네트워크 용어집

부품 번호: E53822
2014년 7월

ORACLE

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

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이센스 계약서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이센스 계약서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이센스, 전송, 배포, 진열, 실행, 발행, 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 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 주기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이센스한 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, 라이센스 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 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이센스에 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 등록상표입니다.

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

목차

이 설명서 사용

- **개요** - Oracle Solaris 네트워크에서 사용되는 공통적인 네트워크 용어 및 머리글자어의 정의를 제공합니다.
- **대상** - 시스템 관리자
- **필요한 지식** - 기본 및 일부 고급 네트워크 관리 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=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 Oracle Solaris의 네트워크 용어

이 용어집에서는 백서, 사양 및 사용자/교육 설명서를 작성하는 작성자를 지원하고 일관성 있게 사용될 수 있도록 Oracle Solaris에서 공통적으로 사용되는 네트워크 용어 및 머리글자어를 정의합니다. 이 용어집에는 일반적으로 모든 네트워크에 적용되는 전체 용어 목록이 포함되지 않습니다. 또한 이 용어집의 용어 대부분은 Oracle Solaris 네트워크 기술과 관련됩니다.

용어집

3DES (Triple-Data Encryption Standard) 데이터를 3회 암호화하기 위해 DES(데이터 암호화 표준) 암호화 알고리즘을 적용하는 대칭 키 암호화 방법입니다. 3DES에는 키 길이 168비트가 필요합니다. 3DES를 3중 DES라고도 합니다.

6to4 IPv4 네트워크를 통해 IPv6 패킷을 전송하는 자동 터널링 방식입니다. 6to4 터널은 격리된 IPv6 사이트가 명시적 터널을 구성할 필요 없이 IPv4를 경유하여 자동 터널을 넘어 통신할 수 있도록 해줍니다.

인터넷 제어 메시지 프로토콜(Internet Control Message Protocol) ICMP를 참조하십시오.

Address Resolution Protocol(주소 결정 프로토콜) ARP를 참조하십시오.

Advanced Encryption Standard(고급 암호화 표준) AES를 참조하십시오.

AES (고급 암호화 표준) 대칭 128비트 블록 데이터 암호화 기술. AES는 미국 정부 암호화 표준입니다.

anet resource(anet 리소스) 기본적으로 모든 Oracle Solaris 영역에 자동으로 구성되는 VNIC입니다. VNIC를 참조하십시오.

anycast address(애니캐스트 그룹) 동일한 애니캐스트 IPv6 주소를 가진 인터페이스 그룹입니다. Oracle Solaris IPv6 구현은 애니캐스트 주소 및 그룹의 생성을 지원하지 않습니다. 그러나 Oracle Solaris IPv6 노드가 애니캐스트 그룹으로 트래픽을 보낼 수 있습니다.

anycast address(애니캐스트 주소) 일반적으로 여러 노드에 속하는 인터페이스 그룹에 지정되는 IPv6 주소입니다. 애니캐스트 주소로 보낸 패킷은 해당 주소를 가진 가장 가까운 인터페이스로 경로가 지정됩니다. 패킷의 경로는 경로 지정 프로토콜의 거리 측정을 준수합니다.

ARP (주소 결정 프로토콜) IP 주소와 이더넷 주소 간의 동적 매핑을 제공하는 프로토콜입니다. ARP는 IPv4 네트워크에서만 사용됩니다. IPv6 네트워크에서는 프로토콜 주소 변환에 Neighbor Discovery 프로토콜을 사용합니다. 자세한 내용은 RFC 826 (http://tools.ietf.org/html/rfc826)을 참조하십시오.

asymmetric key cryptography(비대칭 키 암호화) 메시지를 암호화 및 해독하기 위해 메시지의 발신자 및 수신자가 서로 다른 키를 사용하는 암호화 시스템입니다. 비대칭 키는 대칭 키 암호화에 대한 보안 채널을 설정하는 데 사용됩니다. Diffie-Hellman protocol(Diffie-Hellman 프로토콜)은 비대칭 키 프로토콜의 예입니다.

asymmetric routing(비대칭 경로 지정) 경로에서 패킷이 소스에서 대상으로 이동할 때 발생하지만 소스로 돌아가는 동안 다른 경로를 사용합니다. 일반적으로 계층 3(네트워크 계층)으로 경로 지정된 네트워크에서 보입니다.

asynchronous PPP(비동기 PPP) 한 번에 한 문자씩 데이터를 전송하는 비동기 직렬 회선을 통한 PPP 형식입니다. 가장 일반적인 형식의 PPP인 다이얼 업 링크에는 비동기 PPP 통신이 사용됩니다.

authentication(인증) 원격 사용자 또는 프로그램 등의 엔티티를 통해 네트워크에서 제공되는 ID를 검증하는 작업입니다.

authentication header(인증 헤더) 기밀성 없이 IP 데이터그램에 인증과 무결성을 제공하는 확장 헤더입니다.

autonomous system(자율 시스템) 라우터와 네트워크가 여러 개 포함된 사이트의 네트워크 토폴로지를 관리하는 데 사용되는 단일 경로 지정 도메인입니다. 이 경로 지정 도메인은 하

나 이상 IP 접두어의 연결된 그룹이고 분명히 정의된 단일 경로 지정 정책을 포함합니다. 자세한 내용은 RFC 1930 (http://tools.ietf.org/html/rfc1930)을 참조하십시오.

backup router(백업 라우터) 활성 상태이나 마스터 상태가 아닌 VRID에 대한 VRRP 인스턴스를 백업 라우터라고 합니다. VRID에 대한 백업 라우터 수에는 제한이 없습니다. 현재 마스터 라우터에서 오류가 발생할 경우 백업 라우터가 마스터 라우터 역할을 맡습니다.

bandwidth delay product(대역폭 지연 곱) 네트워크를 통해 전송되는 데이터 양을 결정합니다. 이 데이터는 사용 가능한 네트워크 대역폭과 연결 대기 시간 또는 라운드 트립 시간의 곱입니다.

BGP (Border Gateway Protocol) 자율 시스템 간에 경로 지정 정보를 교환하는 프로토콜입니다. 자세한 내용은 RFC 4271 (http://www.ietf.org/rfc/rfc4271.txt)을 참조하십시오.

bidirectional tunnel(양방향 터널) IP 데이터그램을 양방향으로 모두 전송할 수 있는 터널입니다.

Blowfish 32-448비트의 가변 길이 키를 사용하는 대칭 블록 암호화 알고리즘입니다. 저작자인 Bruce Schneier에 따르면, Blowfish는 키를 자주 바꾸지 않는 응용 프로그램에 최적화되어 있습니다.

BOOTP (Internet Bootstrap Protocol) 네트워크 클라이언트가 서버에서 IP 주소를 얻는 데 사용되는 프로토콜입니다.

Border Gateway Protocol BGP를 참조하십시오.

broadcast(브로드캐스트) 네트워크에서 보낸 사람을 제외하고 서브넷의 모든 시스템에 패킷을 동시에 전송하는 데 사용되는 방법입니다. 일반적으로 브로드캐스트 패킷은 서브넷을 벗어나 경로가 지정되지 않습니다.

CA (인증 기관) 디지털 인증서를 발행하는 신뢰된 타사 조직 또는 회사입니다. 디지털 인증서는 디지털 서명 및 공개-개인 키 쌍을 만드는 데 사용됩니다. CA는 고유 디지털 인증서가 부여된 개인의 ID를 보장합니다.

CA(인증 기관) CA를 참조하십시오.

Callback Control Protocol(콜백 제어 프로토콜) CBCP를 참조하십시오.

CBCP (콜백 제어 프로토콜) 콜백 세션을 협상하기 위해 사용되는 독점적 Microsoft PPP 확장자입니다. Solaris PPP 4.0은 이 프로토콜의 클라이언트(초기 호출자)측만 지원합니다.

CCP (압축 제어 프로토콜) 링크에서 데이터 압축 사용을 협상하는 PPP의 하위 프로토콜입니다. 헤더 압축과 달리 CCP는 링크에서 전송되는 패킷의 모든 데이터를 압축합니다.

certificate revocation list(인증서 해지 목록) CRL을 참조하십시오.

Challenge Handshake Authentication Protocol(Challenge Handshake 인증 프로토콜) CHAP를 참조하십시오.

channel service unit(채널 서비스 장치) CSU를 참조하십시오.

CHAP (Challenge-Handshake 인증 프로토콜) PPP 링크에서 호출자의 ID를 확인하는 데 사용할 수 있는 인증 프로토콜입니다. CHAP 인증은 챌린지 및 응답의 개념을 사용하며 이때 호출을 수신하는 시스템이 호출자로 하여금 ID를 제공하도록 요구합니다.

password authentication protocol(암호 인증 프로토콜)을 참조하십시오.

CHAP secret(CHAP 보안) 식별 목적으로 사용되며 PPP 링크에서 두 피어에 모두 알려지는 ASCII 또는 이진 문자열입니다. CHAP 보안은 시스템의 `/etc/ppp/chap-secrets` 파일에 일반 텍스트로 저장되지만 암호화된 형태여도 PPP 링크로 전송되지 않습니다. CHAP 프로토콜은 호출자가 사용하는 CHAP 보안의 해시가 수신자의 `/etc/ppp/chap-secrets` 파일에 있는 호출자에 대한 CHAP 보안 항목의 해시와 일치하는지 확인합니다.

chat script(채트 스크립트) 원격 피어와의 사이에 통신 링크를 설정하는 방법을 모뎀에 지시하는 명령입니다. PPP 및 UUCP 프로토콜 모두 다이얼 업 링크와 다이얼 백 호출을 설정하기 위해 채트 스크립트를 사용합니다.

