RouterOS de Mikrotik

Autores:

- Pablo Boronat Pérez (Universitat Jaume I)
- Miguel Pérez Francisco (Universitat Jaume I)
- David Rubert Viana (Universitat Jaume I)

Introducción

Mikrotik RouterOS es un sistema operativo basado en Linux y especializado en enrutamiento para trabajar con PCs o con las placas base de Mikrotik RouterBOARD. Es un sistema privativo cerrado pero muy potente para realizar tareas de enrutado en una red: puede actuar como firewall, VPN Server y Cliente, Gestor de ancho de banda, QoS, punto de acceso inalámbrico, ...

Acceso al sistema

Para poder acceder al router hay que conectar el ordenador utilizando un cable UTP al router a través del POE (*Power ower ethernet*, dispositivo que permite alimentar eléctricamente el router a través del cable UTP).

Una vez conectado, el mikrotik emite un pitido indicando que se ha iniciado el proceso de arranque. Al finalizar emite un doble pitido lo cual indica que el dispositivo ya está listo para operar.

La cuenta por omisión es `admin` sin password (hay que presionar `Enter` cuando se solicite). Se puede cambiar el password usando el comando '/password'. La IP por defecto de los dispositivos suele ser la 192.16.88.1/24 en la interfaz `ether1` (la que tiene el POE).

En el ordenador hay que poner una IP en la misma subred que el dispositivo. Si la IP del dispositivo es la que viene de fábrica (192.168.88.1/24) se puede poner en el ordenador la IP 192.168.88.10/24, por ejemplo.

Winbox. Acceso por MAC y por IP

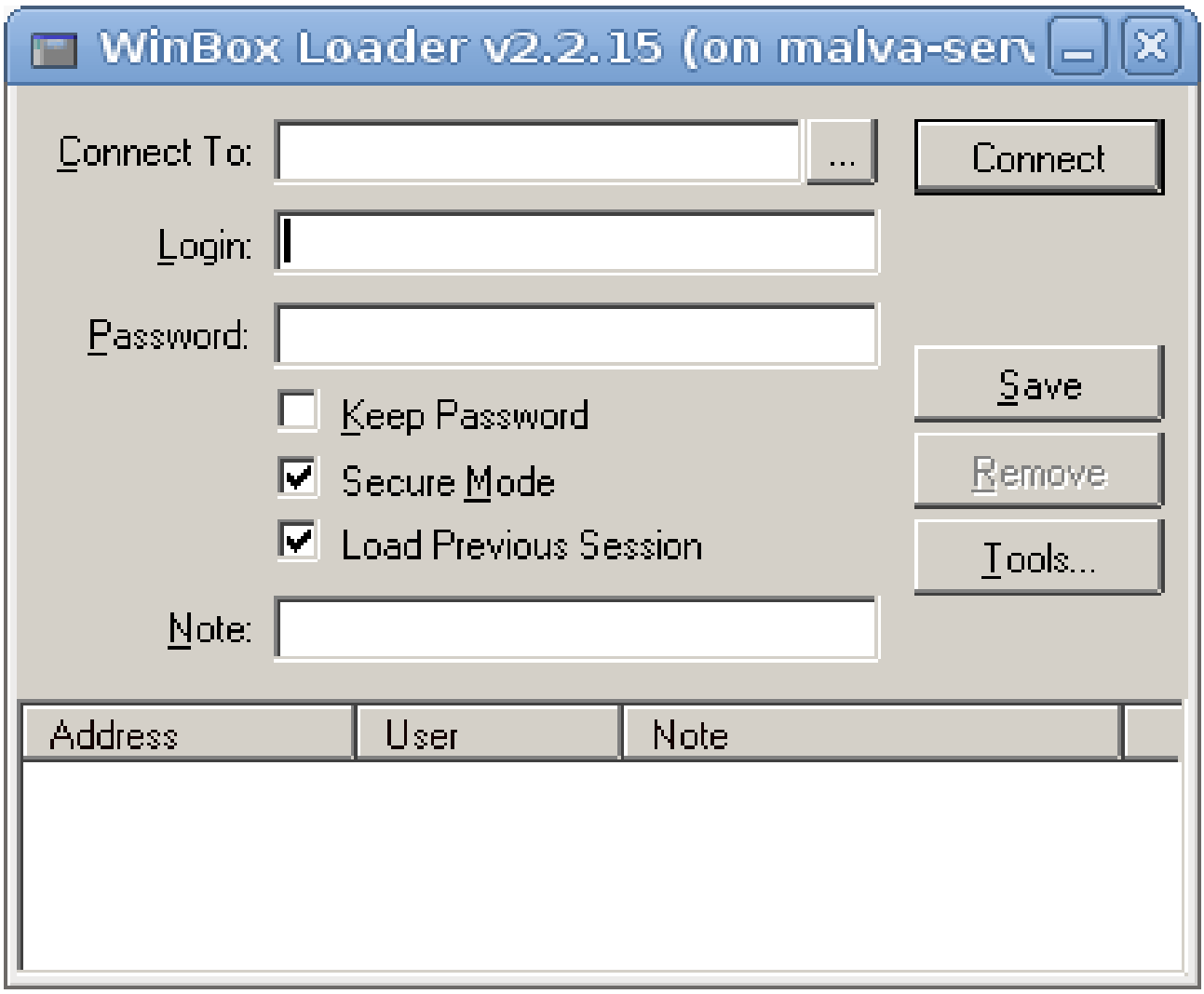
`Winbox` es una utilidad para windows que permite la administración del sistema RouterOS utilizando una interfaz gráfica sencilla. `Winbox` es una aplicación diseñada para windows, en ordenadores con GNU/Linux o MacOS se puede ejecutar utilizando wine (*wine* es una aplicación que permite ejecutar programas de windows en entornos GNU/Linux).

Todas las funciones de la interfaz winbox son muy parecidas a las órdenes de la consola aunque algunas de las configuraciones avanzadas y críticas del sistema no están disponibles en winbox.

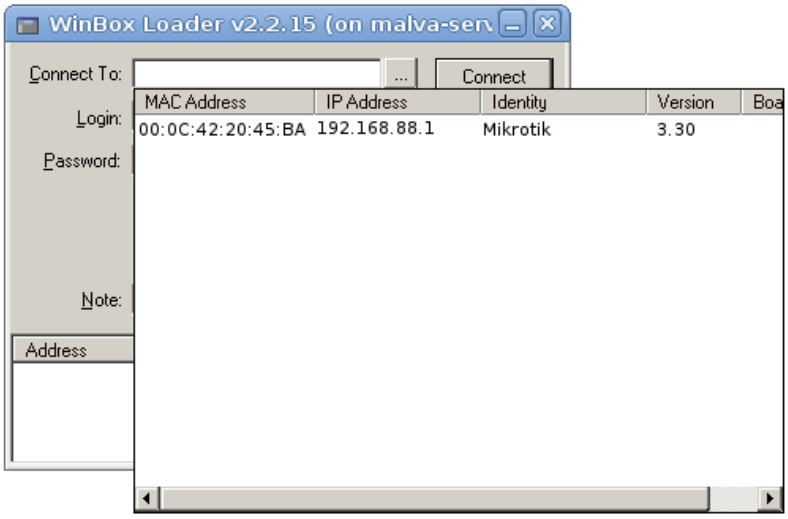
Winbox se puede descargar directamente desde el router accediendo a el mediante un navegador web utilizando su IP como se muestra en al siguuiente figura.

