Redes Wireless y WDS con el HostAP

Ricardo Galli

Dpt. de Ciències Matemàtiques i Informàtica
Universitat de les Illes Balears

Temas

- Generalidades
  - Tarjetas
  - Seguridad y cifrado
  - wireless-tools: iwconfig
  - Configuración del kernel y PCMCIA
- Configuración de un Punto de Acceso
  - IP routing, NAT, *bridging*. Configuración de un *bridge*
- Que es el Sistema de Distribución
- WDS: encaminamiento IP, *bridging*
  - Configuración wds# manual y automático
- Consideraciones finales

DISCLAIMER

- Uso muchas palabras anglosajonas.
- Mi abuelo y un vecino eran radioaficionados, pero yo no tengo idea.
- Tampoco entiendo la UN-85.
- ¿No es una tontería estar montando APs con Linux con lo barato que están los AP?
- Cuestión de *hacking*, la historia se repite.

Por donde empezar

- Jean Tourrilhes

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/

- Ricardo Galli :-)

http://bulmalug.net/body.phtml?nIdNoticia=1309

http://bulmalug.net/body.phtml?nIdNoticia=1624

Tarjetas/drivers más comunes

- Hermes u orinoco_cs
- PrismII
  - Hostap: permite trabajar en modo AP
  - orinoco_cs
- Cisco Aironet
  - Módulo del kernel
  - Cisco (http://www.cisco.com/public/sw-center/sw-wireless.shtml)
- Airport

Modos

- Ad-hoc
- Infraestructura Básica (BSS)
  - *Master* o Punto de Acceso
  - Managed
- Infraestructura Extendida (ESS)
  - Múltiples Puntos de Acceso
  - *Roaming*

También lo sabéis, siguiente...

Tema del Cifrado

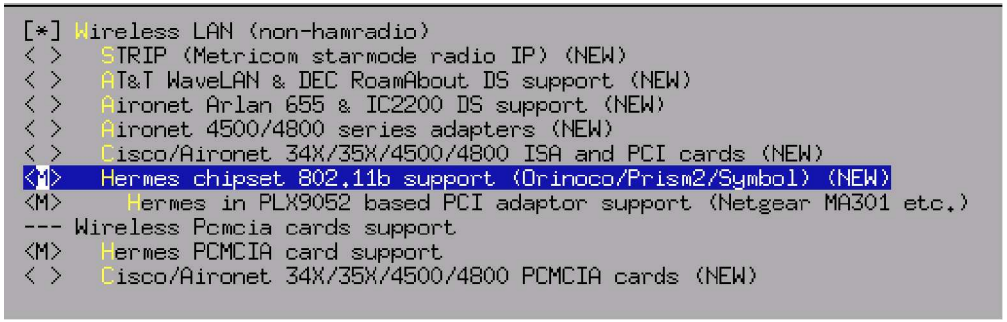
- Abierto. NO!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! ¿O sí?
- Cifrado: WEP
  - No es "muy" seguro, es relativamente sencillo de encontrar las claves, pero necesita bastante tráfico.
  - Es siempre mejor que no usar cifrado: los 2 excursionistas y el oso.
- Existen métodos propietarios, se están estudiando nuevos estándares.
- Considerar que están visibles en Internet.

iwconfig

- Identificador de red (*essid*)
- Frecuencia o canal (*freq/channel*)
- Modo (*mode: master|managed|ad-hoc*)
- Velocidad (*rate*)
- Clave de encriptación (*key*)
- Potencia de transmisión (*txpower*)
- etc.

Configuración del kernel

- Las PCMCIA
- Módulos de los dispositivos



Las PCMCIA

- Directorio /etc/pcmcia
- Modificar los *.opts
- cardctl ident

```
Socket 0:
  product info: "3Com", "3C574-TX Fast EtherLink PC Card", "A", "001"
  manfid: 0x0101, 0x0574
  function: 6 (network)
Socket 1:
  product info: "802.11", "11Mbps Wireless LAN Card", "v08C1", ""
  manfid: 0xc250, 0x0002
  function: 6 (network)
```

- /etc/pcmcia/config.opts

```
card "Conceptronic Wireless"
  version "802.11", "11Mbps Wireless LAN Card"
# mandi 0x0101, 0x0574
#  bind "orinoco_cs"
  bind "hostap_cs"
```

Configuración de PCMCIA (Debian)

- wireless.opt
- networks.opt
  - No dejar ningún "*,*,*,*)"

Todo se configura en /etc/network interfaces

/etc/network/interfaces (Debian)

```
auto eth1
# ejemplo con dhcp
iface eth1 inet dhcp
 #address 192.168.0.140
 #netmask 255.255.255.0
 #network 192.168.0.0
 #gateway 192.168.0.1
 wireless_essid Nombre_de_red
 wireless_mode Managed
 wireless_key s:mi_clave
 wireless_rate auto
 wireless_nick sofi
```

¿Y en RedHat?

