

Prácticas de Redes de Ordenadores Móviles

gsyc-profes@gsys.es, Noviembre de 2006

1. Introducción al Nokia 770

1.1. Actualización del Sistema Operativo

Lo primero será actualizar el Sistema Operativo a la última versión disponible, actualmente la *Software Edition 2006 version 2.2006.39-14*. Esto borrará todo lo que tengas en la memoria del Nokia.

1. Entra en un PC del laboratorio. Crea en `/tmp` un directorio que se llame como tu *login*, y guarda en él los ficheros que descargarás en esta práctica¹.
2. Descarga la imagen del sistema desde el web del proyecto maemo².
3. Para *flashear* la imagen necesitarás el programa `flasher-2.0` para Linux en Intel, también disponible en el web de maemo³.
4. Dale permiso de ejecución a `flasher-2.0`.
5. Apaga el 770. Desconecta la alimentación. Conéctalo por USB al PC. Como *root* ejecuta el comando para grabar la imagen:

```
./flasher-2 -F SU-18_2006SE_2.2006.39-14_PR_F5_MR0_ARM.bin -f -R
```

cuando diga *Suitable USB device not found, waiting*, enciende el 770.
6. Tras unos segundos, te pedirá que configures idioma, fecha, hora y nombre del dispositivo. Ponle el nombre que prefieras. Cuando te ofrezca configurar un teléfono, cancela.
7. Activa en el 770 el modo *investigación y desarrollo*. Para ello, apaga el 770, verifica que la alimentación está desconectada y el USB conectado al PC. Ejecuta el comando

```
./flasher-2.0 --enable-rd-mode
```

Y cuando aparezca el mensaje *device not found*, enciende el 770.

¹Este directorio se borrará al reiniciar el PC, si por algún motivo prefieres conservarlo, crea uno en tu *home*

²http://maemo.org/downloads/nokia_770

³<http://maemo.org/downloads/d3.php>

1.2. Configuración WIFI

1. Le daremos al 770 la dirección IP de algún PC del laboratorio que esté libre. Elige una *víctima*, toma nota de su configuración IP (dirección, máscara, puerta de enlace y servidor de DNS) y desconecta su cable de red. No olvides conectarlo de nuevo al acabar la práctica.
2. En el 770, haz clic sobre el icono con la bola del mundo en la parte superior derecha de la pantalla. Pulsa *seleccionar conexión*, busca la conexión *test.miguel* e intenta conectarte. (Esto lo hemos hecho solo para añadir esta conexión a las conexiones conocidas).
Desconéctate para poder configurarla. Ahora configura la conexión en
`Herramientas | Panel de control | conectividad | conexiones | editar`
Responde a todas las preguntas con los valores por omisión, y en *ajustes avanzados* configura la red, con los datos que tomaste del PC *víctima*.
3. Comprueba que desde el PC puedes hacer *ping* al Nokia. Comprueba que puedes navegar por Internet en el Nokia.

1.3. Instalación de ssh y xterm

1. Ahora instalaremos un terminal X (*xterm*). En los sistemas basados en Linux Debian, es muy fácil instalar programas (si todo va bien). Basta con indicar la dirección del *repositorio* ⁴, un sitio web donde se recopila el *software*, y a continuación elegir el programa a instalar.
Vete a `Herramientas | Administrador de Aplicaciones`
Vete a `Catálogo | Instalar aplicaciones nuevas` y observa las aplicaciones disponibles.
2. Añadiremos un repositorio más completo: Haz clic sobre la pestaña superior para que aparezca el menú y elige
`Herramientas | Catálogo de Aplicación | Nueva`
Añade
`http://repository.maemo.org/
Distribution mistral
Components free non-free`
Actualiza la lista de paquetes. Observa que ahora en el apartado *instalar aplicaciones nuevas* tienes más programas disponibles. En el apartado *todos*, instala *osso-xterm*.
3. Verás que ahora tienes un *X Terminal* en el apartado *extras* del menú principal del 770. Ejecútalo.
Conviértete en superusuario con el comando `sudo gainroot`
4. Ahora instalaremos el servidor ssh en el 770.
Comprueba que lo tienes disponible
`apt-cache search ssh`

⁴El administrador de aplicaciones del 770 denomina *catálogo* a lo que normalmente llamamos *repositorio*

Instálalo

```
apt-get install ssh
```

5. En el 770, ponle contraseña al superusuario

```
passwd
```

El usuario por omisión es **user**. Ponle también contraseña

```
passwd user
```

6. Desde el PC, entra en el Nokia con una sesión ssh. Hazlo como root y como el usuario **user**. Habitualmente trabajaremos en el Nokia desde el PC usando ssh, para tener un teclado y una pantalla más cómodos.
7. Edita en el *home* del PC un fichero de una línea llamado *probando*, escribe dentro cualquier cosa. Usando scp, copia este fichero en el *home* de *user* en el Nokia.
8. Copia el fichero `/etc/passwd` del Nokia en el directorio `/tmp/` de tu PC.
9. Con los comandos de las transparencias de introducción a Linux, explora la capacidad del Nokia: Tamaño del *disco*, memoria, CPU, etc
10. Repasa en el Nokia otros comandos básicos de Linux.

