Principales elementos de una red

En esta parte, definiremos los términos indispensables para una buena comprensión del entorno de red. Mencionaremos las diferencias fundamentales entre las redes organizadas en torno a servidores y las redes que funcionan entre pares. Veremos en qué casos utilizar cada uno de los dos sistemas.

1. Desde la perspectiva del software

a. Principios

El sistema operativo de red es un sistema complejo compuesto por diferentes capas lógicas (protocolos de comunicación, capa de aplicación...). Permite a varias personas interconectadas (físicamente) trabajar con los mismos recursos.

Proporciona un control de acceso a la red (seguridad de conexión, seguridad en el acceso a los recursos) coordinando al mismo tiempo los accesos simultáneos (administra a menudo colas de espera para los dispositivos exclusivos).

b. Definiciones

Desde un punto de vista del software, los ordenadores conectados a una red se dividen en dos categorías en función de las acciones que efectúan sobre esta.

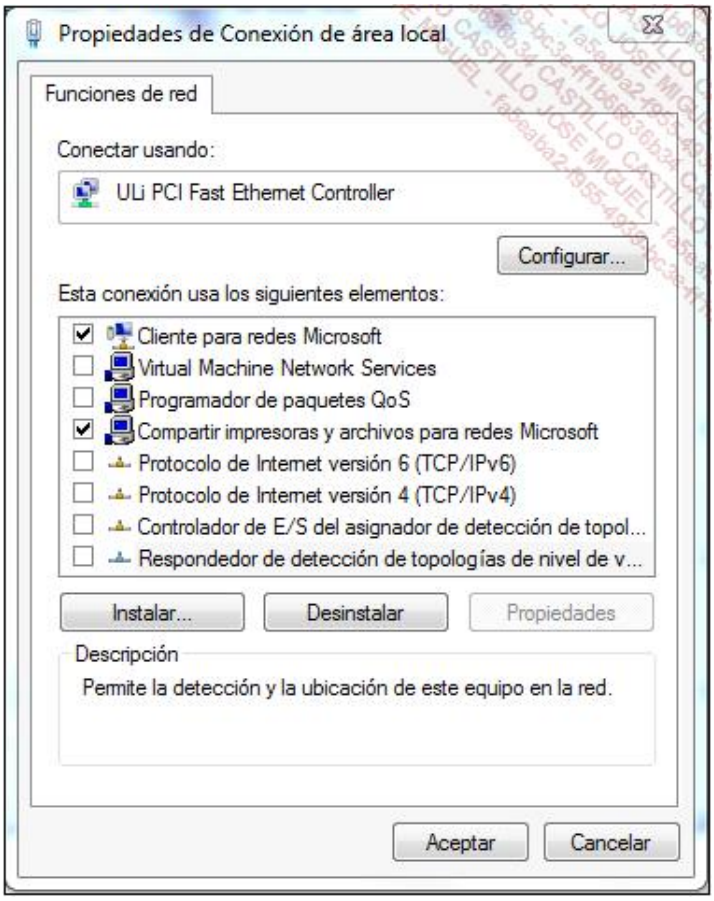
Un *cliente* es el solicitante de servicios. Puede ser, por ejemplo, un puesto de trabajo de usuario que solicita servicios de aplicaciones, de archivos, de impresión...

Estos servicios los ofrece una entidad lógica llamada *servidor*.

Los sistemas operativos de red son capaces de pedir u ofrecer servicios. Por el contrario, su orientación principal es diferente, ya que dan prioridad a una u otra posibilidad. Un puesto de trabajo, que no tiene como objetivo principal ofrecer servicios a la red, dispone un sistema que prioriza el aspecto cliente.

En cambio, un sistema operativo de servidor proporciona servicios más eficientes. Es capaz de soportar hardware más avanzado y administrar capacidades (memoria, espacio en disco) más importantes.

Al evolucionar, los sistemas operativos de red han adquirido cierto número de capacidades complementarias. Por ejemplo, un sistema operativo como Windows ofrece servicios de archivos, de impresión y de alojamiento/distribución de sitios web, sin necesidad de instalar software de terceros. Obviamente, las posibilidades que ofrecen las versiones destinadas a los usuarios finales son bastante más limitadas.



Propiedades de red en un cliente Windows 8.1: las funcionalidades del cliente (Cliente para redes Microsoft) y del servidor (Compartir...) están activadas.

