# Glossary of Networking Terms

**Part No: E54755**
November 2016

Glossary of Networking Terms

**Part No: E54755**

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

**Documentation Accessibility**

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

**Access to Oracle Support**

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

**Référence: E54755**

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu’elles soient exemptes d’erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d’applications de gestion des informations. Ce logiciel ou matériel n’est pas conçu ni n’est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d’applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l’utilisation de ce logiciel ou matériel pour ce type d’applications.

Ce logiciel ou matériel et la documentation qui l’accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l’accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

**Accessibilité de la documentation**

Pour plus d’informations sur l’engagement d’Oracle pour l’accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l’adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

**Accès aux services de support Oracle**

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d’informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

# Contents

# Using This Documentation

- **Overview** – Provides definitions of common networking terms and acronyms used in the context of Oracle Solaris networking.
- **Audience** – System administrators.
- **Required knowledge** – Basic and some advanced network administration skills.

## Product Documentation Library

Documentation and resources for this product and related products are available at `http://www.oracle.com/pls/topic/lookup?ctx=E53394`.

## Feedback

Provide feedback about this documentation at `http://www.oracle.com/goto/docfeedback`.

♦ ♦ ♦ CHAPTER 1

# Networking Terms in Oracle Solaris

This glossary defines commonly used networking terms and acronyms in Oracle Solaris to assist anyone in writing white papers, specifications, and user and training documentation and to help ensure consistent usage. This glossary does not include an exhaustive list of terms that generally apply to all of networking. Also, many of the terms in this glossary are specific to Oracle Solaris networking technologies.

## Glossary

**3DES** (Triple-Data Encryption Standard) A symmetric-key encryption method that applies the Data Encryption Standard (DES) cipher algorithm to encrypt data three times. 3DES requires a key length of 168 bits. 3DES is also referred as Triple-DES.

**6to4** An automatic tunneling mechanism that transfers IPv6 packets over an IPv4 network. 6to4 tunnels enable isolated IPv6 sites to communicate across an automatic tunnel over an IPv4 without the need to configure explicit tunnels.

**Address Resolution Protocol** See ARP.

**Advanced Encryption Standard** See AES.

**AES** (Advanced Encryption Standard) A symmetric 128-bit block data encryption technique. AES is the U.S. government encryption standard.

**`anet` resource** A VNIC or an IPoIB partition datalink that is configured by using the `zonecfg` command for Oracle Solaris Zones and instantiated when the zone boots. See also VNIC.

**anycast address** An IPv6 address that is assigned to a group of interfaces, usually belonging to different nodes. A packet that is sent to an anycast address is routed to the nearest interface having that address. The packet's route is in compliance with the routing protocol's measure of distance.

**anycast group** A group of interfaces with the same anycast IPv6 address. The Oracle Solaris implementation of IPv6 does not support the creation of anycast addresses and groups. However, Oracle Solaris IPv6 nodes can send traffic to anycast groups.

**ARP** (Address Resolution Protocol) A protocol that provides dynamic mapping between IP addresses and the Ethernet addresses. ARP is used with IPv4 networks only. IPv6 networks use the Neighbor Discovery Protocol for translating protocol addresses. For more information, see RFC 826 (`http://tools.ietf.org/html/rfc826`).

**asymmetric key cryptography** An encryption system in which the sender and receiver of a message use different keys to encrypt and decrypt the message. Asymmetric keys can be used to establish a secure channel for symmetric key encryption. The Diffie-Hellman protocol is an example of an asymmetric key protocol.

**asymmetric routing** Occurs when a packet travels from a source to a destination in a path but takes a different path while returning to the source. Commonly seen in the Layer-3 (network layer) routed networks.

**asynchronous PPP** A form of PPP over asynchronous serial lines, which transfer data one character at a time. The most common form of PPP configuration, the dial-up link, uses asynchronous PPP communications.

**authentication** The act of verifying the identity that is supplied over the network by a remote user or entity, such as a program.

**authentication header** An extension header that provides authentication and integrity without confidentiality to IP datagrams.

**autonegotiation** An Ethernet procedure in which two connected devices share their capabilities regarding transmission parameters, such as speed, duplex mode, and flow control. The connected devices use the highest performance transmission mode that they support.

**autonomous system** A single routing domain that is used for administering the network topology of sites with multiple routers and networks. This routing domain is a connected group of one or more IP prefixes and has a single and clearly defined routing policy. For more information, see RFC 1930 (`http://tools.ietf.org/html/rfc1930`).

**backup router** A VRRP instance for a VRID that is active but not in the master state is called a backup router. Any number of backup routers can exist for a VRID. A backup router assumes the role of a master router if the current master router fails. See also VRRP and VRID.

**bandwidth control** Enables you to control the available bandwidth of a physical NIC on a per-application, per-port, per-protocol, and per-address basis.

**bandwidth delay product** Determines the amount of data sent through the network. This data is the product of the available network bandwidth and the connection latency or round-trip time.

**bandwidth share** The minimum share of the bandwidth that the VNIC will get when there is competition from other VNICs on the same datalink.

**BGP** (Border Gateway Protocol) A protocol that exchanges routing information between autonomous systems. For more information, see RFC 4271 (`http://www.ietf.org/rfc/rfc4271.txt`).

**bidirectional tunnel** A tunnel that can transmit packets in both directions.

**Blowfish** A symmetric block cipher algorithm that takes a variable-length key from 32 bits to 448 bits. Its author, Bruce Schneier, claims that Blowfish is optimized for applications where the key does not change often.

**BOOTP** (Internet Bootstrap Protocol) A protocol that is used by a network client to obtain an IP address from a server.

**Border Gateway Protocol** See BGP.

**broadcast** In networking, a method that is used to transmit packets simultaneously to every system on a subnet except the sender. Broadcast packets are usually not routed beyond the subnet.

**CA** (certificate authority) A trusted third-party organization or company that issues digital certificates. The digital certificates are used to create digital signatures and public-private key pairs. CA guarantees the identity of the individual who is granted the unique digital certificate.

**Callback Control Protocol** See CBCP.

**CBCP** (Callback Control Protocol) A proprietary Microsoft PPP extension that is used to negotiate a callback session. Solaris PPP 4.0 supports only the client (initial caller) side of this protocol.

**CCP** (Compression Control Protocol) A subprotocol of PPP that negotiates the use of data compression on the link. Unlike header compression, CCP compresses all the data within packets that are sent on the link.

**certificate authority** See CA.

**certificate revocation list** See CRL.

**Challenge Handshake Authentication Protocol** See CHAP.

**channel service unit** See CSU.

**CHAP** (Challenge Handshake Authentication Protocol) An authentication protocol that can be used to verify the identity of a caller on a PPP link. CHAP authentication uses the notion of *challenge* and *response*, where the system that receives a call challenges the caller to prove its identity.

