Configuración y diagnóstico de TCP/IP en Windows

Área de Arquitectura y Tecnología de Computadores – Versión 1.0.915, 24/03/2022

Objetivos

En esta sesión se pretende que el alumno se familiarice con la configuración del conjunto de protocolos de red TCP/IP, que son la base de Internet. Se estudiarán utilidades de red orientadas a la configuración y al diagnóstico de TCP/IP desde la interfaz de comandos de Windows.

Conocimientos y materiales necesarios

Para poder realizar esta sesión el alumno debe:

- Conocer el concepto de red de computadores.
- Conocer cómo pasar de decimal a binario.
- Saber hacer la operación lógica AND a nivel de bits.
- Acudir al laboratorio de prácticas con el libro de apuntes de la asignatura.
- Durante la sesión se plantearán una serie de preguntas que pueden responder en el correspondiente cuestionario en el Campus Virtual. Puedes abrir el cuestionario en otra pestaña del navegador pinchando en el enlace mientras mantienes pulsada la tecla Ctrl.

1. Utilidades de configuración y diagnóstico de TCP/IP desde la interfaz de comandos

La conexión de un computador a la red se realiza a través de un medio físico (cable, fibra óptica o aire) que conecta la interfaz de red del equipo a una red, típicamente de área local. Los sistemas operativos proporcionan una serie de utilidades que permiten configurar y realizar diagnósticos de la red. En el caso de Windows, las utilidades más destacadas son **`ipconfig`**, **`ping`**, **`tracert`**, **`netstat`**, **`nslookup`** y **`arp`**. Todas ellas se pueden invocar desde la interfaz de comandos del sistema. La forma más sencilla para obtener una interfaz de comandos en pulsar en el botón **Inicio de Windows**, y en el cuadro de texto **Buscar programas y archivos** escribir `cmd` y a continuación pulsar Enter.

1.1. ipconfig : Internet protocol configuration

La utilidad **`ipconfig`** proporciona información acerca de la configuración de red en el equipo, en concreto acerca de la configuración IP. Además, permite editar parámetros de una interfaz de red cuando esta se configura mediante DHCP.

La ejecución de la orden *ipconfig* proporciona la siguiente información:

- La **dirección IP** asignada a cada interfaz de red, bien de forma manual o de forma dinámica mediante DHCP.
- La **máscara de red**, que indica qué parte de la dirección IP identifica a la red y qué parte identifica al equipo dentro de la red.
- La **puerta de enlace** predeterminada, que indica la dirección IP del equipo que conecta la red de área local con el resto de Internet.

- Escribe en la ventana de comandos *ipconfig*, pulsa Enter y observa la salida. A continuación, rellena la tabla siguiente con los parámetros configurados para la interfaz que permite comunicar al equipo con la red de área local.

Dirección IP:	
Máscara de subred:	
Puerta de enlace:	

- A partir de la máscara de red deberías poder determinar cuántos de los 32 bits que se forman la dirección IP se utilizan para especificar la red y cuántos se utilizan para especificar la máquina. ¿Cuántos bits se utilizan para identificar máquinas en la red? Responde en el cuestionario: pregunta 1. ¿Cuántas máquinas con direcciones IP distintas pueden conectarse a esta red de área local? Responde en el cuestionario: pregunta 2.

La utilidad *ipconfig* tiene más posibilidades de uso. Para mostrar todos los posibles usos junto con su explicación escribe en la interfaz de comandos **`ipconfig /?`**. En nuestro caso, sólo vamos a ver tres de esos usos: **`ipconfig /all`**, **`ipconfig /release`** e **`ipconfig /renew`**.

La orden *ipconfig /all* devuelve toda la información disponible sobre la interfaz de red. La información disponible depende de la forma en la que se ha obtenido la dirección IP, si la asignación es fija o se asigna de forma automática mediante DHCP.

- Ejecuta *ipconfig /all* a través de la interfaz de comandos. ¿Tiene el equipo asignada una dirección de Internet fija, o hay otro equipo en la red que le asigna una dirección? Responde en el cuestionario: pregunta 3.
- Completa la siguiente tabla para la interfaz de la conexión de área local (como puedes comprobar, además de la interfaz de red física, aparecen interfaces de red virtuales, o software):

Dirección física:	
DHCP habilitado:	
Servidor DHCP:	
Servidor DNS:	
Concesión concedida:	

  Si la asignación de dirección IP automática mediante DHCP está habilitada, verás que la dirección IP asignada tiene un tiempo de duración determinado, ¿cuánto aproximadamente? Si no entiendes algún aspecto de la información mostrada, pregunta a tu profesor.