Compression Control Protocol(압 CCP를 참조하십시오.

축 제어 프로토콜)

CRL (인증서 해지 목록) CA에서 해지한 공개 키 인증서 목록입니다. CRL은 IKE를 통해 유지 관리하는 CRL 데이터베이스에 저장됩니다.

CSU (채널 서비스 장치) 전용 전자 통신 회선에 로컬 인터페이스를 제공하고 해당 회선을 종료하는 동기식 전자 통신 장치입니다. 미국에서는 CSU가 T1 회선을 종료하고 DS1 또는 DSX 인터페이스를 제공합니다. 기타 국가에서 대개 전자 통신 회사 공급자가 CSU를 소유합니다.

data address(데이터 주소) 데이터의 소스 또는 대상 주소로 사용할 수 있는 IP 주소입니다. 데이터 주소는 IPMP 그룹의 일부이며 그룹의 모든 인터페이스에서 트래픽을 보내고 받는 데 사용될 수 있습니다. 또한 그룹의 한 인터페이스가 작동하는 경우 IPMP 그룹의 데이터 주소 세트를 계속해서 사용할 수 있습니다.

Data Center Bridging Exchange Protocol(데이터 센터 브리징 교환 프로토콜) DCBX를 참조하십시오.

data center bridging(데이터 센터 브리징) DCB를 참조하십시오.

Data Encryption Standard(데이터 암호화 표준) DES를 참조하십시오.

data service unit(데이터 서비스 장치) DSU를 참조하십시오.

datalink multipathing aggregation(데이터 링크 다중 경로 통합) DLMP aggregation (DLMP 통합)을 참조하십시오.

DCB (데이터 센터 브리징) 같은 네트워크 링크를 공유하는 여러 트래픽 유형의 대역폭, 상대적 우선 순위, 플로우 제어를 관리하는 데 사용되는 L2 기술입니다(예: 네트워크와 저장소 프로토콜 간에 데이터 링크 공유 시).

DCBX (데이터 센터 브리징 교환 프로토콜) 데이터 센터 브리징 기능에 대한 구성 정보를 교환하려고 호스트 간에 통신하는 데 사용되는 프로토콜입니다.

DefaultFixed NCP 네트워크 구성이 인스턴스화되지만 모니터되지는 않는 시스템의 유일한 고정적 프로파일입니다.

demilitarized zone DMZ를 참조하십시오.

denial of service attack(서비스 거부 공격) 수신 네트워크 패킷이 의도적으로 또는 의도치 않게 서버를 제압하는 공격입니다. 서버 처리량에 크게 영향을 미치거나 서버가 오버로드되어 작동하지 않을 수 있습니다.

DEPRECATED address (DEPRECATED 주소) IPMP 그룹에서 데이터의 소스 주소로 사용할 수 없는 IP 주소입니다. 일반적으로 IPMP 테스트 주소는 DEPRECATED입니다. 하지만 아무 주소나 DEPRECATED로 표시하여 해당 주소가 소스 주소로 사용되지 않도록 할 수 있습니다.

DES (데이터 암호화 표준) ANSI에 의해 ANSI X.3.92로 표준화된 대칭 키 64비트 블록 데이터 암호화 방법입니다. DES에서는 56비트 키를 사용합니다.

DHCP (동적 호스트 구성 프로토콜) 클라이언트-서버 방식을 사용하여 TCP/IP 네트워크에서 호스트의 자동 네트워크 구성을 가능하게 하는 프로토콜입니다. 이 프로토콜을 사용하여 TCP/IP 네트워크의 호스트에서 지정된 IP 주소를 요청하여 가져오고, 연결된 네트워크에 대한 정보를 검색할 수도 있습니다. IPv4용 DHCP에 대한 자세한 내용은 RFC 2131 (https://www.ietf.org/rfc/rfc2131.txt)을 참조하고, IPv6용 DHCP에 대한 자세한 내용은 RFC 3315 (http://www.ietf.org/rfc/rfc3315.txt)를 참조하십시오.

DHCP unique identifier(DHCP 고유 식별자) DUID를 참조하십시오.

dial-in server(다이얼 인 서버) 다이얼 아웃 시스템에서 호출을 받은 후 다이얼 업 PPP 링크의 수신자 끝을 협상하고 설정하는 피어입니다. “다이얼 인 서버”라는 용어는 공통으로 사용되지만 다이얼 인 서버는 클라이언트 서버 패러다임에 따라 작동하지 않습니다. 단순히 다이얼 업 링크를 설정하라는 요청에 응답하는 피어입니다. 구성 후, 다이얼 업 서버는 임의의 수만큼의 다이얼 아웃 시스템에서 호출을 수신할 수 있습니다.

dial-out machine(다이얼 아웃 시스템) 다이얼 업 PPP 링크를 설정하기 위한 호출을 시작하는 피어입니다. 구성 후, 다이얼 아웃 시스템은 다이얼 인 서버를 임의의 수만큼 호출할 수 있습니다. 다이얼 아웃 시스템은 대개 다이얼 업 링크가 설정되기 전에 인증 자격 증명을 제공합니다.

dial-up PPP link(다이얼 업 PPP 링크) 전화선이나 유사한 통신 매체(예: ISDN에서 제공하는 매체) 끝에서 피어 및 모뎀이 작동하는 PPP 연결입니다. “다이얼 업”이라는 용어는 피어의 전화 번호를 사용하여 로컬 모뎀이 원격 피어로 전화를 걸 때 링크 협상의 시퀀스를 말합니다. 다이얼 업 링크는 가장 일반적이고 비용이 적게 드는 PPP 구성입니다.

Diffie-Hellman protocol(Diffie-Hellman 프로토콜) 두 명의 사용자가 기존 정보 없이 보안되지 않은 통신 매체를 통해 보안 키를 교환할 수 있는 비대칭 암호화 키 계약 프로토콜입니다. 공개 키 암호화는 비대칭 암호화 키 계약 프로토콜을 기반으로 합니다.

diffserv model(diffserv 모델) IP 네트워크에서 차등화 서비스를 구현하기 위한 IETF(Internet Engineering Task Force) 구조 표준입니다. IP 네트워크에서 diffserv 모델은 네트워크 트래픽을 분류 및 관리하고 IPQoS를 제공하기 위한 간단하고 확장 가능한 방식을 제공합니다. 주 모듈에는 분류자, 측정자, 표시자, 스케줄러, 삭제자가 있습니다. IPQoS는 분류자, 측정자, 표시자 모듈을 구현합니다. 자세한 내용은 RFC 2475 (http://www.ietf.org/rfc/rfc2475.txt)를 참조하십시오.

digital signature(디지털 서명) 발신자를 고유하게 식별하는, 전자적으로 전송된 메시지에 첨부된 디지털 코드입니다.

direct memory access DMA를 참조하십시오.

direct server return DSR을 참조하십시오.

DLMP aggregation (DLMP 통합) (데이터 링크 다중 경로 통합) 여러 스위치를 지원하고 데이터 링크에 대한 연속 연결을 제공하는 링크 통합 유형입니다. 스위치가 실패하면 통합은 다른 스위치를 사용하여 해당 데이터 링크에 대한 연결을 계속 제공합니다. 이 유형의 링크 통합에는 스위치 구성이 필요하지 않습니다. 단일 스위치에서 DLMP 통합을 만들 수도 있습니다.

DMA (Direct Memory Access) 일부 장치에서는 CPU의 도움 없이 주 메모리 및 기타 장치와 관련된 데이터 전송을 수행할 수 있습니다. 이 유형의 데이터 전송을 DMA(Direct Memory Access)라고 합니다.

DMZ (DeMilitarized Zone) 조직의 전용 네트워크에 대한 공개 액세스를 방지하려고 설정된 격리 네트워크입니다. 격리 네트워크에는 웹 서버, 익명 FTP 서버, 데이터베이스와 같이 회사가 공개하는 리소스가 포함됩니다.

DN (고유 이름) 일반 문자열을 사용하여 공유 정보를 나타내는 표준화된 방법입니다. DN은 LDAP 및 X.509 인증서와 같은 기술에서 사용됩니다.

DN(고유 이름) DN을 참조하십시오.

DNS (Domain Name System) 이름 지정 정책과 도메인 및 시스템 이름을 엔터프라이즈 외부의 주소(예: 인터넷의 주소)에 매핑하기 위한 방식을 제공하는 서비스입니다. DNS는 인터넷에서 사용되는 네트워크 정보 서비스입니다. 자세한 내용은 RFC 1034 (http://tools.ietf.org/html/rfc1034)를 참조하십시오.

DOI (Domain Of Interpretation) DOI는 데이터 형식, 네트워크 트래픽 교환 유형 및 보안 관련 정보의 이름 지정 규약을 정의합니다. 보안 관련 정보의 예로 보안 정책, 암호화 알고리즘, 암호화 모드 등이 있습니다.

domain name system(DNS, 도메인 이름 시스템) DNS를 참조하십시오.

domain of interpretation DOI를 참조하십시오.

DR (동적 재구성) 시스템이 실행되는 동안 시스템 하드웨어를 재구성하는 데 사용되는 운영 체제 기능입니다. DR을 사용하면 정상적인 시스템 운영을 거의 중단하지 않고 하드웨어 리소스를 추가하거나 바꿀 수 있습니다. Oracle의 모든 Sun 플랫폼에서 DR을 지원하는 것은 아닙니다. 일부 플랫폼은 NIC와 같은 특정 하드웨어 유형의 DR만 지원합니다.