See also password authentication protocol.

**CHAP secret** An ASCII or binary string that is used for identification purposes and is known to both peers on a PPP link. The CHAP secret is stored in clear text in a system's `/etc/ppp/chap-secrets` file but is never sent over the PPP link, not even in encrypted form. The CHAP protocol verifies that a hash of the CHAP secret that is used by a caller matches a hash of the CHAP secret entry for the caller in the recipient's `/etc/ppp/chap-secrets` file.

**chat script** Instructions that tell a modem how to establish a communications link between itself and a remote peer. Both the PPP and UUCP protocols use chat scripts for establishing dial-up links and dial-back calling.

**community VLAN** A type of secondary VLAN. The ports associated with community VLANs can communicate with the primary VLAN and the other ports that are in the same community VLAN. Multiple community VLANs can be created within a primary VLAN domain.

**Compression Control Protocol** See CCP.

**CRL** (certificate revocation list) A list of public key certificates that have been revoked by a CA. CRLs are stored in the CRL database that is maintained through IKE.

**CSU** (channel service unit) A synchronous telecommunications device that provides a local interface to a leased telecommunications line and terminates that line. In the United States, a CSU terminates a T1 line and provides a

DS1 or DSX interface. Internationally, the CSU is typically owned by the telephone company provider.

**data address** An IP address that can be used as the source or destination address for data. Data addresses are part of an IPMP group and can be used to send and receive traffic on any interface in the group. Moreover, the set of data addresses in an IPMP group can be used continuously provided that one interface in the group is functioning.

**data center bridging** See DCB.

**Data Center Bridging Exchange Protocol** See DCBX.

**Data Encryption Standard** See DES.

**data service unit** See DSU.

**datalink multipathing aggregation** See DLMP aggregation.

**DCB** (data center bridging) An L2 technology that is used to manage the bandwidth, relative priority, and flow control of multiple traffic types that share the same network link, for example, when sharing a datalink between networking and storage protocols.

**DCBX** (Data Center Bridging Exchange Protocol) A protocol that enables communication between hosts to exchange configuration information about the data center bridging features.

**`DefaultFixed` NCP** The system's only fixed NCP in which the network configuration is instantiated but not monitored.

**demilitarized zone** See DMZ.

**denial of service attack** An attack where incoming network packets intentionally or inadvertently overwhelm a server. A server’s throughput can be significantly impacted or the server can become overloaded and nonfunctional.

**`DEPRECATED` address** An IP address that cannot be used as the source address for data in an IPMP group. Usually, IPMP test addresses are `DEPRECATED`. However, any address can be marked `DEPRECATED` to prevent the address from being used as a source address.

**DES** (Data Encryption Standard) A symmetric-key 64-bit block data encryption method standardized by ANSI as ANSI X.3.92. DES uses a 56-bit key.

**DHCP** (Dynamic Host Configuration Protocol) A protocol that enables automatic network configuration of hosts in a TCP/IP network by using a client-server mechanism. This protocol enables hosts on a TCP/IP network to request and get the assigned IP addresses, and also to discover information about the network to which they are attached. For more information about DHCP for IPv4, see RFC 2131 (`http://www.ietf.org/rfc/rfc2131.txt`) and DHCP for IPv6, see RFC 3315 (`http://www.ietf.org/rfc/rfc3315.txt`).

**DHCP unique identifier** See DUID.

**dial-in server** The peer that negotiates and establishes the recipient end of a dial-up PPP link after receiving a call from a dial-out machine. Though the term “dial-in server” is in common use, the dial-in server does not function in accordance with the client-server paradigm. Rather, it is simply the peer that responds to the request to set up a dial-up link. After it is configured, a dial-in server can receive calls from any number of dial-out machines.

**dial-out machine** The peer that initiates the call to establish a dial-up PPP link. After it is configured, the dial-out machine can call any number of dial-in servers. The dial-out machine typically provides authentication credentials before the dial-up link can be established.

**dial-up PPP link** A PPP connection that involves a peer and a modem at either end of a telephone line or similar communications medium, such as a medium that is provided by ISDN. The term “dial-up” refers to the sequence in link negotiation when the local modem dials up the remote peer by using the peer's telephone number. The dial-up link is the most common and least expensive PPP configuration.

**Diffie-Hellman protocol** An asymmetric cryptographic key agreement protocol that enables two users to exchange a secret key over an insecure communication medium without any prior information. Asymmetric cryptographic key agreement is the basis of public key cryptography.

**diffserv model** An Internet Engineering Task Force architectural standard for implementing differentiated services on IP networks. In an IP network, the diffserv model provides a simple and scalable mechanism for classifying and managing network traffic and providing IPQoS. The major modules are classifier, meter, marker, scheduler, and dropper. IPQoS implements the classifier, meter, and marker modules. For more information, see RFC 2475 (`http://www.ietf.org/rfc/rfc2475.txt`).

**digital signature**
A digital code that is attached to an electronically transmitted message that uniquely identifies the sender.

**direct memory access**
See DMA.

**direct server return**
See DSR.

**distinguished name**
See DN.

**DLMP aggregation**
(datalink multipathing aggregation) A type of link aggregation that supports multiple switches and provides continuous connectivity to its datalinks. When a switch fails, the aggregation continues to provide connectivity to its datalinks by using the other switches. This type of link aggregation does not require switch configuration. DLMP aggregation can also be created on a single switch.

**DMA**
(direct memory access) Some devices can perform data transfers that involve main memory and other devices without the help of the CPU. This type of data transfer is known as direct memory access (DMA).

**DMZ**
(demilitarized zone) An isolated network that is set up to prevent public access to an organization's private network. The isolated network can contain resources that a company offers to the public, such as web servers, anonymous FTP servers, and databases.

**DN**
(distinguished name) A standardized method of using ordinary strings to represent shared information. DN is used in technologies such as LDAP and X.509 certificates.

**DNS**
(domain name system) A service that provides the naming policy and mechanisms for mapping domain and machine names to addresses outside of the enterprise, such as those on the Internet. DNS is the network information service used by the Internet. For more information, see RFC 1034 (`http://tools.ietf.org/html/rfc1034`).

**DOI**
(domain of interpretation) A DOI defines data formats, network traffic exchange types, and conventions for naming security-relevant information. Security policies, cryptographic algorithms, and cryptographic modes are examples of security-relevant information.

