

Glosario de términos de redes

ORACLE®

Referencia: E53820
Julio de 2014

Copyright © 2011, 2014, Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comunique por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera licencias en nombre del Gobierno de EE.UU. se aplicará la siguiente disposición:

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

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus filiales declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus filiales. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden ofrecer acceso a contenidos, productos o servicios de terceros o información sobre los mismos. Ni Oracle Corporation ni sus filiales serán responsables de ofrecer cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros y renuncian explícitamente a ello. Oracle Corporation y sus filiales no se harán responsables de las pérdidas, los costos o los daños en los que se incurra como consecuencia del acceso o el uso de contenidos, productos o servicios de terceros.

Contenido

Uso de esta documentación	5
1 Términos de redes de Oracle Solaris	7
Glosario	7

Uso de esta documentación

- **Descripción general:** proporciona definiciones de términos y acrónimos comunes de redes utilizados en el contexto de redes de Oracle Solaris.
- **Destinatarios:** administradores de sistemas.
- **Conocimientos requeridos:** básicos y algunos conocimientos avanzados sobre redes.

Biblioteca de documentación del producto

En la biblioteca de documentación (<http://www.oracle.com/pls/topic/lookup?ctx=E36784>), se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

Los clientes de Oracle tienen acceso a soporte electrónico por medio de My Oracle Support. Para obtener más información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o, si tiene alguna discapacidad auditiva, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>.

Comentarios

Envíenos comentarios acerca de esta documentación mediante <http://www.oracle.com/goto/docfeedback>.

Términos de redes de Oracle Solaris

En este glosario, se definen los términos y los acrónimos de redes más usados en Oracle Solaris para ayudar a quien escribe documentación, especificaciones y documentación de formación, y para ayudar a garantizar su uso uniforme. Este glosario no incluye una lista exhaustiva de los términos que normalmente se aplican a todas las redes. Además, muchos de los términos de este glosario son específicos de las tecnologías de redes de Oracle Solaris.

Glosario

3DES	(Triple-Data Encryption Standard, estándar de cifrado de datos triple) Un método de cifrado de clave simétrica que aplica el algoritmo de cifrado estándar de cifrado de datos (DES) para cifrar los datos tres veces. 3DES necesita un tamaño de clave de 168 bits. 3DES también es conocido como Triple-DES.
6to4	Un mecanismo de colocación automática de que transfiere paquetes de IPv6 sobre una red IPv4. Los túneles 6to4 permiten que los sitios IPv6 aislados se comuniquen a través de un túnel automático en una red IPv4 sin la necesidad de configurar túneles específicos.
acceso directo a memoria	Consulte DMA .
adaptador de terminal de red digital de servicios integrados	Consulte adaptador de terminal RDSI .
adaptador de terminal RDSI	(Integrated Services Digital Network terminal adaptor, adaptador de terminal de red digital de servicios integrados) Un dispositivo de adaptación de señal que proporciona una interfaz similar a un módem para un enlace PPP por marcación telefónica a través de una red RDSI. Los archivos de configuración de Solaris PPP 4.0 se utilizan para configurar un adaptador de terminal RDSI cuando se utiliza como módem estándar.

AES	(Advanced Encryption Standard) Una técnica de cifrado de datos en bloques de 128 bits. AES es el estándar de cifrado del gobierno de los EE. UU.
agregación de enlaces	Un método para combinar varios enlaces en un sistema en una sola unidad lógica para aumentar el rendimiento del tráfico de red.
agregación de troncos	Una agregación de enlaces que se basa en el estándar IEEE 802.3ad. Las agregaciones de troncos funcionan mediante la activación de varios flujos de tráfico que se distribuyen en un juego de puertos agregados. El estándar IEEE 802.3ad requiere configuración del conmutador, además de extensiones de propiedad del proveedor del conmutador para poder trabajar en varios conmutadores.
agregación DLMP	(datalink multipathing aggregation, agregación de rutas múltiples de enlaces de datos) Un tipo de agregación de enlaces que admite varios conmutadores y proporciona conectividad continua a sus enlaces de datos. Cuando un conmutador falla, la agregación sigue proporcionando la conectividad a sus enlaces de datos con el resto de los conmutadores. Este tipo de agregación de enlaces no requiere configuración de conmutador. La agregación DLMP también se puede crear en un solo conmutador.
agregaciones de rutas múltiples de enlaces de datos	Consulte agregación DLMP .
algoritmo de hash seguro	Consulte SHA-1 .
almacén de claves	La ubicación en el disco o una tarjeta en el que se almacenan las claves criptográficas.
anillos de la NIC	En las NIC, los anillos de recepción (Rx) y los anillos de transmisión (Tx) son recursos de hardware mediante los que el sistema recibe y envía paquetes de red, respectivamente.
anuncio de enrutador	Proceso en el que los enrutadores anuncian su presencia junto con otros parámetros de enlace e Internet, de manera periódica o como respuesta a un mensaje de solicitud de enrutador.
anuncio de vecinos	Respuesta a mensaje de solicitud de vecino o proceso de un nodo que envía anuncios de vecino no solicitados para anunciar un cambio de dirección de capa de enlace.
ARP	(Address Resolution Protocol, protocolo de resolución de direcciones) Un protocolo que proporciona asignación dinámica entre las direcciones IP y

	las direcciones Ethernet. ARP sólo se utiliza con redes IPv4. Las redes IPv6 utilizan el protocolo ND (Neighbor Discovery) para convertir direcciones de protocolo. Para obtener más información, consulte RFC 826 (http://tools.ietf.org/html/rfc826) .
asociación de identidad	Consulte IA .
asociación de seguridad	Consulte SA .
ataque de denegación de servicio	Ataque en el que los paquetes de red entrantes superan un servidor de manera intencionada o involuntariamente. El rendimiento de un servidor puede verse significativamente afectado o el servidor puede verse sobrecargado o no operativo.
ataque smurf	El proceso de creación de interrupciones o congestiones graves de la red mediante el uso de paquetes de solicitud de ICMP echo dirigidos a una o varias direcciones de difusión desde ubicaciones remotas.
autenticación	El acto de verificar la identidad suministrada a través de la red por un usuario o una entidad remota, como un programa.
autoconfiguración sin estado	Proceso mediante el cual un host genera sus propias direcciones IPv6 combinando su dirección MAC y un prefijo de IPv6 anunciado por un enrutador IPv6 local.
autoridad de certificación	Consulte CA .
autoridad de números asignados de Internet	Consulte IANA .
base de datos de asociaciones de seguridad	Consulte SADB .
base de datos de políticas de seguridad	Consulte SPD .
BGP	(Border Gateway Protocol, puerta de enlace de borde) Un protocolo que intercambia información de enrutamiento entre sistemas autónomos. Para obtener más información, consulte RFC 4271 (http://www.ietf.org/rfc/rfc4271.txt) .

Blowfish	Algoritmo cifrado de bloques simétricos con una clave de tamaño variable que va de 32 a 448 bits. Bruce Schneier, su creador, afirma que Blowfish se optimiza en el caso de aplicaciones en que la clave se modifica con poca frecuencia.
BOOTP	(Internet Bootstrap Protocol, protocolo de inicio de Internet) Un protocolo que utiliza un cliente de red para obtener una dirección IP de un servidor.
CA	(autoridad de certificación) Una organización o compañía de terceros de confianza que emite certificados digitales. Los certificados digitales se utilizan para crear firmas digitales y pares de claves pública-privada. La autoridad de certificación garantiza la identidad de la persona a la que se concede el certificado digital exclusivo.
calidad de servicio IP	Consulte IPQoS .
capa de conexión segura	Consulte SSL .
carga de seguridad encapsuladora	Consulte ESP .
carga útil	Los datos que se transportan en un paquete. La carga útil no incluye la información de encabezado que se necesita para que el paquete llegue a su destino.
CBCP	(Callback Control Protocol, protocolo de control de devolución de llamadas) Una extensión PPP de Microsoft que se utiliza para negociar una sesión de devolución. Solaris PPP 4.0 sólo admite la parte del cliente (emisor de la llamada inicial) de este protocolo.
CCP	(Compression Control Protocol, protocolo de control de compresión) Un subprotocolo de PPP que negocia el uso de compresión de datos en el enlace. A diferencia de la compresión de encabezado, CCP comprime todos los datos de los paquetes que se envían en el enlace.
CHAP	(Challenge Handshake Authentication Protocol, protocolo de autenticación por reconocimiento de demanda) Un protocolo de autenticación que se puede utilizar para verificar la identidad de un emisor de llamada en un enlace PPP. La autenticación CHAP utiliza la noción de <i>demanda y respuesta</i> , por lo que el equipo que recibe una llamada demanda al emisor de la llamada que demuestre su identidad. Consulte también protocolo de autenticación de contraseña .

