

Tema 3. Tecnología Ethernet

1.- Introducción

La mayoría de los usuarios, cuando hablan de redes, **hacen referencia a la Red de Área Local, también conocida como LAN. No se debe** ignorar que detrás de esta denominación se encuentra un estándar llamado **Ethernet**, el cual determina las particularidades físicas y eléctricas que debe poseer una red tendida con este sistema.

También conocido como **IEEE 802.3**, esta norma define, **además de las características eléctricas, de longitud y diámetro de los cables, todos los elementos en juego dentro de una red**, es decir como debe ser conectado en cada escenario en particular y muchos otros parámetros.



Los orígenes de la tecnología Ethernet se puede rastrear prácticamente hasta principios de la década de 1970, siendo **Robert Metcalfe**, un ingeniero graduado en el **MIT** y la compañía **Xerox**, los principales precursores de ella. En la actualidad es el método más simple, seguro, y económico de montar una red entre computadoras, debido fundamentalmente a su flexibilidad, ya que entre otras tantas

características es posible utilizarse desde cable coaxial hasta fibra óptica para poder implementar una red con esta tecnología.

2.- Principio de funcionamiento. Colisiones.

La idea básica detrás de Ethernet es que todos los PC's dentro de una red, envíen y reciban datos de una forma en que se evite cualquier tipo de superposición, lo que sería desastroso. Es por ello que los datos que se envían o reciben mediante este estándar, deben ser fragmentados en fracciones más pequeñas y enviados a través de un método conocido como **Conmutación de paquetes**.



Básicamente esto consiste en que si una de los PC's de la red, quiere enviar un paquete de datos a otra, debe ser empaquetado, lo que finalmente da como resultado un paquete, el cual consta de varios datos tales como cabecera, dirección del dispositivo en la red a quién va destinado y qué dispositivo de la red lo está enviando. Además contiene datos de control y otras informaciones relativas al mismo como la cantidad de datos que transporta y otros.

Como dato importante, cabe destacar que estos paquetes se envían a todas los dispositivos que conforman la red, siendo los propios aparatos los que determinan si el paquete va dirigido a ellos o no, denegando todos los paquetes que no se dirigen estrictamente al dispositivo en particular.

Otro dato a tener en cuenta es que todos los dispositivos de una red pueden transmitir paquetes en cualquier momento en que así se requiera, sin embargo esto puede provocar problemas cuando dos

dispositivos intentan hacerlo al mismo tiempo, conociéndose este hecho como **colisión**.

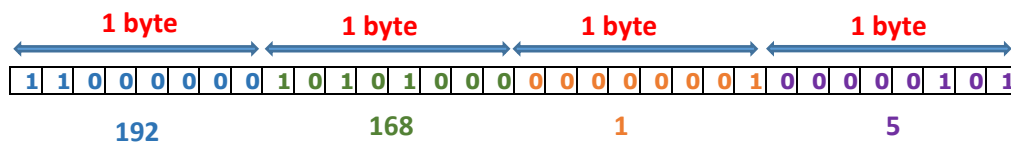


Es por ello que se creó **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** cuya traducción al español es *Acceso múltiple con escucha de portadora y detección de colisiones*, el cual es un protocolo utilizado en las redes Ethernet para solucionar este problema.

Mediante **CSMA/CD**, es posible que los dispositivos escuchen la red para determinar si el canal y los recursos se encuentran libres. En caso afirmativo, se podrá realizar la transmisión para no colisionar con otros paquetes.

3.- Dirección IP versión 4.

Una dirección IP, es un número formado por un total de 32 bits:



Con 32 bits, se puede llegar a expresar un número en decimal que va desde 0 hasta $2^{32} = 4.294.967.296$

Para facilitar el manejo de este número tan grande, usaremos lo que se llama **notación decimal punteada**. Se trata de pasar a decimal cada uno de los bytes anteriores, separándolos con un punto.

