Un **proxy**, en una [red informática](http://es.wikipedia.org/wiki/Red_inform%C3%A1tica), es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina ***A*** solicita un recurso a una ***C***, lo hará mediante una petición a ***B***; ***C*** entonces no sabrá que la petición procedió originalmente de ***A***. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: proporcionar caché, control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, etc.

Su finalidad más habitual es la de **servidor proxy**, que consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc. Esta función de **servidor proxy** puede ser realizada por un programa o dispositivo.

* El uso más común es el de **servidor proxy**, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.
	+ De ellos, el más famoso es el **servidor proxy web** (comúnmente conocido solamente como «**proxy**»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
	+ También existen proxy para otros protocolos, como el **proxy de FTP**.
	+ El [proxy ARP](http://es.wikipedia.org/wiki/Proxy_ARP) puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.
* [Proxy (patrón de diseño)](http://es.wikipedia.org/wiki/Proxy_%28patr%C3%B3n_de_dise%C3%B1o%29) también es un [patrón de diseño](http://es.wikipedia.org/wiki/Patr%C3%B3n_de_dise%C3%B1o) ([programación](http://es.wikipedia.org/wiki/Programaci%C3%B3n)) con el mismo esquema que el proxy de red.
* Un componente [hardware](http://es.wikipedia.org/wiki/Hardware) también puede actuar como intermediario para otros.

Como se ve, **proxy** tiene un significado muy general, aunque siempre es sinónimo de **intermediario**. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo que la solicitó.

Hay dos tipos de proxys atendiendo a quien es el que quiere implementar la política del proxy:

* **proxy local**: En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).
* **proxy externo**: El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc.

**Ventajas**

En general (no sólo en informática), los proxies hacen posible:

* **Control**: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
* **Ahorro**. Sólo *uno* de los usuarios (el proxy) ha de estar preparado para hacer el trabajo real. Con estar **preparado** queremos decir que es el único que necesita los recursos necesarios para hacer esa funcionalidad. Ejemplos de recursos necesarios para hacer la función pueden ser la capacidad y lógica de cómputo o la dirección de red externa (IP).
* **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer [caché](http://es.wikipedia.org/wiki/Cach%C3%A9): guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
* **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
* **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

**Desventajas**

En general (no sólo en informática), el uso de un intermediario puede provocar:

* **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.
* **Abuso**. Al estar dispuesto a recibir peticiones de muchos [usuarios](http://es.wikipedia.org/wiki/Usuario) y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
* **Carga**. Un proxy ha de hacer el trabajo de *muchos* usuarios.
* **Intromisión**. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de[caché](http://es.wikipedia.org/wiki/Cach%C3%A9) y guarda copias de los datos.
* **Incoherencia**. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los [servidores](http://es.wikipedia.org/wiki/Servidor) proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en caché sigue siendo la misma que la existente en el servidor remoto.
* **Irregularidad**. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como [TCP/IP](http://es.wikipedia.org/wiki/TCP/IP)).

### Proxy SOCKS

[1](http://es.wikipedia.org/wiki/Proxy#cite_note-1) Los proxy [SOCKS](http://es.wikipedia.org/wiki/SOCKS) son muy diferentes de los proxys 'normales'. Cuando por ejemplo usas un proxy [HTTP](http://es.wikipedia.org/wiki/HTTP) lo que éste hace es coger las peticiones HTTP y hace la petición por ti y te devuelve los resultados. Haciendo un símil con la vida real es como si alguien nos pidiera que le pasáramos la sal de la mesa y el proxy la cogiera y nos la diera.

Sin embargo lo que hace el protocolo SOCKS, es casi equivalente a establecer un túnel IP con un [cortafuegos](http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29) y a partir de ahí las peticiones del protocolo son entonces realizadas desde el cortafuegos.

El cliente negocia una conexión con el servidor proxy [SOCKS](http://es.wikipedia.org/wiki/SOCKS) usando el protocolo SOCKS, nivel 5 del modelo OSI (capa de sesión). Una vez establecida la conexión todas la comunicaciones entre el cliente y proxy se realizan usando el protocolo SOCKS. El cliente le dice al proxy SOCKS que es lo que quiere y el proxy se comunica con el servidor externo y obtiene los resultados y se los manda al cliente. De esta forma el servidor externo sólo tiene que estar accesible desde el proxy SOCKS que es el que se va a comunicar con él.

El cliente que se comunica con SOCKS puede estar en la propia aplicación (Ej. [Firefox](http://es.wikipedia.org/wiki/Firefox), [putty](http://es.wikipedia.org/wiki/Putty%22%20%5Co%20%22Putty)), o bien en la pila de protocolos TCP/IP a donde la aplicación enviará los paquetes a un túnel SOCKS.

En el proxy SOCKS es habitual implementar, como en la mayoría de proxys, autenticación y loggeo de las sesiones.

### Proxies transparentes

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración. Una ventaja de tal es que se puede usar para redes de empresa.