DS codepoint(DS 코드점) DSCP를 참조하십시오.

DSCP (DS 코드점) 패킷 헤더의 DS(차별화 서비스) 필드에 포함된 6비트 값입니다. DSCP는 패킷 전달 방식을 나타냅니다. 자세한 내용은 RFC 2474 (https://www.ietf.org/rfc/rfc2474.txt)를 참조하십시오.

DSR (Direct Server Return) 통합 로드 밸런서에서 백엔드 서버에 대한 수신 요청의 균형을 조정하지만 서버에서 클라이언트로 전달되는 반환 트래픽이 통합 로드 밸런서를 무시하게 하는 모드입니다.

DSU (데이터 서비스 장치) 전용 회선 PPP 링크에서 사용되는 동기식 전자 통신 장치입니다. DSU는 전자 통신 회선에서 사용되며 표준 데이터 통신 인터페이스를 제공하는 데이터 프레이밍 형식입니다.

dual stack(이중 스택) 터널링 방식을 사용하지 않고 IPv4 및 IPv6 프로토콜이 둘 다 같은 네트워크 기반구조에서 작동하게 하는 TCP/IP 프로토콜 스택입니다. Oracle Solaris 네트워크는 이중 스택입니다. 이 이중 스택 기법은 호스트와 라우터에서 둘 다 지원됩니다.

DUID (DHCP Unique Identifier) DHCPv6 지원 시스템에서 클라이언트 시스템을 식별하는 데 사용되는 식별자입니다.

Dynamic Host Configuration Protocol, 동적 호스트 구성 프로토콜 DHCP를 참조하십시오.

dynamic packet filter(동적 패킷 필터) stateful packet filter(stateful 패킷 필터)라고도 합니다.

dynamic reconfiguration (동적 재구성) DR을 참조하십시오.

dynamic routing(동적 경로 지정) 시스템에서 IPv4 네트워크용 RIP 및 IPv6 네트워크용 RIPng와 같은 경로 지정 프로토콜을 사용하여 경로 지정 테이블을 자동으로 업데이트하는 경로 지정 유형입니다. 동적 경로 지정은 호스트가 여러 개 있는 대규모 네트워크에서 사용하는 것이 가장 좋습니다.

ECMP (Equal-Cost Multi-Path) 비용이 같은 여러 경로를 따라 패킷의 경로를 지정하기 위한 경로 지정 기법입니다. 전달 엔진은 다음 홉에 의해 경로를 식별합니다. 패킷을 전달할 때 라우터는 사용할 다음 홉(경로)을 결정해야 합니다. 자세한 내용은 RFC 2992 (http://tools.ietf.org/html/rfc2992)를 참조하십시오.

edge virtual bridging(에지 가상 브리징) EVB를 참조하십시오.

elastic virtual switch(EVS, 탄력적 가상 스위치) EVS를 참조하십시오.

encapsulating security payload(보안 페이로드 캡슐화) ESP를 참조하십시오.

encapsulation (캡슐화) 패킷이 네트워크 프로토콜 스택을 통해 이동함에 따라 각 계층의 프로토콜은 기본 헤더에서 필드를 추가하거나 제거합니다. 송신 호스트의 프로토콜이 패킷 헤더에 데이터를 추가하면 이 프로세스를 데이터 캡슐화라고 합니다.

enhanced transmission selection(향상된 전송 선택) ETS를 참조하십시오.

ENM (외부 네트워크 수정자) 반응적 네트워크 구성의 외부에 있지만 네트워크 구성을 변경 및 수정할 수 있는 응용 프로그램에 대해 생성되는 프로파일입니다. ENM을 사용하면 VPN 응용 프로그램 등의 응용 프로그램이나 스크립트에서 NCP 및 위치 프로파일에 지정된 구성이 아닌 자체 네트워크 구성을 수행해야 하는 경우를 지정할 수 있습니다.

equal-cost multi-path ECMP를 참조하십시오.

ESP (보안 페이로드 캡슐화) IP 데이터그램에 대한 무결성, 기밀성 및 재생 보호를 제공하는 확장 헤더입니다.

ESSID (Extended Service Set Identifier) 인터넷에 연결 및 액세스하기 위한 컴퓨터나 네트워크 장치의 식별 및 주소로 사용되는 전자 표시자 또는 식별자입니다. 802.11b 무선 네트워크의 고유 이름입니다.

Ethernet(이더넷) 근거리 통신망을 형성하기 위해 여러 컴퓨터 시스템을 연결하는 데 사용되는 시스템입니다. 이더넷은 프로토콜을 사용하여 정보 전달을 제어하고 두 개 이상 시스템에 의한 동시 전송을 방지할 수 있습니다.

etherstub Oracle Solaris 네트워크 스택의 데이터 링크 계층(L2)에 구성된 의사 이더넷 NIC입니다. 시스템의 다른 가상 네트워크 및 이더넷 네트워크와 격리되는 개인 가상 네트워크를 구성하기 위해 물리적 링크 대신 etherstub를 통해 VNIC를 만들 수 있습니다.

ETS (향상된 전송 선택) DCB 우선 순위를 기반으로 응용 프로그램에 NIC의 대역폭을 할당하는 DCB 기능입니다.

EVB (에지 가상 브리징) 호스트에서 가상 링크 정보를 외부 스위치와 교환하게 하는 L2 기술입니다. EVB는 트래픽 SLA 적용을 스위치에 오프로드합니다.

EVS (Elastic Virtual Switch) 여러 서버에 걸쳐 탄력적 가상 스위치에 연결된 여러 서버에서 가상 시스템 간의 네트워크 연결을 설정하는 기능을 제공하는 Oracle Solaris의 소프트웨어 가상 스위치입니다.

EVS client(EVS 클라이언트) 탄력적 가상 스위치를 관리하는 소스 EVS 구성 요소입니다.

EVS controller(EVS 컨트롤러) 여러 노드에서 탄력적 가상 스위치의 구성 및 상태를 유지 관리하는 EVS 구성 요소입니다.

EVS node(EVS 노드) 포함된 VNIC가 탄력적 가상 스위치에 연결된 호스트입니다.

expect-send PPP 및 UUCP 채트 스크립트에 사용되는 스크립트 형식입니다. 채트 스크립트는 원격 피어로부터 예상할 텍스트나 명령으로 시작합니다. 다음 행에는 로컬 호스트가 피어에서 정확한 예상 문자열을 수신한 후 *sent*할 응답이 있습니다. 후속 행에서는 통신을 설정하는 데 필요한 모든 명령이 성공적으로 협상될 때까지 로컬 호스트와 피어 사이에 expect-send 명령을 반복합니다.

extended accounting(확장 계정) 작업 또는 프로세스에 따라 자원 소비를 기록하는 유연한 방법입니다.

extended service set identifier ESSID를 참조하십시오.

external network modifier(외부 네트워크 수정자) ENM을 참조하십시오.

failure detection time(실패 감지 시간) FDT를 참조하십시오.

failure detection(실패 감지) 인터페이스 또는 인터페이스에서 인터넷 계층 장치로의 경로가 더 이상 작동하지 않을 경우 이를 감지하는 프로세스입니다. IPMP(IP Network Multipathing) 및 DLMP(데이터 링크 다중 경로)에는 링크 기반(기본값) 및 프로브 기반(옵션)의 두 가지 실패 감지 유형이 포함됩니다.

fault management resource identifier FMRI를 참조하십시오.

FDT (실패 감지 시간) 인터페이스에서 인터넷 계층으로의 인터페이스나 경로가 더는 작동하지 않는지를 감지하는 데 필요한 시간입니다.

filter(필터) IPQoS 구성 파일에 클래스의 특성의 정의하는 규칙 세트입니다. IPQoS 시스템이 IPQoS 구성 파일에서 필터를 준수하는 트래픽 플로우를 처리하기 위해 선택합니다. packet filter(패킷 필터)를 참조하십시오.

firewall(방화벽) 조직의 개인 네트워크 또는 인트라넷을 인터넷에서 격리시켜 외부 침입으로부터 보호하는 하드웨어 또는 소프트웨어입니다. 방화벽은 패킷 필터링, 프록시 서버 및 NAT를 포함할 수 있습니다.

fixed network configuration mode(고정적 네트워크 구성 모드) 네트워크 조건이 변경되는지에 관계없이 시스템에서 인스턴스화된 구성이 지속되는 네트워크 구성 모드입니다. 인터페이스 추가와 같은 해당 변경 사항이 발생하면 시스템이 새 환경에 적응하도록 네트워크를 재구성해야 합니다.

flow accounting(플로우 계산) IPQoS에서 트래픽 플로우에 대한 정보를 누적하고 기록하는 프로세스입니다. IPQoS 구성 파일에 `flowacct` 모듈의 매개변수를 정의하여 플로우 계산을 설정할 수 있습니다.

flow(플로우) 리소스를 사용하여 네트워크 패킷을 처리하는 방식을 추가로 제어하기 위한 사용자 정의된 패킷 분류 방법입니다.

FMRI (Fault Management Resource Identifier) Oracle Solaris의 각 소프트웨어 패키지에 대한 식별자입니다. FMRI에는 패키지 게시자, 패키지 이름 및 소프트웨어 패키지 버전이 포함됩니다.

GARP VLAN Registration Protocol(GARP VLAN 등록 프로토콜) GVRP를 참조하십시오.

