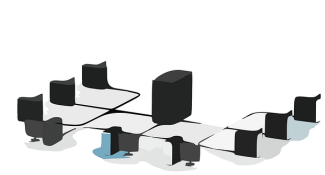
Interconexión de equipos en redes locales I

Caso práctico



Una vez que María conoce todas las posibles soluciones al diseño de una red, se ha decidido por implementar una de las aulas de la academia con una red de área local cableada. María debe conocer todas las posibilidades de interconexión de sus equipos dentro de un aula. Está interesado en que el equipo que utilice el profesor sea accesible para el alumnado y que compartan un lugar común donde puedan desarrollar una comunicación entre alumnado y profesorado

1.- Introducción

A la hora conectar equipos el modelo de referencia mayoritariamente utilizado a nivel mundial es el TCP-IP. Por tanto, para la configuración de los dispositivos se sigue este modelo de cuatro capas y analizando cada una de ellas:

1. A nivel de **acceso a la red**, como hemos visto en los temas anteriores, el direccionamiento que se usa habitualmente en redes locales (ethernet normalmente) es la dirección MAC y esta viene configurada por el fabricante. Es decir, normalmente no es necesario que sea conocida para ninguna instalación de red y viene grabada en el chip del dispositivo de forma que no es editable.
2. A nivel de **transporte** son las aplicaciones y el sistema operativo quien gestiona los puertos, tenemos 2 casos:
    - Las aplicaciones de servidor, que prestan servicios, suelen tener establecido por norma que puerto utilizar (por ejemplo, un servidor web utiliza siempre el puerto 80 y el 443 para conexiones seguras).
    - Las aplicaciones cliente, que usan los servicios mencionados, utilizan los puertos que le va asignando el sistema operativo (por ejemplo, el navegador web, cada vez que abrimos una pestaña, solicita un puerto libre al sistema operativo desde el cual trabaja y utilizará como remite de sus peticiones).
3. A nivel de **aplicación** el direccionamiento suele ser gestionado por el usuario o por el software (por ejemplo, en el correo electrónico es el usuario quien decide desde que dirección de correo comunicar y con cual dirección de correo quiere comunicar)
4. A **nivel de red o internet** suele ser necesaria una configuración, aunque sea mínima, y es el aspecto que un profesional de la informática debe conocer más a fondo.

2.- Segmentación de la red. Dominios de colisión y difusión

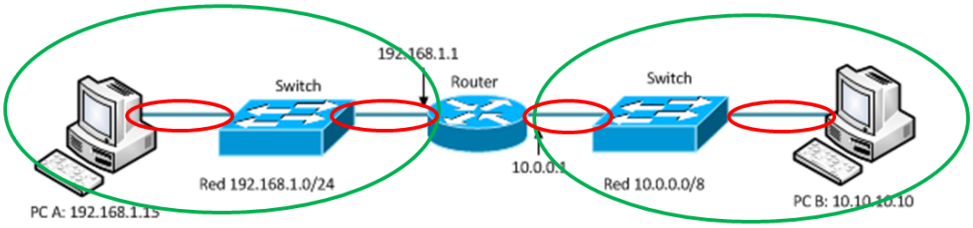
Para evitar una saturación del tráfico de datos que afecte a toda la red se realizan segmentaciones de red para evitar:

- Colisiones, por ejemplo, si hay muchos equipos conectados a un punto de acceso es muy probable que dos equipos intentan transmitir al mismo tiempo produciendo una colisión:

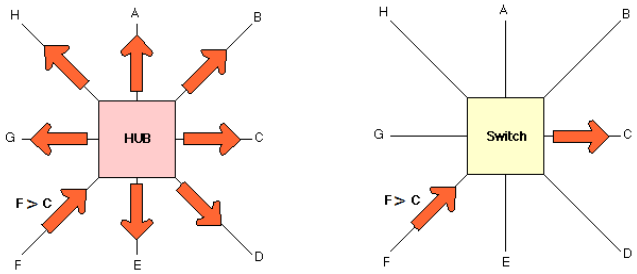
- Grandes difusiones, es decir, evitar que la información llege a muchos equipos.

La segmentación se puede llevar a cabo utilizando puentes, switchs o routers.

El router crea dominios de difusión (en verde) y el switch crea dominios de colisión (en rojo):



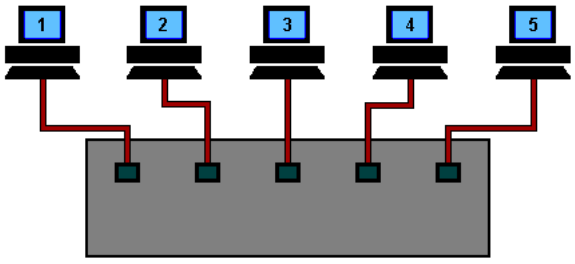
Un switch es un dispositivo de interconexión de nivel 2 que es capaz de generar diferentes dominios de colisión. La diferencia entre un hub (concentrador) y un switch (conmutador) es que un hub recibe información por un puerto (conexión) y la reenvía por todos los demás mientras que un switch reenvía la información solamente por los puertos a los que va dirigida.



¿Cómo evita las colisiones un switch?

Los switchs reconocen las direcciones Ethernet (MAC) que llegan por sus diferentes puertos (conexiones). En un paquete recibido por el switch, este examina las direcciones MAC origen y destino y las compara con una lista almacenada en el switch (llamada tabla de direcciones MAC). Después de comparar las direcciones que vienen en el paquete con las almacenadas, el conmutador escoge la ruta apropiada y lo reenvía solamente por el puerto correcto.