clave de privacidad equivalente a cable	Consulte clave WEP .
clave WEP	(wired equivalent privacy key, clave de privacidad equivalente a cable) Una clave que establece conexiones con una red inalámbrica segura.
cliente	Los conmutadores virtuales de un conmutador virtual elástico se agrupan de forma lógica. Cada grupo lógico se denomina un cliente. Los recursos definidos de un conmutador virtual elástico dentro de un cliente no son visibles fuera del espacio de nombre de ese cliente. El cliente actúa como contenedor de todos los recursos del contenido de forma conjunta.
cliente EVS	Un componente EVS desde el que puede gestionar conmutadores virtuales elásticos.
código de autenticación de mensajes basados en hash	Consulte HMAC .
comportamiento por salto	Consulte PHB .
confidencialidad directa perfecta	Consulte PFS .
configuración automática de IPv6	Proceso mediante el cual un host configura automáticamente su dirección IPv6 a partir del prefijo del sitio y la dirección MAC local.
conmutador virtual	Una entidad que facilita la comunicación entre máquinas virtuales. El conmutador virtual genera bucles de tráfico entre máquinas virtuales dentro de la máquina física y no envía este tráfico a través de cables. Los conmutadores virtuales pueden ser gestionados mediante EVS y se instancian automáticamente cuando se crean las VNIC.
conmutador virtual elástico	Consulte EVS .
contabilidad ampliada	Una manera flexible de registrar el consumo de recursos por tareas o procesos.

contabilidad de flujos	Un proceso de recopilación y registro de información relativa a los flujos de tráfico en IPQoS. La contabilidad de flujos se puede establecer definiendo los parámetros del módulo <code>flowacct</code> en el archivo de configuración de IPQoS.
control de flujo basado en prioridades	Consulte PFC .
Controlador EVS	El componente EVS que mantiene la configuración y el estado de los conmutadores virtuales elásticos en varios nodos.
criptografía de clave simétrica	Sistema de cifrado en que el emisor y el receptor de un mensaje comparten una sola clave común. Esa clave común se emplea para cifrar y descifrar el mensaje. estándar de cifrado avanzado es un ejemplo de una clave simétrica.
criptografía de claves asimétricas	Sistema de cifrado en el que el emisor y el receptor de un mensaje emplean claves distintas para cifrar y descifrar dicho mensaje. Las claves asimétricas se usan para establecer un canal seguro de cifrado simétrico de claves. protocolo de Diffie-Hellman es un ejemplo de protocolo de claves asimétricas.
criptografía por clave pública	Un algoritmo criptográfico que requiere dos claves diferentes enlazadas matemáticamente. La clave pública está disponible en general. La clave privada sólo la conoce el destinatario del mensaje. La criptografía de clave pública también es conocida como criptografía asimétrica.
CRL	(certificate revocation list, lista de revocación de certificados) Una lista de certificados de claves públicas revocados por una CA. Estas listas se almacenan en la base de datos de CRL que se mantiene con IKE.
CSU	(channel service unit, unidad de servicio de canal) Un dispositivo de telecomunicaciones síncrono que proporciona una interfaz local a una línea de telecomunicaciones arrendada y termina la línea. En los Estados Unidos, una CSU termina una línea T1 y proporciona una interfaz DS1 o DSX. Internacionalmente, la CSU suele ser propiedad de la compañía telefónica proveedora.
DCB	(puente de centro de datos) Tecnología L2 que se utiliza para gestionar el ancho de banda, la prioridad relativa y el control de flujo de varios tipos de tráfico que comparten el mismo enlace de red, por ejemplo, al compartir un enlace de datos entre los protocolos de red y almacenamiento.
DCBX	(Data Center Bridging Exchange Protocol, protocolo de intercambio del puente de centro de datos) Un protocolo que permite la comunicación entre los hosts para intercambiar información de configuración acerca de las funciones de puente de centro de datos.

DES	(Data Encryption Standard, estándar de cifrado de datos) Un método de cifrado de datos en bloques de 64 bits de clave simétrica estandarizado mediante ANSI, como ANSI X.3.92. DES utiliza una clave de 56 bits.
descubrimiento de enrutadores	Proceso de los hosts que buscan enrutadores residentes en un enlace conectado.
descubrimiento de vecinos	Mecanismo de IP que permite a los hosts encontrar otros hosts que residen en un enlace conectado.
detección de errores	Proceso en el que se detecta que deja de funcionar una interfaz o la ruta de una interfaz a un dispositivo de capa de Internet. Rutas múltiples de red IP (IPMP, IP Network Multipathing) y rutas múltiples de enlaces de datos (DLMP) incluyen dos tipos de detección de fallos: basada en enlaces (predeterminada) y basada en sondeos (opcional).
detección de reparaciones	Proceso en el que se detecta si una tarjeta de interfaz de red o la ruta de dicha tarjeta a un dispositivo de capa 3 comienza a funcionar correctamente después de un fallo.
DHCP	(Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host) Un protocolo que permite la configuración automática de red de los hosts de una red TCP/IP mediante un mecanismo de cliente-servidor. Este protocolo permite que los hosts de una red TCP/IP soliciten y sean asignados direcciones IP, y, además, que detecten información sobre la red a la cual están conectados. Para obtener más información sobre DHCP para IPv4, consulte RFC 2131 (https://www.ietf.org/rfc/rfc2131.txt) and DHCP for IPv6, see RFC 3315 (http://www.ietf.org/rfc/rfc3315.txt) .
difusión	En redes, es un método que se utiliza para transmitir paquetes de forma simultánea a todos los equipos de una subred, excepto el remitente. Los paquetes de difusión por lo general no son enviados más allá de la subred.
dirección de datos	Dirección IP que puede utilizarse como dirección de origen o destino de datos. Las direcciones de datos forman parte de un grupo IPMP y se pueden usar para enviar y recibir tráfico en cualquier interfaz del grupo. Además, el conjunto de direcciones de datos de un grupo IPMP se puede utilizar continuamente siempre que funcione una interfaz en el grupo.
dirección de difusión IPv4	Una dirección de red IPv4 cuya parte principal del host de la dirección es de bits de todo cero (10.50.0.0) o todo uno (10.50.255.255). Un paquete que se envía a una dirección de difusión desde un equipo de la red local se distribuye a todos los equipos de dicha red.
dirección de difusión por proximidad	Dirección IPv6 que se asigna a un grupo de interfaces, generalmente pertenecientes a nodos distintos. El paquete que se envía a una dirección de difusión por proximidad se dirige a la interfaz más próxima que contenga

	dicha dirección. La ruta del paquete se atiene a la medición de distancia del protocolo de enrutamiento.
dirección de multidifusión	Una dirección IPv4 o IPv6 que identifica un grupo de interfaces. Un paquete enviado a una dirección multidifusión se distribuye a todas las interfaces del grupo.
dirección de prueba	Dirección IP en un grupo IPMP que debe usarse como dirección de origen o destino de sondas; no debe emplearse como dirección de origen o destino para tráfico de datos.
dirección de unidifusión	Dirección IPv6 que identifica una sola interfaz de un nodo compatible con IPv6. Una dirección de unidifusión se compone de prefijo de sitio, ID de subred e ID de interfaz.
dirección de uso local	Dirección de unidifusión que sólo tiene un ámbito de enrutamiento local (dentro de una subred o una red de suscriptores). Esta dirección puede tener también un ámbito de exclusividad local o global.
dirección DEPRECATED	Dirección IP que no sirve como dirección de origen de datos que están en un grupo IPMP. En general, las direcciones de prueba IPMP son del tipo DEPRECATED. Ahora bien, cualquier dirección se puede marcar como DEPRECATED para impedir que pueda utilizarse como dirección de origen.
Dirección IP virtual	Consulte VRIP .
dirección local de enlace	Designación que se usa para asignar una dirección a un solo enlace para, por ejemplo, la configuración automática de direcciones en IPv6. De forma predeterminada, la dirección local de enlace se crea a partir de la dirección MAC del sistema.
dirección MAC	(Media Access Control address, dirección de control de acceso a medios) Una dirección exclusiva que se asigna a una interfaz de red. La dirección MAC se utiliza para la comunicación en el segmento de red física.
dirección privada	Dirección IP que no se puede enrutar por Internet. Las redes internas utilizan las direcciones privadas en los host que no necesitan conexión con Internet. Para obtener más información acerca de las direcciones privadas IPv4, consulte RFC 1918 (https://tools.ietf.org/html/rfc1918) . Para obtener más información acerca de las direcciones privadas IPv6, consulte RFC 4193 (http://www.ietf.org/rfc/rfc4193.txt) .
Dirección URL	(localizador de recursos uniformes) Una cadena de caracteres que identifica un recurso en Internet o una intranet privada.
dispositivo LAN virtual	Consulte dispositivo VLAN .