Un **proxy transparente** combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP).

### Reverse Proxy / Proxy inverso

Un *reverse proxy* es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

* Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
* Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración [SSL](http://es.wikipedia.org/wiki/Transport_Layer_Security) (Security Sockets Layer).
* Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).
* Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.

### Proxy NAT (Network Address Translation) / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el [NAT](http://es.wikipedia.org/wiki/NAT).

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a [Internet](http://es.wikipedia.org/wiki/Internet). Se dispone de una única [dirección IP](http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP) pública, que tiene que ser compartida. Dentro de la red de área local ([LAN](http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local)) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a [Internet](http://es.wikipedia.org/wiki/Internet). El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los [Cortafuegos](http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29) y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero [encaminador](http://es.wikipedia.org/wiki/Encaminador%22%20%5Co%20%22Encaminador).

### Proxy abierto

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de [spam](http://es.wikipedia.org/wiki/Spam%22%20%5Co%20%22Spam). Un proxy se usa, normalmente, para almacenar y redirigir servicios como el [DNS](http://es.wikipedia.org/wiki/DNS) o la navegación [Web](http://es.wikipedia.org/wiki/Web), mediante el [cacheo](http://es.wikipedia.org/wiki/Cach%C3%A9) de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración "abierta" a todo [internet](http://es.wikipedia.org/wiki/Internet), se convierte en una herramienta para su uso indebido.

Debido a lo anterior, muchos servidores, como los de [IRC](http://es.wikipedia.org/wiki/IRC), o [correo electrónicos](http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico), deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

### Cross-Domain Proxy

Típicamente usado por Tecnologías web asíncronas (flash, ajax, comet, etc) que tienen restricciones para establecer una comunicación entre elementos localizados en distintos dominios.

En el caso de [AJAX](http://es.wikipedia.org/wiki/AJAX), por seguridad sólo se permite acceder al mismo dominio origen de la página web que realiza la petición. Si se necesita acceder a otros servicios localizados en otros dominios, se instala un **Cross-Domain proxy**[2](http://es.wikipedia.org/wiki/Proxy#cite_note-Constituci.C3.B3n-2) en el dominio origen que recibe las peticiones ajax y las reenvia a los dominios externos.

En el caso de flash, también han solucionado creando la revisión de archivos [xml](http://es.wikipedia.org/wiki/Xml%22%20%5Co%20%22Xml) de [Cross-Domain](http://es.wikipedia.org/w/index.php?title=Cross-Domain&action=edit&redlink=1), que permiten o no el acceso a ese dominio o subdominio.

Ejemplos:

<http://freeproxy.en.softonic.com/download>

**Los niveles de las redes VLAN**

Una **VLAN** (acrónimo de *virtual LAN*, «**red de área local virtual**») es un método de crear [redes](http://es.wikipedia.org/wiki/Red_de_computadoras) lógicamente independientes dentro de una misma red física.[1](http://es.wikipedia.org/wiki/VLAN#cite_note-1) Varias VLANs pueden coexistir en un único[conmutador](http://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29) físico o en una única red física. Son útiles para reducir el tamaño del [dominio de difusión](http://es.wikipedia.org/wiki/Dominio_de_difusi%C3%B3n) y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un [enrutador](http://es.wikipedia.org/wiki/Enrutador) o un conmutador de capa 3 y 4.

Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes [segmentos](http://es.wikipedia.org/w/index.php?title=Segmento_de_red&action=edit&redlink=1) de una [red de área local](http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local). Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.



**Clasificación**

Aunque las más habituales son las **VLANs basadas en puertos** (nivel 1), las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen:

* **VLAN de nivel 1 (por puerto)**. También conocida como “port switching”. Se especifica qué puertos del switch pertenencen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que reconfigurar las VLANs si el usuario se mueve físicamente. Es la más común y la que se explica en profundidad en este artículo.
* **VLAN de nivel 2 por direcciones MAC**. Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.
* **VLAN de nivel 2 por tipo de protocolo**. La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX...
* **VLAN de nivel 3 por direcciones de subred (subred virtual)**. La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLANs.
* **VLAN de niveles superiores**. Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico... La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día...

**Protocolos**

Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el [IEEE 802.1Q](http://es.wikipedia.org/wiki/IEEE_802.1Q), [STP](http://es.wikipedia.org/wiki/Spanning_Tree_Protocol) y [VTP](http://es.wikipedia.org/wiki/VTP) (cuyo equivalente IEEE es GVRP). El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que se asociada inmediatamente con la información de la VLAN. El cometido principal de Spanning Tree Protocol (STP) es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos. VTP (VLAN Trunking Protocol) es un protocolo propietario de Cisco que permite una gestión centralizada de todas las VLANs.