Un switch aprende del entorno las direcciones MAC que le rodean y crear tablas para recordar donde está cada una, es lo que le diferencia del concentrador o hub. Crean canales virtuales de comunicación entre pares de puertos de tal forma que la comunicación entre un par de puertos no se ve afectada por otra comunicación entre cualquier otro par de puertos y así evita colisiones:



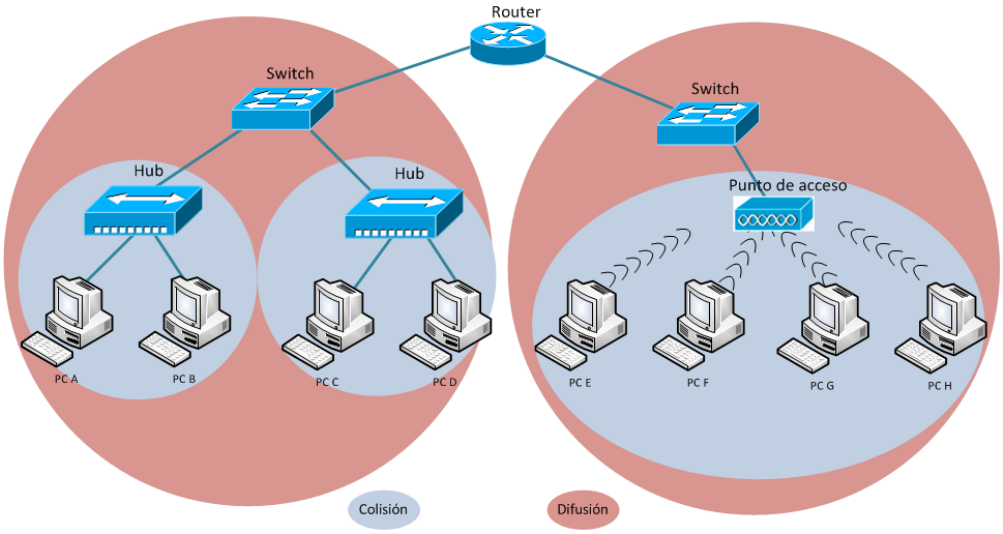
El switch no crea dominios de difusión, puesto que esto son segmentaciones a nivel 3, es decir, un dominio de difusión equivale a una red y el dispositivo que separa unas redes de otras es el router.

Los dominios de difusión son los sitios de la red que se pueden separar de acuerdo con la dirección de red que los identifica. Los dispositivos capaces de crear dominios de difusión, o mejor dicho, de separar dominios de difusión, son los routers.

Si en una red introducimos un router, por lo menos tendremos la capacidad de crear dos dominios de difusión diferentes, ya que un router como mínimo debe tener la capacidad de trabajar con dos direcciones de red diferentes, dicho de otra forma, si en una red ponemos un router crearemos 2 subredes a partir de la original.

Un dominio de difusión típico es el que tenemos en nuestro hogar, está separado del resto de internet por el router-DSL o fibra que tenemos instalado, de forma, que el tráfico entre equipos de nuestro hogar nunca sale al exterior. El tráfico irá al exterior cuando, por ejemplo, visitemos una página web.

Por tanto, el tráfico de nuestro hogar no colisiona con el tráfico exterior. Dicho de otro modo dentro de un dominio de difusión puede haber uno o más dominios de colisión. Un dominio de colisión está dentro de un dominio de difusión.



Ejercicio Resuelto

En una instalación de red típica de un hogar: Un router de fibra con 4 conexiones alámbricas y WIFI, tenemos conectados 2 PCs por cable directamente al router y 2 tablets por WIFI.

¿qué dominios de colisión y de difusión encontraríamos?

Mostrar retroalimentación

Dominios de difusión solo hay uno que es en el que están todos los dispositivos de nuestra red los 2 PCs y las 2 tablets.

Dominios de colisión hay 3: cada cable que sale del router es uno (como tenemos 2 PCs conectados serían 2 dominios de colisión diferentes) y la red WIFI es un único dominio de colisión para todos los equipos conectados inalámbricamente (o sea, las 2 tablets son un dominio de colisión)

3.- Fundamentos del nivel de acceso a red

El elemento principal de un switch es su tabla de direcciones MAC, esta tabla contiene las direcciones MAC de los dispositivos del entorno y a partir de ella el switch conoce el puerto por el que debe envía un determinado paquete de datos.

En el momento inicial, de fábrica, el switch tiene la tabla de direcciones MAC vacía.

Para llenar la tabla de direcciones MAC hay dos formas:

- Dinámicamente, de la información que envían los dispositivos el switch aprende en que puerto esta cada dispositivo y anota en la tabla la dirección MAC del dispositivo y el puerto del switch al que se encuentra conectado directa o indirectamente.
- Estáticamente, a partir de la información introducida en el switch por el administrador de la red.

En este video se puede ver como aprende el switch y rellena su tabla de direcciones MAC

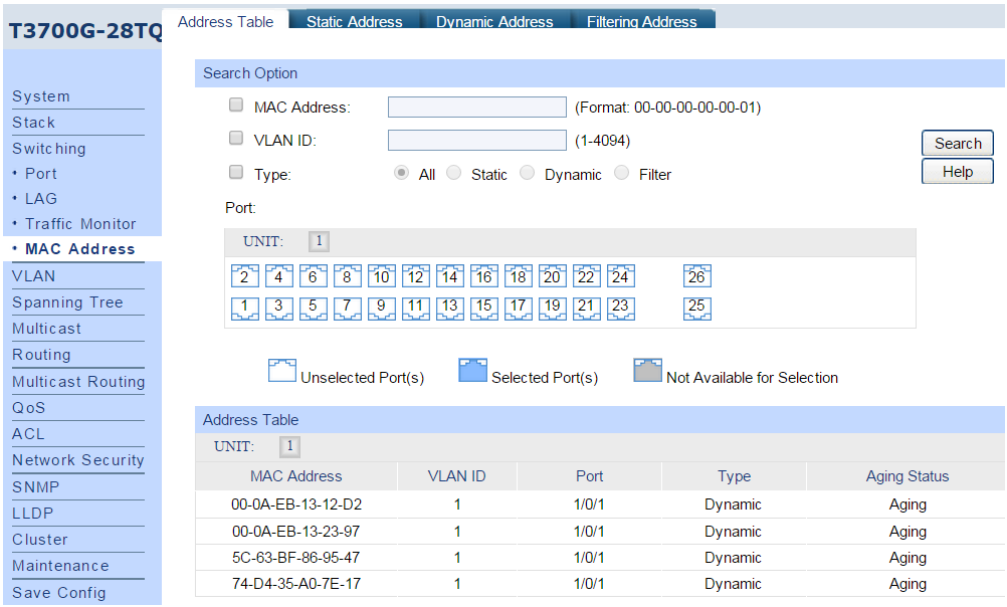
http://www.youtube.com/embed/mnfkwe6ri_E

Una entrada en la tabla de direcciones MAC se descarta automáticamente o expiran después de un determinado tiempo. La eliminación de entradas antiguas en la tabla de direcciones MAC asegura que la memoria de switch no se llenará y permite garantizar el funcionamiento correcto del switch ya que podrían producirse apagado de equipos, conexión de un equipo en otro puerto del switch, etc.

