

# Protocolos IPv4 e IPv6

Esté el usuario en un entorno de red doméstico o profesional, la conectividad es una parte esencial para asegurar la comunicación. Los ordenadores se comunican entre sí utilizando el protocolo IP (*Internet Protocol*). Los técnicos de soporte deben poseer una buena comprensión de los protocolos IPv4 e IPv6, que garantizan la transmisión de la información para resolver los problemas de red.

El hecho de que las direcciones IPv4 públicas se agoten ha favorecido el uso de técnicas de traducción de direcciones (NAT, *Network Address Translation*), así como la proliferación del protocolo IPv6, sucesor de IPv4.

Al igual que sus predecesores, Windows 10 proporciona características de red avanzadas, que vamos a detallar en este capítulo.

## 1. Direcciones IPv4

IPv4 es una versión del protocolo de Internet que forma la base de la red Internet. Se basa en un modelo de direcciones que permite transmitir datos entre sistemas operativos iguales o diferentes.

La dirección IPv4 única de un ordenador permite a los demás ordenadores ubicados en la misma red comunicarse con él. Cada interfaz de un host IPv4 puede poseer una o más direcciones IP.

Esta dirección IPv4 codificada en 32 bits está dividida en 4 octetos de 8 bits representados por números decimales.

Por ejemplo: 172.16.1.2 es una dirección IPv4 privada (no accesible directamente desde Internet) cuya máscara de subred es 255.255.0.0.

Como las direcciones IPv4 están definidas en 32 bits, pueden direccionar como máximo  $2^{32}$  direcciones, es decir 4.294.967.296.

La dirección está compuesta por dos partes: el ID del equipo, que representa la dirección única del ordenador, y el ID de la red, que indica la subred a la que pertenece este ordenador.

La máscara de subred, compuesta por 4 octetos, especifica el lugar que ocupan el ID del equipo y el ID de la red. Se basa en una subred, que es un segmento de la red. Los routers sirven para separar las subredes entre sí y gestionar una red de clase A, B o C en diferentes ubicaciones físicas y, de este modo, segmentar el tráfico.

Por ejemplo, la clase A (de 1 a 127) tiene como máscara de subred predeterminada 255.0.0.0 y permite utilizar 126 redes para gestionar 16.777.214 hosts por red.

Particulares y empresas utilizan diariamente dos tipos de direcciones IP:

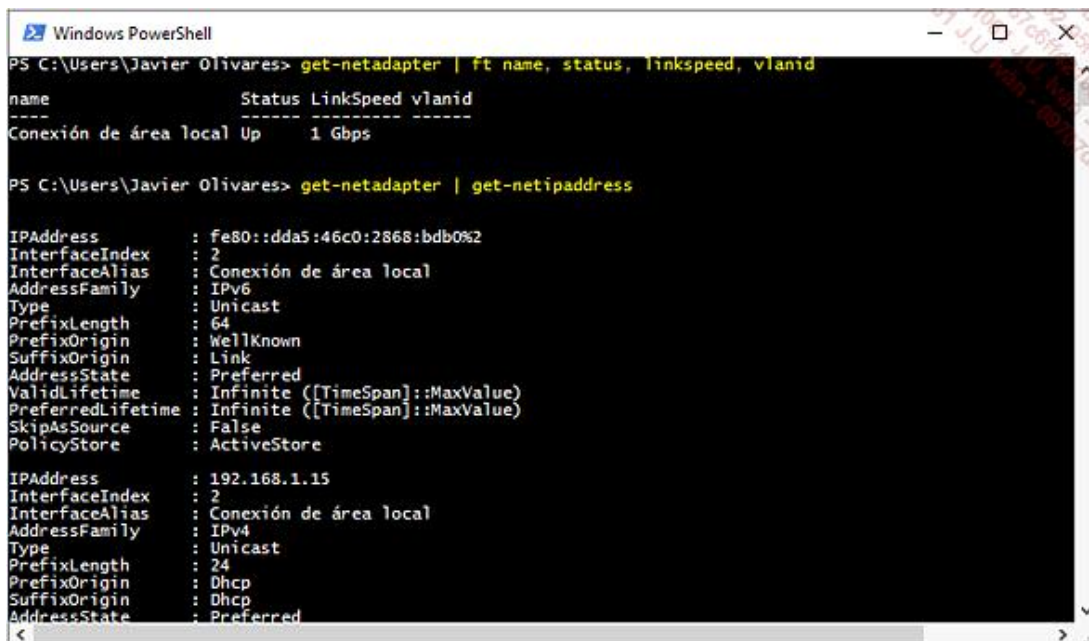
- Dirección pública: necesaria para un cliente Windows 10 que se conecta directamente por Internet, la IP pública es única, puede ser conmutada (routed) y la asigna el ICANN (*Internet Corporation for Assigned Names and Numbers*), cuyo sitio de Internet es: <http://www.icann.org/>.
- Dirección privada: no puede ser conmutada en Internet, esta dirección IP se asigna de manera local por la organización, generalmente empleando un servidor DHCP. Debe convertirse para poder comunicarse con las direcciones públicas de Internet, empleando NAT. Existen cuatro bandas de direcciones IP que son no conmutables, es decir, no son accesibles directamente desde Internet:
  - Direcciones IP de clase A: 10.0.0.1 a 10.255.255.254 para las redes importantes que necesitan soportar un gran número de hosts.
  - Direcciones IP de clase B: 172.16.0.1 a 172.31.255.254, permiten crear redes privadas de tamaño medio.

- Direcciones IP de clase C: 192.168.0.1 a 192.168.255.254, para redes privadas de pequeño tamaño.
- APIPA (*Automatic Private Internet Protocol Addressing*): 169.254.0.0 a 169.254.255.255, dirección que el cliente Windows 10 se asignará automáticamente en caso de no encontrar un servidor DHCP.

El comando **ipconfig /all** permite mostrar la configuración IP de un puesto con Windows 10.

Mediante PowerShell, puede visualizarse mucha información sobre la configuración de red:

- **get-netadapter | ft Name, Status, Linkspeed, VlanID** muestra las interfaces de red, así como información sobre el estado, la velocidad del vínculo y la VLAN asociada. Para obtener información más precisa, introduzca el comando **get-netadapter | format-list -property \***.
- **get-netadapter | Get-NetIPAddress** permite visualizar información detallada de la configuración IP del puesto con Windows 10. La dirección del servidor DNS no se muestra. Utilice el comando **Get-DnsClientServerAddress** para obtenerla.



```

Windows PowerShell
PS C:\Users\Javier Olivares> get-netadapter | ft name, status, linkspeed, vlanid
name                Status LinkSpeed VlanID
-----
Conexión de área local Up      1 Gbps

PS C:\Users\Javier Olivares> get-netadapter | get-netipaddress

IPAddress      : fe80::dda5:46c0:2868:bdb0%2
InterfaceIndex : 2
InterfaceAlias : Conexión de área local
AddressFamily  : IPv6
Type           : Unicast
PrefixLength   : 64
PrefixOrigin   : WellKnown
SuffixOrigin    : Link
AddressState    : Preferred
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : ActiveStore

IPAddress      : 192.168.1.15
InterfaceIndex : 2
InterfaceAlias : Conexión de área local
AddressFamily  : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin   : Dhcp
SuffixOrigin    : Dhcp
AddressState    : Preferred
  
```

Para definir una dirección IP en un conjunto de puestos con Windows 10, utilice el comando PowerShell **New-NetIPAddress**. Para modificar una dirección IP asignada a una interfaz Wi-Fi, introduzca el comando **Set-NetIPAddress -InterfaceAlias "Wi-Fi" -IPv4Address 192.168.10.5 -PrefixLength "24"**.

La lista de comandos PowerShell vinculados al protocolo TCP/IP está disponible en la siguiente dirección:  
<http://technet.microsoft.com/en-us/library/hh826123>

## a. Puerta de enlace

Una puerta de enlace, generalmente un router, garantiza el envío de los paquetes en los casos en que los ordenadores se comuniquen desde redes diferentes (intranet/extranet).

Sirven a menudo como repetidores para formar una intranet. La puerta de enlace transmite los paquetes de una interfaz de red a otra empleando una serie de reglas. Cuando un cliente Windows 10 quiere comunicarse con otro ordenador, utiliza un simple proceso para transmitir los datos:

1. El puesto emisor utilizará su máscara de subred para calcular su dirección de red lógica. A continuación, aplicará su máscara de subred al puesto de destino para calcular la dirección de red lógica del puesto. Si las

direcciones de red lógica de ambos puestos son idénticas, le envía el paquete. En caso contrario, pasa a la etapa 2.

2. El puesto verificará si posee una puerta de enlace predeterminada, un router por ejemplo, y efectuará el mismo procedimiento que en la etapa 1 para controlar si la puerta de enlace predeterminada y él mismo se encuentran en la misma red. Si este fuera el caso, el paquete se envía a la puerta de enlace predeterminada; si no, se abandona.
3. La puerta de enlace predeterminada recibirá el paquete y lo analizará. El router utilizará su tabla de enrutamiento para saber si cuenta con información que le permita saber dónde está situada la red del host de destino. Si hubiera una correspondencia, el paquete viajará hasta el host pasando por uno o más routers. El paquete puede ser abandonado en cualquier router. Si no hubiera correspondencia, el router abandona el paquete.

Para conocer la dirección IP de la puerta de enlace predeterminada del cliente Windows 10, ejecute el comando **netsh interface ipv4 show address** o **ipconfig /all** y visualice la dirección IP correspondiente a la línea **Puerta de enlace predeterminada**.

## 2. Direcciones IPv6

La versión 6 del protocolo IP es la conclusión de los trabajos dirigidos por la IETF (*Internet Engineering Task Force*) para paliar el agotamiento inevitable de las direcciones públicas IPv4. Las direcciones ya no se definen en 32 bits, sino en 128 bits (en bloques de 16 bits, separados por :) con una notación hexadecimal. El tamaño de las subredes se fija, en adelante, en 64 bits y utiliza un prefijo (barra diagonal /) para definir el ID de red.

El protocolo IPv6 permite utilizar  $3.4 \times 10^{38}$  direcciones para definir los hosts.

Los 64 últimos bits de una dirección IPv6 son el identificador de la interfaz, que es el equivalente al ID de host de una dirección IPv4. Cada interfaz de una red IPv6 debe poseer un identificador de interfaz único, lo que permite prescindir de la dirección MAC (*Media Access Control*) de la tarjeta de red.

El aumento de espacio de direccionamiento es, pues, consecuente.

Una dirección IPv6 será, por ejemplo: fe80:0053:0000:0000:4804:0db0:479d:f61e/64

Para simplificar su lectura, es posible reemplazar "0000" por "0": fe80:0053:0:0:4804:0db0:479d:f61e/64

A continuación, es posible eliminar los primeros "0" de cada bloque: fe80:53:0:0:4804:db0:479d:f61e/64

Por último, reemplazaremos los bloques consecutivos de "0" por "::": fe80:53::4804:db0:479d:f61e/64

Se ofrecen tres tipos de dirección IPv6:

- Unidifusión: se utiliza para la comunicación directa entre hosts, la dirección de unidifusión identifica una interfaz única. Es la más utilizada. Hay disponibles cuatro direcciones similares al direccionamiento IPv4:
  - Dirección global: equivalente a una dirección pública IPv4, esta dirección es accesible desde Internet IPv6 y empieza siempre con "001".
  - Dirección local de enlace: similar a la dirección privada automática (APIPA), esta dirección siempre comienza por "fe80".
  - Dirección local de sitio: dirección que comienza por "fec0", corresponde a la dirección privada IPv4 y necesita un servidor DHCPv6. Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2 ofrecen este rol.
  - Direcciones especiales: estas direcciones son equivalentes a la dirección indefinida ("::" o 0:0:0:0:0:0:0:0) y a la dirección de bucle invertido ("::1" o 0:0:0:0:0:0:0:1).

- Multidifusión: identifica a varias interfaces. Este tipo de dirección se utiliza para la comunicación de uno a varios hosts definidos como usuarios de la misma dirección. Los paquetes IPv6 se entregan en todas las interfaces definidas por esta dirección.
- Difusión por proximidad (anycast): se utilizan varias interfaces, pero los paquetes se entregan en la más cercana en términos de distancia de ruta (número de saltos). Este tipo de dirección sirve principalmente para localizar servicios o routers.

Un cliente Windows 10 puede obtener una dirección IP de un servidor DHCPv6 (configuración con estado) o, en su ausencia, atribuirse una él mismo (configuración sin estado). La configuración manual siempre puede actualizarse desde el **Centro de redes y recursos compartidos** o bien mediante el comando **netsh**.

El lenguaje PowerShell contiene un conjunto de comandos que permiten efectuar las operaciones frecuentes: **Set-NetIPv6Protocol** para modificar la configuración del protocolo IPv6 o **Get-NetIPv6Protocol** para obtener información de él.

El registro de un host IPv6 en un servidor DNS se realiza bajo la forma "AAAA": esta permite establecer la correspondencia entre un nombre de dominio y su dirección IPv6.

