

Redes Locales - 1º SMR

Tema 3: Instalación / configuración de los equipos de red

Por May Calle

3.1 Procedimientos de instalación.....	1
3.2 Adaptadores de red y controladores de dispositivos	2
3.2.1 Adaptadores de red.....	2
3.2.2 Controladores de dispositivos.....	4
3.3 Protocolos.....	5
3.4 TCP/IP. Estructura. Clases IP.....	5
3.4.1 Características del protocolo IP.....	6
3.5 Direcciones IP. IPv4. IPv6.....	6
3.5.1 Direcciones IP.....	6
3.5.2 IPv4.....	6
3.5.3 IPv6.....	8
3.6 Asignación de direcciones IP. Máscaras de red. Segmentación de redes.....	10
3.6.1 Direcciones IP, máscaras de red y gateway por defecto.....	10
3.6.2 Dirección de red y de broadcast.....	11
3.6.3 Clases de direcciones IP.....	12
3.6.4 Direcciones IP públicas y privadas.....	14
3.6.5 Segmentación de redes.....	16
3.7 Configuración de los adaptadores de red en sistemas operativos libre y propietarios.....	22
3.7.1 Determinar la dirección IP, máscara y gateway de un equipo.....	22
3.7.2 Configurar manualmente la dirección IP, máscara y gateway.....	23
3.8 Asignación automática de direcciones IP: DHCP	28
3.9 Sistema de nombres de dominio (DNS).....	30
3.9.1 Nslookup.....	31
3.10 Introducción a los recursos compartidos.....	33
3.10.1 Compartir carpetas.....	36
3.10.2 Montar una unidad de red.....	37

3.1 Procedimientos de instalación

Hoy en día realizar la instalación de una red local es bastante sencillo. Los sistemas operativos actuales detectan automáticamente el hardware instalado. Esto facilita la instalación del hardware de red (tarjeta de red, switch, router, etc). Además, los dispositivos de red suelen venir con una configuración por defecto que permite, en muchos casos, que la red funcione simplemente conectando los dispositivos.

Por ejemplo, Windows 10 reconoce las tarjetas de red automáticamente, y marca por defecto la opción de obtener la configuración de red de forma automática para cada equipo de la red. En redes domésticas, la tarea de proporcionar una configuración de red de forma automática la suele realizar el mismo router que proporciona acceso a Internet, mientras que en redes más grandes, esta tarea la realiza uno de los equipos conectados a la red. En ambos casos, se resuelve gracias a un determinado servicio de red denominado DHCP, que estudiaremos más adelante.

3.2 Adaptadores de red y controladores de dispositivos

3.2.1 Adaptadores de red

El adaptador de red, tarjeta de red o NIC (*Network Interface Card*) es un dispositivo electrónico que permite a un terminal (ordenador, impresora...) acceder a una red y compartir recursos (datos o dispositivos). Hay diversos tipos de adaptadores de red en función del tipo de cableado o arquitectura que se utilice en la red.

Cada tarjeta de red tiene un número de identificación único de 48 bits en hexadecimal que asignan los fabricantes legales de hardware llamado dirección MAC (*Media Access Control*; control de acceso al medio) también conocido como dirección física.

Estas direcciones únicas de hardware son administradas por el “Instituto de Ingeniería Eléctrica y Electrónica” (*IEEE, Institute of Electronic and Electrical Engineers*). Los tres primeros octetos (24 bits) del número MAC, identifican al proveedor específico y es conocido como número OUI (*Organizationally unique identifier, identificador único de organización*) y es designado por el IEEE. El OUI combinado con otro número de 24 bits forman la dirección MAC completa.

Las características de la tarjeta de red definen en parte, las características de la red. Al escoger e instalar una NIC se deben tener en cuenta algunas características como la velocidad de conexión, tipo de conexión, conectores y topología, normas compatibles y sistemas operativos en qué funciona.

3.2.1.1 Adaptadores para red cableada e inalámbrica

Las tarjetas de red para red **cableada** deben tener un puerto para conectar los cables. Hay diversos tipos de adaptadores en función del tipo de cableado (coaxial fino, coaxial grueso, etc) o arquitectura de red que se utilice (por ejemplo, Token Ring), pero actualmente el más común es el adaptador tipo Ethernet con conector RJ45.



Tarjeta de red con conector RJ45



Tarjeta de red con conector RJ45 y BNC

Hay adaptadores Ethernet disponibles en USB o tarjeta PCI, resultan útiles si el equipo no tiene conectores LAN o si se necesitan más.

Los adaptadores para redes **inalámbricas** no disponen de conexión para red cableada y transmiten información de manera inalámbrica mediante tecnología WiFi.

3.2.1.2 Tipos de adaptadores según su conexión al PC

A continuación se indican las distintas formas de conectar un adaptador de red al equipo. En todas ellas, disponemos tanto de adaptadores para red cableada como inalámbrica.

USB

Son muy fáciles de usar e instalar. Se conectan a cualquier puerto USB. Hay versiones con un tamaño como el de un pendrive y otros micro o mini, bastante más pequeños. Se usan principalmente en ordenadores portátiles que no tengan el WiFi integrado (en general, modelos antiguos), aunque también sirven para ordenadores de sobremesa que quieran conectarse a Internet de forma inalámbrica, e incluso para equipos que no tengan conexión Ethernet, facilitando un adaptador USB a Ethernet.



Adaptador de red USB



Adaptador USB a Ethernet RJ45

CardBus, PCMCIA ó PC Cards

En general, sólo pueden utilizarse en ordenadores portátiles. Tienen una forma parecida a una tarjeta de crédito. Se conectan en unas ranuras específicas que incluyen algunos portátiles. Su ventaja es que no sobresale y permiten dejar libre un conector USB para usarlo con otros dispositivos.



Adaptador de red PCMCIA para redes cableadas



Adaptador de red PCMCIA para redes inalámbricas

Adaptadores PCI o PCI Express

Se orientan a ordenadores de sobremesa. Como su nombre indica, hay que insertarlos en ranuras PCI ó PCI Express de la placa base. Algunos sirven para conexiones WiFi. Hay modelos con antenas y otros que no las tienen aunque sean también para conexiones inalámbricas. Otros adaptadores PCI incluyen conectores Ethernet para conexiones cableadas.



Adaptador de red PCI para redes cableadas



Adaptador de red PCI Express para redes inalámbricas

Adaptadores PowerLine o PLC

La tecnología PowerLine es poco conocida aunque tiene mucho que ofrecer. Permite transmitir los datos a través de los mismos cables que usa la instalación eléctrica. Con estos adaptadores cualquier enchufe eléctrico de la casa se transforma en un adaptador de red. Tienen unas clavijas para conectarlos a los enchufes y conectores Ethernet para conectarlos a un PC u otros dispositivo. Su uso es adecuado para casos en los que a la señal inalámbrica le falta intensidad o tiene baja cobertura.



Adaptador PowerLine para redes cableadas e inalámbricas

Ejercicios propuestos

3.2.1 Para cada uno de los adaptadores vistos en el apartado anterior, compara precios entre dos ó tres adaptadores del mismo tipo (USB, PCMCIA, PCI, PCI Express y PowerLine) indicando foto del dispositivo, marca, modelo, características, precio y enlace dónde has encontrado dicha información.

3.2.2 Indica, según tu opinión, cuáles son las principales ventajas y desventajas de cada tipo de adaptador.

3.2.2 Controladores de dispositivos

Cuando el sistema operativo no detecta automáticamente el hardware instalado, hay que instalar los controladores o drivers del fabricante. Un driver no es más que un software que permite al sistema operativo interactuar con un determinado dispositivo.

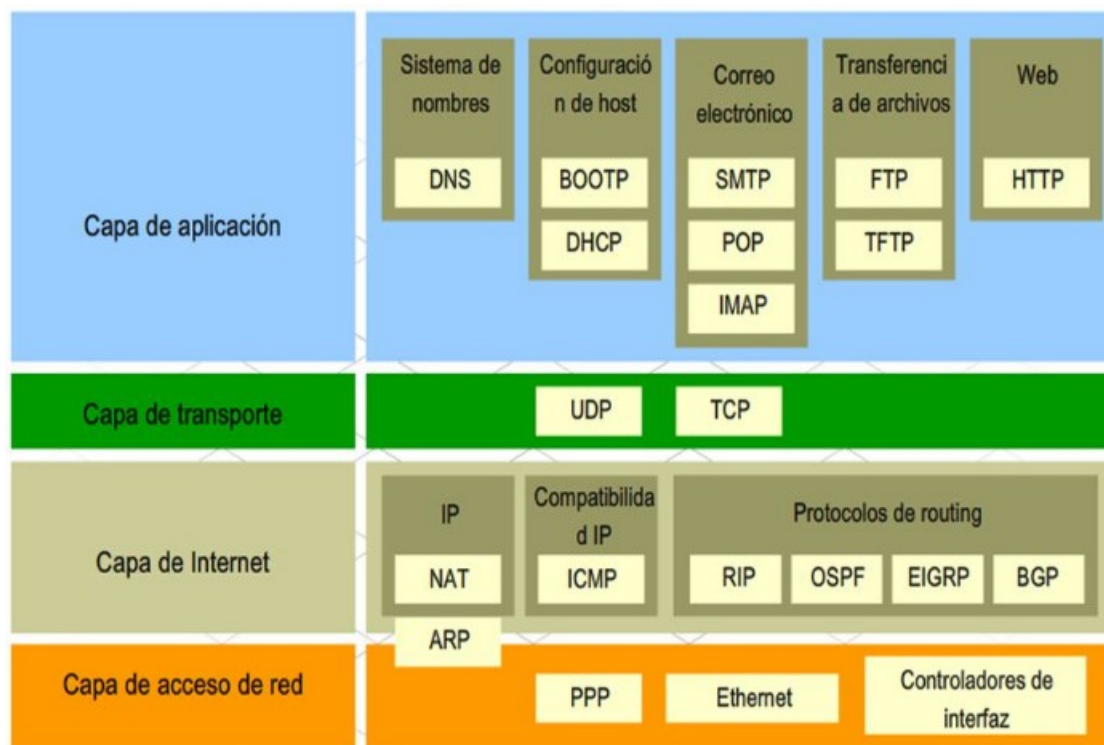
Por otro lado, existen los packet driver que son unos tipos de drivers genéricos empleados en la familia de sistemas operativos Windows que proporcionan una interfaz de comunicación común del sistema con cualquier tipo de tarjeta de red que se le conecte. De esta forma, se evita el tener que buscar e instalar los drivers específicos de cada tarjeta, pero a cambio es posible que no se exploten al máximo las capacidades de la tarjeta de red.

3.3 Protocolos

Los protocolos usados en las redes de comunicación son un conjunto de reglas que permiten a dos máquinas comunicarse entre sí en una red aunque tengan una arquitectura y sistemas operativos diferentes. Están adaptados a las características del emisor, el receptor y el canal, además deben definir los detalles de cómo transmitir y entregar un mensaje. Para que dos máquinas puedan establecer una comunicación deben emplear los mismos protocolos. Éstos pueden estar implementados con software o hardware.

El conjunto de protocolos más extendido son los de la arquitectura de red TCP/IP, que incluye todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos. Cada capa del modelo TCP/IP abarca una serie de protocolos.

A continuación se muestran los protocolos más conocidos para cada una de las capas del modelo TCP/IP.



Protocolos de modelo TCP/IP

Aparte del conjunto de protocolos TCP/IP, existen también otros conjuntos de protocolos ya más desfasados, como AppleTalk o IPX, que no veremos aquí.

3.4 TCP/IP. Estructura. Clases IP

El protocolo por excelencia de la capa de red es el protocolo de Internet o protocolo IP. Existen dos variantes o versiones del mismo: versión 4 (IPv4) y versión 6 (IPv6). La primera, más antigua, asigna direcciones lógicas de 4 bytes a los equipos de las redes, como veremos a continuación. La segunda, más reciente, amplió el nº de bytes para las direcciones lógicas, permitiendo así tener más equipos conectados. Aún sigue prevaleciendo IPv4 en las redes de todo el mundo, aunque en algunos casos se está incorporando ya IPv6.

3.4.1 Características del protocolo IP

En cualquiera de sus versiones, el protocolo IP fue concebido para minimizar la sobrecarga de la red y la información que se añade en los paquetes, y por tanto sus características principales son:

- Es un protocolo sin conexión, es decir, no establece ninguna relación ni canal de comunicación entre origen y destino del mensaje, sino que se limita a enviar paquetes de uno a otro sin importar el camino. Sería equivalente a enviar una carta a alguien sin avisarle previamente de que se la vamos a enviar. El servicio postal, cuando recibe la carta, no sabe si el destinatario está disponible, si vive donde decimos o si se la podrá hacer llegar.
- No es confiable (no se garantiza que los paquetes lleguen al destino). Volviendo al símil de la carta, sería como enviar una carta sin remitente. Si por lo que sea el servicio de correos no localiza al destinatario, o el contenido del sobre se deteriora, no tiene forma de hacernos saber que no se ha podido hacer llegar la carta en condiciones a su destino. Para garantizar

esta confiabilidad, existen mecanismos y protocolos específicos en la capa de transporte (protocolo TCP).

- Es independiente de los medios físicos por los que circulan los paquetes. Es responsabilidad de la capa de enlace preparar los paquetes para ser enviados por los medios concretos por los que vayan a circular.

3.5 Direcciones IP. IPv4. IPv6

3.5.1 Direcciones IP

Hemos visto en la capa de enlace que, con el fin de evitar saturar una red de mensajes innecesarios, conviene dividir las redes grandes en subredes más pequeñas, y que cada una se ocupe de gestionar sus propios mensajes, y procesar las direcciones MAC de los equipos conectados a esa red. Pero, ¿qué pasa cuando queremos enviar un mensaje desde una red a otra? ¿O cuando un equipo cambia de red? Podemos establecer una similitud entre este hecho y las personas: el DNI de una persona no cambia, siempre es el mismo, y además no hay dos iguales. Sería el equivalente a su "dirección MAC". Sin embargo, esa persona puede vivir en lugares diferentes a lo largo de su vida, e incluso podría vivir en una calle que se llamase igual, pero en ciudades diferentes en momentos diferentes. Lo mismo ocurre con los equipos, podemos asignarles un tipo de dirección, llamada dirección lógica que puede variar en función de la red a la que están conectados. Esta dirección lógica, también llamada **dirección IP**, permite identificar equipos de otras redes, y enviarles mensajes.