- Cambiaron en las últimas versiones, antes era muy complicado
  - /etc/sysconfig/network-scripts/ifcfg-ethX

```
DEVICE=eth1
MODE=managed
ESSID="Nombre_de_red"
RATE=auto
TXPOWER=auto
KEY="s:mi_clave" # Solo si va encriptado
BOOTPROTO=static
IPADDR=192.168.0.3
BROADCAST=192.168.0.255
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
```

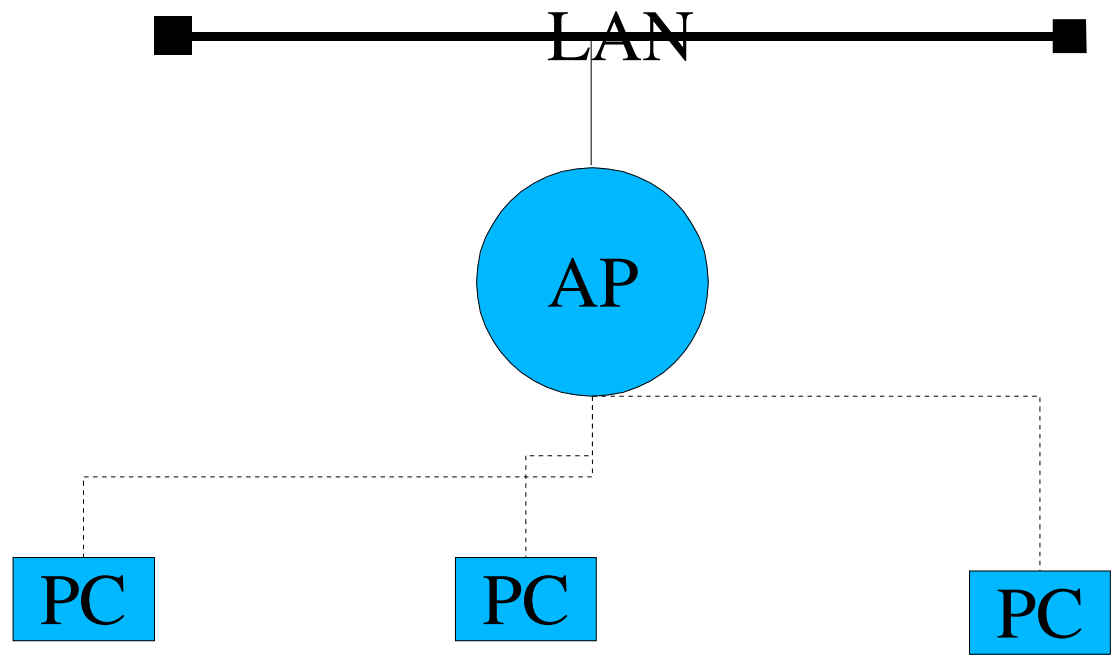
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/DISTRIBUTIONS.txt

