# 网络术语词汇表

文件号码 E53823
2014 年 7 月

# 目录

# 使用本文档

- **概述** – 提供 Oracle Solaris 网络上下文中常用的网络术语和首字母缩略词的定义。
- **目标读者** – 系统管理员。
- **必备知识** – 基本和一些高级的网络管理技能。

## 产品文档库

有关本产品的最新信息和已知问题均包含在文档库中，网址为：http://www.oracle.com/pls/topic/lookup?ctx=E36784。

## 获得 Oracle 支持

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

## 反馈

可以在 http://www.oracle.com/goto/docfeedback 上提供有关此文档的反馈。

♦ ♦ ♦ 第 1 章

# 1 Oracle Solaris 中的网络术语

此术语表定义了 Oracle Solaris 中的常用网络术语和首字母缩略词，为编写白皮书、规范以及用户和培训文档的人提供协助，并帮助确保一致的使用。此术语表并未涵盖通常适用于所有网络的术语的详尽列表。另外，此术语表中的许多术语是特定于 Oracle Solaris 网络技术的。

## 术语表

| | |
|---|---|
| 3DES | （Triple-Data Encryption Standard，三重数据加密标准）一种对称密钥加密方法，该方法应用数据加密标准 (Data Encryption Standard, DES) 加密算法对数据加密三次。3DES 要求密钥长度为 168 位。3DES 也称为三重 DES。 |
| 6to4 | 通过 IPv4 网络传输 IPv6 包的自动隧道连接机制。通过 6to4 隧道，隔离的 IPv6 站点可以通过自动隧道在 IPv4 上进行通信，而无需配置显式隧道。 |
| Address Resolution Protocol（地址解析协议） | 请参见 ARP。 |
| Advanced Encryption Standard（高级加密标准） | 请参见 AES。 |
| AES | Advanced Encryption Standard（高级加密标准）。一种对称加密方法，可提供 128 位块数据加密技术。AES 是指美国政府的加密标准。 |
| **anet** resource（anet 资源） | 缺省情况下自动为所有 Oracle Solaris 区域配置的 VNIC。另请参见 VNIC。 |
| anycast address（任播地址） | 为一组接口（通常属于不同的节点）分配的 IPv6 地址。发送到任播地址的包将被路由到最近的具有该地址的接口。包的路由符合路由协议的距离度量原则。 |
| anycast group（任播组） | 一组具有相同任播 IPv6 地址的接口。Oracle Solaris 实现的 IPv6 不支持创建任播地址和任播组。不 |

| | |
|---|---|
| | 过，Oracle Solaris IPv6 节点可以将通信流量发送到任播组。 |
| ARP | （地址解析协议）一种在 IP 地址和以太网地址之间提供动态映射的协议。ARP 只用于 IPv4 网络。IPv6 网络使用相邻节点搜索协议来转换协议地址。有关更多信息，请参见 RFC 826 (http://tools.ietf.org/html/rfc826)。 |
| asymmetric key cryptography（非对称密钥加密） | 一种加密系统，消息的发送者和接收者使用不同的密钥对消息进行加密和解密。非对称密钥用于为对称密钥加密建立一个安全信道。Diffie-Hellman protocol（Diffie-Hellman 协议）就是一种非对称密钥协议。 |
| asymmetric routing（非对称路由） | 当采用一种路径将包从源传递到目标而采用不同的路径返回到源时，将发生此情况。常见于第 3 层（网络层）路由网络。 |
| asynchronous PPP（异步 PPP） | 一种异步串行线路上的 PPP 形式，异步串行线路一次传送一个字符数据。拨号链路是 PPP 最常见的配置形式，它采用异步 PPP 通信。 |
| authentication header（验证头） | 为 IP 数据报提供验证和完整性而不提供保密性的扩展头。 |
| authentication（验证） | 检验由远程用户或实体（如程序）通过网络提供的身份的动作。 |
| autonomous system（自治系统） | 单个路由域，用于管理具有多个路由器和网络的站点的网络拓扑。此路由域是一组连接的一个或多个 IP 前缀并且具有单个明确定义的路由策略。有关更多信息，请参见 RFC 1930 (http://tools.ietf.org/html/rfc1930)。 |
| backup router（备用路由器） | 处于活动状态但不处于主状态的 VRID 的 VRRP 实例称为备用路由器。VRID 可以存在任意数量的备用路由器。如果当前主路由器出现故障，则备用路由器将承担主路由器的角色。 |
| bandwidth delay product（带宽延迟乘积） | 确定通过网络发送的数据量。此数据是可用网络带宽与连接延迟或往返时间的乘积。 |
| BGP | （边界网关协议）用于在自治系统之间交换路由信息的协议。有关更多信息，请参见 RFC 4271 (http://www.ietf.org/rfc/rfc4271.txt)。 |
| bidirectional tunnel（双向隧道） | 可以双向传输 IP 数据报的隧道。 |

| | |
|---|---|
| Blowfish | 一种对称块加密算法，它采用 32 位到 448 位的可变长度密钥。其作者 Bruce Schneier 声称 Blowfish 已针对密钥不经常更改的应用程序进行优化。 |
| BOOTP | （Internet 引导协议）网络客户机用来从服务器获取 IP 地址的协议。 |
| Border Gateway Protocol（边界网关协议） | 请参见 BGP。 |
| broadcast（广播） | 在网络中，用于同时将包传送到子网上除发送方以外的每个计算机的方法。广播包通常不会路由至子网之外。 |
| CA | （证书颁发机构）颁发数字证书的可信第三方组织或公司。数字证书用于创建数字签名和公钥/私钥对。CA 保证被授予唯一数字证书的个人的身份。 |
| Callback Control Protocol（回调控制协议） | 请参见 CBCP。 |
| CBCP | （回叫控制协议）专有 Microsoft PPP 扩展，用于协商回叫会话。Solaris PPP 4.0 仅支持此协议的客户机（初始调用方）端。 |
| CCP | （压缩控制协议）PPP 的子协议，协商链路上数据压缩的使用。与头压缩不同，CCP 会压缩在链路上发送的包中的所有数据。 |
| certificate authority（证书颁发机构） | 请参见 CA。 |
| certificate revocation list（证书撤销列表） | 请参见 CRL。 |
| Challenge Handshake Authentication Protocol（质询握手验证协议） | 请参见 CHAP。 |
| channel service unit（通道服务单元） | 请参见 CSU。 |
| CHAP | （质询握手验证协议）一种验证协议，可用于验证 PPP 链路上调用方的身份。CHAP 验证使用质询和响应的概念，其中接收调用的计算机会质询调用方以证明其身份。<br><br>另请参见password authentication protocol（口令验证协议）。 |