El **protocolo de etiquetado IEEE 802.1Q** es el más común para el etiquetado de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el [ISL](http://es.wikipedia.org/wiki/ISL) (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el [VLT](http://es.wikipedia.org/wiki/VLT) (Virtual LAN Trunk) de 3Com. El IEEE 802.1Q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde sólo cambia el valor del campo Ethertype, que en las tramas 802.1Q vale X'8100, y se añaden dos bytes para codificar la prioridad, el CFI y el VLAN ID. Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con bridges y switches sin capacidad de VLAN.

Para evitar el bloqueo de los switches debido a las tormentas broadcast, una red con topología redundante tiene que tener habilitado el **protocolo STP**. Los switches utilizan STP para intercambiar mensajes entre sí (BPDUs, Bridge Protocol Data Units) para lograr de que en cada VLAN sólo haya activo un camino para ir de un nodo a otro.

En los dispositivos Cisco, **VTP (VLAN trunking protocol)** se encarga de mantener la coherencia de la configuración VLAN por toda la red. VTP utiliza tramas de nivel 2 para gestionar la creación, borrado y renombrado de VLANs en una red sincronizando todos los dispositivos entre sí y evitar tener que configurarlos uno a uno. Para eso hay que establecer primero un **dominio de administración VTP**. Un dominio VTP para una red es un conjunto contiguo de switches unidos con enlaces trunk que tienen el mismo nombre de dominio VTP.

Los switches pueden estar en uno de los siguientes modos: servidor, cliente o transparente. El **servidor** es el modo por defecto, anuncia su configuración al resto de equipos y se sincroniza con otros servidores VTP. Un switch **cliente** no puede modificar la configuración VLAN, simplemente sincroniza la configuración en base a la información que le envían los servidores. Por último, un switch está en modo **transparente** cuando sólo se puede configurar localmente pues ignora el contenido de los mensajes VTP.

VTP también permite «podar» (función VTP prunning), lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino. Con lo que se ahorra ancho de banda en los posiblemente saturados enlaces trunk.

**VLAN basadas en el puerto de conexión**

Con las VLAN de nivel 1 (basadas en puertos), el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Habitualmente es el administrador de la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

Los puertos de un switch pueden ser de dos tipos, en lo que respecta a las características VLAN: puertos de acceso y puertos trunk. Un **puerto de acceso** (switchport mode access) pertenece únicamente a una VLAN asignada de forma estática (VLAN nativa). La configuración por defecto suele ser que todos los puertos sean de acceso de la VLAN 1. En cambio, un **puerto trunk** (switchport mode trunk) puede ser miembro de múltiples VLANs. Por defecto es miembro de todas, pero la lista de VLANs permitidas es configurable.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo simplemente sabe que es miembro de una subred y que puede ser capaz de hablar con otros miembros de la subred simplemente enviando información al segmento cableado. El switch es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El switch también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

**Diseño de VLANs**

Actualmente, las redes institucionales y corporativas modernas suelen estar configuradas de forma jerárquica dividiéndose en varios grupos de trabajo. Razones de seguridad y confidencialidad aconsejan también limitar el ámbito del tráfico de difusión para que un usuario no autorizado no pueda acceder a recursos o a información que no le corresponde. Por ejemplo, la red institucional de un campus universitario suele separar los usuarios en tres grupos: alumnos, profesores y administración. Cada uno de estos grupos constituye un dominio de difusión, una VLAN, y se suele corresponder asimismo con una [subred IP](http://es.wikipedia.org/wiki/Subred)diferente. De esta manera la comunicación entre miembros del mismo grupo se puede hacer en nivel 2, y los grupos están aislados entre sí, sólo se pueden comunicar a través de un [router](http://es.wikipedia.org/wiki/Router%22%20%5Co%20%22Router).

La definición de múltiples VLANs y el uso de enlaces trunk, frente a las [redes LAN](http://es.wikipedia.org/wiki/LAN) interconectadas con un router, es una solución escalable. Si se deciden crear nuevos grupos se pueden acomodar fácilmente las nuevas VLANs haciendo una redistribución de los puertos de los switches. Además, la pertenencia de un miembro de la comunidad universitaria a una VLAN es independiente de su ubicación física. E incluso se puede lograr que un equipo pertenezca a varias VLANs (mediante el uso de una tarjeta de red que soporte trunk).



Imagine que la universidad tiene una red con un rango de direcciones IP del tipo 172.16.XXX.0/24, cada VLAN, definida en la capa de enlace de datos (nivel 2 de OSI), se corresponderá con una subred IP distinta: VLAN 10. Administración. Subred IP 172.16.10.0/24 VLAN 20. Profesores. Subred IP 172.16.20.0/24 VLAN 30. Alumnos. Subred IP 172.16.30.0/24

En cada edificio de la universidad hay un switch denominado de acceso, porque a él se conectan directamente los sistemas finales. Los switches de acceso están conectados con enlaces trunk (enlace que transporta tráfico de las tres VLANs) a un switch troncal, de grandes prestaciones, típicamente Gigabit Ethernet o 10-Gigabit Ethernet. Este switch está unido a un router también con un enlace trunk, el router es el encargado de llevar el tráfico de una VLAN a otra.