Si de la información anterior obtienes que la asignación de direcciones IP está basada en DHCP, podemos ver el funcionamiento de las órdenes *ipconfig /release* e *ipconfig /renew*. En caso contrario, no tendrán ningún efecto.

- Ejecuta desde el interfaz de comandos la orden *ipconfig /release*. La ejecución de esta orden envía al servidor DHCP una notificación de liberación de la dirección IP actual. En la barra de tareas del sistema aparecerá una notificación indicando que el equipo se ha quedado sin red.
- Para solicitar una nueva dirección IP, ejecuta ahora la orden *ipconfig /renew*. Esta orden solicita al servidor DHCP una nueva IP. La nueva dirección asignada al equipo, ¿es la misma que tenía o ha cambiado? Responde en el cuestionario: pregunta 4.

1.2. ping

La utilidad *ping* permite obtener una estimación del estado de la conexión midiendo el tiempo de ida y vuelta (*round-trip delay time* o RTD) de un paquete a la máquina cuya dirección se indica como destino. Para ello, se almacena el instante de tiempo en el que se envía un paquete y cuando llega la respuesta de la máquina destino se calcula la diferencia entre el tiempo actual y el guardado. La implementación de *ping* se basa en el protocolo **ICMP** (*Internet Control Message Protocol*), uno de los protocolos de control en Internet, y utiliza dos mensajes concretos de este protocolo, *Echo request* y *Echo reply*.

Aunque la obtención del tiempo es importante, el uso más habitual de la orden *ping* es determinar si la red está funcionando bien y si hay algún fallo de conexión o de funcionamiento del DNS encargado de asociar direcciones IP a los nombres de los equipos.

La utilidad *ping* se usa de la siguiente forma: *ping [opción] destino*, donde opción viene representada por una letra precedida por el signo menos y destino es una dirección IP o un nombre de dominio. Si escribimos solamente *ping* nos mostrará en pantalla las posibles opciones de uso.

- Rellena la siguiente tabla haciendo *ping* a las distintas direcciones que aparecen y recopilando los datos que se piden en la tabla.

Dirección servidor	% P. Perdidos	T. Mínimo	T. Máximo	T. Medio
`www.unioviedo.es`				
`www.unileon.es`				
`www.berkeley.edu`				
`www.u-tokyo.ac.jp`				

Los resultados obtenidos con *ping* no dan información de por qué el tiempo de ida y vuelta es mayor en unos destinos que en otros. En ocasiones no se obtiene respuesta a la orden *ping*; esto indica que no es posible alcanzar la dirección indicada, pero no proporciona información sobre la causa. Puede deberse a que el equipo al que corresponde esa dirección está caído o no disponible, o bien que la red está tan saturada que los paquetes no llegan en un tiempo razonable y se descartan.

En algunas ocasiones, no recibir respuesta a un *ping* no significa nada de lo anterior: es posible que el administrador del equipo destinatario del *ping* haya configurado el equipo para no responder a ese tipo de mensajes. Esta tarea se puede realizar creando una regla para el firewall del sistema que bloquee las conexiones entrantes del protocolo ICMP. Por ejemplo, si ejecutas un *ping* al servidor `www.microsoft.com`, no recibirás respuesta, en cambio si te conectas a través de un servidor web, verás que el equipo sí está activo y funcionando.

1.3. tracert: trace router

`tracert` es una herramienta de diagnóstico de red que permite conocer la ruta que sigue un paquete para llegar al equipo destino sobre una red IP. La ruta está indicada por el conjunto de enrutadores, o *routers*, que atraviesa el paquete en su viaje y que le encaminan hacia su destino. Esta herramienta cuenta el número de saltos o *routers* por los que el paquete pasa en su camino hacia el destino. Para cada *router*, informa del tiempo que ha tardado en alcanzarlo.