Existen diferentes versiones de winbox, algunas versiones de winbox no son compatibles con versiones más avanzadas de RouterOS, por ello es conviene descargarse la versión correspondiente del router que queremos configurar. En otro caso puede que algunas opciones no funcionen adecuadamente.

Para acceder con winbox al router hay que ejecutarlo haciendo doble clic sobre el programa. Al hacerlo aparecerá una ventana como la siguiente



Si pinchamos sobre los puntos suspensivos se muestran los routers a los que se tiene acceso



Como se observa se muestra la MAC y la IP del router, puede que se muestren varios routers si estamos conectados a una red. Basta con seleccionar el router (o escribir directamente la IP o MAC en la casilla `Connect to`) indicar el `login` y el `password` y pulsar sobre el botón `Connect` para acceder al dispositivo.

`/tool mac-telnet`
`00:02:6F:06:59:42`http://wiki.mikrotik.com/wiki/MAC_access

Ejercicio 3.1

Terminal

Otra forma posible de acceder al sistema RouterOS es mediante un ssh a la IP del router.

```
ssh admin@192.168.88.1

The authenticity of host '192.168.88.1 (192.168.88.1)' can't be
established.
DSA key fingerprint is
3e:0a:03:81:70:50:3f:9a:71:0d:98:29:5b:ee:4a:77.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.88.1' (DSA) to the list of
known hosts.
admin@10.228.130.1's password:



  MMM      MMM       KKK                          TTTTTTTTTTT
KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT
KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III
KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III
KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III
KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III
KKK  KKK

  MikroTik RouterOS 3.30 (c) 1999-2009
http://www.mikrotik.com/

(12 messages not shown)
jun/01/2011 13:29:32 system,error,critical login failure for user
admin from 10.228.130.62 via ssh
jan/02/1970 01:00:07 system,error,critical router rebooted without
proper shutdown, probably power outage

[admin@CS-UJI-BiblAP] >
export
/export
/interface wireless export
printprint advancedprint detail
/interface print
/interface wireless print advanced
```

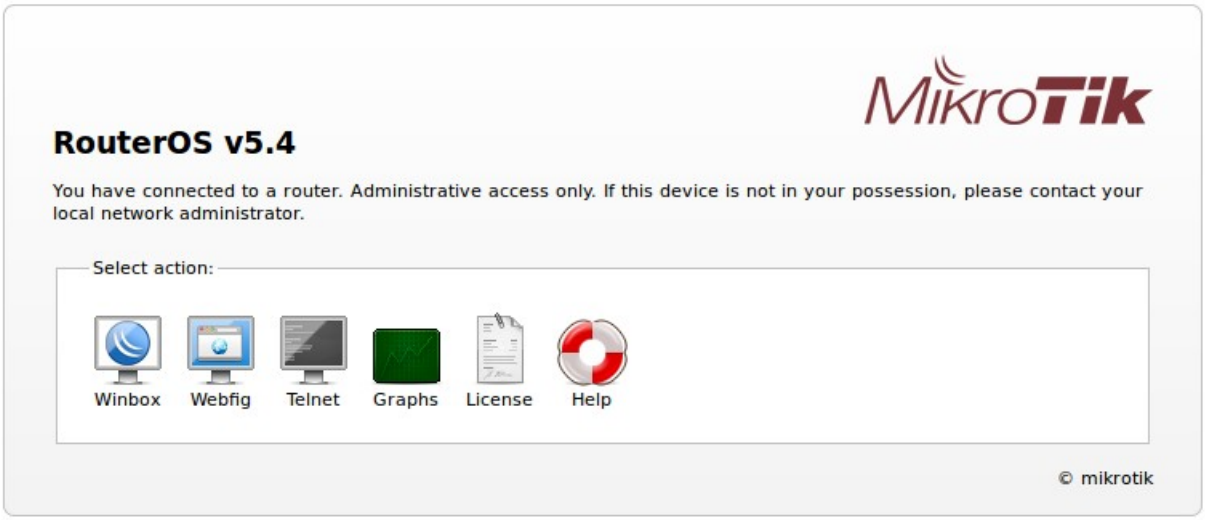
Ejercicio 3.2`/export`

WebFig

Desde la versión 5 de RouterOS existe la posibilidad de configurar el router utilizando WebFig, una utilidad web para configurar el router.

La ventaja de WebFig es que se puede acceder directamente desde el router y no se requiere software adicional (excepto navegador web con JavaScript). Como Webfig es independiente de la plataforma, se puede utilizar desde cualquier dispositivo sin necesidad de un software desarrollado para la plataforma específica. Se trata de una alternativa al WinBox, ambos tienen un diseño similar.

Se puede acceder a WebFig mediante un navegador utilizando la dirección IP del router que se quiere configurar o consultar. Al hacer clic en el icono de webfig, el sistema solicitará el nombre de usuario y la contraseña. Tras lo cual se podrá acceder a las distintas opciones del sistema.