El protocolo se utiliza para varias funcionalidades, tales como DirectAccess, reconexión VPN o la compartición segura de archivos...

En cuanto a seguridad, IPV6 soporta el protocolo IPsec de forma nativa, garantizando así el cifrado de los datos que transmite entre los hosts.

IPv6 implementa la entrega por orden de prioridad: la cabecera del paquete contiene un campo que define el tiempo de tratamiento de la información. Esta mejora es particularmente útil cuando el usuario se conecta a un vídeo difundido con tecnología de streaming; los datos deberían llegarle muy rápido.

El principal punto negativo de este protocolo es la incompatibilidad entre las direcciones IPv4 e IPv6, debido a diferencias de diseño en las cabeceras IPv6.

Es necesario utilizar un protocolo de tunelización como 6to4, ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) o Teredo, que encapsulan los paquetes IPv6 en paquetes IPv4 para atravesar los routers IPv4.

Para paliar el problema de comunicación entre un cliente IPv4 y un cliente IPv6, Windows 10 implementa por defecto una configuración de doble pila, que consiste en atribuir al ordenador dos direcciones IP, una IPV4, otra IPv6, y que proporciona una capa de transporte y una trama compartida para los dos protocolos.


Además, Windows 10 permite establecer conexiones de Escritorio remoto (consulte el capítulo Gestión de clientes Windows - Acceso remoto) en los hosts con direcciones IPv6.

Windows 10 aporta funcionalidades al usar el protocolo IPv6, en comparación con los anteriores sistemas de Microsoft:

- Mejor gestión de la conectividad en Internet: en las anteriores versiones del sistema operativo Windows, cuando un host remoto IPv6 no estaba accesible debido a un fallo en la ruta, la conexión se efectuaba con el protocolo IPv4, ralentizando el acceso al recurso. Windows 10 se asegura ahora de la conectividad de una red IPv6 conocida como disponible. Si no lo está, el sistema desactiva el uso del protocolo IPv6 para el host de destino y se conecta directamente con el protocolo IPv4.
- NAT64/DNS64: cuando aparece tráfico entrante IPv6 con destino a un host IPv4, NAT64 garantiza la conversión de la dirección. DNS64 resuelve el nombre de un ordenador IPv4 en una dirección IPv6 convertida. Se utiliza NAT64/DNS64 en la característica DirectAccess, proporcionada con Windows Server 2012.
- Soporte de PowerShell: con las anteriores versiones de Windows, el comando Netsh se utilizaba para realizar acciones

en el protocolo IPv6. En adelante, PowerShell proporciona nuevas posibilidades, como la gestión de direcciones IPv6.

Visualizar la configuración IPv6 de un cliente Windows 10 es una tarea sencilla gracias al comando **ipconfig /all**.



```
Administrador: Símbolo del sistema

C:\WINDOWS\system32>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : WIN-DFU6CV07VU4
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no
Lista de búsqueda de sufijos DNS: home

Adaptador de Ethernet Conexión de área local:


Sufijo DNS específico para la conexión. . : home
Descripción . . . . . : Intel(R) PRO/1000 MT Network Connection
Dirección física. . . . . : 00-0C-29-2B-5D-F0
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::dda5:46c0:2868:bdb0%2(Preferido)
Dirección IPv4. . . . . : 192.168.1.15(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 6 de enero de 2016 11:42:55
La concesión expira . . . . . : jueves, 7 de enero de 2016 11:42:55
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 234884137
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1E-10-93-6C-00-0C-29-2B-5D-F0
Servidores DNS. . . . . : 192.168.1.1
NetBIOS sobre TCP/IP. . . . . : habilitado

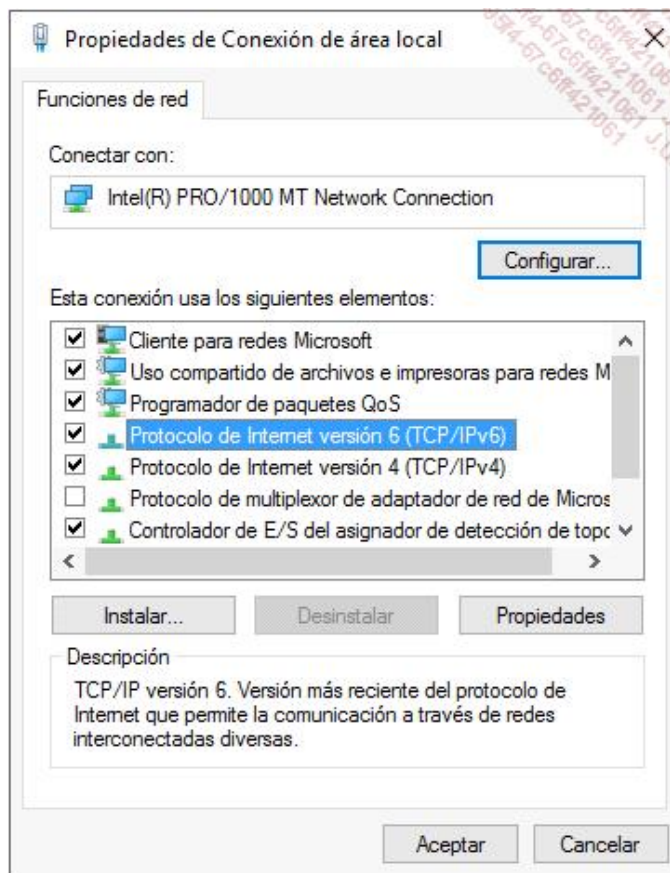
Adaptador de túnel isatap.home:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : home
Descripción . . . . . : Microsoft ISATAP Adapter
```

También es posible utilizar el comando **netsh interface ipv6 show address**.

Para desactivar IPv6, bastará con utilizar el **Centro de redes y recursos compartidos** y desactivar el protocolo en las propiedades de la tarjeta de red:

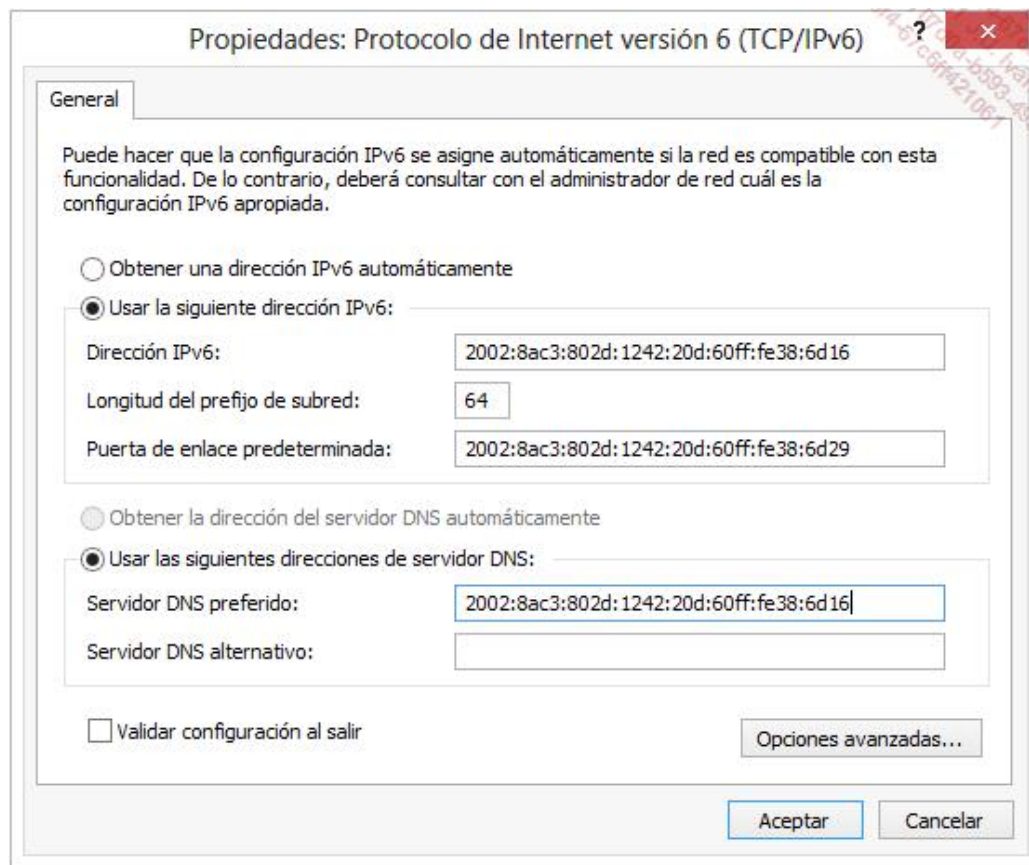
- Pulse las teclas  y **R** y, a continuación, introduzca **ncpa.cpl** en la ventana **Ejecutar** y confirme con [Intro].
- En la ventana **Conexiones de red**, seleccione la tarjeta de red en la que quiere desactivar el protocolo IPv6, haga clic con el botón derecho y seleccione **Propiedades**.
- En la ventana **Propiedades de Conexión de área local**, desmarque la opción **Protocolo de Internet versión 6 (TCP/IPv6)**.



→ Confirme haciendo clic en **Aceptar**.

Al igual que en las propiedades IPv4, seleccionando las propiedades del **Protocolo de Internet versión 6 (TCP/IPv6)** el administrador puede definir manualmente una dirección IPv6, así como la longitud de prefijo de subred, la puerta de enlace predeterminada y los servidores DNS. Puede usarse también el comando **netsh**.





### 3. Reparación IP

La resolución de problemas vinculados a la conectividad de red puede realizarse de varias maneras con Windows 10: a través del Centro de redes y recursos compartidos o bien empleado comandos como `ipconfig` o `netsh`.

Windows 10 integra una serie de herramientas de resolución de problemas de red:

- El registro del **Sistema**, accesible desde el **Visor de eventos**, cataloga los errores o los avisos asociados a los servicios de red.
- **IPconfig** muestra la configuración de red TCP/IP, permite renovar la dirección DHCP (comandos `ipconfig /release`, `ipconfig /renew`) o vaciar la caché de resolución DNS (`ipconfig /flushdns`).
- **Ping** verifica la conectividad con un equipo remoto mediante ICMP (*Internet Control Message Protocol*).
- **Nslookup** interroga a los DNS referenciados y comprueba la existencia de registros de búsquedas.
- **Tracert** muestra las rutas tomadas por un paquete de datos IP transmitido desde un equipo con Windows 10 hasta otro equipo conectado a la red IP.
- **Resolver problemas**: Windows 10 realiza una serie de comandos de red de diagnóstico y presenta un informe de resolución (consulte la sección Diagnósticos de red de Windows, más adelante en este capítulo).

Para verificar la conectividad de un cliente Windows 10 en una red empresarial, bastará con respetar el siguiente procedimiento desde una línea de comandos:

1. Visualizar la configuración IP: `ipconfig /all` o `netsh interface ipv6 show address` para la información relativa a IPv6.
2. `ping 127.0.0.1` o `ping ::1` (test de la dirección de bucle invertido).
3. `ping fec0` o `ping fe80` (APIPA) para verificar la dirección privada del cliente.

4. Opcional: **ping 001** (dirección pública en Internet del sistema Windows 10 local).
5. ping de la dirección IP de la puerta de enlace predeterminada.
6. ping de la máquina remota conectada a Internet.

## a. Netsh

El comando `ipconfig`, bien conocido por los administradores, está todavía disponible con Windows 10. Muestra la configuración IPv4 o IPv6 por interfaz física o virtual. De todas formas, solo puede ejecutarse de manera local. Microsoft presenta la herramienta de script por línea de comandos `netsh`, que permite mostrar o modificar la configuración de red de un ordenador con Windows 10 de manera local o remota.

La configuración de DHCP, de las interfaces IPv4 e IPv6, de IPsec, del enrutamiento, del servicio RPC (*Remote Procedure Call*) o de WINS se ve así enormemente facilitada.

Para ejecutar `netsh`, bastará con abrir una ventana de símbolo del sistema, introducir **netsh** y confirmar con la tecla [Intro].

Por ejemplo, para visualizar la configuración IPV6 del cliente Windows 10:

→ Desde un **Símbolo del sistema**, introduzca **netsh interface ipv6 show address**.

```

C:\WINDOWS\system32>netsh interface ipv6 show address

Interfaz 4: isatap.home
-----
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Otros      Obsoleto      infinite    infinite fe80::5efe:192.168.1.15%4

Interfaz 1: Loopback Pseudo-Interface 1
-----
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Otros      Preferido     infinite    infinite ::1

Interfaz 5: Teredo Tunneling Pseudo-Interface
-----
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Público    Preferido     infinite    infinite 2001:0:9d38:6abd:3862:3e9b:3f57:fe0
Otros      Preferido     infinite    infinite fe80::3862:3e9b:3f57:fe0%5

Interfaz 2: Conexión de área local
-----
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Otros      Preferido     infinite    infinite fe80::dda5:46c0:2868:bdb0%2

```

→ El comando **netsh interface ipv6 set address "Privado" FE80::5 anycast** definirá la interfaz llamada "Privada" con una dirección IPv6 fija de tipo anycast.