Se puede asignar una dirección MAC a una interface o puerto de forma permanente. Algunas razones para asignar una dirección MAC estática a una interface pueden ser:

- El switch no hace expirar automáticamente la dirección MAC.
- Se pretende mejorar la seguridad y evitar que cualquier máquina pueda conectarse a la red

Los datos que encontramos en una tabla MAC como **mínimo** son: dirección MAC, puerto y tipo (dinámico o estático).



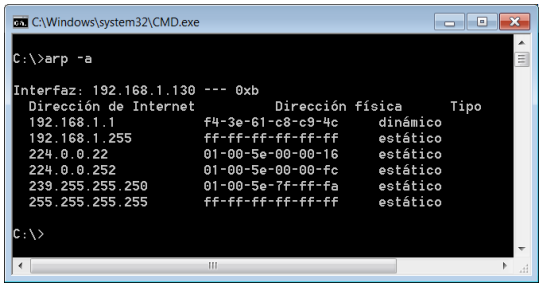
3.1.- El protocolo ARP

El protocolo ARP ofrece dos funciones básicas:

- Resolución de direcciones IP a direcciones MAC
- Mantenimiento de una caché de las asignaciones.

Cuando un dispositivo quiere comunicar con otro, a nivel de aplicación se suelen manejar nombres (origen y destino) que, por el protocolo DNS, acaban traduciéndose en IPs. Este problema vuelve a aparecer cuando se pasa del nivel IP al acceso a la red, debemos traducir las IPs en MAC, aquí es donde aparece el protocolo ARP, que viene a ser el equivalente al protocolo DNS en un nivel inferior.

Cuando el paquete pasa al nivel de acceso a red, se consulta la tabla denominada tabla ARP o caché ARP. La tabla ARP almacena en la RAM del dispositivo una relación de IPs con sus MACs correspondientes (En Windows podemos ver esta tabla con arp –a). Si el destino se encuentra en la tabla ARP, los datos son enviados a la MAC destino indicada en la tabla, pero si no se encuentra se envía un broadcast (destino MAC: FF-FF-FF-FF-FF-FF) que llega a todos los dispositivos de la red y, al que responderá el dispositivo que tenga la IP que se busca.



La tabla ARP se mantiene dinámicamente, se aprende del tráfico que llega al dispositivo, de broadcast, o de entradas estáticas en la tabla ARP.

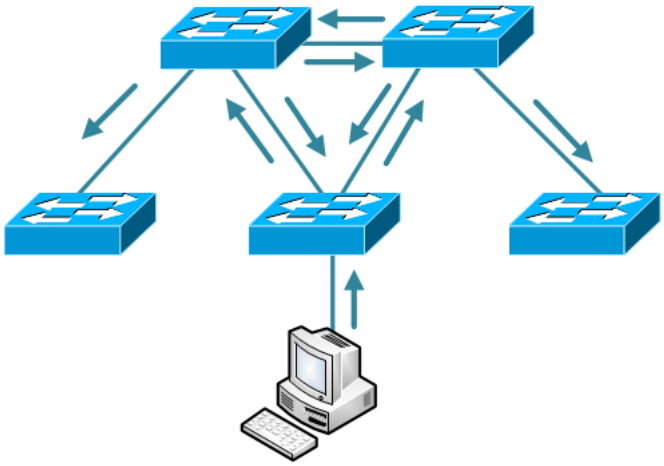
Para cada dispositivo, un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado.

Con la opción -a se muestra la tabla ARP y con la opción -s se introduce una entrada estática.

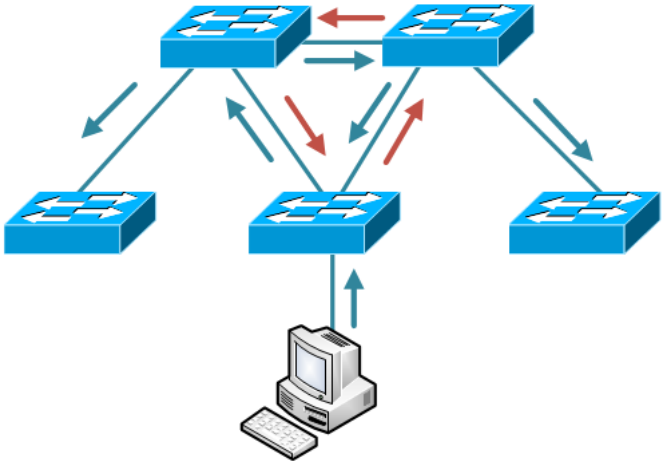
3.2.- Las tormentas de broadcast

Como consecuencia de lo que hemos comentado en el apartado anterior hay ocasiones en que el dispositivo no sabe la MAC destino y para conseguir averiguarla envía un paquete a todos los dispositivos de la red (broadcast), si en la red tenemos conexiones entre switchs que formen un circuito cerrado puede suceder que la petición ARP esté dando vueltas y, muchas peticiones de este tipo pueden saturar la red, esto es lo que se denomina tormenta de broadcast.

Supongamos el siguiente esquema, el PC con IP 192.168.0.100 quiere acceder al PC con IP 192.168.0.200, en su tabla ARP no se encuentra una línea asociada a esta IP, desconoce su MAC. Y ahora supongamos que este PC 192.168.0.200 no se encuentra en la LAN, se emitirá una petición ARP de broadcast que se propagará por todos los switchs, cada switchs recibirá la petición y la reenviará por todos sus puertos.