dispositivo VLAN	(virtual LAN device, dispositivo LAN virtual) Interfaces de red que proporcionan reenvío de tráfico en el nivel de Ethernet (enlace de datos) del protocolo de pila IP.
DMA	(direct memory access, acceso directo a la memoria) Algunos dispositivos pueden realizar transferencias de datos que implican a la memoria principal y otros dispositivos sin la ayuda de la CPU. Este tipo de transferencia de datos se conoce como acceso directo a la memoria (DMA).
DMZ	(demilitarized zone, zona desmilitarizada) Una red aislada que se configura para evitar el acceso público a una red privada de la organización. La red aislada normalmente puede contener los recursos que una compañía ofrece al público, como servidores web, servidores FTP anónimos y bases de datos.
DN	(distinguished name, nombre distintivo) Método estandarizado para usar cadenas comunes que representan información compartida. DN se utiliza en tecnologías como LDAP y certificados X.509.
DNS	(domain name system, sistema de nombre de dominio) Un servicio que proporciona las directivas y los mecanismos de nomenclatura para la asignación de dominio y los nombres del equipo para direcciones fuera de la empresa, como las de Internet. DNS es el servicio de información de la red utilizado por Internet. Para obtener más información, consulte RFC 1034 (http://tools.ietf.org/html/rfc1034) .
DOI	(domain of interpretation, dominio de interpretación) El dominio de interpretación define los formatos de los datos, los tipos de intercambio de tráfico de red y las convenciones de denominación de información relacionada con la seguridad. Ejemplos de información relacionada con la seguridad son los algoritmos y modos criptográficos, y las directrices de seguridad.
dominio de interpretación	Consulte DOI .
DR	(dynamic reconfiguration, reconfiguración dinámica) Una función del sistema operativo que se utiliza para volver a configurar el hardware del sistema mientras el sistema se está ejecutando. Con la DR, es posible agregar recursos de hardware o reemplazarlos con poca o sin interrupción para los sistemas operativos normales. No todas las plataformas de Sun de Oracle admiten DR. Es posible que algunas plataformas sólo admitan DR de determinados tipos de hardware, como NIC.
DSCP	(DS codepoint, punto de código DS) Valor de 6 bits que se incluye en el campo de servicios diferenciados (DS) del encabezado de un paquete. DSCP indica la forma en que se debe reenviar un paquete. Para obtener más información, consulte RFC 2474 (https://www.ietf.org/rfc/rfc2474.txt) .

DSR	(direct server return, retorno de servidor directo) Un modo que permite al equilibrador de carga integrado equilibrar las solicitudes entrantes a los servidores back-end, pero permite que el tráfico vuelva de los servidores a los clientes eludiendo al equilibrador de carga.
DSU	(data service unit, unidad de servicio de datos) Un dispositivo de telecomunicaciones síncrono que se utiliza en un enlace PPP de línea arrendada. El dispositivo DSU convierte formatos de estructura de datos utilizados en líneas de telecomunicaciones y proporciona una interfaz de datos de comunicaciones estándar.
DUID	(DHCP unique identifier, indentificador único de DHCP) Un identificador que se utiliza para identificar el sistema cliente en un sistema activado para DHCPv6.
ECMP	(equal-cost multi-path, rutas múltiples de igual costo) Técnica de enrutamiento para enrutar paquetes a lo largo de varias rutas de igual costo. El motor de envío identifica las rutas a través del siguiente salto. Al reenviar un paquete, el enrutador debe decidir el salto siguiente (la ruta) que desea utilizar. Para obtener más información, consulte RFC 2992 (http://tools.ietf.org/html/rfc2992) .
emisores de llamadas de confianza	En PPP, los pares remotos a los cuales un servidor de marcación de entrada concede acceso incluyendo las credenciales de seguridad de los pares en las bases de datos de los secretos de CHAP o PAP del servidor.
encabezado	Consulte encabezado IP .
encabezado de autenticación	Encabezado de extensión que proporciona autenticación e integridad, sin confidencialidad, a datagramas IP.
encabezado de paquete	Consulte encabezado IP .
encabezado IP	Datos que identifican de forma exclusiva un paquete de Internet. El encabezado contiene direcciones de origen y destino del paquete. Una opción dentro del encabezado permite agregar más bytes. El encabezado IPv4 contiene 20 bytes de datos y el encabezado de IPv6 contiene 40 bytes de datos.
encapsulado	Cuando el paquete se transfiere a través de la pila de protocolo de red, los protocolos de cada capa agregan o eliminan campos del encabezado básico. Cuando un protocolo del host de envío agrega datos al encabezado del paquete, el proceso se denomina encapsulado de datos.
encapsulado mínimo	Forma opcional de túnel de IPv4 en IPv4 válida para agentes internos, externos y nodos móviles. El encapsulado mínimo presenta 8 o 12 bytes menos de estructura general que IP en encapsulado IP.

enlace PPP de línea arrendada	Conexión PPP que implica un host y un CSU/DSU conectados a un medio de red síncrona arrendado de un proveedor. El portador óptico 3 (OC3) y el portador T (T1) son ejemplos comunes de medios de línea arrendada. Si bien son más fáciles de administrar, los enlaces de líneas arrendadas son más costosos que los enlaces PPP por marcación telefónica y, por lo tanto, son menos comunes.
enlace PPP por marcación telefónica	Una conexión PPP que afecta a un par y un módem al final de una línea telefónica o un medio de comunicación similar, como un medio proporcionado por RDSI. El término “marcación” hace referencia a la secuencia en la negociación del enlace cuando el módem local llama al par remoto mediante el número de teléfono del par. El enlace por marcación telefónica es la configuración PPP más común y menos costosa.
ENM	(external network modifier, modificador de red externo) Un perfil que se crea para aplicaciones externas a la configuración de red reactiva, pero que puede cambiar y modificar una configuración de red. Los ENM proporcionan la capacidad para especificar cuándo las aplicaciones o las secuencias de comandos (por ejemplo, de una aplicación VPN) deben realizar su propia configuración de red externa a la configuración especificada en el NCP y los perfiles de ubicación.
enrutador	Un sistema que tiene más de una interfaz, ejecuta protocolos de enrutamiento y reenvía paquetes de datos entre las redes de los equipos. Los enrutadores dirigen el tráfico en Internet y conectan dos o más líneas de datos de redes diferentes. Un enrutador reenvía un paquete de datos de un enrutador a otro a través de la red hasta que el paquete llega a su destino.
enrutador de respaldo	Una instancia de VRRP para un VRID que está activo, pero no en el estado maestro, se denomina enrutador de copia de seguridad. Puede existir cualquier cantidad de enrutadores de copia de seguridad para un VRID. Un enrutador de copia de seguridad asume el rol de enrutador maestro si falla el enrutador maestro actual.
enrutador maestro	Una instancia de VRRP que realiza la función de enrutamiento para el enrutador virtual en un momento determinado. Únicamente hay un enrutador maestro activo a la vez para un VRID determinado. El enrutador maestro controla las direcciones IPv4 o IPv6 que están asociadas con el enrutador virtual. El enrutador virtual reenvía los paquetes que se envían a la dirección IP del enrutador maestro.
enrutamiento asimétrico	Se produce cuando se transfiere un paquete desde un origen a un destino en una ruta, pero toma una ruta diferente al volver al origen. Normalmente, se observa en las redes enrutadas de la capa 3 (capa de red).
enrutamiento dinámico	Un tipo de enrutamiento en el que el sistema actualiza automáticamente la tabla de enrutamiento mediante protocolos de enrutamiento, como RIP