Configuración de un Punto de Acceso: HostAP

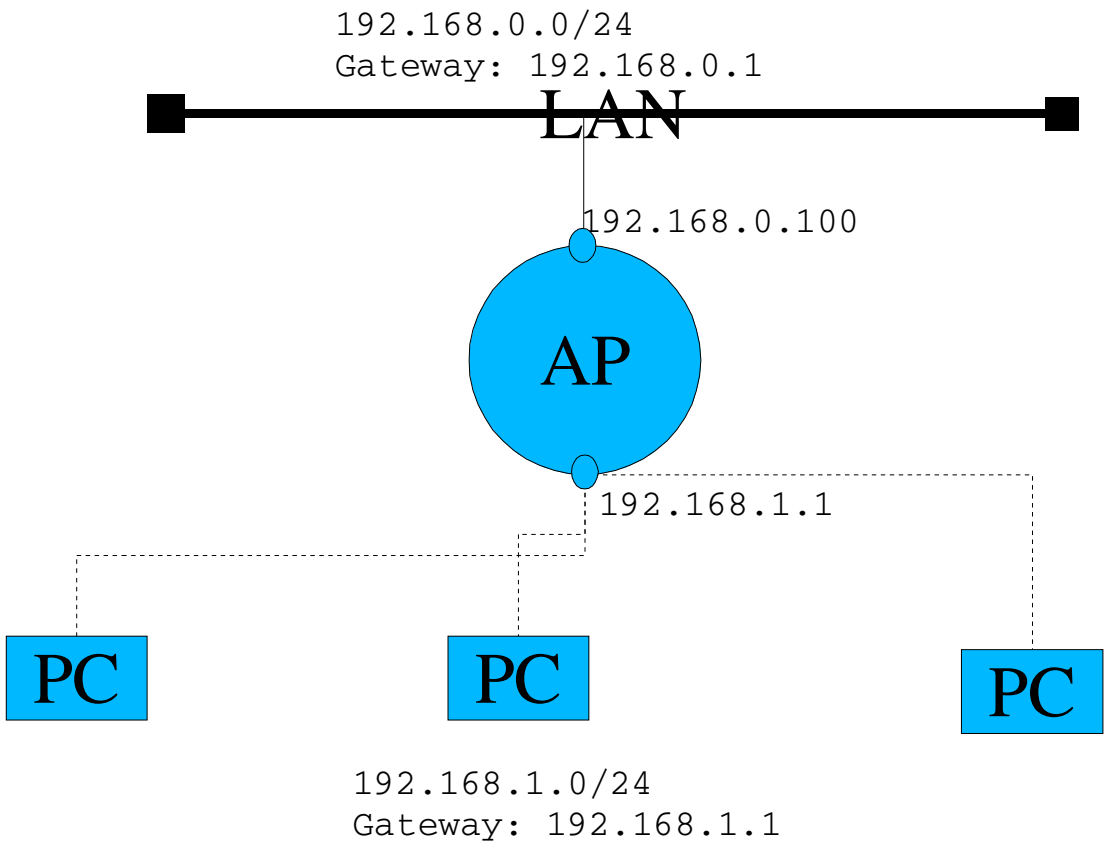
- Sólo con tarjetas del chipset PrismII: Conceptronics, Senao, D-Link 650...
- http://hostap.epitest.fi/
- Conocimientos mínimos de redes IP, DHCP, bridging, NAT.