Pero la petición de broadcast no encontrará respuesta y habrá conexiones en las que estará dando vueltas produciendo una tormenta de broadcast.



El origen de las tormentas de broadcast está en la redundancia de las rutas

Los switchs inundan con peticiones broadcast todas las interfaces o puertos, salvo la interface por donde llegó la trama de petición con la esperanza de que el destinatario desconocido se encuentre en alguno de los segmentos de red. Si no aparece se producen bucles en nuestra instalación, esto puede llevar a una "tormenta de broadcast".

Una forma de evitar estas tormentas es conectar los switchs de la red en estructura de árbol, donde en la zona troncal colocaríamos los switchs más rápidos.

3.3.- El protocolo spanningtree

Este protocolo se encuentra en la capa dos del modelo OSI, la principal función de este protocolo es gestionar los bucles que se encuentren en la topología de la red. (Ojo, el hecho de que haya bucles no significa un mal diseño de red, puede que queramos tener distintas rutas para evitar que una mala conexión bloquee la comunicación de red)

El funcionamiento de STP es calcular una ruta única entre los dispositivos de red y mantiene los enlaces redundantes desactivados, solamente se activarán en caso de un fallo. El protocolo STP utiliza un algoritmo para transforma una red física en malla en una red lógica en árbol.

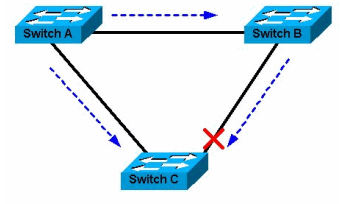
Ejercicio Resuelto

Tenemos 3 swtichs conectados en bucle, estos switch utilizan el protocolo STP

¿Qué ocurrirá cuando empiecen a intercambiar información por este protocolo?

Mostrar retroalimentación

Los switchs descubren que hay un bucle y proceden a anular una de las conexiones



4.- Fundamentos del nivel de internet

A nivel de la capa de Internet o red se utiliza la dirección IP para el direccionamiento, es decir, para que un dispositivo pueda conectarse en red necesita una dirección IP.

La dirección IP es una dirección de red lógica que identifica un dispositivo en particular dentro de la red de forma única, es decir, no puede haber dos dispositivos dentro de la misma red con el mismo número de IP.

El direccionamiento en Internet es distinto del que podemos llevar a cabo en las redes LAN. En el espacio WAN las direcciones las gestiona InterNIC, mientras que en las LAN son gestionadas por el administrador de la red. Esto implica que en una LAN podemos escoger el número y el tipo de direcciones que queramos dentro de los rangos reservados para ello, pero no en Internet. Si queremos que una dirección sea válida para viajar en Internet tenemos que solicitarla y pagar por ella (esto es lo que nuestro ISP hace y nos lo repercute a nosotros).

El objetivo principal es el mismo, poder tener identificados todos los elementos de una red para poder establecer comunicaciones entre sí

La dirección IP es asignada por InterNIC (Internet Network Information Center), ahora llamada ICANN (Internet Corporation for Assigned Names and Numbers).

4.1.- Dirección IPv4

Como vimos en la primera unidad es número de 32 bits, con este método se pueden identificar 2^{32} (4.294.967.296) direcciones, aunque no se puedan utilizar todas para identificar equipos.

Una dirección IP consta de dos partes, es decir, los 32 bits se dividen en dos grupos:

- Identificador de red: Va desde el comienzo de la dirección hasta un número concreto de bits.
- Identificador de equipo: Va desde el término del identificador de red hasta el último de los 32 bits.

Ejemplo: 192.168.0.1 expresado en binario 11000000.10101000.00000000.00000001

En este caso hay 24 bits para identificar la red y 8 para identificar a los equipos dentro de la red.

Ejemplo: 10.0.0.1 expresado en binario 00001010.00000000.00000000.00000001

Es decir 8 bits para identificar la red

Mientras más bits utilicemos para la identificación de red menos bits podremos utilizar para los equipos y como consecuencia más pequeña será la red. Para indicar esta delimitación de identificador de red e identificador de equipo se utiliza la máscara, que es una expresión de 32 bits, donde los bits de red están todos a 1 y los bits de equipo están todos a 0.

En el caso de los dos ejemplos anteriores:

11000000.10101000.00000000.00000001

Su máscara será 1111111.11111111.11111111.00000000 que expresado en decimal será 255.255.255.0, en notación corta /24

00001010.00000000.00000000.00000001

Su máscara será 1111111.00000000.00000000.00000000, que expresado en decimal será 255.0.0.0, en notación corta /8

En los 90 fue abandonado el primer sistema de direcciones IP con clase, este sistema consistía en que dependiendo de los primeros bits de la dirección IP se determinaba la máscara según la siguiente tabla de clases:

CLASE	RANGO	Máscara (notación decimal y corta)		Nº de IPs disponibles en la red
A	1.0.0.0 - 127.255.255.255	255.0.0.0	/8	16777216
B	128.0.0.0 - 191.255.255.255	255.255.0.0	/16	65536
C	192.0.0.0 - 223.255.255.255	255.255.255.0	/24	256
D	224.0.0.0 - 239.255.255.255	Reservadas para multicast		
E	240.0.0.0 - 247.255.255.255	Reservadas para usos experimentales		

Además de las direcciones marcadas como reservadas hay otras que no se pueden usar:

- 0.0.0: Se utiliza cuando se están arrancando las estaciones, hasta la carga del sistema operativo, luego no se usa.
- 0.0.1: Para especificar la estación actual, cuando se desea especificar el ordenador local (al igual que podría utilizar la IP asignada).
- Bits identificativos de dispositivo con todo 0: Indica la red actual, NO se puede asignar a ningún dispositivo
- Bits identificativos de dispositivo con todo 1: Difusión (broadcast). Para enviar mensajes a todas las estaciones dentro de la misma subred (todas las estaciones con el mismo número de red). NO se puede asignar a ningún dispositivo.

No hay que confundir las direcciones de difusión de las subredes (para enviar mensajes a las estaciones de la misma subred) con las direcciones de la clase D, que se utilizan para agrupar estaciones y enviarlas mensajes de difusión (pueden pertenecer a redes o subredes distintas).

