그룹 만들기

ILB 서버 그룹을 만들려면 먼저 서버 그룹에 포함될 서버를 식별합니다. 서버는 호스트 이름 또는 IP 주소 및 선택적 포트로 지정할 수 있습니다. 그런 다음 관리자로 다음 명령을 실행합니다.

```
# ilbadm create-servergroup -s servers=server1,server2,server3 servergroup
```

선행 밑줄(_)이 앞에 붙은 고유한 서버 ID가 추가된 각 서버에 대해 생성됩니다.

참고 - 서버가 다중 서버 그룹에 속할 경우 여러 서버 ID를 가질 수 있습니다.

ILB 서버 그룹에 백엔드 서버 추가

백엔드 서버를 서버 그룹에 추가하려면 관리자로 전환하고 다음 명령을 실행합니다.

```
# ilbadm add-server -s server=server1[,server2...] servergroup
```

서버 사양은 호스트 이름 또는 IP 주소를 포함해야 하고, 선택적 포트 또는 포트 범위를 포함할 수도 있습니다. 서버 그룹 내에서 IP 주소가 동일한 서버 항목은 허용되지 않습니다. 선행 밑줄(_)이 앞에 붙은 고유한 서버 ID가 추가된 각 서버에 대해 생성됩니다.

참고 - IPv6 주소는 대괄호로 묶어야 합니다.

예 6-1 ILB 서버 그룹 만들기 및 백엔드 서버 추가

다음 예에서는 세 개의 백엔드 서버가 있는 webgroup이라는 서버 그룹을 만듭니다.

```
# ilbadm create-servergroup -s \
servers=192.168.89.11,192.168.89.12,192.168.89.13 webgroup
```

```
# ilbadm show-servergroup
SGNAME          SERVERID          MINPORT  MAXPORT  IP_ADDRESS
webgroup        _webgroup.0      --        --        192.168.89.11
webgroup        _webgroup.1      --        --        192.168.89.12
webgroup        _webgroup.2      --        --        192.168.89.13
```

다음 예에서는 webgroup1이라는 서버 그룹을 만들고 세 개의 백엔드 서버를 서버 그룹에 추가합니다.

```
# ilbadm create-servergroup webgroup1
# ilbadm add-server -s server=[2001:0db8:7::feed:6]:8080,\
[2001:0db8:7::feed:7]:8080,[2001:0db8:7::feed:8]:8080 webgroup1
```

ILB 서버 그룹에서 백엔드 서버 사용 또는 사용 안함으로 설정

먼저 다시 사용 또는 사용 안함으로 설정할 백엔드 서버의 IP 주소, 호스트 이름 또는 서버 ID를 식별합니다. 서버 그룹의 서버를 사용 또는 사용 안함으로 설정하려면 먼저 서버 그룹과 규칙을 연관시켜야 합니다.

서버가 다중 서버 그룹에 속할 경우 여러 서버 ID를 가질 수 있습니다. 서버 ID와 연관된 특정 규칙에 대해 서버를 다시 사용 또는 사용 안함으로 설정할 서버 ID를 지정해야 합니다.

- 사용으로 설정된 서버를 사용 안함으로 설정하려면 다음 명령을 입력합니다.

```
# ilbadm disable-server server1
```

선택한 서버(사용으로 설정됨)가 사용 안함으로 설정됩니다. 커널은 트래픽을 이 서버에 전달하지 않습니다.

- 사용 안함으로 설정된 서버를 다시 사용으로 설정하려면 다음 명령을 입력합니다.

```
# ilbadm enable-server server1
```

선택한 서버(사용 안함으로 설정됨)가 다시 사용으로 설정됩니다.

- 서버의 상태를 표시하려면 다음 명령을 입력합니다.

```
# ilbadm show-server [[-p] -o field[,field...]] [rulename]
```

참고 - 서버가 속하는 서버 그룹이 규칙과 연관된 경우에만 서버가 상태를 사용으로 설정됨 또는 사용 안함으로 설정됨으로 표시합니다.

예 6-2 ILB 서버 그룹에서 백엔드 서버를 사용 안함 및 다시 사용으로 설정

다음 예에서는 서버 ID가 `_websg.1`인 서버가 사용 안함으로 설정된 다음 다시 사용으로 설정됩니다.

```
# ilbadm enable-server _websg.1
# ilbadm disable-server _websg.1
```

ILB 서버 그룹에서 백엔드 서버 삭제

`ilbadm remove-server` 명령을 사용하여 한 ILB 서버 그룹이나 모든 서버 그룹에서 백엔드 서버를 제거합니다. 먼저 서버 그룹에서 제거할 서버의 서버 ID를 식별합니다.

```
ilbadm show-servergroup -o all
```

서버 ID는 서버가 서버 그룹에 추가될 때 시스템에 지정되는 IP 주소의 고유 이름입니다.

그런 다음 서버를 삭제합니다.

```
# ilbadm remove-server -s server=server-ID server-group
```

NAT 또는 Half-NAT 규칙에서 서버를 사용 중인 경우 제거 전에 `disable-server` 하위 명령을 사용하여 서버를 사용 안함으로 설정합니다. 자세한 내용은 [“ILB 서버 그룹에서 백엔드 서버 사용 또는 사용 안함으로 설정” \[55\]](#)을 참조하십시오. 서버가 사용 안함으로 설정되면

연결 드레이닝 상태로 진입합니다. `ilbadm show-nat` 명령을 사용하여 정기적으로 NAT 테이블을 검사하여 서버에 여전히 연결이 있는지 확인합니다. 모든 연결이 드레인된 후에(`show-nat` 명령 출력에 서버가 표시되지 않음) `remove-server` 명령을 사용하여 서버를 제거할 수 있습니다.

`conn-drain` 시간 초과 값이 설정된 경우 시간 초과 기간 종결 시 연결 드레이닝 상태가 완료됩니다. `conn-drain` 시간 초과값의 기본값은 0이며, 이는 연결이 적절하게 종료될 때까지 연결 드레이닝 대기기를 의미합니다.

예 6-3 ILB 서버 그룹에서 백엔드 서버 삭제

다음 예에서는 서버 그룹 `sg1`에서 서버 ID가 `_sg1.2`인 서버를 제거합니다.

```
# ilbadm remove-server -s server=_sg1.2 sg1
```

ILB 서버 그룹 삭제

이 절에서는 ILB 서버 그룹을 삭제하는 방법을 설명합니다. 활성 규칙에서 사용되는 서버 그룹은 삭제할 수 없습니다.