Un servidor puede estar dedicado o no. Si está dedicado, solo puede ofrecer uno de los servicios habituales. Estas configuraciones son ideales. Permiten dimensionar el hardware en función de las necesidades del servicio. Un servidor de archivos dedicado no tendrá necesidad de un microprocesador potente, al contrario que su aplicación. Para una empresa, dedicar los servidores a una u otra tarea es una solución que suele ser costosa, aunque se mejora la eficacia y la administración.

El aumento de las capacidades y de la potencia de los servidores hace además que se puedan simultanear servicios en una máquina física.

La *virtualización* de servidores aporta una respuesta a esta problemática. Estos programas permiten la simulación de varios servidores virtuales en una única plataforma física.

c. El sistema operativo de red

El sistema operativo de red (NOS - *Network Operating System*) o SOR (Sistema Operativo de Red) es el que, a menudo, condiciona la arquitectura de la red.

Como ejemplos de sistemas operativos, se distinguen los sistemas organizados en torno a un servidor y los basados en una arquitectura de puesto a puesto.

Puesto a puesto

Cuando todos los puestos tienen un papel idéntico y son a la vez clientes de los recursos disponibles y servidores, se habla de red de igual a igual, de par a par (*peer-to-peer*), o también de puesto a puesto. En este tipo de

estructura, que en general agrupa pocos puestos, los recursos, las operaciones de seguridad y las tareas de administración se distribuyen en el conjunto de la red. No puede haber un control centralizado. Generalmente, cada usuario es administrador de su propio puesto. Este tipo de organización implica que los usuarios no sean completamente neófitos y puedan trabajar en un entorno correctamente estructurado.

Otro inconveniente es que no se puede centralizar la gestión de los usuarios en una única base de datos de la red; es decir, no se puede controlar el acceso a los recursos en función de los nombres de los usuarios.

En un entorno de ordenadores cuyo sistema operativo es Microsoft Windows 7 u 8 en sus ediciones no profesionales, hablaremos de grupos de trabajo (*workgroup*).

Red centralizada

Cada usuario dispone de un nombre y una contraseña para identificarse, que debe introducir en el momento de la apertura de una sesión de red. También se centraliza la base de datos de los usuarios de la red.

Así es posible controlar el acceso a los recursos utilizando la seguridad a nivel de usuario: es decir, se individualizan los permisos para cada usuario en función de cada uno de los recursos disponibles. De esta manera, es mucho más fácil saber quién hace qué y en qué momento. Se nombra administrador a un usuario específico que tiene por función administrar el conjunto de los recursos de la red. Es el usuario que tiene más poder sobre el conjunto de la red.

Podemos citar MS Windows Server 2008 o 2012 como sistemas operativos de arquitectura centralizada.

Seguridad a nivel de recursos

Hablamos de seguridad a nivel de recursos para hacer hincapié en el hecho de que es en los recursos donde se centra la seguridad. Se asignan las contraseñas para los recursos necesarios independientemente de los usuarios.

En un principio, no es necesario darse a conocer utilizando explícitamente el nombre de usuario y la contraseña. Sin embargo, cuando solicitemos el acceso a un nuevo recurso, será necesario precisar que disponemos de los permisos correspondientes. Productos como Windows 7 u 8 en sus diferentes versiones familiares funcionan bajo esta premisa. Las contraseña asociadas a los recursos se guardan para que el usuario no tenga que introducirlos nuevamente cada vez que accede.

Es decir, asociamos permisos específicos a este recurso compartido para permitir accesos regidos por contraseña (independientemente de los usuarios).