El inconveniente de este sistema es que limita las posibilidades y, debemos elegir entre tres tamaños para nuestra red: C que nos permite hasta 256 IPs en nuestra red, B que nos permite hasta 65536 IPs en nuestra red y A que nos permite hasta 16777216 IPs en nuestra red, a estas IPs hay que restarle 2 (red y difusión) que son las que están disponibles para los dispositivos.

Y la ventaja es que es muy cómodo de utilizar porque el identificador de red acaba coincidiendo con una de las cuatro cifras decimales en que se expresan las IPs habitualmente.

Actualmente se utiliza un direccionamiento sin clase, es decir, se puede usar máscaras diferentes a /8 /16 /24, lo que permite ajustar la máscara al tamaño de red deseado, así por ejemplo si en la red vamos a tener 2000 equipos elegimos una máscara /21 que nos permite hasta 2048 valores diferentes y no elegimos una máscara /16 donde desaprovechamos más de 63000 IPs.

Y por último, se han establecido otros rangos de direcciones IP para ser asignados a redes locales que se conectan a Internet a través de un proxy o mediante un router que sigue un protocolo NAT.

CLASE	RANGO RESERVADO
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

A parte de los diferentes protocolos que se pueden utilizar, existen técnicas para poder aprovechar mejor estas direcciones (subredes, superredes, CIDR).

El agotamiento del espacio de direcciones IPv4 por la expansión de Internet ha provocado la adopción de diferentes técnicas para un mejor reparto de las direcciones. Una de estas técnicas la vemos en todas las pequeñas redes que comparten conexón a internet : **NAT , Network Address Translation**, esta traducción se realiza en los routers que dan la conexión a internet, de forma que cuando consultamos una web por ejemplo, el router sustituye la IP priviada por la IP pública y envia la petición.

Autoevaluación

¿Pertenecen las IPs 192.168.0.15 y 192.168.0.129 a la misma red?

- ○ Si
- ○ No
- ○ No se puede decir con seguridad

Incorrecto: Incorrecto, para saber si pertenecen a la misma red necesitamos saber el tamaño de la red, es decir, 192.168.0.15 está en una red, pero ¿Dónde empieza? ¿En 192.168.0.0 o en otra IP? ¿Dónde acaba en 192.168.0.255 o en 192.168.1.255 o …?. Esa información nos la da la máscara, que es el dato que falta.

Incorrecto: Incorrecto, para saber si pertenecen a la misma red necesitamos saber el tamaño de la red, es decir, 192.168.0.15 está en una red, pero ¿Dónde empieza? ¿En 192.168.0.0 o en otra IP? ¿Dónde acaba en 192.168.0.255 o en 192.168.1.255 o …?. Esa información nos la da la máscara, que es el dato que falta.

Correcto No se puede decir con seguridad: Efectivamente, para saber si están en la misma red necesitamos conocer el tamaño de la red y esa información la indica la máscara.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

Ejercicio Resuelto

En un instituto la configuración IP de nuestro equipo es la siguiente:

IP: 172.23.160.118

Máscara: 255.255.252.0

Puerta de enlace: 172.23.160.1

DNS: 8.8.8.8

¿Cuántos equipos puede haber en el instituto?

¿Es una IP un poco extraña, no?

Mostrar retroalimentación

Para saber cuantos equipos puede haber solo tenemos que analizar la máscara:

Su máscara será 1111111.11111111.111111**00**.**00000000** que expresado en decimal será 255.255.252.0, en notación corta /22, por tanto, las posiciones rojas que son las que podremos manipular en las IPs de los equipos nos dan para 2 elevado a 10 combinaciones diferentes, es decir, para 1024 IPs diferentes, pero tenemos que restar 2 IPs (la primera y la

última que se dedican a identificar la red y a broadcast o difusión la última). Eso nos da un tamaño de red de hasta 1022 dispositivos conectados.

La IP no es extraña, normalmente se usamos IPs privadas en empresas y domicilios, y el rango de IPs más habitual es 192.168.x.x pero si la red es un poco más grande (mayor de 253 equipos) el rango estandar a usar es 172.16-31.x.x

4.2.- Dirección IPv6

IPv6 surge para poder solucionar todos los problemas que IPv4 no resuelve. El mayor de los problemas es la escasez de direcciones IP en Internet.

Mientras IPv4 tiene un espacio de direcciones de 2^{32} (4.294.967.296), IPv6 tiene 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456).

Las máscaras para identificar subredes, routers y rangos de direcciones IPv6 son expresadas de la misma forma que en la notación CIDR utilizada en IPv4.

En IPv6 la longitud del prefijo indica un conjunto mínimo de bits comunes del PREFIJO que no se deben cambiar y que identifican unívocamente a cualquier clase de la DIRECCION IPv6.

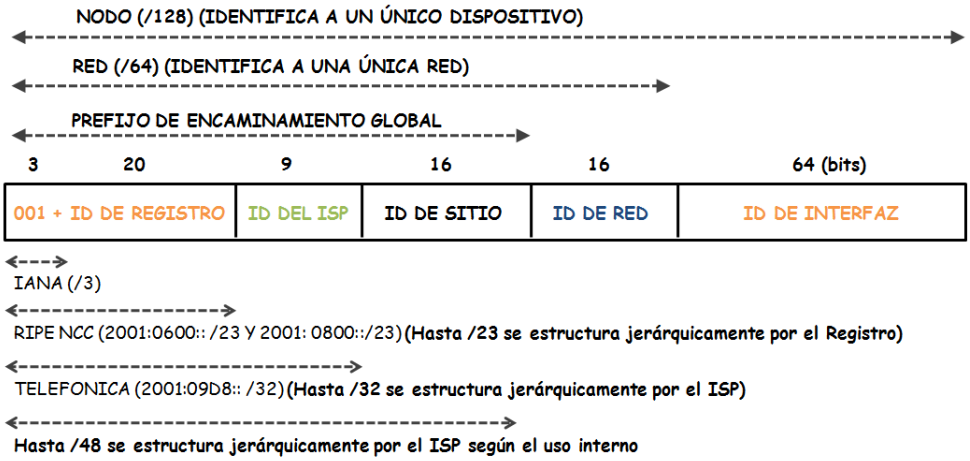
En las redes IPv6 el prefijo es siempre /64, es decir, las redes en IPv6 son de tamaño fijo.