2. Enlaces Bluetooth en el Nokia 770

2.1. IEEE 802.15.1 -*BlueTooth*

BlueTooth o IEEE 802.15.1 aparece en 1998, es una norma desarrollada por un consorcio de empresas con el objetivo de permitir comunicación inalámbrica mediante radiofrecuencia entre dispositivos generalmente pequeños y próximos: ordenadores, PDAs, teléfonos móviles, periféricos etc. Un requisito fundamental para estos dispositivos es que sean baratos: en 2005 el precio de un módulo *BlueTooth* producido a gran escala es de unos 3 dólares. Esta tecnología soporta hasta 8 dispositivos en una *piconet* o WPAN (*Wireless Personal Area Network*, una red inalámbrica para la conexión de los dispositivos próximos a una persona).

BlueTooth opera en la banda de 2,56 GHz y ofrece hasta 1Mbps, que se reducen a 434 Kbps al descontar la sobrecarga de los protocolos. El alcance máximo es de entre 10 y 100 metros, aunque los resultados obtenidos en la práctica por la mayoría de los equipos disponibles comercialmente son muy inferiores al venir provistos de antenas de mala calidad. En 2004 se definió la norma *BlueTooth v2.0*, con una velocidad de transmisión de 3Mbps (1307 Kbps para datos). En el web hay mucha información sobre este protocolo, recomendamos el artículo en la *wikipedia* (en inglés).

En la norma *Bluetooth* se definen perfiles, que son servicios a nivel de aplicación. Cada dispositivo ofrece uno o más servicios, como por ejemplo

- Service Discovery Application Profile (SDAP). Permite conocer qué servicios ofrecen otros dispositivos próximos. Todos los equipos *Bluetooth* cuentan con este perfil. Emplea el protocolo SDP (*Service Discovery Protocol*).
- Human Interface Device Profile (HID). Proporciona soporte para teclados, ratones, *joysticks*, etc
- Object Push Profile (OPP). Permite enviar ficheros como fotografías o tarjetas de visita.
- Personal Area Networking Profile (PAN). Este servicio hace posible usar *Bluetooth* como protocolo de enlace bajo una red TCP/IP. Emplea el protocolo BNEP (*Bluetooth Network Encapsulation Protocol*). Es el servicio que utilizaremos en estas prácticas.

Existen muchos otros perfiles: para dispositivos *manos libres*, auriculares, emisión de vídeo, etc. Para una lista completa, consultar el artículo *bluetooth profile* en la *wikipedia* (en inglés).

2.2. Protocolo BNEP

El escenario de uso más habitual del protocolo BNEP es la siguiente: Una máquina como el Nokia 770 que no tiene acceso por sí misma a Internet se denomina PANU (PAN User). Establece un enlace *Bluetooth* con un NAP (Network Access Point), una estación que actúa como *router*, ofreciendo al PANU acceso a otra red, típicamente Internet. El NAP puede estar conectado a Internet mediante cualquier tecnología. Las aplicaciones suelen llamar al NAP simplemente *teléfono*.

En este apartado estableceremos un enlace BNEP, donde el Nokia 770 será el PANU y el PC será el NAP. Para trabajar en el 770 cómodamente, lo conectaremos a la red mediante Wi-Fi. Esto nos

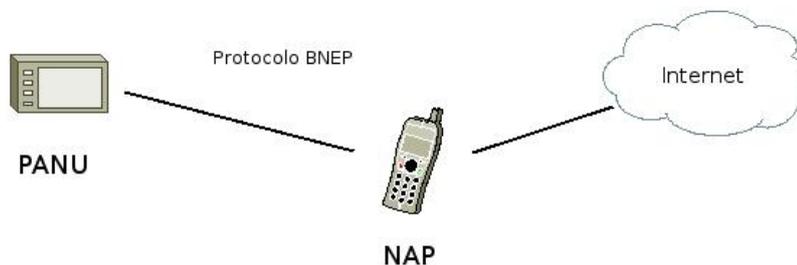


Figura 1: Conexión BNEP

permitirá entrar mediante ssh y teclear en un teclado *de verdad* (cuanto tengamos la conexión *BlueTooth* funcionando, podremos prescindir del acceso Wi-Fi).