먼저 서버 그룹에 대한 모든 사용 가능한 정보를 표시합니다.

```
# ilbadm show-servergroup -o all
sgname      serverID    minport    maxport    IP_address
specgroup   _specgroup.0 7001      7001      192.168.68.18
specgroup   _specgroup.1 7001      7001      192.168.68.19
test123     _test123.0   7002      7002      192.168.67.18
test123     _test123.1   7002      7002      192.168.67.19
```

다음 명령을 입력합니다.

```
# ilbadm delete-servergroup servergroup
```

활성 규칙에서 서버 그룹을 사용 중인 경우 삭제를 실패합니다.

다음 예에서는 `webgroup`이라는 서버 그룹을 제거합니다.

```
# ilbadm delete-servergroup webgroup
```

ILB에서 상태 검사 모니터링

ILB는 다음과 같은 선택적 유형의 서버 상태 검사를 제공합니다.

- 내장 핑 프로브
- 내장 TCP 프로브

- 내장 UDP 프로브
- 상태 검사로 실행할 수 있는 사용자 제공 사용자 정의 테스트

기본적으로 ILB는 상태 검사를 수행하지 않습니다. 로드 균형 조정 규칙을 만들 때 각 서버 그룹에 대해 상태 검사를 지정할 수 있습니다. 로드 균형 조정 규칙당 하나의 상태 검사만 구성할 수 있습니다. 가상 서비스가 사용으로 설정된 동안, 사용으로 설정된 가상 서비스와 연관된 서버 그룹에서 상태 검사가 자동으로 시작되고 정기적으로 반복됩니다. 가상 서비스를 사용 안함으로 설정하면 즉시 상태 검사가 중지됩니다. 가상 서비스를 다시 사용으로 설정하면 이전 상태 검사 상태는 보존되지 않습니다.

상태 검사를 실행하기 위해 TCP, UDP 또는 사용자 정의 테스트 프로브를 지정할 때 ILB는 기본적으로 핑 프로브를 보내 지정된 TCP, UDP 또는 사용자 정의 테스트 프로브를 서버로 보내기 전에 서버에 연결할 수 있는지 확인합니다. 핑 프로브가 실패하면 해당 서버가 사용 안함으로 설정되고 상태 검사 상태가 unreachable이 됩니다. 핑 프로브는 성공하지만 TCP, UDP 또는 사용자 정의 테스트 프로브가 실패하면 서버가 사용 안함으로 설정되고 상태 검사 상태는 dead가 됩니다.

UDP 프로브를 제외한 기본 핑 프로브를 사용 안함으로 설정할 수 있습니다. 핑 프로브는 항상 UDP 상태 검사에 대한 기본 프로브입니다.

상태 검사 생성

상태 검사를 만들고 로드 균형 조정 규칙을 만들 때 서버 그룹에 상태 검사를 지정할 수 있습니다. 다음 예에서는 2개의 상태 검사 객체, hc1 및 hc-myscript가 생성됩니다. 첫번째 상태 검사는 내장 TCP 프로브를 사용합니다. 두번째 상태 검사는 사용자 정의 테스트인 /var/tmp/my-script를 사용합니다.

```
# ilbadm create-healthcheck -h hc-timeout=3,\
hc-count=2,hc-interval=8,hc-test=tcp hc1
# ilbadm create-healthcheck -h hc-timeout=3,\
hc-count=2,hc-interval=8,hc-test=/var/tmp/my-script hc-myscript
```

인수는 다음과 같습니다.

hc-timeout	상태 검사가 완료되지 않은 경우 실패한 것으로 간주되는 시간 초과를 지정합니다.
hc-count	hc-test 상태 검사 실행 시도 횟수를 지정합니다.
hc-interval	연속 상태 검사 사이의 간격을 지정합니다. 모든 서버에 동시에 프로브를 보내는 것을 피하기 위해 실제 간격은 $0.5 * hc-interval$ 및 $1.5 * hc-interval$ 사이에서 무작위로 설정됩니다.
hc-test	상태 검사 유형을 지정합니다. 내장 상태 검사(예: tcp, udp 및 ping) 또는 전체 경로 이름으로 지정해야 하는 외부 상태 검사를 지정할 수 있습니다.

참고 - hc-test의 포트 사양은 create-rule 하위 명령의 hc-port 키워드로 지정됩니다. 자세한 내용은 [ilbadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

사용자가 제공한 사용자 정의 테스트는 바이너리 또는 스크립트일 수 있습니다.

- 테스트는 시스템의 어느 위치에나 있을 수 있습니다. create-healthcheck 하위 명령을 사용할 때는 절대 경로를 지정해야 합니다.

create-rule 하위 명령에서 상태 검사 사양의 일부로 테스트를 지정하는 경우(예: /var/tmp/my-script) 다음과 같이 ilbd 데몬이 프로세스를 포크하고 테스트를 실행합니다.

```
/var/tmp/my-script $1 $2 $3 $4 $5
```

인수는 다음과 같습니다.

\$1	VIP(리터럴 IPv4 또는 IPv6 주소)
\$2	서버 IP(리터럴 IPv4 또는 IPv6 주소)
\$3	프로토콜(UDP, TCP를 문자열로)
\$4	숫자 포트 범위(hc-port에 대한 사용자 지정 값)
\$5	테스트에서 실패를 반환하기 전에 대기해야 하는 최대 시간(초) 지정된 시간을 넘어 테스트를 실행하면 테스트가 중지될 수 있고 실패로 간주됩니다. 이 값은 사용자 정의 값으로 hc-timeout에 지정됩니다.

- 사용자 제공 테스트는 모든 인수를 사용할 필요가 없지만, 반드시 다음 중 하나를 반환해야 합니다.
 - 마이크로초 단위의 RTT(라운드 트립 시간)
 - 테스트에서 RTT를 계산하지 않는 경우 0
 - 실패한 경우 -1

기본적으로 상태 검사 테스트는 PRIV_PROC_FORK, RIV_PROC_EXEC 및 RIV_NET_ICMPACCESS 권한으로 실행됩니다.

더 광범위한 권한 세트가 필요한 경우 테스트에 setuid를 구현해야 합니다. 권한에 대한 자세한 내용은 [privileges\(5\)](#) 매뉴얼 페이지를 참조하십시오.

상태 검사 나열

구성된 상태 검사에 대한 자세한 정보를 얻으려면 다음 명령을 실행합니다.

```
# ilbadm show-healthcheck
```

HCNAME	TIMEOUT	COUNT	INTERVAL	DEF_PING	TEST
hc1	3	2	8	Y	tcp
hc2	3	2	8	N	/var/usr-script

상태 검사 결과 표시

`ilbadm list-hc-result` 명령을 사용하여 상태 검사 결과를 얻을 수 있습니다. 규칙이나 상태 검사가 지정되지 않은 경우 모든 상태 검사가 나열됩니다.