Un prefijo de dirección IPv6 se representa con la siguiente notación:

direccion-ipv6/longitud-prefijo

Las direcciones identifican interfaces individuales o conjuntos de interfaces. Se clasifican en tres tipos:

- Anycast identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast.
- Multicast identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección.
- Unicast identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Hay dos tipos:
  - Dirección unicast local de sitio (privada): No es enrutable fuera de la red. Es el equivalente a la ipv4 privada. NO recomendado su uso.
  - Dirección unicast local exclusiva. Sustituyen a las anteriores.
  - Dirección unicast local de enlace (privada): Para tareas internas.
  - Dirección unicast global (pública): Es única en el mundo, por lo que se pueden enrutar a nivel mundial sin ninguna modificación, son las que utiliza una máquina conectada a internet. Las direcciones unicast globales normalmente están compuestas por un prefijo de enrutamiento global de 48 bits y un ID de subred de 16 bits



En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

Para saber más

El Gobierno de España tiene una web sobre información de IPv6:

IPv6

4.3.- Subredes

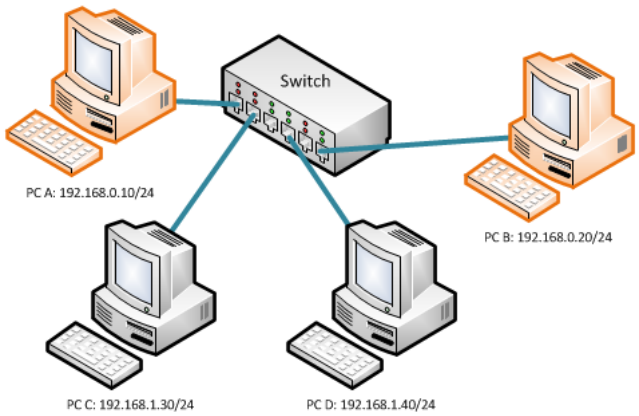
Como vimos, una dirección IP consta de dos partes, identificador de red e identificador de equipo. Un equipo se comunica solamente con los equipos que tienen el mismo identificador de red.

En este sentido hay 3 conceptos muy relacionados en redes:

- CIDR (Classless Inter-Domain Routing), en 1993 se estableció el enrutamiento entre dominios sin clases, es decir, declara obsoleto la asignación de máscaras “naturales” (A B y C) dependiendo de los bits de comienzo de la IP y establece que se puede utilizar máscara diferentes a los prefijos naturales anteriores, ajustando así más el tamaño de las redes. Este concepto engloba los dos siguientes:
- VLSM (Variable Length Subnet Mask), significa que a la hora de crear subredes, en vez de crear subredes todas iguales, es decir, con la misma máscara (por ejemplo dividir una red /24 en 4 subredes /26), creamos subredes con máscaras diferentes de forma que las divisiones realizadas se adaptan lo mejor posible a los tamaños necesarios.
- Sumarización, digamos que es el proceso inverso a la realización de subredes con VLSM, para evitar que en los routers las tablas de enrutamiento sean muy extensas indicando cada uno de los diferentes caminos a cada una de las diferentes subredes se admite englobar en una sola red diferentes subredes y simplificar la tabla de enrutamiento de forma que solo se presente una entrada con la red resumida y el camino a seguir.

Para identificar una red se utiliza la primera IP posible junto con la máscara. Por ejemplo 192.168.0.0/24 identifica a la red que comienza en la IP 192.168.0.0 y acaba con la última combinación posible 192.168.0.255. Es decir, los primeros 24 bits (3 bloques decimales) identifican la red y no cambian, los últimos 8 bits (último bloque decimal) identifican a los equipos, cambian desde la primera combinación 0 (00000000) hasta la última 255 (11111111).

Supongamos el siguiente esquema de red:



En este caso, aunque todos los equipos están conectados a un switch, la comunicación solo funcionará entre PC A y PC B por un lado, y entre PC C y PC D por otro.

¿Por qué? Porque el PC A tiene la IP 192.168.0.10, su máscara es /24, es decir, que los bits identificativos de red son los primeros 24 bits, o dicho de otra forma, los tres primeros bloques decimales identifican la red (192.168.0) y el último bloque decimal (10) identifica al equipo dentro de la red, o lo que es lo mismo, los últimos 8 bits identifican al equipo. De forma similar sucede con el resto de equipos, puesto que todos tienen la máscara /24, sus tres primeros bloques decimales identifican la red. Por tanto, hay 2 redes (la que comienza por 192.168.0 y la que comienza por 192.168.1).

Como un equipo solo comunica con los equipos de su red el PC A solo comunica con PC B, que es el que tiene los mismos bits identificativos de red y viceversa. Y el PC C solo comunica el PC D y viceversa.

¿Qué sucede si el usuario del PC A quiere comunicar con el PC C? Pues, sencillamente, que el sistema ni siquiera intenta la comunicación porque no el PC C no está en su red.

Cuando por cualquier motivo necesitamos dividir nuestra red para independizar unos equipos de otros realizamos una técnica llamada subneting o hacer subredes.

Para hacer esta división basta con aumentar el número de bits dedicados a identificar la red, a medida que aumentan los bits de red disminuyen los bits de identificación de equipos, es decir, las redes obtenidas son más pequeñas.

