Tema 6: Dispositivos de conexión a redes

1. Introducción

Las redes de computadores son sistemas de transmisión de datos que se forman cuando dos o más ordenadores están conectados entre sí. Aunque se empezaron a conectar ordenadores entre sí a principios de los años 1940, no cabe duda de que la popularización de las redes ha sido gracias al fenómeno Internet. Sus orígenes se remontan a los años 1970, pero se popularizó a partir la aparición del World Wide Web a principios de los años 1990.

La importancia (y la complejidad) de las redes de ordenadores hace que exista una asignatura troncal dedicada a este tema en la carrera. Por lo tanto, en esta asignatura sólo se verán conceptos básicos de configuración e instalación de dispositivos de conexión a redes y se supondrá al alumno familiarizado con conceptos fundamentales como protocolo, paquete, dirección de red, capas ISO/OSI, cables... En particular, se espera que sepa cómo funcionan los protocolos Ethernet y TCP/IP.

A modo de recordatorio, se definen brevemente a continuación algunos términos básicos relacionados con las redes:

- **Nodo:** Cualquier dispositivo conectado a la red.
- **Segmento:** Porción de la red separada por un conmutador, puente o enrutador.
- ***Backbone*:** Cableado principal de la red.
- **Repetidor:** Dispositivo que transmite la señal sólo amplificándola.
- **Puente (*bridge*):** Dispositivo similar al repetidor, pero que además analiza el destino de los datos y sólo retransmite la señal si es necesario.
- **Concentrador (*hub*):** Dispositivo que conecta varios dispositivos a la misma red. Retransmite la información que le llega por una de sus entradas al resto de bocas.
- **Conmutador (*switch*):** Dispositivo similar a un concentrador, pero que además analiza el destino de los datos y sólo retransmite la señal por la boca que sea necesaria.
- **Enrutador (*router*):** Dispositivo que conecta distintas redes.
- **Pasarela (*gateway*):** Dispositivo que permite comunicarse entre distintos protocolos. En ocasiones (por ejemplo, en Windows, traducido como «puerta de enlace») este nombre se utiliza para dispositivos que hacen en realidad de enrutadores.

2. Conexiones punto a punto entre equipos próximos

Las conexiones punto a punto son aquellas en las que se unen directamente sólo dos ordenadores, habitualmente para transmitir archivos o para compartir recursos. La forma tradicional de hacer estas conexiones es mediante un cable que una los dos equipos a través de alguno de los puertos de E/S, típicamente el puerto serie (utilizando el estándar RS 232) o el puerto paralelo, consiguiendo con la segunda opción mayor velocidad.

En los ordenadores actuales es habitual disponer de una tarjeta de red Ethernet. Conectando dos tarjetas de red mediante un cable cruzado también es posible transmitir datos.

Otra alternativa es utilizar los puertos USB para comunicar los ordenadores. El USB tiene un diseño asimétrico en el que se supone que hay un sistema controlador (y sólo uno) y varios dispositivos que dependen de él. Si conectásemos dos ordenadores directamente con un cable USB normal estaríamos conectando dos dispositivos controladores y la conexión no funcionaría. Por esta razón son necesarios cables que llevan incorporado un dispositivo que permite que los dos ordenadores se vean.

Tras realizar la conexión física por cualquiera de los medios anteriores, hay que ejecutar en los dos ordenadores algún programa que permita comunicarlos mediante un protocolo. Windows incluye el software necesario y lo denomina DCC (*Direct Cable Connection*, conexión directa por cable). Su uso se realiza a través del asistente que aparece creando una nueva conexión de red. Debe decidirse cuál de los equipos será el *invitado* y cuál el *anfitrión* o *host*. El equipo anfitrión será el encargado de establecer los parámetros adecuados de la comunicación y el que compartirá los recursos de red.