192.168.1.5

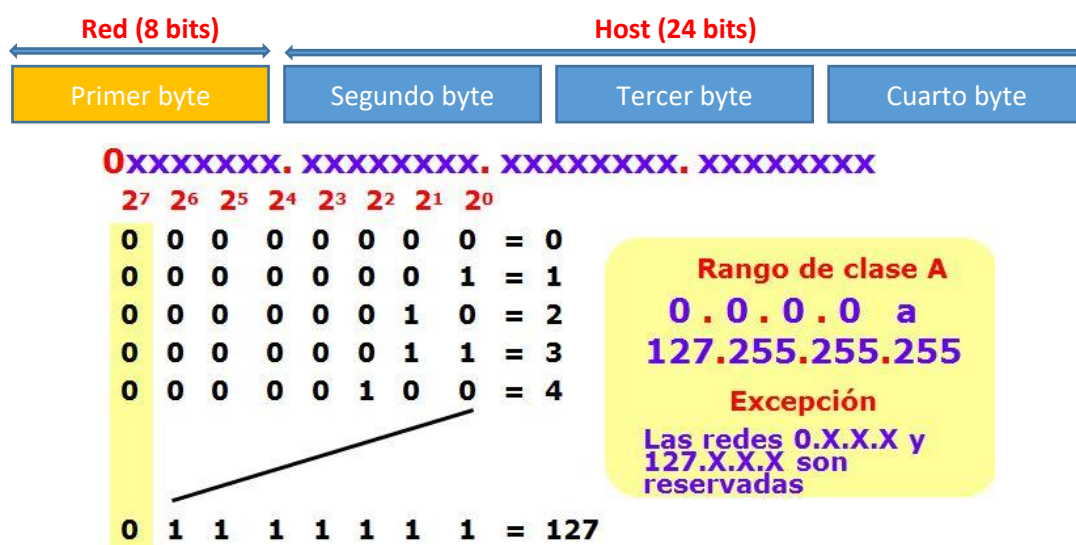
Las direcciones IP deben identificar, en cada red, a los dispositivos que la forman. La dirección IP **puede cambiar** ya sea por cambios en la red o porque el dispositivo encargado dentro de la red, de asignar las direcciones IP (router), decida asignar otra IP (por ejemplo, con el protocolo **DHCP**). A esta forma de asignación de la dirección IP, se denomina dirección IP **dinámica**.

$$\text{Número de host} = 2^8 \times \text{número de bytes asignados para host}$$

$$\text{Número de redes} = 2^8 \times \text{número de bytes asignados para redes}$$

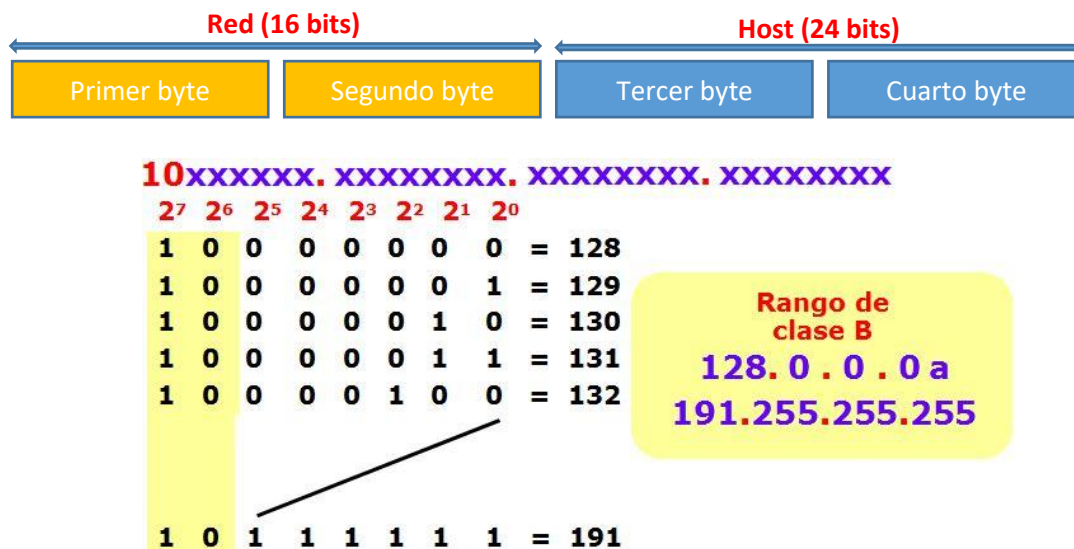
De los 4 bytes que forman una dirección IPV4, algunos bytes, identifican a los host y otros a la red a la que pertenecen. En función del número de bytes que identifican a la red, hablamos de **clases de ip**. Para identificar las clases, se usan los primeros bits del primer byte.

