

Principales familias de protocolos

Con la aparición de las redes locales, se utilizaron distintos protocolos de capas medias y altas, a menudo vinculados a un editor de programas. Con el tiempo se han ido sustituyendo por el estándar de hecho TCP/IP.

1. IPX/SPX

a. Antecedentes

Históricamente, se ha utilizado esta familia de protocolos con las redes Novell Netware hasta la versión 3.12. TCP/IP ya estaba disponible en esta versión, pero IPX/SPX era absolutamente necesario para asegurar el buen funcionamiento del sistema operativo, además de, en algunas ocasiones, el TCP/IP. Hoy en día casi nadie lo utiliza, incluso aunque a menudo esté configurado en las impresoras de red.

b. Protocolos

Internetwork Packet eXchange (IPX) actúa en las capas de red y transporte. Provee, como IP, un servicio sin conexión ni seguridad.

IPX es enrutable e identifica un equipo a través de una dirección lógica que no requiere, como IP, un plan de direccionamiento estático. Una dirección IPX es la concatenación de un número de red externo, en 4 bytes, y de la dirección MAC del dispositivo, en 6 bytes. La asignación de direcciones IPX es automática y, por añadidura, la resolución de direcciones lógicas en direcciones físicas es instantánea, ya que la dirección física forma parte de la dirección IPX.



Las direcciones IPX se presentan, por ejemplo, de la siguiente manera: 0000CAFE: 00-A0-00-26-37-10, donde 0000CAFE es el número de red lógica en hexadecimal en 4 bytes y 00-A0-00-26-37-10 es la dirección MAC de la tarjeta de red.

En Netware, no se debe confundir el número de red externo (vinculado a los dispositivos) con el número de red interno (vinculado a las aplicaciones). Este último está vinculado a la estructura interna de Novell que asocia las aplicaciones de un servidor a un número de nodo y un número de red. El servidor funciona entonces como un router interno que conmuta la red física (número de red externo) con la red lógica (las aplicaciones del servidor). Así pues, un servidor Novell posee dos direcciones de red, una dirección interna y otra externa.

Como para IP, todos los nodos conectados a la misma red física deben tener el mismo número de red (externo) y cada dirección IPX debe ser única en la red. Del mismo modo, los números de red internos utilizados deben ser únicos.

Una de las particularidades de IPX es la de poder provocar un cortocircuito en el modelo OSI, al dirigirse directamente a la capa 5 del destinatario y no forzosamente a SPX. Los protocolos IP + TCP corresponden a IPX + SPX, mientras que los protocolos IP + UDP corresponden únicamente a IPX.

Sequenced Packet eXchange (SPX) se aplica en la capa Transporte del modelo OSI y garantiza una entrega fiable de los paquetes (orientada a la conexión).

2. NetBIOS

a. Antecedentes

Network Basic Input/Output System (NetBIOS) fue introducido por IBM en 1985, quien lo optimizó para redes pequeñas. Su implementación es sencilla, pero no es enrutable. Introduce nombres NetBIOS para identificar los puestos de la red, sin administrar direcciones lógicas. No existe más que una resolución de nombre en direcciones MAC. Además, es el propio equipo el que administra esta solución enviando una difusión a la red.

b. Principio

La simplicidad de este protocolo y el hecho de que consuma pocos recursos de memoria hace que NetBIOS todavía sea utilizado por los productos de Microsoft, IBM y Novell.

Las *Application Programming Interface* (API) NetBIOS se han desarrollado ampliamente para PC, para permitir una independencia del protocolo subyacente utilizado.

Las fuentes de NetBIOS están disponibles, encapsuladas en tramas LLC (802.2) o encapsuladas en IPX o en TCP/IP.

Muchos de los productos Microsoft todavía funcionan con NetBIOS. Sin embargo, se puede utilizar cualquier otro protocolo de capas 3 y 4, como TCP/IP, IPX/SPX o NetBEUI.

NetBIOS sigue estando presente en los sistemas operativos MS Windows, a través de NBT (*NetBIOS over TCP/IP*).

Hasta la llegada de Windows 2000, los sistemas operativos de Microsoft obligaban a utilizar NetBIOS, en particular por su popular servicio de archivos *Server Message Block* (SMB).



