

BREVE RESUMEN DEL FUNCIONAMIENTO DEL TCP-IP **E IMPLEMENTACIÓN EN WINDOWS**

INTRODUCCIÓN

He querido preparar este pequeño resumen debido fundamentalmente a los posibles desconocimientos por parte de los usuarios de su funcionamiento y debido a que nunca se debe estar jugando con los parámetros del TCP sin saber qué es lo que se está tocando. Igualmente, Microsoft ha intentado ayudar al usuario final, poniendo una serie de "Asistentes" a su disposición. Pero el problema que veo en estos Asistentes, es que el utilizarlos "conjuntamente" con modificaciones manuales posteriores a los parámetros del TCP, puede dejar inoperativa nuestra maquina.

Estos asistentes están muy bien para el usuario final. Pero precisamente para eso: el usuario totalmente final, es decir, aquel usuario que nunca va a entrar en los parámetros del TCP a modificarlos.

Un porcentaje muy alto de gente, tiene, o bien, mínimos conocimientos del TCP y se arriesga a andar tocando parámetros, o tiene un amigo que a su vez ha leído que..... (el típico 'experto' no se sabe en qué, o bien, se encuentra publicados en el web cosas a las que nunca debería hacer caso.....

Entiendo igualmente que Microsoft, y esto sirva como crítica a ellos, nunca ha terminado de ajustar estos asistentes. Si se utilizan debería impedirse el acceso manual a las configuraciones TCP, o bien quedar lo suficientemente ocultas para que ya no pueda modificarse manualmente excepto por un experto.

En particular, y aunque parezca mentira, existen dos grandes caballos de batalla: la implementación del NetBios sobre TCP-IP (responsable de "ver" los otros equipos en la red) y la implementación de la conexión compartida a Internet (ICS - Internet Connection Sharing).

Vamos a repasar un poco los conceptos...

PROTOCOLO IP

El IP es el 'Internet Protocol'. Existen varios protocolos dentro de lo que en lenguaje vulgar denominamos TCP-IP. Existen ICMP, ARP, etc... que son los denominados paquetes de control del TCP-IP. Y existen los que yendo bajo IP puro, encapsulan los mensajes TCP y udp. Estos últimos son los que nos van a interesar, ya que son los normalitos que utilizan las aplicaciones a las que estamos acostumbrados: navegadores, y en general comunicaciones bajo TCP.

PUERTOS

En TCP-IP, pueden definirse 65536 puertos. Es decir, un puerto, no es nada mas que un numero de 16 bits (2 elevado a 16 es el numero anterior), y que se utiliza para que un determinado programa se comunique con la pila TCP. Es decir, un programa se hace

"dueño" de un puerto, y es capaz de enviar y recibir datos por él.

Los puertos de números bajos: inferiores al 1024, están reservados para el TCP-IP y normalmente tienen nombre propio: el 21 es el FTP, el 23 el telnet, el 80 es el servidor web... etc).

Los puertos superiores quedan libres pudiendo utilizarles cualquier aplicación y para cualquier uso.

DIRECCIÓN IP

Cada máquina conectada a una red Internet, constituye un host que debe ser único. Para ello, cada máquina debe tener una dirección IP (de 4 bytes) única en toda la red.

Esta dirección es de 4 bytes. Cada byte, puede tener un número desde 0 a 255. Y normalmente la representación normal de esta dirección es por los 4 números en decimal anteriores, separados por puntos. Por ejemplo: 192.168.0.1

El número 255 queda reservado normalmente para direcciones de broadcasting (direcciones genéricas a toda una subred, y por ahora debemos obviarla).

Debe existir una dirección IP en cada interfase de red. Una interfase de red, es una tarjeta de red, o un módem en comunicación telefónica, o un simple cable de conexión entre PCs, por ejemplo en el puerto paralelo, que vaya a realizar una comunicación IP.

MÁSCARA IP

Para que las máquinas bajo TCP-IP, sepan cómo y por dónde enviar un mensaje, es importante el tema de la máscara. La máscara es aquella serie de 4 números (como si fuese una dirección IP), que ejecutado bit a bit con una dirección IP, le indica al sistema si esta dirección IP pertenece a la subred local -y por tanto es alcanzable mediante broadcast- o no pertenece a la subred local, y por tanto el mensaje TCP, hay que enviarlo al gateway o puerta de enlace de nuestra red.