Clase A: El primer byte, es asignado para identificar la red y los tres restantes, para identificar el host. Todas las ip de los dispositivos que forman una red de clase A, tendrán el primer byte, idénticos. El primer bit del primer byte siempre es 0. Esta clase es para redes muy grandes, tales como las de una gran compañía internacional. Del IP con un primer octeto a partir de 0 al 127 son parte de esta clase. Los otros tres octetos son usados para identificar cada anfitrión. Esto significa que hay 126 redes de la clase A con 16.777.214 ($2^{24} - 2$) posibles anfitriones para un total de 2.147.483.648 (2^{31}) direcciones únicas del IP. Las redes de la clase A totalizan la mitad de las direcciones disponibles totales del IP.



Rango de direcciones privadas: de 10.0.0.0 a 10.255.255.255.
 La máscara de red predeterminada será la 255.0.0.0

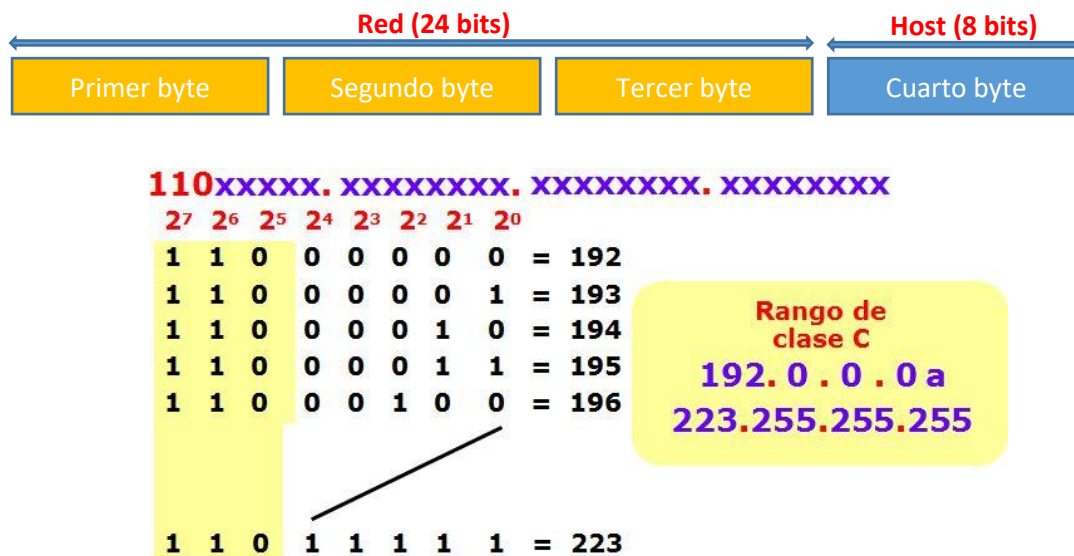
Clase B: El primer y segundo byte, son asignados para identificar la red y los dos restantes, para identificar el host. Todas las ip de los dispositivos que forman una red de clase B, tendrán el primer y segundo bytes, idénticos. Los dos primeros bits del primer byte, siempre serán 10. La clase B se utiliza para las redes de tamaño mediano. Un buen ejemplo es un campus grande de la universidad. Las direcciones del IP con un primer octeto a partir del 128 al 191 son parte de esta clase. Las direcciones de la clase B también incluyen el segundo octeto como parte del identificador neto. Utilizan a los otros dos octetos para identificar cada anfitrión (host). Esto significa que hay 16.384 (2^{14}) redes de la clase B con 65.534 ($2^{16} - 2$) anfitriones posibles cada uno para un total de 1.073.741.824 (2^{30}) direcciones únicas del IP. Las redes de la clase B totalizan un cuarto de las direcciones disponibles totales en el mundo.



Rango de direcciones privadas: de 172.16.0.0 a 172.31.255.255.
 La máscara de red predeterminada será la 255.255.0.0

Clase C: Los tres primeros bytes, son asignados para identificar la red y el restante, para identificar el host. Todas las ip de los dispositivos que forman una red de clase C, tendrán el primer, el segundo y el tercer bytes, idénticos. Los tres primeros bits, del primer byte, siempre serán 110. Las direcciones de la clase C se utilizan comúnmente para los negocios pequeños a medianos de tamaño. Las direcciones del IP con un primer octeto a partir del 192 al 223 son parte de esta clase. Las direcciones de la clase C también incluyen a segundos y terceros octetos como parte del identificador neto. Utilizan al último octeto para identificar cada anfitrión. Esto significa que hay 2.097.152 (2^{21}) redes de la clase C con 256 ($2^8 - 2$) anfitriones posibles

cada uno para un total de 536.870.912 (2^{29}) direcciones únicas del IP.
Las redes de la clase C totalizan un octavo de las direcciones disponibles totales del IP.