En las versiones Unix/Linux que implementan SaMba (SMB rescrito por Andrew Tridgel), NetBIOS se instala automáticamente en forma de un demonio nmbd.

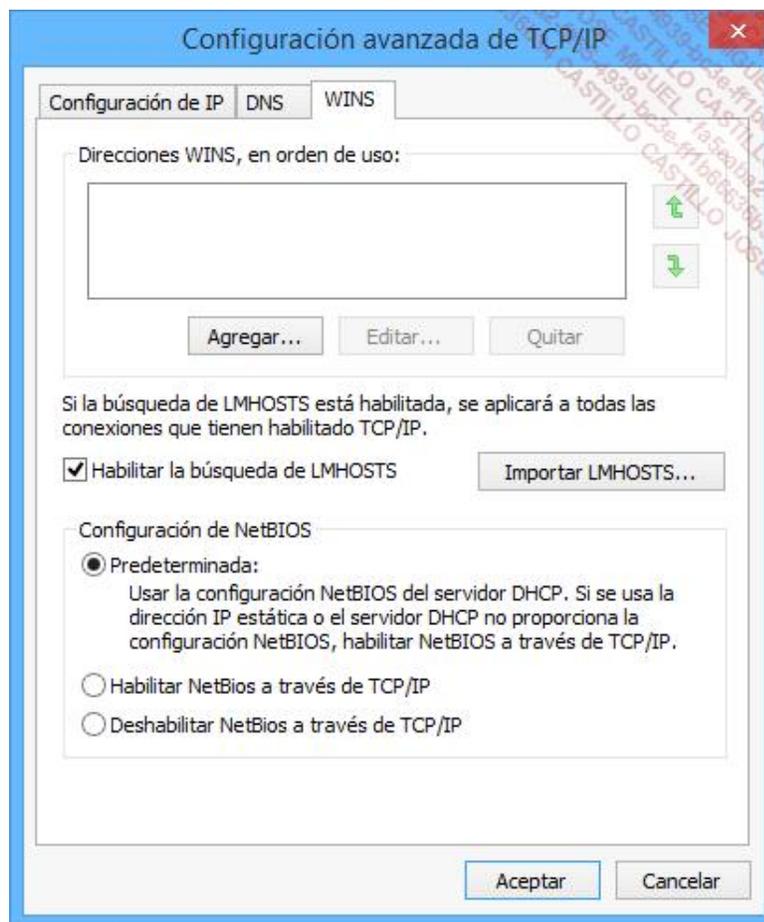
c. Los nombres NetBIOS

Utilización

Una estación de trabajo o un servidor Windows se pueden localizar por su nombre NetBIOS, de 15 caracteres, más un 16.º de identificación del servicio.

Los nombres NetBIOS se resuelven por medio de difusiones, utilizando un archivo local LMHosts o a través de un servidor *Windows Internet Name Service* (WINS).

Utilizar o no NetBIOS con TCP/IP se puede definir en la Configuración avanzada de TCP/IP:



Configuración de la resolución NetBIOS con TCP/IP

- Observe que un ordenador UNIX/Linux no responde nunca a una petición de resolución de nombre NetBIOS por difusión, al contrario de lo que pasa con un ordenador que tiene un sistema operativo de Microsoft.

Constitución

En una red NetBIOS, cada ordenador debe disponer de un nombre único de 15 caracteres como máximo.

Los nombres NetBIOS puede contener todos los caracteres alfanuméricos, además de los siguientes: ! @ # \$ % ^ & () - _ ' { } . ~

- No se pueden utilizar caracteres que se puedan asociar a caracteres genéricos, como el asterisco o la interrogación.

Se aconseja no utilizar espacios en los nombres NetBIOS, aunque algunas aplicaciones los pueden manejar. Así, se puede utilizar el siguiente comando, siempre que se envíen los parámetros entre dobles comillas:

```
Net view "\\EL SERVIDOR"
```