**domain name system**
See DNS.

**domain of interpretation** See DOI.

**DR** (dynamic reconfiguration) An operating system feature that is used to reconfigure system hardware while the system is running. By using DR, hardware resources can be added or replaced with little or no interruption to normal system operations. Not all Sun platforms from Oracle support DR. Some platforms might only support DR of certain types of hardware such as NICs.

**DS codepoint** See DSCP.

**DSCP** (DS codepoint) A 6-bit value that is included in the Differentiated Service (DS) field of a packet header. DSCP indicates how a packet must be forwarded. For more information, see RFC 2474 (`https://www.rfc-editor.org/rfc/rfc2474.txt`).

**DSR** (direct server return) A mode that allows the Integrated Load Balancer to balance the incoming requests to the back-end servers but lets return traffic from the servers to the clients bypass the Integrated Load Balancer.

**DSU** (data service unit) A synchronous telecommunications device that is used on a leased-line PPP link. DSU converts between data-framing formats that are used on telecommunications lines and provides a standard data communications interface.

**dual stack** A TCP/IP protocol stack that enables both IPv4 and IPv6 protocols to operate on the same network infrastructure without the use of tunneling mechanism. Oracle Solaris networking is a dual stack. This dual stack technique is supported on both hosts and routers.

**DUID** (DHCP unique identifier) An identifier that is used to identify the client system in a DHCPv6 enabled system.

**Dynamic Host Configuration Protocol** See DHCP.

**dynamic packet filter** Also known as stateful packet filter.

**dynamic reconfiguration** See DR.

**dynamic routing** A type of routing in which the system automatically updates the routing table by using routing protocols such as RIP for IPv4 networks and RIPng for IPv6 networks. Dynamic routing is best used on large networks with many hosts.

**ECMP** (equal-cost multi-path) A routing technique for routing packets along multiple paths of equal cost. The forwarding engine identifies paths by next-hop. When forwarding a packet, the router must decide which next-hop (path) to use. For more information, see RFC 2992 (http://tools.ietf.org/html/rfc2992).

**edge virtual bridging** See EVB.

**elastic virtual switch** See EVS.

**encapsulating security payload** See ESP.

**encapsulation** As the packet travels through the network protocol stack, the protocols at each layer either add or remove fields from the basic header. When a protocol on the sending host adds data to the packet header, the process is called data encapsulation.

**enhanced transmission selection** See ETS.

**ENM** (external network modifier) A profile that is created for applications that are external to reactive network configuration but can change and modify a network configuration. ENMs provide the ability to specify when applications or scripts, for example, a VPN application, must perform its own network configuration external to that specified in the NCP and Location profiles.

**equal-cost multi-path** See ECMP.

**ESP** (encapsulating security payload) An extension header that provides integrity, confidentiality, and replay protection to IP datagrams.

**ESSID** (extended service set identifier) An electronic marker or identifier that serves as an identification and address for a computer or network device to connect and access the Internet. It is an identifying name for all 802.11 wireless networks.

**Ethernet** A system that is used for connecting a number of computer systems to form a local area network. Ethernet can use protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

**etherstub** A virtual Ethernet switch that is configured at the datalink layer (L2) of the Oracle Solaris network stack. You can create VNICs over etherstubs instead of physical links for the purpose of constructing a private virtual network that is isolated from other virtual networks on the system, as well as from the external network.

**ETS** (enhanced transmission selection) A DCB feature that allocates bandwidth on a NIC to the applications based on the DCB priority.

**EVB** (Edge Virtual Bridging) An L2 technology that enables hosts to exchange virtual link information with an external switch. EVB offloads the enforcement of traffic SLAs to the switch.

**EVS** (elastic virtual switch) A software virtual switch in Oracle Solaris that provides the ability to span multiple servers, thus providing network connectivity between the virtual machines on multiple servers connected to the elastic virtual switch.

**EVS client** An EVS component from which you manage elastic virtual switches.

**EVS controller** The EVS component that maintains the configuration and status of elastic virtual switches across multiple nodes.

**EVS manager** The entity that communicates with the EVS controller to define the L2 network topologies and the IP addresses that must be used on those L2 networks.

**EVS node** A host whose VNICs connect to an elastic virtual switch.

**expect-send** A scripting format that is used in PPP and UUCP chat scripts. The chat script begins with the text or instruction to *expect* from the remote peer. The next line contains the response to be *sent* from the local host after it receives the correct expect string from the peer. Subsequent lines repeat the expect-send instructions between local host and peer until all instructions that are required to establish communications are successfully negotiated.

**extended accounting** A method that enables you to record resource consumption statistics on a task, process, flow, or network component. You can regularly record the datalink and flow statistics over a period of time in a log file. You can retrieve this data later for analysis.

Enables the recording of resource consumption statistics on a task, process, flow, or network component. The datalink and flow statistics can be regularly recorded over a period of time in a log file so that they can be retrieved later for analysis.

See also network accounting.

**extended service set identifier** See ESSID.

**external network modifier** See ENM.

**failure detection** The process of detecting when an interface or the path from an interface to an Internet layer device no longer works. IP network multipathing (IPMP) and datalink multipathing (DLMP) include two types of failure detection: link based (default) and probe based (optional).

**failure detection time** See FDT.

**fault management resource identifier** See FMRI.

**FCoE** (Fibre Channel over Ethernet) A T11 standard that transports encapsulated Fibre Channel frames over Enhanced Ethernet. FCoE enables network convergence and cost-effective storage area network (SAN) expansion in large deployments.

**FDT** (failure detection time) The amount of time required for detecting whether an interface or path from an interface to an Internet layer device no longer works.

**Fibre Channel over Ethernet** See FCoE.

**filter** A set of rules that define the characteristics of a class in the IPQoS configuration file. The IPQoS system selects for processing any traffic flows that conform to the filters in its IPQoS configuration file. See packet filter.

**firewall** Hardware or software that isolates an organization's private network or intranet from the Internet, thus protecting it from external intrusions. A firewall can include packet filtering, proxy servers, and NAT.

**fixed network configuration mode** A network configuration mode in which the instantiated configuration on the system is persistent, regardless of whether any changes in network conditions occur. When such changes occur, such as the addition of interfaces, you have to reconfigure the network for the system to adapt to the new environment.

**Flat network** Used to implement an elastic virtual switch. All VM instances can be placed on the same segment without a VLAN or VXLAN. There is no VLAN tagging or other types of network segregation.

**flow** Customized way of categorizing network packets based on a single attribute or a combination of attributes. The attributes that serve as the basis for creating flows are derived from the information in a network packet's header. Flows can be associated with an SLA and used for observability.

**flow accounting**

A process of accumulating and recording information about traffic flows in IPQoS. Flow accounting can be established by defining parameters for the `flowacct` module in the IPQoS configuration file.