El comando `netsh` permite también configurar reglas del firewall o BranchCache. Consulte la ayuda para conocer los comandos disponibles: `netsh /?`.

Para limpiar la caché del cliente Windows 10, introduzca el comando **netsh interface ipv6 delete neighbors** como administrador local.

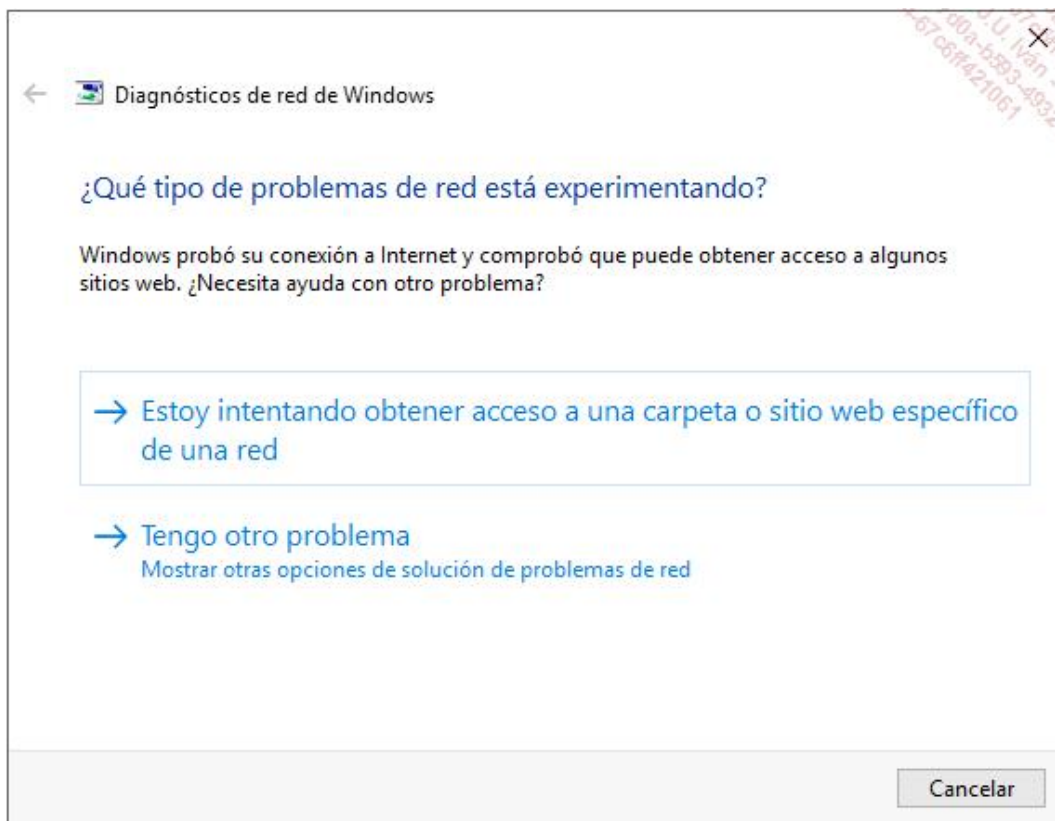
## b. Diagnósticos de red de Windows



Windows 10 ofrece la herramienta **Diagnósticos de red de Windows** para asistir al administrador en la resolución de los problemas de conectividad más frecuentes.

Accesible haciendo clic con el botón derecho en el icono de red situado en la zona de notificación de la barra de tareas del escritorio y, a continuación, seleccionando **Solucionar problemas**, esta herramienta permite corregir problemas tales como el acceso fallido a un sitio web, la imposibilidad de usar DirectAccess o fallos en la conexión a una red (física, inalámbrica, etc.). Después de haber realizado las acciones correctivas, se genera un informe de resolución de problemas, destinado al administrador, en el que se incluyen las operaciones efectuadas (ejemplo: ipconfig o tracert) en archivos con formato de texto.



El usuario utiliza un asistente que le presenta preguntas para aislar el problema y corregirlo automáticamente.



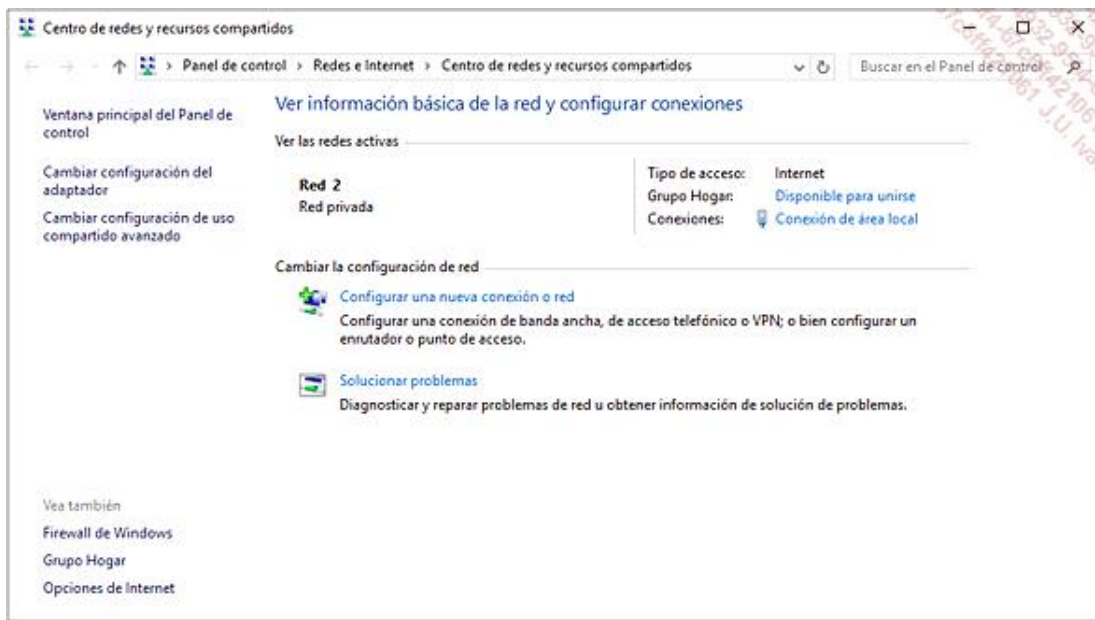
# Centro de redes y recursos compartidos

El **Centro de redes y recursos compartidos** es una interfaz que agrupa las funciones clave para la administración de la red: su estado, configuración, creación de una nueva conexión y reparación. Con Windows 10, esta herramienta se ha simplificado.

Es accesible de varias maneras:

- A través del **Panel de control**.
- Desde el icono  o  situado en la barra de tareas.
- Mediante el campo de búsqueda, introduciendo las palabras **centro red**.
- O mediante el siguiente comando:

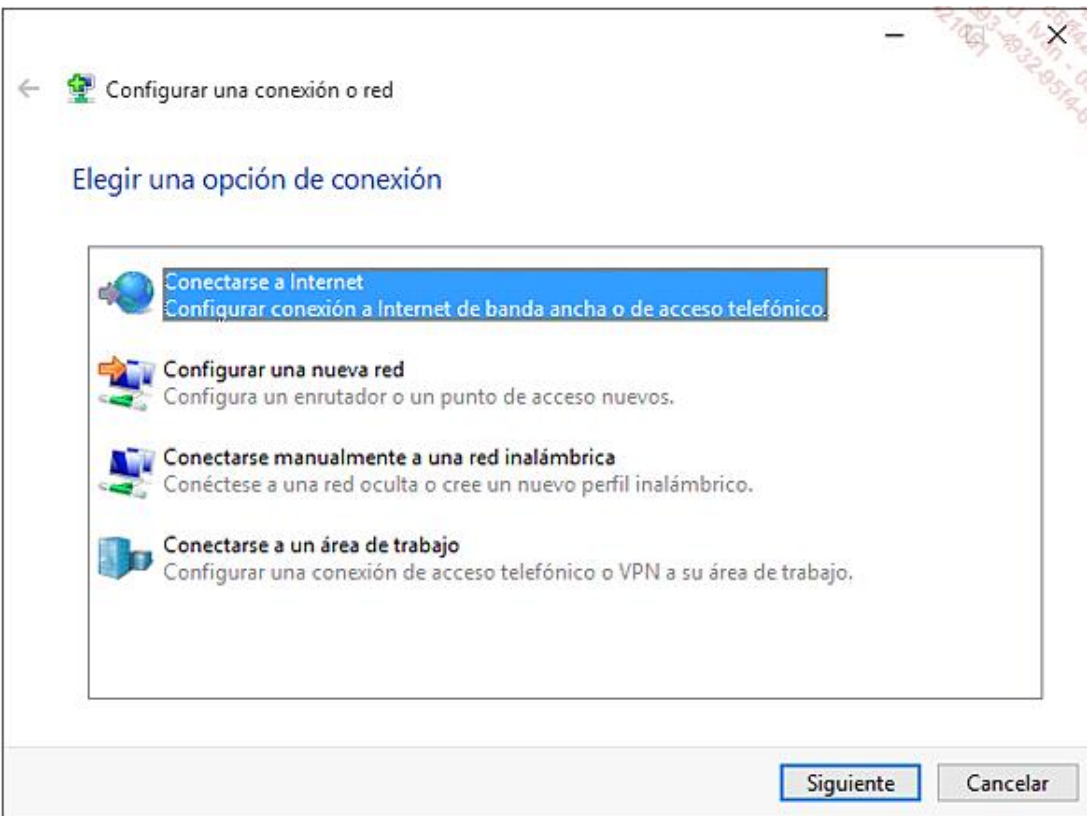
**control.exe /name Microsoft.NetworkAndSharingCenter**



Aunque una cuenta con privilegios estándar puede ejecutar el Centro de redes y recursos compartidos y realizar algunas tareas, los cambios de configuración solo puede realizarlos un miembro del grupo Administradores o un miembro del grupo **Operadores de configuración de red**.

El centro de redes y recursos compartidos permite crear una nueva conexión o una nueva red mediante un asistente:

- En la ventana **Centro de redes y recursos compartidos**, haga clic en **Configurar una nueva conexión o red**.



→ Elija el tipo de conexión que desea crear entre las cuatro opciones siguientes:

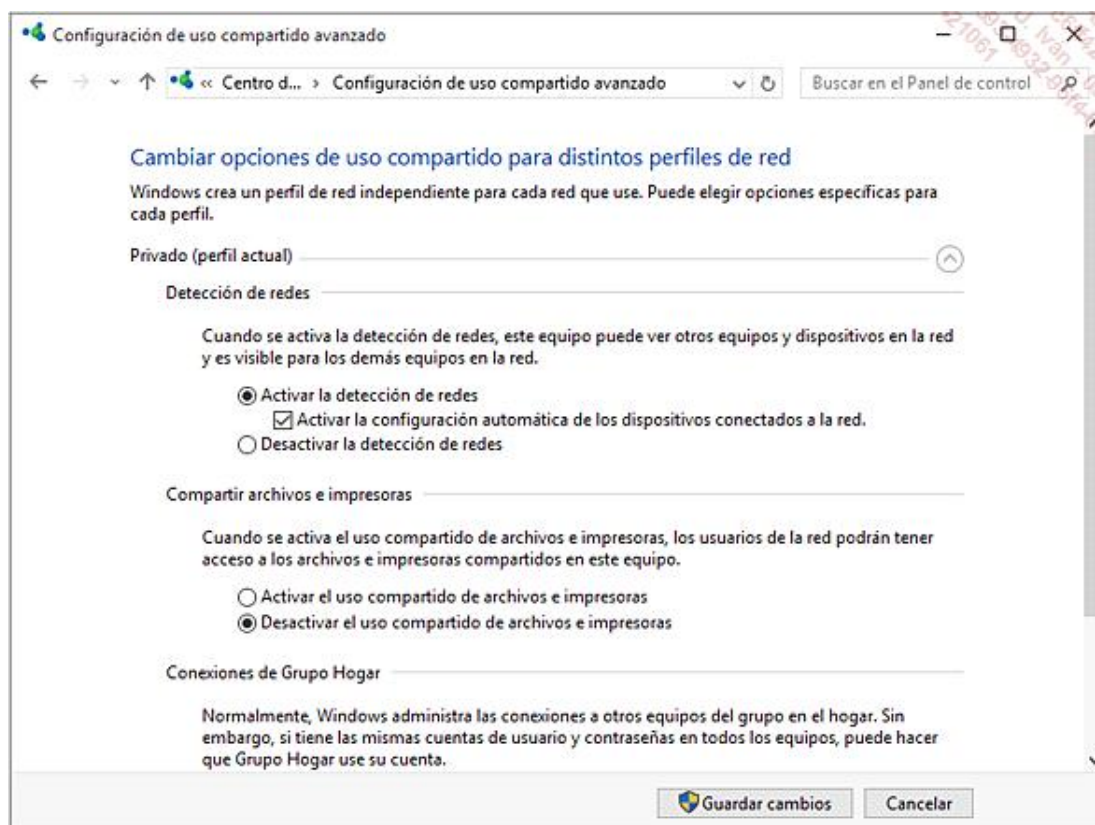
- **Conectarse a Internet:** configura una conexión de banda ancha PPoE (*Point-to-Point Protocol over Ethernet*), ADSL o cable. Es posible definir una conexión de banda ancha a baja velocidad si se cuenta con un módem RTC (Red telefónica conmutada) o RDSI (Red digital de servicios integrados) en el ordenador.
- **Configurar una nueva red:** muestra la lista de puntos de acceso o routers que pueden configurarse con Windows 10.
- **Conectarse manualmente a una red inalámbrica** (consulte la sección Gestión de redes inalámbricas).
- **Conectarse a un área de trabajo:** crea una nueva conexión VPN (SSTP, PPTP...) o banda estrecha a través de un modem RTC.