다음 예에는 `rule1`이라는 규칙과 연관된 상태 검사 결과가 표시되어 있습니다.

```
# ilbadm show-hc-result rule1
RULENAME  HCNAME      SERVERID  STATUS  FAIL  LAST      NEXT      RTT
rule1     hc1         _sg1:0   dead    10   11:01:19  11:01:27  941
rule1     hc1         _sg1:1   alive   0    11:01:20  11:01:34  1111
```

참고 - `show-hc-result` 명령은 규칙에 연관된 상태 검사가 있을 경우에만 상태 검사 결과를 표시합니다.

출력의 `LAST` 열에는 서버에서 상태 검사가 수행된 시간이 표시됩니다. `NEXT` 열에는 다음 상태 검사가 수행될 시간이 표시됩니다.

상태 검사 삭제

`ilbadm delete-healthcheck` 명령을 사용하여 상태 검사를 삭제합니다. 다음 예에서는 `hc1`이라는 상태 검사를 삭제합니다.

```
# ilbadm delete-healthcheck hc1
```

ILB 규칙 구성

이 절에서는 `ilbadm` 명령을 사용하여 로드 균형 조정 규칙을 생성, 삭제 및 나열하는 방법에 대해 설명합니다.

ILB 알고리즘

ILB 알고리즘은 트래픽 분배를 제어하고 다양한 로드 분배 및 서버 선택 특성을 제공합니다.

ILB는 두 가지 작동 모드에 대해 다음 알고리즘을 제공합니다.

- 라운드 로빈 - 라운드 로빈 알고리즘에서는 로드 밸런서가 회전을 기준으로 서버 그룹에 요청을 지정합니다. 서버에 요청이 지정되면 목록 끝으로 서버가 이동됩니다.
- *src-IP* 해시 - 소스 IP 해시 메소드에서 로드 밸런서는 수신 요청의 소스 IP 주소에 대한 해시 값을 기반으로 서버를 선택합니다.
- *src-IP, port* 해시 - 소스 IP, 포트 해시 메소드에서는 로드 밸런서가 수신 요청의 소스 IP 주소 및 소스 포트에 대한 해시 값을 기반으로 서버를 선택합니다.
- *src-IP, VIP* 해시 - 소스 IP, VIP 해시 메소드에서는 로드 밸런서가 수신 요청의 소스 IP 주소 및 대상 IP 주소에 대한 해시 값을 기반으로 서버를 선택합니다.

ILB 규칙 만들기

ILB에서 가상 서버는 로드 균형 조정 규칙으로 표시되며 다음 매개변수로 정의됩니다.

- 가상 IP 주소
- 전송 프로토콜: TCP 또는 UDP
- 포트 번호(또는 포트 범위)
- 로드 균형 조정 알고리즘
- 로드 균형 조정 모드(DSR, Full-NAT 또는 Half-NAT)
- 일련의 백엔드 서버로 구성된 서버 그룹
- 서버 그룹의 각 서버에 대해 실행할 수 있는 선택적 서버 상태 검사
- 상태 검사에 사용할 선택적 포트

참고 - 특정 포트 또는 `ilbd` 데몬이 서버 포트 범위에서 임의적으로 선택하는 포트에 대해 건전성 검사를 지정할 수 있습니다.

- 가상 서비스를 표시할 규칙 이름

규칙을 만들려면 먼저 다음 작업을 수행해야 합니다.

- 적절한 백엔드 서버를 포함하는 서버 그룹을 만듭니다. 자세한 내용은 [“ILB에서 서버 그룹 및 백엔드 서버 정의” \[54\]](#)를 참조하십시오.
- 상태 검사를 만들어 서버 상태 검사를 규칙과 연관시킵니다. 자세한 내용은 [“상태 검사 생성” \[58\]](#)을 참조하십시오.
- 규칙과 연관될 VIP, 포트 및 선택적 프로토콜을 식별합니다.
- 사용할 작업을 식별합니다(DSR, Half-NAT 또는 Full-NAT).
- 사용될 로드 균형 조정 알고리즘을 식별합니다. 자세한 내용은 [“ILB 알고리즘” \[60\]](#)을 참조하십시오.

ILB 규칙은 `ilbadm create-rule` 명령을 사용하여 만듭니다. `ilbadm create-rule` 명령 사용에 대한 자세한 내용은 [ilbadm\(1M\)](#) 매뉴얼 페이지를 참조하십시오.

구문은 다음과 같습니다.

```
# ilbadm create-rule -e -i vip=IPAddr,port=port,protocol=protocol \
-m lbalg=lb-algorithm,type=topology-type,proxy-src=IPAddr1-IPAddr2,\
pmask=value -h hc-name=hc1 -o servergroup=sg rule1
```

참고 - -e 옵션은 만들 규칙을 사용으로 설정합니다. 그렇지 않으면 기본적으로 사용 안함으로 설정됩니다.

예 6-4 상태 검사 세션 지속성이 사용된 Full-NAT 규칙 만들기

이 예에서는 hc1이라는 상태 검사와 sg1이라는 서버 그룹을 만듭니다. 서버 그룹은 두 개의 서버로 구성되고 각각 포트 범위를 가지고 있습니다. 마지막 명령은 rule1이라는 규칙을 만들어 사용으로 설정하고 서버 그룹 및 상태 검사에 규칙을 연관시킵니다. 이 규칙이 Full-NAT 작동 모드를 구현합니다. 서버 그룹 및 상태 검사 생성은 규칙 생성보다 선행되어야 합니다.

```
# ilbadm create-healthcheck -h hc-test=tcp,hc-timeout=2,\
hc-count=3,hc-interval=10 hc1
# ilbadm create-servergroup -s server=192.168.0.10:6000-6009,192.168.0.11:7000-7009 sg1
# ilbadm create-rule -e -p -i vip=10.0.0.10,port=5000-5009,\
protocol=tcp -m lbalg=rr,type=NAT,proxy-src=192.168.0.101-192.168.0.104,pmask=24 \
-h hc-name=hc1 -o servergroup=sg1 rule1
```

지속 매핑을 만들면 클라이언트의 소스 IP 주소와 일치하는 가상 서비스를 대상으로 하는 연결이나 패킷 또는 둘 모두에 대한 후속 요청이 동일한 백엔드 서버로 전달됩니다. CIDR(Classless Inter-Domain Routing) 표기법의 접두어 길이는 0-32의 값(IPv4의 경우) 및 0-128의 값(IPv6의 경우)입니다.

Half-NAT 또는 Full-NAT 규칙 생성 시 connection-drain 시간 초과 값을 지정하십시오. conn-drain 시간 초과 기본값은 0이며, 이는 연결이 적절하게 종료될 때까지 연결 드레잉 계속 대기를 의미합니다.