Para que la conexión directa funcione correctamente, deberá instalarse el protocolo NetBEUI o el protocolo Newtware Link. Por defecto, el asistente para la conexión en red añadirá a la conexión directa sólo el protocolo TCP/IP, que no permite que el equipo invitado acceda a los recursos compartidos. Si no se va a utilizar el protocolo TCP/IP, es conveniente desactivarlo. Si se desea conectar el equipo invitado a Internet, lo más cómodo es activar la opción *Compartir la conexión a Internet* del equipo anfitrión. Esta opción activará un servidor DHCP (*Dynamic Host Configuration Protocol*) que proporcionará una dirección IP privada al cliente; las peticiones desde esa dirección IP privada serán transformadas en peticiones con su IP por el anfitrión utilizando NAT (*Network Address Translation*); por lo tanto, el anfitrión hará enrutamiento entre la red privada y la red pública.

En Windows Vista Microsoft ha dejado de incluir DCC porque considera que la ubicuidad de dispositivos Ethernet, Bluetooth, USB y Wi-Fi lo ha hecho obsoleto.

3. Módems

Los módems son dispositivos que se utilizan para modular una señal analógica de tal forma que se codifique en ella información digital; también hacen el proceso inverso para extraer de la señal analógica la información que lleva

codificada. La forma de codificar la información consiste en modificar parámetros de la señal analógica. A este proceso se le denomina «modulación» y a la señal utilizada para llevar la información, «onda portadora».

3.1 Módems telefónicos

La utilidad de los módems telefónicos es que permiten utilizar las líneas de teléfono analógicas (denominadas «RTB» o «Red Telefónica Básica»), que están desplegadas por todo el mundo desde hace años, para transmitir información digital a largas distancias. De esta manera se pueden comunicar ordenadores distintos, bien sea para compartir información directamente entre ellos, bien sea para que un servidor que está conectado por otro medio a Internet ofrezca ese acceso a la red a un cliente.

La modulación de las señales sigue diferentes estándares, que están directamente relacionados con la velocidad de transmisión de datos a través de la línea que puede alcanzarse. Es habitual además que los módems soporten funciones de fax, especificadas en sus propias normas. Las siguientes tablas muestras las normas más habituales de modulación y de fax.

Tabla 1. Estándares de modulación

Norma	Velocidad de bajada máxima
V.92	56 000 bps
V.90	56 000 bps
V.34+	33. 00 bps
V.34	28 800 bps
V.32bis	14 400 bps
V.32	9 600 bps
V.23	4 800 bps
V.22bis	2 400 bps
V.22 y Bell 212A	1 200 bps
V.21 y Bell 103	300 bps

Tabla 2. Estándares de fax

Norma	Velocidad máxima
V.17	14 400 bps
V.29	9 600 bps
V.27ter	4 800 bps
V.21	300 bps

Los módems actuales pueden funcionar con el estándar V.92, que es muy similar al V.90 pero introduce algunas ventajas:

- Mayor velocidad de subida (hasta 48 000 bps, mientras que V.90 sólo permitía hasta 33 600 bps).
- Mayor velocidad en la negociación de la conexión.
- *Modem On Hold*: Tecnología que permite que el módem no corte la conexión cuando se recibe una llamada. Durante el tiempo de la llamada, la conexión de datos queda a la espera sin recibir ni enviar nuevos datos.

Este estándar, sin embargo, no ha sido implementado en España por las compañías proveedoras, así que se funciona habitualmente con el V.90.

Existen estándares para la corrección de errores debidos al ruido en las líneas, como el V.42, y estándares que especifican sistemas de compresión, como por ejemplo el V.44.

Al principio los módems se conectaban al PC a través de un puerto serie (que se suele denominar «COM»); ahora hay módems internos que se conectan directamente al bus PCI, módems que se conectan al USB o incluso módems integrados en la placa base; sin embargo, desde el punto de vista del sistema operativo se siguen viendo como si estuvieran conectados a un puerto COM virtual. El ordenador controla el módem enviando cadenas a ese puerto COM. La compañía Hayes desarrolló un estándar de órdenes, los «comandos Hayes», que se popularizaron y en la actualidad es utilizado por casi todos los módems. En este estándar a los ordenadores se les denominados «*Data Terminal Equipment*» o DTE y a los módems, «*Data Communications Equipment*» o DCE.