Desde la página principal del Centro de redes y recursos compartidos, haciendo clic en **Solucionar problemas**, se inicia un asistente que permite especificar el tipo de problema que hay que resolver (Internet, recurso compartido, grupo en el hogar, tarjeta de red, conexiones entrantes e impresoras) y, a continuación, analiza el equipo y propone una solución. Se genera un informe con las pruebas efectuadas.



El Centro de redes y recursos compartidos clasifica la conexión de red de una interfaz física o virtual en un perfil específico, en función de la ubicación del ordenador: **Privada** (domicilio), **Dominio** (dominio Active Directory) o **Pública** (red no segura, como la ofrecida en un cibercafé). Cuando se selecciona un perfil durante la primera conexión a una red, se crean reglas específicas en el firewall.


Las reglas generales para las carpetas compartidas y las impresoras pueden configurarse por perfil, mediante la opción **Cambiar configuración de uso compartido avanzado** de la página principal del Centro de conexiones y recursos compartidos. De esta forma, es posible activar la compartición de archivos y de impresoras, el descubrimiento de redes o incluso autorizar a Windows 10 a gestionar los grupos en el hogar.




## 1. Creación de un servidor VPN

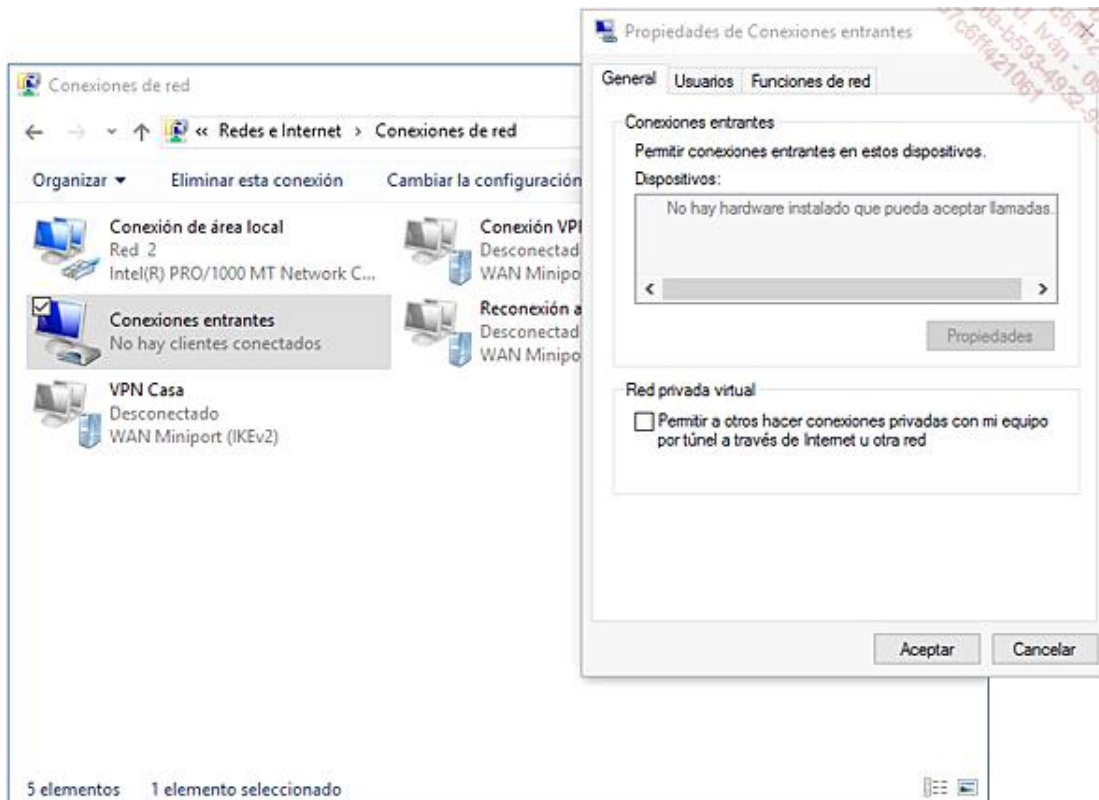
Al igual que las anteriores versiones cliente de Microsoft, Windows 10 puede proporcionar las funciones básicas de un **servidor VPN**: cifrado de las comunicaciones y creación de un túnel seguro. El servicio **Enrutamiento y acceso remoto** activa la recepción de conexiones entrantes. El usuario remoto que quiera conectarse a un puesto de trabajo con Windows 10 debe poseer una cuenta local en él y ser autorizado explícitamente.

Para crear un servidor VPN, abra una sesión como administrador en un ordenador equipado con Windows 10 y siga este procedimiento:

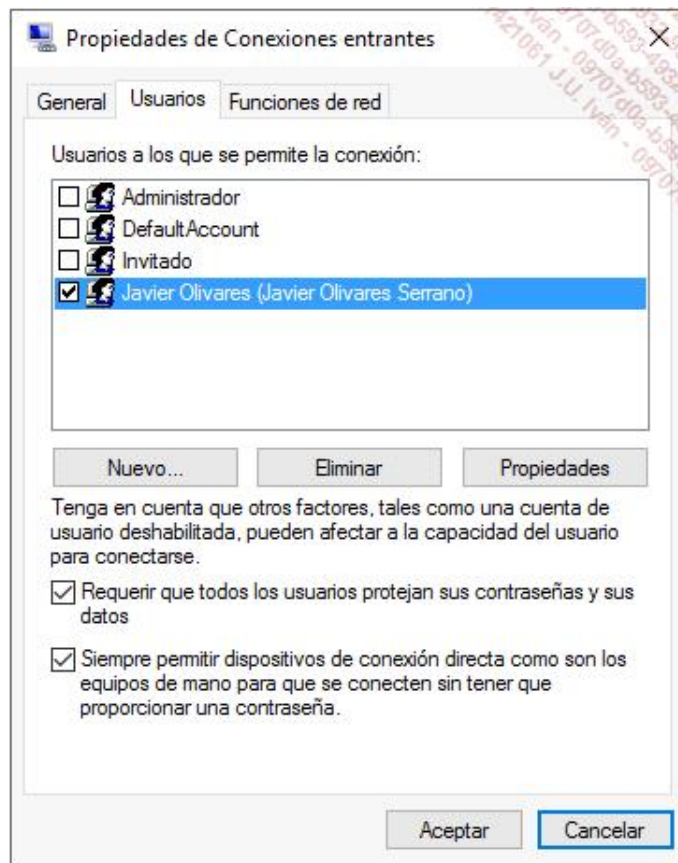
- Desde la interfaz, pulse las teclas  y **R** y, a continuación, introduzca **services.msc** en la ventana **Ejecutar** y confirme con [Intro].
- En la ventana **Servicios**, haga clic con el botón derecho y seleccione **Enrutamiento y acceso remoto** y, a continuación, **Propiedades**. En el campo **Tipo de inicio**, seleccione **Automático** y confirme haciendo clic en el botón **Aplicar**.
- A continuación, haga clic en los botones **Iniciar** y **Aceptar**. Cierre la ventana **Servicios**.

En el Centro de redes y recursos compartidos, vamos ahora a configurar el servidor VPN:

- Desde la pantalla de inicio, pulse las teclas  y **R** y, a continuación, introduzca **ncpa.cpl** en la ventana **Ejecutar** y confirme con [Intro].
- En la ventana **Conexiones de red**, el icono **Conexiones entrantes** estará ahora visible. Haga clic en él con el botón derecho y seleccione **Propiedades**.
- Marque la opción **Permitir a otros hacer conexiones privadas con mi equipo por túnel a través de Internet u otra red**.

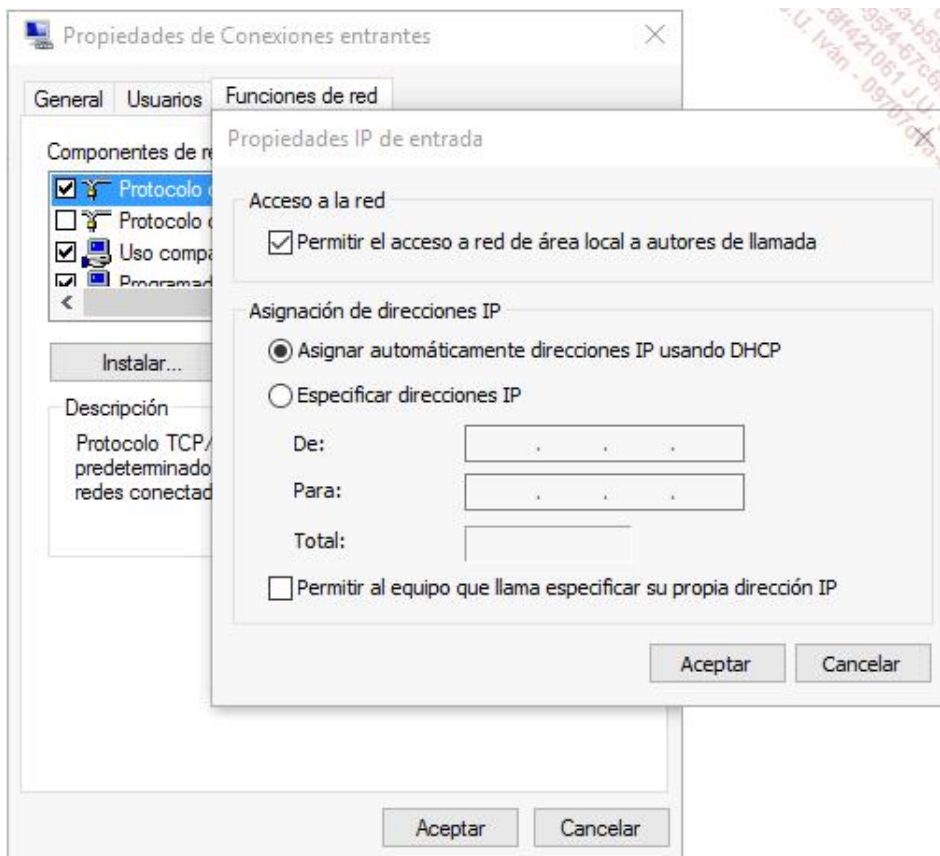


- A continuación, seleccione la pestaña **Usuarios** y marque los usuarios locales autorizados a conectarse a su puesto de trabajo de Windows 10. Asegúrese de que existe una contraseña definida para estas cuentas; en caso contrario, aparecerá un error cuando se intente inicializar el túnel VPN. Puede **Requerir que todos los usuarios protejan sus contraseñas y sus datos** para poderse conectar, o bien **Siempre permitir dispositivos de conexión directa como son los equipos de mano para que se conecten sin tener que proporcionar una contraseña**.



- Haga clic en la pestaña **Funciones de red** y, a continuación, en el botón **Propiedades** del **Protocolo de Internet versión 4 (TCP/IPv4)**. En el campo **Acceso a la red**, asegúrese de que la opción **Permitir el acceso a red de área local a autores de llamada** esté marcada. Haga clic en **Especificar direcciones IP** y defina el rango de direcciones IP conforme a su red que se asignará a las conexiones VPN remotas.