	para redes IPv4 y RIPng para redes IPv6. Es mejor utilizar el enrutamiento dinámico en redes de gran tamaño con muchos hosts.
enrutamiento estático	Un proceso en el que el administrador de red del sistema puede agregar rutas manualmente a la ruta de enrutamiento.
equilibrador de carga integrado	Consulte ILB .
equipo de marcación de salida	Es el par que inicia la llamada para establecer un enlace PPO por marcación telefónica. Una vez configurado, el equipo de marcación de salida puede invocar cualquier número de servidores de marcación de entrada. El equipo de marcación de salida, por lo general, proporciona credenciales de autenticación antes de que pueda establecerse el enlace por marcación telefónica.
ESP	(encapsulating security payload, carga de seguridad encapsuladora) Un encabezado de extensión que brinda integridad, confiabilidad y protección contra repeticiones para datagramas IP.
ESSID	(extended service set identifier, identificador de conjunto de servicios extendidos) Un marcador o identificador que sirve como identificación y dirección para un equipo o dispositivo de red para que se conecte y tenga acceso a Internet. Es un nombre de identificación subyacente de una red inalámbrica 802.11b.
estándar de cifrado avanzado	Consulte AES .
estándar de cifrado de datos	Consulte DES .
estándar de cifrado de datos triple	Consulte 3DES .
estructura de gestión de claves de Oracle Solaris	Consulte KMF .
Ethernet	Un sistema que se utiliza para conectar un número de sistemas informáticos para formar una red de área local. Puede utilizar protocolos para controlar la transferencia de información y para evitar la transmisión simultánea por parte de dos o más sistemas.

etherstub	Una NIC pseudo Ethernet que se configura en la capa de enlace de datos (L2) de la pila de red de Oracle Solaris. Permite crear tarjetas de interfaz virtual sobre etherstubs, en lugar de enlaces físicos, para construir una red virtual privada aislada de otras redes virtuales en el sistema, así como de la red externa.
ETS	(enhanced transmission selection, selección de transmisión mejorada) Una función de DCB que asigna el ancho de banda a las aplicaciones según la prioridad de DCB.
EVB	(Edge Virtual Bridging, puente virtual perimetral) Una tecnología L2 que permite a los hosts intercambiar información de enlace virtual con un conmutador externo. EVB descarga la aplicación de los SLA de tráfico en el conmutador.
EVS	(elastic virtual switch, conmutador virtual elástico) Conmutador virtual de software en Oracle Solaris que brinda la capacidad de abarcar varios servidores, por lo que proporciona conectividad de red entre los equipos virtuales con varios servidores conectados al conmutador virtual elástico.
expansión de carga	Proceso de distribuir tráfico de entrada o salida en un conjunto de interfaces. Como consecuencia de la expansión de carga, se obtiene un mayor rendimiento. La expansión de carga sólo se produce cuando el tráfico de red fluye hacia varios destinos que utilizan múltiples conexiones. Las dos clases de expansión de carga son la expansión de carga de entrada, para tráfico de entrada, y de salida, para tráfico de salida.
expect-send	Un formato de secuencia de comandos que se utiliza en secuencias de comandos de chat PPP y UUCP. La secuencia de comandos de chat comienza con el texto o la instrucción <i>expect</i> desde el par remoto. La siguiente línea contiene la respuesta que se <i>enviará</i> (<i>sent</i>) desde el host local después de que reciba la cadena <i>expect</i> correcta desde el par. Las líneas siguientes repiten las instrucciones <i>expect-send</i> entre el host local y el par hasta que todas las instrucciones necesarias para establecer comunicaciones se negocien correctamente.
FDT	(failure detection time, tiempo de detección de fallos) La cantidad de tiempo necesaria para detectar si una interfaz o la ruta de una interfaz a un dispositivo de capa de Internet ya no funciona.
filtro	Conjunto de reglas que establecen las características de una clase en el archivo de configuración de IPQoS. El sistema IPQoS selecciona para procesar cualquier flujo de tráfico de datos que se adecue a los filtros de su archivo de configuración de IPQoS. Consulte filtro de paquetes .
filtro de paquetes	Función de firewall que se puede configurar para permitir o denegar el paso de determinados paquetes a través de un firewall.

filtro de paquetes con estado	Un filtro de paquetes que puede supervisar el estado de las conexiones activas y recurrir a la información obtenida para establecer los paquetes de red que podrán pasar a través del firewall . Al efectuar el seguimiento y relacionar solicitudes y respuestas, un filtro de paquetes con estado puede detectar respuestas que no coincidan con una consulta.
filtro de paquetes dinámico	También conocido como filtro de paquetes con estado .
firewall	Hardware o software que aísla la intranet o red de una organización particular de Internet, con lo cual queda protegida de intrusiones externas. Un firewall puede abarcar filtrado de paquetes, servidores proxy y NAT.
firma digital	Código digital que se vincula con un mensaje transmitido electrónicamente y que identifica al remitente de forma exclusiva.
flujo	Una forma personalizada de categorizar los paquetes para controlar aún más la manera en que se utilizan los recursos para procesar paquetes de red.
FMRI	(fault management resource identifier, identificador de recurso de gestión de fallos) Un identificador para cada paquete de software en Oracle Solaris. FMRI incluye el editor del paquetes, el nombre del paquete y la versión del paquete de software.
función física	Consulte PF .
función virtual	Consulte VF .
gestión de claves	La gestión de claves criptográficas. Esta gestión incluye la generación, el intercambio, el almacenamiento, el uso y el reemplazo de claves en el nivel del usuario, entre usuarios o sistemas.
gestor de coordinación de reconfiguración	Consulte RCM .
GLDv3	(Generic LAN Driver version 3, controlador LAN genérico versión 3) La estructura GLDv3 es una interfaz basada en llamadas de función de complementos MAC y rutinas de servicio y estructuras del controlador MAC. La estructura GLDv3 implementa los puntos de entrada STREAMS necesarios en nombre de los controladores compatibles con GLDv3 y gestiona la compatibilidad con DLPI.
grupo de difusión por proximidad	Grupo de interfaces que tienen la misma dirección de dirección por proximidad IPv6. La implementación de IPv6 en Oracle Solaris no permite crear direcciones ni grupos de difusión por proximidad. Sin embargo, los

nodos IPv6 de Oracle Solaris pueden enviar tráfico a grupos de difusión por proximidad.

grupo IPMP	Un grupo con múltiples rutas IP consiste en una serie de interfaces de red con un conjunto de direcciones de datos que el sistema trata como intercambiables para mejorar la disponibilidad y utilización de la red. El grupo IPMP, incluidas todas sus direcciones de datos e interfaces IP subyacentes, lo representa una interfaz IPMP.
GVRP	(General Attribute Registration Protocol, protocolo de registro de atributo general) Un protocolo utilizado por un sistema cliente para registrar automáticamente los identificadores de VLAN con conmutadores conectados.
HMAC	(hash-based message authentication code, código de autenticación de mensajes basados en hash) Un método de hashing por clave para autenticar mensajes. HMAC es un algoritmo de autenticación de claves secreto que se utiliza junto a una función de hash criptográfica iterativa, como por ejemplo MD5 o SHA-1, en combinación con una clave secreta compartida. La capacidad criptográfica de HMAC depende de las propiedades de la función de hash subyacente.
host multired	Sistema con más de una interfaz y que no reenvía paquetes. Un host multired puede ejecutar protocolos de enrutamiento.
IA	(identity association, asociación de identidad) El método utilizado por un servidor y un cliente para identificar, agrupar y gestionar un conjunto de direcciones IPv6 relacionadas.
IAID	(identity association identifier, identificador de identidad de asociación) Un identificador que se utiliza para identificar la interfaz del sistema cliente en un sistema activado para DHCPv6.
IANA	(Internet Assigned Numbers Authority, autoridad de números asignados de Internet) Una organización que delega las direcciones IP registradas a los registros de Internet de todo el mundo
ICMP	(Internet Control Message Protocol, protocolo de mensajes de control de Internet) Un protocolo que informa errores e intercambia mensajes de control. Es útil para diagnosticar problemas de red.
ID de enrutador virtual	Consulte VRID .
ID de segmento VXLAN	Consulte también VNI .