Las órdenes Hayes se forman con la cadena **AT** (de «atention») seguida de otros caracteres que indican lo que debe realizar el módem. Por ejemplo, **ATI** le indica al módem que transmita información sobre sus características, **ATD***num* le indica que marque el número *num*, **ATA** le indica que conteste a una llamada... El estándar trabaja con dos modos:

- **Modo comunicación**: Cualquier cadena que envía el DTE al DCE es enviada por la salida de este hacia el otro DCE al que estará conectado. Asimismo, cualquier cadena recibida por el DCE es enviada al DTE.
- **Modo órdenes**: Las cadenas que envía el DTE se interpretan como órdenes para el DCE.

Para salir del modo comunicación y volver al modo de órdenes se utiliza una cadena especial denominada «secuencia de escape».

Es interesante saber que existen estas órdenes Hayes porque habitualmente desde el sistema operativo se puede configurar una cadena de inicialización con órdenes que se le envían al módem, como por ejemplo que apague su sonido o que haga pausas más largas a la hora de llamar, lo que puede solucionar algunos problemas de conexión.

Una forma de probar las órdenes Hayes es conectarse directamente al puerto COM, enviar cadenas y ver lo que el módem responde. Para ello se puede utilizar algún programa de terminal, como por ejemplo el **HyperTerminal** que incluye Windows. Hay que tener en cuenta que este programa permite dos tipos de conexión:

- Conexión directa al módem: El programa es el que se encarga de enviar las órdenes Hayes al puerto, de manera transparente para el usuario.
- Conexión al puerto COM: El programa permite enviar las órdenes que teclee el usuario al puerto.

3.2 Cablemódems

Los cablemódems son dispositivos utilizados para conectar ordenadores a redes de cable coaxial. Estas redes se extendieron en primer lugar por Estados Unidos

para transmitir televisión y luego se decidió utilizar el ancho de banda sobrante como forma de conexión a Internet.

La configuración de los cablemódems se realiza a través de unos ficheros que recibe durante el arrancado del proveedor de Internet (*Internet Service Provider* o ISP). También recibe ficheros de actualización del *firmware* si es necesario. Esta configuración es transparente para el usuario.

La configuración en el ordenador, que se conecta al cablemódem a través de una tarjeta de red y un cable de par trenzado o a través de un puerto USB, suele consistir en seleccionar utilizar DHCP para que reciba la configuración de red (dirección IP, máscara, puerta de enlace, DNS...) del cablemódem.

Hay que tener en cuenta que muchos cablemódems no funcionan sólo como módems sino también como enrutadores. En este caso, habitualmente el proveedor de servicios le da una dirección pública al cablemódem y este organiza una subred privada con los elementos que se conecten a él a través de NAT.

3.3 Módems ADSL

Los módems ADSL permiten utilizar de manera más efectiva las líneas de teléfono tradicionales, consiguiendo velocidades de transmisión más altas. Para ello utilizan para llevar datos parte del espectro no empleado para voz.

La forma de conexión de los módems ADSL es similar a la utilizada por los cablemódems.

4. Tarjetas de red

Las tarjetas de red (*Network Interface Card* o NIC) sirven de interfaz entre el ordenador y una red. Solían ser una tarjeta conectada al bus PCI, pero en la actualidad casi todas las placas base incorporan el controlador y los conectores adecuados. Hay diversos tipos, pero en la actualidad las más habituales con diferencia son las que permiten conectarse a una red Ethernet. Estas redes desarrolladas en principio por Xerox acabaron siendo la base del estándar 802.3, que es el tipo de red de área local (*Local Area Network* o LAN) más frecuente. Debido a la popularidad de este tipo de redes, cuando se habla de una «tarjeta de red» casi siempre se está haciendo referencia a una tarjeta de red Ethernet.

La forma de conexión más habitual de estas tarjetas es el conector RJ-45 para par trenzado. Para cable coaxial se usa un conector BNC.

Cada tarjeta tiene un identificador único denominado dirección MAC (*Medium Access Control*), por pertenecer a esa capa del estándar ISO/OSI. Esta dirección tiene 48 bits y se suele dar expresando cada byte en hexadecimal y separándolos por dos puntos, como por ejemplo 01:23:45:67:89:AB.