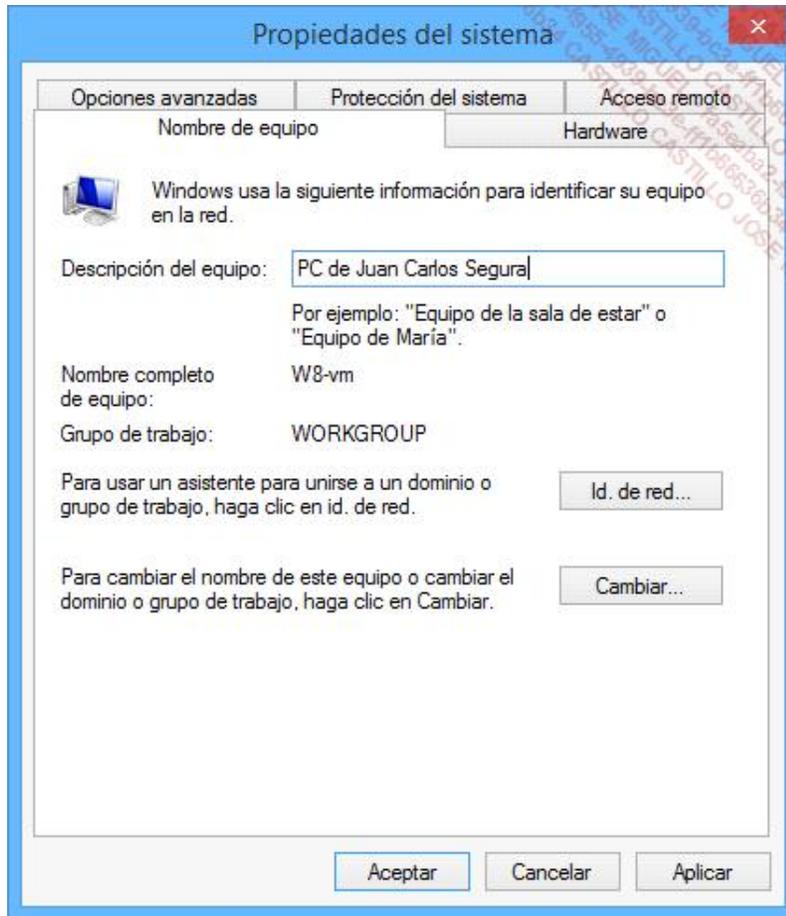
Implementación de una nomenclatura NetBIOS

Es necesario establecer una denominación para cada equipo, del tal modo que facilite su identificación. Por ejemplo, se puede considerar una denominación en función de su ubicación física, de su sistema operativo o del

usuario que trabaja con el equipo.

Configuración de un nombre NetBIOS de ordenador

Es necesario introducir un nombre para el ordenador durante la instalación del sistema operativo. El nombre se puede modificar en cualquier momento, siempre que se tengan permisos.



Nombre completo del ordenador Windows

Este nombre NetBIOS sirve para construir identificadores para las aplicaciones NetBIOS que se ejecutan localmente en el ordenador. Estos nombres son accesibles en un ordenador que disponga de un sistema operativo Windows que ejecute NBT (*NetBIOS over TCP/IP*).

Por ejemplo, a partir de la línea de comando en un ordenador con Windows, obtenemos la siguiente lista de nombres registrados localmente y en remoto en un servidor Windows de red.

```

Administrador: Símbolo del sistema
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Windows\system32>nbtstat -n

Ethernet:
Dirección IP del nodo: [10.0.2.15] Id. de ámbito : []

Tabla de nombres locales NetBIOS

Nombre                Tipo                Estado
-----
W8-UM                 <20>              Único              Registrado
W8-UM                 <00>              Único              Registrado
WORKGROUP             <00>              Grupo              Registrado
WORKGROUP             <1E>              Grupo              Registrado
WORKGROUP             <1D>              Único              Registrado
MSBROWSE              <01>              Grupo              Registrado

C:\Windows\system32>

```

- He aquí algunos identificadores NetBIOS habituales: NombreOrdenador <00> Cliente para redes Microsoft y NombreOrdenador <20> Compartir archivos, impresión Microsoft.

3. TCP/IP

a. Antecedentes

La red ARPANET, nombre de la organización militar *Advanced Research Projects Agency* (ARPA) nació en 1969. La creó el *Department of Defense* (DoD), de EE. UU., para conectar diferentes sitios informatizados y en un primer momento conectó cuatro institutos universitarios. Se conectaron progresivamente una serie de centros militares y de investigación, públicos y privados, que participaron activamente en esta implementación.