ILB 규칙 나열

규칙의 구성 세부 사항을 나열하려면 다음 명령을 실행합니다. 규칙 이름이 지정되지 않으면 모든 규칙에 대한 정보가 제공됩니다.

```
# ilbadm show-rule
RULENAME      STATUS  LBALG      TYPE    PROTOCOL  VIP          PORT
rule-http     E       hash-ip-port NAT     TCP       10.0.0.1    80
rule-dns      D       hash-ip    NAT     UDP       10.0.0.1    53
rule-abc      D       roundrobin NAT     TCP       2001:db8::1 1024
rule-xyz      E       ip-vip     NAT     TCP       2001:db8::1 2048-2050
```

ILB 규칙 삭제

`ilbadm delete-rule` 명령을 사용하여 규칙을 삭제합니다. 모든 규칙을 삭제하려면 `-a` 옵션을 추가합니다. 다음 예에서는 `rule1` 규칙을 삭제합니다.

```
# ilbadm delete-rule rule1
```

사용 사례: ILB 구성

이 절에서는 Half-NAT 토폴로지를 사용하여 두 서버 사이의 트래픽 로드 균형을 조정하기 위한 ILB 설정 단계에 대해 설명합니다. “ILB 작동 모드” [44]의 NAT 토폴로지 구현을 참조하십시오.

1. 관리자로 로그인합니다.

자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “지정된 관리 권한 사용”을 참조하십시오.

2. ILB의 서버 그룹을 설정합니다.

두 서버는 192.168.1.50 및 192.169.1.60입니다. 다음 명령을 입력하여 이러한 두 서버로 구성된 서버 그룹 `srvgrp1`을 만듭니다. ILB에서 서버 그룹 설정에 대한 자세한 내용은 “ILB 서버 그룹 만들기” [54]를 참조하십시오.

```
# ilbadm create-sg -s servers=192.168.1.50,192.168.1.60 srvgrp1
```

3. 백엔드 서버를 설정합니다.

백엔드 서버는 ILB를 이 시나리오의 기본 라우터로 사용하도록 설정됩니다. 두 서버에서 다음 명령을 실행합니다.

```
# route add -p default 192.168.1.21
```

이 명령을 실행하면 두 서버 모두에서 서버 응용프로그램이 시작됩니다. 5000 포트에서 수신하는 TCP 응용프로그램이라고 가정합니다. 백엔드 서버 설정에 대한 자세한 내용은 “ILB 서버 그룹에 백엔드 서버 추가” [55]를 참조하십시오.

4. `hc-srvgrp1`이라는 간단한 상태 검사를 설정합니다. 다음 명령을 입력하여 상태 검사를 만듭니다.

```
# ilbadm create-hc -h hc-test=tcp,hc-timeout=3,\
hc-count=3,hc-interval=60 hc-srvgrp1
```

간단한 TCP 레벨 상태 검사를 사용하여 서버 응용프로그램에 접근할 수 있는지 감지합니다. 이러한 검사는 60초마다 수행됩니다. 상태 검사는 최대 3번을 시도하고 각 시도마다 최대 3초 동안 대기하면서 서버가 양호한지 확인합니다. 모든 3번의 시도를 실패할 경우 서버를 `dead`로 표시합니다. 상태 검사 모니터링 및 만들기에 대한 자세한 내용은 “ILB에서 상태 검사 모니터링” [57]을 참조하십시오.

5. 다음 명령을 입력하여 ILB 규칙을 설정합니다.

```
# ilbadm create-rule -e -p -i vip=10.0.2.20,port=5000 -m \
lbalg=rr,type=half-nat,pmask=32 \
-h hc-name=hc-srvgrp1 -o servergroup=srvgrp1 rule1_rr
```

이 규칙에서는 지속성(32비트 마스크 포함)이 사용됩니다. 로드 밸런스 알고리즘은 round robin입니다. 서로 다른 ILB 알고리즘에 대한 자세한 내용은 “[ILB 알고리즘](#)” [60]을 참조하십시오. 서버 그룹 srvgrp1이 사용되며 사용되는 상태 검사 방식은 hc-srvgrp1입니다. ILB 규칙 만들기에 대한 자세한 내용은 “[ILB 규칙 만들기](#)” [61]를 참조하십시오.

ILB 통계 표시

이 절에서는 ilbadm 명령을 사용하여 서버 통계 또는 규칙 통계 인쇄와 같은 정보를 얻는 방법에 대해 설명합니다. NAT 테이블 정보 및 세션 지속성 매핑 테이블을 표시할 수도 있습니다.

통계 정보 표시

ilbadm show-statistics 명령을 사용하여 다음 예에 표시된 대로 로드 분배 세부 사항을 봅니다.

```
# ilbadm show-statistics
PKT_P  BYTES_P  PKT_U  BYTES_U  PKT_D  BYTES_D
9      636      0      0      0      0
```

PKT_P	처리된 패킷
BYTES_P	처리된 바이트
PKT_U	처리되지 않은 패킷
BYTES_U	처리되지 않은 바이트
PKT_D	삭제된 패킷
BYTES_D	삭제된 바이트

NAT 연결 테이블 표시

ilbadm show-nat 명령을 사용하여 NAT 연결 테이블을 표시합니다. 이 명령의 연속적 실행에서 요소의 상대적 위치는 중요하지 않습니다. 예를 들어, 특히 혼잡한 시스템에서 ilbadm

show-nat 10 명령을 두 번 실행하는 경우 실행할 때마다 동일한 10개 항목이 표시되지 않을 수 있습니다. 개수 값이 지정되지 않은 경우 전체 NAT 연결 테이블이 표시됩니다.

예 6-5 NAT 연결 테이블 항목

다음 예에서는 NAT 연결 테이블에서 5개 항목이 표시됩니다.

```
# ilbadm show-nat 5
UDP: 124.106.235.150.53688 > 85.0.0.1.1024 >>> 82.0.0.39.4127 > 82.0.0.56.1024
UDP: 71.159.95.31.61528 > 85.0.0.1.1024 >>> 82.0.0.39.4146 > 82.0.0.55.1024
UDP: 9.213.106.54.19787 > 85.0.0.1.1024 >>> 82.0.0.40.4114 > 82.0.0.55.1024
UDP: 118.148.25.17.26676 > 85.0.0.1.1024 >>> 82.0.0.40.4112 > 82.0.0.56.1024
UDP: 69.219.132.153.56132 > 85.0.0.1.1024 >>> 82.0.0.39.4134 > 82.0.0.55.1024
```

항목의 형식은 다음과 같습니다.

T: IP1 > IP2 >>> IP3 > IP4

T	해당 항목에서 사용된 전송 프로토콜
IP1	클라이언트 IP 주소 및 포트
IP2	VIP 및 포트
IP3	Half-NAT 모드에서 클라이언트 IP 주소 및 포트 Full-NAT 모드에서 클라이언트 IP 주소 및 포트
IP4	백엔드 서버 IP 주소 및 포트

세션 지속성 매핑 테이블 표시

ilbadm show-persist 명령을 사용하여 세션 지속성 매핑 테이블을 표시합니다.