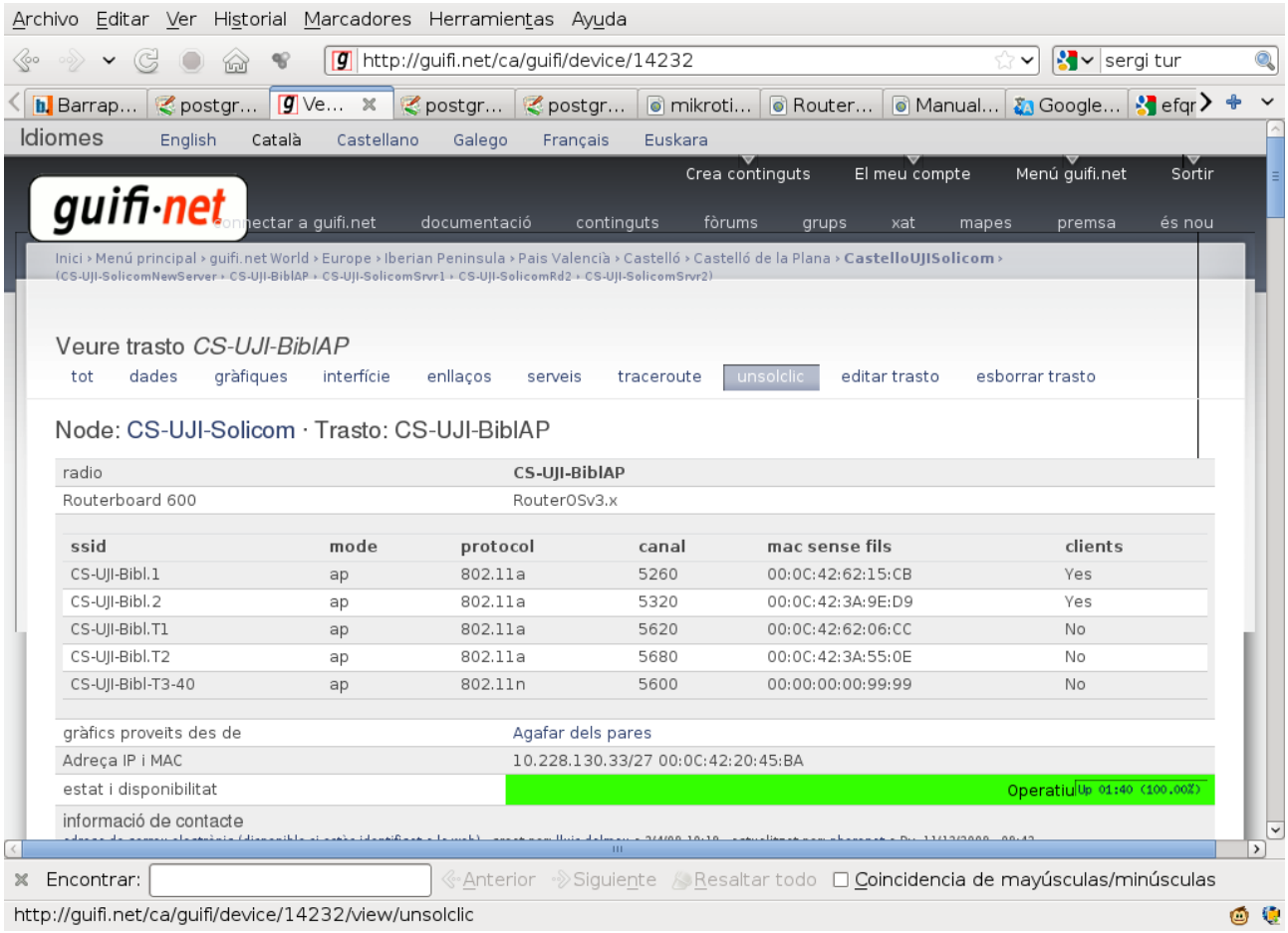


Unsolclic

Utilizando algunas de las formas explicadas en el punto anterior, se puede acceder al dispositivo y configurarlo para actuar como supernodo (Punto de acceso, AP). Hay que definir los ESSID de las distintas tarjetas de radio, la frecuencia (canal) a la que trabaja, la IP de cada interfaz, enrutamiento dinámico, ... Para realizar esta configuración se precisa tener conocimientos avanzados de redes y del sistema RouterOS.

Para facilitar la instalación y configuración de un supernodo la web de guifi.net permite generar la configuración una vez introducida la información necesaria en la web. Como se ha comentado en el capítulo 1 (Crear un nodo multirradio), la web de guifi.net permite definir un supernodo para dar cobertura a nodos clientes.

Si se han dado esos pasos en guifi.net, se puede acceder a la configuración del dispositivo a través del enlace unsolclic que aparece en la web



La configuración para un mikrotik consiste en una serie de órdenes que se han de ejecutar en el terminal (si se utiliza el winbox o el webFig hay que pulsar sobre «New Terminal»). Para aplicar la configuración se ha de copiar las órdenes del unsolclic y pegarlas en el terminal. Así se va ejecutando la configuración.

```
# Generado por:
# RouterOSv3.x
:log info "Unsolclic for 14232-CS-UJI-BiblAP going to be
executed."
#
# Configuration for RouterOS 3.30
# Dispositivo: 14232-CS-UJI-BiblAP
#
# ATENCIÓN: Versión beta
#
# Métodos para subir/ejecutar este script:
# 1.-Como un script. Sube este texto como un script bien con:
#     a.Winbox (con Linux es necesario wine)
#     b.Terminal (telnet, ssh...)
#    Entonces ejecuta el script con:
#      > /system script run nombre_del_script
# 2.-Fichero importado:
#     Guarda este texto en un fichero, luego súbelo al router
#     utilizando ftp con un nombre como "script_name.rsc".
#     (ten en cuenta que la extensión ".rsc" es necesaria)
#     Ejecuta el fichero importado utilizando el comando:
```

```
#      > /import nombre_del_script
# 3.-Telnet copiar&pegar:
#     Abre una sesión de terminal, y copia y pega el texto
#     directamente en la ventana de la terminal.
#
# Notas:
# -el paquete routing-test es necesario. Asegúrate de que está
activado en paquetes del sistema

...

/ system identity set name=CS-UJI-BiblAP
#
# DNS (client & server cache) zone: 11275
/ip dns set primary-dns=10.228.130.162 secondary-
dns=10.228.130.162 allow-remote-requests=yes
:delay 1
#
# NTP (client & server cache) zone: 11275
/system ntp client set enabled=yes mode=unicast primary-
ntp=10.228.130.162 secondary-ntp=10.228.130.162
:delay 1
#
# Servidor de ancho de banda
/ tool bandwidth-server set enabled=yes authenticate=no allocate-
udp-ports-from=2000
#
# SNMP
/snmp set contact="guifi@guifi.net" enabled=yes location="CS-UJI-
Solicom"
#
# Guest user
/user
:foreach i in [find group=read] do={/user remove $i;}
add name="guest" group=read address=0.0.0.0/0 comment=""
disabled=no

...
```

Al principio del fichero se puede observar una serie de comentarios sobre cómo aplicar el unsolclic y sobre paquetes que hay que tener instalados. A continuación empiezan las órdenes de configuración.

Para activar las radios hay que ejecutar:

```
/interface wireless enable 0
/interface wireless enable 1
...
```

donde 0, 1, etc. indica el número de tarjeta de radio. Si se utiliza el winbox se puede acceder a las interfaces wireless utilizando directamente el botón wireless.

Al aplicar el unsolclic, si se produce algún error, se muestra en color rojo, lo cual permite localizarlos fácilmente.

`/system reset-configuration`[1)]

Eliminar el DHCP

Como se ha comentado en el primer capítulo, es conveniente deshabilitar el DHCP. Para hacerlo, hay que eliminar las líneas que hacen referencia a él en el unsolclic,

A continuación se muestran las líneas que habría que comentar.

```
# DHCP
:foreach i in [/ip pool find name=dhcp-wLan/Lan] do={/ip pool
remove $i;}
/ip pool add name=dhcp-wLan/Lan ranges=10.228.130.39-10.228.130.62
:foreach i in [/ip dhcp-server find name=dhcp-wLan/Lan] do={/ip
dhcp-server remove $i;}
/ip dhcp-server add name=dhcp-wLan/Lan interface=wLan/Lan address-
pool=dhcp-wLan/Lan disabled=no
:foreach i in [/ip dhcp-server network find
address="10.228.130.32/27"] do={/ip dhcp-server network remove
$i;}
/ip dhcp-server network add address=10.228.130.32/27
gateway=10.228.130.33 domain=guifi.net comment=dhcp-wLan/Lan
/ip dhcp-server lease
:foreach i in [find comment=""] do={remove $i;}
:delay 1
add address=10.228.130.34 mac-address=00:15:6D:93:50:C4 client-
id=ALZonaRd1 server=dhcp-wLan/Lan
add address=10.228.130.35 mac-address=00:15:6D:DD:50:F3 client-
id=CdPCamiRd1 server=dhcp-wLan/Lan
add address=10.228.130.36 mac-address=00:15:6D:9A:77:C5 client-
id=VRUJI100Rd1 server=dhcp-wLan/Lan
...
```