Comprobaremos que disponemos de las librerías adecuadas tanto en el PC como en el 770, que cada máquina reconoce su interfaz *Bluetooth* local y también el remoto si está visible. Estableceremos una conexión L2CAP entre los ordenadores e instalaremos en el núcleo del Nokia el módulo para bnep. En el PC lanzaremos el demonio *pand*, que ofrecerá el perfil NAP. Tras comprobar desde el 770 que NAP está disponible, crearemos una conexión PAN entre las máquinas. Con esto tendremos un interfaz *Bluetooth* en cada máquina que podremos configurar como cualquier interfaz IP.

1. En primer lugar configuraremos el código PIN para *BlueTooth* en el PC. El PIN un número de 4 dígitos que será la contraseña de todas las conexiones que hagamos entre dos dispositivos. El valor por defecto es 1234, lo cambiaremos editando el fichero `/etc/bluetooth/pin` (es necesario hacerlo como *root*).
2. Conectamos el 770 a la red mediante Wi-Fi.

Mediante ssh abrimos una sesión como root en el 770 y comprobamos que tenemos instalado *BlueZ*, que es la implementación de *Bluetooth* estándar en Linux.

```
Nokia770-26:~# dpkg -l |grep -i bluez
ii bluez-utils      2.25-cvs20060504osso2   Bluetooth tools and daemons
ii libbluetooth1   2.25-cvs20060428       Library to use the BlueZ Linux Bluetooth sta
```

Comprobamos esto mismo también en el PC.

3. En el PC abrimos una nueva shell, para ver los *logs* del sistema

```
root@mazinge:~# tail -f /var/log/syslog
```

Modificamos el tamaño de esta ventana para que ocupe tres o cuatro líneas y lo dejamos en un rincón de nuestro escritorio. Aunque no lo mencionemos de nuevo en este guión, debemos consultar continuamente este fichero.

4. Emplearemos el comando `hcitool`, que sirva para configurar conexiones *bluetooth*. Lo invocamos en el 770 sin argumentos para comprobar que está disponible y para conocer sus opciones.

```
Nokia770-26:~# hcitool
Nokia770-26:~# hcitool | more
```

Hacemos lo mismo en el PC, y consultamos su página de manual.

```
koji@mazinger:~$ man hcitool
```

5. Pinchamos la *mochila Bluetooth* (el adaptador usb) y averiguamos su dirección, que anotaremos (preferentemente en un fichero).

```
koji@mazinger:~$ hcitool dev
Devices:
    hci0    00:02:72:01:A3:3D
```

Hacemos lo mismo en el 770. Observamos que el dispositivo no aparece, puesto que para ahorrar energía, el 770 lo mantiene apagado. Para que se active, desde el GUI de el 770 exploramos los dispositivos disponibles.

Herramientas | Panel de Control | Teléfono | Nueva

Ejecutamos de nuevo `hcitool dev` en el 770, comprobamos que reconoce el dispositivo y anotamos su dirección.

El dispositivo sólo permanece activo unos cuantos segundos, así que en los próximos apartados tendremos que repetir esta operación continuamente, aunque no volveremos a mencionarlo en este guión. (Cuando tengamos una conexión BNEP establecida esto ya no será necesario).

6. Comprobamos que desde el 770 vemos el PC

```
Nokia770-26:~# hcitool scan
Scanning ...
    00:16:CB:40:B3:C9    Ordenador de Juan
    00:02:72:01:A3:3D    mazinge-0
```

Hacemos lo mismo desde el PC, aunque no veremos el 770 porque por omisión no anuncia su presencia.

7. Desde el 770 establecemos una conexión *Bluetooth* con el PC

```
Nokia770-26:~# hcitool cc 00:02:72:01:A3:3D
```

Comprobamos que podemos enviar paquetes del protocolo de enlace de *BlueTooth* (L2CAP, *Logical Link Control and Adaptation Protocol*) desde el 770 hasta el PC

```
Nokia770-26:~# l2ping 00:02:72:01:A3:3D
Ping: 00:02:72:01:A3:3D from 00:12:37:39:17:F5 (data size 44) ...
```

```
44 bytes from 00:02:72:01:A3:3D id 0 time 27.83ms
44 bytes from 00:02:72:01:A3:3D id 1 time 45.56ms
44 bytes from 00:02:72:01:A3:3D id 2 time 23.59ms
```

(Interrumpimos el comando con Ctrl C)

Podemos comprobar que desde el PC el 770 no es visible. Consultamos en el PC la página de manual de l2ping

```
koji@mazinge:~/ man l2ping
```