| | |
|---|---|
| CHAP secret（CHAP 密钥） | ASCII 或二进制字符串，用于标识目的。PPP 链路上的两个对等点都可识别这两种字符串。CHAP 机密以明文格式存储在系统的 `/etc/ppp/chap-secrets` 文件中，但从不会通过 PPP 链路发送，即便使用加密格式也是如此。CHAP 协议检验调用方使用的 CHAP 机密散列，确定它是否与接收方的 `/etc/ppp/chap-secrets` 文件中调用方的 CHAP 机密散列项相匹配。 |
| chat script（聊天脚本） | 指示调制解调器如何在其自身与远程对等点之间建立通信链路的一些指令。PPP 和 UUCP 协议都使用聊天脚本来建立拨号链路和回拨调用。 |
| Compression Control Protocol（压缩控制协议） | 请参见 CCP。 |
| CRL | （证书撤销列表）已由 CA 撤销的公钥证书的列表。CRL 存储在 CRL 数据库中，该数据库通过 IKE 进行维护。 |
| CSU | （通道服务单元）一种同步电信设备，它为租用的电信线路提供本地接口并且充当该线路的终端。在美国，CSU 充当 T1 线路的终端并且提供 DS1 接口或 DSX 接口。在国际上，CSU 通常归电话公司提供商所有。 |
| data address（数据地址） | 可以用作数据的源地址或目标地址的 IP 地址。数据地址属于某个 IPMP 组，可以用来发送和接收组中任何接口上的通信。而且，只要 IPMP 组中有一个接口在工作，就可以连续使用 IPMP 组中的一组数据地址。 |
| Data Center Bridging Exchange Protocol（数据中心桥接交换协议） | 请参见 DCBX。 |
| data center bridging（数据中心桥接） | 请参见 DCB。 |
| Data Encryption Standard（数据加密标准） | 请参见 DES。 |
| data service unit（数据服务单元） | 请参见 DSU。 |
| datalink multipathing aggregation（数据链路多路径聚合） | 请参见 DLMP aggregation（DLMP 聚合）。 |
| DCB | （数据中心桥接）一种 L2 技术，用于管理共享相同网络链路的多个通信类型的带宽、相对优先级和流控 |

| | |
|---|---|
| | 制，例如，在网络协议和存储协议之间共享数据链路时。 |
| DCBX | （数据中心桥接交换协议）使主机之间的通信能够交换有关数据中心桥接功能的配置信息的协议。 |
| **DefaultFixed** NCP | 系统的唯一固定 NCP，在其中网络配置会进行实例化但不受监视。 |
| demilitarized zone（非军事化区） | 请参见 DMZ。 |
| denial of service attack（拒绝服务攻击） | 传入网络包有意或无意耗尽服务器的攻击。服务器的吞吐量会受到严重影响，服务器也可能变得超载且无法正常工作。 |
| **DEPRECATED** address（DEPRECATED 地址） | 在 IPMP 组中不能用作数据的源地址的 IP 地址。通常，IPMP 测试地址为 DEPRECATED。不过，可以将任何地址标记为 DEPRECATED，以防止将该地址用作源地址。 |
| DES | （数据加密标准）对称密钥 64 位块数据加密方法，由 ANSI 标准化为 ANSI X.3.92。DES 使用 56 位密钥。 |
| DHCP | （动态主机配置协议）通过使用客户机/服务器机制支持 TCP/IP 网络中主机的自动网络配置的协议。通过此协议，TCP/IP 网络上的主机可以请求并获得指定的 IP 地址，也可以搜索有关主机所连接到的网络的信息。有关用于 IPv4 的 DHCP 的更多信息，请参见 RFC 2131 (https://www.ietf.org/rfc/rfc2131.txt)；有关用于 IPv6 的 DHCP 的更多信息，请参见 RFC 3315 (http://www.ietf.org/rfc/rfc3315.txt)。 |
| DHCP unique identifier（DHCP 唯一标识符） | 请参见 DUID。 |
| dial-in server（拨入服务器） | 一种对等点，它在接收来自拨出计算机的调用后，协商并建立拨号 PPP 链路的接收端。尽管“拨入服务器”是常用术语，但拨入服务器的作用与客户机/服务器模型并不一致。更确切地说，拨入服务器只是响应对设置拨号链路的请求的对等点。拨入服务器配置后，可接收来自任意数量的拨出计算机的调用。 |
| dial-out machine（拨出计算机） | 发出调用，要求建立拨号 PPP 链路的对等点。配置拨出计算机后，可调用任意数量的拨入服务器。通常，拨出计算机会先提供验证凭证，然后才能建立拨号链路。 |

| | |
|---|---|
| dial-up PPP link（拨号 PPP 链路） | 一种 PPP 连接，在电话线路（或类似通信介质，如 ISDN 提供的介质）的一端有一个对等点和一个调制解调器。术语“拨号”指的是本地调制解调器使用远程对等点的电话号码向该对等点拨号时，所使用的链路协商顺序。拨号链路是最常见最经济的 PPP 配置。 |
| Diffie-Hellman protocol（Diffie-Hellman 协议） | 使两个用户可以在以前没有任何信息的情况下通过不安全的通信介质交换密钥的非对称加密密钥协议。非对称加密密钥协议是公钥加密的基础。 |
| diffserv model（diffserv 模型） | Internet 工程任务组体系结构标准，用于在 IP 网络上实现区分服务。在 IP 网络中，diffserv 模型提供了一种用于分类和管理网络通信并提供 IPQoS 的简单的可扩展机制。主要模块是分类器、计量器、标记器、调度程序和丢包器。IPQoS 实现分类器、计量器和标记器模块。有关更多信息，请参见 RFC 2475 (http://www.ietf.org/rfc/rfc2475.txt)。 |
| digital signature（数字签名） | 附加到以电子方式传输的消息的数字代码，可唯一地标识发送者。 |
| direct memory access（直接内存访问） | 请参见 DMA。 |
| direct server return（服务器直接返回） | 请参见 DSR。 |
| distinguished name（标识名） | 请参见 DN。 |
| DLMP aggregation（DLMP 聚合） | （数据链路多路径聚合）一种链路聚合类型，它支持多个交换机并提供其数据链路的持续连接。当交换机出现故障时，聚合会使用其他交换机继续为其数据链路提供连接。此类型的链路聚合不要求配置交换机。也可以在单个交换机上创建 DLMP 聚合。 |
| DMA | （直接内存访问）一些设备可以执行涉及主内存和其他设备的数据传送，而无需 CPU 的帮助。这种类型的数据传送称为直接内存访问 (direct memory access, DMA)。 |
| DMZ | （非军事化区）设置为禁止对组织专用网络进行公共访问的隔离网络。此隔离网络可以包含公司为公众提供的资源，例如 Web 服务器、匿名 FTP 服务器和数据库。 |
| DN | （标识名）使用普通字符串表示共享信息的标准化方法。DN 用于 LDAP 和 X.509 证书等技术。 |

| | |
|---|---|
| DNS | （域名系统）一种服务，它提供的命名策略和机制用于将域名和计算机名映射为企业外部地址（例如 Internet 上的地址）。DNS 是由 Internet 使用的网络信息服务。有关更多信息，请参见 RFC 1034 (http://tools.ietf.org/html/rfc1034)。 |
| DOI | （系统解释域）DOI 定义数据格式、网络通信流量交换类型和安全相关信息的命名约定。安全策略、加密算法和加密模式都属于安全相关信息。 |
| domain name system（域名系统） | 请参见 DNS。 |
| domain of interpretation（系统解释域） | 请参见 DOI。 |
| DR | （动态重新配置）用于在系统运行的同时重新配置系统硬件的操作系统功能。通过使用 DR，可以在正常系统操作很少中断或无中断的情况下，添加或替换硬件资源。并非 Oracle 提供的所有 Sun 平台都支持 DR。有些平台可能仅支持某些类型的硬件（例如 NIC）的 DR。 |
| DS codepoint（DS 代码点） | 请参见 DSCP。 |
| DSCP | （DS 代码点）包括在包头的区分服务 (Differentiated Service, DS) 字段中的 6 位值。DSCP 指示必须如何转发包。有关更多信息，请参见 RFC 2474 (https://www.ietf.org/rfc/rfc2474.txt)。 |
| DSR | （服务器直接返回）一种模式，在该模式下，集成的负载平衡器可以平衡后端服务器的传入请求，而使从服务器返回到客户机的通信流量绕过集成的负载平衡器。 |
| DSU | （数据服务单元）在租用线路 PPP 链路上使用的同步电信设备。DSU 在电信线路上使用的数据帧格式之间进行转换，并且提供标准数据通信接口。 |
| dual stack（双栈） | 一个 TCP/IP 协议栈，使 IPv4 和 IPv6 协议可以在同一个网络基础结构上工作，而无需使用隧道连接机制。Oracle Solaris 网络是双栈。主机和路由器上都支持此双栈技术。 |
| DUID | （DHCP 唯一标识符）用于在启用 DHCPv6 的系统中标识客户机系统的标识符。 |
| Dynamic Host Configuration Protocol（动态主机配置协议） | 请参见 DHCP。 |