Modificaciones si se ha definido un nodo híbrido

Si se ha definido un nodo híbrido (un router mikrotik con antenas de ubiquiti en modo bridge) el unsolclic que genera la web (a fecha de 20/6/2011) no se puede aplicar directamente. Hay que hacer una serie de cambios:

- Quitar el interfaz `wlan1` del bridge `wLan/Lan`, basta con comentar (anteponiéndole una #) la línea

```
add interface=wlan1 bridge=wLan/Lan
```

- Quitar la definición de las radios. Se puede borrar o comentar (anteponiéndole una #), por ejemplo para eliminar la definición de la

[1)] Esta opción no se puede realizar mediante el winbox ni mediante el webfig

primera radio del nodo de la Biblioteca de la UJI, habría que comentar el siguiente trozo:

```
/interface wireless set wlan1 name="wlan1" \
radio-name="CS-UJI-Bibl.1" mode=ap-bridge ssid="guifi.net-CS-UJI-
Bibl.1" \
band="5ghz" \
frequency-mode=regulatory-domain country=spain antenna-gain=18 \
frequency=5260 \
dfs-mode=none \
antenna-mode=ant-a wds-mode=static wds-default-bridge=none wds-
default-cost=100 \
wds-cost-range=50-150 wds-ignore-ssid=yes hide-ssid=no
:delay 1
```

- Quitar la definición de enlaces WDS, ya que estos enlaces los hacen los dispositivos de ubiquiti. Hay que quitar el código de este estilo.

```
# Type: wds/p2p
# Remove all existing wds interfaces
:foreach i in [/interface wireless wds find master-
interface=wlan1] \
do={:foreach n in [/interface wireless wds get $i name] \
do={:foreach inum in [/ip address find interface=$n] \
do={/ip address remove $inum;};}; \
/interface wireless wds remove $i;}
/ interface wireless wds
add name="wds_UJIHumanasRd1" master-interface=wlan1 wds-
address=00:15:6D:10:96:66 disabled=no
```

- Cambiar las interfaces sobre las que se definen los enlaces troncales, en vez de ser la interfaces wds_XXXXX debe ser la interfaz ether en la que está conectado el dispositivo de ubiquity. Así el codigo

```
/ ip address add address=172.16.107.138/30 network=172.16.107.136
broadcast=172.16.107.139 interface=wds_UJIHumanasRd1 disabled=no
comment="wds_UJIHumanasRd1"
/ routing ospf interface
:foreach i in [/routing ospf interface find
interface=wds_UJIHumanasRd1] do={/routing ospf interface remove
$i;}
add interface=wds_UJIHumanasRd1
/ routing ospf network
:foreach i in [/routing ospf network find
network=172.16.107.136/30] do={/routing ospf network remove $i;}
add network=172.16.107.136/30 area=backbone disabled=no
/ routing bgp peer
:foreach i in [find name=UJIHumanasRd1] do={/routing bgp peer
remove $i;}
add name="UJIHumanasRd1" instance=default remote-
address=172.16.107.137 remote-as=23616 \
multihop=no route-reflect=no ttl=1 in-filter=ospf-in out-
filter=ospf-out disabled=yes
```

debe cambiarse por

```
/ ip address add address=172.16.107.138/30 network=172.16.107.136
broadcast=172.16.107.139 interface=ether2 disabled=no
comment="wds_UJIHumanasRd1"
/ routing ospf interface
:foreach i in [/routing ospf interface find interface=ether2]
do={/routing ospf interface remove $i;}
add interface=ether2
/ routing ospf network
:foreach i in [/routing ospf network find
network=172.16.107.136/30] do={/routing ospf network remove $i;}
add network=172.16.107.136/30 area=backbone disabled=no
/ routing bgp peer
:foreach i in [find name=ether2] do={/routing bgp peer remove $i;}
add name="ether2" instance=default remote-address=172.16.107.137
remote-as=23616 \
multihop=no route-reflect=no ttl=1 in-filter=ospf-in out-
filter=ospf-out disabled=yes
```

donde ether2 puede cambiar en función de a qué interfaz este conectado el dispositivo de ubiquity

```
/ ip address …commentether
```

- Añadir las interfaces por cable y las subredes utilizadas para administrar los aparatos de ubiquiti en el protocolo OSPF. Así por ejemplo a la línea

```
/ ip address add address=10.228.189.41/29 network=10.228.189.40
broadcast=10.228.189.47 interface=ether2 disabled=no comment=""
```

Hay que añadirle

```
/ ip address add address=10.228.189.41/29 network=10.228.189.40
broadcast=10.228.189.47 interface=ether2 disabled=no comment=""
/ routing ospf interface add interface=ether2
/ routing ospf network add network=10.228.189.40/29 area=backbone
disabled=no
```

Cada una de las antenas «esclavas» hay que configurarlas manualmente. Se debe definir, entre otras cosas, el enlace WDS, SSID, país, canal, modo de trabajo en bridge, IP administrativa y puerta de enlace. Todo ello se verá en el siguiente tema.

Ejercicio 3.3

Ejercicio 3.4

```
/interface wireless/ip address
```

Nodos híbridos con Omnitik:

- https://docs.google.com/document/d/1VU56JXudZKrohGrRGOTFVv_TBC93HgNz2XPJBZxzERI/edit
- https://docs.google.com/document/d/1hQJ7o9OEs0m_LqmR0h4ln_dk5VwrhE-r8Edb8as2QY8/edit

Configuración y herramientas

En este apartado se van a comentar distintas opciones de configuración que parecen interesantes en el día a día de trabajo con los routers. Para profundizar más en el tema se puede consultar el manual de RouterOS (http://wiki.mikrotik.com/wiki/Category:Manual).

Interfaces

`/interface`

En este apartado del sistema operativo se pueden configurar las interfaces del router (en estos apuntes se verá principalmente las interfaces ethernet y wireless).

`/interface print`

```
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE            MTU   L2MTU
 0  R  ether1                              ether           1500  1600
 1  R  ether2                              ether           1500  1600
 2     ether3                              ether           1500  1600
 3  R  wlan1                               wlan            1500  2304
 4  R  wlan2                               wlan            1500  2304
 5  X  wlan3                               wlan            1500
 6  R  wlan4                               wlan            1500  2304
 7  R  wLan/Lan                            bridge          1500  1600
 8     wds_VRPlazaMajor10Rd2               wds             1500
 9  R  wds_CSCEFIRERd2                     wds             1500  2304
10  R  wds_bncssmAPSantiago124MRd1         wds             1500  2304
```

Las interfaces marcadas con una R indica que están funcionando, las que tienen una X están deshabilitadas, las que no aparece ninguna marca indica que no se están utilizando.