Veamos un ejemplo, disponemos de la red 172.16.0.0/16 y queremos dividirla en 256 subredes (2^8), para ello aumentamos los bits de red de /16 a /24, esos ocho bits nos van a dar 256 combinaciones que son: 172.16.0.0/24 172.16.1.0/24 172.16.2.0/24, y así sucesivamente hasta 172.16.256.0/24

Red original:

1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
172								16								0								0							

Subredes resultantes

1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
172								16								0								0							
1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0

172	16	1	0

… así sucesivamente hasta:

1 1 0 0 0 0 0 0	0 0 0 1 0 0 0 0	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0
172	16	255	0

Debes conocer

En internet podemos encontrar calculadoras específicas para crear subredes como la que se muestra en el siguiente enlace, bastará con indicar la dirección IP (172.16.0.0), la máscara original (16) y la máscara final (24):

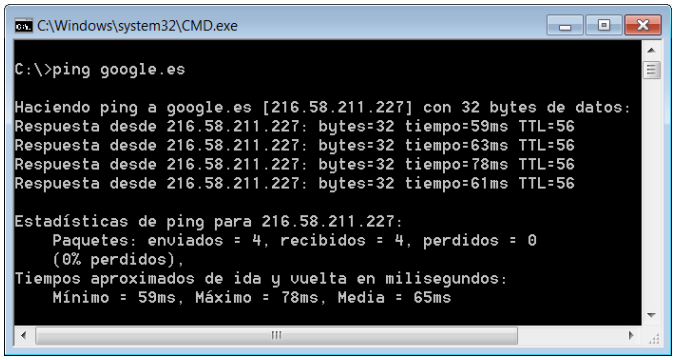
https://aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi1

4.4.- ICMP

El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

En este protocolo están basadas las herramientas ping y traceroute, que envían mensajes de petición echo ICMP para comprobar si un dispositivo está disponible, el tiempo de respuesta y la cantidad de dispositivos que atraviesa.

Es muy típico usar estas herramientas para comprobar la conexión con nuestro router.



5.- Fundamentos del nivel de aplicación

En la capa de aplicación están los protocolos más cercanos al usuario, son los más conocidos, cada protocolo está asociado a un servicio, una aplicación que está a la espera en un puerto determinado de peticiones de clientes.

Los puertos predeterminados de los servicios más habituales son:

Puerto	Servicio
UDP 67	DHCP
UDP 53	DNS
TCP 80	HTTP
TCP 443	HTTPS
TCP 21	FTP

5.1.- DHCP

Asignación en IPv4:

El direccionamiento dinámico es un mecanismo que nos proporciona una configuración de los parámetros de red de forma automática. La dirección proporcionada es la adecuada para que nuestro nodo funcione correctamente en la red, ya sea una LAN o una WAN. Este mecanismo recibe el nombre de servicio DHCP (Dinamic Host Configuration Protocol).

DHCP puede usarse cuando el número de direcciones IP es menor que el número de computadores y todos no están conectados a la vez, como en un proveedor de servicio de Internet (ISP), de esta manera se desaprovechan menos las direcciones.

Para que funcione este mecanismo deberá existir un servidor de direcciones DHCP en la red, encargado de asignar las direcciones a los host. Además, los host deberán configurar sus interfaces de red de manera que ejecuten el servicio DHCP, generalmente existe siempre una opción de configuración tal como “Obtener una dirección IP automáticamente”.

El protocolo DHCP se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131. Para redes con IPv6 se ha creado DHCPv6 publicado como RFC 3315.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

1. **Asignación manual o estática:** Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.
2. **Asignación automática:** Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
3. **Asignación dinámica:** el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

En IPv4 hay que mencionar también la **autoconfiguración** (si el cliente no obtiene IP puede generar aleatoriamente una propia), de hecho la IETF reserva el rango 169.254.0.0/16, como se indica en RFC 3330. **Esto es síntoma de que el servicio DHCP no funciona o no hay conexión hasta él.**

El diálogo entre cliente y servidor DHCP se lleva a cabo a través de los puertos UDP 68 en el cliente y 67 en el servidor

Un cliente DHCP obtiene una concesión para una dirección IP de un servidor DHCP. Antes que se acabe el tiempo de la concesión, el servidor DHCP debe renovar la concesión al cliente o bien este deberá obtener una nueva concesión.

Un servidor DHCP puede proveer de una configuración opcional al dispositivo cliente: Dirección del servidor DNS, Puerta de enlace, Máscara de subred, Tiempo máximo de espera del ARP, MTU (Unidad de Transferencia Máxima), Servidores NTP (Protocolo de Tiempo de Red). Servidor SMTP, Servidor TFTP, Nombre del servidor WINS.

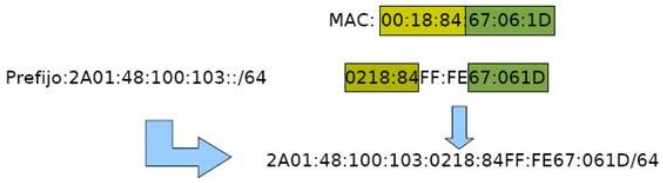
El servidor DHCP guardará en una base de datos las IP que vaya concediendo.

Asignación en IPv6:

En IPv6 el protocolo usado es DCHPv6 que aunque **no** es usado habitualmente tiene sentido porque brinda más control al administrador de la red sobre las asignaciones.

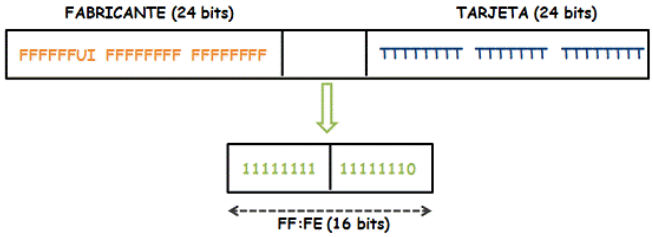
Hay varios tipos de configuración:

1. **Configuración manual**. Similar a IPv4, pero no es usada en la práctica
2. **Configuración dinámica sin estado (el dispositivo genera la IP) con EUI-64 (sin servidor DHCP)**



En IPv6 se supone que los dispositivos que no son PC, así como las terminales de computadoras, están conectados a la red. El mecanismo de configuración automática se introdujo para permitir networkingplug-and-play de estos dispositivos a fin de lograr la reducción de los gastos administrativos.

El dispositivo aprende el prefijo /64 y calcula el resto de su IP utilizando eui-64.



Se pone a 1 el bit U para indicar alcance universal. Si lo pusiéramos a 0 indicaríamos que el alcance es local. Se pone a 0 el bit I para indicar que es una dirección de unidifusión (Individual). Si lo pusiéramos a 1 indicaríamos multidifusión (Grupo).