예 6-6 세션 지속성 매핑 테이블 항목

다음 예에서는 세션 지속성 매핑 테이블에서 5개 항목이 표시됩니다.

```
# ilbadm show-persist 5
rule2: 124.106.235.150 --> 82.0.0.56
rule3: 71.159.95.31 --> 82.0.0.55
rule3: 9.213.106.54 --> 82.0.0.55
rule1: 118.148.25.17 --> 82.0.0.56
rule2: 69.219.132.153 --> 82.0.0.55
```

항목의 형식은 다음과 같습니다.

R: IP1 --> IP2

R	지속성 항목이 연결된 규칙
IP1	클라이언트 IP 주소
IP2	백엔드 서버 IP 주소

구성 가져오기 및 내보내기

내보내기 및 가져오기 하위 명령은 한 시스템에서 다른 시스템으로 구성을 이동하는 데 사용 됩니다. 예를 들어, 활성-수동 구성을 위해 VRRP를 사용하여 ILB의 백업을 설정하려는 경우 구성을 파일로 내보내고 백업 시스템에서 가져오면 됩니다. `ilbadm export` 명령은 현재 ILB 구성을 사용자 지정 파일로 내보냅니다. 그런 다음 이 정보를 `ilbadm import` 명령의 입력으로 사용할 수 있습니다.

별도로 구성을 유지하라고 지시하지 않는 한, `ilbadm import` 명령은 기존 구성을 가져오기 전에 삭제합니다. 파일 이름을 생략하면 명령은 `stdin`에서 읽거나 `stdout`에 씁니다.

ILB 구성을 내보내려면 `export-config` 명령을 사용합니다. 다음 예는 `import` 명령을 사용하여 가져오기에 적합한 형식으로 현재 구성을 `/var/tmp/ilb_config` 파일로 내보냅니다.

```
# ilbadm export-config /var/tmp/ilb_config
```

ILB 구성을 가져오려면 `import-config` 명령을 사용합니다. 다음 예는 `/var/tmp/ilb_config` 파일의 내용을 읽고 기존 구성을 대체합니다.

```
# ilbadm import-config /var/tmp/ilb_config
```

고가용성을 위한 ILB 구성

이 장에서는 VRRP 기능을 사용하여 ILB의 고가용성(HA) 구성을 설명합니다. ILB는 DSR 및 Half-NAT 토폴로지를 사용하여 고가용성을 위해 구성됩니다. Half-NAT 및 DSR 토폴로지는 VRRP를 사용하여 ILB 규칙의 가상 IP 주소를 보호합니다. 하지만 Half-NAT 토폴로지에서 VRRP는 백엔드 서버를 접하고 있는 기본 로드 밸런서의 IP 주소를 보호하는 데도 사용됩니다. 그러면 기본 로드 밸런서가 실패할 경우 백엔드 서버가 대기(수동) 로드 밸런서를 사용하도록 전환됩니다.

VRRP에 대한 자세한 내용은 [3장. VRRP\(Virtual Router Redundancy Protocol\) 사용](#)을 참조하고, ILB 구성 및 관리 방법에 대한 자세한 내용은 [6장. 통합 로드 밸런서 구성 및 관리](#)를 참조하십시오.

이 장의 내용:

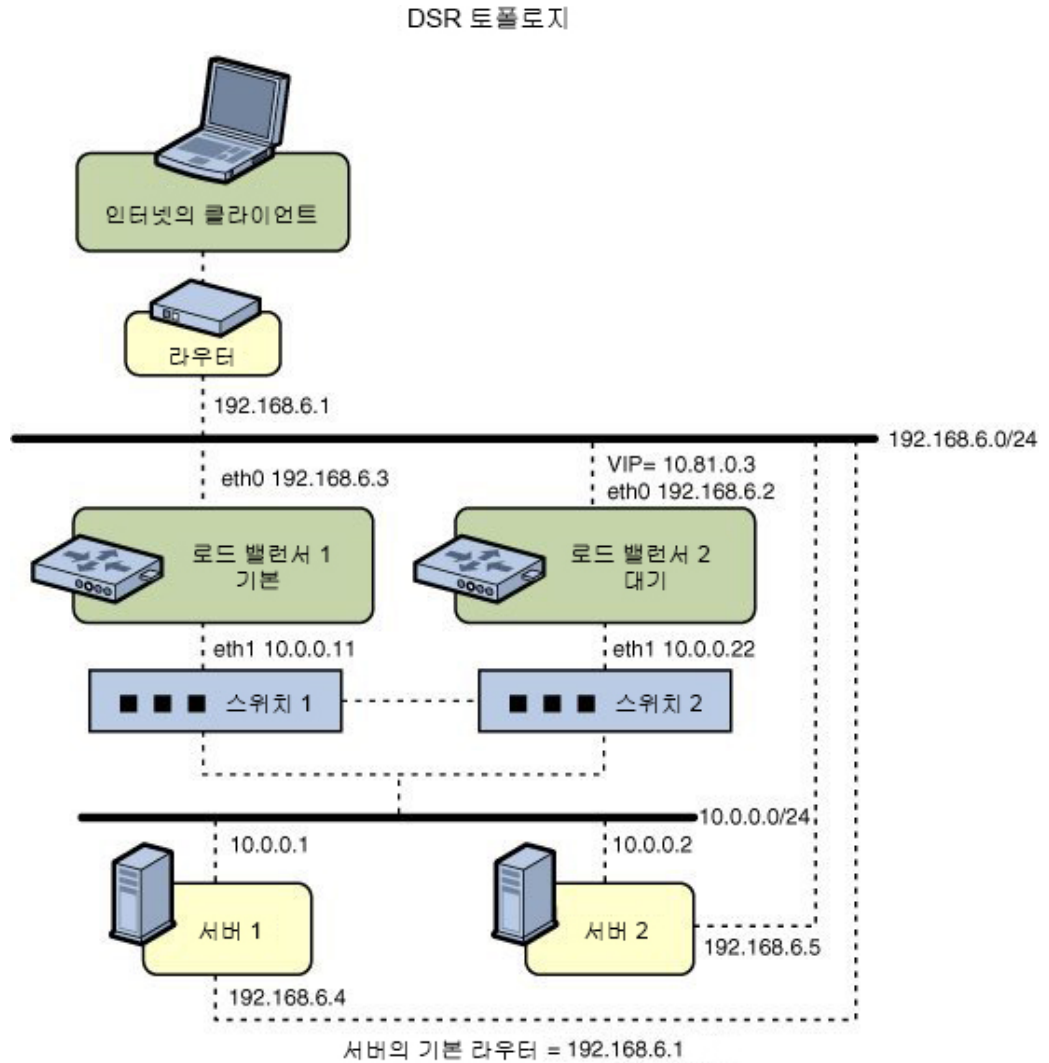
- “DSR 토폴로지를 사용하여 고가용성 ILB 구성” [67]
- “Half-NAT 토폴로지를 사용하여 고가용성 ILB 구성” [70]