| | |
|---|---|
| dynamic packet filter（动态包过滤器） | 也称为stateful packet filter（有状态包过滤器）。 |
| dynamic reconfiguration（动态重新配置） | 请参见 DR。 |
| dynamic routing（动态路由） | 一种路由类型，系统通过使用诸如用于 IPv4 网络的 RIP 和用于 IPv6 网络的 RIPng 这样的路由协议来自动更新路由表。在具有许多主机的大型网络上使用动态路由的效果最好。 |
| ECMP | （等成本多路径）沿多个等成本路径路由包的路由技术。转发引擎按下一个跃点标识路径。当转发包时，路由器必须确定要使用的下一个跃点（路径）。有关更多信息，请参见 RFC 2992 (http://tools.ietf.org/html/rfc2992)。 |
| edge virtual bridging（边缘虚拟桥接） | 请参见 EVB。 |
| elastic virtual switch（弹性虚拟交换机） | 请参见 EVS。 |
| encapsulating security payload（封装安全有效负荷） | 请参见 ESP。 |
| encapsulation（封装） | 当包经由网络协议栈时，每一层上的协议都会在基本头中添加或删除字段。当发送主机上的协议向包头中添加数据时，此过程即称为数据封装。 |
| enhanced transmission selection（增强传输选择） | 请参见 ETS。 |
| ENM | （外部网络修饰器）为属于反应性网络配置外部，但可以更改和修改网络配置的应用程序创建的配置文件。通过 ENM，可以指定应用程序或脚本（例如 VPN 应用程序）必须何时执行自己的网络配置（在 NCP 和位置配置文件中指定的配置之外的配置）。 |
| equal-cost multi-path（等成本多路径） | 请参见 ECMP。 |
| ESP | （封装安全有效负荷）为 IP 数据报提供完整性、保密性和重放保护的扩展头。 |
| ESSID | （扩展服务集标识符）用作计算机或网络设备的标识和地址以连接和访问 Internet 的电子标记或标识符。它是 802.11b 无线网络的标识名称。 |

| | |
|---|---|
| Ethernet（以太网） | 用于连接一些计算机系统以形成局域网的系统。以太网可以使用协议来控制信息的传递，并避免两个或更多系统同时传输信息。 |
| etherstub | 在 Oracle Solaris 网络栈的数据链路层 (L2) 上配置的伪以太网 NIC。您可以在 etherstub（而非物理链路）上创建 VNIC，以便构建与系统上的其他虚拟网络以及外部网络隔离的专用虚拟网络。 |
| ETS | （增强传输选择）根据 DCB 优先级为应用程序分配 NIC 上的带宽的 DCB 功能。 |
| EVB | （边缘虚拟桥接）用于供主机与外部交换机交换虚拟链路信息的 L2 技术。EVB 将通信 SLA 的实施转移到交换机。 |
| EVS | （弹性虚拟交换机）Oracle Solaris 中的一种软件虚拟交换机，该交换机提供了跨越多个服务器的功能，因而在连接到弹性虚拟交换机的多个服务器上的虚拟机之间提供了网络连接。 |
| EVS client（EVS 客户机） | 从中管理弹性虚拟交换机的 EVS 组件。 |
| EVS controller（EVS 控制器） | 用于维护多个节点之间的弹性虚拟交换机的配置和状态的 EVS 组件。 |
| EVS node（EVS 节点） | 其 VNIC 连接到弹性虚拟交换机的主机。 |
| expect-send（期待发送） | 在 PPP 和 UUCP 聊天脚本中使用的一种脚本格式。此聊天脚本以期待来自远程对等点的文本或指令开头。接下来的一行包含从对等点接收到正确的 expect 字符串后，要从本地主机发送的响应。后续行会重复本地主机和对等点之间的 expect-send（期待发送）指令，直到建立通信所需的所有指令协商成功。 |
| extended accounting（扩展记帐） | 以任务或进程为单位记录资源占用情况的灵活方法。 |
| extended service set identifier（扩展服务集标识符） | 请参见 ESSID。 |
| external network modifier（外部网络修饰器） | 请参见 ENM。 |
| failure detection time（故障检测时间） | 请参见 FDT。 |
| failure detection（故障检测） | 检测一个接口或从接口到 Internet 层设备的路径何时不再工作的过程。IP 网络多路径 (IP Network |

| | |
|---|---|
| | Multipathing, IPMP) 和数据链路多路径 (datalink multipathing, DLMP) 包括两种类型的故障检测：基于链路的故障检测（缺省）和基于探测的故障检测（可选）。 |
| fault management resource identifier（故障管理资源标识符） | 请参见 FMRI。 |
| FDT | （故障检测时间）检测一个接口或从接口到 Internet 层设备的路径是否不再工作所需的时间量。 |
| filter（过滤器） | IPQoS 配置文件中定义类特性的规则集合。IPQoS 系统选择符合其 IPQoS 配置文件中过滤器的任何通信流以进行处理。请参见packet filter（包过滤器）。 |
| firewall（防火墙） | 将组织的专用网络或内联网与 Internet 隔离，从而防止它受到外部侵入的硬件或软件。防火墙包括包过滤、代理服务器和 NAT。 |
| fixed network configuration mode（固定网络配置模式） | 无论网络状况是否发生任何变化，系统上的实例化配置都具有持久性的网络配置模式。当发生这种更改（例如，添加接口）时，必须为系统重新配置网络以适应新环境。 |
| flow accounting（流记帐） | IPQoS 中累积和记录有关通信流的信息的过程。通过在 IPQoS 配置文件中定义 `flowacct` 模块的参数，可以建立流记帐。 |
| flow（流） | 为了进一步控制如何使用资源来处理网络包而对这些包进行分类的定制方式。 |
| FMRI | （故障管理资源标识符）Oracle Solaris 中的每个软件包的标识符。FMRI 包含软件包的发布者、名称和版本。 |
| GARP VLAN Registration Protocol（GARP VLAN 注册协议） | 请参见 GVRP。 |
| GLDv3 | （通用 LAN 驱动程序 v3）GLDv3 框架是 MAC 插件和 MAC 驱动程序服务例程与结构的基于函数调用的接口。GLDv3 框架代表符合 GLDv3 的驱动程序实现必要的 STREAMS 入口点，并处理 DLPI 兼容性。 |
| GVRP | （一般属性注册协议）客户机系统用来在连接的交换机中自动注册 VLAN ID 的协议。 |