GLDv3 (일반 LAN 드라이버 버전 3) GLDv3 프레임워크는 MAC 플러그인과 MAC 드라이버 서비스 루틴 및 구조의 함수 호출 기반 인터페이스입니다. GLDv3 프레임워크는 GLDv3 호환 드라이버 대신 필요한 STREAMS 시작점을 구현하고 DLPI 호환성을 처리합니다.

GVRP (General Attribute Registration Protocol) 연결된 스위치에 VLAN ID를 자동으로 등록하려고 클라이언트 시스템에서 사용되는 프로토콜입니다.

hash-based message authentication code(해시 기반 메시지 인증 코드) HMAC를 참조하십시오.

header(헤더) IP header(IP 헤더)를 참조하십시오.

HMAC (해시 기반 메시지 인증 코드) 메시지 인증을 위해 입력한 해싱 방법입니다. HMAC는 비밀 공유 키와 조합하여 MD5 또는 SHA-1과 같은 반복 암호화 해시 기능과 함께 사용되는 보안 키 인증 알고리즘입니다. 기본 해시 기능의 등록 정보에 따라 HMAC의 암호화 강도가 달라집니다.

hop(홉) 두 호스트를 구분하는 라우터 수를 식별하는 데 사용되는 측정값입니다. 3개의 라우터가 소스 및 대상을 구분하는 경우 호스트가 서로 4홉씩 떨어져 있습니다.

IA (ID 연관) 서버 및 클라이언트에서 관련된 IPv6 주소 세트를 식별, 그룹화, 관리하기 위해 사용되는 방법입니다.

IAID (Identity Association IDentifier) DHCPv6 지원 시스템에서 클라이언트 시스템의 인터페이스를 식별하는 데 사용되는 식별자입니다.

IANA (Internet Assigned Numbers Authority) 등록된 IP 주소를 전 세계 인터넷 레지스트리에 위임하는 조직입니다.

ICMP (인터넷 제어 메시지 프로토콜) 오류를 보고하고 제어 메시지를 교환하는 프로토콜입니다. 네트워크 문제를 진단하는 데 유용합니다.

ICMP 에코 요청 패킷 응답을 요청하기 위해 인터넷을 통해 컴퓨터로 전송되는 패킷입니다. 해당 패킷을 일반적으로 "ping" 패킷이라고 하며 IP 네트워크에서 호스트의 연결을 테스트하는 데 사용됩니다.

identity association identifier IAID를 참조하십시오.

identity association(ID 연관) IA를 참조하십시오.

IKE (Internet Key Exchange) IKE는 IPsec SA(보안 연관)에 대한 인증된 키 관련 자료의 프로비전을 자동화합니다.

ILB (통합 로드 밸런서) 시스템에서 네트워크 처리의 로드를 사용 가능한 리소스 간에 분산하게 하는 L3 및 L4 기술입니다. ILB를 사용하여 안정성과 확장성을 향상하고 네트워크 서비스의 응답 시간을 최소화할 수 있습니다.

InfiniBand 교환 패브릭을 기반으로 하는 I/O 기술입니다. I/O 장치를 호스트에 연결하고 호스트 간에 통신할 수 있도록 대역폭이 높고, 대기 시간이 짧은 상호 연결을 제공합니다. InfiniBand는 고성능 컴퓨팅 및 엔터프라이즈 데이터 센터에서 사용됩니다.

integrated load balancer(통합 로드 밸런서) ILB를 참조하십시오.

Integrated Services Digital ISDN TA를 참조하십시오.

Network terminal adaptor (Integrated Services Digital Network 터미널 어댑터)

Internet Assigned Numbers Authority IANA를 참조하십시오.

Internet Bootstrap Protocol BOOTP를 참조하십시오.

Internet key exchange IKE를 참조하십시오.

Internet Protocol Control Protocol(인터넷 프로토콜 제어 프로토콜) IPCP를 참조하십시오.

Internet Protocol Version 6 Control Protocol(인터넷 프로토콜 버전 6 제어 프로토콜) IPCP를 참조하십시오.

Internet Protocol, version 4(인터넷 프로토콜, 버전 4) IPv4를 참조하십시오.

Internet Protocol, version 6(인터넷 프로토콜, 버전 6) IPv6을 참조하십시오.

Internet Protocol(인터넷 프로토콜) 인터넷을 통해 한 컴퓨터에서 다른 컴퓨터로 데이터가 전송되는 프로토콜입니다.

Internet registry(인터넷 레지스트리) IR을 참조하십시오.

Internet Security Association and Key Management Protocol ISAKMP를 참조하십시오.

IP header(IP 헤더) 인터넷 패킷을 고유하게 식별하는 데이터입니다. 헤더는 패킷의 소스 및 대상 주소를 포함합니다. 헤더 내의 옵션을 사용하여 바이트를 더 추가할 수 있습니다. IPv4 헤더에는 20바이트 데이터가 포함되고 IPv6 헤더에는 40바이트 데이터가 포함됩니다.

IP Multipathing(IP 다중 경로) IPMP를 참조하십시오.

IP Quality of Service IPQoS를 참조하십시오.

IP security(IP 보안) IPsec을 참조하십시오.

IP-in-IP 캡슐화 IP 패킷 내의 IP 패킷을 캡슐화하기 위한 방식입니다. encapsulation (캡슐화)을 참조하십시오.

IPCP (인터넷 프로토콜 제어 프로토콜) 링크에서 피어의 IP 주소를 협상하는 PPP의 하위 프로토콜입니다. 또한 IPCP는 링크의 헤더 압축을 협상하며 네트워크 계층 프로토콜을 사용할 수 있도록 합니다.

IPMP (IP 다중 경로) 시스템에서 네트워크에 지속적으로 액세스하게 해주는 L3(계층 3) 기술입니다. IPMP를 사용하면 여러 IP 인터페이스를 IPMP 그룹으로 구성할 수 있습니다.

IPMP group(IPMP 그룹) IP 다중 경로 그룹은 네트워크 가용성과 사용률 향상을 위해 시스템에서 교환 가능한 것으로 처리되는 데이터 주소 세트를 가진 네트워크 인터페이스 세트로 구성됩니다. 모든 기본 IP 인터페이스와 데이터 주소를 비롯한 IPMP 그룹은 IPMP 인터페이스로 나타냅니다.

IPnet VNIC가 탄력적 가상 스위치와 연결된 IPv4 또는 IPv6 주소 블록입니다. IPv4 또는 IPv6 주소 블록은 블록에 대한 기본 라우터가 있는 같은 서브넷에 있고 Oracle Solaris Elastic Virtual Switch 기능과 함께 사용됩니다.

IPQoS	(IP Quality of Service) diffserv model(diffserv 모델) 표준의 구현과 가상 LAN에 대한 플로우 계정 및 802.1D 표시를 제공하는 소프트웨어 기능입니다. IPQoS를 사용하면 여러 레벨의 네트워크 서비스를 고객과 응용 프로그램에 제공할 수 있습니다.
IPsec	(IP 보안) IP 패킷을 인증 및 암호화하여 IP 통신에 대한 보호를 제공하는 보안 구조입니다.
IPv4	(인터넷 프로토콜, 버전 4) 32비트 주소 공간을 지원하는 인터넷 프로토콜 버전입니다. IPv4를 간략하게 IP라고도 합니다. 자세한 내용은 RFC 791 (http://www.ietf.org/rfc/rfc791.txt)을 참조하십시오.
IPv4 broadcast address(IPv4 브로드캐스트 주소)	주소의 호스트 부분에 모두 0(10.50.0.0)이거나 모두 1비트 (10.50.255.255)가 포함된 IPv4 네트워크 주소입니다. 로컬 네트워크의 시스템에서 브로드캐스트 주소로 보낸 패킷은 해당 네트워크의 모든 시스템에 전달됩니다.
IPv6	(인터넷 프로토콜, 버전 6) 128비트 주소 공간을 지원하는 인터넷 프로토콜 버전입니다. 자세한 내용은 RFC 2460 (http://www.ietf.org/rfc/rfc2460.txt)을 참조하십시오.
IPv6 auto configuration (IPv6 자동 구성)	호스트가 사이트 접두어와 로컬 MAC 주소에서 IPv6 주소를 자동으로 구성하는 프로세스입니다.
IR	(인터넷 레지스트리) IP 주소와 AS(자율 시스템) 번호가 포함된 인터넷 번호의 등록 정보가 들어 있는 레지스트리입니다.
ISAKMP	(Internet Security Association and Key Management Protoco) SA 속성 형식 설정과 SA 협상, 수정 및 삭제를 위한 공통 프레임워크입니다. ISAKMP는 IKE 교환 처리를 위한 IETF 표준입니다.
ISDN TA	(Integrated Services Digital Network 터미널 어댑터) ISDN을 통해 다이얼 업 PPP 링크를 위해 모뎀과 유사한 인터페이스를 제공하는 신호 적용 장치입니다. 표준 모뎀으로 사용될 때 Solaris PPP 4.0 구성 파일을 사용하여 ISDN TA를 구성할 수 있습니다.
key management (키 관리)	암호화 키에 대한 관리입니다. 이 관리에는 사용자 또는 시스템 간의 사용자 레벨에서 수행되는 키의 생성, 교환, 저장, 사용, 교체가 포함됩니다.
keystore name(키 저장소 이름)	관리자가 키 저장소에 지정하는 이름입니다. 암호화 프레임워크에서 키 저장소 이름을 '토큰' 또는 '토큰 ID'라고도 합니다.
keystore(키 저장소)	암호화 키가 저장되는 디스크 또는 카드의 위치입니다.