Con esta orden se puede consultar la información sobre las distintas interfaces definidas en el router.

Otras características importantes dentro de interfaces son:

- `bonding`: Permite agregar varias interfaces para aumentar el ancho de banda de un enlace y ser más tolerante a fallos (http://wiki.mikrotik.com/wiki/Manual:Interface/Bonding)
- `bridge` Permite unir mediante un puente a varias interfaces (http://wiki.mikrotik.com/wiki/Manual:Interface/Bridge). Por ejemplo el unsolclic genera un bridge entre la interfaz `ether1` y `wlan1` llamado `wLan/Lan`.
- `disable`: permite deshabilitar una interfaz
- `enable`: permite habilitar una interfaz

*puentebridge*LAN*switch*

Ethernet

```
/interface ethernet
```

En este apartado se pueden configurar y acceder a la información de las ethernets del router (http://wiki.mikrotik.com/wiki/Manual:Interface/Ethernet).

```
[admin@CS-UJI-BiblAP] > /interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME                                                MTU   MAC-
ADDRESS       ARP
 0 R  ether1                                              1500
00:0C:42:20:45:BA enabled
 1 R  ether2                                              1500
00:0C:42:20:45:BB enabled
 2    ether3                                              1500
00:0C:42:20:45:BC enabled
```

Cuando se está escribiendo una orden en el terminal, al pulsar el tabulador, el sistema completa la orden

```
/inter<TAB>
```

se tranforma en

```
/interface
```

Si se pulsa el interrogante, muestra las posibles opciones que se pueden dar a la orden que se está escribiendo

```
[admin@CS-UJI-BiblAP] > /interface ?
.. -- go up to root
bonding -- Interface bonding
bridge -- Bridge interfaces
comment -- Set comment for items
disable -- Disable interface
edit --
enable -- Enable interface
eoip -- Ethernet over IP tunnel interface
ethernet -- Ethernet interfaces

...
```

Si, cuando se ha escrito la orden se pulsa dos veces el tabulador, se muestran también las posibles opciones pero sin mostrar la ayuda

```
[admin@CS-UJI-BiblAP] > /interface <TAB><TAB>
..          ipip          ovpn-server   pptp-client  comment  find

bonding     l2tp-client   ppp-client    pptp-server  disable  get

bridge      l2tp-server   ppp-server    vlan         edit
monitor-traffic
eoip        mesh          pppoe-client  vrrp         enable   print

ethernet    ovpn-client   pppoe-server  wireless     export   set
```

Ejercicio 3.5

Ejercicio 3.6ethbackup

Wireless. WDS

/interface wireless

wirelessEn este apartado se pueden configurar y acceder a la información de las interfaces inalámbricas del router (http://wiki.mikrotik.com/wiki/Manual:Interface/Wireless).

RouterOS permite trabajar con los protocolos 802.11a, 802.11b, 802.11g y 802.11n, también ofrece posibilidades de cifrado (WPA, WEP, AES, ...), Sistema de Distribución Inalámbrico (WDS), Selección dinámica de frecuencia (DFS), ...

```
[admin@CS-UJI-BiblAP] > /interface wireless print
Flags: X - disabled, R - running
 0  R name="wlan1" mtu=1500 mac-address=00:0C:42:62:15:CB
arp=enabled
      interface-type=Atheros AR5413 mode=ap-bridge
ssid="guifi.net-CS-UJI-Bibl.1"
      frequency=5260 band=5ghz scan-list=default antenna-mode=ant-
a wds-mode=static
      wds-default-bridge=none wds-ignore-ssid=yes default-
authentication=yes
      default-forwarding=yes default-ap-tx-limit=0 default-client-
tx-limit=0
      hide-ssid=no security-profile=default compression=no

 1  R name="wlan2" mtu=1500 mac-address=00:0C:42:3A:9E:D9
arp=enabled
      interface-type=Atheros AR5413 mode=ap-bridge
ssid="guifi.net-CS-UJI-Bibl.2"
      frequency=5320 band=5ghz scan-list=default antenna-mode=ant-
a wds-mode=static
      wds-default-bridge=none wds-ignore-ssid=yes default-
authentication=yes
      default-forwarding=yes default-ap-tx-limit=0 default-client-
tx-limit=0
      hide-ssid=no security-profile=default compression=no

 2 X  name="wlan3" mtu=1500 mac-address=00:0C:42:62:06:CC
arp=enabled
      interface-type=Atheros AR5413 mode=ap-bridge
ssid="guifi.net-CS-UJI-Bibl.T1"
...
```

Algunas opciones interesantes de este apartado son:

```
access-list -- The access list
add -- Create a new item
disable -- Disable items
enable -- Enable items
info -- Wireless interface information
registration-table -- The registration table
remove -- Remove item
```

```
scan -- Scan for the wireless devices
sniffer -- Wireless sniffer
```

`/interface wireless registration-table` es una opción muy interesante que permite ver qué nodos cliente o nodos con enlace WDS estan conectados en un AP, en qué radio y la calidad de la señal.

```
[admin@CS-UJI-BiblAP] > /interface wireless registration-table
print
 # INTERFACE     RADIO-NAME       MAC-ADDRESS       AP  SIGNAL-
STRENGTH TX-RATE UPTIME
 0 wlan2         UBNT             00:15:6D:3C:6D:2D no  -
59dBm@6Mbps    54Mbps  2w3d6h45m2s
 1 wlan2         UBNT             00:15:6D:3C:4F:B6 no  -
78dBm@6Mbps    54Mbps  2w3d6h45m1s
 2 wlan1         UBNT             00:15:6D:D2:D6:FC no  -
77dBm@18Mbps   48Mbps  2w3d6h45m
11 wlan2         UBNT             00:15:6D:8E:2E:8B no  -
85dBm@6Mbps    18Mbps  4d1h38m38s
12 wlan4         BenicasApSntgT0- 00:0C:42:61:86:69 yes -
89dBm@6Mbps    12Mbps  3d10h9m36s
21 wlan1         UBNT             00:15:6D:D0:1A:9D no  -
88dBm@6Mbps    6Mbps   1h24m52s
22 wlan2                          00:15:6D:D0:93:F2 no  -
86dBm@6Mbps    6Mbps   3m12s
```

Con `/interface wireless scan wlan1` se puede realizar un scaneo de los APs que hay alrededor utilizando la radio `wlan1`.