El mecanismo de funcionamiento de *tracert* se basa en mensajes *Echo request* y *Echo reply* del protocolo ICMP y en la propiedad TTL (*time to live*) del protocolo IP. Esta propiedad sirve para limitar la vida de un paquete para que no esté vagando en el interior de la red si no consigue llegar a su destino. El valor TTL del paquete se inicializa con un número que se decrementa en una unidad cada vez que atraviesa un *router*.

La herramienta *tracert* inicialmente envía un paquete con el valor de su campo TTL a 1. Cuando el paquete llega al primer *router*, este decrementa el valor del campo TTL y obtiene cero, lo que significa "tiempo excedido". Ante un paquete con tiempo excedido, el *router* lo desecha y envía al emisor un paquete ICMP de tipo *TIME EXCEEDED*. Es el origen se anota el tiempo de ida y vuelta y el router que envió el paquete de vuelta.

El proceso se repite incrementando cada vez el valor del campo TTL en una unidad hasta que finalmente el campo TTL tiene un valor suficientemente elevado para que alcance su destino. Para evitar la posible pérdida de paquetes, la orden *tracert* envía tres paquetes, obteniendo el tiempo empleado en cada uno de ellos, que normalmente será el mismo, aunque no tiene por qué suceder así. De hecho, en ocasiones, el tiempo empleado por el paquete en realizar el recorrido de ida y vuelta puede ser muy elevado. Según el funcionamiento del protocolo IP no existe ninguna garantía de que el camino de vuelta sea el mismo que se empleó para la ida, lo cual también afecta a la interpretación del tiempo de viaje empleado por el paquete. En ese caso, se mostrará un asterisco en pantalla en lugar del tiempo.

- Rellenar la siguiente tabla ejecutando la orden *tracert destino*, sustituyendo *destino* por las distintas direcciones que aparecen en la tabla.

Dirección servidor	Nº de saltos	Tpo. al último salto
`www.unioviedo.es`		
`www.unileon.es`		
`www.berkeley.edu`		
`www.u-tokyo.ac.jp`		

- Compara el tiempo empleado en alcanzar el último salto, que has anotado en la tabla, con el valor obtenido al utilizar la orden *ping*, ¿cómo son? Responde en el cuestionario: pregunta 5.

Los servidores con los que se ha trabajado están en ubicaciones distintas: en Asturias, en León, en Madrid, en Estados Unidos y Japón.

- ¿Existe alguna relación apreciable entre el tiempo que has registrado y la localización geográfica del equipo? Responde en el cuestionario: pregunta 6.
- Compara ahora el tiempo registrado con el número de saltos necesarios para alcanzar el equipo de destino. ¿Observas ahora alguna relación? Responde en el cuestionario: pregunta 7.

1.4. netstat: network statistics

La utilidad **`netstat`** proporciona información sobre la interfaz de red, así como estadísticas de uso de los distintos protocolos de red.

- En la interfaz de comandos del sistema, escribe *netstat /?*. Se mostrarán las opciones de uso de esta herramienta.
- Utiliza la opción adecuada para mostrar todas las conexiones activas y puertos disputestos a recibir paquetes en tu equipo. ¿Qué opción has tenido que usar? Responde en el cuestionario: pregunta 8.
- Abre un navegador web, accede a `www.youtube.com` y reproduce cualquier video. Mientras se está reproduciendo, ejecuta la orden *netstat*. Podrás identificar qué conexiones de red se están utilizando para recibir la información de este servidor web.

Como se ha indicado anteriormente, *netstat* permite obtener estadísticas de uso de los distintos protocolos de red.

- Ejecuta la orden *netstat -s -p ICMP* para mostrar las estadísticas de uso del protocolo ICMP.
- Ejecuta la orden *ping www.google.es* y muestra de nuevo las estadísticas de uso del protocolo ICMP. ¿Cuántos mensajes se han enviado al ejecutar la utilidad *ping*? Responde en el cuestionario: pregunta 9. ¿Y cuántos mensajes se han recibido? Responde en el cuestionario: pregunta 10.
- Haz ahora un *ping* a la dirección IP de tu equipo. ¿Cuántos mensajes ICMP se han enviado? Responde en el cuestionario: pregunta 11. ¿Y cuántos se han recibido? Responde en el cuestionario: pregunta 12. ¿Qué otros valores han cambiado en las estadísticas? Responde en el cuestionario: pregunta 13.