KMF (Oracle Solaris 키 관리 프레임워크) X.509 인증서 또는 공개/개인 키 쌍을 포함하는 공개 키 객체 관리를 위한 도구 및 프로그래밍 인터페이스를 제공하는 프레임워크입니다. 또한 KMF는 응용 프로그램의 X.509 인증서 사용을 정의하는 정책 관리용 도구를 제공합니다.

LACP (링크 통합 제어 프로토콜) 링크 통합 그룹의 시스템 간에 네트워크 구성 정보를 동적으로 교환하기 위한 IEEE 802.3ad 표준입니다. 이 프로토콜을 통해 링크 통합 그룹을 자동으로 구성하고 유지 관리할 수 있습니다.

LCP (링크 제어 프로토콜) 피어 간의 초기 링크 매개변수 세트를 협상하는 데 사용되는 PPP의 하위 프로토콜입니다. LCP는 연결된 장치의 ID를 확인하고 링크 구성에서 오류를 검색하고 전송할 수 있는 패킷 크기를 결정합니다.

LDAP (Lightweight Directory Access Protocol) IP 네트워크를 통해 디렉토리 정보를 관리하는 데 사용되는 클라이언트-서버 프로토콜입니다. LDAP를 사용하면 정보 저장, 검색, 배포를 단일 지점에서 관리할 수 있습니다. LDAP를 사용하면 LDAP 이름 지정 서비스를 사용하는 클라이언트와 서버가 서로 통신할 수 있습니다. 자세한 내용은 RFC 4511 (https://tools.ietf.org/rfc/rfc4511.txt)을 참조하십시오.

leased-line PPP link(전용 회선 PPP 링크) 공급자가 임대한 동기식 네트워크 매체에 연결된 호스트 및 CSU/DSU를 포함하는 PPP 연결입니다. OC3(Optical Carrier 3) 및 T1(T carrier)은 전용 회선 매체의 일반적인 예입니다. 전용 회선 링크는 다이얼 업 PPP 링크에 비해 관리가 쉬워도 비용이 많이 들기 때문에 일반적이지 않습니다.

Lightweight Directory Access Protocol, 경량 디렉토리 액세스 프로토콜 LDAP를 참조하십시오.

Link Aggregation Control Protocol(링크 통합 제어 프로토콜) LACP를 참조하십시오.

link aggregation(링크 통합) 시스템의 여러 링크를 단일 논리 장치로 결합하여 네트워크 트래픽 처리량을 늘리는 방법입니다.

Link Control Protocol(링크 제어 프로토콜) LCP를 참조하십시오.

Link Layer Discovery Protocol

LLDP를 참조하십시오.

link-local address(링크 로컬 주소)

IPv6에서 자동 주소 구성과 같은 용도로 단일 링크의 주소 지정에 사용되는 지정입니다. 기본적으로 link-local 주소는 시스템의 MAC 주소에서 생성됩니다.

LLDP

(Link Layer Discovery Protocol) IEEE 802 LAN(근거리 통신망)에서 네트워크 장치가 관련 기능, ID 및 현재 상태를 다른 네트워크 장치에 알리는 데 사용되는 링크 계층 프로토콜입니다.

load spreading(로드 확산)

인터페이스를 통해 인바운드 또는 아웃바운드 트래픽을 분배하는 프로세스입니다. 로드 확산을 사용하면 더 높은 처리량을 달성할 수 있습니다. 로드 확산은 네트워크 트래픽이 다중 연결을 사용하는 여러 대상으로 흐르고 있을 때만 발생합니다. 두 가지 유형의 로드 확산은 인바운드 트래픽에 사용되는 인바운드 로드 확산과 아웃바운드 트래픽에 사용되는 아웃바운드 로드 확산입니다.

local-use address(로컬-사용 주소)

서브넷 또는 가입자 네트워크 내에서 로컬 경로 지정 가능 범위만 있는 유니캐스트 주소입니다. 이 주소는 로컬 또는 전역 고유성 범위를 가질 수도 있습니다.

MAC address(MAC 주소)

(Media Access Control 주소) 네트워크 인터페이스에 지정된 고유한 주소입니다. MAC 주소는 물리적 네트워크 세그먼트에 대한 통신에 사용됩니다.

marker(표시자)

1. 패킷의 전달 방법을 나타내는 값으로 IP 패킷의 DS 필드를 표시하는 diffserv 구조 및 IPQoS의 모듈입니다. IPQoS 구현에서 표시자 모듈은 `dscpmk`입니다.

2. 이더넷 데이터그램의 가상 LAN 태그를 사용자 우선 순위 값으로 표시하는 IPQoS 구현의 모듈입니다. 사용자 우선 순위 값은 VLAN 장치가 포함된 네트워크에서 데이터그램의 전달 방법을 나타냅니다. 이 모듈을 `dlcosmk`라고 합니다.

master router(마스터 라우터)

지정된 시점에 가상 라우터에 대해 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.

maximum transmission unit(최대 전송 단위)

MTU를 참조하십시오.

MD5

디지털 서명을 포함하여 메시지 인증용으로 사용되는 반복적인 암호화 해시 함수입니다.

meter(측정자) 특정 클래스에 대한 트래픽 플로우의 비율을 측정하는 diffserv 구조의 모듈입니다. IPQoS 구현에는 `tokenmt` 및 `tswtclmt`의 두 측정자가 포함됩니다.

Microsoft CHAP MS-CHAP를 참조하십시오.

minimal encapsulation(최소 캡슐화) 홈 에이전트, 외래 에이전트, 모바일 노드에서 지원할 수 있는 선택적 형태의 IPv4-in-IPv4 터널링입니다. 최소 캡슐화는 IP-in-IP 캡슐화보다 오버헤드가 8 또는 12바이트 더 적습니다.

MS-CHAP (Microsoft CHAP) PPP용 독점 Microsoft 인증 프로토콜입니다. Solaris PPP 4.0에서는 클라이언트 모드와 서버 모드 모두에서 이 프로토콜의 버전 1과 2가 지원됩니다.

MTU (최대 전송 단위) 링크를 통해 전송할 수 있는 옥테트 단위 제공된 가장 큰 데이터 단위 크기입니다.

multicast address(멀티캐스트 주소) 인터페이스 그룹을 식별하는 IPv4 또는 IPv6 주소입니다. 멀티캐스트 주소로 보낸 패킷은 그룹의 모든 인터페이스로 전달됩니다.

multicast(멀티캐스트) 데이터그램 패킷을 IP 네트워크의 여러 시스템으로 보내는 데 사용되는 네트워크 계층 프로시저입니다. 브로드캐스트 경로 지정과 달리 패킷이 모든 시스템에서 처리되지는 않습니다. 멀티캐스트를 사용하려면 DVMRP(Distance Vector Multicast Routing Protocol)와 같은 특정 경로 지정 프로토콜을 사용하여 라우터를 구성해야 합니다. DVMRP에 대한 자세한 내용은 RFC 1075 (http://tools.ietf.org/rfc/rfc1075.txt)를 참조하십시오.

multihomed host(멀티홈 호스트) 패킷 전달을 수행하지 않는 여러 개의 인터페이스가 있는 시스템입니다. 멀티홈 호스트는 경로 지정 프로토콜을 실행할 수 있습니다.

NAT (네트워크 주소 변환) 한 네트워크에서 사용되는 IP 주소를 다른 네트워크에서 알려진 다른 IP 주소로 변환합니다. 필요한 전역 IP 주소 수를 제한하는 데 사용됩니다.

NCP (네트워크 구성 프로파일) Oracle Solaris에서 시스템 네트워크 구성을 관리하는 프로파일입니다. 시스템에서 NCP는 한 번에 하나만 활성 상태일 수 있습니다.

NCU (네트워크 구성 단위) NCP를 정의하는 모든 등록 정보가 포함된 개별 구성 객체입니다. 각 NCU는 물리적 링크 또는 인터페이스를 나타내며 해당 링크나 인터페이스의 구성을 정의하는 등록 정보를 포함합니다.

neighbor advertisement(이웃 알림) 이웃 간청 메시지에 대한 응답 또는 link-layer 주소 변경을 공지하기 위해 노드가 청하지 않은 이웃 알림을 보내는 프로세스입니다.

neighbor discovery(이웃 검색)

호스트가 연결된 링크에 상주하는 다른 호스트를 찾을 수 있는 IP 방식입니다.

neighbor solicitation(이웃 요청)

이웃의 link-layer 주소를 결정하기 위해 노드에서 보낸 간청입니다. 또한 이웃 간청은 캐시된 link-layer 주소에서 이웃에 아직 연결할 수 있는지 확인합니다.

network address translation(네트워크 주소 변환)

NAT를 참조하십시오.

network configuration profiles(네트워크 구성 프로파일)

NCP를 참조하십시오.

network configuration unit(네트워크 구성 단위)

NCU를 참조하십시오.

Network File System(네트워크 파일 시스템)

NFS를 참조하십시오.

network information service(네트워크 정보 서비스)

NIS를 참조하십시오.

network interface card(네트워크 인터페이스 카드)

NIC를 참조하십시오.

Network Time Protocol

NTP를 참조하십시오.

NFS

(네트워크 파일 시스템) 네트워크에서 공유되는 파일에 원격으로 액세스하는 데 사용되는 파일 시스템 프로토콜입니다.