`scan`**Ejercicio 3.7**

WDS

`/interface wireless wds`

En este apartado se pueden definir enlaces WDS (*Wireless Distribution System*) entre routers de la red. WDS se utiliza para ampliar una red inalámbrica mediante múltiples puntos de acceso que, normalmente, comparten el mismo ESSID (es decir, que el tráfico entre celdas wifi en vez de ir por una red cableada también es inalámbrico). Sin embargo en guifi.net los enlaces WDS se utilizan para realizar los enlaces troncales punto a punto entre dos routers (aunque en ocasiones se enlazan más de dos routers):

```
[guest@CS-UJI-BiblAP] > /interface wireless wds print
Flags: X - disabled, R - running, D - dynamic
 0     name="wds_VRPlazaMajor10Rd2" mtu=1500 mac-
address=00:00:00:00:00:00 arp=enabled
       master-interface=wlan3 wds-address=00:0C:42:64:48:EE

 1  R  name="wds_CSCEFIRERd2" mtu=1500 mac-
address=00:0C:42:3A:55:0E arp=enabled
       master-interface=wlan4 wds-address=00:0C:42:62:06:C0

 2  R  name="wds_bncssmAPSantiago124MRd1" mtu=1500 mac-
address=00:0C:42:3A:55:0E
```

```
       arp=enabled master-interface=wlan4 wds-
address=00:0C:42:61:86:69
```

Los enlaces WDS se hacen utilizando la MAC del otro AP con el que se quiere conectar y utilizando en ambos APs el mismo canal. Como se ve en el ejemplo, cada enlace tiene una interfaz inalámbrica con la que se va a realizar el enlace y la `wds-address` (la MAC) del otro router. Los enlaces que se han establecido (R) tienen como `mac-address` la de la radio propia que establece el enlace, mientras que los enlaces que no se han establecido tienen una `mac-address` nula.

En `/interface wireless` también se pueden definir algunos parámetros sobre el enlace WDS, uno de ellos, `wds-ignore-ssid=yes` es muy importante si los APs gastan diferentes ESSID.

Otras opciones interesantes de este apartado:

```
add -- Create a new item
disable -- Disable items
enable -- Enable items
print -- Print values of item properties
remove -- Remove item
set -- Change item properties
```

Ejercicio 3.8

IP

`/ip`

En este apartado se puede configurar y consultar todo lo referente al nivel 3 del protocolo TCP/IP. A continuación se comentan algunas de las características más importantes.

Direcciones IP

`/ip address`

Este apartado permite configurar las direcciones IP de cada una de las interfaces de un router (http://wiki.mikrotik.com/wiki/Manual:IP/Address)

```
[admin@CS-UJI-BiblAP] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         BROADCAST       INTERFACE

 0   ;;; default configuration
     192.168.88.1/24    192.168.88.0    192.168.88.255  ether1

 1   10.228.130.33/27   10.228.130.32   10.228.130.63   wLan/Lan

 2   10.228.130.1/27    10.228.130.0    10.228.130.31   wlan2

 3   ;;; CSUJISolicomSrvr1
     10.228.130.161/29  10.228.130.160  10.228.130.167  ether2

 4 I ;;; wds_VRPlazaMajor10Rd2
```

```
     172.16.107.10/30   172.16.107.8    172.16.107.11
wds_VRPlazaMajor10Rd2
 5   ;;; wds_CSCEFIRERd2
     172.16.107.14/30   172.16.107.12   172.16.107.15
wds_CSCEFIRERd2
 6   ;;; Enlace UJI-Humanas
     172.16.107.138/30  172.16.107.136  172.16.107.139  ether2
```

Ejercicio 3.9

Cortafuegos

```
/ip firewall
```

En este apartado se pueden configurar el cortafuegos del router (http://wiki.mikrotik.com/wiki/Manual:IP/Firewall). Reglas de acceso, redirecionamiento de puertos, NAT, ...

```
address-list --
calea --
connection -- Active connections
filter -- Firewall filters
layer7-protocol --
mangle -- The packet marking management
nat -- Network Address Translation
service-port -- Service port management
```

El siguiente ejemplo muestra como filtrar tráfico p2p proveniente de unas determinadas IPs (10.228.146.130, un proxy y 10.228.146.66, un hotspot), permitir el tráfico dentro de guifi.net (10.0.0.0/8 y 172.0.0.0/8) y permitir cualquier tipo de tráfico provenient de una determinada IP y hacia ella, las 10.228.146.130, con lo que dicha IP tendrá acceso directo a Internet.

```
[admin@CullaVstbllAjnmtRd1] > /ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=drop p2p=all-p2p src-
address=10.228.146.130 out-interface=wLan/Lan

 1   chain=forward action=drop p2p=all-p2p src-
address=10.228.146.66 out-interface=wLan/Lan

 2   chain=forward action=accept src-address=10.0.0.0/8 dst-
address=10.0.0.0/8

 3   chain=forward action=accept src-address=172.0.0.0/8 dst-
address=172.0.0.0/8

 4   chain=forward action=accept src-address=10.228.146.130

 5   chain=forward action=accept dst-address=10.228.146.130

 6   chain=forward action=drop
```

Ejercicio 3.10 El siguiente ejemplo muestra cómo hacer NAT (utilizando source nat) de una red privada hacia guifi.net

```
[admin@CS-UJI-BiblAP] > /ip firewall nat print

Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat action=src-nat to-addresses=10.228.130.33 src-
address=192.168.0.0/16  dst-address=!192.168.0.0/16
```

Ejercicio 3.11

Rutas

```
/ip route print
```

En este apartado de puede configurar rutas estáticas y consultar la tabla de rutas que está utilizando el router (http://wiki.mikrotik.com/wiki/Manual:IP/Route)

En el siguiente ejemplo se muestran la tabla de rutas de un router. Se pueden ver que hay rutas «Conectadas» (C), son subredes en las que participa el router, rutas estáticas (S) y rutas que se han aprendido por OSPF (o).

```
[admin@CS-UJI-BiblAP] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY-STATE GATEWAY
DISTANCE INTERFACE
 0 ADo  10.228.33.0/27                     reachable
172.16.107.58     110      ether2
 1 ADC  10.228.130.0/27    10.228.130.1
0        wlan2
 2 ADC  10.228.130.32/27   10.228.130.33
0        wLan/Lan
 3 ADC  10.228.130.160/29  10.228.130.161
0        ether2
 4 ADo  10.228.130.177/32                  reachable
172.16.107.58     110      ether2
 5 A S  10.228.130.224/27                  reachable
172.16.107.41     1        wLan/Lan
 7 ADo  10.228.131.0/27                    reachable
172.16.107.58     110      ether2
 8 ADo  10.228.131.32/27                   reachable
172.16.107.58     110      ether2
 9 ADo  10.228.131.64/27                   reachable
172.16.107.58     110      ether2
...
```

Ejercicio 3.12Ejercicio 3.13

Otras opciones

Otras opciones interesantes de este apartado son

```
arp -- ARP entries management
dns -- DNS settings
hotspot -- HotSpot servers management
```

Logs y sniffer

Un *sniffer* o *husmeador* es una utilidad que permite capturar el tráfico que pasa por el router, por ello puede ayudar a detectar problemas de red. Del mismo modo los logs del sistema también son muy útiles en la detección de problemas ya que muestran información sobre las acciones que se han producido en el router: clientes que se han conectado/desconectado, información OSPF, ...

La orden `/log print` muestra los logs del sistema. en `/system logging` se puede definir qué acciones se quieren almacenar en los logs del sistema.

En `/tool sniffer` hay un sencillo sniffer.