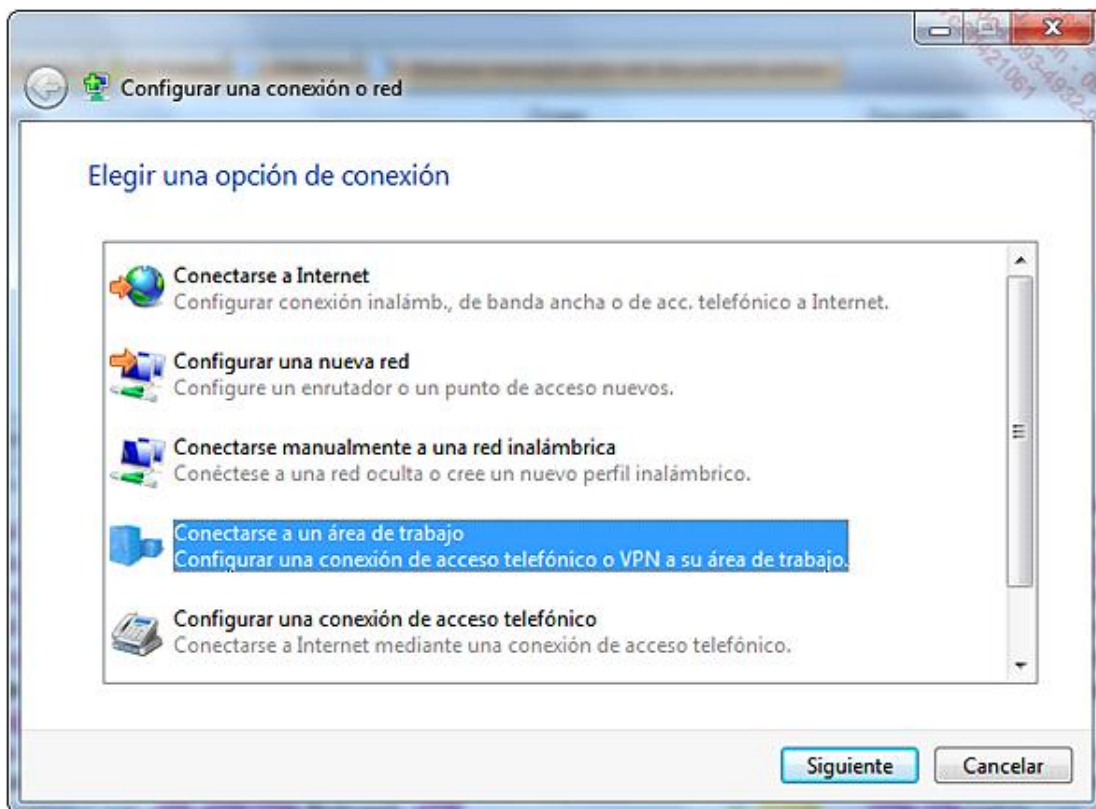
→ Confirme haciendo clic en el botón **Aceptar**.

La configuración del servidor VPN de Windows 10 está ahora terminada.

## 2. Configuración de una conexión VPN

Vamos a probar la eficacia de la conexión desde otro puesto de Windows. En este ejemplo, utilizaremos un ordenador con Windows 7:

- Haga clic en el menú **Inicio** , abajo a la izquierda de la pantalla, y, a continuación, en **Panel de control**. Haga doble clic en **Redes e Internet** y en **Centro de redes y recursos compartidos**.
- En la ventana **Centro de redes y recursos compartidos**, haga clic en **Configurar una nueva conexión o red**. En las opciones de conexión, seleccione **Conectarse a un área de trabajo**.



- Confirme pulsando **Siguiente**.
- A continuación, seleccione **Usar mi conexión a Internet (VPN)**. En el campo **Dirección Internet**, introduzca la dirección IP o el nombre DNS del servidor VPN Windows 10. Proporcione un nombre a la conexión VPN. Haga clic en el botón **Siguiente**.
- Introduzca un nombre de usuario y una contraseña creados en el equipo de Windows 10 y confirme pulsando **Conectar**.

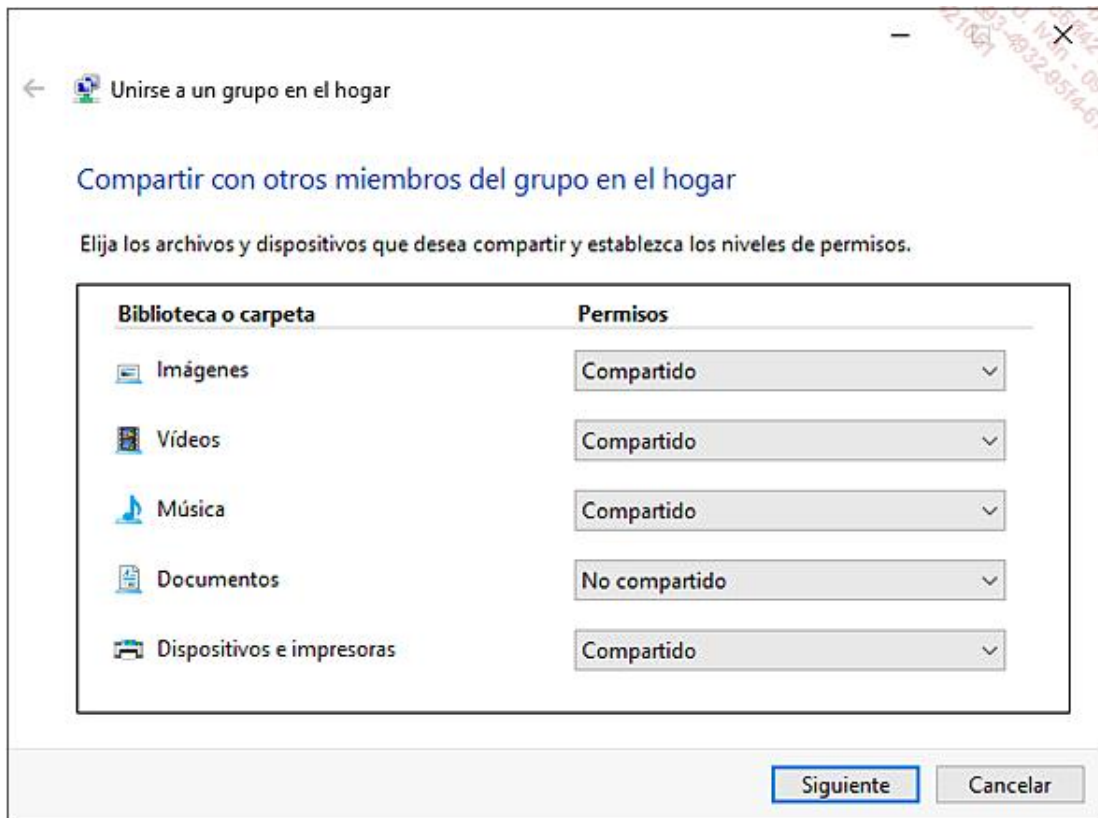
En adelante, estará conectado a un servidor VPN Windows 10.

### 3. Grupo en el hogar

En un lugar privado, como una casa o un apartamento, los ordenadores y los dispositivos están conectados generalmente a la misma red, gestionada por un punto de acceso inalámbrico o un router. Windows 10 permite compartir archivos, impresoras y contenido multimedia con otros hosts de la misma red, protegidos por una contraseña: es el **Grupo en el hogar**. Para crearlo, la ubicación de red de la conexión debe estar definida obligatoriamente como **Privada**.

Desde la interfaz del Centro de redes y recursos compartidos, haga clic en **Grupo hogar**:

- Haga clic en el botón **Grupo en el hogar** y, a continuación, en el botón **Siguiente**. Seleccione el tipo de datos que desea compartir: **Imágenes**, **Videos**, **Música**, **Documentos** y **Dispositivos e impresoras**.



- Haga clic en **Siguiente**.
- El sistema genera una contraseña aleatoria que es posible imprimir. Esta contraseña puede modificarse y se utilizará para configurar otros puestos de trabajo miembros del mismo grupo en el hogar.
- Haga clic en el botón **Finalizar**.

En la interfaz de configuración del grupo en el hogar, también es posible autorizar la difusión del contenido multimedia almacenado en el equipo de Windows 10, en un televisor o en una consola de juegos de tipo Xbox. En todo momento, el usuario puede modificar lo que comparte con el grupo en el hogar haciendo clic en **Cambiar lo que comparte con el grupo en el hogar**.

La conexión a un grupo en el hogar existente exige que el puesto con Windows 10 no haya creado otro grupo. En ese caso, haga clic en el botón **Unirse** en la interfaz **Grupo Hogar** del Panel de control o del Centro de redes y recursos compartidos.

# Gestión de redes inalámbricas

Usadas con frecuencia para proporcionar acceso a Internet en lugares públicos, una red inalámbrica es un conjunto de equipos interconectados por señales de radio, a diferencia de una red cableada, que utiliza conectores RJ45. La norma IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 describe las especificaciones para implementar redes locales inalámbricas.

La gestión de redes inalámbricas es una tarea importante para un administrador, porque generan problemas de seguridad derivados de la desaparición del perímetro de red y están sujetas a interferencias. Sin embargo, facilitan la movilidad y la flexibilidad de los usuarios itinerantes.

Existen dos modos de conexión a una red inalámbrica: el modo ad hoc y el modo infraestructura. Con el primero, la conexión de un equipo con Windows 10 se efectúa de su tarjeta de red inalámbrica a la de otro equipo, empleando una contraseña compartida: es el equivalente al concepto de grupo de trabajo.

En el modo infraestructura, el cliente Windows 10 se conecta directamente a un punto de acceso inalámbrico, que se encarga de la transferencia y seguridad de los datos intercambiados: la arquitectura es similar a un dominio Microsoft. Una red inalámbrica, en modo ad hoc o infraestructura, tiene siempre un nombre, visible u oculto, el SSID (*Service Set Identifier*).

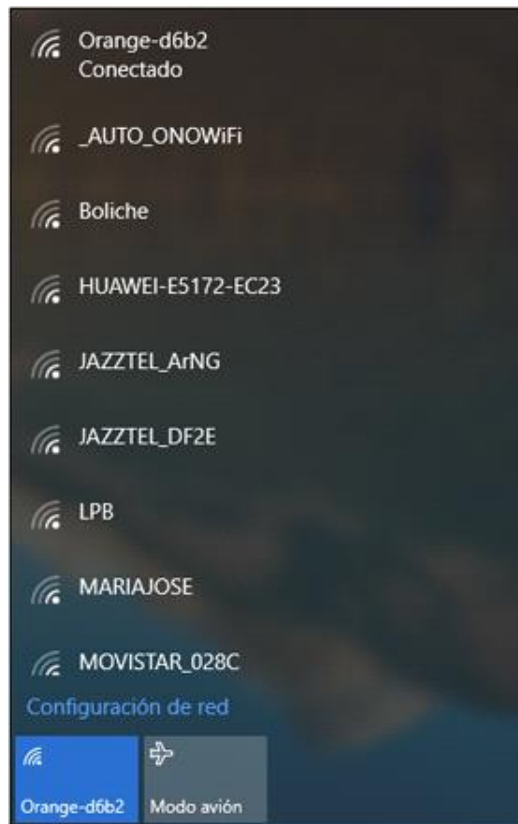
Windows 10 proporciona compatibilidad completa con todas las normativas del mercado: 802.11a (54 Mbits/s), 802.11b (11 Mbits/s), 802.11g (54 Mbits/s) y 802.11n (600 Mbits/s). Por supuesto, la calidad del uso de una red inalámbrica depende de la tarjeta de red y del controlador asociado.

La seguridad de las redes inalámbricas combina métodos de autenticación y de cifrado. Windows 10 puede conectarse a un punto de acceso inalámbrico empleando una autenticación por sistema abierto, clave compartida (WEP), 802.1 X o PSK. En cuanto al cifrado, las claves WEP (*Wired Equivalent Privacy*) y WPA (*Wi-Fi Protected Access*) Enterprise (TKIP, AES) están disponibles.

Pero si la seguridad del cliente es esencial, la del punto de acceso es primordial: piense en desactivar la publicación del SSID, activar el filtrado de direcciones MAC y utilizar software que emita SSID falsos. Estas acciones se realizan desde la configuración avanzada de su módem ADSL (Livebox, Zyxel, etc.).

La conexión a una red inalámbrica, proceso delicado para un neófito, se ve ahora simplificada con Windows 10: existe una vista única que permite gestionar las conexiones remotas (VPN, RTC, etc.), inalámbricas, de red e Internet.

Simplemente haga clic en el icono de red situado en la barra de tareas para mostrar todas las redes cableadas e inalámbricas.



La conexión de un cliente a un punto de acceso inalámbrico necesita conocer el nombre de la red (SSID) e introducir una clave (WEP, WPA, etc.) para ser autenticado.

Cuando la red no necesita una clave para conectarse (red abierta), pero obliga al usuario a introducir un nombre de usuario y una contraseña en una página de Internet, Windows 10 detecta este método de identificación y permite introducir las credenciales automáticamente.

La configuración de una red inalámbrica se efectúa de tres maneras diferentes:

- Mediante el cuadro de diálogo **Conectarse manualmente a una red inalámbrica**. Accesible desde el **Centro de redes y recursos compartidos**, este asistente permite configurar manualmente los parámetros de una red inalámbrica:
  - Introduzca **centro redes** en el campo de búsqueda situado en la barra de tareas y, a continuación, seleccione **Centro de redes y recursos compartidos**. Haga clic en **Configurar una nueva conexión o red**.
  - En la ventana **Configurar una nueva red**, seleccione **Conectarse manualmente a una red inalámbrica** y, a continuación, confirme haciendo clic en el botón **Siguiente**.
  - Introduzca la información de conexión a la red inalámbrica, como el **Nombre de la red** (SSID), el **Tipo de seguridad**, el **Tipo de cifrado** así como la **Clave de seguridad**:

← Conectarse manualmente a una red inalámbrica

Escriba la información de la red inalámbrica que desea agregar.