NIC (네트워크 인터페이스 카드) 컴퓨터를 네트워크에 연결하는 네트워크 어댑터 카드입니다. 일부 NIC는 `igb` 카드와 같은 여러 물리적 인터페이스를 가질 수 있습니다.

NIC rings(NIC 링) NIC에서 수신(Rx) 링과 전송(Tx) 링은 각각 시스템이 네트워크 패킷을 받고 보내는 하드웨어 리소스입니다.

NIS (네트워크 정보 서비스) NIS는 네트워크상의 시스템과 사용자에 대한 핵심 정보를 포함하는 분산 네트워크 데이터베이스입니다.

node(노드) 컴퓨터 네트워크에서 노드는 데이터 전송을 위한 연결 지점 또는 끝점입니다.

NTP (Network Time Protocol) 시스템 시간을 설정 및 유지 관리하는 데 사용되는 프로토콜입니다. NTP 소프트웨어는 RFC 5905 (https://tools.ietf.org/html/rfc5905)에 정의된 버전 4 표준의 전체 구현인 `ntpd` 데몬으로 구현됩니다.

Open Systems Interconnection model (Open Systems Interconnection 모델) OSI model(OSI 모델)을 참조하십시오.

Oracle Solaris Key Management Framework(Oracle Solaris 키 관리 프레임워크) KMF를 참조하십시오.

OSI model(OSI 모델) (Open Systems Interconnection 모델) 네트워크를 통해 데이터를 전송해야 하는 방식을 설명하는 ISO(International Standard Organization)에서 설계된 표준 모델입니다.

outcome(결과) IPQoS에서 트래픽 측정 결과로 수행할 작업입니다. IPQoS 측정자에는 빨간색, 노란색 및 녹색의 세 가지 결과가 있습니다. IPQoS 구성 파일에서 결과를 정의합니다.

packet filter(패킷 필터) 방화벽을 통해 지정된 패킷을 허용하도록 구성하거나 허용하지 않도록 구성할 수 있는 방화벽 기능입니다.

packet header(패킷 헤더) IP header(IP 헤더)를 참조하십시오.

packet(패킷) 통신 회선을 통해 하나의 단위로 전송되는 정보 그룹입니다. IP header(IP 헤더)와 payload(페이로드)를 포함합니다.

PAP (암호 인증 프로토콜) PPP 링크에서 호출자의 ID를 확인하는 데 사용할 수 있는 인증 프로토콜입니다. PAP는 링크를 통해 전달되는 일반 텍스트 암호를 사용하며 끝점 시스템 중 하나에 암호를 저장할 수 있게 해줍니다. 예를 들어, PAP는 호출을 수신하는 시스템의 UNIX `passwd` 데이터베이스에 있는 로그인 및 암호 항목을 사용하여 호출자의 ID를 확인합니다.

password authentication protocol(암호 인증 프로토콜) PAP를 참조하십시오.

payload(페이로드) 패킷에 전달된 데이터입니다. 페이로드는 패킷을 대상으로 가져오는 데 필요한 헤더 정보를 포함하지 않습니다.

PCIe (peripheral component interconnect express) 컴퓨터를 주변 장치와 연결하는 직렬 I/O 버스입니다.

per-hop behavior(홉별 동작) PHB를 참조하십시오.

perfect forward secrecy(완전 순방향 비밀성) PFS를 참조하십시오.

peripheral component interconnect express PCIe를 참조하십시오.

PF (물리적 기능) SR-IOV 사양에 정의된 SR-IOV 기능을 지원하는 PCI 기능입니다. PF는 SR-IOV 기능 구조를 포함하며 SR-IOV 기능을 관리하는 데 사용됩니다. PF는 다른 PCIe 장치처럼 검색, 관리 및 조작할 수 있는 완전형 PCIe 기능입니다. PF에는 전체 구성 리소스가 있으며, PCIe 장치를 구성하고 제어하는 데 사용할 수 있습니다.

PFC (우선 순위 기반 플로우 제어) 데이터 링크 레벨 플로우 제어 방식입니다. PFC는 IEEE 802.1p CoS(Class of Service) 값을 포함하도록 표준 PAUSE 프레임을 확장합니다. PFC에서는 데이터 링크의 모든 트래픽을 중지하지 않고 PFC 프레임에서 사용으로 설정된 CoS 값에 대한 트래픽만 선택적으로 일시 중지합니다.

PFS (완전 순방향 비밀성) PFS에서 데이터 전송을 보호하는 키는 추가 키를 파생하는 데 사용되지 않습니다. 또한 데이터 전송을 보호하는 키의 소스도 추가 키를 파생하는 데 사용되지 않습니다. PFS는 IKE의 인증된 키 교환에 적용됩니다.

PHB (홉별 동작) 홉을 순회할 때 패킷의 트래픽 클래스에 지정된 우선 순위입니다.

physical function(물리적 기능) PF를 참조하십시오.

physical interface(물리적 인터페이스) 시스템의 링크 연결입니다. 이 연결은 종종 장치 드라이버와 NIC로 구현됩니다. 일부 NIC는 여러 연결 지점(예: `igb`)을 가질 수 있습니다.

PKI (공개 키 기반구조) 디지털 인증서, CA 및 인터넷 트랜잭션에 관련된 각 당사자의 유효성을 확인 및 인증하는 기타 등록 기관으로 이루어진 시스템입니다.

Point-to-Point Protocol(지점 간 프로토콜) PPP를 참조하십시오.

port VLAN identifier PVID를 참조하십시오.

PPP (지점 간 프로토콜) 지점 간 매체를 통해 데이터그램을 전송하기 위한 표준 방법을 제공하는 링크 계층 프로토콜입니다. PPP 구성은 피어라고 하는 끝점 컴퓨터 두 대와 전화선 또는 통신을 위해 피어에 사용되는 다른 양방향 링크로 구성됩니다. 두 피어 사이의 하드웨어와 소프트웨어 연결이 *PPP* 링크입니다.

PPP는 PAP, CHAP, LCP 및 CCP를 포함하여 여러 하위 프로토콜로 구성됩니다.

PPP over Ethernet PPPoE를 참조하십시오.

PPPoE (PPP over Ethernet) 호스트가 이더넷 링크를 통해 PPP 세션을 실행할 수 있게 해주는 프로토콜입니다. PPPoE는 공통적으로 DSL(디지털 가입자 회선) 서비스와 함께 사용됩니다.

Precision Time Protocol PTP를 참조하십시오.

priority-based flow control(우선 순위 기반 플로우 제어)

PFC를 참조하십시오.

private address(개인 주소)

인터넷을 통해 경로를 지정할 수 없는 IP 주소입니다. 개인 주소는 인터넷 연결이 필요하지 않은 호스트의 내부 네트워크에서 사용할 수 있습니다. IPv4 개인 주소에 대한 자세한 내용은 RFC 1918 (https://tools.ietf.org/html/rfc1918)을 참조하십시오. IPv6 개인 주소에 대한 자세한 내용은 RFC 4193 (http://www.ietf.org/rfc/rfc4193.txt)을 참조하십시오.

private virtual network(개인 가상 네트워크)

시스템에 있는 다른 가상 네트워크와 외부 네트워크에서 모두 격리된 가상 네트워크입니다. 개인 가상 네트워크는 etherstub를 통해 구성됩니다.

proxy server(프록시 서버)

클라이언트와 다른 서버 사이에 있는 중간 서버입니다. 캐싱 서비스, 관리 제어 및 보안을 제공합니다. 예를 들어 프록시 서버를 사용하여 특정 웹 사이트에 대한 액세스를 차단할 수 있습니다.

PTP

(Precision Time Protocol) 브로드캐스트 도메인의 여러 시스템에서 시스템 시계를 동기화하는 데 사용되는 IEEE 프로토콜입니다. PTP 소프트웨어는 IEEE 표준 1588-2008에 정의된 PTP 버전 2의 구현인 `ptpd` 데몬으로 구현됩니다.

public key cryptography(공개 키 암호화)

수학적으로 연결된 두 개의 다른 키가 필요한 암호화 알고리즘입니다. 공개 키는 모든 사람이 사용할 수 있습니다. 개인 키는 메시지의 수신자만 알 수 있습니다. 공개 키 암호화를 비대칭 암호화라고도 합니다.

public key infrastructure(공개 키 기반 구조)

PKI를 참조하십시오.

PVID

(port VLAN identifier) 링크에 전송되고 링크에서 수신되는 태그가 지정되지 않은 패킷에 대해 가정되는 기본 VLAN ID입니다.

RARP

(Reverse Address Resolution Protocol) IP(인터넷 프로토콜) 주소와 이더넷 주소 간에 동적으로 매핑되는 프로토콜입니다. RARP를 사용하여 근거리 통신망에서 MAC 주소를 IP 주소로 확인합니다. 자세한 내용은 RFC 903 (http://tools.ietf.org/rfc/rfc903.txt)을 참조하십시오.