Si la máscara está mal en algunos de los equipos, pueden suceder problemas de todo tipo.

Por ejemplo, la dirección 192.168.0.1 con máscara 255.255.255.0 indica que son alcanzables en la subred local todas las máquinas de dirección 192.168.0.x (siendo x cualquiera) y que cualquier otra máquina es alcanzable únicamente enviando el paquete al gateway por defecto.

Quien quiera pormenorizar en este tema, puede verse el manual "Fundamentos del TCP-IP", del cual soy autor, y que he puesto a vuestra disposición en repetidas ocasiones.

SOCKET

Un socket no es nada más que un canal de comunicaciones entre dos hosts TCP. Por tanto, un socket queda totalmente definido por 4 números: la dirección IP y el puerto de la máquina origen y la dirección IP y el puerto de la máquina destino.

Cuando estamos viendo una página web por ejemplo, los datos que vemos han viajado en un socket. Este socket se ha establecido entre la máquina origen (la dirección IP de `www.microsoft.com`, por ejemplo), y el puerto 80 (que es el puerto de los servidores web), y la dirección IP de la máquina destino (nuestra IP) y un puerto cualquiera que el navegador ha seleccionado en ese momento del rango de los puertos libres en nuestra máquina.

DNS

Servidor de Nombres. Normalmente cuando nos referimos a una dirección, no estamos casi nunca escribiendo la dirección IP de 4 números. Lo normal es escribir un nombre, por ejemplo `www.microsoft.com`.

Pero tal y como visto anteriormente, nuestra máquina solo entiende de direcciones IP. Por tanto, es necesario que alguien traduzca el nombre en la dirección IP. Ese "alguien" es un servidor DNS (Domain Name Solver).

Normalmente, nuestro TCP, debe tener asignado la dirección IP del DNS, es decir qué máquina de internet (o intranet) nos va a resolver los nombres. Cada vez que a nuestra máquina le digamos un nombre, lo primero que hará será consultar al DNS para tener su dirección y poder referirse a ella por dirección.

Todos los nombre de Internet, deben localizarse en un DNS. Por ello, cuando nos conectamos a Internet, o bien hemos configurado los DNS de nuestra conexión telefónica, o bien nuestro proveedor de acceso a internet (ISP) nos lo puede asignar, al igual que nos asigna dirección IP, en el momento de establecer la comunicación.

El DNS de nuestro ISP, evidentemente no tendrá todas las direcciones de Internet, pero para aquellas que no tenga, tiene a su vez las direcciones de otros DNS a los cuales les reenvía (forwarding) la pregunta.

Al final, sea quien sea el que tiene la dirección real, el caso es que a nuestra máquina le llegará y por tanto, nuestra máquina (mejor dicho el programa que lo necesita en ese momento), a partir de entonces podrá referirse por dirección al otro PC o al otro servidor.

DHCP

Es el mecanismo estándar por el cual una máquina en internet, es capaz de dar automáticamente direcciones IP a las máquinas que se conectan sin dirección IP.

Hemos comentado que la dirección IP debe ser única en Internet. Pero por desgracia, no existen suficientes direcciones IP para que cada uno de nosotros tengamos una asignada. Y menos, si queremos distribuir y racionalizar esto un poco, es decir, distribuir las direcciones IP por rangos.

Por ello, los proveedores de Internet, suelen tener asignado un rango de direcciones, y lo normal es que los PC's no tengan dirección IP en la conexión telefónica. El proveedor de Internet, tiene entonces un servidor DHCP que nos dará una dirección en ese

momento, de su rango de direcciones libre. Ese servidor DHCP, igualmente almacena y guarda en un fichero, a quien le ha dado la dirección IP al objeto de poder ser consultado en cualquier auditoría).

OTROS PROTOCOLOS

Existen otra serie de protocolos de mensajería y control: ICMP, IGMP, ARP, etc,... que aunque viajan por internet, son siempre transparentes al usuario final. Normalmente y por desgracia, estos son los más susceptibles a los temas de hacking.

¿CÓMO VIAJA FÍSICAMENTE UN MENSAJE?