Nombre de la red: JJOS1

Tipo de seguridad: WPA2-Personal

Tipo de cifrado: AES

Clave de seguridad: ..... ☒ Ocultar caracteres

☒ Iniciar esta conexión automáticamente

☐ Conectarse aunque la red no difunda su nombre

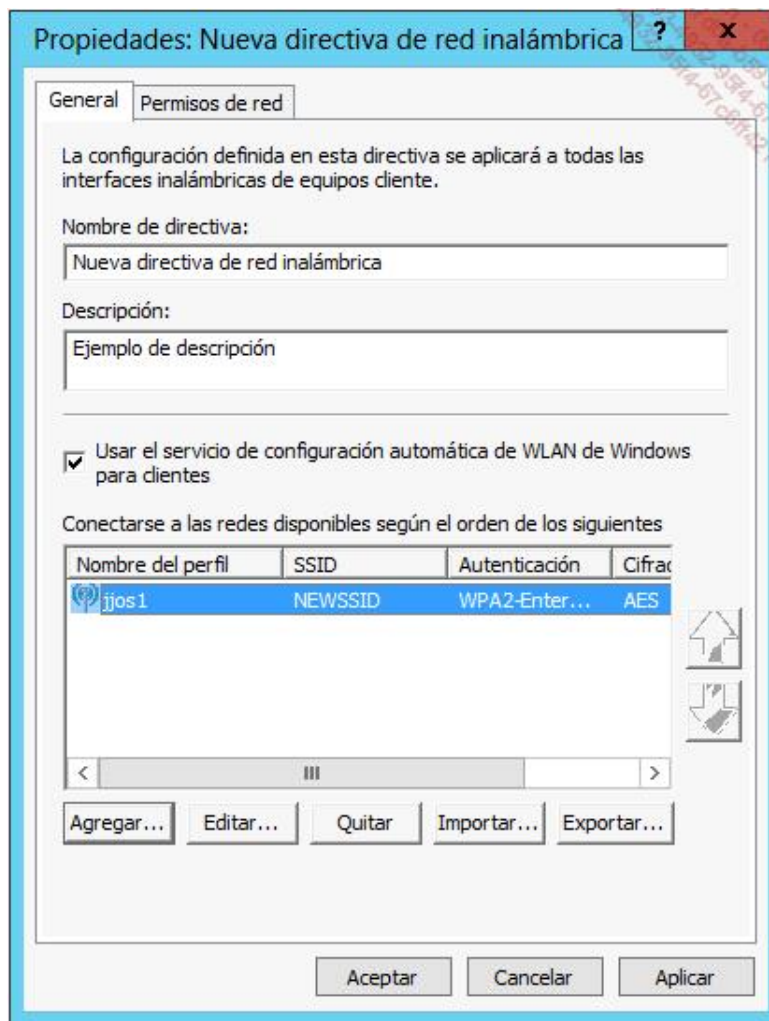
Advertencia: esta opción podría poner en riesgo la privacidad del equipo.

Siguiente Cancelar

→ A continuación, haga clic en los botones **Siguiente** y **Aceptar**.

- Por línea de comandos: el comando **netsh wlan** permite configurar de manera local o remota las redes inalámbricas. Por ejemplo, el comando **netsh wlan connect name=Profile1 ssid=JJOS1 interface="wi-fi"** creará una conexión a la red "JJOS1" desde la tarjeta de red llamada wi-fi del cliente Windows 10.
- Mediante una directiva de grupo: en un entorno gobernado con Active Directory, el administrador puede configurar de forma homogénea las redes inalámbricas en los puestos con Windows 10 mediante un objeto de directiva de grupo. Esto se hace a través del nodo **Configuración del equipo - Directivas - Configuración de Windows - Configuración de seguridad y Directivas de red inalámbrica (802.11)**. Puede definir las redes inalámbricas preferidas, los parámetros de seguridad apropiados o impedir la conexión a redes específicas.





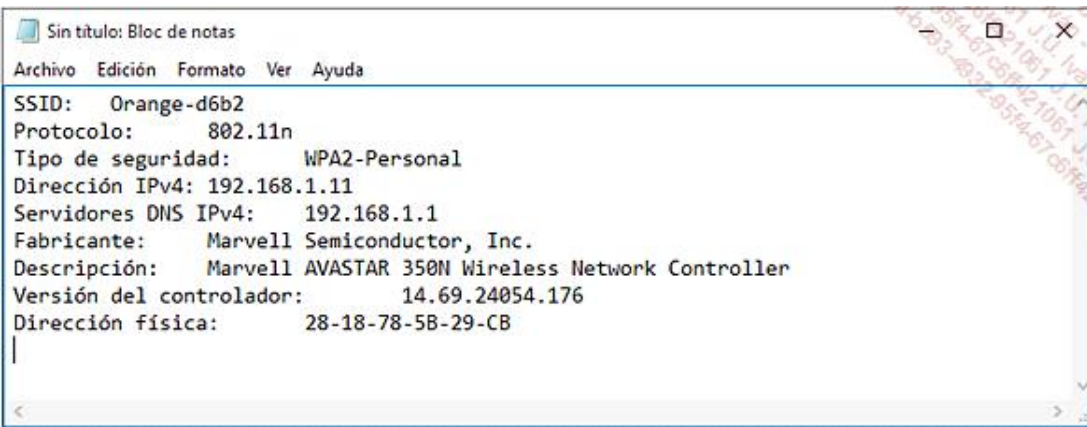
Cuando una conexión a una red inalámbrica es lenta o resulta imposible de establecer, el administrador investiga la causa del problema y lleva a cabo acciones correctivas. Cuanto más fuerte sea la señal, mejor será el rendimiento obtenido. Un punto de acceso situado a una distancia significativa del puesto de trabajo puede explicar un tiempo de latencia importante. La presencia de un componente Bluetooth puede interferir con la señal de una red inalámbrica.

Un armario metálico o el espesor de una pared pueden explicar la debilidad de la señal, al igual que la interferencia creada por los teléfonos inalámbricos. En ciertos casos, considere definir un número de canal diferente en el punto de acceso.

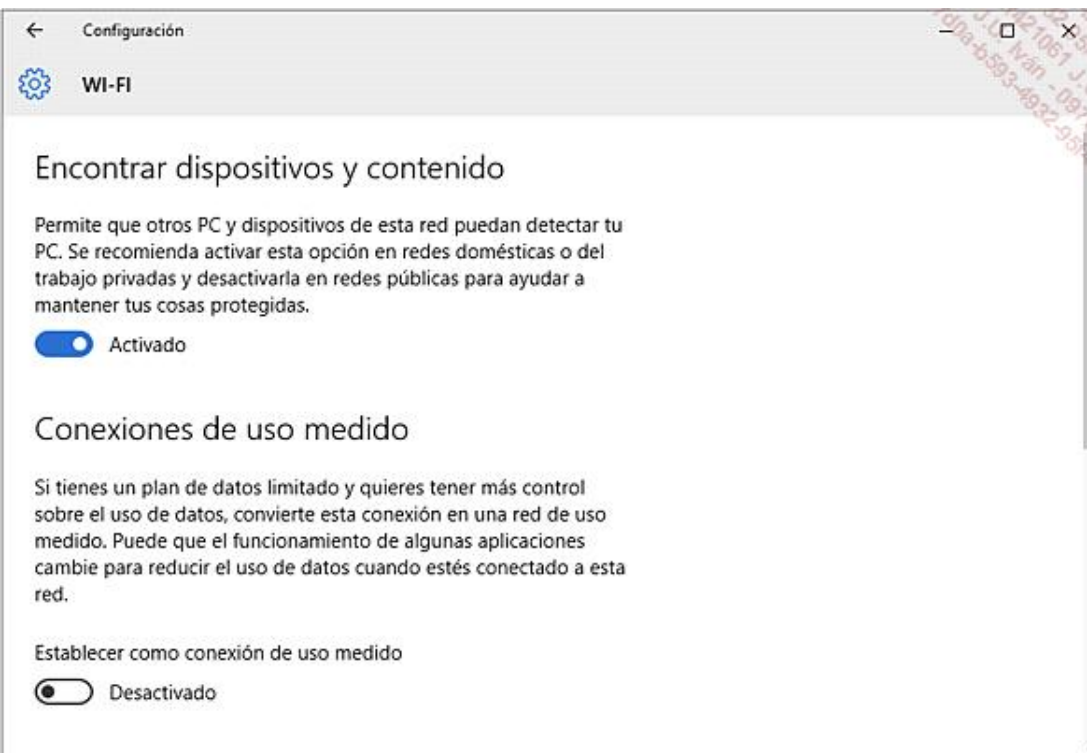
Si la red inalámbrica a la que el cliente desea conectarse no se muestra, verifique que la tarjeta inalámbrica está activada y dispone del controlador adecuado. Algunos puntos de acceso inalámbricos no publican su SSID para mejorar la seguridad.

El usuario también puede copiar en el portapapeles la configuración de una red inalámbrica específica (sin la contraseña) desde la nueva interfaz:

- Haga clic en el menú **Inicio** y en **Configuración**. Haga doble clic en **Red e Internet**. Haga clic en **Wi-Fi** y **Opciones avanzadas**. En las propiedades de la red inalámbrica actual, haga clic en el botón **Copiar**. Pegue el resultado en el bloc de notas:

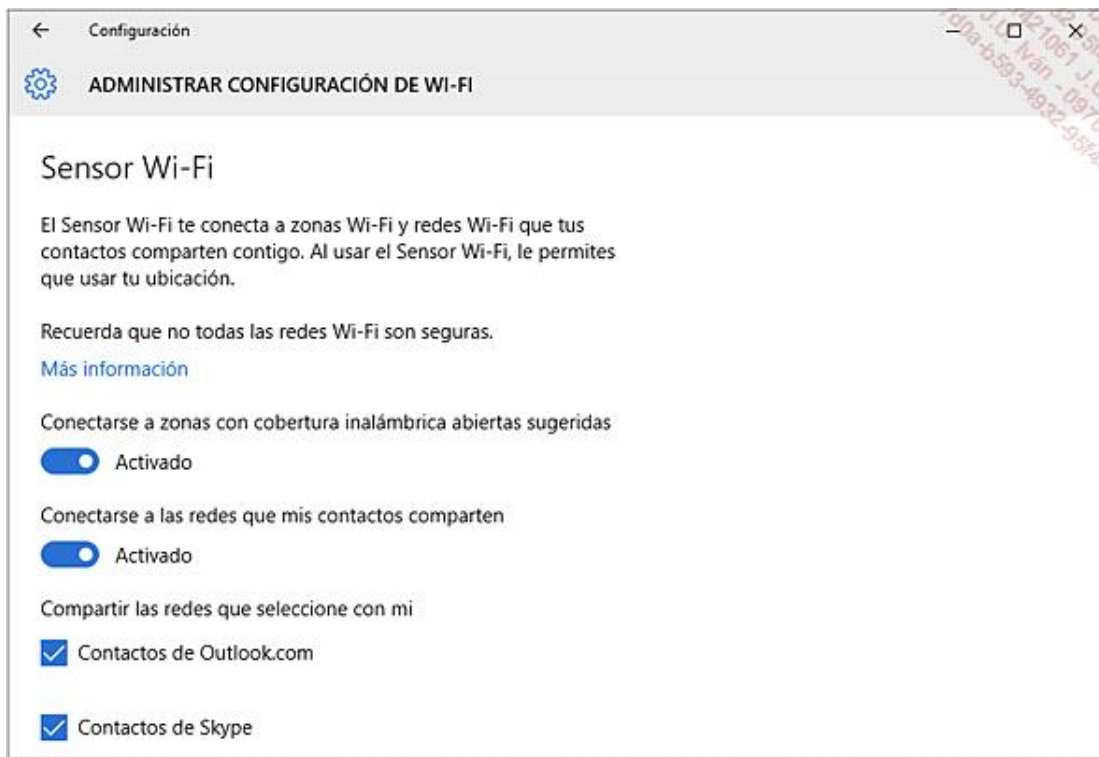


Otros parámetros están disponibles en esta interfaz, como la posibilidad de hacer visible el equipo con Windows 10 en una red privada, o el hecho de poder definir la conexión actual como limitada para reducir los costes de uso.



## 1. Wi-Fi Sense

Una nueva e interesante funcionalidad es la posibilidad que se ofrece a sus amigos y contactos (Facebook, Skype, etc.) de acceder a la red inalámbrica a la que está conectado mediante su cuenta Passport, y así compartir con ellos su acceso a Internet: es el **Sensor Wi-Fi** (Wi-Fi Sense) accesible desde **Administrar configuración de WI-FI**.