**flow attributes**

Attributes that are derived from the information in a network packet's header that serve as the basis for creating flows. The attributes can include the transport protocol name, IP address, application port number, and DS field.

**flow priority**

The priority with which packets belonging to a flow are processed. If the `priority` property of a flow is set to `high`, all the packets belonging to that flow are processed ahead of other packets on the same datalink. This property is used to create a flow for applications that are latency sensitive.

**FMRI**

(fault management resource identifier) An identifier for each service, hardware resource, or software package in Oracle Solaris. For packages, the FMRI includes the package publisher, package name, and version of the software package.

**GARP VLAN Registration Protocol**

See GVRP.

**GLDv3**

(Generic LAN Driver version 3) The GLDv3 framework is a function calls-based interface of MAC plugins and MAC driver service routines and structures. The GLDv3 framework implements the necessary STREAMS entry points on behalf of GLDv3 compliant drivers and handles DLPI compatibility.

**GVRP**

(General Attribute Registration Protocol) A protocol that is used by a client system to automatically register VLAN IDs with attached switches.

**hash-based message authentication code**

See HMAC.

**HMAC**

(hash-based message authentication code) A keyed hashing method for message authentication. HMAC is a secret key authentication algorithm that is used with an iterative cryptographic hash function, such as SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

**hop**

A measure that is used to identify the number of routers that separate two hosts. If three routers separate a source and destination, the hosts are four hops away from each other.

**host** A network host is any device or a computer connected to a computer network. A network host provides services, information resources, and applications to users or other nodes on the network.

**IA** (identity association) The method used for a server and a client to identify, group, and manage a set of related IPv6 addresses.

**IAID** (identity association identifier) An identifier that is used to identify the interface on the client system in a DHCPv6 enabled system.

**IANA** (Internet Assigned Numbers Authority) An organization that delegates registered IP addresses to the Internet registries around the world. For more information, see `http://www.internetassignednumbersauthority.org/`.

**ICMP** (Internet Control Message Protocol) A protocol that is used to detect and report errors in a network. For more information, see RFC 792 (`https://tools.ietf.org/html/rfc792`) and RFC 4443 (`https://tools.ietf.org/html/rfc4443`).

**ICMP echo request packet** A packet that is sent to a system on the Internet to solicit a response. Such packets are commonly known as "ping" packets and are used to test the reachability of the hosts on an IP network.

**identity association** See IA.

**identity association identifier** See IAID.

**IKE** (Internet key exchange) IKE automates the provision of authenticated keying material for IPsec security associations (SAs). Fore more information, see RFC 2409 (`https://www.rfc-editor.org/rfc/rfc2409.txt`) and RFC 7296 (`https://tools.ietf.org/html/rfc7296`).

**ILB** (Oracle Solaris Integrated Load Balancer) An L3 and L4 technology that enables a system to spread the load of network processing amongst available resources. ILB can be used to improve reliability and scalability, and to minimize the response time of network services.

**InfiniBand** A I/O technology that is based on switched fabrics. It provides high bandwidth, low latency interconnect for attaching I/O devices to hosts and for host-to-host communication. InfiniBand is used in high-performance computing and enterprise data centers.

**Integrated Services** See ISDN TA.

**Digital Network terminal adaptor**

**Internet Assigned Numbers Authority** See IANA.

**Internet Bootstrap Protocol** See BOOTP.

**Internet Control Message Protocol** See ICMP.

**Internet key exchange** See IKE.

**Internet Protocol Control Protocol** See IPCP.

**Internet Protocol Version 6 Control Protocol** See IPCP.

**Internet Protocol, version 4** See IPv4.

**Internet Protocol, version 6** See IPv6.

**Internet registry** See IR.

**Internet Security Association and Key** See ISAKMP.

**Management Protocol**

**IP header**
The data that uniquely identifies an Internet packet. The header includes source and destination addresses for the packet. An option within the header allows further bytes to be added. The IPv4 header contains 20 bytes of data and the IPv6 header contains 40 bytes of data.

**IP in IP encapsulation**
The mechanism for encapsulating IP packets within IP packets. See encapsulation.

**IP Multipathing**
See IPMP.

**IP Quality of Service**
See IPQoS.

**IP security**
See IPsec.

**IPCP**
(Internet Protocol Control Protocol) A subprotocol of PPP that negotiates the IP addresses of the peers on the link. IPCP also negotiates header compression for the link and enables the use of the network layer protocols.

**IPMP**
(IP Multipathing) A Layer 3 (L3) technology that ensures that a system has continuous access to the network. With IPMP, you configure multiple IP interfaces into an IPMP group.

**IPMP group**
An IP multipathing group consists of a set of network interfaces with a set of data addresses that are treated as interchangeable by the system to improve network availability and utilization. The IPMP group, including all its underlying IP interfaces and data addresses, is represented by an IPMP interface.

**IPnet**
A block of IPv4 or IPv6 addresses that are associated with an elastic virtual switch. The block of IPv4 or IPv6 addresses exists on the same subnet with a default router for the block and is used with the Oracle Solaris Elastic Virtual Switch feature.

**IPoIB VNICs**
A type of VNIC that enables the transport of the IP packets over IB connections. A partition key must be specified when this VNIC is created.

**IPQoS**
(IP Quality of Service) A software feature that provides an implementation of the diffserv model standard, plus flow accounting and 802.1D marking for virtual LANs. By using IPQoS, different levels of network services to customers and applications can be provided.

**IPsec**
(IP security) The security architecture that provides protection for IP communications by authenticating and encrypting IP packets.

**IPv4**

(Internet Protocol, version 4) A version of the internet protocol that supports a 32-bit address space. IPv4 is sometimes referred to simply as IP. For more information, see RFC 791 (`http://www.ietf.org/rfc/rfc791.txt`).

**IPv4 broadcast address**

An IPv4 network address with the host portion of the address containing all zeroes (10.50.0.0) or all one bits (10.50.255.255). A packet that is sent to a broadcast address from a system on the local network is delivered to all systems on that network.

**IPv6**

(Internet Protocol, version 6) A version of the internet protocol that supports a 128-bit address space. For more information, see RFC 2460 (`http://www.ietf.org/rfc/rfc2460.txt`).

**IPv6 autoconfiguration**

The process by which a host automatically configures its IPv6 address from the site prefix and the local MAC address.

**IR**

(Internet registry) A registry that contains registration information of Internet numbers that include IP addresses and autonomous system (AS) numbers.

**ISAKMP**

(Internet Security Association and Key Management Protocol) A common framework for establishing the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP is the IETF standard for handling an IKE exchange.