A la hora de salir el mensaje "físico" por el cable, este ya no entiende de dirección IP. Entiende únicamente de la dirección física de la tarjeta de red destino. (Cada tarjeta de red, lleva internamente un número único en el mundo y que los fabricantes de hardware garantizan que es único).

Por ello, se debe convertir de nuevo, la dirección IP destino en la dirección MAC (la dirección física de la tarjeta destino comentada anteriormente).

Precisamente el protocolo APR mencionado anteriormente, lo utiliza, entre otras cosas, el propio TCP-IP para tener las direcciones MAC o bien de las máquinas destino a las cuales queremos alcanzar, o bien la dirección MAC del gateway o puerta de enlace de nuestra subred con la red externa o internet.

* Lo anterior es básicamente la implementación del TCP-IP bajo internet, o bien los conceptos con los que nos vamos a manejar a partir de ahora.

Existe una segunda implementación (que no es posible utilizar por internet), de la implementación LM (Lan Manager, definida por IBM a principios de la década de los 80), que nos permite utilizar el TCP-IP en las intranet, o bien en las redes domésticas. La implementación de Lan Manager se hace con la resolución de nombre NetBios sobre TCP-IP. Es decir, es un protocolo llamado NetBios y que se encapsula en mensajes TCP.

(para entender el tema del encapsulado, baste un pequeño ejemplo -y muy basto-, ¿es posible viajar el coche desde Madrid a New York?... Pues sí: comienzo mi viaje en coche hasta la costa, allí meto el coche en un barco ('encapsulo'), atravieso el Atlántico, llego al puerto, saco el coche ('desencapsulo') y continúo hasta mi destino).

HAGAMOS UN BREVE RESUMEN

Aunque lo que hemos visto hasta aquí, es muy básico, prácticamente todos hemos tenido que configurar la conexión a Internet y siempre lo hemos hecho rutinario.

Nuestro ISP nos daba las instrucciones. Generalmente no había que configurar nada y en algunos casos, los DNS's del ISP.

Con lo que hemos visto, supongo que hemos comprendido un poquito como funciona: tenemos un interfase de red (el modem) sin dirección IP. Al conectarnos, solicita de un servidor DHCP una dirección IP, así como los DNS's si estos no estuviesen configurados.

Según recibe la dirección IP en la nueva interfase de red, Windows cambia automáticamente las rutas de envío. Esto puede verificarse ejecutando el comando:

```
route print
```

antes y después de la conexión.

Acabo de conectarme e Internet y la salida de ese comando me informa de:

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	62.37.149.2	62.37.149.2	1
62.36.208.19	255.255.255.255	62.37.149.2	62.37.149.2	1
62.37.149.2	255.255.255.255	127.0.0.1	127.0.0.1	1
62.255.255.255	255.255.255.255	62.37.149.2	62.37.149.2	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.255.0	192.168.0.1	192.168.0.1	1
192.168.0.1	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.255	255.255.255.255	192.168.0.1	192.168.0.1	1
224.0.0.0	224.0.0.0	62.37.149.2	62.37.149.2	1
224.0.0.0	224.0.0.0	192.168.0.1	192.168.0.1	1
255.255.255.255	255.255.255.255	192.168.0.1	192.168.0.1	1

Default Gateway: 62.37.149.2

Esta tabla de rutas indica por dónde saldrán nuestro mensajes IP. La manera de leerla es desde abajo hacia arriba.

Localizamos desde abajo a arriba, las líneas que tienen como gateway el 127.0.0.1 (que es el 'localhost', es decir la dirección de 'loppback' de nuestra propia maquina.

La primera entrada que encontramos es la que tiene como IP 192.168.0.1 (curiosamente, la dirección IP de mi tarjeta de red).

En la línea anterior, nos indica que todos los paquetes a la dirección 192.168.0.x (pongo

una x ya que la mascara es 255.255.255.0) saldrán por el gateway 192.168.0.1 que es mi tarjeta de red. Es decir, para mi red local, la salida de los paquetes IP es por mi tarjeta de red.

Continuando, vemos que el siguiente 127.0.0.1, pertenece a la dirección 127.0.0.0. Esta entrada se ignora ya que es el propio 'loopback' local. Es decir el que se utiliza normalmente entre aplicaciones, que a pesar de ejecutarse en la misma máquina, se comunican entre ellas vía TCP-IP, como si estuviesen en máquinas diferentes.