| | |
|---|---|
| hash-based message authentication code（散列消息验证代码） | 请参见 HMAC。 |
| header（数据包头） | 请参见 IP header（IP 头）。 |
| HMAC | （散列消息验证代码）用于进行消息验证的加密散列方法。HMAC 是密钥验证算法，与重复加密散列函数（例如 MD5 或 SHA-1）以及机密共享密钥配合使用。HMAC 的加密能力取决于底层散列函数的特性。 |
| hop（跃点） | 用于标识分隔两个主机的路由器数量的度量。如果源主机和目标主机之间有三个路由器，则这两个主机之间有四个跃点。 |
| IA | （身份关联）服务器和客户机用来标识、分组和管理一组相关 IPv6 地址的方法。 |
| IAID | （身份关联标识符）用于在启用 DHCPv6 的系统中标识客户机系统的接口的标识符。 |
| IANA | （Internet 编号分配机构）将注册的 IP 地址授予世界各地的 Internet 注册机构的组织。 |
| ICMP | （Internet 控制消息协议）报告错误并交换控制消息的协议。它有助于诊断网络问题。 |
| ICMP echo request packet（ICMP 回显请求包） | 发送到 Internet 上的计算机以要求响应的包。这种包通常称为 "ping" 包，并且用于测试 IP 网络上的主机的可访问性。 |
| identity association identifier（身份关联标识符） | 请参见 IAID。 |
| identity association（身份关联） | 请参见 IA。 |
| IKE | （Internet 密钥交换）IKE 用于自动为 IPsec 安全关联 (Security Association, SA) 提供经过验证的加密材料。 |
| ILB | （集成负载平衡器）使系统能够在可用资源之间分配网络处理负载的 L3 和 L4 技术。ILB 可用于提高网络服务的可靠性和可伸缩性，并最大程度地缩短网络服务的响应时间。 |
| InfiniBand | 基于交换光纤结构的 I/O 技术。它为将 I/O 设备连接到主机以及主机到主机通信提供了高带宽、低延迟的互连。InfiniBand 在高性能的计算和企业数据中心中使用。 |

| | |
|---|---|
| integrated load balancer（集成负载平衡器） | 请参见 ILB。 |
| Integrated Services Digital Network terminal adaptor（集成服务数字网络终端适配器） | 请参见 ISDN TA。 |
| Internet Assigned Numbers Authority（Internet 编号分配机构） | 请参见 IANA。 |
| Internet Bootstrap Protocol（Internet 引导协议） | 请参见 BOOTP。 |
| Internet Control Message Protocol（Internet 控制消息协议） | 请参见 ICMP。 |
| Internet key exchange（Internet 密钥交换） | 请参见 IKE。 |
| Internet Protocol Control Protocol（Internet 协议控制协议） | 请参见 IPCP。 |
| Internet Protocol Version 6 Control Protocol（Internet 协议版本 6 控制协议） | 请参见 IPCP。 |
| Internet Protocol, version 4（Internet 协议版本 4） | 请参见 IPv4。 |
| Internet Protocol, version 6（Internet 协议版本 6） | 请参见 IPv6。 |
| Internet Protocol（Internet 协议） | 在 Internet 上将数据从一台计算机发送到另一台计算机时所用的协议。 |
| Internet registry（Internet 注册机构） | 请参见 IR。 |
| Internet Security Association and Key Management Protocol（Internet 安全关联和密钥管理协议） | 请参见 ISAKMP。 |
| IP header（IP 头） | 唯一标识 Internet 包的数据。该头包括包的源地址和目标地址。使用该头中的一个选项可以添加更多字 |

| | |
|---|---|
| | 节。IPv4 头包含 20 字节数据，IPv6 头包含 40 字节数据。 |
| IP in IP encapsulation（IP-in-IP 封装） | 在 IP 包中封装 IP 包的机制。请参见encapsulation（封装）。 |
| IP Multipathing（IP 多路径） | 请参见 IPMP。 |
| IP Quality of Service（IP 服务质量） | 请参见 IPQoS。 |
| IP security（IP 安全性） | 请参见 IPsec。 |
| IPCP | （Internet 协议控制协议）PPP 的子协议，用于协商链路上对等点的 IP 地址。IPCP 还会协商链路的头压缩，并允许使用网络层协议。 |
| IPMP | （IP 多路径）确保系统可以持续访问网络的第 3 层 (L3) 技术。通过 IPMP，可以将多个 IP 接口配置到一个 IPMP 组中。 |
| IPMP group（IPMP 组） | IP 多路径组由具有一组数据地址的一组网络接口组成，系统将这些数据地址视为可互换地址，从而提高网络可用性和利用率。IPMP 组（包括其所有底层 IP 接口和数据地址）由一个 IPMP 接口表示。 |
| IPnet | 与弹性虚拟交换机关联的 IPv4 地址块或 IPv6 地址块。IPv4 地址块或 IPv6 地址块存在于同一个子网上（该块有默认路由器）并且与 Oracle Solaris 弹性虚拟交换机功能配合使用。 |
| IPQoS | （IP 服务质量）一种软件功能，提供 diffserv model（diffserv 模型）标准的实现以及虚拟 LAN 的流记帐和 802.1D 标记。通过使用 IPQoS，可以为客户和应用程序提供不同级别的网络服务。 |
| IPsec | （IP 安全性）通过验证和加密 IP 包为 IP 通信提供保护的安全体系结构。 |
| IPv4 | （Internet 协议版本 4）支持 32 位 地址空间的 Internet 协议版本。IPv4 有时简称为 IP。有关更多信息，请参见 RFC 791 (http://www.ietf.org/rfc/rfc791.txt)。 |
| IPv4 broadcast address（IPv4 广播地址） | IPv4 网络地址，其主机部分的所有位全为 0 (10.50.0.0) 或全为 1 (10.50.255.255)。从本地网络上的计算机发送到广播地址的包将被传送到该网络中的所有计算机。 |

| | |
|---|---|
| IPv6 | （Internet 协议版本 6）支持 128 位地址空间的 Internet 协议版本。有关更多信息，请参见 RFC 2460 (http://www.ietf.org/rfc/rfc2460.txt)。 |
| IPv6 autoconfiguration（IPv6 自动配置） | 主机根据站点前缀和本地 MAC 地址自动配置其 IPv6 地址的过程。 |
| IR | （Internet 注册机构）包含 Internet 编号（包括 IP 地址和自治系统 (autonomous system, AS) 的编号）的注册信息的注册机构。 |
| ISAKMP | （Internet 安全关联和密钥管理协议）用于建立 SA 属性格式以及协商、修改和删除 SA 的通用框架。ISAKMP 是处理 IKE 交换的 IETF 标准。 |
| ISDN TA | （集成服务数字网络终端适配器）一种信号调整设备，为 ISDN 上的拨号 PPP 链路提供与调制解调器类似的接口。Solaris PPP 4.0 配置文件用于配置用作标准调制解调器的 ISDN TA。 |
| key management（密钥管理） | 加密密钥的管理。这种管理包括在用户级别（用户或系统之间）生成、交换、存储、使用和替换密钥。 |
| keystore name（密钥库名称） | 管理员为密钥库指定的名称。在加密框架中，密钥库名称也称为“令牌”或“令牌 ID”。 |
| keystore（密钥库） | 磁盘或卡上存储加密密钥的位置。 |
| KMF | （Oracle Solaris 密钥管理框架）提供用于管理公钥对象（包括 X.509 证书和公钥/私钥对）的工具和编程接口的框架。KMF 还提供了一种工具，用于管理定义应用程序如何使用 X.509 证书的策略。 |
| LACP | （链路聚合控制协议）在一个链路聚合组中的各个系统之间动态交换网络配置信息的 IEEE 802.3ad 标准。此协议可帮助自动配置和维护链路聚合组。 |
| LCP | （链路控制协议）PPP 的子协议，用于协商对等点之间的一组初始链路参数。LCP 用于检查链路设备的身份，搜索链路配置中的错误，并确定可接受的包传输大小。 |
| LDAP | （轻量目录访问协议）用于管理 IP 网络上的目录信息的客户机/服务器协议。LDAP 实现了信息存储、检索和分发的单个管理点。LDAP 让使用 LDAP 命名服务的客户机和服务器可以相互通信。有关更多信息，请参见 RFC 4511 (https://tools.ietf.org/rfc/rfc4511.txt)。 |
| leased-line PPP link（租用线路 PPP 链路） | 一种 PPP 连接，包括连接到从提供商处租用的同步网络介质的主机和 CSU/DSU。租用线路介质的常见 |