**ISDN TA**

(Integrated Services Digital Network terminal adaptor) A signal-adapting device that provides a modem-like interface for a dial-up PPP link over an ISDN. Solaris PPP 4.0 configuration files are used to configure an ISDN TA when used as a standard modem.

**isolated VLAN**

A type of secondary VLAN. The ports that are associated with this type of VLAN can communicate only with the primary VLAN and not with any other secondary VLAN. Only one isolated VLAN can be created within a primary VLAN domain.

**key management**

The management of cryptographic keys. This management includes the generation, exchange, storage, use, and replacement of keys at the user level, either between users or systems.

**keystore**

The location on the disk or card where cryptographic keys are stored.

**keystore name**

The name that the administrator gives to the keystore. In the Cryptographic Framework, the keystore name is also called the 'token' or 'token ID'.

**KMF**

(Oracle Solaris Key Management Framework) A framework that provides tools and programming interfaces for managing public key objects that include X.509 certificates and public or private key pairs. KMF also provides a tool for managing policies that define the use of X.509 certificates by applications.

**LACP** (Link Aggregation Control Protocol) An IEEE 802.3ad standard for dynamically exchanging network configuration information among systems in a link aggregation group. This protocol helps to automatically configure and maintain link aggregation groups.

**large receive offload** See LRO.

**LCP** (Link Control Protocol) A subprotocol of PPP that is used to negotiate the initial set of link parameters between the peers. LCP checks the identity of the linked device, searches for errors in the link configuration, and determines the acceptable packet size for transmission.

**LDAP** (Lightweight Directory Access Protocol) A client-server protocol that is used to manage directory information over an IP network. LDAP enables a single point of management for storage, retrieval, and distribution of information. LDAP enables clients and servers that use LDAP naming services to communicate with each other. For more information, see RFC 4511 (`https://tools.ietf.org/rfc/rfc4511.txt`).

**leased-line PPP link** A PPP connection that involves a host and a CSU/DSU that are connected to a synchronous network medium leased from a provider. Optical Carrier 3 (OC3) and T carrier (T1) are common examples of leased-line media. Though easier to administer, leased-line links are more expensive than dial-up PPP links and therefore are less common.

**Lightweight Directory Access Protocol** See LDAP.

**link aggregation** A method of combining several links on a system into a single logical unit to increase the throughput of network traffic and provide high availability. Link aggregation is an L2 entity that includes DLMP aggregation and trunk aggregation.

**Link Aggregation Control Protocol** See LACP.

**Link Control Protocol** See LCP.

**Link Layer Discovery Protocol** See LLDP.

**link-local address** A designation that is used for addressing on a single link for purposes such as automatic address configuration in IPv6. By default, the link-local address is created from the system's MAC address.

**LLDP** (Link Layer Discovery Protocol) A link layer protocol that enables network devices to advertise their capabilities, identity, and current status to other network devices on an IEEE 802 local area network (LAN).

**load spreading** The process of distributing inbound or outbound traffic over a set of interfaces. With load spreading, higher throughput is achieved. Load spreading occurs only when the network traffic is flowing to multiple destinations that use multiple connections. The two types of load spreading are inbound load spreading for inbound traffic and outbound load spreading for outbound traffic.

**local-use address** A unicast address that has only a local routeability scope (within the subnet or within a subscriber network). This address also can have a local or global uniqueness scope.

**LRO** (large receive offload) A technology that merges successive incoming packets into a single packet before the packets are delivered to the IP layer. The incoming packets must share the same transport protocol, local or remote IP address, and port number. This set of attributes are also known as a five-tuple.

**MAC address** (Media Access Control address) An unique address that is assigned to a network interface. The MAC address is used for communication on the physical network segment.

**marker** A module in the diffserv architecture that marks a packet with a value that indicates how the packet must to be forwarded.

**master router** A VRRP instance that performs the routing function for the virtual router at a given time. Only one master router is active at a time for a given VRID. The master router controls the IPv4 or IPv6 address or addresses that are associated with the virtual router. The virtual router forwards the packets that are sent to the IP address of the master router. See also VRRP and VRID.

**maximum transmission unit** See MTU.

**meter** A module in the diffserv architecture that measures the rate of traffic flow for a particular class. The IPQoS implementation includes two meters, `tokenmt` and `tswtclmt`.

**Microsoft CHAP** See MS-CHAP.

**minimal encapsulation** An optional form of IPv4 in IPv4 tunneling that can be supported by home agents, foreign agents, and mobile nodes. Minimal encapsulation has 8 or 12 bytes less of overhead than the IP in IP encapsulation.

**MS-CHAP** (Microsoft CHAP) A proprietary Microsoft authentication protocol for PPP. Solaris PPP 4.0 supports versions 1 and 2 of this protocol in both client and server mode.

**MTU** (maximum transmission unit) The size of the largest data unit, given in octets, that can be transmitted over a link.

**multicast** A network layer procedure that is used to send datagram packets to multiple systems on an IP network. Unlike broadcast routing, packets are not handled by every system. Multicast requires the routers to be configured with specific routing protocols such as Distance Vector Multicast Routing Protocol (DVMRP). For more information about DVMRP, see RFC 1075 (`http://tools.ietf.org/rfc/rfc1075.txt`).

**multicast address** An IPv4 or IPv6 address that identifies a group of interfaces. A packet that is sent to a multicast address is delivered to all of the interfaces in the group.

**multihomed host** A system that has more than one interface and that does not perform packet forwarding. A multihomed host can run routing protocols.

**NAT** (network address translation) The translation of an IP address used within one network to a different IP address known within another network. Used to limit the number of global IP addresses that are needed.

**NCP** (network configuration profile) The profiles that manage the system's network configuration in Oracle Solaris. Only one NCP can be active on a system at a time.

**NCU** (network configuration unit) An individual configuration object that contains all the properties that defines an NCP. Each NCU represents a physical link or an interface and contains properties that define the configuration for that link or interface.

**neighbor advertisement** A response to a neighbor solicitation message or the process of a node sending unsolicited neighbor advertisements to announce a link-layer address change.

**neighbor discovery** An IP mechanism that enables hosts to locate other hosts that reside on an attached link.

**neighbor solicitation** A solicitation that is sent by a node to determine the link-layer address of a neighbor. A neighbor solicitation also verifies that a neighbor is still reachable by a cached link-layer address.

**network accounting** A method that is used to capture statistics about network traffic in a log file for tracking, provisioning, consolidation, or billing purposes.