Ascendiendo en la lista, nos encontramos que el siguiente 127.0.0.1, pertenece a la dirección 62.37.149.2. Curiosamente es justo la dirección IP que nos acaba de dar nuestro proveedor de Internet (ISP).

Se puede verificar esto, ejecutando el comando:

```
ipconfig /all
```

Bien, ascendiendo hacia arriba, ignoramos todas las que tienes máscara 255.255.255.255, y la primera que queda es: 0.0.0.0 (con máscara a ceros) sale precisamente (gateway) por la dirección IP de mi interfase de conexión a Internet (modem). Esto indica que cualquier dirección que no haya sido enviada antes (es decir, cualquier otra que no sea mi red local), saldrá por el modem.

Bien, lo visto en estas líneas, puede parecer un poco pesado y un poco raro. Pero es importantísimo cuando tenemos mas de una interfase de red, el saber leer correctamente la tabla de rutas.

Esta tabla que acabamos de ver, puede modificarse mediante el comando "route". Pueden añadirse y quitarse rutas de red. Si ejecutamos:

```
route /?
```

nos dará la sintaxis completa.

Lo importante de lo que hemos visto hasta ahora, es que estos conceptos que hasta el momento los he centrado en Internet, no solo son para Internet. Son para cualquier red TCP-IP (incluida nuestra posible red local).

MEJORAS IMPLEMENTADAS DESDE W98 HASTA W2000

Hasta el momento hemos visto que es necesario siempre una dirección IP para que funcione una comunicación TCP-IP.

La pregunta que surge es: yo he instalado W98 (o W2000), no he dado ninguna dirección IP, no sé ni lo que es un servidor de direcciones DHCP y que yo sepa no existe en mi red, y curiosamente me funciona todo ¿como es eso?....

Bien, la respuesta es sencilla: Microsoft, a partir de W98 (y superiores) implementó el concepto de 'Autonet Configuration'. Este mecanismo lo que hace, es que cuando no hay dirección IP, investiga en la red para localizar un servidor DHCP. Si no lo encuentra en los primeros tres intentos, se "inventa" un dirección IP cualquiera en el rango de direcciones 169.254.x.y de clase B (es decir, con mascara 255.255.0.0) y para evitar que esa IP inventada ya exista, investiga en la red mediante el protocolo ARP si ya está duplicada. Si estuviese, se "inventa" otra y repite el proceso.

De esta manera, nuestra red siempre tendrá direcciones IP dentro del mismo rango de direcciones (por tanto lo PC's se verán entre ellos,... pero eso lo veremos más adelante...) y no hemos tenido que configurar nada.

Por supuesto, las direcciones que hemos visto hasta ahora:

192.168.0.x (clase C: es decir mascara 255.255.255.0)
169.254.x.y (clase B: es decir mascara 255.255.0.0)

Y esta otra:

10.x.y.z (clase A: es decir mascara 255.0.0.0)

Son direcciones "reservadas" en Internet. Es decir, no puede existir ninguna máquina en Internet con estas direcciones. Por tanto, son las candidatas primeras a utilizar en nuestra red local.

CONCLUSIÓN Y TIP

TIP: El mecanismo que acabamos de describir para "autoasignarse" dirección IP en una red que no tenga servidores DHCP, es evidentemente un mecanismo lento. Las normas del TCP-IP (RFC), indican los tiempos de espera (time out) entre cada uno de los intentos para localizar un servidor DHCP, los tiempos de búsqueda y espera del protocolo ARP, etc. Por tanto este mecanismo hará que nuestro PC se demore unos 20-30 segundos más de lo debido en arrancar.

Si queremos eliminar esta demora, simplemente asignando a los PCs de nuestra red alguna de las direcciones (evidentemente dentro del rango de direcciones) que hemos comentado antes, nos ahorraremos ese tiempo en arrancar el PC.

NOTA: Si tenemos instalado el ICS (conexión compartida a Internet en W98SE o WME o W2000), no deben asignarse direcciones IP ya que automáticamente la maquina que comparta el modem se convierte en servidor DHCP, colisionando por tanto con las configuraciones manuales que podamos asignar. Más adelante veremos en profundidad el ICS.