identificador de asociación de identidad	Consulte IAID .
identificador de conjunto de servicios extendidos	Consulte ESSID .
identificador de recursos de gestión de errores	Consulte FMRI .
identificador de red virtual	Consulte VNI .
identificador de VLAN de puerto	Consulte PVID .
Identificador único de DHCP	Consulte DUID .
IKE	(Internet key exchange, intercambio de claves de Internet) IKE automatiza el suministro de material de claves autenticadas para las asociaciones de seguridad (SA) de IPsec.
ILB	(integrated load balancer, equilibrador de carga integrado) Una tecnología de L3 y L4 que permite que un sistema distribuya la carga de procesamiento de red mediante los recursos disponibles. El ILB se puede utilizar para mejorar la confiabilidad y escalabilidad, y para minimizar el tiempo de respuesta de los servicios de red.
indicador de recursos uniforme	Consulte URI .
índice de parámetros de seguridad	Consulte SPI .
InfiniBand	Una tecnología de E/S basada en tejidos conmutados. Proporciona gran ancho de banda, baja latencia de interconexión para conectar dispositivos de E/S en hosts y para comunicación de host a host. InfiniBand se utiliza en centros de datos empresariales y de computación de alto rendimiento.

infraestructura de clave pública	Consulte PKI .
instancia de estación virtual	Consulte VSI .
intercambio de claves de Internet	Consulte IKE .
interconexión rápida de componentes periféricos	Consulte PCIe .
interfaz en espera	Interfaz física que se emplea para transportar tráfico de datos sólo si otra interfaz física haya sufrido algún problema.
interfaz física	Conexión de un sistema con un enlace. Esta conexión se suele implementar como un controlador de dispositivos además de una NIC. Algunas tarjetas de interfaz de red pueden presentar varios puntos de conexión, por ejemplo, iGb.
IP en encapsulado IP	Mecanismo para encapsular paquetes IP dentro de paquetes IP. Consulte encapsulado .
IPCP	(Internet Protocol Control Protocol, protocolo de control de protocolo de Internet) Un subprotocolo de PPP que negocia las direcciones IP de los pares en el enlace. IPCP también negocia la compresión de encabezado para el enlace y permite el uso de los protocolos de capa de red.
IPMP	(IP Multipathing, rutas múltiples de IP) Una tecnología de capa 3 (L3) que garantiza el acceso continuo por parte de un sistema a la red. Con IPMP, puede configurar varias interfaces IP en un grupo IPMP.
IPnet	Un bloque de direcciones IPv4 o IPv6 que están asociadas a un conmutador virtual elástico. El bloque de direcciones IPv4 o IPv6 existe en la misma subred con un enrutador predeterminado para el bloque y se utiliza con la función de conmutador virtual elástico de Oracle Solaris.
IPQoS	(IP Quality of Service, calidad de servicio IP) Función de software que permite la implementación del estándar modelo DiffServ , además de contabilidad de flujo y marcación 802.1D para LAN virtuales. Con IPQoS, se pueden proporcionar diferentes niveles de servicios de red a clientes y aplicaciones.

IPsec	(IP security, seguridad IP) La arquitectura de seguridad que proporciona protección para las comunicaciones IP mediante la autenticación y el cifrado de paquetes IP.
IPv4	(Internet Protocol, version 4, protocolo de Internet, versión 4) Una versión del protocolo de Internet que admite un espacio de dirección de 32 bits. IPv4 en ocasiones se denomina simplemente IP. Para obtener más información, consulte RFC 791 (http://www.ietf.org/rfc/rfc791.txt) .
IPv6	(Internet Protocol, version 6, protocolo de Internet, versión 6) Una versión de protocolo de Internet que admite espacio de direcciones de 128 bits. Para obtener más información, consulte RFC 2460 (http://www.ietf.org/rfc/rfc2460.txt) .
IR	(Internet registry, registro de internet) Un registro que contiene la información de registro de los números de Internet que incluyen direcciones IP y números de sistema autónomo (SA)
ISAKMP	(Internet Security Association and Key Management Protocol, protocolo de gestión de claves y asociaciones de seguridad de Internet) Estructura habitual para establecer el formato de los atributos SA, así como para negociar, modificar y suprimir SA. ISAKMP es el estándar IETF para gestionar un intercambio IKE.
KMF	(Oracle Solaris Key Management Framework, estructura de gestión de claves de Oracle Solaris) Una estructura que proporciona herramientas e interfaces de programación para gestionar objetos de clave pública que incluyen certificados X.509 y pares de claves públicas o privadas. KMF también proporciona una herramienta para administrar políticas que definen el uso de certificados X. 509 por parte de las aplicaciones.
LACP	(Link Aggregation Control Protocol, protocolo de control de agregación de enlaces) Estándar IEEE 802.3ad para intercambiar dinámicamente información de configuración de red entre sistemas en un grupo de agregación de enlaces. Este protocolo ayuda a configurar automáticamente y mantener grupos de agregación de enlaces.
LCP	(Link Control Protocol, protocolo de control de enlace) Un subprotocolo de PPP que se utiliza para negociar el conjunto inicial de parámetros de enlace entre los pares. LCP comprueba la identidad del dispositivo enlazado, busca errores en la configuración de enlace y determina el tamaño aceptable del paquete para la transmisión.
LDAP	(Lightweight Directory Access Protocol, protocolo de acceso a directorios ligero) Un protocolo cliente-servidor que se utiliza para gestionar información de directorios a través de una red IP. LDAP activa un único punto de gestión para el almacenamiento, la recuperación y la distribución de la información. LDAP permite a los clientes y servidores que utilicen

	los servicios de nombres LDAP comunicarse entre sí. Para obtener más información, consulte RFC 4511 (https://tools.ietf.org/rfc/rfc4511.txt) .
lista de revocación de certificados	Consulte CRL .
LLDP	(Link Layer Discovery Protocol, protocolo de descubrimiento de capa de enlace) Protocolo de capa de enlace que permite a los dispositivos de red anunciar sus capacidades, su identidad y el estado actual a otros dispositivos de red en una red de área local (LAN) IEEE 802.
localizador de recursos uniformes	Consulte Dirección URL .
marcador	<ol style="list-style-type: none">1. Módulo de la arquitectura DiffServ e IPQoS que marca el campo DS de un paquete IP con un valor que indica la forma en que se reenvía el paquete. En la implementación de IPQoS, el módulo marker es <code>dscpmk</code>.2. Módulo de la implementación de IPQoS que marca la etiqueta de LAN virtual de un datagrama de Ethernet con un valor de prioridad de usuario. El valor de prioridad de usuario indica la forma en que los datagramas deben reenviarse en una red con dispositivos VLAN. Este módulo se denomina <code>dlcosmk</code>.
MD5	Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales.
medidor	Módulo de la arquitectura DiffServ que mide la velocidad del flujo de tráfico de una determinada clase. La implementación de IPQoS presenta dos medidores, <code>tokenmt</code> y <code>tswtclmt</code> .
Microsoft CHAP	Consulte MS-CHAP .
modelo de interconexión de sistemas abiertos	Consulte modelo OSI .
modelo DiffServ	Estándar de arquitectura de Internet Engineering Task Force para implementar distintas clases de servicios en redes IP. En una red IP, el modelo diffserv proporciona un mecanismo simple y escalable para clasificar y gestionar el tráfico de red y proporcionar IPQoS. Los módulos principales son clasificador, medidor, marcador, programador y descartador. IPQoS implementa los módulos clasificador, medidor y marcador. Para obtener más información, consulte RFC 2475 (http://www.ietf.org/rfc/rfc2475.txt) .