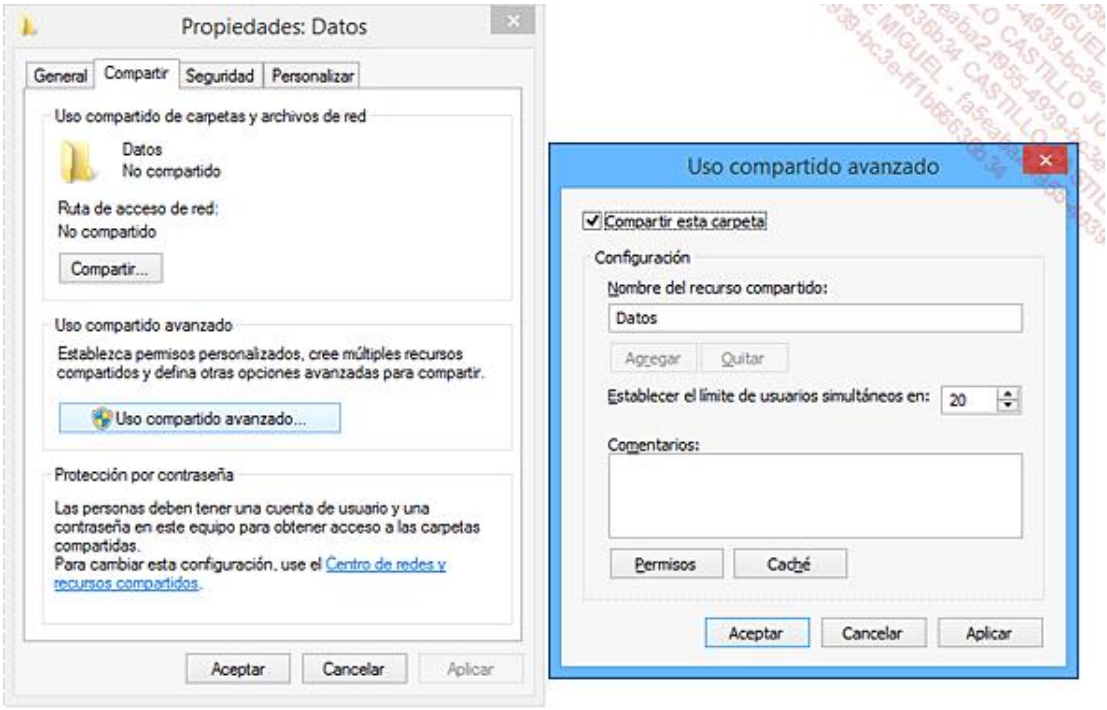
De hecho, si un usuario quiere impedir a otro acceder a su recurso, debe modificar la contraseña e informar al resto de los usuarios (a los que quiera permitir el acceso).

Seguridad a nivel de usuario

La seguridad a nivel de usuario, por el contrario, permite asignar permisos más específicos a cada usuario para un recurso dado. Es necesario que antes cada uno se identifique ante una entidad de referencia.

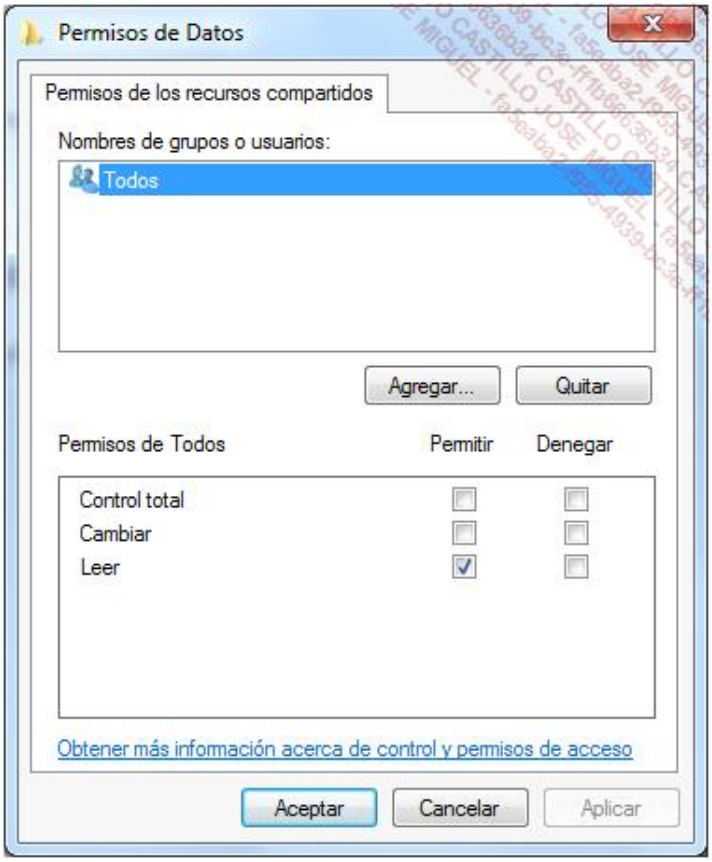
Esta puede ser local (ordenador con Windows 7 u 8) o remota (servidor con una base de datos de usuarios). Es necesario abrir una sesión para autentificarse y así permitir un acceso transparente a los recursos a los cuales el usuario accederá más tarde.