**network address translation** See NAT.

**network configuration profiles** See NCP.

**network configuration unit** See NCU.

**Network File System** See NFS.

**network information service** See NIS.

**network interface card** See NIC.

**Network Time Protocol** See NTP.

**NFS** (Network File System) A file system protocol that is used to remotely access shared files across a network. Oracle Solaris supports NFSv2, NFSv3, NFSv4, and NFSv4.1 versions. For more information about the NFS versions, see RFC 1094, RFC 1831, and RFC 5661 respectively.

**NIC** (network interface card) A network adapter card that connects a computer to a network. Some NICs can have multiple physical interfaces, such as the `igb` card.

**NIC rings** On NICs, receive (Rx) rings and transmit (Tx) rings are hardware resources through which the system receives and sends network packets, respectively.

**NIS** (network information service) A distributed network database containing key information about the systems and the users on the network.

**node** In a computer network, a node is a connection point or an end point for the transmission of the data.

**NTP** (Network Time Protocol) A protocol that is used to set and maintain the system time. The NTP software is implemented as the `ntpd` daemon, which is a complete implementation of the version 4 standard as defined in RFC 5905 (`https://tools.ietf.org/html/rfc5905`).

**Open Systems Interconnection model** See OSI model.

**Oracle Solaris Integrated Load Balancer** See ILB.

**Oracle Solaris Key Management Framework** See KMF.

**OSI model** (Open Systems Interconnection model) A standard model designed by the International Standard Organization (ISO) that describes how data must be transmitted over a network.

**outcome** In IPQoS, the action to take as a result of metering traffic. The IPQoS meters have three outcomes: red, yellow, and green. You define the outcomes in the IPQoS configuration file.

**packet** A group of information that is transmitted as a unit over communication lines. Contains a MAC header and a payload, and possibly also contain an IP header.

**packet filter** A firewall function that can be configured to allow or disallow specified packets through a firewall.

**packet header** See IP header.

**PAP** (password authentication protocol) An authentication protocol that can be used to verify the identity of a caller on a PPP link. PAP uses a cleartext password that is passed over the link, which makes it possible to store the password on one of the endpoint systems. For example, PAP can use the login and password entries in the UNIX `passwd` database on the system that receives a call to verify the identity of the caller.

**paravirtualized NIC** See PV NIC.

**password authentication protocol** See PAP.

**payload** The data that is carried in a packet. The payload does not include the header information that is required to get the packet to its destination.

**PCIe** (peripheral component interconnect express) A serial I/O bus that connects a computer with its peripherals.

**per-hop behavior** See PHB.

**perfect forward secrecy** See PFS.

**peripheral component interconnect express** See PCIe.

**PF** (physical function) A PCI function that supports the SR-IOV capabilities as defined in SR-IOV specification. A PF contains the SR-IOV capability structure and is used to manage the SR-IOV functionality. PFs are fully featured PCIe functions that can be discovered, managed, and manipulated like any other PCIe device. PFs have full configuration resources, and can be used to configure or control the PCIe device.

**PFC** (priority-based flow control) A datalink level flow control mechanism. PFC extends the standard PAUSE frame to include the IEEE 802.1p class of service (CoS) values. In PFC, the traffic is paused selectively only for the CoS values that are enabled in the PFC frame instead of halting all the traffic on the datalink.

**PFS** (perfect forward secrecy) In PFS, the key that is used to protect transmission of data is not used to derive additional keys. Also, the source of the key that is used to protect data transmission is never used to derive additional keys. PFS applies to the authenticated key exchange in IKE.

**PHB** (per-hop behavior) A priority that is assigned to a traffic class of a packet when traversing a hop.

**physical function** See PF.

**physical interface** A system's attachment to a link. This attachment is often implemented as a device driver plus a NIC. Some NICs can have multiple points of attachment, for example, `igb`.

**PKI** (public key infrastructure) A system of digital certificates, CAs, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

**Point-to-Point Protocol** See PPP.

**port VLAN identifier** See PVID.

**PPP** (Point-to-Point Protocol) A link layer protocol that provides a standard method for transferring datagrams over point-to-point media. A PPP configuration consists of two endpoint computers called *peers*, and the telephone lines or other bidirectional link that the peers use for communication. The hardware and software connection between the two peers is considered the *PPP link*.

PPP is composed of a number of subprotocols, including PAP, CHAP, LCP, and CCP.

**PPP over Ethernet** See PPPoE.

**PPPoE** (PPP over Ethernet) A protocol that enables hosts to run PPP sessions over an Ethernet link. PPPoE is commonly used with Digital Subscriber Line (DSL) services.

**Precision Time Protocol** See PTP.

**primary MAC client** The MAC client that represents the NIC or PV NIC and has its own address and other attributes of L2 (MAC) and L3 (IP) layers.

**primary VLAN** Standard (IEEE 802.1Q) VLAN.

**priority-based flow control** See PFC.

**private address** An IP address that is not routeable through the Internet. Private addresses can used by internal networks on hosts that do not require Internet connectivity. For more information about IPv4 private addresses, see RFC 1918 (`https://tools.ietf.org/html/rfc1918`). For more information about IPv6 private addresses, see RFC 4193 (`http://www.ietf.org/rfc/rfc4193.txt`).

**private virtual network** A virtual network that is isolated both from other virtual networks that are on the system, as well as from the external network. Private virtual networks are configured over etherstubs.

**private VLAN** See PVLAN.

**promiscuous trunk port** A port configured on the top-level switch uplink port that can communicate with both the isolated and the community VLANs.

**proxy server** An intermediary server between a client and another server. It provides caching service, administrative control, and security. For example, a proxy server can be used to prevent access to certain web sites.

**PTP** (Precision Time Protocol) An IEEE protocol that is used to synchronize the system clock across multiple systems in a broadcast domain. The PTP software is implemented as the `ptpd` daemon, which is an implementation of the PTP Version 2 as defined in the IEEE standard 1588-2008.

**public key cryptography** A cryptographic algorithm, which requires two different keys that are mathematically linked. The public key is available to everyone. The private key is known only to the recipient of the message. Public key cryptography is also known as asymmetric cryptography.

**public key infrastructure** See PKI.

**PV NIC** An entity that resides in the hypervisor of the guest operating system and is the equivalent of the physical NIC in the host, for example, `zvnet` in the kernel zone.

**PVID** (port VLAN identifier) The default VLAN ID that is assumed for untagged packets sent to and received from a link.

**PVLAN** (private VLAN) A subdivision of a VLAN to isolate network traffic. PVLAN partitions the VLAN, which is a single broadcast domain into smaller sub-domains.

**PVLAN secondary trunk port** A port that is configured on the intermediate switches to allow PVLAN traffic to span multiple switches.