modelo OSI	(Open Systems Interconnection model, modelo de interconexión de sistemas abiertos) Un modelo estándar diseñado por la Organización Internacional para la Estandarización (ISO) que describe cómo se deben transmitir los datos a través de una red.
modificador de red externo	Consulte ENM .
modo de configuración de red fijo	Un modo de configuración de red en que las instancias de una configuración del sistema son permanentes, independientemente de si se producen cambios en las condiciones de red. Cuando se producen los cambios, como la agregación de interfaces, debe volver a configurar la red para que el sistema se adapte al entorno nuevo.
modo de configuración de red reactivo	Un modo de configuración de red en el que el sistema se adapta automáticamente a cualquier cambio en las condiciones de la red sin necesidad de reconfiguración manual.
MS-CHAP	(Microsoft CHAP) Un protocolo de autenticación para PPP de Microsoft. Solaris PPP 4.0 admite las versiones 1 y 2 de este protocolo en el modo de cliente y de servidor.
MTU	(maximum transmission unit, unidad de transmisión máxima) El tamaño de la unidad de datos más grande, en octetos, que puede transmitirse a través de un enlace.
multidifusión	Un procedimiento de capa de red que se utiliza para enviar paquetes de datagramas en varios equipos en una red IP. A diferencia de enrutamiento de difusión, los paquetes no se manejan por cada equipo. La multidifusión requiere que los enrutadores estén configurados con protocolos de enrutamiento específicos, como el protocolo de enrutamiento de multidifusión (DVMRP). Para obtener más información sobre DVMRP, consulte RFC 1075 (http://tools.ietf.org/rfc/rfc1075.txt) .
NAT	(network address translation, traducción de direcciones de red) Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red. Se utiliza para limitar la cantidad de direcciones IP globales que se necesitan.
NCP	(network configuration profile, perfil de configuración de red) Los perfiles que gestionan la configuración de red del sistema en Oracle Solaris. Sólo puede haber un NCP activo en un sistema a la vez.
NCP DefaultFixed	El único NCP fijo del sistema en el que la configuración de red se instancia, pero no se supervisa.
NCU	(network configuration unit, unidad de configuración de red) Objeto de configuración individual que contiene todas las propiedades que define

	un NCP. Cada NCU representa un enlace físico o una interfaz, y contiene propiedades que definen la configuración de ese enlace o interfaz.
NFS	(Network File System, sistema de archivos de red) Un protocolo de sistema de archivos que se utiliza para acceder de manera remota a los archivos compartidos en una red.
NIC	(network interface card, tarjeta de interfaz de red) Una tarjeta de adaptador de red que conecta un equipo a una red. Algunas tarjetas de interfaz de red pueden tener varias interfaces físicas, por ejemplo la tarjeta igb.
NIS	(network information service, servicio de información de la red) Una base de datos de red distribuida que contiene información clave sobre los sistemas y los usuarios de la red.
nodo	En una red de equipos, un nodo es un punto de conexión o un punto final para la transmisión de los datos.
nodo EVS	Un host cuyas VNIC se conectan a un conmutador virtual elástico.
nombre del almacén de claves	El nombre que el administrador asigna a un almacén de claves. En la estructura criptográfica, el nombre del almacén de claves también es conocido como "token" o "ID de token".
nombre distintivo	Consulte DN .
NTP	(Network Time Protocol, protocolo de hora de red) Un protocolo que se utiliza para definir y mantener la hora del sistema. El software NTP se implementa como el daemon ntpd, que es una implementación completa de la versión 4 estándar, como se define en RFC 5905 (https://tools.ietf.org/html/rfc5905) .
PAP	(password authentication protocol, protocolo de autenticación de contraseña) Un protocolo de autenticación que se puede utilizar para verificar la identidad de un emisor de llamada en un enlace PPP. PAP utiliza una contraseña no cifrada que se transfiere al enlace, lo que hace posible almacenar la contraseña en uno de los equipos de punto final. Por ejemplo, PAP puede utilizar las entradas de inicio de sesión y contraseña en la base de datos de UNIX passwd del equipo que recibe una llamada para verificar la identidad del emisor de la llamada.
paquete	Grupo de información que se transmite como una unidad a través de líneas de comunicación. Contiene un encabezado IP y una carga útil .
paquete icmp echo request	Paquete que se envía a un sistema en Internet para solicitar una respuesta. Esos paquetes son conocidos comúnmente como paquetes "ping" y se utilizan para probar el alcance de los hosts en una red IP.

PCIe	(peripheral component interconnect express, interconexión de componentes periféricos rápida) Un bus de E/S en serie que conecta un equipo con sus periféricos.
perfiles de configuración de red	Consulte NCP .
PF	(physical function, función física) Una función PCI que admite funcionalidades SR-IOV definidas en la especificación de SR-IOV. Una función física contiene la estructura de funcionalidad SR-IOV y se utiliza para gestionar la funcionalidad de SR-IOV. Las funciones físicas son funciones PCIe completas que se pueden detectar, gestionar y manipular como cualquier otro dispositivo PCIe. Las funciones físicas tienen recursos de configuración completos y se pueden utilizar para configurar o controlar el dispositivo PCIe.
PFC	(priority-based flow control, control de flujo basado en prioridades) Mecanismo de control de flujo del nivel del enlace de datos. El PFC amplía trama PAUSE estándar para que se incluyan los valores de clase de servicio (CoS) de IEEE 802.1p. En PFC, el tráfico es pausado de manera selectiva sólo para los valores de CoS activados en la trama PFC, en lugar de detener todo el tráfico del enlace de datos.
PFS	(perfect forward secrecy, confidencialidad directa perfecta) En PFS, la clave que se emplea para proteger la transmisión de datos no se aplica en la derivación de claves adicionales. La fuente de la clave que se usa para proteger la transmisión de datos tampoco se emplea en la derivación de claves adicionales. PFS se aplica para el intercambio de claves autenticadas en IKE.
PHB	(per-hop behavior, comportamiento por salto) Prioridad que se asigna a una clase de tráfico de un paquete al atravesar un salto.
pila doble	Una pila de protocolo TCP/IP que permite que los protocolos IPv4 e IPv6 operen en la misma infraestructura de red sin el uso de un mecanismo de colocación en túneles. La red de Oracle Solaris es una pila doble. Esta técnica de pila doble es compatible en hosts y enrutadores.
PKI	(public key infrastructure, infraestructura de clave pública) Sistema de certificados digitales, autoridades de certificación y otras autoridades de registro que verifican y autentican la validez de cada parte que interviene en una transacción por Internet.
PPP	(Point-to-Point Protocol, protocolo punto a punto) Un protocolo de capa de enlace de datos que proporciona un método estándar para transferir datagramas por medios punto a punto. Una configuración PPP consta de dos equipos de punto final llamados <i>iguales</i> y las líneas telefónicas u otro enlace

	<p>bidireccional que los pares utilicen para las comunicaciones. La conexión de software y hardware entre los dos pares se considera el <i>enlace PPP</i>.</p> <p>PPP se compone de un número de subprotocolos, incluidos PAP, CHAP, LCP y CCP.</p>
PPP a través de Ethernet	Consulte PPPoE .
PPP asíncrono	Una forma de PPP en líneas de serie asíncronas, que transfieren datos un carácter a la vez. La forma más común de configuración de PPP, el enlace por marcación telefónica, utiliza comunicaciones PPP asíncronas.
PPP síncrono	Una forma de PPP que se ejecuta en líneas digitales síncronas, que transfieren datos como un flujo continuo de bits básicos. Un enlace de línea arrendada PPP utiliza PPP síncrono.
PPPoE	(PPP over Ethernet, PPP a través de Ethernet) Un protocolo que permite a los hosts ejecutar sesiones de PPP sobre un enlace Ethernet. PPPoE se suele utilizar con los servicios de línea de suscripción digital (DSL).
prioridad de usuario	Valor de 3 bits que implementa marcas de clase de servicio (CoS). CoS define la forma en que los datagramas de Ethernet se reenvían en una red de dispositivos VLAN.
producto de retraso de ancho de banda	Determina la cantidad de datos enviados a través de la red. Estos datos son el producto del ancho de banda disponible en la red y la latencia de conexión o el tiempo de ida y vuelta
programa de copia de UNIX a UNIX	Consulte UUCP .
protocolo de acceso a directorios ligero	Consulte LDAP .
protocolo de aplicación inalámbrica	Consulte WAP .
protocolo de árbol de expansión	Consulte STP .
protocolo de autenticación de contraseña	Consulte PAP .

protocolo de autenticación por desafío mutuo	Consulte CHAP .
protocolo de configuración dinámica de host	Consulte DHCP .
protocolo de configuración y detección de VSI	Consulte VDP .
protocolo de control de agregación de enlaces	Consulte LACP .
protocolo de control de compresión	Consulte CCP .
protocolo de control de devolución de llamadas	Consulte CBCP .
protocolo de control de enlaces	Consulte LCP .
protocolo de control de protocolo de internet	Consulte IPCP .
protocolo de control versión 6 de protocolo de Internet	Consulte IPCP .
protocolo de datagramas de usuario	Consulte UDP .