Rango de direcciones privadas: de 192.168.0.0 a 192.168.255.255. La máscara de red predeterminada será la 255.255.255.0

Existen dos clases más de ip, las clases **D** y **E**. La clase de D se usa para **multicasting** y la clase E para **investigación y desarrollo**.

Broadcast - los mensajes que se dirigen a todas las computadoras en una red se envían como broadcast. Estos mensajes utilizan siempre La dirección IP 255.255.255.255.

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

4.- Cálculo de subredes.

En redes de computadoras, cuando una red se vuelve muy grande, conviene dividirla en **subredes**, para reducir el tamaño de los dominios broadcast o simplemente, para hacer la red más manejable administrativamente. Mediante la división en subredes, una única dirección IP, por ejemplo, de Clase A, se puede utilizar para crear pequeñas sub-redes que proporcionen una mejor de gestión de la red.

Realizaremos a continuación, un ejemplo de cálculo de subred.

Ejemplo

A una compañía se le ha asignado la red **200.3.25.0**. Es una red de **clase C**, lo cual significa que puede disponer de 254 direcciones diferentes (la primera y la última dirección están reservadas, no son utilizables, ya que la primera es la dirección de la **propia** red y la última es la de **broadcast**). La **máscara de red** es **255.255.255.0 (o /24)**. La compañía decide dividir esta red en **8 subredes**. Se pide calcular:

- Las direcciones de cada subred.
- Las máscaras de cada subred.
- Las direcciones de broadcast de cada subred.
- Los rangos de direcciones de los host de cada subred.
- Número de host totales de cada red.

La máscara de red original en binario es:

255								255								255								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0

Como nos piden **8 subredes**, necesitaremos pedir prestados 3 bits para referenciar estas tres redes con lo cual, la máscara de subred tiene que recorrer tres bits más. Ampliaremos la máscara con tres bits de la porción que corresponde al host. Esto resultará en una máscara de subred tipo /27, que en binario sería:

255								255								255								224							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

255.255.255.224

Cada subred tendrá $2^5 = 32$ direcciones posibles, pero solo tendrá $2^5 - 2 = 30$ direcciones asignables a los hosts, puesto que la primera dirección (con todos los bits de host a 0) identifica a la propia subred y la última dirección de cada subred (todos los bits de host a 1) se reserva para el broadcast.

El número total de subredes, será $2^{\text{número de bits prestados}} = 8$ que es justo, el número de subredes que nos pedía el ejercicio. Con todo ello, podríamos realizar un informe final tal como:

Subred 1

Dirección de red: **200.3.25.0**

Dirección de Broadcast: **200.3.25.31**

Máscara de red: **255.255.255.224**

Número total de hosts posibles: **30**

Rango útil de ip: **200.3.25.1** hasta **200.3.25.30**

Aunque esta subred, al ser la primera, no se puede usar.

Subred 2

Dirección de red: **200.3.25.32**

Dirección de Broadcast: **200.3.25.63**

Máscara de red: **255.255.255.224**

Número total de hosts posibles: **30**

Rango útil de ip: **200.3.25.33** hasta **200.3.25.62**

Subred 3

Dirección de red: **200.3.25.64**

Dirección de Broadcast: **200.3.25.95**

Máscara de red: **255.255.255.224**

Número total de hosts posibles: **30**

Rango útil de ip: **200.3.25.65** hasta **200.3.25.94**

Y así sucesivamente; de cada subred a la siguiente, el último byte aumenta en 32. Dependiendo del tipo de máscara de subred utilizado.

5.- Dirección MAC.

La dirección **MAC** es un identificador **único** que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados, desde un ordenador o móvil hasta routers, impresoras u otros dispositivos. Sus siglas vienen del inglés, y significan **Media Access Control**. Como hay dispositivos con diferentes tarjetas de red, como una para WiFi y otra para Ethernet, algunos pueden tener diferentes direcciones MAC dependiendo de por dónde se conecten.

Dirección MAC

01:3A:1D:54:6B:32

Identificador Unico del fabricante (OUI)

identificador del producto (UAA)

Las direcciones MAC están formadas por 48 bits representados generalmente por dígitos hexadecimales. Como cada carácter hexadecimal, equivale a cuatro bits, tenemos un total de 12 caracteres hexadecimales. Es decir, la dirección MAC acaba siendo formada por **12 dígitos agrupados en seis parejas** separadas generalmente por dos puntos, aunque también puede haber un guión o nada en absoluto.