8. Desde el 770 establecemos una conexión con el PC y comprobamos la potencia de la señal recibida

```
Nokia770-26:~# hcitool cc 00:02:72:01:A3:3D
Nokia770-26:~# hcitool rssi 00:02:72:01:A3:3D
RSSI return value: 6
```

9. Para usar el protocolo BNEP tenemos que cargar en el núcleo de linux el módulo bnep. En la mayoría de las máquinas linux podríamos usar el comando `modprobe` al que solo hay que indicar el nombre del módulo (`modprobe bnep`), pero en el 770 tenemos que usar `insmod` y la localización exacta del módulo:

```
Nokia770-26:~# insmod /mnt/initfs/lib/modules/2.6.16.27-omap1/bnep.ko
```

10. Comprobamos que tenemos disponible en el PC el demonio PAN. Para ello ejecutamos el comando `pand` sin argumentos. También consultamos su página de manual.

```
koji@mazinge:~$ pand
koji@mazinge:~$ man pand
```

Comprobamos que también está disponible en el 770. Como root, lanzamos el demonio en el PC

```
root@mazinge:~ pand -s -r NAP
```

Este comando hace que quede lanzado el demonio, que permanezca a la escucha de conexiones entrantes y que se comporte como NAP (un *teléfono*).

Comprobamos que el proceso está activo

```
koji@mazinge:~$ ps -ef |grep pand
root    11410      1  0 13:14 ?        00:00:00 pand -s -r NAP
koji    2602 30556   0 21:03 pts/7    00:00:00 grep pand
```

11. Ahora haremos uso del servicio de descubrimiento de vecinos (protocolo SDP). Desde el PC consultamos el manual del comando `sdptool`.

```
koji@mazinge:~$ man sdptool
```

En el 770 ejecutamos el comando, para comprobar que el PC nos ofrece servicio de NAP

```
Nokia770-26:~# sdptool browse 00:02:72:01:A3:3D
Browsing 00:02:72:01:A3:3D ...
Service Name: Network Access Point
Service RecHandle: 0x10000
Service Class ID List:
  "Network Access Point" (0x1116)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 15
  "BNEP" (0x000f)
    Version: 0x0100
    SEQ16: 800 806
Profile Descriptor List:
  "Network Access Point" (0x1116)
    Version: 0x0100
```

12. Ahora cuando desde el GUI del 770 seleccionemos nuestro *teléfono* (el PC), nos ofrecerá vincularnos con él y nos preguntará su PIN.
13. Desde el 770 creamos una conexión PAN con el PC

```
Nokia770-26:~# pand -c 00:02:72:01:A3:3D
```

En `/var/log/syslog` veremos un mensaje

```
New connection from 00:12:37:39:17:F5 bnep%d
```

(Podemos ignorar el error que muestra en GUI del nokia indicando que el dispositivo no dispone de servicios que se puedan usar).

Con esto tenemos disponible en cada máquina un interfaz de red llamado `bnep0`. En el 770 le asignamos la dirección IP 10.0.0.2 (que pertenece a un rango de direcciones reservado para redes privadas):

```
ifconfig bnep0 10.0.0.2
```

y en el PC

```
ifconfig bnep0 10.0.0.1
```

Ahora comprobamos que el interfaz `bnep` esté funcionando, tanto en el 770

```
Nokia770-26:~# ifconfig
bnep0    Link encap:Ethernet  HWaddr 00:12:37:39:17:F5
         inet addr:10.0.0.2  Bcast:10.255.255.255  Mask:255.0.0.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:14 errors:0 dropped:0 overruns:0 frame:0
         TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:1294 (1.2 KiB)  TX bytes:1112 (1.0 KiB)
```

como en el PC

```
ifconfig
koji@mazinger:~/rom$ ifconfig
bnep0    Link encap:Ethernet  HWaddr 00:02:72:01:A3:3D
         inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
         inet6 addr: fe80::202:72ff:fe01:a33d/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:14 errors:0 dropped:0 overruns:0 frame:0
         TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:1132 (1.1 KiB)  TX bytes:1294 (1.2 KiB)
```

(Hemos omitido aquí la salida correspondiente al resto de interfaces).

En el 770 hacemos ping a nuestro propio interfaz

```
Nokia770-26:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=64 time=0.3 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.3 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.3 ms
```

(Interrumpimos el comando con Ctrl C)

Hacemos ping al interfaz del PC

```
Nokia770-26:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=64 time=75.5 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=21.3 ms

--- 10.0.0.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 21.3/48.4/75.5 ms
```

Observamos que el tiempo que tardan los paquetes en ir y venir es ligeramente mayor.

Desde el PC también hacemos ping a su propio interfaz y al del 770.

14. Desde el PC hacemos ssh como root a la dirección IP del interfaz *Bluetooth* del 770.