1.5. nslookup: name server lookup

La utilidad **`nslookup`** permite solicitar al DNS la traducción de un nombre de dominio a una dirección IP o viceversa. Además, permite comprobar si el servidor de nombres, la máquina que se encarga de traducir nombres de dominio a direcciones IP, está funcionando bien o no.

En la sección sobre, al explicar el funcionamiento de la orden *ping* se comentó que esta utilidad podía provocar fallo de conexión y, sin embargo, no ser síntoma de un fallo de la red. En ocasiones, puede ser debido a que la máquina que actúa como servidor de nombres no está funcionando correctamente.

- Ejecuta la orden *nslookup destino*, sustituyendo *destino* por cada una de las direcciones que aparecen el la siguiente tabla. Rellena la tabla asociando a cada nombre de máquina al menos una de las direcciones IP que tiene asignadas.

Nombre servidor	Dirección IP asignada
`www.unioviedo.es`	
`www.unileon.es`	
`www.berkeley.edu`	
`www.u-tokyo.ac.jp`	

1.6. arp

La utilidad **`arp`** permite mostrar y editar las tablas de traducción entre direcciones IP y direcciones física o MAC que utiliza el protocolo ARP (*Address Resolution Protocol*). Las tareas de edición requieren privilegios de administración en el equipo. Al igual que las herramientas anteriores tiene varias posibilidades de uso, que se pueden listar con la orden *arp*.

- Muestra todas las entradas de la tabla de traducción ARP con la orden *arp -a*. ¿Cuál es la dirección física de la puerta de enlace predeterminada asociada a la conexión de área local del equipo?

En la información mostrada, el campo tipo indica si las entradas en la tabla están almacenadas de forma permanente (estático) o temporal (dinámico).

2. Ejercicios adicionales

2.1. IP scanner

Aparte de las utilidades de red proporcionadas por el sistema operativo, en este caso Windows 7, existen multitud de herramientas, muchas de ellas con licencia gratuita, para diagnosticar problemas en la red. Unas de las herramientas más utilizadas son las que permiten visualizar los equipos a los que se puede acceder a través de la red utilizando el protocolo IP. Mediante herramientas de este tipo se pueden confirmar o descartar problemas en la red cuando se intenta acceder a recursos disponibles en otro equipo de la red. A continuación vamos a ver un ejemplo.

- Accede a la web `www.advanced-ip-scanner.com` y descarga el programa *Advanced IP Scanner* (tienes una copia disponible en el Campus Virtual).
- Ejecuta el programa en la versión portátil, sin instalarlo en el equipo.
- Introduce, en el cuadro de texto que aparece bajo el menú, el rango de direcciones IP de la subred del laboratorio de prácticas y pulsa `Scan`. Se mostrarán todos los equipos accesibles.
- Selecciona la opción **View > Expand all**. Se mostrarán los recursos compartidos por cada equipo de la red.

Como has podido comprobar, este ejercicio hace uso de una herramienta que escanea todos los equipos de una red. Por motivos de seguridad, y legales, esta tarea se debería de realizar solo en redes en las que seas administrador o tengas permiso para hacerlo.

Como has visto en el ejemplo de uso de la herramienta *arp*, cuando un equipo se quiere comunicar con otro, debe conocer la dirección de física de su interfaz de red, o de la interfaz de red del *router* a través del cual tiene que enviar el paquete para llegar a él.

Cuando un equipo se quiere comunicar con otro que está en la misma subred consulta en su tabla de traducción interna si existe una entrada para la dirección IP del destinatario con su dirección física asociada. En caso de que esta entrada no exista, el equipo emisor envía una petición ARP destino de una trama *broadcast* a todos los equipos de la subred para que el equipo con esa dirección IP indique su dirección MAC.

En el caso de que la dirección IP de destino no se encuentre dentro de la subred, el emisor consulta en su tabla de traducción interna si existe una entrada para la dirección IP de la puerta de enlace predeterminada. En caso de que esta entrada no exista envía una petición ARP destino de una trama *broadcast* a todos los equipos de la subred para que la puerta de enlace indique su dirección MAC.

- Muestra el contenido de la tabla de traducción del protocolo ARP. Deberás observar que se han actualizado las entradas para todos los equipos de la subred que están activos. ¿Por qué crees que sucede esto? Responde en el cuestionario: pregunta 14.