Otra cosa que tienes que tener en cuenta es que la mitad de los bits de una dirección MAC, tres de las seis parejas, identifican al fabricante, y la otra mitad al modelo. Por ejemplo, los números 01:3A:1D del ejemplo de dirección **pertenecen siempre al mismo fabricante**, mientras que los últimos seis determinan el modelo de dispositivo. Hay buscadores especializados para saber el fabricante de un dispositivo dependiendo de los primeros seis dígitos de su MAC.

Como son identificadores únicos, las MAC pueden ser utilizadas por un administrador de red para permitir o denegar el acceso de determinados dispositivos a una red. En teoría son fijas para cada dispositivo, aunque **existen maneras de cambiarlas** en el caso de que quieras hacerlas más reconocibles en tu red o evitar bloqueos.

Esta exclusividad de cada MAC hacia un único dispositivo también exige que tengas especial cuidado. Por ejemplo, cuando te conectas o intentas conectarte a un router, **tu móvil u ordenador le enviará automáticamente su MAC**. Es una de las razones por las que tienes que saber siempre dónde te conectas a Internet y a quién le pertenece esta red.

6.- Diferencia entre hub, switch y router.

Para poder interconectar diferentes dispositivos con el estándar Ethernet, y haciendo uso del popular conector RJ-45, es necesario disponer de una serie de dispositivos para conectarlos, concretamente de un **hub**, de un **switch** o de un **router**.

- Lo primero que tenemos que tener claro es que un **hub** es mucho más simple que un switch, y **actualmente ya no se utilizan** debido al rendimiento que proporcionan y a las pocas posibilidades de configuración que disponemos. Cuando usamos un hub y un equipo envía una trama de datos a la red, esta trama pasa por el hub, y el propio dispositivo se encarga de enviarlo por todas las bocas de red excepto por donde la ha recibido. Es decir, el hub no sabe a qué equipo va destinado y los envía a todos.



- Cuando conectamos un equipo a un **switch** este internamente tiene una CAM (Content Addressable Memory) donde almacena información importante de la red, como las direcciones MAC que hay conectadas en los diferentes puertos físicos y si tenemos alguna VLAN asociada a un determinado puerto. De esta forma, cuando al switch le llega un paquete de datos de algún equipo, lee el encabezado de datos y sabe a qué equipo va y lo desvía por el puerto correcto, mirando previamente la tabla CAM construida. Es decir, la diferencia es que el hub envía todos los datos que recibe por todos los puertos y el switch lo envía solo al puerto del equipo correcto. Un detalle importante es que el switch utiliza una arquitectura store-and-forward, es decir, almacena la trama de datos en un pequeño buffer, para posteriormente reenviarla a su destinatario correcto.



Los **routers** son elementos encaminadores que son capaces de identificar los paquetes que le llegan y en caso de que el destinatario no se encuentre en uno de sus puertos locales, redirigir la solicitud hacia su puerta de enlace.



7.- Configuración del Router neutro getNet, desactivando el DHCP y usando una ip fuera de peligro

1.- Router neutro: su entrada de datos es directamente la toma de internet del proveedor mediante RJ-11.

2.- Router modem ADSL: su entrada de datos es un puerto de un router neutro mediante RJ-45.

Para desactivar el DHCP del router y cambiar su ip y que al conectar a internet, no interceda con los restantes routers del instituto y los de los propios compañeros de clase.

1.- Resetear el router. 3 segundos el botón de Reset y soltamos.

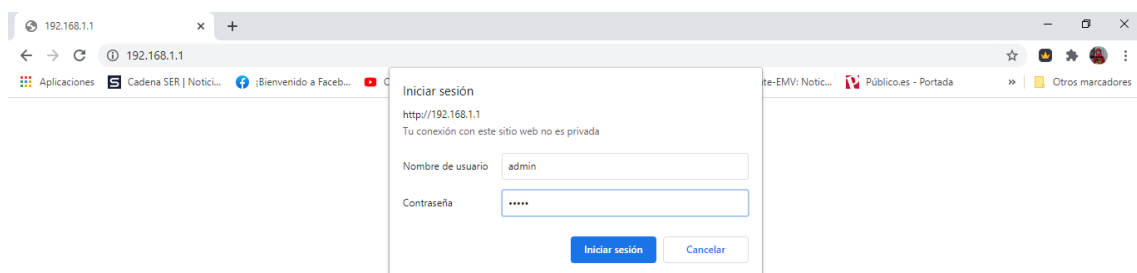
2.- Por defecto ahora el router tiene el DHC type en modo server y con la ip 192.168.1.1