DSR 토폴로지를 사용하여 고가용성 ILB 구성

기본 로드 밸런서와 대기 로드 밸런서의 두 가지 로드 밸런서를 설정할 수 있습니다. 기본 로드 밸런서는 마스터 라우터로 작동하고 대기(수동) 로드 밸런서는 백업 라우터로 작동합니다. ILB 규칙의 가상 IP 주소는 가상 라우터 IP 주소로 작동합니다. VRRP 부속 시스템은 기본 로드 밸런서가 실패했는지 여부를 확인합니다. 기본 로드 밸런서가 실패하면 대기 로드 밸런서가 기본 로드 밸런서의 역할을 맡습니다.

다음 그림은 HA를 구현하도록 ILB 연결을 구성하기 위한 DSR 토폴로지를 보여줍니다.

그림 7-1 DSR 토폴로지를 사용하여 HA ILB 구성



로드 밸런서의 모든 VIP는 서브넷 192.168.6.0/24를 대상으로 하는 인터페이스에 구성됩니다.

▼ DSR 토폴로지를 사용하여 고가용성 ILB를 구성하는 방법

기본 및 대기 로드 밸런서가 모두 ILB 규칙, 서버 그룹 및 상태 검사에 대해 동일한 구성을 가지도록 구성할 수 있습니다. 두 로드 밸런서가 VRRP를 사용하도록 설정할 수 있습니다. 또한 규칙의 가상 IP 주소가 가상 라우터 주소가 되도록 설정합니다. 그러면 VRRP 부속 시스템은 로드 밸런서 중 하나가 항상 활성 상태인지 확인합니다.

1. 관리자로 로그인합니다.

자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “지정된 관리 권한 사용”을 참조하십시오.

2. 기본 및 대기(수동) 로드 밸런서가 모두 동일한 설정을 가지도록 구성합니다.

```
# ilbadm create-servergroup -s server=10.0.0.1,10.0.0.2 sg1
# ilbadm create-rule -i vip=10.81.0.3,port=9001 \
-m lbalg=hash-ip-port,type=DSR -o servergroup=sg1 rule1
```

3. 로드 밸런서 1이 기본 로드 밸런서로 작동하도록 구성합니다.

```
LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
LB1# ipadm create-ip vnic1
LB1# ipadm create-addr -d -a 10.81.0.3/24 vnic1
```

vrrp1 라우터의 우선 순위는 vrrpadm 명령을 사용하여 255로 설정됩니다. 우선 순위 값은 라우터가 마스터 라우터, 즉 활성 로드 밸런서가 되도록 합니다.

4. 로드 밸런서 2가 대기 로드 밸런서로 작동하도록 구성합니다.

```
LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
LB2# ipadm create-ip vnic1
LB2# ipadm create-addr -d -a 10.81.0.3/24 vnic1
```

앞의 구성은 다음 실패 시나리오에 대한 보호를 제공합니다.

- 로드 밸런서 1이 실패하면 로드 밸런서 2가 기본 로드 밸런서가 됩니다. 로드 밸런서 2가 VIP 10.81.0.3에 대한 주소 해석을 인수하고 클라이언트의 모든 패킷을 대상 IP 주소 10.81.0.3으로 처리합니다.
로드 밸런서 1을 복구하면 로드 밸런서 2가 대기 모드로 돌아갑니다.
- 로드 밸런서 1의 인터페이스가 하나 또는 둘 모두 실패하는 경우 로드 밸런서 2가 기본 로드 밸런서 역할을 인수합니다. 로드 밸런서 2가 VIP 10.81.0.3에 대한 주소 해석을 인수하고 클라이언트의 모든 패킷을 대상 IP 주소 10.81.0.3으로 처리합니다.
로드 밸런서 1의 인터페이스가 둘 모두 양호해지면 로드 밸런서 2가 대기 모드로 돌아갑니다.