protocolo de descubrimiento de capa de enlace	Consulte LLDP .
protocolo de Diffie-Hellman	Un protocolo de claves criptográficas asimétricas que permite a dos usuarios intercambiar una clave secreta mediante un medio de comunicación no seguro, sin información previa. Las claves criptográficas asimétricas son la base de la criptografía de clave pública.
protocolo de gestión de claves y asociaciones de seguridad de Internet	Consulte ISAKMP .
protocolo de hora de precisión	Consulte PTP .
protocolo de hora de red	Consulte NTP .
protocolo de información de enrutamiento	Consulte RIP .
protocolo de información de enrutamiento de próxima generación	Consulte RIPng .
protocolo de inicio de Internet	Consulte BOOTP .
protocolo de intercambio del puente de centro de datos	Consulte DCBX .
protocolo de Internet	Protocolo con el cual se envían datos de un sistema a otro por Internet.

protocolo de Internet, versión 4	Consulte IPv4 .
protocolo de Internet, versión 6	Consulte IPv6 .
protocolo de redundancia de enrutador virtual	Consulte VRRP .
protocolo de registro VLAN GARP	Consulte GVRP .
protocolo de resolución de direcciones	Consulte ARP .
protocolo de resolución de direcciones inverso	Consulte RARP .
protocolo de transporte de control del flujo	Consulte SCTP .
protocolo punto a punto	Consulte PPP .
protocolo simple de administración de red	Consulte SNMP .
protocolo trivial de transferencia de archivos	Consulte TFTP .
proxy SSL en el nivel del núcleo	El proxy configurable se ejecuta en el núcleo para acelerar las comunicaciones del servidor web que están protegidas por la capa de conexión segura (SSL).

PTP	(Precision Time Protocol, Protocolo de hora de precisión) Un protocolo IEEE que se utiliza para sincronizar el reloj del sistema en varios sistemas, en un dominio de difusión. El software PTP se implementa como el daemon <code>ptpd</code> , que es una implementación de la versión de PTP 2 como se define en el estándar IEEE 1588-2008.
puente de centro de datos	Consulte DCB .
puente virtual perimetral	Consulte EVB .
puerta de enlace de borde	Consulte BGP .
puerto de enlace superior	Un enlace de datos mediante la que se crean las VNIC, cuando utiliza la función EVS de Oracle Solaris.
puerto virtual	El punto de conexión entre la VNIC y un conmutador virtual elástico. Un puerto virtual encapsula diferentes parámetros de configuración de red que es heredado por la VNIC cuando se conecta al puerto virtual.
punto de código DS	Consulte DSCP .
PVID	(port VLAN identifier, identificador de VLAN de puerto) El ID de VLAN predeterminado que se asume para paquetes sin etiquetas enviados desde un enlace y recibidos de éste.
RARP	(Reverse Address Resolution Protocol, protocolo de resolución de direcciones inverso) Un protocolo que asigna de forma dinámica entre direcciones protocolo de Internet (IP) y Ethernet. RARP se utiliza para resolver direcciones MAC en direcciones IP en la red de área local. Para obtener más información, consulte RFC 903 (http://tools.ietf.org/rfc/rfc903.txt) .
RCM	(reconfiguration coordination manager, gestor de coordinación de reconfiguración) Una estructura que gestiona la eliminación dinámica de los componentes del sistema y ayuda a registrar y liberar recursos del sistema de forma ordenada.
reconfiguración dinámica	Consulte DR .
recurso anet	Una VNIC que se configura automáticamente para todas las zonas de Oracle Solaris de forma predeterminada. Consulte también VNIC .

red de área local virtual	Consulte VLAN .
red de área local virtual extensible	Consulte VXLAN .
red privada virtual	Una red virtual que está aislada de otras redes virtuales que están en el sistema y de la red externa. Las redes virtuales privadas se configuran mediante etherstubs.
red privada virtual	Consulte VPN .
red virtual	Una red que emula una red física y es una combinación de recursos de red de hardware y software.
redireccionar	En un enrutador, proceso para informar a un host sobre un primer salto más apropiado para llegar a un determinado destino.
registro de Internet	Consulte IR .
repetición de ataque	Un ataque de red en el que un intruso captura un paquete durante la transmisión de datos. El paquete capturado es reemplazado por un paquete fraudulento o repetido más tarde. Para protegerse contra tales ataques, un paquete puede contener un campo que se incrementa durante la vida útil de la clave secreta que protege el paquete.
resultado	En IPQoS, acción que se realiza como consecuencia de la medición del tráfico. Los medidores de IPQoS tienen tres resultados: rojo, amarillo y verde. En el archivo de configuración de IPQoS, puede definir los resultados.
retorno de servidor directo	Consulte DSR .
retransmisión reflectante	Una función en EVB que proporciona una opción para enviar el tráfico entre máquinas virtuales en el cable, para que sea enviado a un bucle de retorno por la red externa. Esto le permite pasar de gigabit Ethernet (GbE) a 10 GbE virtualizados, preservando las políticas de TI en conmutadores externos.
RIP	(Routing Information Protocol, protocolo de información de enrutamiento) Un protocolo de puerta de enlace interno que enruta paquetes IPv4 y mantiene la tabla de enrutamiento de todos los hosts en la LAN. Para obtener más información, consulte RFC 2453 (https://tools.ietf.org/html/rfc2453) .
RIPng	(Routing Information Protocol next generation, protocolo de información de enrutamiento de próxima generación) Un protocolo de puerta de enlace

	interno que enruta paquetes IPv6 y mantiene la tabla de enrutamiento de todos los hosts en la LAN. Para obtener más información, consulte RFC 2080 (http://tools.ietf.org/rfc/rfc2080.txt) .
RSA	Método para la obtención de firmas digitales y criptosistemas de claves públicas.
rutas múltiples de igual costo	Consulte ECMP .
rutas múltiples de IP	Consulte IPMP .
SA	(security association, asociación de seguridad) Asociación que establece las propiedades de seguridad entre un primer host y un segundo host.
SADB	(security associations database, base de datos de asociaciones de seguridad) Una tabla de asociaciones de seguridad que especifica claves criptográficas y algoritmos criptográficos. Las claves y los algoritmos se utilizan en la transmisión segura de datos.
salto	Medida que se usa para identificar la cantidad de enrutadores que hay entre dos hosts o sistemas. Si un origen y un destino están separados por tres enrutadores, los sistemas están a una distancia de cuatro saltos.
SCTP	(Stream Control Transport Protocol, protocolo de transporte de control del flujo) Protocolo de capas de transporte que brinda comunicaciones relativas a las conexiones de manera parecida a TCP. Además, SCTP permite varias direcciones permanentes, en que uno de los puntos finales de la conexión puede tener más de una dirección IP. Para obtener más información, consulte RFC 4960 (http://tools.ietf.org/html/rfc4960) .
secreto de CHAP	Una serie ASCII o cadena binaria que se utiliza para fines de identificación y es conocida por ambos pares en un enlace PPP. El secreto de CHAP se almacena como texto sin cifrar en un archivo <code>/etc/ppp/chap-secrets</code> del sistema, pero nunca se envía a través del enlace PPP, ni siquiera en formato cifrado. El protocolo CHAP verifica que un hash del secreto de CHAP utilizado por un emisor de llamada coincida con un hash de la entrada del secreto de CHAP del emisor de la llamada en el archivo <code>/etc/ppp/chap-secrets</code> del destinatario.
secuencia de comandos de chat	Instrucciones que le indican a un módem la forma de establecer un enlace de comunicaciones entre en sí mismo y un par remoto. Tanto los protocolos PPP como los UUCP emplean secuencias de comandos de chat para establecer los enlaces por marcación telefónica y las llamadas de respuesta.