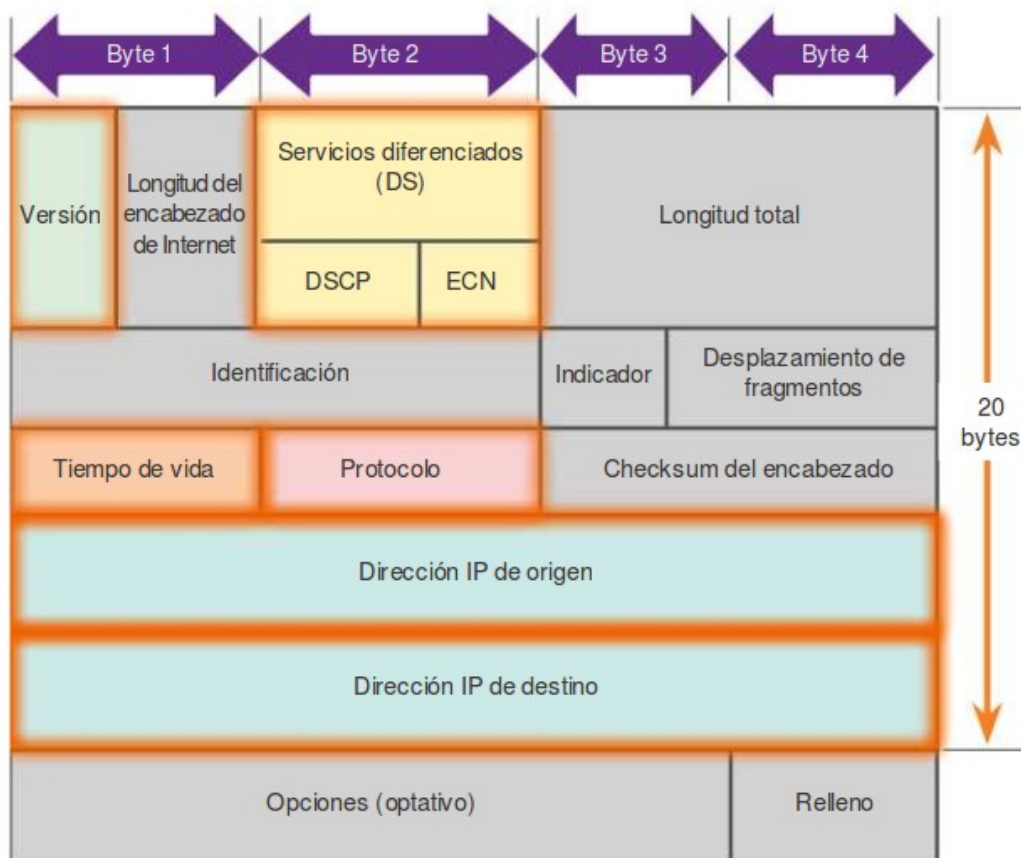
3.5.2 IPv4

El protocolo IPv4 fue concebido a principios de los años 80 para asignar una dirección lógica a todos los equipos conectados a una red. Consiste básicamente en una dirección de 4 bytes que identifica de forma unívoca a cada equipo de la red. En sus inicios, existían pocas conexiones a la red, y cada equipo podía tener su dirección propia y diferente al resto. Hoy en día, este protocolo presenta una serie de limitaciones importantes que veremos más adelante.

Los paquetes IPv4 constan de dos partes: el **encabezado**, con información relacionada con las características del paquete, y el **contenido**, con la información que le llega de la capa de transporte y los datos propiamente dichos.

3.5.2.1 Encabezado IPv4

Los campos que incluye el encabezado IPv4 son los siguientes:



A continuación se explican cada uno de los campos:

- **Versión:** sirve para identificar la versión del paquete IP. Para los paquetes IPv4, este campo siempre tiene el valor 0100.
- **Servicios diferenciados (DS):** se utiliza para indicar la prioridad de cada paquete.
- **Longitud total:** indica el tamaño total del paquete (fragmento), incluidos el encabezado y los datos, en bytes. La longitud mínima del paquete es de 20 bytes (encabezado de 20 bytes + 0 bytes de datos), y la máxima es de 65535 bytes.
- **Tiempo de vida (TTL):** es una especie de contador que se va decrementando cada vez que el paquete pasa por un router, para que, en caso de que no se encuentre el destinatario, en algún momento el contador llegue a 0 y el paquete se destruya y no se quede vagando por la red.
- **Protocolo:** indica el tipo de datos que transporta el paquete, lo que permite a la capa de red pasar los datos al protocolo de capa superior correspondiente. Los valores comunes son ICMP, TCP y UDP.
- **Checksum del encabezado:** se utiliza para la verificación de errores del encabezado IP. El checksum del encabezado se vuelve a calcular en el receptor y se compara con el valor en el campo checksum del paquete. Si los valores no coinciden, se descarta el paquete.
- **Dirección IP de origen:** dirección IP del emisor del paquete.
- **Dirección IP de destino:** dirección IP del receptor del paquete.

Los campos **Identificación**, **Indicador** y **Desplazamiento de fragmentos** se emplean cuando un router debe fragmentar el paquete para poder reenviarlo a otro medio con una unidad máxima de transferencia inferior. Se utilizan para poder reconstruir el paquete original sin fragmentar. Por ejemplo, en redes de fibra óptica (FDDI) la unidad máxima de transferencia es de 4470 bytes mientras que en redes Ethernet el tamaño habitual es de 1500 bytes. Por lo que al pasar de un medio a otro, sería necesario fragmentar los paquetes.

3.5.2.2 Limitaciones

Con el tiempo, se ha visto que el protocolo IPv4 tiene una serie de limitaciones importantes:

- Por un lado, la cantidad de direcciones IP que se pueden obtener con esos 4 bytes puede llegar a ser insuficiente para el total de la población mundial (podríamos obtener un total de 2^{32} = algo más de 4 mil millones de direcciones, sin descontar direcciones de red o broadcast).
- Además, los routers almacenan en tablas internas por dónde redirigir los paquetes a sus destinos. El aumento del número de direcciones IP consume cada vez más recursos de los routers.
- Finalmente, debido a la limitación o escasez de direcciones, en entornos domésticos o privados se acude normalmente a la traducción de direcciones (NAT), mediante la cual varios equipos con direcciones privadas comparten una única dirección pública de salida a Internet. Esto también sobrecarga de trabajo al router, que cuando recibe paquetes de fuera debe traducir a cuál de sus ordenadores internos va dirigido.

Para intentar paliar estos problemas, se propusieron algunas alternativas. Una de ellas fue el desarrollo de un nuevo protocolo de Internet, IPv6, cuyas características veremos a continuación.

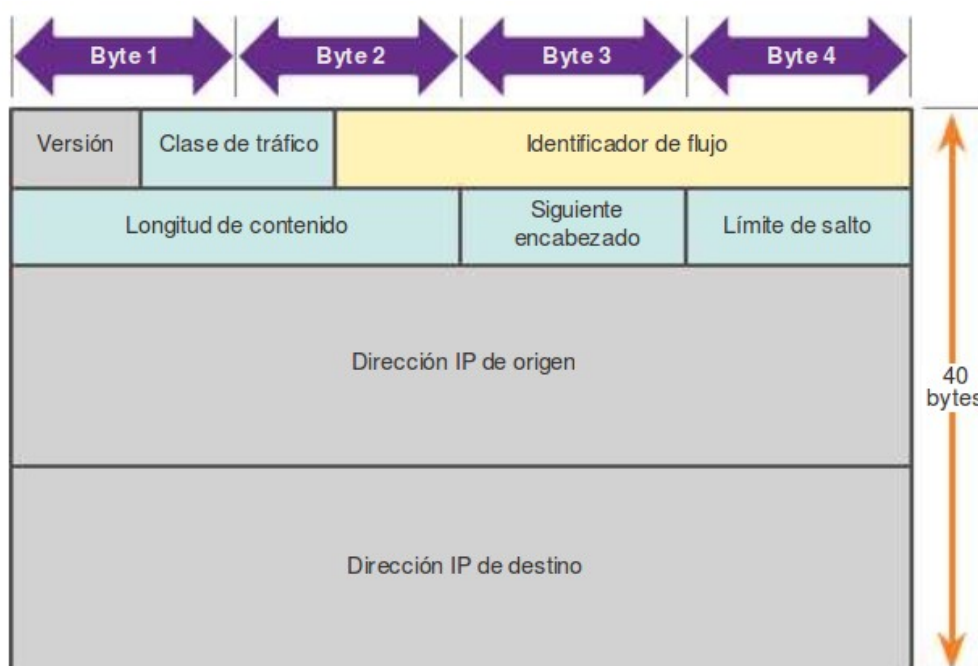
3.5.3 IPv6

Durante los años 90, y conscientes del inminente problema que se avecinaba con IPv4, el Internet Engineering Task Force (IETF) comenzó a buscar una alternativa, que cristalizó en el desarrollo del nuevo protocolo IPv6. Como mejoras respecto a su predecesor, podemos citar las siguientes:

- Más espacio de direcciones disponibles, ya que las direcciones IPv6 constan de 16 bytes en lugar de 4.
- Encabezados más simples, lo que supone también menos carga de trabajo en los routers para procesarlos.
- Eliminación de la necesidad de NAT. Con tal cantidad de direcciones IPv6 públicas, no se necesita traducción de direcciones de red (NAT) ya que cada equipo puede tener su propia dirección IPv6.
- Seguridad integrada. IPv6 admite capacidades de autenticación y privacidad de forma nativa.

3.5.3.1 Encabezado IPv6

Los campos que incluye el encabezado IPv6 son los siguientes:



Vemos que se simplifican muchos campos. A continuación se explican cada uno de los campos:

- **Versión:** campo de 4 bits que identifica la versión del paquete IP. Para los paquetes IPv6, este campo siempre tiene el valor 0110.
- **Clase de tráfico:** campo de 8 bits equivalente al campo Servicios diferenciados (DS) de IPv4. Se utiliza para clasificar paquetes y controlar la congestión del tráfico.
- **Identificador de flujo:** campo de 20 bits que proporciona un servicio especial para aplicaciones en tiempo real. Se puede utilizar para indicar a los routers y switches que deben mantener la misma ruta para el flujo de paquetes, y así evitar que estos se reordenen.
- **Longitud de contenido:** campo de 16 bits equivalente al campo Longitud total del encabezado de IPv4.
- **Siguiendo encabezado:** campo de 8 bits equivalente al campo Protocolo de IPv4. Indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente.
- **Límite de saltos:** campo de 8 bits que reemplaza al campo TTL de IPv4. Cuando cada router reenvía un paquete, este valor disminuye su valor en uno. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje de ICMPv6 al host emisor en el que se indica que el paquete no llegó a su destino.
- **Dirección IP de origen:** campo de 128 bits que identifica la dirección IPv6 del host emisor.
- **Dirección IP de destino:** campo de 128 bits que identifica la dirección IPv6 del host receptor.

Los paquetes IPv6 también pueden contener **encabezados de extensión (EH)**, que proporcionan información optativa de la capa de red.

3.6 Asignación de direcciones IP. Máscaras de red. Segmentación de redes

3.6.1 Direcciones IP, máscaras de red y gateway por defecto

Las direcciones IP más recientes (IPv6) están formadas por 16 bytes, como hemos dicho anteriormente. Se representan normalmente mediante 32 dígitos hexadecimales, agrupados de cuatro en cuatro, y separados por dos puntos. Por ejemplo:

2001:0db8:3c55:0015:0a2b:1a00:abdf:ff12

Sin embargo, este tipo de direcciones aún no está demasiado difundido, y suele predominar más el formato IPv4, por lo que nos centraremos en este último.

Las direcciones IP tradicionales (IPv4) están formadas por 4 bytes (32 bits), representados en formato decimal, separando cada byte con un punto. Por ejemplo: 193.155.52.211

La **dirección IP** se divide, a su vez, en dos partes:

- Una parte que **identifica a la red** donde está conectado el equipo
- Otra parte que **identifica al equipo dentro de la red** a la que pertenece

Para determinar qué parte de la dirección IP es de la red y cuál del equipo, se emplea otra secuencia de 4 bytes llamada **máscara de red**. Dicha máscara debe cumplir un patrón determinado: debe estar formada por una secuencia de unos seguida de una secuencia de ceros. Dicho de otra forma, los 4 bytes se estructuran en un grupo de unos seguido de un grupo de ceros.

Las tres máscaras de red más habituales son:

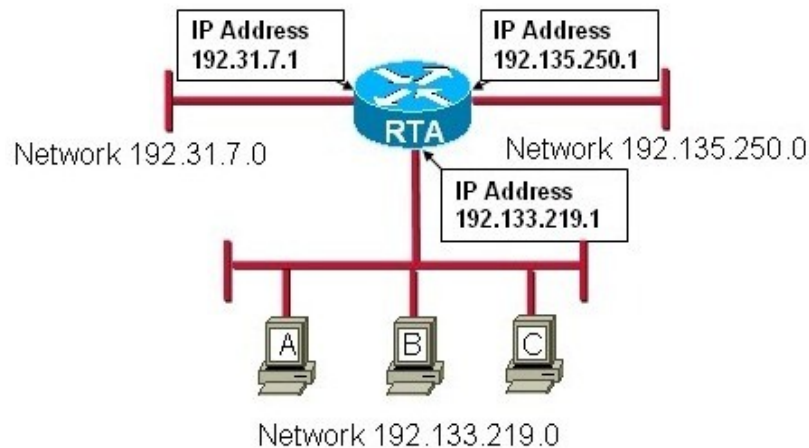
- 255.0.0.0 (a unos el primer byte y a ceros el resto)
- 255.255.0.0 (a unos el primer y segundo byte y a ceros el resto)
- 255.255.255.0 (a ceros el cuarto byte y a unos el resto)

Estas tres máscaras se pueden representar de forma abreviada indicando cuántos bits tienen a uno. Se representarían como /8, /16 o /24, respectivamente.

¿Cómo se interpretan las máscaras? Los bits que están a uno corresponden a los bits de red en la dirección IP, y los bits a cero corresponden a los bits de equipo. Así, por ejemplo, si un equipo tiene la dirección IP 192.168.1.13 y la máscara 255.255.255.0 (lo que podríamos representar de forma abreviada como 192.168.1.13 /24), quiere decir que sus tres primeros bytes (192.168.1) identifican la red a la que pertenece, y el último byte (13) identifica al equipo dentro de esa red. Si queremos conectar otro equipo a la misma red, deberá tener la misma parte de red (192.168.1) y variar el byte asignado a los equipos (en lugar de 13, otro número como por ejemplo 14).