Por ejemplo, para permitir que los usuarios accedan a una carpeta de un sistema Windows, en primer lugar es necesario compartirla.



Compartir una carpeta en Windows

Los permisos de acceso se deben asociar a este recurso compartido en función de las cuentas de usuarios o de su grupo de pertenencia.



Ejemplos de sistemas operativos de red

Los sistemas operativos de red de **Microsoft** están separados en dos familias. Windows 2000 Server (NT5.0) y Windows Server 2003 (NT5.2) son los sucesores de Windows NT4 Server. Para el usuario, Windows 2000 Profesional (NT5.0) y Windows 98 tuvieron como sucesor a Windows XP (NT5.1), en edición familiar o profesional.

La siguiente generación, Windows Vista (núcleo 6.0), ha sido el predecesor de la versión 6.1 del núcleo, con Windows 7 en el puesto de trabajo del usuario.

En el lado del Servidor, encontramos Windows Server 2008 (núcleo 6.0) y Windows Server 2008 R2 (núcleo 6.1).

A continuación, Windows 8 se basa en el núcleo 6.2, igual que Windows Server 2012.

Finalmente, Windows 8.1 y Windows Server 2012 R2 se basan en el núcleo 6.3.

Línea de comandos en Windows 8.1

Los diferentes sistemas de tipo **UNIX** se dedican esencialemente a tareas de servidor. Se pueden citar entre ellos a Sun Solaris, HP-UX, o incluso IBM AIX.

Linux es un sistema operativo muy importante. La versión del núcleo de Linux permite identificar las funcionalidades que se han añadido.

La primera versión estable que se publicó en marzo de 1994 fue la 1.0. Ofrecía todos los servicios clásicos de un sistema UNIX.

La versión 2.0 se publicó en julio de 1996 con mejoras en la gestión de arquitecturas de muchos más modelos de procesadores, más módulos y una gestión más completa de la red.

En enero de 1999, se lanzó la versión 2.2 que implementaba NTFS e IPv6.

Uno de los aportes importantes de la versión 2.4 que apareció en enero de 2001 fue, entre otros, el soporte de USB, PCMCIA y también NFSv3.

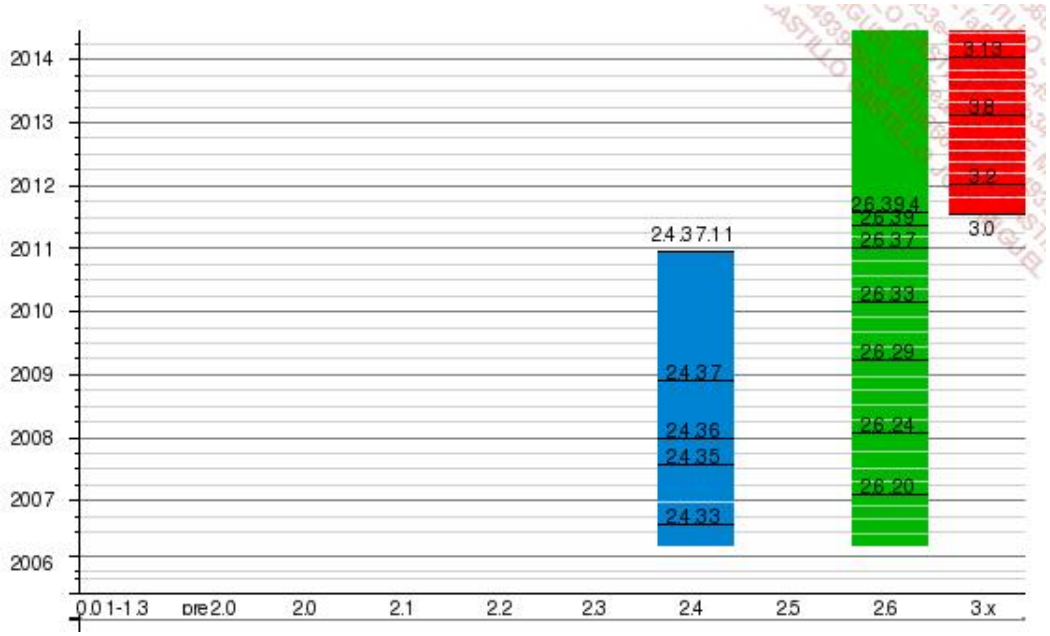
La versión 2.6 se lanzó en diciembre de 2003, y ofreció un verdadero núcleo preemptivo, así como NFSv4.