En ausencia del router, el equipo solo podrá generar la dirección de enlace local, aunque esto será suficiente para que haya comunicación con los demás equipos de la red.

3. **Configuración automática sin estado (con servidor DHCPv6)** El servidor DHCP no asigna las IPs pero si aporta información adicional. Por tanto, los clientes del modo sin estado DHCPv6 usan DHCPv6 para obtener parámetros de configuración de red distintos de la dirección IPv6 (por ejemplo, direcciones de servidor DNS).
4. **Configuración automática con estado o "statefull" (con servidor DHCPv6)**En el modo con estado DHCPv6, los clientes obtienen la dirección IPv6 y otros parámetros de configuración de red mediante DHCPv6. Además el servidor DHCP recuerda las IPs

Nota: la máscara de subred la proporcionan los anuncios de enrutador, no el servidor DHCPv6. En DHCPv6 también se permite a los clientes la solicitud de múltiples direcciones IPv6.

Autoevaluación

La IP de nuestro equipo es 169.254.120.251 ¿que podemos concluir?

- ○ Nada. Todo es correcto.
- ○ Es una IP de autoconfiguración. Hay algún problema para conseguir la IP del servidor
- ○ Posiblemente es una IP estática

No. Se trata de una IP de autoconfiguración y, por tanto, nuestro equipo no ha obtenido IP del servidor DHCP lo que indica que debe haber algún problema para conectar con el mismo.

Opción correcta

No. Es una IP de autoconfiguración, generada de forma dinámica y porque hay algún problema para conectar con el servidor DHCP.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

5.2.- DNS

DNS, Domain Name System (Sistema de Nombres de Dominio), hace referencia tanto a un servicio que responde a peticiones de número de IP de un nombre o nombre de un número de IP. La principal tarea que realiza es asociar nombres e IP.

Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet.

Reflexiona

Si hacemos un símil con la red telefónica, las direcciones IP equivaldrían a los números de teléfono. Si un usuario quiere establecer comunicación con otro, debe marcar un número en el terminal.

En las redes informáticas, si un PC quiere establecer comunicación con otro, debe disponer de una dirección (dirección IP). De hecho, cuando escribimos una dirección URL (http://www.urldeejemplo.com/camino/al/recurso) en nuestro navegador, estamos "marcando" realmente la dirección IP con la que queremos conectarnos. Esto es posible gracias al servicio DNS, con él podemos utilizar letras en lugar de números (son más fáciles de recordar), es decir, el servicio DNS asocia a los nombres direcciones IP, por poner un símil es como una guía telefónica

Una vez que todos los equipos tienen asignada una dirección, se pueden emplear técnicas (subredes, superredes, CIDR) para que la gestión de estas direcciones agilice el funcionamiento de la red. En la red de teléfono se empleaban los prefijos (942 Cantabria, 985 Asturias, 91 Madrid, 93 Barcelona, etc.).

5.3.- HTTP

Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto) es, dicho de forma sencilla, el lenguaje de comunicación que se utiliza en la Web para que los clientes y los servidores puedan entenderse entre sí. De manera un poco más formal, HTTP es un protocolo a nivel de aplicación que se utiliza en sistemas de información hipermedia, colaborativos y distribuidos. Es el principal método de intercambio de información en WWW (World Wide Web), que no es lo mismo que Internet, ya que éste es un servicio, quizás el más utilizado, pero Internet se compone de muchos más protocolos, servicios y funcionalidades.

La palabra Hipertexto procede de la característica de estas páginas que permite saltar de unas a otras, ofreciendo zonas que actúan como enlaces

Para saber más

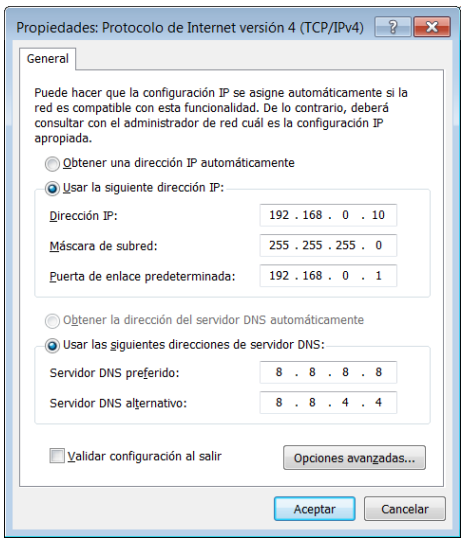
Puedes conocer algo más sobre el protocolo HTTP en este video

5.4.- Configuración del adaptador

Aunque lo más cómodo es una configuración automática de los parámetros de red, en determinados casos (en muchas ocasiones para resolver problemas en nuestra red) debemos configurar manualmente los parámetros de nuestra conexión a internet.

Estos son:

- Dirección IP, deber ser única en la nuestra red.
- Máscara de red: determina el tamaño de nuestra red.
- Puerta de enlace predeterminada: la IP del dispositivo de nuestra red por el que accedemos al exterior. Evidentemente un router que es el dispositivo que separa redes.
- DNS: IP del dispositivo (habitualmente fuera de nuestra red) o dispositivos, que nos permiten escribir direcciones web sin necesidad de conocer la IP.



Anexo. Licencia de Recursos

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	Autoría: Clker-Free-Vector-Images Licencia: Pixabay License Procedencia: https://pixabay.com/vectors/server-network-local-wired-311338/		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría:Godred Fairhurst Licencia: CC BY-SA 3.0 Procedencia:https://erg.abdn.ac.uk/users/gorry/course/lan-pages/hub.html		Autoría:Desconocido Licencia: CC BY-SA 3.0 Procedencia:https://instrumentationtools.com/ether bus-animation/
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla ICANN
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría:Desconocido Licencia: Desconocido Procedencia:https://www.muyseguridad.net/2015/12/14/servidores-dns-raiz/		Autoría:Desconocido Licencia: CC BY-SA 3.0 Procedencia:https://instrumentationtools.com/ether bus-animation/