| | |
|---|---|
| | 示例是光载波 3 (Optical Carrier 3, OC3) 和 T 载波 (T carrier, T1)。尽管租用线路链路更易于管理，但它的成本要比拨号 PPP 链路高得多，所以使用得比较少。 |
| Lightweight Directory Access Protocol（轻量目录访问协议） | 请参见 LDAP。 |
| Link Aggregation Control Protocol（链路聚合控制协议） | 请参见 LACP。 |
| link aggregation（链路聚合） | 将系统上的若干个链路合并到单个逻辑单元以增加网络通信的吞吐量的方法。 |
| Link Control Protocol（链路控制协议） | 请参见 LCP。 |
| Link Layer Discovery Protocol（链路层搜索协议） | 请参见 LLDP。 |
| link-local address（链路本地地址） | IPv6 中用于在单个链路上寻址以实现自动配置地址等目的的标识。缺省情况下，链路本地地址是从系统的 MAC 地址创建的。 |
| LLDP | （链路层搜索协议）使网络设备能够向 IEEE 802 局域网 (local area network, LAN) 上的其他网络设备通告其功能、身份和当前状态的链路层协议。 |
| load spreading（负荷分配） | 在一组接口中分配传入或传出通信的过程。通过负荷分配，可以获得较高的吞吐量。仅当网络通信流向使用多个连接的多个目标时，才会发生负荷分配。负荷分配有两种类型：传入负荷分配（对于传入通信）和传出负荷分配（对于传出通信）。 |
| local-use address（本地使用地址） | 只能在本地范围内（在子网内或在用户网络内）路由的单播地址。此地址还可以具有本地或全局唯一性范围。 |
| MAC address（MAC 地址） | （介质访问控制地址）分配给网络接口的唯一地址。MAC 地址用于物理网段上的通信。 |
| marker（标记器） | 1. diffserv 体系结构和 IPQoS 中的一个模块，它使用指示包转发方式的值标记 IP 包的 DS 字段。在 IPQoS 实现中，标记器模块是 `dscpmk`。<br><br>2. IPQoS 实现中的一个模块，它使用用户优先级值标记以太网数据报的虚拟 LAN 标记。用户优先级值指示 |

| | |
|---|---|
| | 使用 VLAN 设备在网络中转发数据报的方式。此模块称为 `dlcosmk`。 |
| master router（主路由器） | 在给定时间执行虚拟路由器的路由功能的 VRRP 实例。对于给定的 VRID，一次只能有一个主路由器处于活动状态。主路由器控制与虚拟路由器关联的 IPv4 或 IPv6 地址。虚拟路由器转发发送到主路由器的 IP 地址的包。 |
| maximum transmission unit（最大传输单位） | 请参见 MTU。 |
| MD5 | 一种重复加密散列函数，用于进行消息验证（包含数字签名）。 |
| meter（计量器） | diffserv 体系结构中的一个模块，用于度量特定类的通信流速率。IPQoS 实现包括以下两个计量器：`tokenmt` 和 `tswtclmt`。 |
| Microsoft CHAP | 请参见 MS-CHAP。 |
| minimal encapsulation（最小封装） | 家乡代理、外地代理和移动节点支持的可选 IPv4 嵌套隧道传送形式。最小封装的系统开销比 IP-in-IP 封装少 8 或 12 个字节。 |
| MS-CHAP | (Microsoft CHAP) 用于 PPP 的 Microsoft 专有验证协议。Solaris PPP 4.0 支持在客户机和服务器模式下使用此协议的版本 1 和版本 2。 |
| MTU | （最大传输单位）可在链路上传输的最大数据单元的大小，采用八位字节形式。 |
| multicast address（多播地址） | 标识一组接口的 IPv4 或 IPv6 地址。发送到多播地址的包将被传送到组中的所有接口。 |
| multicast（多播） | 一个网络层过程，用于将数据报包发送到 IP 网络上的多台计算机。与广播路由不同，包不会被每台计算机处理。多播要求使用特定的路由协议（例如，距离向量多播路由协议 (Distance Vector Multicast Routing Protocol, DVMRP)）来配置路由器。有关 DVMRP 的更多信息，请参见 RFC 1075 (http://tools.ietf.org/rfc/rfc1075.txt)。 |
| multihomed host（多宿主主机） | 具有多个接口且不执行包转发的系统。多宿主主机可以运行路由协议。 |
| NAT | （网络地址转换）将一个网络中使用的 IP 地址转换为另一个网络中已知的不同 IP 地址的过程。用于限制所需的全局 IP 地址的数目。 |

| | |
|---|---|
| NCP | （网络配置文件）在 Oracle Solaris 中用于管理系统的网络配置的配置文件。在某一时刻，系统中只能有一个 NCP 处于活动状态。 |
| NCU | （网络配置单元）包含所有定义 NCP 的属性的单个配置对象。每个 NCU 表示一个物理链路或一个接口，且包含定义该链路或接口的配置的属性。 |
| neighbor advertisement（相邻节点通告） | 对相邻节点的请求消息的响应，或一个节点发送未经请求的相邻节点通告以通告链路层地址更改的过程。 |
| neighbor discovery（相邻节点搜索） | 一种 IP 机制，使主机可以查找驻留在已连接链路上的其他主机。 |
| neighbor solicitation（相邻节点请求） | 由一个节点发送的请求，用于确定相邻节点的链路层地址。相邻节点请求还通过高速缓存的链路层地址验证相邻节点是否仍然可以访问。 |
| network address translation（网络地址转换） | 请参见 NAT。 |
| network configuration profiles（网络配置文件） | 请参见 NCP。 |
| network configuration unit（网络配置单元） | 请参见 NCU。 |
| Network File System（网络文件系统） | 请参见 NFS。 |
| network information service（网络信息服务） | 请参见 NIS。 |
| network interface card（网络接口卡） | 请参见 NIC。 |
| Network Time Protocol（网络时间协议） | 请参见 NTP。 |
| NFS | （网络文件系统）用于远程访问网络上的共享文件的文件系统协议。 |
| NIC | （网络接口卡）将计算机连接到网络的网络适配器卡。一些 NIC 可以具有多个物理接口，如 `igb` 卡。 |
| NIC rings（NIC 环） | 在 NIC 上，接收 (Rx) 环和传送 (Tx) 环是硬件资源，系统分别通过它们来接收和传送网络数据包。 |
| NIS | （网络信息服务）一种分布式网络数据库，其中包含有关网络上的系统和用户的关键信息。 |