**RARP** (Reverse Address Resolution Protocol) A protocol that maps dynamically between Internet Protocol (IP) and Ethernet addresses. RARP is used to resolve MAC address into an IP address on the local area network. For more information, see RFC 903 (`http://tools.ietf.org/rfc/rfc903.txt`).

**RCM** (reconfiguration coordination manager) A framework that manages the dynamic removal of system components and helps to register and release system resources in an orderly manner.

**reactive network configuration mode** A network configuration mode in which the system automatically adapts to any change in the network condition without requiring manual reconfiguration.

**reconfiguration coordination manager** See RCM.

**redirect** In a router, to inform a host of a better first-hop node to reach a particular destination.

**reflective relay** A feature in EVB that provides an option to send inter-VM traffic on the wire to be looped back by the external switch and enables the consolidation of multiple hosts into multiple VMs or zones on a shared host.

**repair detection** The process of detecting when a NIC or the path from the NIC to a Layer 3 device starts operating correctly after a failure.

**replay attack** A network attack in which a packet is captured by an intruder during data transmission. The captured packet is either replaced with a fraudulent packet or repeated later. To protect against such attacks, a packet can contain a field that increments during the lifetime of the secret key that is protecting the packet.

**Reverse Address Resolution Protocol** See RARP.

**RIP** (Routing Information Protocol) An Internal Gateway Protocol that routes IPv4 packets and maintains the routing table of all the hosts on the LAN. For more information, see RFC 2453 (`https://tools.ietf.org/html/rfc2453`).

**RIPng** (Routing Information Protocol next generation) An Internal Gateway Protocol that routes IPv6 packets and maintains the routing table of all the hosts on the LAN. For more information, see RFC 2080 (`http://tools.ietf.org/rfc/rfc2080.txt`).

**router** A system that has more than one interface, runs routing protocols, and forwards data packets between computer networks. Routers direct traffic on the Internet and connect two or more data lines from different networks. A router forwards a data packet from one router to another through the network until the packet reaches its destination.

**router advertisement** The process of routers advertising their presence together with various link and Internet parameters, either periodically or in response to a router solicitation message.

**router discovery** The process of hosts locating routers that reside on an attached link.

**router solicitation** The process of hosts requesting routers to generate router advertisements immediately, rather than at their next scheduled time.

**Routing Information Protocol** See RIP.

**Routing Information Protocol next generation** See RIPng.

**routing table** A table that contains the routing information for a packet, which helps to determine the best path for the packet to reach its destination.

**RSA** A method for obtaining digital signatures and public key cryptosystems.

**SA** (security association) An association that specifies security properties from one host to a second host. IKE automates the provision of authenticated keying material for IPsec SAs.

**SADB** (security associations database) A table of SAs that specifies cryptographic keys and cryptographic algorithms. The keys and algorithms are used in the secure transmission of data.

**SCTP** (Stream Control Transport Protocol) A transport layer protocol that provides connection-oriented communications in a manner similar to TCP. Additionally, SCTP supports multihoming, in which one of the endpoints of the connection can have more than one IP address. For more information, see RFC 4960 (`http://tools.ietf.org/html/rfc4960`).

**secondary VLAN** A sub-VLAN of a primary VLAN.

**Secure Hashing Algorithm** See SHA-1.

**Secure Remote Procedure Call** See Secure RPC.

**Secure RPC** (Secure Remote Procedure Call) A method that protects remote procedures with an authentication mechanism. The Diffie-Hellman authentication mechanism authenticates both the host and the user who is making a request for a service. The authentication mechanism uses DES encryption. Applications that use Secure RPC include NFS and the NIS naming service.

**secure sockets layer** See SSL.

**security association** See SA.

**security associations database** See SADB.

**security parameter index** See SPI.

**security policy database** See SPD.

**selector** In IPQoS, the element that specifically defines the criteria to be applied to packets of a particular class in order to select that traffic from the network stream. You define selectors in the filter clause of the IPQoS configuration file.

**`sendmail`** A program that acts as a mail transport agent and uses a configuration file to provide aliasing and forwarding, automatic routing to network gateways, and flexible configuration.

**Server Message Block** See SMB.

**service management facility** See SMF.

**SHA-1** (Secure Hashing Algorithm) An algorithm that operates on any input length less than $2^{64}$ to produce a message digest. The SHA-1 algorithm is input to DSA.

**SHA-2** A set of hash algorithms with different block sizes, for example SHA-256 and SHA-512.

**Simple Network Management Protocol** See SNMP.

**single root I/O virtualization** See SR-IOV.

**SMB** (Server Message Block) A protocol that enables clients to access files and request services of a server on the network.

**SMF** (service management facility) A feature that defines the relationships between applications or services so that dependent services can be automatically restarted when necessary.

**smurf attack**

The process of creating severe network congestion or outages by using ICMP echo request packets directed to an IP broadcast address or multiple broadcast addresses from remote locations.

**sniff**

To eavesdrop on computer networks – frequently used as part of automated programs to sift information, such as clear-text passwords, off the wire.

**SNMP**

(Simple Network Management Protocol) A protocol that provides a common way to query, monitor, and manage devices that are connected to IP networks.

**Spanning Tree Protocol**

See STP.

**SPD**

(security policy database) A database that specifies the level of protection to apply to a packet protected by IPsec. The SPD filters IP traffic to determine whether a packet must be discarded, sent on the network, or protected with IPsec.

**SPI**

(security parameter index) An integer that specifies the row in the SADB that a receiver uses to decrypt a received packet.

**spoof**

To gain unauthorized access to a computer by sending a message to it with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, the sender must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that the packets appear to be coming from that host.

**SR-IOV**

(Single Root I/O Virtualization) A standard that enables efficient sharing of Peripheral Component Interconnect Express (PCIe) devices among virtual machines and is implemented in the hardware. The SR-IOV specification enables a virtual machine to be directly connected to the I/O device.

**SSL**

(secure sockets layer) A form of secure low-level encryption that is used by protocols like HTTP and FTP. The SSL protocol includes provisions for server authentication, encryption of data in transit, and optional client authentication.

**SSL kernel proxy**

The configurable proxy runs in kernel to accelerate web server communications that are protected by the secure sockets layer (SSL). The SSL kernel proxy is also known as KSSL.

**standby interface**

A physical interface that is used to carry data traffic only if some other physical interface has failed.

**stateful packet filter**

A packet filter that can monitor the state of active connections and use the information obtained to determine which network packets to allow through the firewall. By tracking and matching requests and replies, a stateful packet filter can screen for a reply that doesn't match a request.

**stateless autoconfiguration** The process of a host generating its own IPv6 addresses by combining its MAC address and an IPv6 prefix that is advertised by a local IPv6 router.