seguridad IP	Consulte IPsec .
selección de transmisión mejorada	Consulte ETS .
selector	En IPQoS, elemento que define los criterios de aplicación en los paquetes de una determinada clase, a fin de seleccionar ese tráfico en el flujo de datos de la red. Los selectores se definen en la cláusula de filtro en el archivo de configuración de IPQoS.
servicio de información de la red	Consulte NIS .
servidor de marcación de entrada	El par que negocia y establece el destinatario final de un enlace por marcación telefónica después de recibir una llamada de un equipo de marcación de salida. Aunque suele utilizarse el término “servidor de marcación de entrada”, el servidor de marcación de entrada no funciona de acuerdo con el paradigma cliente-servidor. En su lugar, simplemente es el par que responde a la solicitud para configurar un enlace por marcación telefónica. Después de que se ha configurado, un servidor de marcación de entrada puede recibir llamadas de cualquier cantidad de equipos de marcación de salida.
servidor proxy	Un servidor intermedio entre un cliente y otro servidor. Proporciona servicio de caché, control administrativo y seguridad. Por ejemplo, un servidor proxy se puede utilizar para impedir el acceso a determinados sitios web.
SHA-1	(Secure Hashing Algorithm, algoritmo de hash seguro) Un algoritmo que opera en cualquier longitud de entrada menor que 2^{64} para producir un resumen del mensaje. El algoritmo SHA-1 es la entrada de DSA.
Siglas inglesas de Internet Control Message Protocol (protocolo de mensajes de control de Internet)	Consulte ICMP .
sistema autónomo	Un dominio de enrutamiento único que se utiliza para administrar la topología de red de los sitios que contienen varios enrutadores y redes. Este dominio de enrutamiento es un grupo conectado de uno o más prefijos IP y tiene una política de enrutamiento única y claramente definida. Para obtener más información, consulte RFC 1930 (http://tools.ietf.org/html/rfc1930).

sistema de archivos de red	Consulte NFS .
sistema de nombre de dominio	Consulte DNS .
SMF	(service management facility, utilidad de gestión de servicio) Función que define las relaciones entre las aplicaciones o los servicios, por lo que los servicios dependientes se pueden reiniciar automáticamente cuando es necesario.
sniff	Acceso no autorizado a redes de equipos; con frecuencia se usa como parte de programas automatizados para tamizar información, por ejemplo, contraseñas de texto no cifrado, de última hora.
SNMP	(Simple Network Management Protocol, protocolo simple de administración de redes) Un protocolo que proporciona una forma habitual de consulta, supervisión y gestión de los dispositivos conectados a redes IP.
solicitud de enrutador	Proceso de los hosts que solicitan enrutadores para la generación inmediata de anuncios de enrutador, en lugar de hacerlo la próxima vez que se hubiera programado.
solicitud de vecino	Solicitud enviada por un nodo para determinar la dirección de capa de enlace de un vecino. Asimismo, una solicitud de vecino verifica que se pueda contactar con un vecino mediante una dirección de capa de enlace almacenada en caché.
SPD	(security policy database, base de datos de políticas de seguridad) Una base de datos que especifica el nivel de protección que se aplica a un paquete protegido por IPsec. SPD filtra el tráfico IP para determinar si un paquete se debe desechar, enviar en la red o ser protegido con IPsec.
SPI	(security parameter index, índice de parámetros de seguridad) Un número entero que especifica la fila que utiliza un destinatario en SADB para descifrar un paquete recibido.
spoof	Obtener acceso no autorizado a un equipo mediante el envío de un mensaje con una dirección IP indicando que el mensaje procede de un host de confianza. Para efectuar spoofing en IP, el remitente debe recurrir a una serie de técnicas para averiguar la dirección IP de un host de confianza; a continuación, debe modificar los encabezados de paquete para simular que los paquetes provienen de ese host.
SR-IOV	(Single Root I/O Virtualization, virtualización de E/S de raíz única) Un estándar que permite compartir dispositivos de interconexión de componentes periféricos rápida (PCIe) entre máquinas virtuales y que se

	implementa en el hardware. La especificación SR-IOV permite que una máquina virtual se conecte de forma directa al dispositivo de E/S.
SSL	(secure sockets layer, capa de conexión segura) Una forma de cifrado de nivel bajo que es utilizado por protocolos como HTTP y FTP. El protocolo SSL incluye provisiones para la autenticación del servidor, el cifrado de los datos en tránsito y la autenticación de cliente opcional.
STP	(Spanning Tree Protocol, protocolo de árbol de expansión) Un protocolo predeterminado utilizado por las redes con puentes para evitar bucles de red que hacen que las subredes se vuelvan inutilizables.
subred	Una subdivisión lógica de una red IP que conecta los sistemas con números de subred y esquemas de dirección IP, incluidas sus máscaras de red respectivas.
tabla de enrutamiento	Una tabla que contiene la información de enrutamiento para un paquete, que ayuda a determinar la mejor ruta de acceso para que el paquete llegue a destino.
tarjeta de interfaz de red	Consulte NIC .
tarjeta de interfaz de red virtual	Consulte vNIC .
TFTP	(Trivial File Transfer Protocol, protocolo trivial de transferencia de archivos) Un protocolo de transferencia de archivos que se utiliza para transferir archivos entre los servidores de configuración de red y los clientes de red. TFTP se utiliza normalmente para la transferencia automática de configuración o de archivos de inicio entre equipos de una red local. Para obtener más información, consulte RFC 1350 (http://www.ietf.org/rfc/rfc1350.txt) .
tiempo de detección de fallos	Consulte FDT .
traducción de la dirección de red	Consulte NAT .
túnel bidireccional	Túnel capaz de transmitir datagramas IP en ambos sentidos.
UDP	(User Datagram Protocol, protocolo de datagramas de usuario) Un protocolo que utiliza un equipo para enviar datagramas a otros equipos de una red

	IP sin configurar canales de transmisión especiales o rutas de datos. Para obtener más información, consulte RFC 768 (http://www.ietf.org/rfc/rfc768.txt) .
unidad de configuración de red	Consulte NCU .
unidad de servicio de canal	Consulte CSU .
unidad de servicio de datos	Consulte DSU .
unidad de transmisión máxima	Consulte MTU .
URI	(uniform resource indicator, indicador de recursos uniformes) Una tecnología de direcciones que identifica recursos en Internet en una intranet privada.
utilidad de gestión de servicios	Consulte SMF .
UUCP	(UNIX-to-UNIX Copy Program, programa de copia de UNIX a UNIX) Un programa que permite a los equipos transferir archivos e intercambiar los correos con entre sí. UUCP también permite a los equipos participar en redes de gran tamaño, como Usenet.
VDP	(VSI Discovery and Configuration Protocol, protocolo de configuración y detección de VSI) Un protocolo utilizado por EVB para intercambiar información acerca de VSI (interfaces del conmutador virtual).
VF	(virtual function, función virtual) Una función SR-IOV asociada a una función física. Una función virtual es una función PCIe ligera que comparte uno o más recursos físicos con la función física y con otras funciones virtuales que están asociadas a la misma función física. A las funciones virtuales solamente se les permite tener recursos de configuración para sus propios comportamientos.
virtualización de E/S de raíz única	Consulte SR-IOV .
VLAN	(virtual local area network, red de área local virtual) Una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo.

VNI	(virtual network identifier, identificador de red virtual) Las VXLAN son identificadas mediante el uso de ID de segmento VXLAN, también conocidos como VNI. Cada enlace de datos VXLAN está asociado con una VNI.
VNIC	(virtual network interface card, tarjeta de interfaz de red virtual) Una entidad L2 o dispositivo de red virtual que se comporta como una NIC física cuando se configura. Puede configurar una VNIC sobre un enlace de datos subyacente para compartirlo entre múltiples zonas o máquinas virtuales (VM) o conectar una VNIC a un conmutador virtual elástico.
VPN	(virtual private network, red privada virtual) Una sola red lógica y segura que emplea túneles en una red pública como Internet.
VRID	(Virtual Router ID, ID de enrutador virtual) Un número único que se utiliza para identificar un enrutador virtual en un segmento de red determinado. Los VRID identifican el enrutador virtual dentro de una LAN.
VRIP	(Virtual IP Address, dirección IP virtual) Una dirección IP asociada con un VRID del cual otros hosts pueden obtener servicio de red. El VRIP gestiona las instancias del VRRP pertenecientes a un VRID.
VRRP	(Virtual Router Redundancy Protocol, protocolo de redundancia de enrutador virtual) Un protocolo que proporciona una alta disponibilidad de direcciones IP, como las que se utilizan para los enrutadores y equilibradores de carga.
VSI	(virtual station instance, instancia de estación virtual) VSI hace referencia a una VNIC configurada en la estación.
VXLAN	(virtual extensible local area network, red de área local virtual extensible) Una tecnología L2 y L3 que superpone una red de enlace de datos (L2) sobre una red IP (L3). Las direcciones VXLAN abordan la limitación de 4K que se impone al utilizar VLAN. Normalmente, las VXLAN se utilizan en una infraestructura de nube para aislar varias redes virtuales.
WAP	(Wireless Application Protocol, protocolo de aplicación inalámbrica) Un protocolo estándar para acceder a información a través de una red inalámbrica móvil.
zona desmilitarizada	Consulte DMZ .