En el caso de que la parte de red de una IP no coincida con las de los equipos de una red, eso significará que pertenece a una red diferente (es decir, por lo general, estará en otra ubicación). En ese caso, debemos indicar una vía de salida de la red actual, en busca de la red a la que pertenece ese equipo. Esa vía de salida se conoce como **puerta de enlace predeterminada o gateway por defecto**. Normalmente, este gateway es la dirección IP del router, en el puerto conectado a la red actual.

Veámoslo con este ejemplo:



Los equipos de la red inferior tienen una dirección IP con la estructura 192.133.219.x, donde la primera parte (192.133.219) corresponde a la parte de red, y la x serán las direcciones de los equipos. Si queremos enviar un mensaje a un equipo con la dirección IP 192.31.7.15, por ejemplo, los equipos de la red comprobarán que su estructura no corresponde con la de su red. En ese caso, enviarán el paquete al gateway por defecto de esa red, que es la IP del router en esa red (192.133.219.1). Una vez allí, el router examinará sus tablas de enrutamiento, buscando por dónde enviar el mensaje a la red 192.31.7, y lo encaminará hacia allí.

3.6.2 Dirección de red y de broadcast

Dentro de los bits asignados a los equipos, existen dos combinaciones que no podemos utilizar para asignar direcciones IP a equipos:

- **Todos los bits de equipo a 0.** Esta dirección resultante, denominada **dirección de red**, se utiliza para identificar la red. En el ejemplo anterior, 192.168.1.0 sería la dirección de red del ejemplo, y no podría asignarse a ningún equipo
- **Todos los bits de equipo a 1.** Esta dirección, denominada **dirección de broadcast**, se utiliza para realizar envíos a todos los equipos de la red. En el ejemplo anterior, 192.168.1.255 sería la dirección de broadcast de la red, y tampoco podría asignarse a ningún equipo.

Las direcciones IP comprendidas entre la dirección de red y la dirección de broadcast son direcciones válidas para asignar a los hosts.

Ejercicios propuestos

3.6.1 Suponiendo una máscara de 255.255.0.0, indica dos IPs válidas para la red 172.17.0.0 (que no sean ni de red ni de broadcast)

3.6.2 Suponiendo una máscara de 255.255.255.0, ¿cuál sería la dirección de red para los equipos de la red 175.12.52.X?

3.6.3 Supón una máscara de 255.0.0.0.

a) Inventa una IP de red para esa máscara

b) Indica 2 direcciones IP válidas para equipos de esa red (que no sean ni de red ni de broadcast)

c) ¿Cuál sería la dirección de broadcast de esa red?

3.6.3 Clases de direcciones IP

Combinando las tres máscaras de red más comunes con los distintos valores que pueden tomar los bytes en una dirección IP, dividimos el rango de direcciones IP en clases, según la siguiente tabla:

Clases de dirección IP					
Clase de dirección	Rango del primer octeto (decimal)	Bits del primer octeto (los bits verdes no se modifican)	Partes de una dirección correspondientes a la red (R) y al host (H)	Máscara de subred por defecto (decimal y binaria)	Cantidad posible de redes y hosts por red
A	De 1 a 127	00000000 - 01111111	R.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 redes ($2^{17}-2$) 16 777 214 hosts por red ($2^{24}-2$)
B	De 128 a 191	10000000 - 10111111	R.R.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16 382 redes ($2^{14}-2$) 65 534 hosts por red ($2^{16}-2$)
C	De 192 a 223	11000000 - 11011111	R.R.R.H	255.255.255.0 11111111.11111111.11111111.00000000	2097,150 redes ($2^{21}-2$) 254 hosts por red (2^8-2)
D	De 224 a 239	11100000 - 11101111	No es para uso comercial como host		
E	De 240 a 255	11110000 - 11111111	No es para uso comercial como host		

- Las direcciones de clase A se emplean para redes grandes, que tengan muchos equipos (por eso se dejan 3 bytes para equipos en la máscara asociada)
- Las direcciones de clase B se emplean para redes medianas (2 bytes para equipos)
- Las direcciones de clase C se emplean para redes pequeñas (1 byte para equipos)
- Las clases D y E se emplean para ciertos tipos de aplicaciones y envíos (aplicaciones o juegos multicast, direcciones experimentales, etc.).

Ejercicios propuestos

3.6.4 ¿A qué clase pertenecen cada una de estas direcciones IP?

- a) 215.34.12.1
- b) 42.3.115.2
- c) 245.115.2.5
- d) 132.56.7.8
- e) 225. 223.2.1
- f) 0.130.12.45
- g) 192.256.15.2

3.6.5 ¿Cuántos equipos admitiría, como máximo, una red que use direcciones de clase C?

3.6.6 Si tenemos la dirección de red 195.0.5.0 y la máscara 255.255.255.0

a) ¿Qué rango de direcciones IP pueden tener los equipos en esa red?

b) ¿Cuál es la dirección de broadcast de la red?

3.6.7 Si tenemos la dirección de red 180.4.0.0 y la máscara 255.255.0.0:

a) ¿Qué rango de direcciones IP pueden tener los equipos en esa red?

b) ¿Cuál es la dirección de broadcast de la red?

3.6.8 Si tenemos la dirección de red 10.30.0.0 y la máscara de subred 255.255.0.0

a) ¿Qué rango de IP podrán tener los hosts de esa red?

b) ¿Cuántas redes podríamos tener con esa máscara?

c) ¿Cuántos hosts por red?

3.6.9 Si tenemos la dirección de red 190.32.132.0 y la máscara de subred 255.255.252.0:

a) ¿Qué rango de IP podrán tener los hosts de esa red?

b) ¿Cuántas redes podríamos tener con esa máscara?

c) ¿Cuántos hosts por red?

3.6.10 El PC con la IP 192.168.25.13 / 24 ¿En qué subred se encuentra?

3.6.11 El PC con la IP 172.48.27.3 /22 ¿En qué subred se encuentra?

3.6.12 Queremos montar una red que pueda tener hasta 1000 equipos

a) ¿Qué clase (A, B o C) emplearías y con qué máscara de red?

b) ¿Qué clase (A, B o C) no podría emplearse en ningún caso?

3.6.4 Direcciones IP públicas y privadas

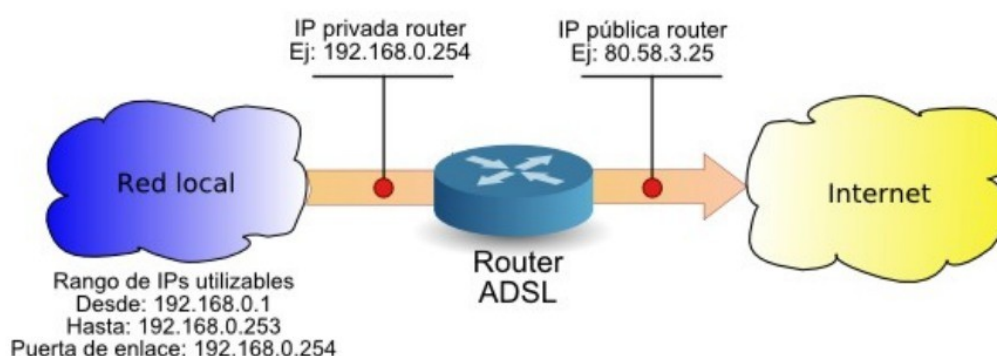
Como hemos visto antes, con el tiempo se fue viendo que la cantidad de direcciones IP que se pueden obtener con IPv4 podría llegar a ser insuficiente para el total de la población mundial. Además de desarrollar entonces el nuevo protocolo IPv6, otra alternativa que se inició de inmediato fue asignar un rango de direcciones IP dentro de cada clase (A, B y C) para uso privado. De esta forma, las empresas podrían utilizar estos rangos de direcciones en sus instalaciones, y podrían ser los mismos para diferentes empresas, ya que cada una tiene su propia red local independiente de la de la otra.

Así, se eligió un pequeño rango de direcciones IP dentro de cada clase, para uso privado e interno de las diferentes empresas o instituciones.

Clase de dirección	Cantidad de números de red reservados	Direcciones de red
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

Vemos que existe una única red privada de clase A (10.x.x.x), para empresas grandes que quiera tener todos los equipos en la misma red lógica. También existen 16 redes de clase B (desde 172.16.x.x hasta 172.31.x.x), y 256 redes de clase C (desde 192.168.0.x hasta 192.168.255.x).

Cualquier equipo que no esté directamente conectado a Internet debe hacer uso de estas direcciones privadas, mientras que los routers o equipos directamente conectados a Internet tendrán asociadas direcciones IP públicas y diferentes al resto. Por ejemplo, en la siguiente imagen podemos ver que el router cuenta con una IP privada para comunicar los equipos de la red local (izquierda) y una IP pública que conecta con Internet (derecha).



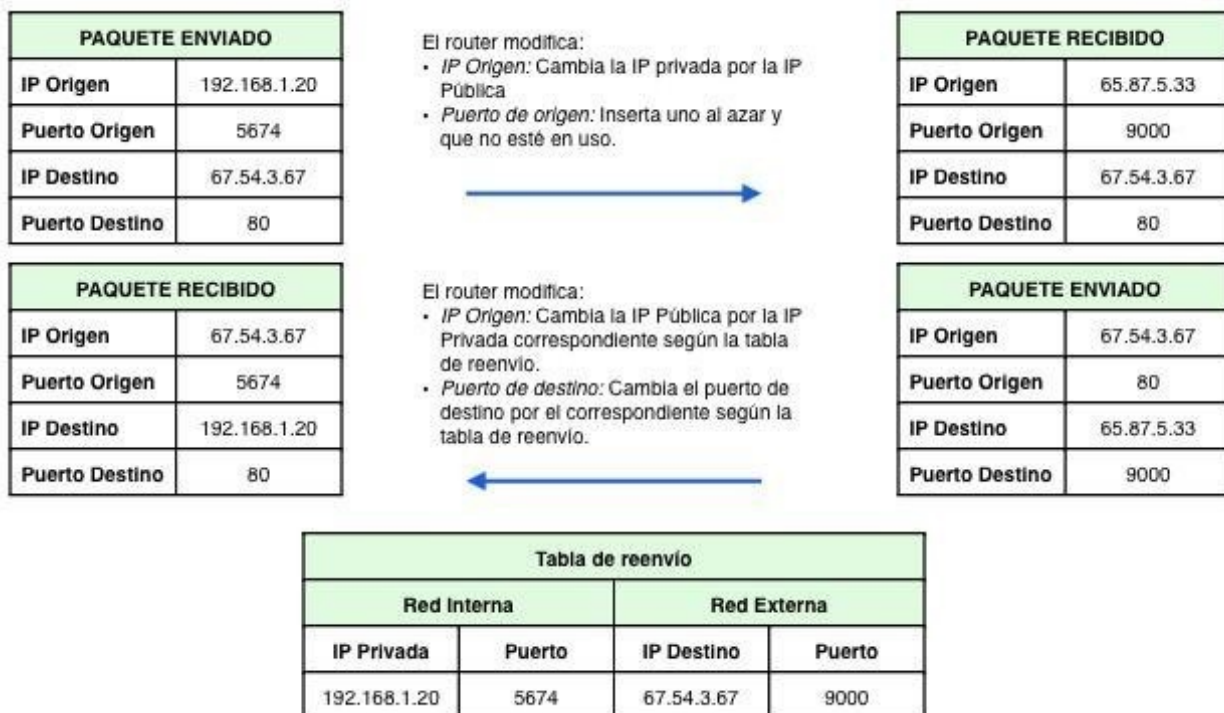
3.6.4.1 NAT: Traducción de direcciones de red

Asociado al uso de direcciones privadas y públicas tenemos la traducción de direcciones de red (NAT, *Network Address Translation*) comentada anteriormente en el apartado 3.5.2.2.

La idea básica que hay detrás de NAT es traducir las IPs privadas de la red en una única IP pública para que la red pueda enviar paquetes al exterior; y traducir luego esa IP pública de nuevo a la IP privada del PC que envió el mensaje, para que pueda recibirlo una vez llega la respuesta. Para poder hacer esto el router hace uso de los puertos lógicos.

En los protocolos de la capa de transporte se dispone de 65.536 puertos lógicos para establecer conexiones. Así, cuando una máquina quiere establecer una conexión con el exterior, el router guarda en una tabla su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar. Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.

A continuación, se muestra una imagen que ilustra el proceso:

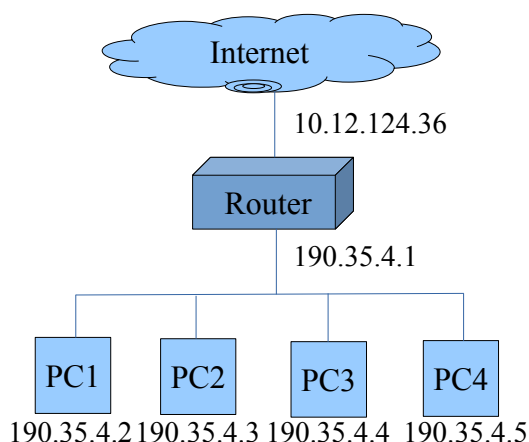


Ejercicios propuestos

3.6.13 Queremos montar 3 redes con 50, 200 y 300 equipos, respectivamente. Elige para cada una su correspondiente dirección de red, empleando la clase adecuada (A, B o C) e indica, para cada red elegida:

- La dirección de red elegida
- La máscara de red asociada
- La dirección de broadcast de dicha red
- El rango de direcciones IP que pueden tener los equipos conectados a esa red

3.6.14 Dado el siguiente esquema de conexión de una red local a Internet a través de un router, y las direcciones IP que se han asignado a cada conexión y equipo (incluyendo las conexiones del router), indica qué cosas están mal y propón una solución alternativa.



3.6.5 Segmentación de redes

Ya hemos visto cómo podemos asignar una dirección de red a una red local, y establecer direcciones IP a los equipos de la misma de forma que pertenezcan a dicha red. Para una empresa o institución, nos puede valer con una red de clase C (en el caso de que disponga de pocos hosts) o de clase B (si dispone de algunos miles de hosts).