RCM

(reconfiguration coordination manager) 시스템 구성 요소의 동적 제거를 관리하고 순차적으로 시스템 리소스를 등록 및 해제하게 도와주는 프레임워크입니다.

reactive network configuration mode(반응적 네트워크 구성 모드) 수동으로 다시 구성할 필요 없이 시스템이 네트워크 조건 변경에 맞게 자동으로 조정되는 네트워크 구성 모드입니다.

reconfiguration coordination manager RCM을 참조하십시오.

redirect(재지정) 라우터에서 특정 대상에 연결하기 위해 더 좋은 첫번째 홉 노드를 호스트에 알려주는 것입니다.

reflective relay(반사 중계) 외부 스위치에 의해 루프백되도록 유선으로 VM 간 트래픽을 전송하는 옵션을 제공하는 EVB의 기능입니다. 이 기능을 사용하면 GbE(기가비트 이더넷)에서 가상화된 10GbE로 이동하면서 외부 스위치에서는 IT 정책을 유지할 수 있습니다.

repair detection(복구 감지) NIC 또는 NIC에서 계층 3 장치로의 경로가 오류 발생 후에 올바르게 작동하기 시작할 때 이를 감지하는 프로세스입니다.

replay attack(재생 공격) 데이터 전송 중에 침입자가 패킷을 캡처하는 네트워크 공격입니다. 캡처된 패킷은 사기성 패킷으로 바뀌거나 나중에 반복됩니다. 이러한 공격으로부터 보호하려면 패킷을 보호 중인 보안 키의 수명 주기 동안 증분하는 필드를 포함할 수 있습니다.

Reverse Address Resolution Protocol(역순 주소 결정 프로토콜) RARP를 참조하십시오.

RIP (Routing Information Protocol) IPv4 패킷의 경로를 지정하고 LAN에 있는 모든 호스트의 경로 지정 테이블을 유지 관리하는 내부 게이트웨이 프로토콜입니다. 자세한 내용은 RFC 2453 (https://tools.ietf.org/html/rfc2453)을 참조하십시오.

RIPng (Routing Information Protocol next generation) IPv6 패킷의 경로를 지정하고 LAN에 있는 모든 호스트의 경로 지정 테이블을 유지 관리하는 내부 게이트웨이 프로토콜입니다. 자세한 내용은 RFC 2080 (http://tools.ietf.org/rfc/rfc2080.txt)을 참조하십시오.

router advertisement (라우터 알림) 정기적으로 또는 라우터 간청 메시지의 응답으로, 라우터가 다양한 링크 및 인터넷 매개변수를 함께 사용하여 자신의 존재를 알리는 프로세스입니다.

router discovery(라우터 검색)	호스트가 연결된 링크에 상주하는 라우터를 찾는 프로세스입니다.
router solicitation(라우터 요청)	호스트가 다음 일정이 잡힌 시간이 아닌, 즉시 라우터 알림을 생성하도록 라우터에 요청하는 프로세스입니다.
router(라우터)	인터페이스가 두 개 이상 있고 경로 지정 프로토콜을 실행하며 컴퓨터 네트워크 간에 데이터 패킷을 전달하는 시스템입니다. 라우터는 인터넷에서 트래픽을 전송하고 여러 네트워크의 데이터 회선을 두 개 이상 연결합니다. 라우터는 패킷이 대상에 도달할 때까지 네트워크를 통해 데이터 패킷을 한 라우터에서 다른 라우터로 전달합니다.
Routing Information Protocol	RIP를 참조하십시오.
Routing Information Protocol next generation	RIPng를 참조하십시오.
routing table(경로 지정 테이블)	패킷에 대상에 도달하는 최적 경로를 결정하게 도와주는 패킷에 대한 경로 지정 정보가 포함된 테이블입니다.
RSA	디지털 서명 및 공개 키 암호화 체계를 얻기 위한 방법입니다.
SA	(보안 연관) 한 호스트의 보안 등록 정보를 두번째 호스트에 지정하는 연관입니다.
SADB	(보안 연관 데이터베이스) 암호화 키와 암호화 알고리즘을 지정하는 SA 테이블입니다. 키 및 알고리즘은 보안 데이터 전송에 사용됩니다.
SCTP	TCP와 유사한 방식으로 연결 지향 통신을 제공하는 전송 계층 프로토콜입니다. 추가적으로, SCTP는 멀티홈 기능을 지원하므로 연결 끝점 중 하나가 여러 개의 IP 주소를 가질 수 있습니다. 자세한 내용은 RFC 4960 (http://tools.ietf.org/html/rfc4960)을 참조하십시오.
Secure Hashing Algorithm(보안 해시 알고리즘)	SHA-1을 참조하십시오.
secure sockets layer	SSL을 참조하십시오.

security association(보안 연관) SA를 참조하십시오.

security associations database(보안 연관 데이터베이스) SADB를 참조하십시오.

security parameter index(보안 매개변수 색인) SPI를 참조하십시오.

security policy database(보안 정책 데이터베이스) SPD를 참조하십시오.

selector(선택기) IPQoS에서 네트워크 스트림의 트래픽을 선택하기 위해 특정 클래스의 패킷에 적용할 기준을 구체적으로 정의하는 요소입니다. IPQoS 구성 파일의 filter 절에 선택기를 정의합니다.

service management facility(서비스 관리 기능) SMF를 참조하십시오.

SHA-1 (보안 해시 알고리즘) 메시지 다이제스트를 생성하기 위해 2^{64}보다 작은 입력 길이에서 작동하는 알고리즘입니다. SHA-1 알고리즘은 DSA로 입력됩니다.

Simple Network Management Protocol, 단순 네트워크 관리 프로토콜 SNMP를 참조하십시오.

single root I/O virtualization SR-IOV를 참조하십시오.

SMF (서비스 관리 기능) 종속 서비스를 필요 시에 자동으로 다시 시작할 수 있도록 응용 프로그램 또는 서비스 간의 관계를 정의하는 기능입니다.

smurf attack(스머프 공격) 원격 위치에서 IP 브로드캐스트 주소 또는 여러 브로드캐스트 주소로 보내는 ICMP 에코 요청 패킷을 사용하여 심각한 네트워크 혼잡 또는 정전을 초래하는 프로세스입니다.

sniff(스니프) 컴퓨터 네트워크에서 도청하는 것입니다. 일반 텍스트 암호, 유선 끄기와 같은 정보를 조사하기 위해 자동화된 프로그램의 일부로 자주 사용됩니다.

SNMP (Simple Network Management Protocol) IP 네트워크에 연결된 장치를 조회, 모니터, 관리하기 위한 일반적인 방법을 제공하는 프로토콜입니다.

Spanning Tree Protocol(STP, 스패닝 트리 프로토콜) STP를 참조하십시오.

SPD (보안 정책 데이터베이스) IPsec으로 보호되는 패킷에 적용할 보호 레벨을 지정하는 데이터베이스입니다. SPD는 IP 트래픽을 필터링하여 패킷을 무시할지, 네트워크에서 전송할지 또는 IPsec으로 보호할지를 결정합니다.

SPI (보안 매개변수 색인) 수신자가 수신된 패킷의 암호를 해독하는 데 사용하는 SADB의 행을 지정하는 정수입니다.

spoof(스푸핑) 메시지가 신뢰된 호스트에서 들어오고 있음을 나타내는 메시지를 IP 주소와 함께 보내어 컴퓨터에 허용되지 않은 액세스를 얻는 것입니다. IP 스푸핑을 실행하는 발신자는 먼저 여러 가지 기술을 시도하여 인증된 호스트의 IP 주소를 찾은 다음 패킷이 해당 호스트에서 들어온 것처럼 나타나도록 패킷 헤더를 수정합니다.

SR-IOV (Single Root I/O Virtualization) 가상 시스템 간에 PCIe(Peripheral Component Interconnect Express) 장치를 효율적으로 공유할 수 있게 하고 하드웨어에서 구현되는 표준입니다. SR-IOV 사양을 사용하여 가상 시스템을 I/O 장치에 직접 연결할 수 있습니다.

SSL (Secure Sockets Layer) HTTP 및 FTP 같은 프로토콜에서 사용되는 보안 하위 레벨 암호화 형식입니다. SSL 프로토콜에는 서버 인증, 전송 중 데이터 암호화 및 선택적 클라이언트 인증에 대한 프로비전이 포함됩니다.

SSL kernel proxy(SSL 커널 프록시) 구성 가능한 프록시는 커널에서 실행되어 SSL(Secure Sockets Layer)로 보호되는 웹 서버 통신 속도를 높입니다.

standby interface(대기 인터페이스) 다른 물리적 인터페이스에서 오류가 발생한 경우에만 데이터 트래픽 전달에 사용되는 물리적 인터페이스입니다.

stateful packet 활성 연결의 상태를 모니터하여 얻은 정보를 바탕으로 네트워크 패킷이 packet filter(패킷 필터)를 통과할지 여부를 확인할 수 있는 firewall(방화

filter(stateful 패킷 필터) 벽)입니다. 요청 및 회신을 추적하고 일치시키면 stateful 패킷 필터가 요청과 일치하지 않는 회신을 차단할 수 있습니다.

stateless auto configuration (stateless 자동 구성) 호스트가 로컬 IPv6 라우터에서 보급한 MAC 주소와 IPv6 접두어를 결합하여 고유의 IPv6 주소를 생성하는 프로세스입니다.

static routing(정적 경로 지정) 시스템 네트워크 관리자가 라우터를 경로 지정 테이블에 수동으로 추가할 수 있는 프로세스입니다.

STP (Spanning Tree Protocol) 하위 네트워크를 사용할 수 없게 만드는 네트워크 루프를 방지하기 위해 브리지된 네트워크에서 사용되는 기본 프로토콜입니다.