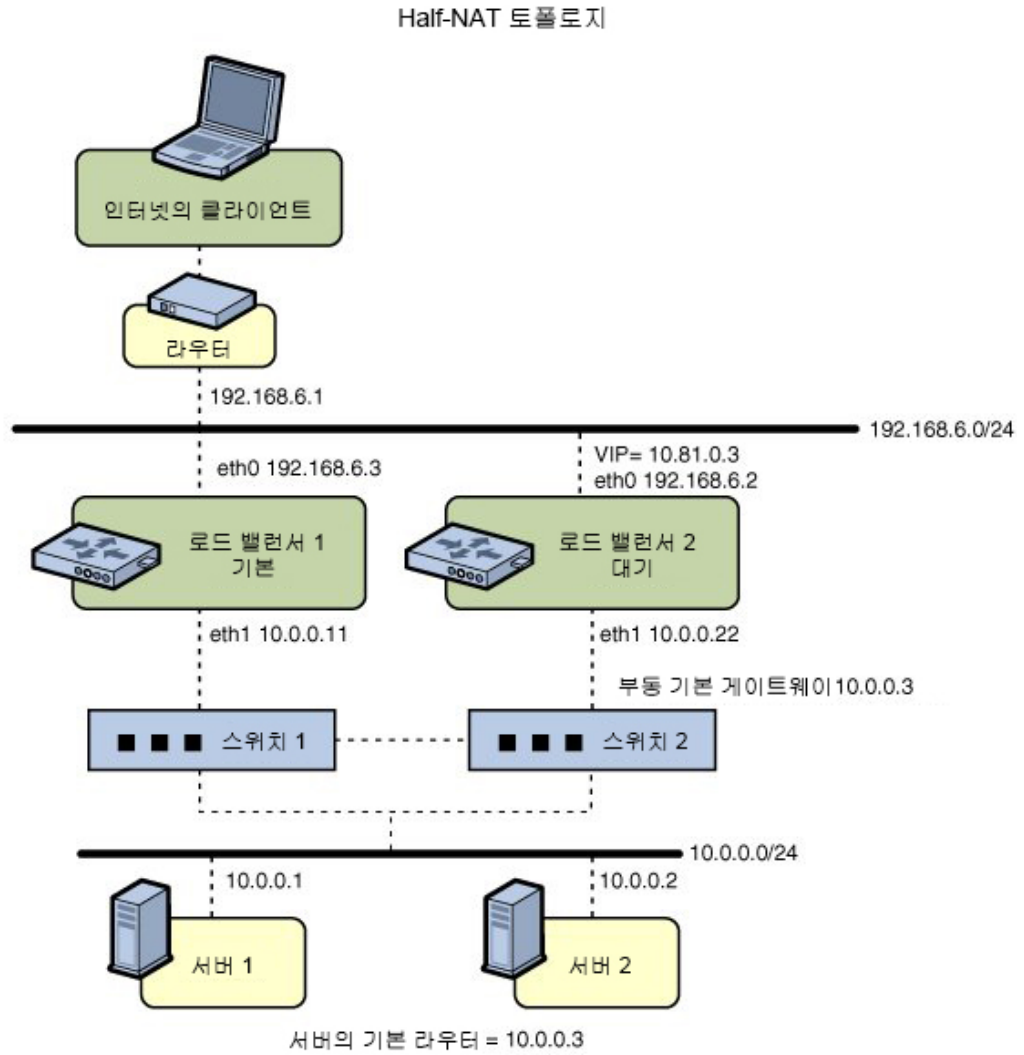
Half-NAT 토폴로지를 사용하여 고가용성 ILB 구성

이 절에서는 Half-NAT 토폴로지를 사용하여 HA를 이루도록 ILB 연결을 설정하는 방법을 설명합니다. 기본 로드 밸런서와 대기 로드 밸런서, 2개의 로드 밸런서를 설정해야 합니다. 기본 로드 밸런서가 실패하면 대기 로드 밸런서가 기본 로드 밸런서의 역할을 맡습니다.

참고 - 현재 ILB 구현은 기본 및 대기 로드 밸런서를 동기화하지 않습니다. 기본 로드 밸런서가 실패하고 대기 로드 밸런서가 역할을 인수하는 경우 기존 연결이 실패합니다. 그러나 동기화 없는 HA는 기본 로드 밸런서가 실패한 상황에서도 여전히 유용합니다.

다음 그림은 HA를 구현하도록 ILB 연결을 구성하기 위한 Half-NAT 토폴로지를 보여줍니다.

그림 7-2 Half-NAT 토폴로지를 사용하여 HA ILB 구성



로드 밸런서의 모든 VIP는 서브넷 192.168.6.0/24를 대상으로 하는 인터페이스에 구성됩니다.

▼ Half-NAT 토폴로지를 사용하여 고가용성 ILB를 구성하는 방법

1. 관리자로 로그인합니다.

자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안”의 “지정된 관리 권한 사용”을 참조하십시오.

2. 기본 및 대기 로드 밸런서를 모두 구성합니다.

```
# ilbadm create servergroup -s server=10.0.0.1,10.0.0.2 sg1
# ilbadm create-rule -ep -i vip=10.81.0.3,port=9001-9006,protocol=udp \
-m lbalg=roundrobin,type=HALF-NAT,pmask=24 \
-h hc-name=hc1,hc-port=9006 \
-t conn-drain=70,nat-timeout=70,persist-timeout=70 -o servergroup=sg1 rule1
```

3. 로드 밸런서 1이 기본 로드 밸런서로 작동하도록 구성합니다.

```
LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB1# ipadm create-ip vnic1
LB1# ipadm create-addr -d -a 10.81.0.3/24 vnic1
LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
LB1# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB1# ipadm create-ip vnic2
LB1# ipadm create-addr -d -a 10.0.0.3/24 vnic2
LB1# vrrpadm create-router -V 2 -A inet -l eth1 -p 255 vrrp2
```

4. 로드 밸런서 2가 대기 로드 밸런서로 작동하도록 구성합니다.

```
LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB2# ipadm create-ip vnic1
LB2# ipadm create-addr -d -a 10.81.0.3/24 vnic1
LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
LB2# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB2# ipadm create-ip vnic2
LB2# ipadm create-addr -d -a 10.0.0.3/24 vnic2
LB2# vrrpadm create-router -V 2 -A inet -l eth1 -p 100 vrrp2
```

5. 부동 기본 게이트웨이의 IP 주소를 두 서버에 추가합니다.

```
# route add default 10.0.0.3
```

이 구성은 다음 실패 시나리오에 대한 보호를 제공합니다.

- 로드 밸런서 1이 실패하면 로드 밸런서 2가 기본 로드 밸런서가 됩니다. 로드 밸런서 2가 VIP 10.81.0.3에 대한 주소 해석을 인수하고 클라이언트의 모든 패킷을 대상 IP 주소 10.81.0.3으로 처리합니다. 로드 밸런서 2도 부동 게이트웨이 주소 10.0.0.3으로 송신한 모든 패킷을 처리합니다.

로드 밸런서 1을 복구하면 로드 밸런서 2가 대기 모드로 돌아갑니다.

- 로드 밸런서 1의 인터페이스가 하나 또는 둘 모두 실패하는 경우 로드 밸런서 2가 기본 로드 밸런서 역할을 인수합니다. 로드 밸런서 2가 VIP 10.81.0.3에 대한 주소 해석을 인수하고 클라이언트의 모든 패킷을 대상 IP 주소 10.81.0.3으로 처리합니다. 로드 밸런서 2도 부동 게이트웨이 주소 10.0.0.3으로 송신한 모든 패킷을 처리합니다.
로드 밸런서 1의 인터페이스가 둘 모두 양호해지면 로드 밸런서 2가 대기 모드로 돌아갑니다.

색인

번호와 기호

- BGP, 11
- direct server return 모드 살펴볼 내용 DSR 모드
 - dladm 명령
 - create-vnic, 33
- DSR 모드
 - 단점, 44
 - 설명, 44
 - 장점, 44
- DSR 토폴로지
 - 구성, 67
- /etc/inet/ndpd.conf 파일, 21
 - 만들기, 21
- EoIB(Ethernet Over InfiniBand)
 - VRRP 및, 28
- Half-NAT 토폴로지
 - 구성, 70
- ILB
 - DSR 모드, 44
 - Full-NAT 규칙 만들기 예, 62
 - ILB 구성 사용 사례, 63
 - ILB 서버 그룹 만들기 및 백엔드 서버 추가 예, 55
 - ILB 서버 그룹에서 백엔드 서버 삭제 예, 57
 - ILB 서버 그룹에서 백엔드 서버를 사용 안함 및 다시 사용으로 설정 예, 56
 - NAT 모드, 44
 - 가져오기
 - 구성, 66
 - 개요, 12
 - 고가용성, 67, 70
 - 관리, 54
 - 구성 요소, 43
 - 구성 하위 명령, 52
 - 규칙, 60
 - 기능, 13
 - 내보내기
 - 구성, 66
 - 명령줄, 52
 - 백엔드 서버, 56
 - 보기 하위 명령, 52
 - 사용 안함으로 설정, 53
 - 사용으로 설정, 53
 - 사용자 권한 부여, 52
 - 상태 검사, 57
 - 서버 그룹, 54
 - 설치, 51
 - 알고리즘, 60
 - 작동 모드, 44
 - 테스트 세부 사항, 59
 - 통계
 - 표시, 64
 - 표시
 - NAT 연결 테이블, 64
 - 세션 지속성 매핑 테이블, 65
 - 통계, 64
 - 프로세스, 48
- ILB 규칙
 - 나열, 61, 62
 - 만들기, 61
 - 삭제, 63
- ILB 서버 그룹
 - 만들기, 54
 - 삭제, 57
 - 정의, 54
 - 추가, 55
 - 표시, 57
- ILB에서 상태 검사
 - 모니터링, 57
- in.ripngd 데몬, 20, 21
- in.routed 데몬
 - 공간 절약 모드, 10
 - 설명, 10