Sin embargo, en una empresa nos puede interesar tener pequeñas redes (llamadas subredes) diferenciadas dentro, conectadas cada una a una conexión de router, de forma que cada una contenga una parte de los equipos. De hecho, las empresas suelen estar compuestas de subredes, que forman parte de una red global de la empresa (también llamada superred). A este tipo de configuración de redes, divididas en subredes conectadas por separado a los routers, se le llama **direccionamiento jerárquico**.

En este sentido, la estructura original de direcciones IP, con clases A, B y C y las máscaras por defecto para cada clase, nos puede ser insuficiente. Por ejemplo, imaginemos que tenemos una empresa con 4 redes de 20 equipos cada una. Podríamos usar direcciones de clase C, pero si a una red le asignamos por ejemplo la dirección 192.168.0.0 /24, a la siguiente la 192.168.1.0 /24, y así sucesivamente, aparte de estar desperdiciando direcciones, ¿cómo agrupamos todas estas redes en una superred que las englobe a todas?

No podríamos. Por otra parte, si optamos por una dirección de clase B como 172.16.0.0 /16, podríamos utilizar máscaras de clase C y asignar las direcciones 172.16.1.0 /24, 172.16.2.0 /24, etc. a las cuatro redes de la empresa. Pero estaríamos utilizando direcciones de clase B y su consiguiente desperdicio de direcciones, para unas pocas redes de unos pocos equipos.

Veremos ahora algunas aproximaciones que solucionan mejor este problema de creación de subredes.

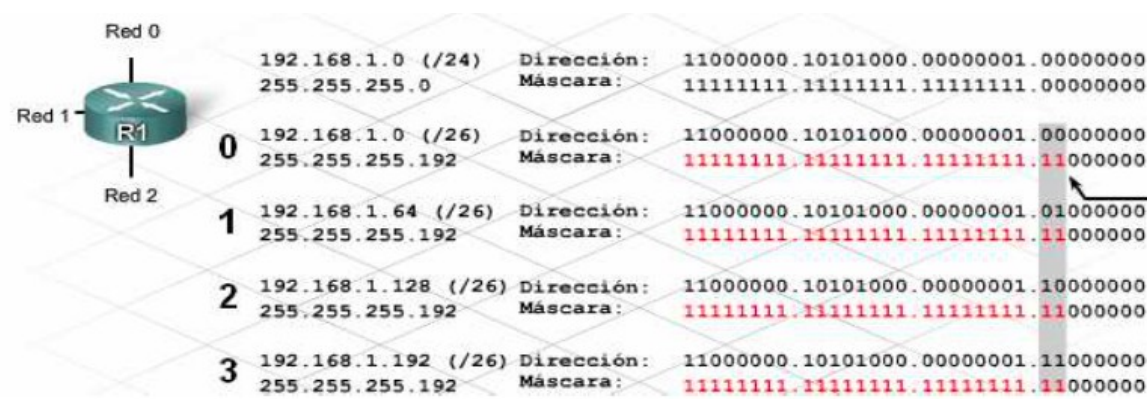
3.6.5.1 Mecanismo básico de división en subredes

La forma más básica de dividir una red en subredes consiste en tomar una dirección de red y máscara por defecto, y después tomar unos pocos bits de la parte de equipos para diferenciar las subredes. Para ello, podemos seguir estos pasos:

1. Identificar todas las subredes que queremos tener en la empresa o institución, y el número de equipos o conexiones que vamos a necesitar en cada red. Vamos a suponer un ejemplo en el que necesitemos tener tres redes, con 7, 20 y 60 equipos, respectivamente.
2. Identificamos cuántos bits nos van a hacer falta para distinguir las redes, y para dar cabida a los equipos de cada red:
 - Para distinguir las 3 redes de nuestro ejemplo, nos harán falta 2 bits (con un bit sólo podemos diferenciar $2^1 = 2$ redes, y con 2 bits podemos diferenciar hasta $2^2 = 4$ redes)
 - Para dar cabida a los equipos de cada red, nos fijamos en la red con más equipos (60, en nuestro caso). A esos equipos hay que sumarles las direcciones de red y broadcast

(cuyas IPs no podremos usar para equipos) y una IP adicional que tendrá el router conectado a esa red (el gateway por defecto). Por lo tanto, necesitaremos un rango de $60 + 3 = 63$ direcciones IP en total. Esto se consigue con 6 bits, ya que $2^6 = 64$ direcciones posibles.

3. Elegimos la clase de dirección IP que mejor se ajuste a nuestras necesidades. En este caso, como necesitaremos 2 bits para distinguir las redes y 6 para los equipos de cada red, necesitaremos un total de 8 bits (1 byte) para gestionarlo todo. Entonces, nos basta con una red de clase C, ya que dispone de 8 bits para equipos. Por ejemplo, podemos usar la dirección de red 192.168.1.0 /24.
4. Con todo lo anterior, establecemos los 4 rangos de direcciones IP partiendo de la dirección base 192.168.1.0, tomando 2 bits más para crear subredes, y los 6 restantes para asignar IPs en cada subred. Nos quedaría una división como la que se representa en esta imagen:



Esquema de direccionamiento: Ejemplo de 4 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Explicamos el proceso seguido en este último paso: partiendo de la dirección raíz 192.168.1.0 /24 (es decir, la dirección de clase C con su máscara por defecto), tomamos 2 bits más para las máscaras de las subredes (es decir, las subredes tendrán 26 bits de máscara), y esos últimos 2 bits los variamos en las direcciones de subred resultantes, para crear las cuatro subredes:

- Una será la 192.168.1.0 (red 0 en el esquema anterior, con los 2 bits extra a 00). Teniendo en cuenta que sólo podemos variar los últimos 6 bits de la dirección, eso nos deja un rango de IP válidas para equipos desde la 192.168.1.1 hasta la 192.168.1.62 (la 192.168.1.63 sería la dirección de broadcast de esta subred)
- Otra será la 192.168.1.64 (red 1, con los 2 bits extra a 01, quedando el último byte como 64 para la dirección de red). Siguiendo el mismo razonamiento de antes, las direcciones

asignables a equipos van desde la 192.168.1.65 a la 192.168.1.126 (la 127 sería la de broadcast)

- Otra será la 192.168.1.128 (red 2, con los 2 bits extra a 10, quedando el último byte como 128 para la dirección de red), con rango de IPs asignables desde la 192.168.1.129 hasta la 192.168.1.190.
- Otra (que no se utilizará, porque sólo hacen falta 3 subredes) será la 192.168.1.192 (red 3, con los 2 bits extra a 11, quedando el último byte como 192 para la dirección de red), con rango desde la 192.168.1.193 hasta la 192.168.1.254.

Estas cuatro subredes (192.168.1.0 /26, 192.168.1.64 /26, 192.168.1.128 /26 y 192.168.1.192 /26) tienen como superred a la dirección tomada inicialmente, 192.168.1.0 /24.

Ejercicios propuestos

3.6.15 Una empresa necesita dividir sus equipos en dos redes, de 60 y 90 equipos respectivamente. Indica qué dirección de superred elegirías, y qué subredes, máscaras y rangos de IPs quedarían.

3.6.16 Repite los pasos del ejercicio anterior para otra empresa con cinco subredes de 5, 10, 15, 20 y 25 equipos.

3.6.17 Contesta razonadamente a estas preguntas:

a) Si tenemos que la dirección IP de un equipo es 192.168.2.24 /28, ¿cuál es la dirección de red en la que está? ¿Qué máscara de red tiene esa red?

b) Dada la dirección de red 192.168.10.64, ¿qué máscara de red tiene asociada? ¿Qué rango de direcciones IP pueden tener los equipos en esa red? ¿Cuántos equipos puede haber conectados entonces, teniendo en cuenta que una conexión debe ir al router?

3.6.18 Supongamos que tenemos una dirección de clase A como 10.*.*. Si queremos usar 3 bits para subredes:

a) ¿Qué subredes se formarían (dirección de red de cada subred, con la parte de hosts a cero)?

b) ¿Qué rango de IPs válidas (asignables a hosts) tendría cada subred?

3.6.19 Una empresa tiene 3 departamentos de 20, 30 y 50 ordenadores, y quiere que cada uno tenga una red distinta.

a) ¿De qué clase (A, B ó C) deberían ser las direcciones de red para poder direccionar los hosts de esas redes?

b) Elige una IP privada de esa clase, e indica qué 3 subredes se crearían y el rango de IPs de cada subred

3.6.20 Si a la empresa anterior se le añaden 2 departamentos más, de 40 ordenadores cada uno:

a) ¿Serviría la misma clase de IP que teníamos? ¿Por qué?

b) En caso de que no sirviera, ¿qué clase de IP deberíamos elegir ahora? Elige una IP privada de esa clase e indica cómo quedarían las 5 subredes necesarias

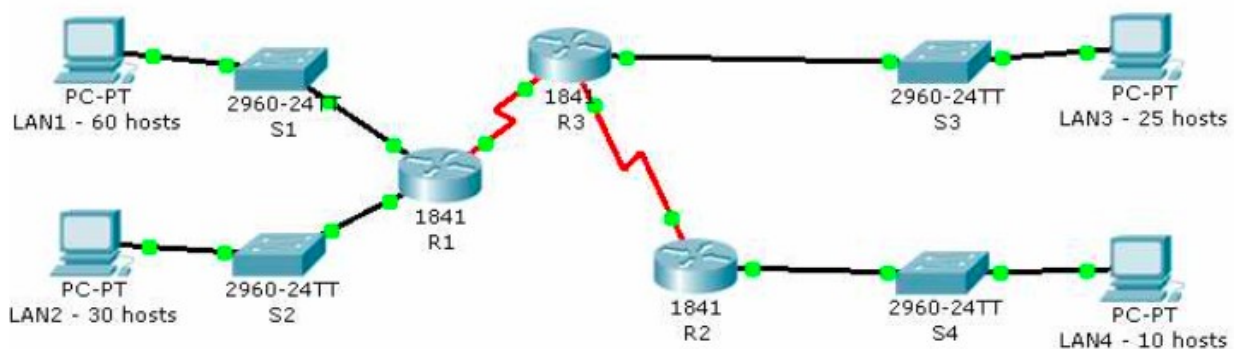
3.6.5.2 Subredes independientes de la clase. CIDR y VLSM

Con el sistema de división en subredes visto antes, seguimos desperdiciando bastante espacio a la hora de crear las subredes, ya que en algunas quedan bastantes direcciones IP sin asignar.

Por ejemplo, si necesitaríamos crear dos subredes de 300 equipos cada una, no nos serviría con una clase C como superred (sólo admitiríamos hasta unos 250 equipos), y tendríamos que elegir una clase B. Después, de esa clase B sólo necesitamos 1 bit para distinguir las dos subredes, y nos quedan los otros 15 bits de equipos para dar IPs en cada subred (es decir, miles de IPs disponibles en cada subred, cuando sólo nos hacen falta 300).

Para un uso más eficiente de las direcciones, se propuso el llamado **enrutamiento entre dominios sin clase** (en inglés, **CIDR**). Su filosofía se basa en prescindir de las clases de direcciones IP y sus máscaras asociadas, sino que cualquier dirección IP puede tener cualquier máscara. Así, tendremos **máscaras de red de longitud variable** (en inglés, **VLSM**), dependiendo de las necesidades de cada subred. Veamos cómo funciona la técnica de división en subredes con VLSM con un ejemplo:

Queremos utilizar una dirección estándar de clase C 192.168.5.0 /24 para crear cuatro subredes en una empresa, con 10, 25, 30 y 60 equipos respectivamente. Además, necesitamos interconectar tres routers entre sí. El esquema básico de conexiones es éste:

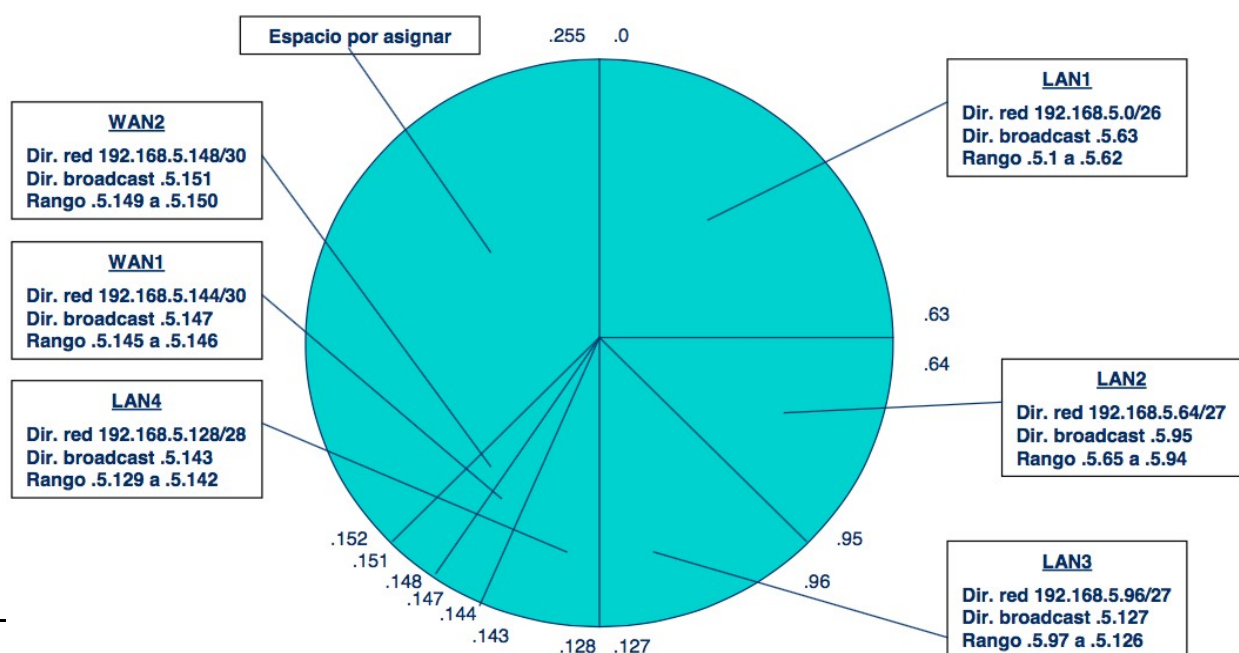


Necesitaremos en total 6 subredes (cuatro para las cuatro LANs, y dos más para las dos conexiones entre routers). Lo que hacemos es ordenarlas de mayor a menor número de conexiones necesarias:

- La red de mayor tamaño será la LAN1 (60 equipos). Necesitaremos 6 bits para asignarles direcciones a todos ($2^6 = 64$ direcciones, menos la de red y broadcast, quedan 62 disponibles). Por lo tanto, usaremos $32 - 6 = 26$ bits para la máscara. Usando la dirección base 192.168.5.0 /24, esta red quedaría así:
 - Dirección de red: 192.168.5.0 /26
 - Direcciones asignables: 192.168.5.1 hasta 192.168.5.62
 - Dirección de broadcast: 192.168.5.63
- Pasamos a la siguiente red, que es la LAN2 (30 equipos). Necesitaremos 5 bits para direccionarlos ($2^5 - 2 = 30$ direcciones justas), y por tanto usaremos $32 - 5 = 27$ bits para la máscara, empezando por donde nos quedamos antes:
 - Dirección de red: 192.168.5.64 /27
 - Direcciones asignables: 192.168.5.65 hasta 192.168.5.94

- Dirección de broadcast: 192.168.5.95
- La siguiente es la LAN3 (25 equipos). Volveremos a necesitar 5 bits, y usaremos 27 para la máscara. Continuamos asignando direcciones donde lo dejamos:
 - Dirección de red: 192.168.5.96 /27
 - Direcciones asignables: 192.168.5.97 hasta 192.168.5.126
 - Dirección de broadcast: 192.168.5.127
- La siguiente es la LAN4 (10 equipos). Para ellos necesitaremos 4 bits ($2^4 - 2 = 14$ direcciones disponibles), y usaremos $32 - 4 = 28$ bits de máscara.
 - Dirección de red: 192.168.5.128 /28
 - Direcciones asignables: 192.168.5.129 a 192.168.5.142
 - Dirección de broadcast: 192.168.5.143
- Nos quedan las conexiones WAN. En ambas necesitaremos dos direcciones (una para cada router conectado a la WAN), y por tanto harán falta 2 bits ($2^2 - 2 = 2$ direcciones justas). Usaremos $32 - 2 = 30$ bits de máscara. Así, la primera WAN quedaría así:
 - Dirección de red: 192.168.5.144 /30
 - Direcciones asignables: 192.168.5.145 y 192.168.5.146
 - Dirección de broadcast: 192.168.5.147
- Y la segunda WAN así:
 - Dirección de red: 192.168.5.148 /30
 - Direcciones asignables: 192.168.5.149 y 192.168.5.150
 - Dirección de broadcast: 192.168.5.151

Todo este esquema de direccionamiento se puede representar en forma circular, que se corta en segmentos representando el espacio de las subredes:



También podemos utilizar una tabla para representar cada subred y sus rangos:

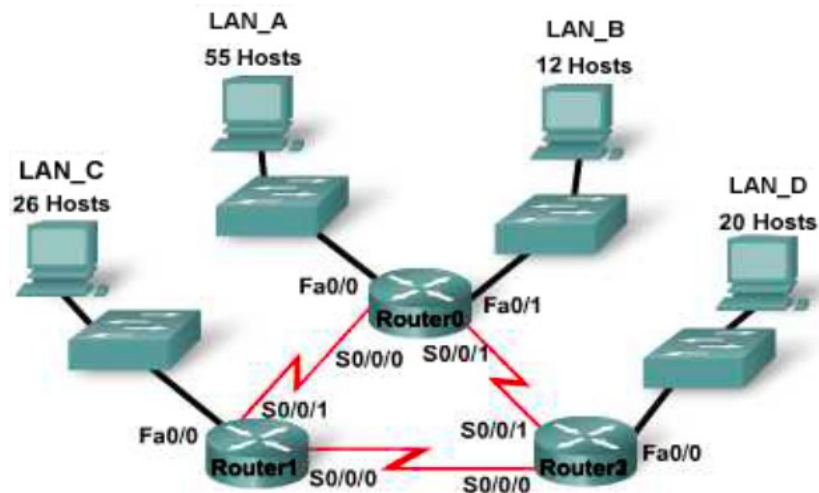
Dirección IP: 192.168.5.0/24

Requisitos de host	/barra	cantidad de hosts	Subred	Rango de host	Broadcast
60	/26	62	192.168.5.0	.1 - .62	.63
30					
25					
10					
2					
2					

Ejercicios propuestos

3.6.21 Repite los pasos vistos en la técnica de subredes con VLSM para una empresa que necesite crear 3 subredes de 15, 30 y 80 equipos, conectadas todas al mismo router.

3.6.22 Repite los pasos para otra empresa con el siguiente diseño de red:



En este caso, tenemos 4 redes locales, y 3 redes WAN para interconectar los tres routers.

3.6.23 Queremos utilizar una dirección estándar de clase C, 192.168.10.0 /24, para crear 3 subredes en una empresa con 30, 55 y 75 equipos respectivamente, estando todas ellas conectadas a un mismo router. Utiliza la técnica de enrutamiento entre dominios sin clase (en inglés, CIDR) para gestionar la configuración de dichas subredes, indicando para cada una su dirección de red y su máscara, el rango de direcciones IP para los hosts y la dirección de broadcast.

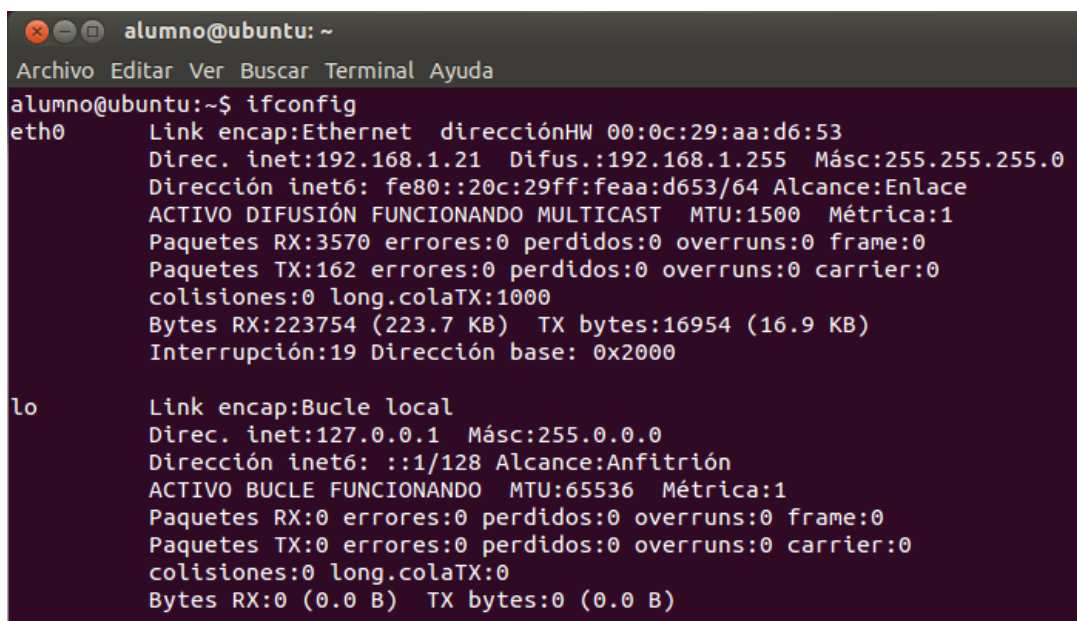
3.6.24 Queremos utilizar una dirección estándar de clase C, 192.168.5.0 /24, para crear 4 subredes en una empresa con 10, 25, 55 y 70 equipos respectivamente, estando todas ellas conectadas a un mismo router. Utiliza la técnica de enrutamiento entre dominios sin clase (en inglés, CIDR) para gestionar la configuración de dichas subredes, indicando para cada una su dirección de red y su máscara, el rango de direcciones IP para los hosts y la dirección de broadcast.

3.7 Configuración de los adaptadores de red en sistemas operativos libre y propietarios

3.7.1 Determinar la dirección IP, máscara y gateway de un equipo

Para determinar la dirección IP de un equipo, además de otra información valiosa como la máscara de red asociada o el gateway por defecto, podemos usar el mismo comando que para determinar su dirección MAC: **ipconfig** (en Windows) o **ifconfig** (en Linux/Mac).