3.- Situamos en el pc con el que vamos a manipular el software del router, una ip fija del rango de la de defecto del router. Por ejemplo la 192.168.1.5. La máscara en el PC será la 255.255.255.0 y la puerta de enlace, la propia del router, 192.168.1.1. Aunque no es necesario, podemos poner ya los servidores DNS primario y secundario: 8.8.8.8 y 4.4.4.4

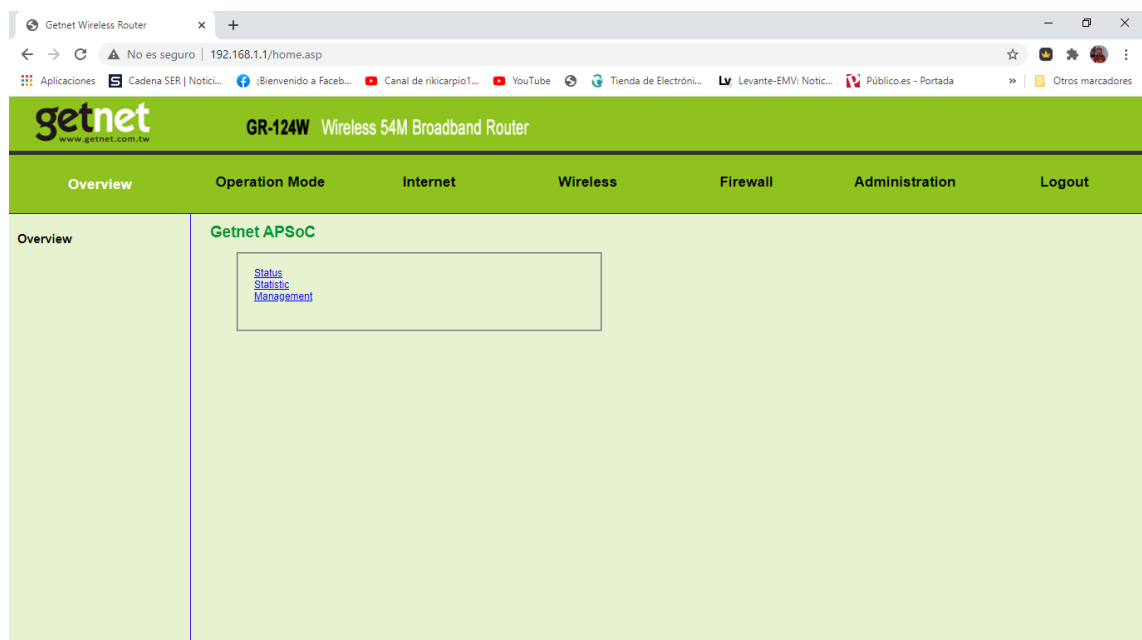
4.- Conectamos con cables Ethernet (cruzados o no) desde la NIC del pc a una puerta cualquiera del router.

5.- En el navegador, accedemos a la dirección <http://192.168.1.1>

6.- Por defecto, el usuario y la contraseña serán admin.



7.- Accederemos al software de configuración del dispositivo



8.- En el apartado internet, podemos observar la ip del router así como la máscara de subred, la dirección MAC del router y varios parámetros más.

The screenshot shows the web interface of a Getnet Wireless Router (GR-124W). The 'Internet' tab is selected, and the 'Local Area Network (LAN) Settings' page is displayed. The page includes a 'LAN Setup' section with the following fields:

LAN Setup	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:1F:1F:9D:29:C8
DHCP Type	Server
Start IP Address	192.168.1.2
End IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.1.1
Secondary DNS Server	192.168.1.1
Default Gateway	192.168.1.1
Lease Time	86400
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>

9.- Desactivación del DHCP. Desplegamos y cambiamos el DHCP type de Server a Disable.

Una prueba interesante, consiste en habilitar el **filtrado de MAC's**. Consiste en **deshabilitar la seguridad por contraseña** de nuestra red wifi. Después detallamos un listado de direcciones físicas que corresponden a los dispositivos **que se pueden conectar** a nuestra red wifi o por el contrario, un listado de MAC's que tienen el **acceso denegado**. De este modo, nos evitamos las incomodidades derivadas de utilizar una contraseña.