En teoría, la dirección MAC de la tarjeta no debería poder cambiarse. Por esta razón, en ocasiones se utiliza como método de seguridad, de tal manera que no se permite el acceso a ciertos servicios más que a unas direcciones MAC conocidas. Sin embargo, hay medios de cambiar la dirección (lo que se denomina *spoofing*) y, por lo tanto, no es un buen método de autenticación.

Las tarjetas de red más habituales en la actualidad funcionan a 10/100 Mbps, aunque cada vez empieza a ser más frecuente encontrar tarjetas Gigabit Ethernet que pueden funcionar hasta 1 Gbps. También existen tarjetas que utilizan el protocolo 10-gigabit Ethernet.

5. Cableado

Escoger el tipo de cableado con el que se instala una red es fundamental. Los principales tipos de cable son:

- **Cable directo:** Hilos de cobre aislados. Se usa para cables serie o paralelo. Sufre muchas interferencias, así que no es adecuado para realizar redes sino sólo para conectar dos dispositivos cercanos.
- **Coaxial:** Se utiliza sobre todo para conexiones en bus. Es frágil, lento (hasta 10 Mbps) y por estas razones en la actualidad está en desuso.
- **Par trenzado:** Para conexiones en estrella. Es el método más habitual en la actualidad para conectar tarjetas de red a otros equipos con concentradores y enrutadores.
- **Fibra óptica:** Para largas distancias, para conexiones más seguras y para conexiones muy rápidas. Tiene el problema de que las conexiones suelen ser más costosas.

Dentro de los cables de par trenzado, en la actualidad los tres tipos de cable más frecuentes para datos son:

- **Categoría 3 (UTP, STP):** Hasta 10 Mbps. Era el usado para de Ethernet en su configuración original.
- **Categoría 5 (UTP, STP):** Pensado para 100 Mbps, aunque se pueden conseguir velocidades mayores con Gigabit Ethernet.
- **Categoría 6 (UTP, STP):** Pensado para conexiones de Gigabit Ethernet, aunque también es compatible con conexiones más lentas y más rápidas.

Los cables UTP (*Unshielded Twisted Pair)* son cables sin apantallar, más propensos a las interferencias que los STP (*Shielded Twisted Pair*), que son apantallados, pero más caros.

En los cables de par trenzado hay que distinguir entre dos tipos:

- **Cables directos:** Son los cables que se utilizan para unir dispositivos de distinto tipo, por ejemplo un ordenador a un enrutador.
- **Cables cruzados:** Son los cables que se utilizan para unir dispositivos del mismo tipo, por ejemplo dos ordenadores entre sí o dos enrutadores entre sí. En estos cables se cruzan (intercambian) los extremos de enviar y recibir; de ahí reciben su nombre.

En muchas ocasiones, los dispositivos de red modernos realizan un cruzado interno si lo encuentran necesario, por lo que funcionan de igual manera con cables cruzados y directos.

6. Conexiones inalámbricas

Uno de los inconvenientes de los cables es que limitan la movilidad. En la actual proliferación de dispositivos móviles (ordenadores portátiles, PDAs, teléfonos móviles, etc.) se intentan evitar todos los impedimentos a la movilidad y por esta razón han ganado importancia distintos tipos de conexiones inalámbricas. Hay muchos estándares, que se pueden agrupar en dos grandes tipos:

- Conexiones punto a punto: Estándares como irDA (a través de infrarrojos) o Bluetooth (a través de ondas de radio) intentan evitar el uso de cables para conectar dispositivos, pero no están pensados para desarrollar redes de ordenadores.
- Conexiones de red: Estándares que están pensados para hacer redes locales inalámbricas (WLANs) conectando varios equipos. Los más utilizados en la actualidad son los que siguen los estándares IEEE 802.11 (Wi-Fi), aunque también empiezan a utilizarse los que siguen el IEEE 802.16 (WiMAX). Todos utilizan ondas de radio.

Por su importancia, se van analizar con un poco más de detalle los estándares 802.11.