| | |
|---|---|
| node（节点） | 在计算机网络中，节点是指数据传输的连接点或结束点。 |
| NTP | （网络时间协议）用于设置和维护系统时间的协议。NTP 软件作为 `ntpd` 守护进程实现，这是 RFC 5905 (https://tools.ietf.org/html/rfc5905) 中定义的版本 4 标准的完整实现。 |
| Open Systems Interconnection model（开放系统互连模型） | 请参见 OSI model（OSI 模型）。 |
| Oracle Solaris Key Management Framework（Oracle Solaris 密钥管理框架） | 请参见 KMF。 |
| OSI model（OSI 模型） | （开放系统互连模型）国际标准组织 (International Standard Organization, ISO) 设计的标准模型，用于描述应如何在网络上传输数据。 |
| outcome（结果） | 在 IPQoS 中，作为计量通信流量的结果而执行的操作。IPQoS 计量器具有三种结果：红色、黄色和绿色。可以在 IPQoS 配置文件中定义结果。 |
| packet filter（包过滤器） | 一种防火墙功能，可以配置为允许或禁止指定的包通过防火墙。 |
| packet header（包头） | 请参见 IP header（IP 头）。 |
| packet（包） | 通过通信线路作为一个单位传输的一组信息。包含 IP header（IP 头）以及 payload（有效负荷）。 |
| PAP | （口令验证协议）一种验证协议，可用于检验 PPP 链路上调用方的身份。PAP 使用通过链路传送的明文口令，这样就可以将口令存储在其中一台端点计算机上。例如，PAP 可使用接收调用的计算机上 UNIX `passwd` 数据库中的登录和口令项来检验调用方的身份。 |
| password authentication protocol（口令验证协议） | 请参见 PAP。 |
| payload（有效负荷） | 通过包传输的数据。有效负荷不包括将包传输到其目标所需的头信息。 |
| PCIe | （外设部件互连加速）将计算机与其外围设备连接的串行 I/O 总线。 |

| | |
|---|---|
| per-hop behavior（单跳行为） | 请参见 PHB。 |
| perfect forward secrecy（完全正向保密） | 请参见 PFS。 |
| peripheral component interconnect express（外设部件互连加速） | 请参见 PCIe。 |
| PF | （物理功能）用于支持 SR-IOV 功能的 PCI 功能，如 SR-IOV 规范中定义。PF 包含 SR-IOV 功能结构，用于管理 SR-IOV 功能。PF 是全功能的 PCIe 功能，可以像其他任何 PCIe 设备一样进行发现、管理和处理。PF 拥有完全配置资源，可以用于配置或控制 PCIe 设备。 |
| PFC | （基于优先级的流控制）数据链路级别的流控制机制。PFC 扩展了标准 PAUSE 帧以包含 IEEE 802.1p 服务类 (class of service, CoS) 值。在 PFC 中，仅选择性地暂停 PFC 帧中启用的 CoS 值所对应的通信，而不是停止数据链路上的所有通信。 |
| PFS | （完全正向保密）在 PFS 中，不能使用保护数据传输的密钥派生其他密钥。此外，也不能使用保护数据传输的密钥的源派生其他密钥。PFS 适用于 IKE 中经过验证的密钥交换。 |
| PHB | （单跳行为）遍历跃点时分配给包的通信类的优先级。 |
| physical function（物理功能） | 请参见 PF。 |
| physical interface（物理接口） | 系统与链路的连接。此连接通常实现为设备驱动程序和 NIC。一些 NIC 可以具有多个连接点，例如 `igb`。 |
| PKI | （公钥基础结构）由数字证书、CA 和其他注册机构组成的系统，用于检验和验证 Internet 事务中涉及的各方的有效性。 |
| Point-to-Point Protocol（点对点协议） | 请参见 PPP。 |
| port VLAN identifier（端口 VLAN 标识符） | 请参见 PVID。 |
| PPP | （点对点协议）一种链路层协议，提供通过点对点介质传送数据报的标准方法。PPP 配置由称为对等点的 |

| | |
|---|---|
| | 两个端点计算机，以及对等点用于通信的电话线路或其他双向链路组成。两个对等点之间的硬件和软件连接将视为 *PPP* 链路。<br><br>PPP 由许多子协议（包括 PAP、CHAP、LCP 和 CCP）组成。 |
| PPP over Ethernet（基于以太网的 PPP） | 请参见 PPPoE。 |
| PPPoE | （基于以太网的 PPP）允许主机通过以太网链路运行 PPP 会话的协议。PPPoE 通常与数字用户线路 (Digital Subscriber Line, DSL) 服务配合使用。 |
| Precision Time Protocol（精确时间协议） | 请参见 PTP。 |
| priority-based flow control（基于优先级的流控制） | 请参见 PFC。 |
| private address（专用地址） | 无法通过 Internet 进行路由的 IP 地址。无需 Internet 连通性的主机上的家乡网络可以使用专用地址。有关 IPv4 专用地址的更多信息，请参见 RFC 1918 (https://tools.ietf.org/html/rfc1918)。有关 IPv6 专用地址的更多信息，请参见 RFC 4193 (http://www.ietf.org/rfc/rfc4193.txt)。 |
| private virtual network（专用虚拟网络） | 与系统上的其他虚拟网络和外部网络隔离的虚拟网络。通过 etherstub 配置专用虚拟网络。 |
| proxy server（代理服务器） | 位于客户机与另一个服务器之间的中间服务器。它提供高速缓存服务、管理控制和安全性。例如，代理服务器可用于阻止对某些 Web 站点的访问。 |
| PTP | （精确时间协议）用于同步一个广播域中的多个系统的系统时钟的 IEEE 协议。PTP 软件作为 `ptpd` 守护进程实现，这是 IEEE 标准 1588-2008 中定义的 PTP 版本 2 的实现。 |
| public key cryptography（公钥密码学） | 一种加密算法，需要两个数学上链接的不同密钥。公钥对所有用户可用。私钥只对消息接收方公开。公钥密码学也称为非对称密码学。 |
| public key infrastructure（公钥基础结构） | 请参见 PKI。 |
| PVID | （端口 VLAN 标识符）在此链路中收发的不带标记的包所采用的缺省 VLAN ID。 |