Apéndice Comandos MS-DOS

Un usuario avanzado puede sentirse bastante limitado al manejar redes en Windows a través de la herramienta del sistema operativo situada en el panel de control. Si deseas acceder a todo lo que el sistema operativo tiene que ofrecer, tendrás que utilizar el **símbolo del sistema, consola o CMD**.

El símbolo del sistema (*Command prompt*) es la aplicación utilizada en sistemas basados en NT (Windows XP, Windows 7 o Windows 10) para ejecutar comandos MS-DOS (.exe de 16 bits) y otros como scripts con formato .bat y .sys.

La aplicación (solo modo texto) no es necesariamente intuitiva aunque sigue siendo la opción **recomendable para usuarios medios o avanzados** ya que permite realizar tareas de forma más flexible y rápida o acceder a información o funciones que no están disponibles de ninguna otra manera.

Podemos **acceder al CMD** desde el menú de Inicio> Todos los programas> Accesorios> símbolo del sistema. También mediante la barra de búsqueda o archivos del menú de inicio introduciendo "cmd" o "símbolo del sistema".

El acceso a la línea de comandos de Windows puede realizarse **en modo usuario y en modo administrador**, la primera limitada y la segunda más potente y con acceso a todo el equipo.

Comandos útiles para redes Ethernet

Una vez hemos accedido a esta línea de comandos podremos **comunicarnos directamente con el equipo** y realizar una serie de tareas. Aunque se trata de una interfaz de texto, podemos personalizarla en diseño, colores o fuentes accediendo a sus propiedades mediante un clic secundario en el marco del CMD.

Su funcionamiento es sencillo: escribimos el comando (y sus modificadores o parámetros en su caso) y la aplicación CMD hace de intérprete para su ejecución. Hay muchos comandos que podemos utilizar para una amplia variedad de tareas. Indicamos algunos para manejar y solucionar problemas en la red doméstica.

ipconfig

Es uno de los comandos para redes más útiles. Informa de los valores de configuración de red TCP/IP actuales y actualiza la configuración del protocolo DHCP y el sistema de nombres de dominio (DNS).

ping

Prueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP. Por medio del envío de paquetes ICMP, diagnostica el estado, velocidad y calidad de una red determinada.

tracert

Permite conocer los paquetes que vienen desde un host (punto de red). También se obtiene una estadística del RTT o latencia de red de esos paquetes, ofreciendo una estimación de la distancia a la que están los extremos de la comunicación.

```
Administrador: Símbolo del sistema - tracert www.muycomputer.com

C:\WINDOWS\system32>tracert www.muycomputer.com

Traza a la dirección www.muycomputer.com [62.82.203.70]
sobre un máximo de 30 saltos:

 1  <1 ms    <1 ms    <1 ms    192.168.1.1
 2  3 ms     2 ms     2 ms     127.red-80-58-67.staticip.rima-tde.net [80.58.67.127]
 3  12 ms    11 ms    11 ms    165.red-80-58-78.staticip.rima-tde.net [80.58.78.165]
 4  11 ms    26 ms    11 ms    110.red-81-46-8.customer.static.cgg.telefonica.net [81.46.8.110]
 5  *        *        *        Tiempo de espera agotado para esta solicitud.
 6  *
```