Otros

Otras órdenes útiles son:

- `/password`: permite cambiar el password del usuario `admin`.
- `/ping`: realiza un ping a una IP determinada

```
/ping 10.228.166.1
```

```
/ping 10.228.166.1 src-address=10.228.130.1
```

- `/quit`: sale del terminal.

- `/snmp`: permite configurar el protocolo SNMP.
- `/system reboot`: reinicia el router.
- `/system ssh`: permite conectarse a otro router u ordenador utilizando ssh

```
/system ssh 10.228.181.130 user=root
```

- `/tool traceroute`: muestra los routers por los que se pasa para llegar a una determinada IP
- `/file`: contiene los ficheros del router.

Ejercicio 3.14`guest10.228.130.110.228.181.130`

```
site:guifi.net 172.16.107.54
```

hotspot

```
/ip hotspot
```

Permite definir un hotspot para dar acceso a portátiles y dispositivos móviles a guifi.net y/o internet (http://wiki.mikrotik.com/wiki/Manual:Hotspot_Introduction). Permite filtrar por MAC, dar acceso temporal, ...

```
/ip hotspot setup
```

Con esta orden se puede definir de un modo sencillo un hotspot indicando a

través de una serie de preguntas sus parámetros (http://wiki.mikrotik.com/wiki/Manual:IP/Hotspot#HotSpot_Setup)

Hay que configurar el DNS en algún ordenador al que haya acceso desde el router. Para permitir el acceso por MAC durante un determinado tiempo, de los modos de autenticación hay que activar el login por `http chap` y `Trial` simultáneamente.

En el modo `Trial` se indica el tiempo que se permite en la conexión y el tiempo que debe pasar hasta que esa MAC pueda disfrutar de nuevo de la conexión. No hay que activar la autenticación por MAC.

Si se quiere permitir que un ordenador pueda volver a entrar, se puede borrar su entrada en `/ip/hotspot/hosts`.

El usuario para la autenticación no hay que usarlo. En la página web que se ofrece cuando se entra si se activa el modo `Trial`, hay un enlace indicando que se puede entrar. Basta con pulsar ese enlace.

Los límites se aplican a un usuario que se crea en base a la MAC. El usuario que se haya indicado en el perfil del servidor no se usa.

La página web de login está en `/file/hotspot/login.html`.

Precauciones

Imposibilidad de acceder`wlan1wLan/lanpingssh...ether1trialsshwinbox`

`ether2ether3`

DNS Name

Al crear el hotspot pide este parámetro que es el nombre del router en el servidor de nombres. Si no se tiene acceso a un DNS lo mejor es poner un nombre (ya que obliga) y después modificarlo por la IP del router en el hotspot.

- ???quiere decir que se cambia el nombre que se haya puesto por la IP???

Modificar la página del login

Descargar con scp el fichero `/file/hotspot/login.html`

```
scp admin@10.228.131.142:hotspot/login.html .
```

modificarlo y volverlo a subir (si se pone alguna referencia a una imagen también hay que subirla).

```
scp login.html admin@10.228.131.142:hotspot/
```

Es recomendable hacer una copia del fichero antes de modificarlo.

DHCP

`/ip dhcp-server`

Permite definir un servidor DHCP. Como se ha comentado, se desaconseja su uso en guifi.net, pero puede ser útil para redes privadas (conectadas a guifi.net) o para los hotspots (http://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Server).

`/ip pool`

Permite definir rangos de IPs que utilizará el servidor DHCP (http://wiki.mikrotik.com/wiki/Manual:IP/Pools)

Puentes, VLANs

`/interface bridge`

Como se vio en el apartado del unsolclic un bridge permite interconectar varias interfaces (http://wiki.mikrotik.com/wiki/Manual:Interface/Bridge).

`/interface vlan`

De la wikipedia:

Una VLAN (acrónimo de Virtual LAN, 'Red de Área Local Virtual') es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local.

ACLs

`/interface wireless access-list print`

Permite restringir el acceso (por MAC, calidad de señal, ...) a los dispositivos que se quieren conectar al AP.

Túneles

De la wikipedia:

«Se conoce como túnel al efecto de la utilización de ciertos protocolos de red que encapsulan a otro protocolo. Así, el protocolo A es encapsulado dentro del protocolo B, de forma que el primero considera al segundo como si estuviera en el nivel de enlace de datos. La técnica de tunelizar se suele utilizar para trasportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría. Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.»

A efectos prácticos, un túnel permite crear un «enlace vitual» (cifrado o no) entre dos nodos, no necesariamente conectados directamente. Una vez creado el túnel los dos nodos disponen de un enlace directo a través de él.

Existen multitud de herramientas y protocolos para realizar túneles, RouterOs dispone de unos cuantos de ellos en el apartado `/interface`

```
eoip -- Ethernet over IP tunnel interface
ipip -- IP over IP tunnel interfaces
l2tp-client -- Layer Two Tunneling Protocol's client
l2tp-server -- Layer Two Tunneling Protocol's server
ovpn-client --
ovpn-server --
ppp-client -- PPP client
ppp-server -- PPP server
pppoe-client -- PPPoE client interfaces
```

```
pppoe-server -- PPPoE server
pptp-client -- PPTP client
pptp-server -- PPTP server
```

Enrutamiento: OSPF i BGP.

El enrutamiento dinámico se encuentra en el sistema RouterOS en el apartado `/routing`, soporta BGP, OSPF y RIP entre otros (http://wiki.mikrotik.com/wiki/Manual:Routing).

En Castellón guifi.net (a fecha de 22/6/2011) utiliza OSPF como protocolo de enrutamiento dinámico. Se puede acceder a la configuración del OSPF mediante `/routing ospf` (http://wiki.mikrotik.com/wiki/Manual:Routing/OSPF), las opciones que presenta son:

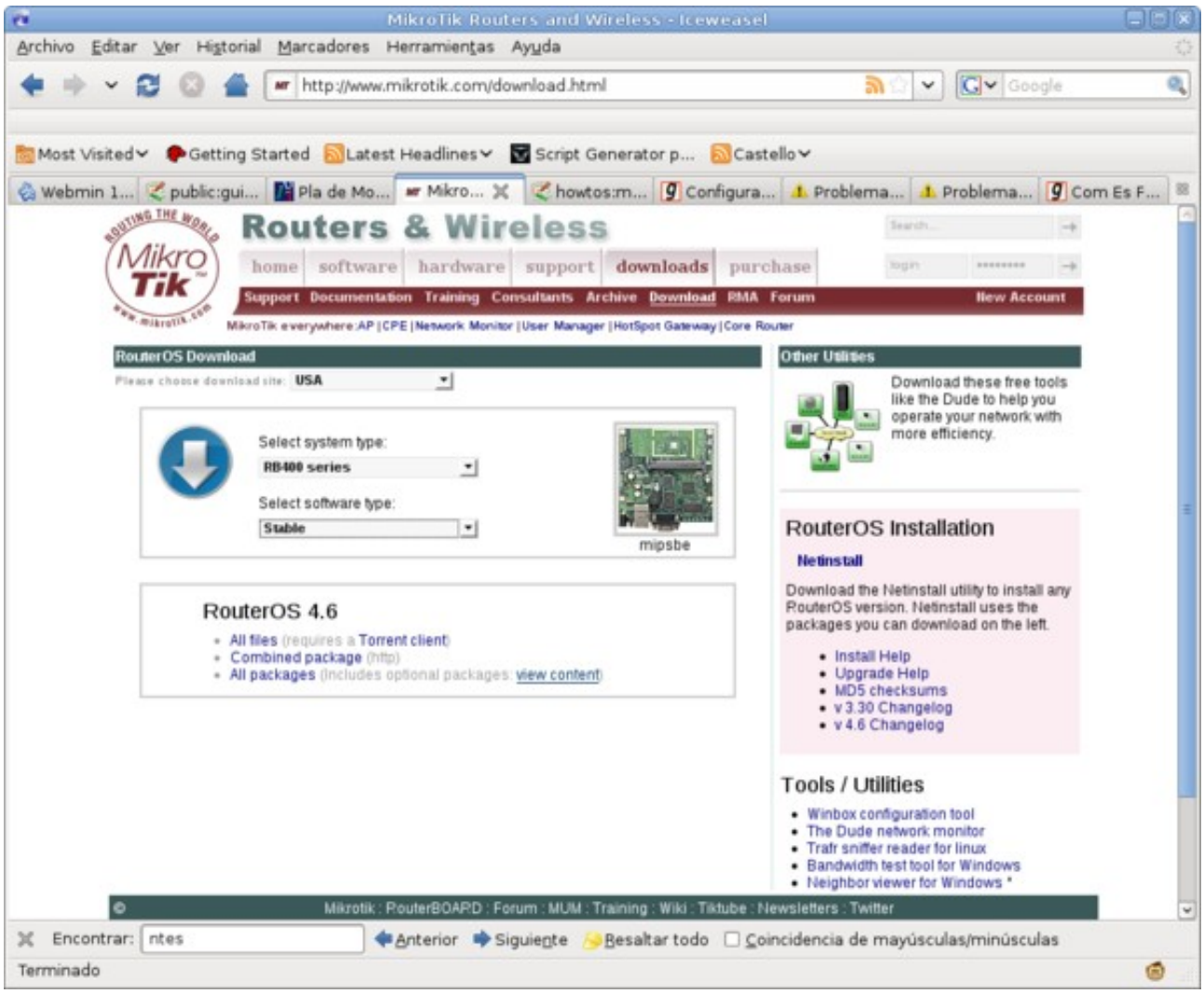
- `instance`: permite definir una instancia del protocolo OSPF con sus parámetros globales (qué rutas se intercambian, valor de las métricas administrativas, ...).
- `interface`: permite añadir y configurar las interfaces que se utilizarán para buscar vecinos OSPF.
- `nbma-neighbor`: para indicar vecinos que no están conectados por una red de difusión.

- `network`: permite definir qué subredes se publican a los vecinos.
- `route`: contiene las rutas que se han recibido por OSPF.

Mantenimineto del sistema

Actualización del sistema operativo

Acceder a http://www.mikrotik.com/download.html y seleccionar la plataforma y versión



Descargar el paquete «Combined package», y ponerlo en el apartado `files` del mikrotik y reiniciar el mikrotik.

Desde un ordenador conectado al mikrotik (debe estar en la misma red que el mikrotik, por ejemplo con la ip 192.168.88.100), hacer un `ftp` (o scp) para mandar el archivo:

```
coscollet:/home/mperez# ftp 192.168.88.1
Connected to 192.168.88.1.
220 MikroTik FTP server (MikroTik 3.31) ready
Name (192.168.88.1:root): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> pass
Passive mode on.
ftp> bin
200 Type set to I
ftp> put routeros-mipsbe-4.6.npk
local: routeros-mipsbe-4.6.npk remote: routeros-mipsbe-4.6.npk
200 PORT command successful
150 Opening BINARY mode data connection for '/routeros-mipsbe-
4.6.npk'
```

```
226 BINARY transfer complete
11437488 bytes sent in 30.28 secs (368.8 kB/s)
ftp> bye
coscollet:/home/mperez#
```

Acceder al mikrotik, comprobar antes que en `file` está el fichero y reincializar el router:

```
coscollet:/home/mperez# ssh admin@192.168.88.1
The authenticity of host '192.168.88.1 (192.168.88.1)' can't be
established.
DSA key fingerprint is
3d:5c:20:32:03:7c:cb:68:77:31:58:4f:c9:9a:ec:3f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.88.1' (DSA) to the list of
known hosts.

  MMM      MMM       KKK                          TTTTTTTTTTT
KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT
KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III
KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III
KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III
KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III
KKK  KKK

The following default configuration has been installed on your
router:
-------------------------------------------------------------------
-------------
IP address 192.168.88.1/24 is on ether1
ether1 is enabled

-------------------------------------------------------------------
-------------
You can type "v" to see the exact commands that are used to add
and remove
this default configuration, or you can view them later with
'/system default-configuration print' command.
To remove this default configuration type "r" or hit any other key
to continue.
If you are connected using the above IP and you remove it, you
will be disconnected.

Confirming configuration

[admin@MikroTik] > /file
[admin@MikroTik] /file> print
 # NAME               TYPE             SIZE
```

```
CREATION-TIME
 0 routeros-mipsb... package          11437488
jan/02/1970 00:04:56
[admin@MikroTik] /file> /system reboot
Reboot, yes? [y/N]:
y
system will reboot shortly
Connection to 192.168.88.1 closed by remote host.
Connection to 192.168.88.1 closed.
```

tras 3 ó 4 minutos el sistema se habrá reinicializado y actualizado.

Copias de seguridad y recuperación

`/export file=backup20110621.txt`

genera un fichero de texto con toda la configuración del sistema. El fichero se almacena en el apartado `/file` y se puede descargar por FTP o scp.

Ejercicio 3.15`export`

`/system backup save name=backup20110621`

genera un fichero binario con el nombre `backup20110621.backup` con toda la configuración del sistema. El fichero se almacena en el apartado `/file` y se puede descargar por FTP o scp.

`/system backup load name=backup20110621`

restaura la configuración almacenada en el fichero `backup20110621.backup` del apartado `/file`.

Enlaces

http://es.wikipedia.org/wiki/MikroTik

http://es.scribd.com/doc/16020012/Mikrotik-Tutorial, Proyecto final de carrera en el que se plantea un caso real y se explican mucha particularidades del sistema

http://www.mikrotikrouteros.com, Información variada en Español. Tiene definidas algunas configuraciones típicas que pueden ser interesantes

http://wiki.mikrotik.com/

http://wiki.mikrotik.com/wiki/MikroTik_RouterOS, Ejemplo de usuarios. Interesante.

http://forum.mikrotik.com/

Otros enlaces

http://www.zero13wireless.net/foro/showthread.php?6438-Introduccion-al-ROUTEROS-Mikrotik

http://www.taringa.net/posts/linux/1181328/Manual-Mikrotik-RouterOS-totalmente-en-Espanol_.html

Tracedump:

```
newBaseSize: 12pt
newBaseSizeInPt: 12
```