El soporte de USB 3.0 o la defragmentación en caliente de ext4 han aparecido en la versión 2.6.31 (septiembre de 2009).

En julio de 2011 apareció la versión 3.0 y desde entonces, han visto la luz numerosas versiones, y se ha acelerado el ritmo de las actualizaciones y mejoras.

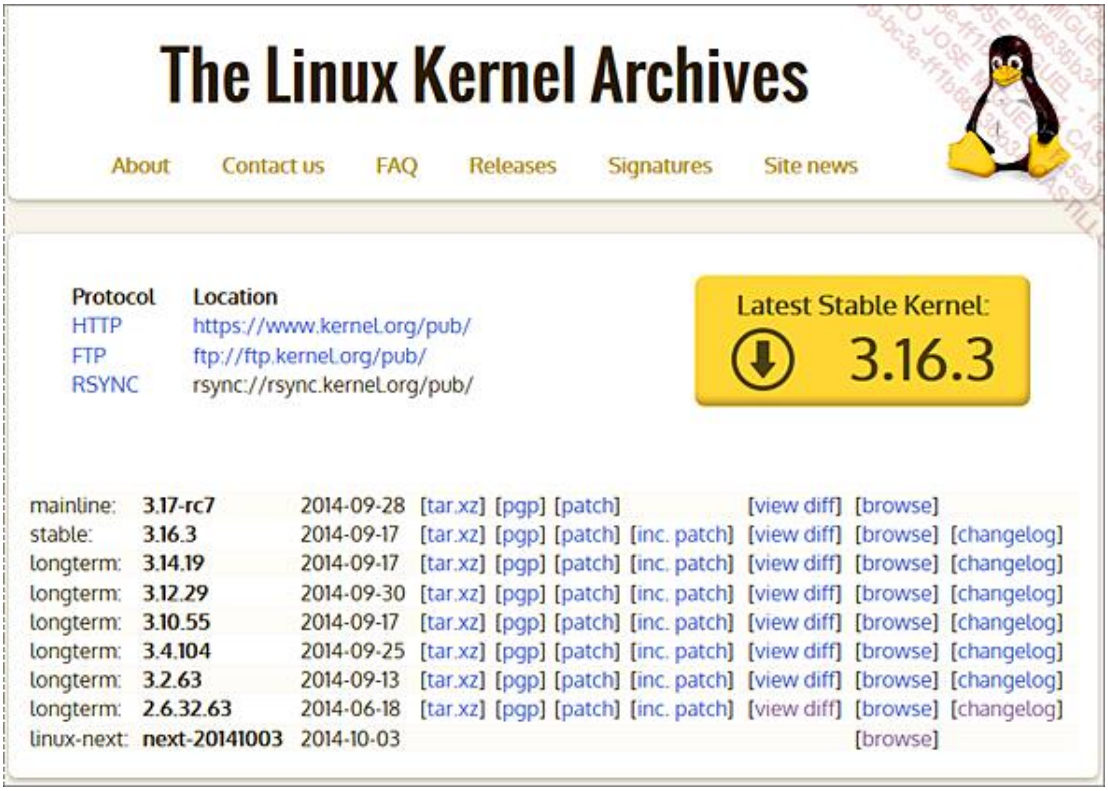
La última versión, 3.16.3, ha aparecido en septiembre de 2014.

El siguiente diagrama representa la evolución de las últimas versiones del núcleo Linux a través de los años.



Evolución de las últimas versiones del núcleo Linux

Observe que, cuando una versión beta se está desarrollando, la segunda cifra del número de versión es impar.



Web de descarga del núcleo de Linux: www.kernel.org

En función de su instalación, Linux puede utilizarse como puesto de trabajo o como servidor.

2. Desde la perspectiva del hardware

a. La interconexión

Para que la comunicación en red sea operativa, en primer lugar es necesario interconectar los equipos entre ellos. Frecuentemente se utiliza una interfaz por cable, como un cable conectado a una tarjeta de red o a un módem. También se puede utilizar la interfaz inalámbrica a través de comunicaciones inalámbricas, que utilizan los infrarrojos, el láser o las ondas de radio.

b. Los protocolos de comunicación

Además del hardware, que garantiza la conectividad y el intercambio de las señales de soporte físico o de ondas, es necesario utilizar normas de comunicación. Estos protocolos permiten dar un sentido a la señal que circula entre las estaciones de trabajo y administrar el acceso al soporte compartido.