| | |
|---|---|
| RARP | （反向地址解析协议）在 Internet 协议 (Internet Protocol, IP) 和以太网地址之间动态映射的协议。RARP 用于将 MAC 地址解析为局域网上的 IP 地址。有关更多信息，请参见 RFC 903 (http://tools.ietf.org/rfc/rfc903.txt)。 |
| RCM | （重新配置协调管理器）用于管理系统组件的动态删除并帮助按顺序注册和释放系统资源的框架。 |
| reactive network configuration mode（反应性网络配置模式） | 一种网络配置模式，在该模式中，系统会自动适应网络状况的任何变化，而无需手动重新配置。 |
| reconfiguration coordination manager（重新配置协调管理器） | 请参见 RCM。 |
| redirect（重定向） | 在路由器中，通告主机有一个更好的第一跃点节点可以到达特定目标。 |
| reflective relay（反射中继） | EVB 中的一项功能，利用此功能，可以选择在网络上发送 VM 间通信，外部交换机将回送该通信。这样，您就可以从千兆位以太网 (gigabit Ethernet, GbE) 移到虚拟化 10GbE，同时保留外部交换机上的 IT 策略。 |
| repair detection（修复检测） | 检测 NIC 或从 NIC 到某个第 3 层设备的路径在出现故障后何时开始正常工作的过程。 |
| replay attack（重放攻击） | 数据传输期间侵入者捕获了包的网络攻击。捕获到的包稍后将替换为欺骗性的包或重复该包。为了避免遭到此类攻击，可以在包中包含一个字段，并使该字段在包的保护密钥的生命周期内递增。 |
| Reverse Address Resolution Protocol（反向地址解析协议） | 请参见 RARP。 |
| RIP | （路由信息协议）路由 IPv4 包并维护 LAN 上所有主机的路由表的内部网关协议。有关更多信息，请参见 RFC 2453 (https://tools.ietf.org/html/rfc2453)。 |
| RIPng | （下一代路由信息协议）路由 IPv6 包并维护 LAN 上所有主机的路由表的内部网关协议。有关更多信息，请参见 RFC 2080 (http://tools.ietf.org/rfc/rfc2080.txt)。 |
| router advertisement（路由器通告） | 路由器通告其存在以及各种链路和 Internet 参数的过程，要么是定期进行通告，要么是作为对路由器请求消息的响应进行通告。 |

| | |
|---|---|
| router discovery（路由器搜索） | 主机查找驻留在已连接链路上的路由器的过程。 |
| router solicitation（路由器请求） | 主机请求路由器以立即（而非下一个预定时间）生成路由器通告的过程。 |
| router（路由器） | 具有多个接口、运行路由协议并在计算机网络之间转发数据包的系统。路由器用于定向 Internet 上的通信并连接来自不同网络的两个或更多数据线。路由器通过网络将数据包从一个路由器转发到另一个路由器，直至数据包到达其目标。 |
| Routing Information Protocol next generation（下一代路由信息协议） | 请参见 RIPng。 |
| Routing Information Protocol（路由信息协议） | 请参见 RIP。 |
| routing table（路由表） | 包含某个包的路由信息的表，可帮助确定该包到达其目标的最佳路径。 |
| RSA | 获取数字签名和公钥密码系统的方法。 |
| SA | （安全关联）指定从一个主机到另一个主机的安全属性的关联。 |
| SADB | （安全关联数据库）指定加密密钥和加密算法的 SA 表。在数据的安全传输中会使用这些密钥和算法。 |
| SCTP | （流控制传输协议）以与 TCP 类似的方式提供面向连接的通信的传输层协议。此外，SCTP 还支持连接多宿主，即连接的端点之一可以具有多个 IP 地址。有关更多信息，请参见 RFC 4960 (http://tools.ietf.org/html/rfc4960)。 |
| Secure Hashing Algorithm（安全散列算法） | 请参见 SHA-1。 |
| secure sockets layer（安全套接字层） | 请参见 SSL。 |
| security association（安全关联） | 请参见 SA。 |
| security associations database（安全关联数据库） | 请参见 SADB。 |
| security parameter index（安全参数索引） | 请参见 SPI。 |

| | |
|---|---|
| security policy database（安全策略数据库） | 请参见 SPD。 |
| selector（选定器） | IPQoS 中的元素，专门用于定义应用于特定类的包的条件，以便从网络流中选择该类通信流量。可以在 IPQoS 配置文件的过滤子句中定义选定器。 |
| service management facility（服务管理工具） | 请参见 SMF。 |
| SHA-1 | （安全散列算法）可以在长度小于 $2^{64}$ 的任意输入上运行以生成消息摘要的算法。SHA-1 算法是 DSA 的输入。 |
| Simple Network Management Protocol（简单网络管理协议） | 请参见 SNMP。 |
| single root I/O virtualization（单一根 I/O 虚拟化） | 请参见 SR-IOV。 |
| SMF | （服务管理工具）用于定义应用程序之间或服务之间的关系，以便相关服务可在必要时自动重新启动的功能。 |
| smurf attack（smurf 攻击） | 使用从远程位置定向到一个 IP 广播地址或多个广播地址的 ICMP 回显请求包以造成严重的网络拥塞或故障的过程。 |
| sniff（探查） | 在计算机网络中窃听 – 通常作为自动化程序的一部分，以便从线路中筛选出信息，如明文口令。 |
| SNMP | （简单网络管理协议）一种协议，该协议提供用于查询、监视和管理连接到 IP 网络的设备的常用方法。 |
| Spanning Tree Protocol（生成树协议） | 请参见 STP。 |
| SPD | （安全策略数据库）指定要应用到 IPsec 所保护包的保护级别的数据库。SPD 对 IP 通信流量进行过滤，以确定一个包是必须被废弃、在网络上发送还是必须用 IPsec 进行保护。 |
| SPI | （安全参数索引）一个整数，用于指定 SADB 中接收者用来对收到的包进行解密的行。 |
| spoof（电子欺骗） | 使用一个 IP 地址（该地址指示消息来自受信任主机）向计算机发送消息，以获取对该计算机的未经授权的 |

| | |
|---|---|
| | 访问。要进行 IP 电子欺骗，发送方必须先使用各种方法查找受信任主机的 IP 地址，然后修改包头以使这些包看起来像是来自该主机。 |
| SR-IOV | （单一根 I/O 虚拟化）一项标准，允许在虚拟机之间高效共享外设部件互连加速 (Peripheral Component Interconnect Express, PCIe) 设备，并且在硬件中实现。SR-IOV 规范允许将虚拟机直接连接到 I/O 设备。 |
| SSL | （安全套接字层）一种安全的低级别加密形式，供 HTTP 和 FTP 等协议使用。SSL 协议包括对服务器验证、传输中数据的加密及可选客户机验证的设置。 |
| SSL kernel proxy（SSL 内核代理） | 在内核中运行的可配置代理，用于加速受安全套接字层 (secure sockets layer, SSL) 保护的 Web 服务器通信。 |
| standby interface（备用接口） | 用于传输数据通信流量的物理接口（仅当某个其他物理接口出现故障时）。 |
| stateful packet filter（有状态包过滤器） | 可以监视活动连接的状态和使用获取的信息确定允许哪些网络包通过 packet filter（包过滤器）的 firewall（防火墙）。通过跟踪和匹配请求与回复，有状态包过滤器可以筛选出与请求不匹配的回复。 |
| stateless autoconfiguration（无状态自动配置） | 主机通过组合其 MAC 地址和 IPv6 前缀（由本地 IPv6 路由器通告）生成自己的 IPv6 地址的过程。 |
| static routing（静态路由） | 系统网络管理员可以将路由手动添加到路由表的过程。 |
| STP | （生成树协议）桥接网络用来防止网络循环使子网不可用的缺省协议。 |
| Stream Control Transport Protocol（流控制传输协议） | 请参见 SCTP。 |
| subnet（子网） | 用于将系统与子网号和 IP 地址架构连接的 IP 网络的逻辑细分，包括其各自的网络掩码。 |
| symmetric key cryptography（对称密钥密码学） | 一种加密系统，其中消息的发送者和接收者共享一个公用密钥。此公用密钥用于对消息进行加密和解密。Advanced Encryption Standard（高级加密标准）就是对称密钥的一个示例。 |
| synchronous PPP（同步 PPP） | 一种在同步数字线路上运行的 PPP，同步数字线路以连续的原始位流的形式传送数据。租用线路 PPP 链路使用同步 PPP。 |