El comando **ipconfig** o **ifconfig**, usado sin parámetros adicionales, muestra la dirección IP, la máscara de red y la puerta de enlace de cada adaptador de red encontrado. Utiliza este comando desde la consola de cmd de Windows o desde un terminal en Linux.



```
alumno@ubuntu: ~$ ifconfig
eth0      Link encap:Ethernet  direcciónHW 00:0c:29:aa:d6:53
          Direc. inet:192.168.1.21  Difus.:192.168.1.255  Másc:255.255.255.0
          Dirección inet6: fe80::20c:29ff:feaa:d653/64  Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:3570 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:162 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:223754 (223.7 KB)  TX bytes:16954 (16.9 KB)
          Interrupción:19 Dirección base: 0x2000

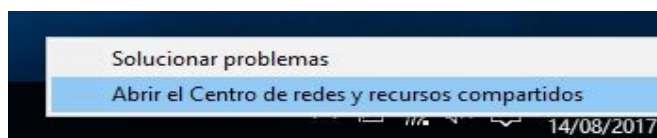
lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128  Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO  MTU:65536  Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:0
          Bytes RX:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Resultado de ejecutar el comando ifconfig -a en Linux

3.7.2 Configurar manualmente la dirección IP, máscara y gateway

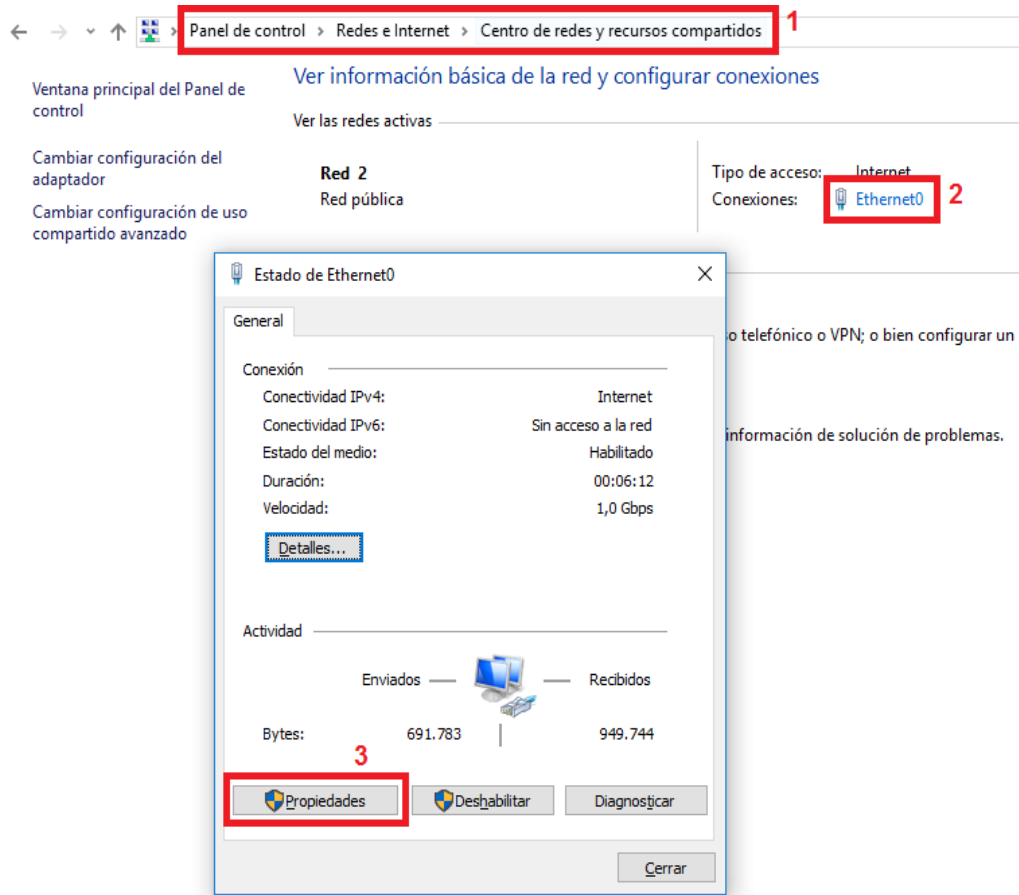
3.7.2.1 Windows

Para configurar estos parámetros en un equipo con Windows 10, ve a “Panel de Control” > “Redes e Internet” > “Centro de redes y recursos compartidos”. También puedes acceder al “Centro de redes y recursos compartidos” desde la barra de tareas, haciendo clic con el botón derecho del ratón sobre el icono de red.



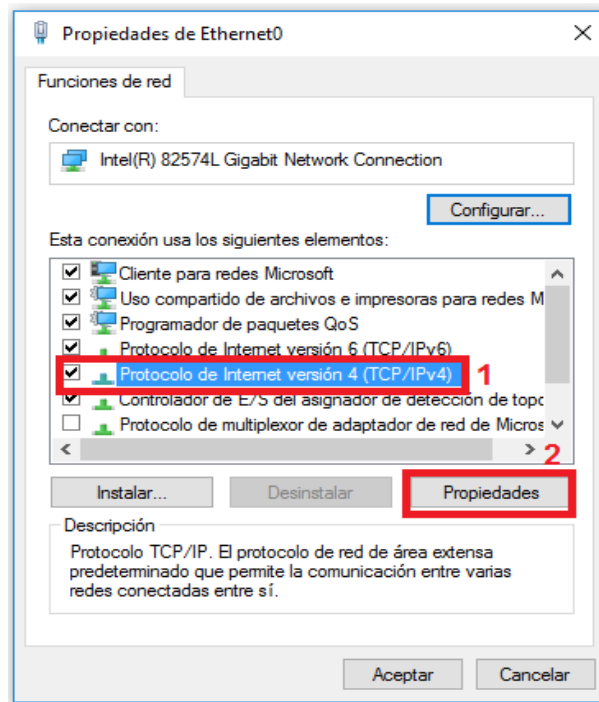
Acceso al centro de redes y recursos compartidos desde la barra de tareas

Haz clic en la conexión activa (2) y en la ventana que aparece, selecciona “*Propiedades*” (3).



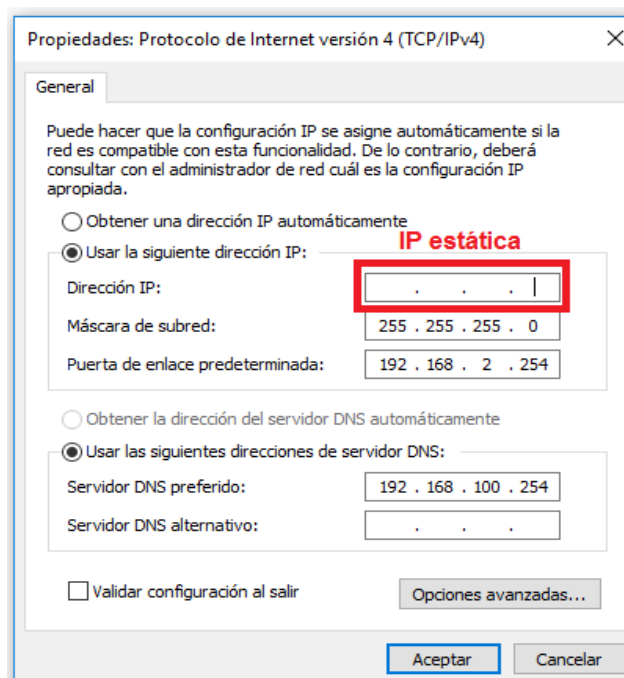
Acceso a las propiedades de la conexión activa en Windows 10

A continuación, en la ventana de propiedades de la conexión, selecciona “*Protocolo de Internet versión 4 (TCP/IPv4)*”, y pulsa el botón de “*Propiedades*”.



Acceso a las propiedades del protocolo IPv4

En dicha ventana de propiedades, marca la opción “Usar la siguiente dirección IP”, e indica una dirección IP, una máscara de subred y una puerta de enlace predeterminada. También puedes especificar debajo los servidores DNS que tengas asociados, o usar algunos conocidos, como los de Google. Por último, acepta todas las ventanas que tengas abiertas.

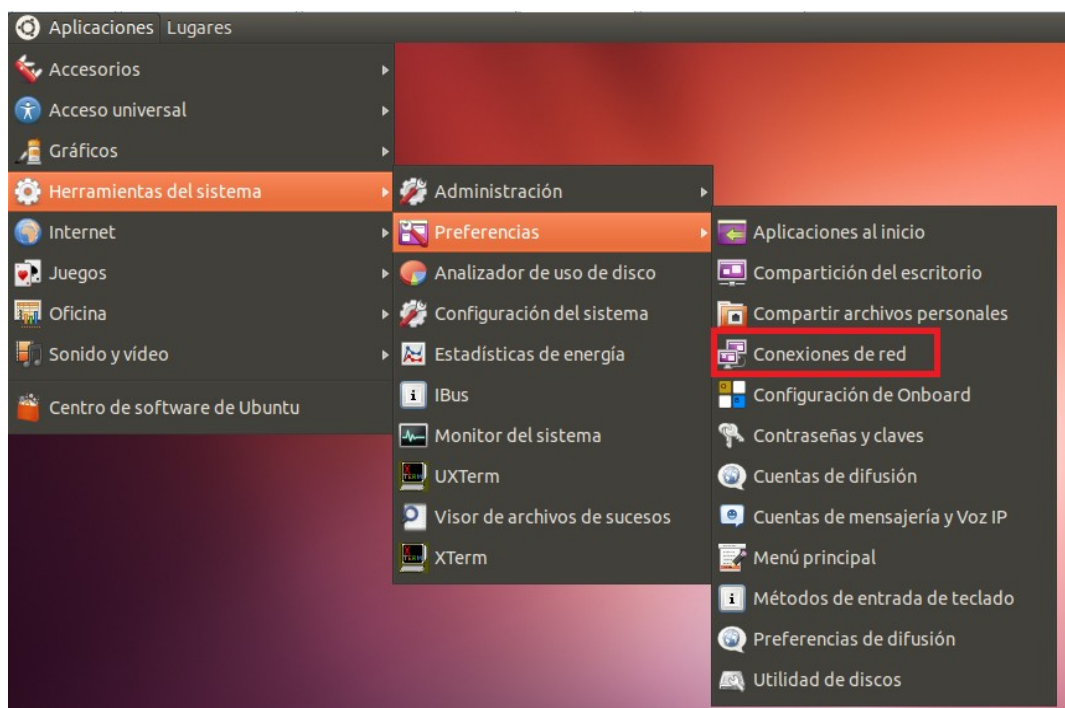


Configuración de una IP estática en Windows 10

3.7.2.2 Linux

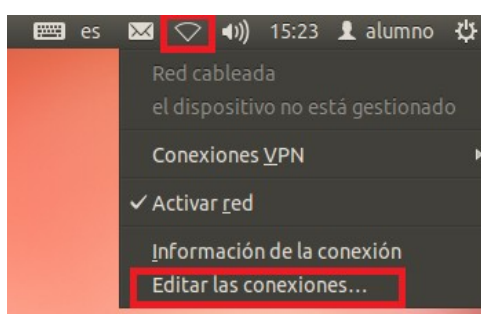
En otros sistemas, como Linux, existen herramientas similares para configurar la dirección IP. Por ejemplo, en Ubuntu se puede configurar una dirección manualmente desde el entorno gráfico o desde terminal, modificando el fichero de configuración de las interfaces de red.

Para **configurar una IP estática desde la interfaz gráfica**, haz clic en “Aplicaciones” > “Herramientas del sistema” > “Preferencias” > “Conexiones de red”.



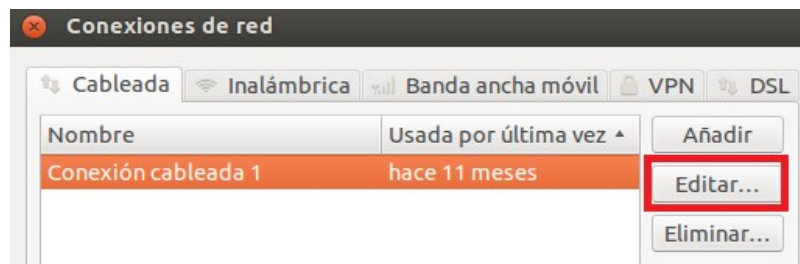
Acceso a las conexiones de red en Ubuntu

O bien, desde la barra de tareas, haciendo clic sobre el icono de conexiones de red, y seleccionando la opción “*Editar conexiones de red*”.



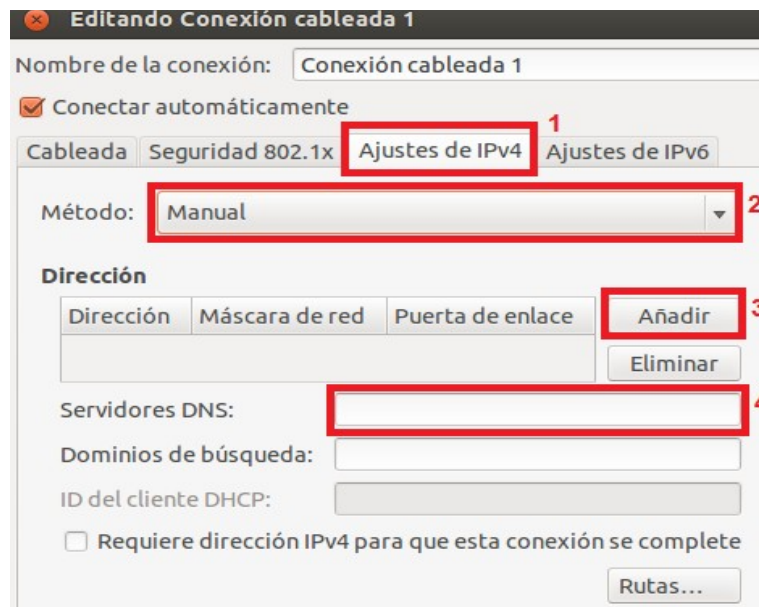
Acceso a las conexiones de red en Ubuntu desde la barra de tareas

En la ventana que aparece puedes ver las interfaces de red que tiene el equipo. En la pestaña “Cableada” puedes ver las interfaces de red ethernet y en la pestaña “Inalámbrica” puedes ver las interfaces de red inalámbrica. Para editar las propiedades de una interfaz solamente tienes que seleccionarla y pulsar el botón de “*Editar*”.



Ventana para editar las conexiones de red

Después ve a la pestaña de “*Ajustes IPv4*” o “*Ajustes IPv6*”, según corresponda, selecciona el método “*Manual*” y especifica la IP, máscara y puerta de enlace que corresponda. Desde la misma ventana también puedes configurar la dirección IP del servidor DNS de tu red.



Edición de las propiedades de una conexión de red

Otra opción es **configurar una IP estática desde un terminal**, para ello debes editar el archivo de configuración de las interfaces de red con el siguiente comando:

```
sudo gedit /etc/network/interfaces
```

Y modificarlo para que quede así:

```
# The loopback network interfaces
auto lo

iface lo inet loopback

# The primary network interface
auto eth0

iface eth0 inet static
address [ dirección IP ] (sin los corchetes!)
netmask [ máscara de red ]
```

```
network [ dirección de red ]  
broadcast [ dirección de broadcast ]  
gateway [ puerta de enlace ]
```

Las dos primeras líneas configuran la interfaz de loopback. La primera línea “auto lo”, indica que se levantará la interfaz de loopback (lo) de forma automática durante el inicio del sistema. Mientras que la segunda línea define que la interfaz lo es de loopback.

Las siguientes líneas configuran la interfaz eth0. La primera línea “auto eth0”, indica que se levantará la interfaz eth0 de forma automática durante el inicio del sistema. Mientras que la segunda línea sirve para indicar que vamos a configurar dicho interfaz de forma estática o manual. El resto de líneas sirven para configurar lo siguiente:

- **address:** es la dirección IP fija que se asigna al equipo
- **netmask:** es la máscara de subred de la dirección IP anterior
- **network:** es la red a la que pertenece esa dirección IP
- **broadcast:** es la dirección IP de difusión de la red
- **gateway:** es la dirección IP de la puerta de enlace predeterminada. Normalmente es la dirección IP del equipo de la red o router por el que podemos salir al exterior o conectarnos a Internet.

El siguiente paso es reiniciar las interfaces de red para aplicar los cambios. Para ello, ejecuta el siguiente comando:

```
sudo /etc/init.d/networking restart
```

Si tuvieras algún problema con la interfaz que acabas de configurar, puedes probar a deshabilitar y habilitar de nuevo la interfaz de red de la siguiente forma:

```
sudo ifconfig eth0 down  
sudo ifconfig eth0 up
```

Ejercicios propuestos

3.7.1 Abre una máquina virtual de Linux y configura manualmente su IP con la dirección IP que te facilitará el profesor. Indica en un documento de texto los pasos que has seguido, y muestra una pantalla en la que se vea que efectivamente la máquina virtual tiene asignada dicha IP.

3.8 Asignación automática de direcciones IP: DHCP

Para configurar de forma automática los parámetros de conexión a la red, existe un protocolo a nivel de aplicación denominado **DHCP** (*Dinamic Host Configuration Protocol* ó *Protocolo de Configuración Dinámica de Hosts*). Utilizándolo, un dispositivo externo (normalmente un router, o un equipo configurado como servidor DHCP) nos proporcionará una dirección IP, máscara, puerta de enlace y servidores DNS para poder estar conectados a la red. La configuración del servidor depende de dicho servidor, pero en general se especifican una serie de parámetros:

- Rango de direcciones que se pueden asignar. Los equipos que se vayan conectando irán obteniendo direcciones de ese rango, normalmente de forma correlativa.
- Máscara de red asociada
- Puerta de enlace o gateway por defecto para salir de la red
- Servidores DNS

También debemos configurar los hosts para que se configuren automáticamente por DHCP. Para ello, vamos al mismo panel visto antes para la configuración manual, y elegimos obtener la dirección automáticamente. Los hosts enviarán una solicitud DHCP al servidor, y el servidor les responderá con una configuración de red, quedando así el equipo incluido en la red.

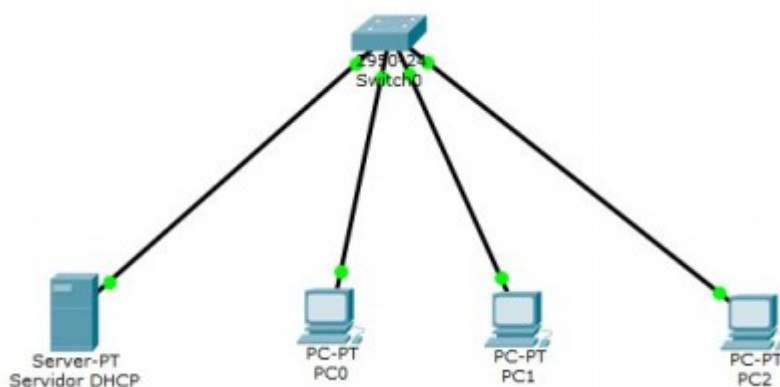
Ejercicios propuestos

3.8.1 Abre la misma máquina virtual de Ubuntu que en el ejercicio anterior y configúrala para que se le asigne de forma automática una dirección IP empleando el protocolo DHCP. Indica en un documento de texto los pasos que has seguido, y muestra una pantalla en la que se vea que efectivamente la máquina virtual tiene asignada una nueva dirección IP.

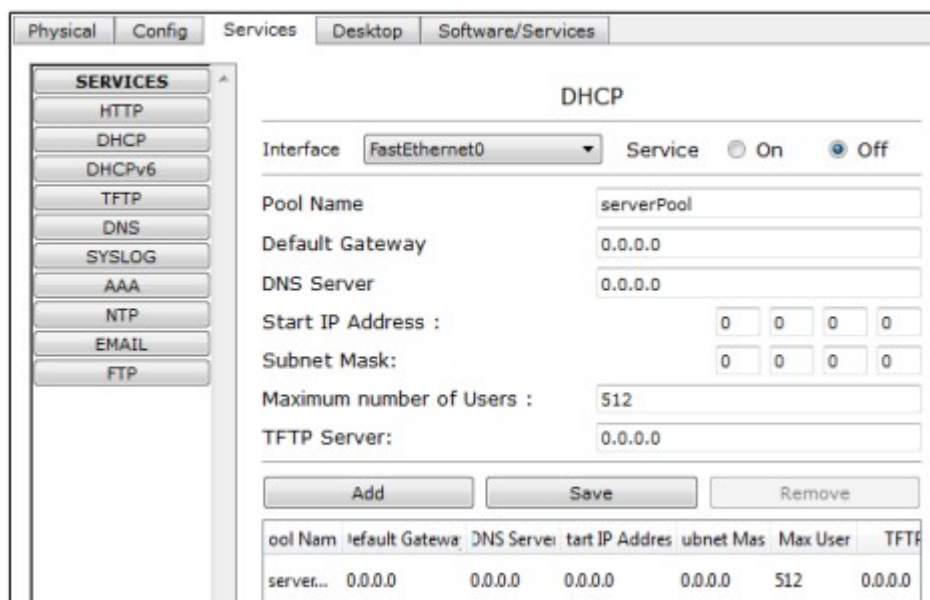
3.8.2 En este ejercicios vas a aprender a configurar un servidor para que asigne direcciones DHCP a los clientes que lo soliciten, y a configurar los clientes para que establezcan su configuración de red de forma automática. Para ello, crea un nuevo documento en Packet Tracer llamado PracticaDHCP.pkt, y sigue estos pasos:

- Añade y conecta los siguientes elementos:
 - Un switch genérico de 24 puertos (tipo 2950-24, por ejemplo)
 - Un servidor genérico (Server-PT), renombrado a “Servidor DHCP”
 - 3 PCs de escritorio

Al final deberá quedarte algo así:



- Haz clic en el servidor, ve a su pestaña Services, y dentro a la opción DHCP. Configura esta opción para que asigne 50 direcciones a partir de la 192.168.1.101 (inclusive) Elige la máscara de red adecuada a esta clase de IP. No establezcas ningún gateway por defecto ni ningún servidor DNS (deja los valores por defecto). Recuerda también activar el servicio (marcar la casilla On en la parte superior derecha).



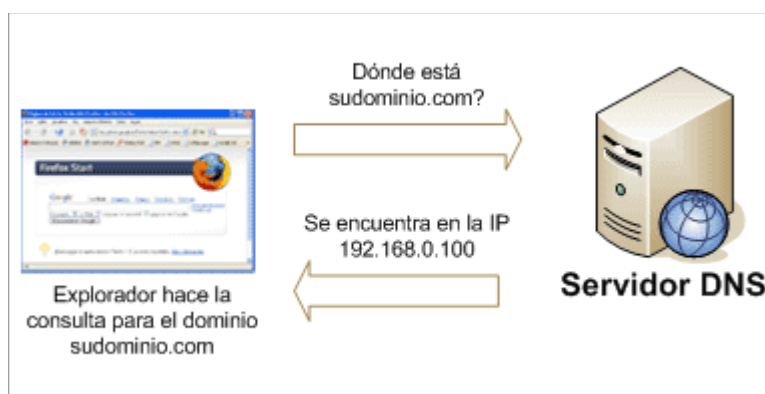
- En cuanto a los PC de escritorio, haz clic en ellos, ve a la pestaña Desktop, y cambia su configuración IP para que acepte DHCP.
- Al hacerlo, automáticamente deberá asignarle una IP de las establecidas en el rango (si el primer intento no funciona, prueba a marcar la casilla Static y luego volver a marcar DHCP en la configuración IP del PC).

Debes entregar el archivo de Packet Tracer y un documento explicando con tus palabras el proceso, incluyendo capturas de pantalla.

3.9 Sistema de nombres de dominio (DNS)

Ya hemos visto que todo dispositivo conectado a una red tiene asignada una dirección física (dirección MAC) y una lógica (dirección IP). Esta última es la que realmente utilizan los routers para saber dónde está ese dispositivo en la red global, y poderle hacer llegar los distintos mensajes.

Sin embargo, cuando queremos acceder a un dispositivo remoto (por ejemplo, un servidor web como Google), no escribimos la dirección IP de Google en el navegador, sino lo que se conoce como **nombre de dominio** (en el caso de Google, escribimos `www.google.es`). A partir de este nombre, se consulta al servidor DNS que tengamos configurado por defecto si conoce la IP para ese nombre de dominio. En caso afirmativo, se logra acceder al recurso solicitado. En caso contrario, el servidor pasa automáticamente esa petición a otro servidor DNS, hasta que la solicitud llega a un servidor que sí conoce la dirección IP asociada al nombre de dominio y entonces la respuesta fluye de nuevo a través de la cadena de servidores DNS hasta llegar al equipo que hizo la solicitud.



Se tiene así una especie de "base de datos global", distribuida en distintos servidores, donde se guardan las correspondencias entre los nombres de dominio y las direcciones asociadas. Esta información está jerarquizada, de forma que los servidores de nivel superior tienen información sobre las principales extensiones de dominio (es decir, dónde encontrar dominios acabados en .com, .net, .org o cualquier otra extensión), los de nivel secundario tienen información sobre los dominios propios de cada extensión (por ejemplo, google.com o php.net), y los de niveles inferiores van afinando más la búsqueda a ciertos tipos de servidores específicos (por ejemplo, el servidor de correo de Google, mail.google.com).

Sin DNS el usuario debería acceder a los recursos mediante el uso de las direcciones IP, lo que resulta poco práctico. Además, como las direcciones IP pueden cambiar, sería complicado mantener una lista actualizada de direcciones.

3.9.1 Nslookup

Nslookup (*Name System lookup*) es una herramienta que permite hacer consultas a un DNS de forma manual. Se utiliza para obtener información de un dominio y resolver posibles problemas con los servidores DNS. Funciona sólo mediante línea de comandos, por lo que para poder usarlo debemos abrir bien un terminal, si estamos en Linux, o bien la ventana del símbolo del sistema (comando cmd), si estamos en Windows.

Al arrancar, por defecto, nslookup ya se conecta al servidor DNS que tenga configurado, mostrando su nombre y su dirección IP (en la imagen, uno de los nodos principales de ONO), seguido del cursor de órdenes, el símbolo ">", desde el que se pueden realizar una serie de consultas.

Para ver una lista de todos los comandos disponibles para nslookup, escribe el comando "?". Para salir del comando nslookup, basta con introducir la palabra "exit".

```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\May>nslookup
Servidor predeterminado: 62.81.16.164.static.user.ono.com
Address: 62.81.16.164

>
```

Si queremos obtener la IP de un dominio, basta con indicar su URL después de la línea de entrada del comando nslookup (>). Por ejemplo la IP de www.gva.es es 193.144.127.85.


```

Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\May>nslookup
Servidor predeterminado: 62.81.16.164.static.user.ono.com
Address: 62.81.16.164

> www.gva.es
Servidor: 62.81.16.164.static.user.ono.com
Address: 62.81.16.164

Respuesta no autoritativa:
Nombre: simac13.gva.es
Addresses: 195.77.16.26
          193.144.127.85
Alias: www.gva.es
>

```

También podemos hacer una consulta puntual de un nombre de dominio adjuntando dicho dominio junto al comando nslookup. Por ejemplo: nslookup www.google.es

```

Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\May>nslookup www.google.es
Servidor: 62.81.16.164.static.user.ono.com
Address: 62.81.16.164

Respuesta no autoritativa:
Nombre: www.google.es
Addresses: 2a00:1450:4003:807::2003
          216.58.210.131

C:\Users\May>

```

El mensaje "*Respuesta no autoritativa*" significa que se consulta a un servidor que no posee autoridad directa para el nombre de dominio consultado. Si fuese autoritativa se puede llegar a acceder a todas las direcciones que contiene el DNS, para después utilizarlo con finalidades fraudulentas.

De modo predeterminado, el comando nslookup realiza consultas al servidor de nombres predeterminado. Sin embargo, es posible consultar un servidor de nombres específico mediante el comando "**server**". Por ejemplo con "server 8.8.8.8", se utilizará el servidor de nombres de Google.

```

C:\Users\May>nslookup
Servidor predeterminado: 62.81.16.164.static.user.ono.com
Address: 62.81.16.164

> server 8.8.8.8
Servidor predeterminado: google-public-dns-a.google.com
Address: 8.8.8.8