A principios de los años setenta, Bob Kahn, del *Defense ARPA* (DARPA), ex-ARPA, trabajó con Vinton Cerf, investigador del Stanford Institute, en nuevos protocolos que permitieran conectar redes. Así nació TCP/IP. En 1976, ARPANET migra a TCP/IP. En 1978, una segunda red se conecta a ARPANET; utiliza las líneas telefónicas y toma el nombre de Internet.

- Hoy en día, ARPANET es una parte de Internet que el DoD utiliza para Investigación y desarrollo.

La integración de los protocolos de Internet en el Unix *Berkeley Software Distribution* (BSD) y la difusión casi gratuita en las universidades contribuyó a mejorar el éxito de esta suite.

b. La suite de protocolos

La familia TCP/IP, de la que participan decenas de protocolos, define un modelo en cuatro capas de red.

Se trata los de protocolos de comunicación y de aplicación más conocidos para conectar sistemas heterogéneos, independientemente de la capa física.

Transmission Control Protocol (TCP) es un protocolo de transporte que asegura un servicio fiable, orientado a la conexión para un flujo importante de bytes.

Al contrario que TCP, *User Datagram Protocol* (UDP) es el protocolo de transporte no orientado a la conexión. Es más rápido pero menos fiable.

Internet Protocol (IP) proporciona un sistema de entrega de paquetes, sin conexión y no fiable. Administra las direcciones lógicas, que dividen el identificador del nodo en un número de red lógico y un número de dispositivo de 4 bytes (en IP versión 4).

➤ El protocolo IPv6, o *IP Next Generation* (NG), está disponible en los sistemas operativos más recientes.

Una de las claves del éxito de los protocolos de Internet reside en el hecho de que el modelo propuesto es independiente de las capas Física y de Conexión de datos (capas 1 y 2 del modelo OSI).

c. Correspondencia con el modelo OSI

Es importante recordar que el modelo TCP/IP se propuso diez años antes que el modelo OSI, y que este se inspiró mucho en algunos protocolos de TCP/IP; sin embargo, cabe remarcar que el modelo OSI define un modelo de 7 capas y que los protocolos de Internet funcionan sobre cuatro.

Modelo OSI	Modelo TCP/IP										
5-6-7	<table border="1"> <tr> <td>Aplicación</td> <td>Telnet</td> <td>ftp</td> <td>dns</td> <td>snmp</td> </tr> <tr> <td></td> <td colspan="4">Windows Sockets</td> </tr> </table>	Aplicación	Telnet	ftp	dns	snmp		Windows Sockets			
Aplicación	Telnet	ftp	dns	snmp							
	Windows Sockets										
4	<table border="1"> <tr> <td>Transporte</td> <td colspan="2">TCP</td> <td colspan="2">UDP</td> </tr> </table>	Transporte	TCP		UDP						
Transporte	TCP		UDP								
3	<table border="1"> <tr> <td>Internet</td> <td colspan="2">IP</td> <td colspan="2">ICMP</td> </tr> <tr> <td></td> <td colspan="2">ARP</td> <td colspan="2"></td> </tr> </table>	Internet	IP		ICMP			ARP			
Internet	IP		ICMP								
	ARP										
1-2	<table border="1"> <tr> <td>Interfaz de red</td> <td>Ethernet</td> <td>Token Ring</td> <td>Otros</td> </tr> </table>	Interfaz de red	Ethernet	Token Ring	Otros						
Interfaz de red	Ethernet	Token Ring	Otros								

d. La implementación en las empresas

Las cualidades de la suite de protocolos TCP/IP, como su capacidad de funcionamiento en cualquier tamaño de red, su eficacia y su carácter evolutivo, hacen que las empresas muestren gran interés por estos protocolos. Inicialmente, interconectaban las redes a través de Internet, sobre todo para aplicaciones de servicio de mensajería y web.

Poco a poco, se han ido adoptando estos protocolos, estandarizados y no vinculados a ningún fabricante o editor específicos, dentro de las redes locales. Las intranet han comenzado a expandirse, utilizando los mismos protocolos y principios que Internet y, como el anonimato es una de sus características, se ha hecho necesario implementar la autenticación del empleado para que pueda acceder a su empresa.

El nombre extranet designa la capacidad que tiene el usuario de acceder a la red local de tipo intranet desde fuera. Aplicando siempre las mismas normas a nivel de red, la autenticación permite reconocer a los usuarios externos de la empresa, que tendrán menos privilegios.