| | |
|---|---|
| tenant（租户） | 弹性虚拟交换机中的虚拟交换机逻辑分组在一起。每个逻辑组称为一个租户。弹性虚拟交换机在一个租户内定义的资源在该租户的名称空间外部不可见。租户用作一个容器，将该租户的所有资源存放在一起。 |
| test address（测试地址） | IPMP 组中只能用作探测器的源地址或目标地址而不能用作数据通信的源地址或目标地址的 IP 地址。 |
| TFTP | （简单文件传输协议）用于在网络配置服务器与网络客户机之间传输文件的文件传输协议。TFTP 通常用于在一个本地网络中的各计算机之间自动传输配置或引导文件。有关更多信息，请参见 RFC 1350 (http://www.ietf.org/rfc/rfc1350.txt)。 |
| Triple-Data Encryption Standard（三重数据加密标准） | 请参见 3DES。 |
| Trivial File Transfer Protocol（简单文件传输协议） | 请参见 TFTP。 |
| trunk aggregation（中继聚合） | 基于 IEEE 802.3ad 标准的链路聚合。通过中继聚合，可以跨一组聚合端口分配多个通信流。要跨多个交换机工作，IEEE 802.3ad 需要交换机配置和交换机供应商专有扩展。 |
| trusted callers（可信调用方） | PPP 中拨入服务器对其授予访问权（通过在此服务器的 PAP 或 CHAP 机密数据库中加入对等点的安全凭证）的远程对等点。 |
| UDP | （用户数据报协议）一台计算机用于将数据报发送至 IP 网络上的其他计算机且无需设置特殊传输通道或数据路径的协议。有关更多信息，请参见 RFC 768 (http://www.ietf.org/rfc/rfc768.txt)。 |
| unicast address（单播地址） | 标识启用了 IPv6 的节点的单个接口的 IPv6 地址。单播地址包括以下几部分：站点前缀、子网 ID 和接口 ID。 |
| uniform resource indicator（统一资源指示符） | 请参见 URI。 |
| uniform resource locator（统一资源定位符） | 请参见 URL。 |
| UNIX-to-UNIX Copy Program（UNIX 对 UNIX 复制程序） | 请参见 UUCP。 |

| | |
|---|---|
| uplink port（上行端口） | 使用 Oracle Solaris EVS 功能时，在其上创建 VNIC 的数据链路。 |
| URI | （统一资源指示符）用于在 Internet 或专用内联网上标识资源的寻址技术。 |
| URL | （统一资源定位符）用于在 Internet 或专用内联网上标识资源的字符串。 |
| User Datagram Protocol（用户数据报协议） | 请参见 UDP。 |
| user-priority（用户优先级） | 一个用于实现服务类 (class-of-service, CoS) 标记的 3 位值。CoS 定义如何在 VLAN 设备网络上转发以太网数据报。 |
| UUCP | （UNIX 对 UNIX 复制程序）使计算机能够传输文件和彼此交换邮件的程序。UUCP 还使计算机能够参与大型网络，例如 Usenet。 |
| VDP | （VSI 搜索和配置协议）EVB 用来交换有关 VSI（虚拟交换机接口）的信息的协议。 |
| VF | （虚拟功能）与物理功能关联的 SR-IOV 功能。VF 是一种轻量级 PCIe 功能，可以与物理功能以及与同一物理功能关联的其他 VF 共享一个或多个物理资源。VF 仅允许拥有用于其自身行为的配置资源。 |
| virtual extensible local area network（虚拟可扩展局域网） | 请参见 VXLAN。 |
| virtual function（虚拟功能） | 请参见 VF。 |
| Virtual IP address（虚拟 IP 地址） | 请参见 VRIP。 |
| virtual LAN device（虚拟 LAN 设备） | 请参见 VLAN device（VLAN 设备）。 |
| virtual local area network（虚拟局域网） | 请参见 VLAN。 |
| virtual network identifier（虚拟网络标识符） | 请参见 VNI。 |
| virtual network interface card（虚拟网络接口卡） | 请参见 VNIC。 |
| virtual network（虚拟网络） | 模拟物理网络并且是硬件和软件网络资源的组合的网络。 |

| | |
|---|---|
| virtual port（虚拟端口） | VNIC 与弹性虚拟交换机之间的连接点。虚拟端口可封装 VNIC 在连接到虚拟端口时继承的各种网络配置参数。 |
| virtual private network（虚拟专用网络） | 请参见 VPN。 |
| Virtual Router ID（虚拟路由器 ID） | 请参见 VRID。 |
| Virtual Router Redundancy Protocol（虚拟路由器冗余协议） | 请参见 VRRP。 |
| virtual station instance（虚拟站实例） | 请参见 VSI。 |
| virtual switch（虚拟交换机） | 便于虚拟机之间通信的实体。虚拟交换机会循环物理计算机内的虚拟机之间的通信（VM 间通信），并且不会在网络上发送此通信。虚拟交换机可通过 EVS 进行管理并在创建 VNIC 时自动实例化。 |
| VLAN | （虚拟局域网）协议栈的数据链路层上对局域网的细分。 |
| VLAN device（VLAN 设备） | （虚拟 LAN 设备）在 IP 协议栈的以太网（数据链路）级别提供通信流量转发的网络接口。 |
| VNI | （虚拟网络标识符）使用 VXLAN 网段 ID（也称为 VNI）标识 VXLAN。每个 VXLAN 数据链路与一个 VNI 相关联。 |
| VNIC | （虚拟网络接口卡）行为方式就像配置的物理 NIC 的 L2 实体或虚拟网络设备。可以在底层数据链路上配置 VNIC，以便在多个区域或虚拟机 (virtual machines, VM) 之间共享 VNIC 或者将 VNIC 连接到弹性虚拟交换机。 |
| VPN | （虚拟专用网络）单个安全逻辑网络，使用跨公共网络（例如 Internet）的隧道。 |
| VRID | （虚拟路由器 ID）用于在给定网段中标识虚拟路由器的唯一编号。VRID 标识 LAN 内的虚拟路由器。 |
| VRIP | （虚拟 IP 地址）与 VRID 关联的 IP 地址，其他主机可通过该地址获取网络服务。VRIP 由属于 VRID 的 VRRP 实例管理。 |
| VRRP | （虚拟路由器冗余协议）提供 IP 地址（例如，用于路由器和负载平衡器的 IP 地址）的高可用性的协议。 |

| | |
|---|---|
| VSI | （虚拟站实例）VSI 指站中配置的 VNIC。 |
| VSI Discovery and Configuration Protocol（VSI 搜索和配置协议） | 请参见 VDP。 |
| VXLAN | （虚拟可扩展局域网）在 IP (L3) 网络之上覆盖数据链路 (L2) 网络的 L2 和 L3 技术。VXLAN 解决了使用 VLAN 时施加的 4K 限制。通常，VXLAN 在云基础结构中用于隔离多个虚拟网络。 |
| VXLAN segment ID（VXLAN 网段 ID） | 另请参见 VNI。 |
| WAP | （无线应用协议）用于通过移动无线网络访问信息的标准协议。 |
| WEP key（WEP 密钥） | （有线对等保密密钥）用于建立与安全 Wi-Fi 网络的连接的密钥。 |
| wired equivalent privacy key（有线对等保密密钥） | 请参见 WEP key（WEP 密钥）。 |
| Wireless Application Protocol（无线应用协议） | 请参见 WAP。 |