pathping

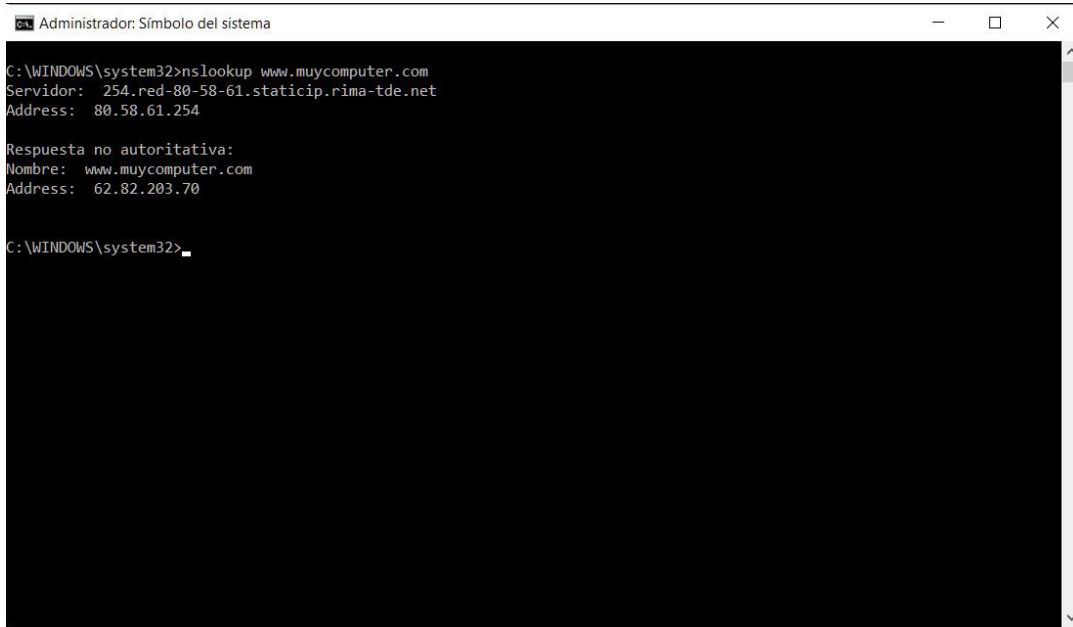
Combina la utilidad de ping y tracert. Es más informativo, por lo que tarda más tiempo para ejecutar. Después de enviar los paquetes a un destino determinado, se analiza la ruta tomada y se calcula la pérdida de paquetes y proporciona detalles entre dos host.

getmac

Obtiene la mac del equipo donde se ejecuta. La dirección MAC es un identificador de 48 bits determinado y configurado por el IEEE y el fabricante (24 bits cada uno). Conocida también como dirección física es única para cada dispositivo.

nslookup

Se emplea para conocer si el DNS está resolviendo correctamente los nombres y las IPs. También nos permite averiguar la dirección IP detrás de un determinado nombre de dominio. Si deseas convertir una dirección IP en un nombre de dominio, sólo tienes que escribirlo en el navegador y ver a dónde conduce.



```
C:\WINDOWS\system32>nslookup www.muycomputer.com
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

Respuesta no autoritativa:
Nombre: www.muycomputer.com
Address: 62.82.203.70

C:\WINDOWS\system32>
```

netstat

Comando potente que muestra estadísticas de la red y permite diagnósticos y análisis. Por defecto, muestra un listado de las conexiones activas de una computadora, tanto entrante como saliente. Incluye el protocolo en uso, las tablas de ruteo, las estadísticas de las interfaces y el estado de la conexión.

netsh

Sinónimo de Shell de red, permite modificar, administrar y diagnosticar la configuración de una red, con más detalle y potencia que los anteriores. Un comando avanzado que ofrece un montón de opciones utilizando sus modificadores y que como ejemplo, permite cambiar el DNS primario y secundario de un equipo.

arp -a

Comando MS-DOS que mantiene en cache la correspondencia entre las direcciones IP y las direcciones físicas del adaptador o tarjeta de red. Es utilizado en tareas de redes para optimizar el rendimiento de las conexiones y para solucionar conflictos.

Links Interesantes

- En los siguientes video puedes encontrar una explicación de que es una dirección MAC

<https://www.youtube.com/watch?v=OlccMIk1MG0>

<https://www.youtube.com/watch?v=F6pbF1YFSPY>

- En el siguiente vídeo puedes ver una explicación sobre las direcciones ip versión 4, por qué se agotaron y por qué necesitamos las direcciones ip versión 6

https://www.youtube.com/watch?v=MEZC_4bdojc

- En el siguiente video, puedes encontrar una estupenda explicación sobre las direcciones ip y las direcciones MAC.

<https://www.youtube.com/watch?v=C1q7mC0kYTc>

- En el siguiente vídeo descriptivo puedes ver una descripción de las diferencias entre hub, switch o router.

<https://www.youtube.com/watch?v=liudX0oskwM>

- En la siguiente página web, puedes encontrar una ordenada explicación sobre los tipos de direcciones IPV4.

<https://www.quia.com/files/quia/users/istomar/DIPS/index.html>

- En el siguiente vídeo, puedes encontrar una explicación sobre el cálculo de subredes.

<https://www.youtube.com/watch?v=IEKR7WtKzDA>

- En el siguiente vídeo, puedes encontrar una explicación sobre el cálculo de subredes.

<https://www.youtube.com/watch?v=Tvs63mIWYI8>