Stream Control Transport Protocol(흐름 제어 전송 프로토콜) SCTP를 참조하십시오.

subnet(서브넷) 각 넷마스크를 포함하여 서브넷 번호 및 IP 주소 스키마와 시스템을 연결하는 IP 네트워크의 논리적 세분화입니다.

symmetric key cryptography (대칭 키 암호화) 메시지의 발신자 및 수신자가 단일의 공통 키를 공유하는 암호화 시스템입니다. 이 공통 키는 메시지를 암호화 및 해독하는 데 사용됩니다. Advanced Encryption Standard(고급 암호화 표준)은 대칭 키의 예입니다.

synchronous PPP(동기식 PPP) 데이터를 원시 비트의 지속적 스트림으로 전송하는 동기식 디지털 회선에서 실행되는 PPP 형식입니다. 전용 회선 PPP 링크는 동기식 PPP를 사용합니다.

tenant(테넌트) 탄력적 가상 스위치의 가상 스위치는 논리적으로 함께 그룹화됩니다. 각 논리 그룹을 테넌트라고 합니다. 테넌트 내의 탄력적 가상 스위치에서 정의 리소스는 테넌트의 이름 공간 외부에 표시되지 않습니다. 테넌트는 모든 테넌트의 리소스를 함께 포함하는 컨테이너로 사용됩니다.

test address(테스트 주소) 프로브의 소스 또는 대상 주소로 사용해야 하고 데이터 트래픽의 소스 또는 대상 주소로 사용하면 안 되는 IPMP 그룹의 IP 주소입니다.

TFTP (Trivial File Transfer Protocol) 네트워크 구성 서버와 네트워크 클라이언트 간에 파일을 전송하는 데 사용되는 파일 전송 프로토콜입니다. 일

	반적으로 TFTP는 로컬 네트워크의 시스템 간에 구성이나 부트 파일을 자동으로 전송하는 데 사용됩니다. 자세한 내용은 RFC 1350 (http://www.ietf.org/rfc/rfc1350.txt)을 참조하십시오.
Triple-Data Encryption Standard(3중 데이터 암호화 표준)	3DES를 참조하십시오.
Trivial File Transfer Protocol	TFTP를 참조하십시오.
trunk aggregation(트렁크 통합)	IEEE 802.3ad 표준을 기반으로 하는 링크 통합입니다. 여러 트래픽 플로우가 통합된 포트 세트에 걸쳐 분산될 수 있게 하면 트렁크 통합이 작동합니다. IEEE 802.3ad가 여러 스위치에서 작동하려면 스위치 구성과 스위치 공급업체에서 제공하는 확장 기능이 필요합니다.
trusted callers(신뢰할 수 있는 호출자)	PPP에서 다이얼 인 서버가 서버의 PAP 또는 CHAP 보안 데이터베이스에 있는 피어의 보안 자격 증명을 포함시켜 액세스를 부여하는 원격 피어입니다.
UDP	(사용자 데이터그램 프로토콜) 컴퓨터에서 특수 전송 채널이나 데이터 경로를 설정하지 않고 IP 네트워크의 다른 컴퓨터에 데이터그램을 전송하는 데 사용되는 프로토콜입니다. 자세한 내용은 RFC 768 (http://www.ietf.org/rfc/rfc768.txt)을 참조하십시오.
unicast address(유니캐스트 주소)	IPv6 사용 노드의 단일 인터페이스를 식별하는 IPv6 주소입니다. 유니캐스트 주소의 부분은 사이트 접두어, 서브넷 ID, 인터페이스 ID입니다.
uniform resource indicator	URI를 참조하십시오.
uniform resource locator	URL을 참조하십시오.
UNIX-to-UNIX Copy Program	UUCP를 참조하십시오.
uplink port(업링크 포트)	Oracle Solaris EVS 기능을 사용할 때 VNIC가 생성되는 데 사용되는 데이터 링크입니다.

URI (Uniform Resource Indicator) 인터넷이나 개인 인트라넷에서 리소스를 식별하는 주소 지정 기술입니다.

URL (Uniform Resource Locator) 인터넷이나 개인 인트라넷에서 리소스를 식별하는 문자열입니다.

User Datagram Protocol(사용자 데이터그램 프로토콜) UDP를 참조하십시오.

user-priority(사용자 우선 순위) CoS(Class-of-Service) 표시를 구현하는 3비트 값입니다. CoS는 VLAN 장치의 네트워크에서 이더넷 데이터그램이 전달되는 방식을 정의합니다.

UUCP (UNIX-to-UNIX Copy Program) 컴퓨터에서 파일을 전송하고 서로 메일을 교환할 수 있게 하는 프로그램입니다. 또한 UUCP를 통해 컴퓨터에서 Usenet과 같은 대규모 네트워크에 참가할 수 있습니다.

VDP (VSI Discovery and Configuration Protocol) EVB에서 VSI(Virtual Switch Interface)에 대한 정보를 교환하는 데 사용되는 프로토콜입니다.

VF (가상 기능) 물리적 기능과 연관된 SR-IOV 기능입니다. VF는 하나 이상의 물리적 리소스를 물리적 기능 및 같은 PF와 연관된 다른 VF와 공유하는 경량형 PCIe 기능입니다. VF는 자체 동작을 위한 구성 리소스만 포함할 수 있습니다.

virtual extensible local area network VXLAN을 참조하십시오.

virtual function(가상 기능) VF를 참조하십시오.

Virtual IP address(가상 IP 주소) VRIP를 참조하십시오.

virtual LAN device(가상 LAN 장치) VLAN device(VLAN 장치)를 참조하십시오.

virtual local area network(가 VLAN을 참조하십시오.

상 근거리 통신망)

virtual network identifier
VNI를 참조하십시오.

virtual network interface card(가상 네트워크 인터페이스 카드)
VNIC를 참조하십시오.

virtual network(가상 네트워크)
물리적 네트워크를 에뮬레이트하고 하드웨어 및 소프트웨어 네트워크 리소스의 조합인 네트워크입니다.

virtual port(가상 포트)
VNIC와 탄력적 가상 스위치 간의 연결 지점입니다. 가상 포트는 가상 포트에 연결될 때 VNIC가 상속하는 다양한 네트워크 구성 매개변수를 캡슐화합니다.

virtual private network(가상 사설망)
VPN을 참조하십시오.

Virtual Router ID(가상 라우터 ID)
VRID를 참조하십시오.

Virtual Router Redundancy Protocol
VRRP를 참조하십시오.

virtual station instance(가상 스테이션 인스턴스)
VSI를 참조하십시오.

virtual switch(가상 스위치)
가상 시스템 간에 통신을 용이하게 하는 엔티티입니다. 가상 스위치는 물리적 시스템 내에서 가상 시스템 간에 트래픽(VM 간 트래픽)을 루프하고 이 트래픽을 유선으로 전송하지 않습니다. 가상 스위치는 EVS에서 관리될 수 있고 VNIC가 생성될 때 자동으로 인스턴스화됩니다.

VLAN
(가상 근거리 통신망) 프로토콜 스택의 데이터 링크 계층에서 근거리 통신망의 세분화를 나타냅니다.

VLAN device(VLAN 장치) (가상 LAN 장치) IP 프로토콜 스택의 이더넷(데이터 링크) 레벨에서 트래픽 전달을 제공하는 네트워크 인터페이스입니다.

VNI (virtual network identifier) VXLAN은 VNI라고도 하는 VXLAN 세그먼트 ID를 사용하여 식별합니다. 모든 VXLAN 데이터 링크는 VNI와 연관됩니다.

VNIC (가상 네트워크 인터페이스 카드) 구성될 때 물리적 NIC처럼 동작하는 L2 엔티티 또는 가상 네트워크 장치입니다. VNIC를 탄력적 가상 스위치에 연결하거나 여러 영역 또는 VM(가상 시스템) 간에 VNIC를 공유하도록 기본 데이터 링크를 통해 VNIC를 구성합니다.

VPN (가상 사설망) 인터넷과 같은 공개 네트워크에서 터널을 사용하는 단일 보안 논리적 네트워크입니다.

VRID (가상 라우터 ID) 지정된 네트워크 세그먼트에서 가상 라우터를 식별하는 데 사용되는 고유한 숫자입니다. VRID는 LAN 내에서 가상 라우터를 식별합니다.

VRIP (가상 IP 주소) 다른 호스트가 네트워크 서비스를 가져오는 VRID와 연결된 IP 주소입니다. VRIP는 VRID에 속한 VRRP 인스턴스에 의해 관리됩니다.

VRRP (Virtual Router Redundancy Protocol) 라우터와 로드 밸런서 등에 사용되는 IP 주소의 고가용성을 제공하는 프로토콜입니다.

VSI (가상 스테이션 인스턴스) VSI는 스테이션에 구성된 VNIC를 나타냅니다.

VSI Discovery and Configuration Protocol VDP를 참조하십시오.

VXLAN (Virtual extensible Local Area Network) 데이터 링크(L2) 네트워크를 IP(L3) 네트워크의 맨 위에 오버레이하는 방식으로 작동하는 L2 및 L3 기술입니다. VXLAN은 VLAN을 사용할 때 적용되는 4K 제한을 해결합니다. 일반적으로 VXLAN은 클라우드 기반구조에서 여러 가상 네트워크를 격리하는 데 사용됩니다.

VXLAN segment ID(VXLAN 세그먼트 ID) VNI를 참조하십시오.

WAP (Wireless Application Protocol) 모바일 무선 네트워크를 통해 정보에 액세스하기 위한 표준 프로토콜입니다.

WEP key(WEP 키) (Wired Equivalent Privacy 키) 보안 Wi-Fi 네트워크와의 연결을 설정하는 키입니다.

wired equivalent privacy key(wired equivalent privacy 키)

WEP key(WEP 키)를 참조하십시오.

Wireless Application Protocol

WAP를 참조하십시오.