- ipadm 명령
 - create-addr, 35
 - IPv4 라우터
 - 구성, 15
 - IPv6
 - in.ripngd 데몬, 20
 - 라우터 알림, 20
 - IPv6 라우터
 - 구성, 19
 - layer 2 VRRP
 - 제한 사항, 28
 - Layer 2 VRRP 및 Layer 3 VRRP 비교, 26, 26
 - Layer 3 VRRP
 - EoIB(Ethernet Over InfiniBand) 지원, 28
 - 개요, 26
 - 불필요한 ARP 및 NDP 메시지 제어, 40
 - 제한 사항, 28
 - NAT 모드
 - 단점, 46
 - 설명, 45
 - 장점, 46
 - ndpd.conf 파일
 - 만들기, IPv6 라우터, 21
 - network address translator 모드 살펴볼 내용
 - NAT 모드
 - OSPF, 11
 - q 옵션
 - in.routed 데몬, 10
 - quagga 경로 지정 프로토콜 모음, 11
 - RDISC
 - 설명, 11
 - RDISC(ICMP Router Discovery) 프로토콜, 11
 - RIP(Routing Information Protocol)
 - 설명, 10
 - RIPng, 11
 - routeadm 명령
 - IPv6 라우터 구성, 21
 - s 옵션
 - in.routed 데몬, 10
 - VRRP, 23
 - EoIB(Ethernet Over InfiniBand) 지원, 28
 - Layer 2 및 Layer 3 비교, 26
 - VNIC 만들기, 32
 - 개요, 23
 - 계획, 31
 - 구성, 32
 - 권한 부여, 32
 - 라우터 사용 안함으로 설정, 37
 - 마스터 라우터, 24
 - 배타적 IP 영역 지원, 28
 - 백업 라우터, 24
 - 상호 작업
 - 다른 네트워크 기능, 28
 - 설명, 12
 - 설치, 31
 - 제한 사항, 28
 - VRRP 라우터
 - Layer 3 VRRP 라우터 구성 예, 35
 - Layer 3 VRRP 라우터에 대한 가상 IP 주소 구성 예, 36
 - VRRP 라우터 구성 사용 사례, 40
 - VRRP 라우터 만들기 예, 34
 - 가상 IP 주소 구성, 35
 - 개요, 12
 - 구성 정보 표시 예, 37
 - 구성 표시, 37
 - 라우터에 대한 가상 IP 주소 구성 예, 36
 - 만들기, 33
 - 사용으로 설정, 36
 - 삭제, 40
 - 수정, 37
 - 시스템에 Layer 3 라우터 구성 정보 표시 예, 39
 - 연관된 IP 주소 표시, 39
 - 연관된 IP 주소 표시 예, 39
 - VRRP 라우터 및 로드 밸런서
 - 사용하는 이유, 14
 - VRRP 라우터와 연관된 IP 주소
 - 표시, 39
 - VRRP VNIC, 32
 - vrrpadm 명령
 - create-router, 32
 - vrrpadm command
 - show-router, 37
- ㄱ
- 경로 지정 테이블
 - in.routed 데몬 만들기, 10
 - 공간 절약 모드, 10
 - 경로 지정 프로토콜
 - BGP, 11
 - OSPF, 11

- RDISC
 - 설명, 11
 - RIP
 - 설명, 10
 - RIPng, 11
 - VRRP, 12
 - 설명, 9
 - 연관된 경로 지정 데몬, 10
 - 고가용성
 - DSR 토폴로지, 67
 - Half-NAT 토폴로지, 70
 - 공간 절약 모드
 - in.routed 데몬 옵션, 10
 - 관리
 - ILB, 54, 57, 60
 - 구성
 - IPv6 지원 라우터, 21
 - VRRP 라우터에 대한 가상 IP 주소, 35
 - 라우터, 9, 15
- ㄴ**
- 네트워크 구성
 - IPv6 라우터, 21
 - 라우터, 15
- ㄷ**
- 데몬
 - in.ripngd 데몬, 20, 21
- ㄹ**
- 라우터
 - BGP, 11
 - OSPF, 11
 - quagga 경로 지정 프로토콜 모음, 11
 - RIPng, 11
 - VRRP, 12
 - 개요, 9
 - 경로 지정 프로토콜
 - 설명, 9
 - 구성, 9
 - IPv6, 21
 - 네트워크에 대한 기본 라우터 구성 예, 17
 - 정의, 9
 - 라우터 구성
 - IPv4 라우터, 15
 - IPv6 라우터, 19
 - 라우터 알림
 - IPv6, 20
- ㅁ**
- 만들기
 - ILB 규칙, 61
 - ILB 서버 그룹, 54
 - VRRP VNIC, 32
 - VRRP 라우터, 33
 - 상태 검사, 58
 - 메시지
 - 라우터 알림, 20
- ㅂ**
- 백엔드 서버
 - 다시 사용으로 설정, 55
 - 사용 안함으로 설정, 55
 - 삭제, 56
 - 불필요한 ARP 및 NDP 메시지, 40
- ㅅ**
- 사용 안함으로 설정
 - VRRP router, 37
 - 사용으로 설정
 - VRRP 라우터, 36
 - 사이트 접두어, IPv6
 - 알림, 라우터에, 21
 - 삭제
 - VRRP 라우터, 40
 - 상태 검사
 - 결과 표시, 60
 - 만들기, 58
 - 삭제, 60
 - 표시, 59
 - 새 기능
 - routeadm 명령, 21
 - 서버-클라이언트, 48
 - 설치

ILB, 51
VRRP, 31
수정
VRRP 라우터, 37

ㅈ
접두어
라우터 알림, 20

ㅊ
추가
ILB 서버 그룹, 55

ㅋ
클라이언트-서버, 48

ㅌ
토폴로지
DSR, 44
Full-NAT, 48
Half-NAT, 47
통합 로드 밸런서 살펴볼 내용 ILB

ㅍ
표시
VRRP 라우터와 연관된 IP 주소, 39
VRRP 라우터의 구성, 37
상태 검사, 59