Wi-Fi Sense no funciona con las redes Wi-Fi que emplean el protocolo 802.1X o aquellas a las que el administrador ha agregado "\_optout" al final de su nombre SSID. Los identificadores de conexión de red inalámbricos se transfieren empleando una conexión cifrada desde un servidor Microsoft y luego se devuelven al equipo de sus contactos si la red Wi-Fi compartida está dentro del rango.

Las personas que se conectan empleando Wi-Fi Sense no cuentan con acceso a la red local del punto de acceso inalámbrico, sino solo a la conexión a Internet que este ofrece.

En términos de seguridad, el empleo de esta funcionalidad es discutible: ¿qué ocurre si se roba un equipo con Windows 10? ¿O durante su pirateo? ¿Y si comparte el acceso a su red inalámbrica con una persona que hace lo mismo con todos sus contactos?

Windows 10 proporciona la herramienta **Diagnósticos de red de Windows** (consulte la sección Protocolos IPv4 e IPv6 - Reparación IP) para resolver los problemas de conexión a una red inalámbrica: el filtrado de direcciones MAC puede, por ejemplo, ser un motivo de errores de autenticación.

## 2. Banda ancha

Las redes 3G y 4G presentan tráfico comprendido entre unos kilobytes y varias decenas de megabytes. Son generalmente menos rápidas porque el tiempo de latencia es alto y utilizan la red de telefonía gestionada por un operador de telefonía (Movistar, Orange, Vodafone, etc.). Estas redes imponen generalmente umbrales de datos con costes muy altos por sobrepasarlos.

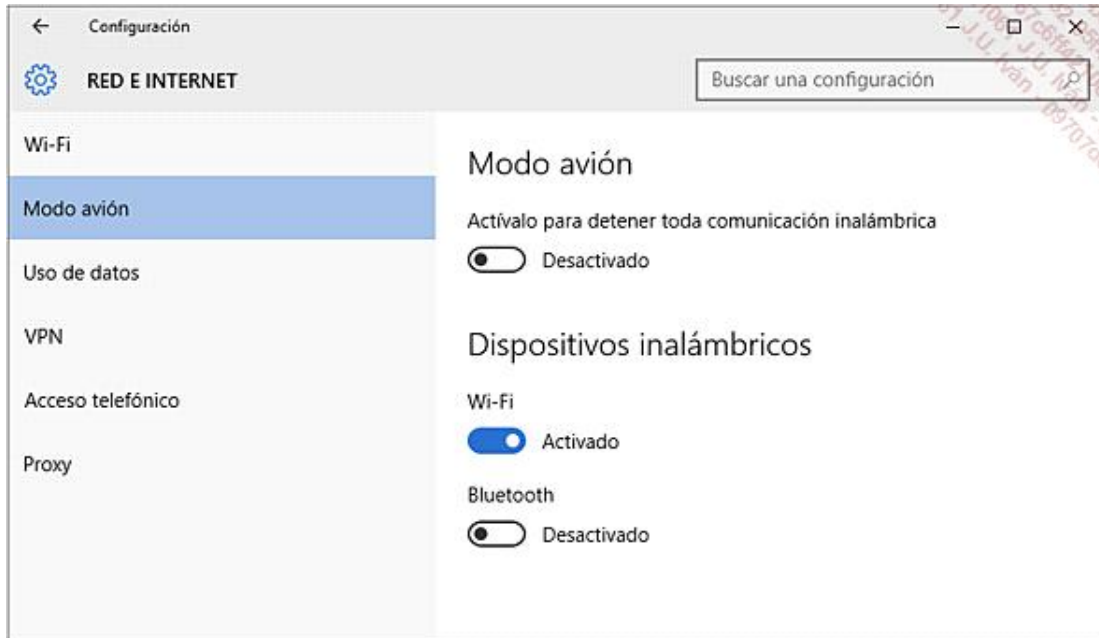
Con Windows 7, los usuarios debían instalar los controladores y el software proporcionados por los proveedores de acceso para configurar las conexiones. Windows 10 simplifica estas exigencias presentando un controlador integral nativo y actualizable mediante Windows Update.

El operador de telefonía móvil se identifica automáticamente y, a continuación, se configura la tarjeta SIM relacionada. Si fuera necesario, se descarga la aplicación propietaria desde la Tienda (Windows Store), permitiendo así pagar la factura, visualizar el consumo de datos o utilizar el soporte técnico!

El usuario puede elegir directamente un plan de datos para gestionar los datos en el sitio de Internet del operador, que se aplicará a los parámetros de conexión.

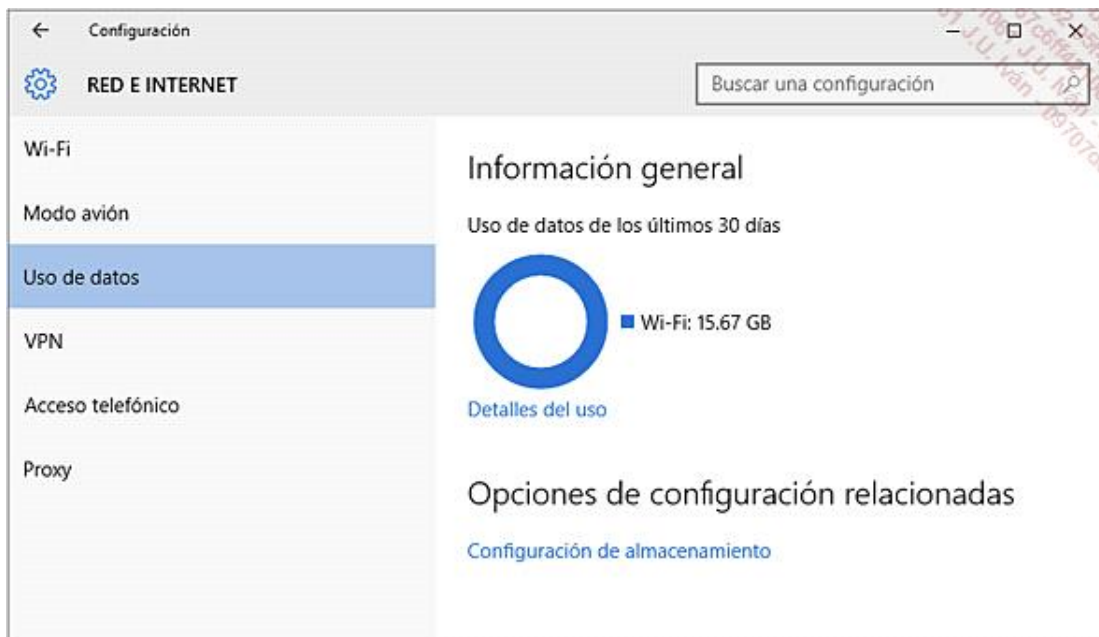
Mediante la norma **MBIM** (*Mobile Broadband Interface Model*), Windows 10 puede explotar los dispositivos de banda ancha desde una interfaz única. De esta forma, es posible activar o desactivar las diferentes tarjetas (Bluetooth, banda ancha, Wi-Fi, etc.):

→ Haga clic en el menú **Inicio** y luego en **Configuración**. Haga clic en **Red e Internet**. Haga clic en el **Modo avión** y active o desactive las interfaces que gestionan las redes inalámbricas.



➤ Usando el modo avión, es posible deshabilitar todos los dispositivos inalámbricos en una sola operación desde el Centro de actividades.

En **configuración**, la sección **Uso de datos** muestra en una única vista el consumo global de los datos Wi-Fi y Ethernet de los últimos 30 días.



El seguimiento del consumo de datos de red empleados por las aplicaciones se encuentra disponible haciendo clic en **Detalles del uso** o, desde el **Administrador de tareas**, en la pestaña **Procesos**.

Además, el sistema analiza el comportamiento del usuario (desconexión manual de una red inalámbrica, tipo de red) y, a continuación, crea una lista de hábitos que mantiene al día. Por ejemplo, si el usuario está conectado a una red "A" y más tarde se desconecta para conectarse a una red "B", Windows 10 pondrá la red "B" más alto en la lista de sus redes preferidas.

Cuando un usuario que utiliza una red de banda ancha móvil se conecta a una red Wi-Fi preferida, Windows 10 lo desconecta automáticamente de la primera red para favorecer la velocidad ofertada por la Wi-Fi. Cuando proceda, el dispositivo de banda ancha se deshabilita, para ahorrar batería.

Antes, un equipo hibernado que salía de ese estado necesitaba un tiempo de espera para reconectarse a la red Wi-Fi utilizada. Con Windows 10, solo hacen falta uno o dos segundos para que el usuario se conecte a la red inalámbrica; el sistema aplica de nuevo rápidamente la información de conexión.

### 3. Pantallas inalámbricas Miracast

Frente a Airplay de Apple o WiDi de Intel, el consorcio Wi-Fi Alliance ha desarrollado una tecnología que permite enviar imágenes y sonido desde un dispositivo móvil (tableta, equipo portátil...) a un televisor, proyector o monitor, empleando redes inalámbricas.

Windows 10 soporta esta funcionalidad en las ediciones del sistema, y presenta Wi-Fi Direct, el protocolo WPA2 que permite dotar de seguridad la transmisión, que soporta del códec H.264 de hardware para la codificación de vídeo, al igual que Wi-Fi 802.11n para la conectividad. Observe que la resolución teórica es de 1080p Full HD.

A su vez, el usuario puede mostrar una presentación en PowerPoint o usar un juego en una pantalla más grande que la de su dispositivo.

Si su pantalla objetivo no soporta la tecnología Miracast, será necesario adquirir un adaptador que se conectará al puerto HDMI del dispositivo de visualización.

Para añadir la pantalla inalámbrica compatible Miracast a su tableta o su PC, realice el siguiente procedimiento:

- Desde el menú **Inicio**, haga clic en **Configuración** y **Sistema**. En la sección **Pantalla**, haga clic en **Conectarse a una proyección inalámbrica**.

Ahora que se ha agregado la pantalla inalámbrica, es sencillo compartir su pantalla:

- Seleccione el tipo de configuración de la visualización entre cuatro opciones: mostrar **Solo pantalla de equipo**, **Duplicar** de manera idéntica en ambas pantallas, **Extender** la visualización o mostrar **Solo segunda pantalla**.

Observe que es necesario que la pantalla inalámbrica esté situada cerca de su dispositivo con Windows 10.

Cuando su PC con Windows 10 cambie a modo bloqueado, o si se desplaza fuera del alcance de su pantalla inalámbrica, se desconectará automáticamente de esta.

### 4. Wi-Fi tethering

La compartición de una conexión de datos móviles (EDGE, 3G o 4G) con otro dispositivo es conocida como «tethering» (conexión de un dispositivo a otro). La conexión por tethering transforma de esta manera el

smartphone en un punto de acceso inalámbrico. Esta característica con frecuencia se factura al usuario por parte del operador de telefonía si se supera una cantidad de datos transmitidos.

Por esto, al insertar una tarjeta SIM o al conectarse a una red de un operador telefónico, Windows 10 puede compartir su conexión a Internet con otros dispositivos. Sin embargo, las actualizaciones de seguridad y de otras aplicaciones no se descargarán, para limitar el ancho de banda utilizado.

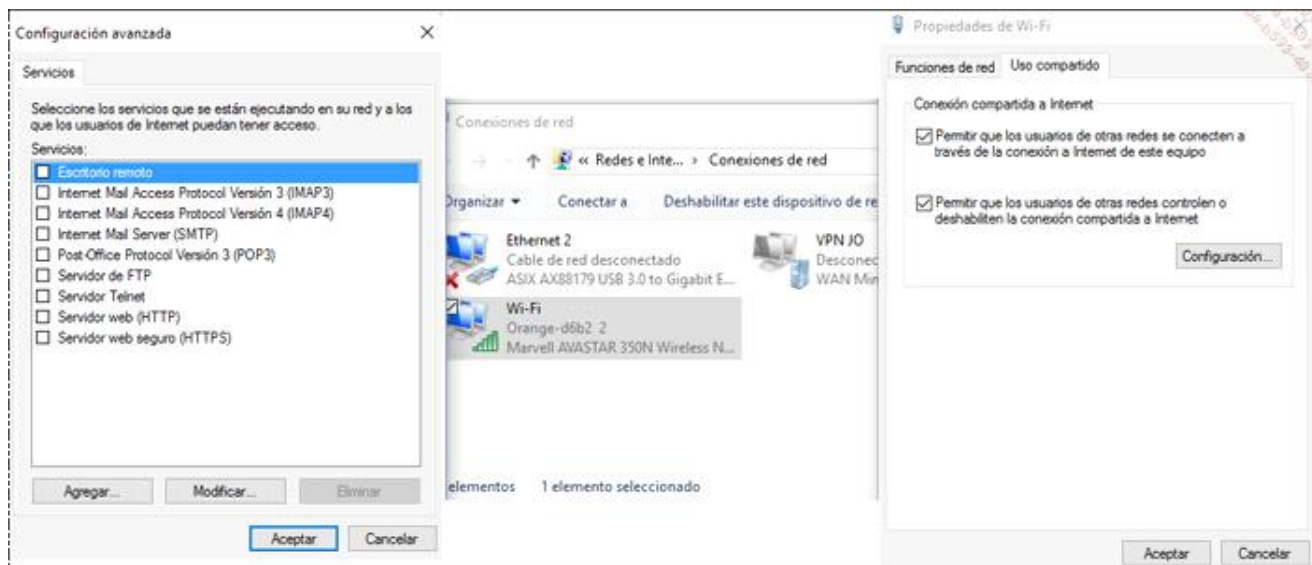
En adelante, es posible convertir el ordenador portátil o la tableta con Windows 10 en punto de acceso inalámbrico para compartir con un máximo de 10 dispositivos la conexión a Internet.