> www.gva.es
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respuesta no autoritativa:
Nombre: simac13.gva.es
Addresses: 195.77.16.26
          193.144.127.85
Alias: www.gva.es
>

```


Con el comando "set type=tipo" se pueden realizar diferentes tipos de consultas, donde "tipo" puede tomar los siguientes valores:

- **A** (*address*): se utiliza para traducir nombres de dominio a direcciones IP, es el valor predeterminado.
- **PTR** (*pointer*): lo inverso del registro A, realiza la traducción de direcciones IP a nombres de dominio.
- **ANY** (*cualquiera*): toda la información que exista.
- **CNAME** (*canonical name*): permite mostrar información relacionada con los alias. Es usado cuando se ejecutan multiples servicios en un servidor con una sola direccion IP.
- **NS** (*name server*): permite obtener información del servidor de nombres relacionado al dominio.
- **MX** (*mail exchange*): permite obtener información relacionada con los servidores de correo de un dominio.
- **HINFO** (*host information*): permite mostrar, siempre y cuando los datos estén disponibles, información relacionada con el hardware y el sistema operativo del host. Generalmente se recomienda no completar esta información al configurar un servidor DNS, ya que puede resultar de utilidad para los piratas informáticos.

Ejercicios propuestos

3.9.1 Utilizando nslookup, indica la IP de tu servidor DNS y obtén la dirección IP de los siguientes dominios: www.eltiempo.es, es.wikipedia.org, www.ubuntu.com. Indica la orden que has utilizado y explica el resultado obtenido (puedes hacer una captura de pantalla).

a) ¿Para alguno de los dominios anteriores obtienes más de una dirección IP? En caso afirmativo, indica para qué nombre de dominio y qué significa que tenga más de una dirección IP asignada

3.9.2 Utilizando el comando adecuado para mostrar toda la información que exista del dominio www.ubuntu.es, y comparalo con el resultado obtenido en el ejercicio anterior.

3.9.10 Busca los servidores de nombre que funcionan para el dominio es.wikipedia.org. Indica la orden que has utilizado y explica el resultado obtenido (puedes hacer una captura de pantalla)

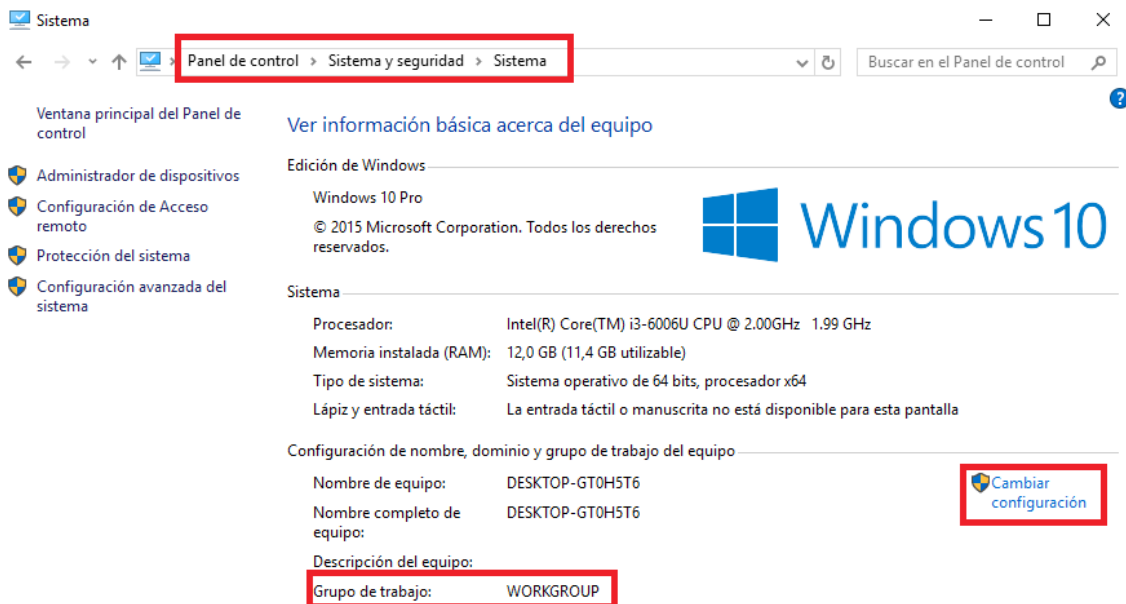
3.10 Introducción a los recursos compartidos

Una vez configurada una red podemos utilizarla para trabajar de forma compartida con los recursos de los que dispongamos (archivos, carpetas, impresoras, etc...). Como es lógico, si queremos compartir archivos y carpetas entre los equipos de una red doméstica, estos deberán estar conectados a la misma red, ya sea mediante cable o wifi.

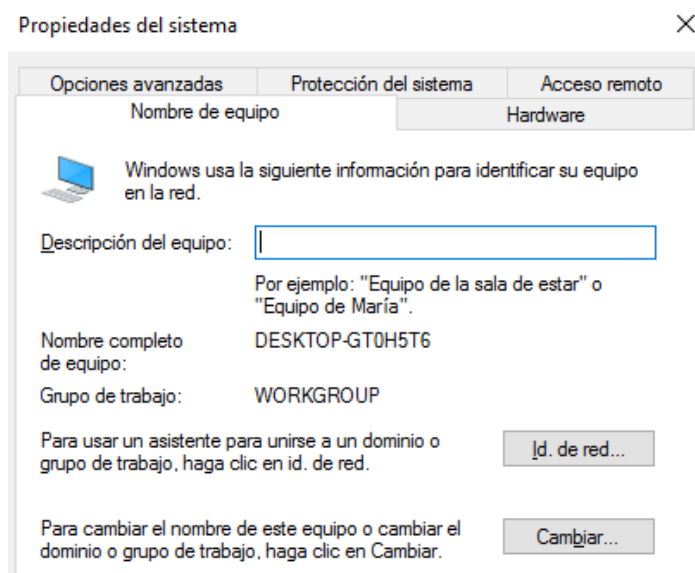
Las redes bajo Windows emplean los **grupos** y los **dominios de trabajo** para agrupar el equipamiento para trabajar en red. Ambos tienen la misma utilidad, agrupar equipos bajo un nombre, pero con una gran diferencia, mientras que en el grupo de trabajo los usuarios que acceden a la red se validan en su equipo y desde ese momento ya tienen acceso a los recursos de la red, en el dominio la validación la realiza un servidor y en función de dicha validación se podrá acceder a

unos recursos u otros, dependiendo del perfil del usuario. En este apartado nos centraremos en los grupos de trabajo.

Para comprobar a qué grupo de trabajo pertenecemos basta seguir la siguiente ruta: “*Panel de control > Sistema y seguridad > Sistema*”, y aparecerá una ventana con la información básica del sistema. En la sección “*Configuración de nombre, dominio y grupo de trabajo del equipo*” aparece el grupo de trabajo al que pertenecemos.

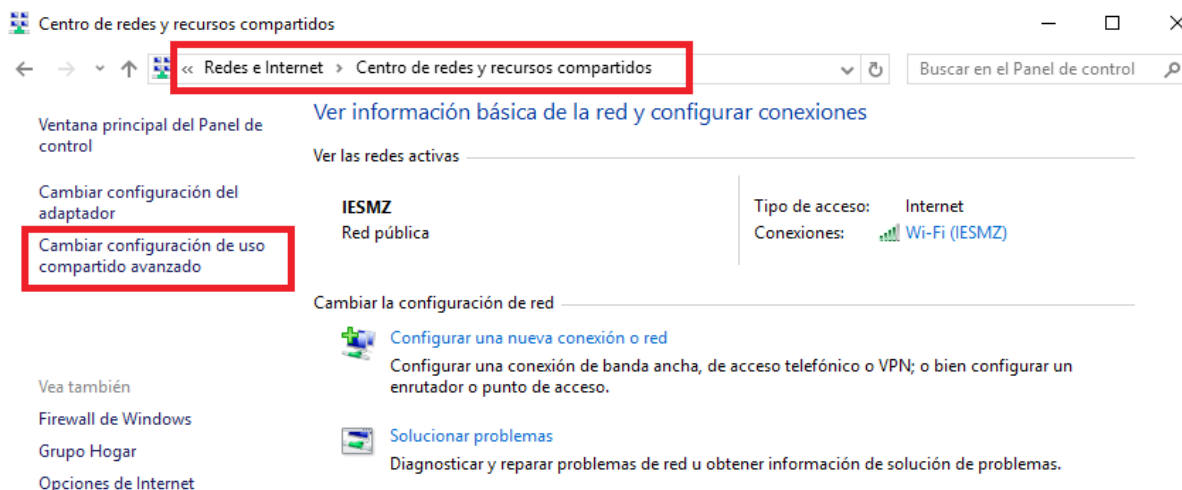


Para unirse un grupo de trabajo existente o cambiar de grupo de trabajo, haremos clic en el enlace “*Cambiar configuración*” que aparece a la derecha de la sección, y seleccionaremos la opción correspondiente en la ventana que aparece. Se iniciará una asistente para ayudarnos en el proceso.



Es importante resaltar que solo podremos ver las carpetas y archivos compartidos en red de aquellos equipos que se encuentren conectados en ese momento, no podremos acceder a carpetas y archivos de equipos que no están conectados a nuestra red doméstica o se encuentran apagados.

Antes de empezar a compartir recursos, debemos activar el uso compartido desde “*Centro de redes y recursos compartidos*”. Ahí seleccionaremos “*Cambiar configuración de uso compartido avanzado*”.



Se abrirá una ventana en la que podrás configurar las opciones de uso compartido para los diferentes perfiles de red. Activa el uso compartido de archivos e impresoras del perfil público.

Cambiar opciones de uso compartido para distintos perfiles de red

Windows crea un perfil de red independiente para cada red que use. Puede elegir opciones específicas para cada perfil.

Privado ▼

Invitado o público (perfil actual) ▲

Detección de redes

Quando se activa la detección de redes, este equipo puede ver otros equipos y dispositivos en la red y es visible para los demás equipos en la red.

☒ Activar la detección de redes

☐ Desactivar la detección de redes

Compartir archivos e impresoras

Quando se activa el uso compartido de archivos e impresoras, los usuarios de la red podrán tener acceso a los archivos e impresoras compartidos en este equipo.

☒ Activar el uso compartido de archivos e impresoras

☐ Desactivar el uso compartido de archivos e impresoras

Todas las redes ▼

Además, dentro de las opciones que se abren, al final del todo y dentro de la sección “*Todas las redes*”, debes marcar la opción de “*Desactivar el uso compartido con protección por contraseña*”. De esta manera evitas que Windows te solicite un usuario y contraseña cuando intentes acceder a las carpetas compartidas en red desde otro equipo.

Uso compartido con protección por contraseña

Quando se activa el uso compartido con protección por contraseña, solo los usuarios con una cuenta y contraseña de usuario en este equipo pueden obtener acceso a los archivos compartidos, a las impresoras conectadas a este equipo y a las carpetas públicas. Para dar acceso a otros usuarios, es necesario desactivar el uso compartido con protección por contraseña.

☐ Activar el uso compartido con protección por contraseña

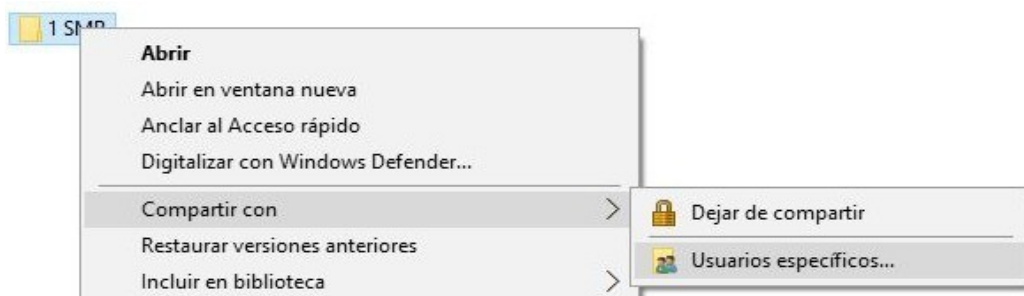
☒ Desactivar el uso compartido con protección por contraseña

El siguiente paso es compartir una carpeta.

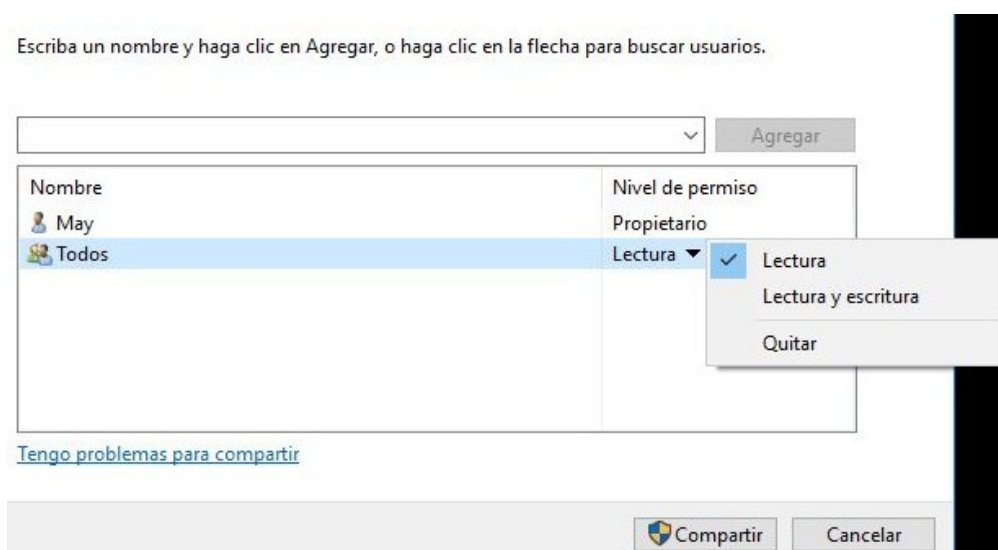
3.10.1 Compartir carpetas

Para compartir una carpeta en Windows 10, sigue los pasos siguientes:

1. Selecciona la carpeta que desees compartir en red y pulsa sobre ella con el botón derecho del ratón seleccionando la opción de “Compartir con > Usuarios específicos...”.

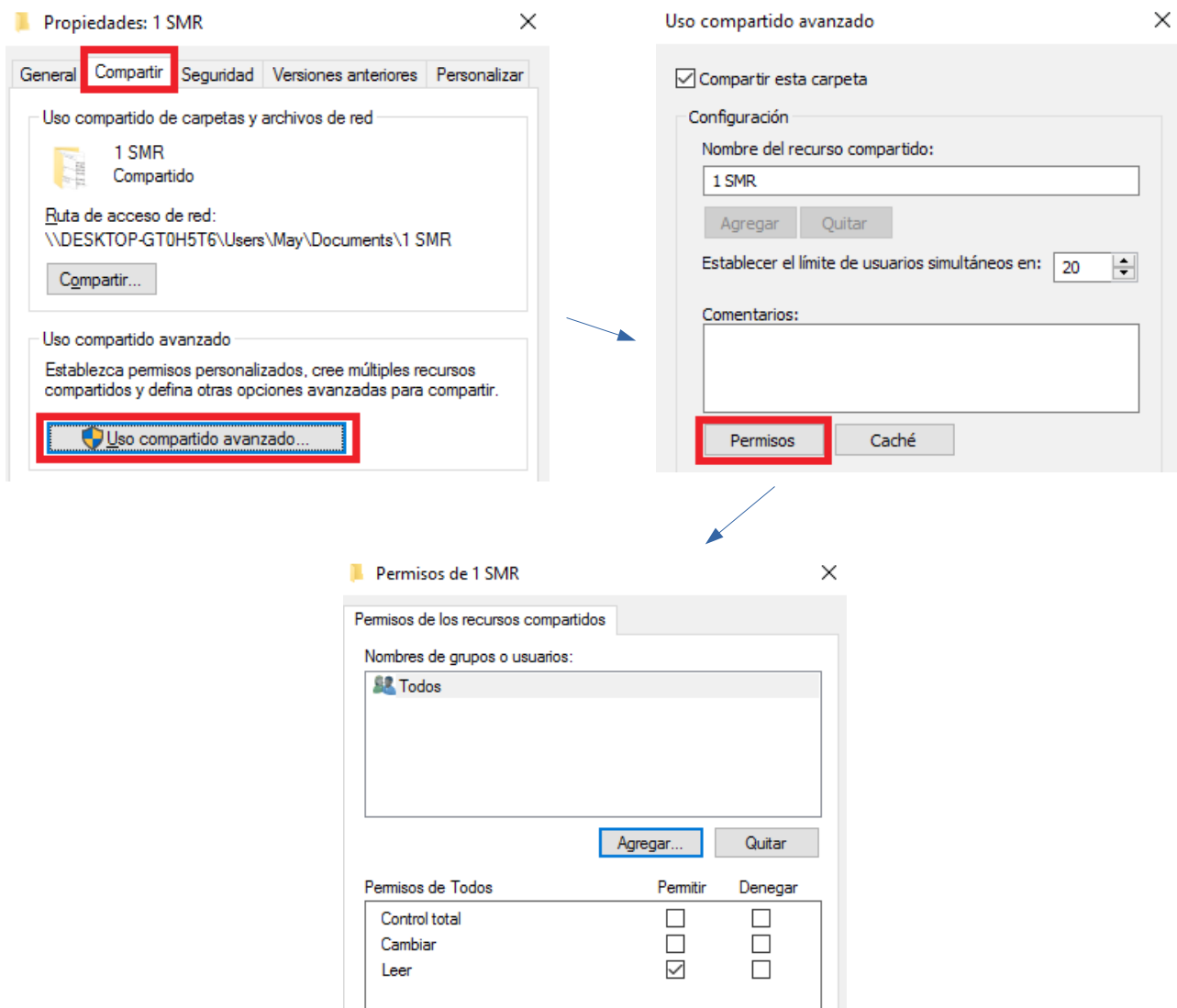


2. Se abrirá un cuadro donde debes elegir con qué equipos de la red compartir la carpeta y su contenido. Por ejemplo, para compartir una carpeta con todos los equipos conectados a la red, selecciona en el desplegable superior “Todos” y pulsa el botón “Agregar”.
3. Bajo la opción de “Nivel de Permiso”, puedes configurar los permisos otorgados a esos equipos. Por defecto aparece el de “Lectura”, es decir, los equipos conectados a la misma red podrán ver los archivos compartidos pero no podrán manipularlos, borrarlos o subir nuevo contenido a la carpeta compartida en red. Pulsando sobre la flecha podremos cambiar el tipo de Permiso.



4. Tras pulsar en “Compartir”, Windows 10 configurará la carpeta para compartirla en red y que sea accesible a todos los equipos de la red.

Si posteriormente quieres establecer una serie de permisos personalizados o definir otras opciones avanzadas, como limitar el número de usuarios simultáneos y/o modificar los permisos a los usuarios que tienen acceso a la carpeta compartida, puedes hacerlo desde las propiedades de la carpeta compartida, seleccionando la pestaña “Compartir > Uso compartido avanzado > Permisos”.



Una vez compartida será accesible desde el icono de “Red” (disponible desde el explorador de Windows) de cualquier equipo que este conectado en la red, aunque no pertenezca al mismo grupo de trabajo. Al abrir este enlace verás que aparecen los ordenadores del grupo de trabajo y haciendo doble clic sobre alguno de ellos podrás acceder las carpetas que tengan compartidas.

Ejercicios propuestos

3.10.1 Crea una carpeta compartida en tu equipo de clase para que puedan verla el resto de compañeros. Otórgale permisos sólo de Lectura. Comprueba que tus compañeros pueden acceder a tu carpeta y tú a la de ellos. En un documento de texto, indica los pasos que has seguido y alguna captura de pantalla que pruebe que efectivamente has podido acceder alguna carpeta compartida.

3.10.2 Montar una unidad de red

Es posible transformar un recurso remoto en particular (carpeta compartida) en una unidad de disco (unidad de red) para que aparezca directamente en el “Explorador de Windows”, de forma similar a lo que ocurre con tu disco local. Para realizar esta operación basta con realizar los siguientes pasos:

1. Abre el explorador de Windows, haz clic con el botón derecho sobre “*Este equipo*” y selecciona la opción “*Conectar a unidad de red*”
2. Se abrirá una ventana en la que tendrás que indicar la letra de unidad para la conexión, la carpeta con la que conectará y si deseas que este disponible siempre al iniciar la sesión de usuario.
3. Pulsa en “*Examinar*” y selecciona una carpeta de red compartida que quieras convertir en unidad de red. Pulsa “*Aceptar*” para finalizar.

De esta forma al abrir “*Explorador de Windows*” ya aparecerá como una unidad de red y se podrá acceder a sus contenidos.

Cuando se monta una unidad de red para que este operativa siempre es necesario que el ordenador que la aloja físicamente este operativo cuando ponemos en marcha nuestro equipo. De lo contrario no se conectará al inicio y ya no lo hará hasta la próxima sesión salvo que nosotros iniciemos una nueva conexión de forma manual.

Ejercicios propuestos

3.10.2 Crea una unidad de red de alguna de las carpetas de red compartidas creadas en el ejercicio anterior. Documenta el proceso seguido.