**static routing** A process in which the system network administrator can manually add routes to the routing table.

**STP** (Spanning Tree Protocol) A default protocol used by the bridged networks to prevent network loops that render the subnetworks unusable.

**Stream Control Transport Protocol** See SCTP.

**subnet** A logical subdivision of an IP network that connects systems with subnet numbers and IP address schemas, including their respective netmasks.

**symmetric key cryptography** An encryption system in which the sender and receiver of a message share a single common key. This common key is used to encrypt and decrypt the message. Advanced Encryption Standard is an example of a symmetric key.

**synchronous PPP** A form of PPP that runs over synchronous digital lines, which transfer data as a continuous stream of raw bits. A leased-line PPP link uses synchronous PPP.

**tenant** A logical group containing an elastic virtual switch and its resources. The resources are not visible outside the tenant's namespace.

**test address** An IP address in an IPMP group which must be used as the source or destination address for probes, and must not be used as a source or destination address for data traffic.

**TFTP** (Trivial File Transfer Protocol) A file transfer protocol that is used to transfer files between the network configuration servers and the network clients. TFTP is generally used for the automated transfer of configuration or boot files between systems in a local network. For more information, see RFC 1350 (`http://www.ietf.org/rfc/rfc1350.txt`).

**transparent interconnection of lots of links** See TRILL.

**TRILL** (transparent interconnection of lots of links) A protocol that is used by bridged networks to prevent network loops without disabling links. TRILL computes the shortest-path information for each TRILL node in the network and uses that information to forward packets to individual destinations. TRILL helps to load-balance the traffic between several paths to the destination.

**Triple-Data Encryption Standard** See 3DES.

**Trivial File Transfer Protocol** See TFTP.

**trunk aggregation** A link aggregation that is based on the IEEE 802.3ad standard. Trunk aggregations work by enabling multiple flows of traffic to be spread across a set of aggregated ports. The IEEE 802.3ad requires switch configuration, as well as switch-vendor proprietary extensions in order to work across multiple switches.

**trusted callers** In PPP, remote peers that a dial-in server grants access to by including the peers' security credentials in the server's PAP or CHAP secrets database.

**UDP** (User Datagram Protocol) A protocol that a computer uses to send datagrams to other computers on an IP network without setting up special transmission channels or data paths. For more information, see RFC 768 (`http://www.ietf.org/rfc/rfc768.txt`).

**unicast address** An IPv6 address that identifies a single interface of an IPv6-enabled node. The parts of the unicast address are site prefix, subnet ID, and interface ID.

**uniform resource indicator** See URI.

**uniform resource locator** See URL.

**UNIX-to-UNIX Copy Program** See UUCP.

**uplink port** A datalink over which VNICs are created, when you use the Oracle Solaris EVS feature.

**URI** (uniform resource indicator) An addressing technology that identifies resources on the Internet or a private intranet.

**URL** (uniform resource locator) A string of characters that identifies a resource on the Internet or a private intranet.

**User Datagram Protocol** See UDP.

**user-priority** A 3-bit value that implements class-of-service (CoS) marks. CoS defines how Ethernet datagrams are forwarded on a network of VLAN devices.

**UUCP** (UNIX-to-UNIX Copy Program) A program that enables computers to transfer files and exchange mails with each other. UUCP also enables computers to participate in large networks such as Usenet.

**VDP** (VSI Discovery and Configuration Protocol) A protocol used by EVB to exchange information about VSIs (Virtual Switch Interfaces).

**VF** (virtual function) A SR-IOV function that is associated with a Physical Function. A VF is a lightweight PCIe function that shares one or more physical resources with the Physical Function and with other VFs that are associated with the same PF. VFs are only allowed to have configuration resources for its own behavior.

**virtual extensible local area network** See VXLAN.

**virtual function** See VF.

**Virtual IP address** See VRIP.

**virtual LAN device** See VLAN device.

**virtual local area network** See VLAN.

**virtual network** A network that emulates a physical network and is a combination of hardware and software network resources.

**virtual network identifier** See VNI.

**virtual network interface card** See VNIC.

**virtual port** The point of attachment between the VNIC and an elastic virtual switch. A virtual port encapsulates various network configuration parameters that is inherited by the VNIC when it connects to the virtual port.

**virtual private network** See VPN.

**Virtual Router ID** See VRID.

**Virtual Router Redundancy Protocol** See VRRP.

**virtual station instance** See VSI.

**virtual switch** An entity that facilitates communication between virtual machines. The virtual switch loops traffic between virtual machines (inter-VM traffic) within the physical machine and does not send this traffic out on the wire. Virtual switches are automatically instantiated when VNICs are created and they are managed by EVS.

**VLAN** (virtual local area network) A subdivision of a local area network at the datalink layer of the protocol stack.

**VLAN device** (virtual LAN device) Network interfaces that provide traffic forwarding at the Ethernet (datalink) level of the IP protocol stack.

**VNI** (virtual network identifier) VXLANs are identified by using VXLAN segment IDs, which are also known as VNIs. Every VXLAN datalink is associated with a VNI.

**VNIC** (virtual network interface card) An L2 entity or virtual network device that behaves just like a physical NIC when configured. You configure a VNIC over an underlying datalink to share it between multiple zones or virtual machines (VMs) or connect a VNIC to an elastic virtual switch.

**VPN** (virtual private network) A single, secure, logical network that uses tunnels across a public network such as the Internet.

**VRID** (Virtual Router ID) A unique number used to identify a virtual router on a given network segment. VRIDs identify the virtual router within a LAN.

**VRIP** (Virtual IP address) An IP address associated with a VRID from which other hosts can obtain network service. The VRIP is managed by the VRRP instances belonging to a VRID.

**VRRP** (Virtual Router Redundancy Protocol) A protocol that provides high availability of IP addresses, such as those that are used for routers and load balancers. For more information, see RFC 5798 (`https://tools.ietf.org/html/rfc5798`).

**VSI** (virtual station instance) VSI refers to a VNIC that is configured on the station.

**VSI Discovery and Configuration Protocol** See VDP.

**VXLAN** (virtual extensible local area network) An L2 and L3 technology that works by overlaying a datalink (L2) network on top of an IP (L3) network. VXLANs address the 4K limitation that is imposed when using VLANs. Typically, VXLANs are used in a cloud infrastructure to isolate multiple virtual networks.

**VXLAN segment ID** See also VNI.

**WAP** (Wireless Application Protocol) A standard protocol to access information over a mobile wireless network.

**WEP key** (wired equivalent privacy key) A key that establishes connections with a secure Wi-Fi network.

**wired equivalent privacy key** See WEP key.

**Wireless Application Protocol** See WAP.