Para activar la compartición de la conexión, siga este procedimiento:

→ Haga clic con el botón derecho del ratón en el icono  o  situados en la parte inferior derecha

de la barra de tareas, y luego en **Abrir el centro de redes y recursos compartidos**. Haga clic con el botón derecho del ratón en la tarjeta de red inalámbrica y luego en **Propiedades**. Seleccione la pestaña **Compartir** y marque la opción **Permitir que los usuarios de otras redes se conecten a través de la conexión a Internet de este equipo**.

El botón **Configuración** permite seleccionar los servicios compartidos con los usuarios, como HTTP, HTTPS o FTP.



Ahora, podrá conectarse a Internet mediante la conexión de su dispositivo a la red inalámbrica transmitida por Windows 10.




# Asignación automática de direcciones IP

Windows 10 soporta, como todo sistema operativo, la obtención de una dirección IP desde un servidor DHCPv4 o DHCPv6. El beneficio para un administrador es importante, porque ya no debe ocuparse de gestionar las direcciones IP asignadas en la red empresarial. Repartir las direcciones IP estáticas consume tiempo y aumenta el riesgo de error.

El servicio **Ciente DHCP** gestiona la inscripción y la actualización de las direcciones IP en el servidor DHCP, al igual que los registros DNS correspondientes.


En caso de fallo del servidor DHCP, el cliente se asignará automáticamente una dirección IP APIPA en la red 169.254.0.0/16. Sin embargo, esta configuración no permitirá utilizar los servicios de Active Directory o de Internet, porque ninguna puerta de enlace, servidor DNS o WINS son definidos por APIPA. Para remediar esta limitación, Microsoft permite utilizar la configuración alternativa.

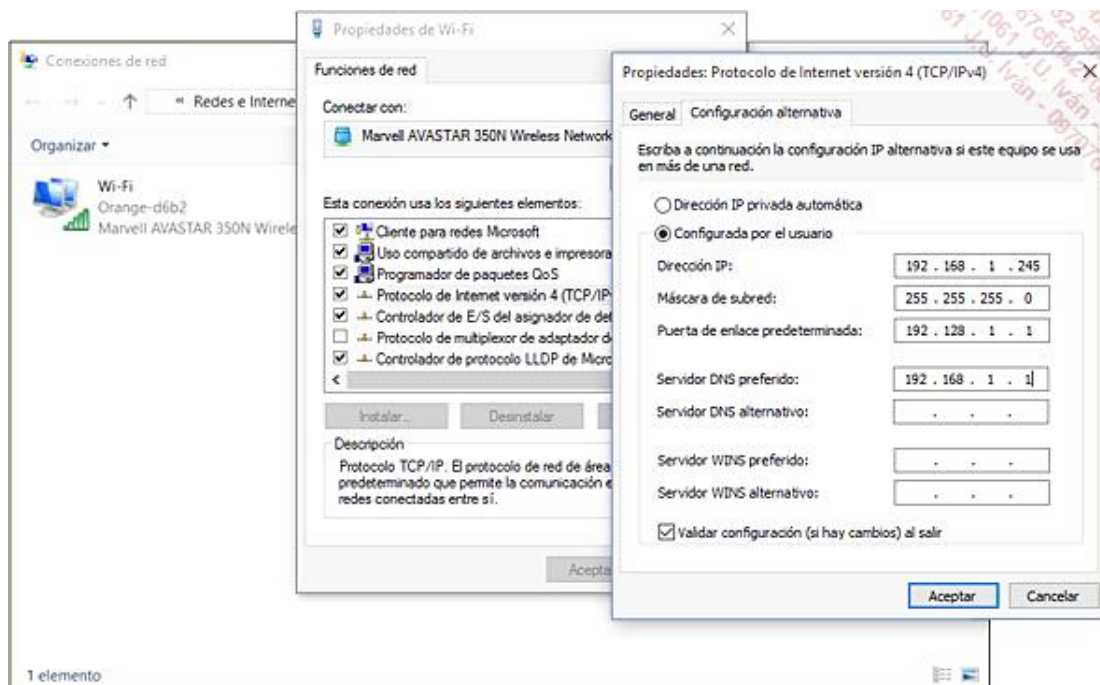
 Un buen medio de evitar el uso de APIPA consiste en configurar DHCP con tolerancia a fallos: dos servidores DHCP ofrecen rangos diferentes de las direcciones disponibles (50% un servidor y 50% el otro) a los clientes DHCP. De esta forma, si uno de ellos no estuviera disponible, el otro seguiría distribuyendo las direcciones IP.

## Configuración alternativa

La pestaña **Configuración alternativa**, disponible en las propiedades IPv4 de una tarjeta de red, permite especificar el componente del cliente Windows 10 en caso de indisponibilidad de un servidor DHCP. El usuario puede elegir entre utilizar la dirección IP privada automática o especificar una dirección IP alternativa manualmente.

Para definir una configuración IP alternativa, siga el procedimiento descrito a continuación:

- Desde el escritorio, pulse las teclas  y **R** y, a continuación, introduzca **ncpa.cpl** en la ventana **Ejecutar** y confirme con [Intro].
- En la ventana **Conexiones de red**, seleccione la tarjeta sobre la que desea definir una configuración de red alternativa, haga clic con el botón derecho y, a continuación, seleccione **Propiedades**.
- En la ventana **Propiedades de Ethernet**, seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** y haga clic en el botón **Propiedades**.
- Seleccione la pestaña **Configuración alternativa**, a continuación marque la opción **Configurada por el usuario** y rellene los campos **Dirección IP**, **Máscara de subred**, **Puerta de enlace predeterminada**, **Servidor DNS preferido**. Por último, marque la opción **Validar configuración (si hay cambios) al salir** para verificar la configuración.




→ Confirme haciendo clic en el botón **Aceptar**.

# Resolución de nombres

Es más fácil recordar el nombre de un sitio que su dirección IP con sus cuatro números: por ejemplo, la dirección IP 173.194.41.215 corresponde actualmente al nombre de dominio `www.google.es`, mucho más fácil de recordar. Un proceso de resolución consiste simplemente en convertir una dirección IP en un nombre.

Un nombre de ordenador (o nombre de host) que utilice el sistema de nombres de dominio puede contener hasta 255 caracteres, con caracteres alfanuméricos, puntos y guiones. Es el sistema utilizado en Internet a través de una resolución DNS (*Domain Name System*).

Un nombre NetBIOS contiene 16 caracteres y utiliza el servicio WINS (*Windows Internet Naming Service*) para resolver sus peticiones.

 Desde Windows 2000, Microsoft aconseja activamente dar prioridad al uso de Active Directory y DNS por encima de WINS, servicio que ha quedado obsoleto.

Windows 10 soporta la resolución de nombres DNS y WINS.

## 1. Sistema de nombres de dominio

Inventado en los años 80, el sistema de nombres de dominio (o DNS) es un servicio que resuelve los nombres de host convirtiéndolos en direcciones IP, y viceversa. Windows 10 utiliza DNS para buscar controladores de dominio Active Directory, recursos como servidores de mensajería (registro MX [*Mail eXchanger*]) y para conectarse a los otros clientes.

Cuando un cliente Windows 10 intenta resolver un nombre de equipo DNS, realiza las siguientes etapas:

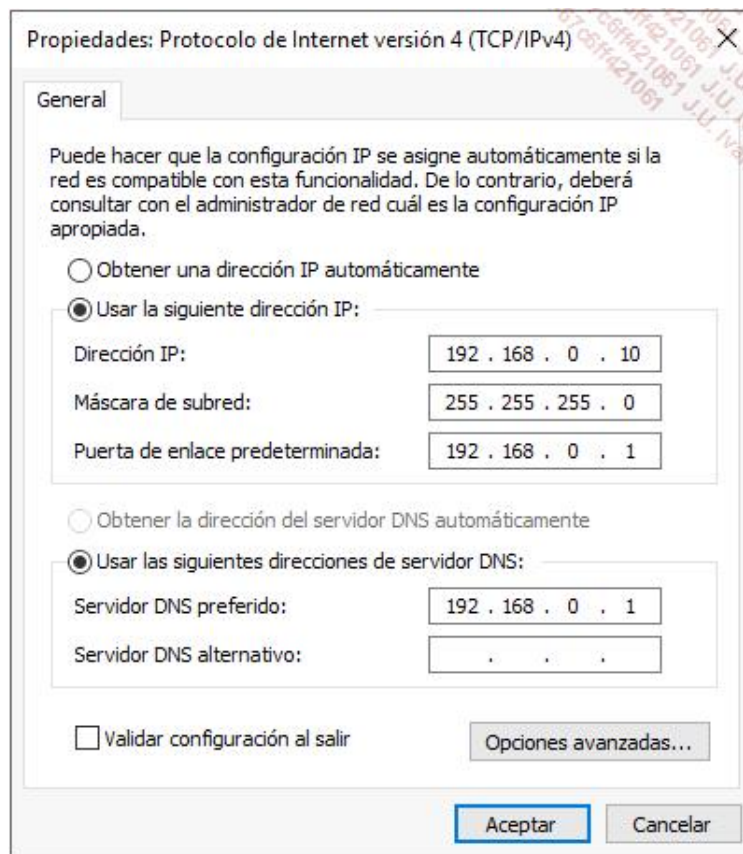
1. ¿Es el nombre solicitado su propio nombre?
2. Se verifica el nombre de host y su correspondencia en el archivo **hosts** local almacenado en la carpeta `%systemroot%\System32\drivers\etc\`.
3. Se trata de resolver desde la caché de DNS: comando **ipconfig /displaydns** para visualizarlo, **ipconfig /flushdns** para vaciar su contenido.
4. Se interroga a los servidores DNS.
5. Si el nombre no se puede resolver, la petición puede redirigirse al servidor WINS.

 El sistema DNS es una parte esencial de un dominio Active Directory Windows Server 2008 o Windows Server 2012, se encuentra perfectamente integrado con el servicio **Dynamic DHCP**, que se encarga de registrar en el DNS las nuevas direcciones IP de los ordenadores.

Para definir la dirección IP de un servidor DNS primario (servidor preferido para la resolución de nombres) en un puesto con Windows 10, puede utilizar el comando netsh desde un símbolo del sistema:

```
netsh interface ipv4 set dnsservers "Ethernet" static 192.168.0.2 primary
```

Puede utilizar también la interfaz gráfica de las propiedades de la tarjeta de red.



Para acceder a una carpeta compartida llamada **Cursos**, situada en un servidor remoto **SRV1** (dirección IP **192.168.0.10**) gestionado por el sistema DNS en un dominio **jjosoft.es**, utilice cualquiera de las siguientes opciones:

- **\\SRV1.jjosoft.es\Cursos**
- **\\192.168.0.10\Cursos**
- **File://192.168.0.10/Cursos**

Si el servidor remoto también funciona como servidor web (rol IIS):

- **http://SRV1.jjosoft.es/Cursos/**

## 2. Windows Internet Name Service

WINS es un servicio que permite resolver nombres NetBIOS en direcciones IPv4. Al igual que DNS, WINS proporciona una base de datos centralizada que almacena las correspondencias, comunicándose si es necesario con un servidor DHCP para gestionar una lista actualizada de nombres NetBIOS.

El cliente Windows 10 permite también resolver una petición WINS empleando su archivo local **LMHOSTS** (%systemroot%\System32\drivers\etc\), que tiene la correspondencia entre las direcciones IP y los nombres NetBIOS de los servidores remotos con los que desea comunicarse empleando el protocolo TCP/IP.

El proceso de resolución WINS es el siguiente:

1. ¿Es el nombre solicitado su propio nombre?

2. Se verifica la caché de nombres remotos. Cada nombre resuelto se aloja en la caché durante 10 minutos, luego se elimina.
3. Se realiza una solicitud al servidor WINS.
4. Se realiza una difusión en el conjunto de la red.
5. Se verifica el archivo LMHOSTS.
6. Se envía la solicitud, en último recurso, a un DNS si está configurado.

Para obtener la dirección IP de un servidor WINS proporcionada por un servidor DHCP, utilice el comando netsh siguiente en un símbolo del sistema:

**netsh interface ipv4 set winsservers name="Ethernet" source=dhcp**

Puede utilizar también la interfaz gráfica de las propiedades de la tarjeta de red.

WINS es una tecnología cada vez menos usada para resolver los nombres de hosts. DNS es su sucesor.