Para empezar, hay que señalar que existen varias versiones:

- 802.11a: Funciona en la banda de los 5 GHz y permite velocidades de hasta 54 Mpbs.
- 802.11b: Funciona en la banda de los 2.4 GHz y permite velocidades de hasta 11 Mbps.
- 802.11g: Funciona en la banda de los 2.4 GHz pero con velocidades de hasta 54 Mbps.
- 802.11n: Puede funcionar en la banda de los 2.4 GHz o en la de los 5 GHz, con velocidades de hasta 600 Mbit/s. Lleva muchos años en desarrollo pero todavía no hay una versión definitiva del estándar.

Hay dos arquitecturas de redes inalámbricas básicas:

- Ad hoc: Consisten en redes *peer-to-peer* (entre pares) en las que cada dispositivo se comunica directamente entre sí sin necesidad de un punto central que los coordine. Funciona bien sólo con pocos dispositivos y están pensadas para el intercambio de datos entre ellos más que para acceder luego a una red externa.
- En infraestructura: En estas redes hay un elemento central, el punto de acceso (*Access Point* o AP), que permite acceder a otras redes y es el que se encarga de coordinar todos los dispositivos unidos a la red.

Los dispositivos que forman parte de una red inalámbrica necesitan tener una tarjeta inalámbrica.

Aunque las redes inalámbricas presentan muchas ventajas, también tienen desventajas:

- Problemas de seguridad: En estas redes la información viaja por el aire, un medio mucho más difícil de controlar que un cable; por lo tanto, es más difícil controlar quién tiene acceso a la red. Para evitar intrusiones es necesario utilizar algún protocolo de seguridad. El primer protocolo implementado fue WEP, pero su seguridad es muy baja. Otra alternativa es limitar el acceso a ciertas direcciones MAC, pero las direcciones MAC viajan en claro y cualquiera puede ver las que están admitidas en la red y cambiar la MAC de su equipo para ser admitido. La mejor alternativa en la actualidad es utilizar el protocolo WPA.
- Problemas de escalabilidad: En los estándares 802.11b y 802.11g se definen 13 canales distintos, pero hay solapamiento entre ellos, de tal manera que sólo se pueden utilizar 3 canales distintos al mismo tiempo, lo que quiere decir que sólo se pueden tener 3 redes inalámbricas distintas en el mismo espacio sin que se degrade la señal por interferencias.
- Baja velocidad: Aunque la velocidad teórica sea de 11 Mbps (802.11b) y 54 Mpbs (802.11g), la velocidad efectiva máxima ronda los 6 Mbps y 20 Mbps respectivamente. Además, los protocolos de seguridad disminuyen la velocidad efectiva.

7. Herramientas para comprobar conexiones

En el caso de que haya un problema en una red, en primer lugar debe determinarse dónde está el problema para, a continuación, estudiar si es un problema de configuración o de hardware estropeado. Algunos elementos que se pueden utilizar para encontrar problemas en las conexiones son:

- Luces del módem o de la tarjeta: Indican si están recibiendo señal.
- Comprobadores de cables: Permiten saber si los cables están funcionando bien.
- Herramientas software:
    - ping: Esta orden, disponible tanto en sistemas Windows como Unix, permite saber si una dirección IP está respondiendo. Es conveniente comprobar que se puede hacer ping al enrutador (puerta de enlace en terminología Windows). También conviene comprobar si funciona el ping con direcciones IP pero no con nombres; si ocurre así, hay un error de resolución de nombres, así que la siguiente prueba será comprobar que se puede hacer ping al servidor de nombres.
    - traceroute: Esta orden, llamada en Windows «tracert», permite ver la ruta que siguen los paquetes en una red. De esta manera se puede comprobar que las tablas de enrutamiento son correctas.
    - nslookup: Permite comprobar a qué nombre se resuelve una dirección IP y viceversa.
    - ipconfig: En sistemas Windows, da la información básica de la red. Con el parámetro **/all** da información más detallada.

- route: Permite obtener información y modificar las tablas de enrutamiento del computador.
- *Sniffers*: Son herramientas que capturan tramas de red y las interpretan a distintos niveles, permitiendo encontrar errores de configuración, paquetes que no deberían estar viajando por un segmento de red, ataques, etc.