Conectividad Wireles-LAN

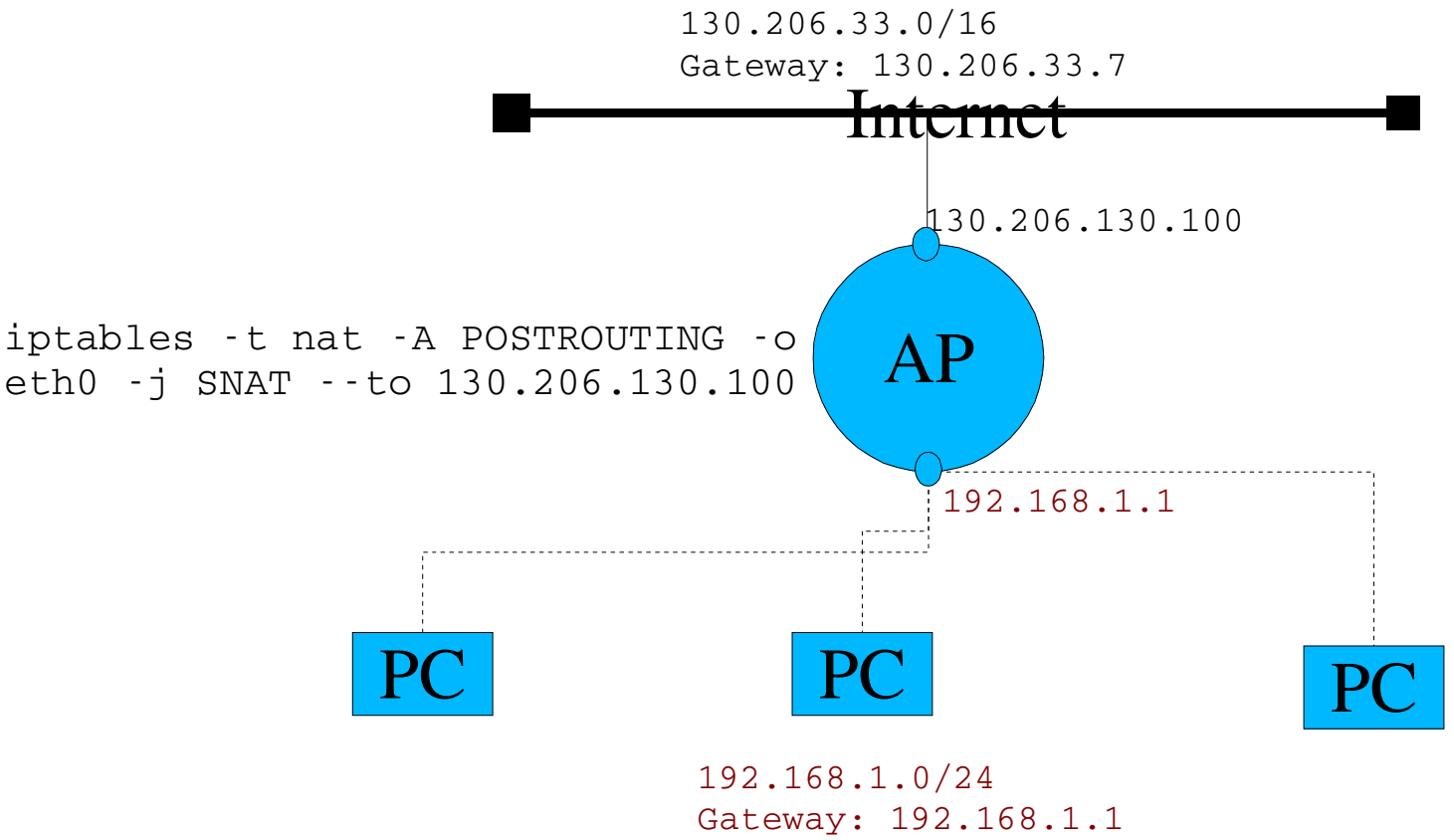
- IP routing
- Bridging
- NAT



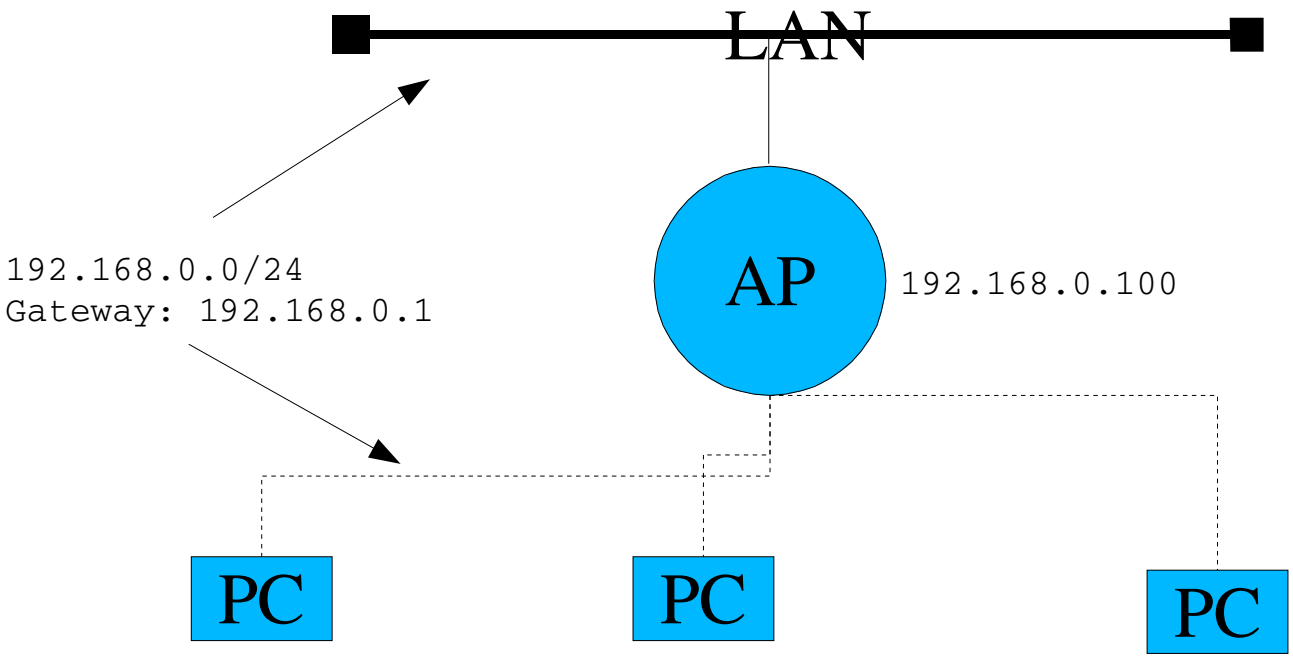
IP Routing


192.168.0.0/24
Gateway: 192.168.0.1
LAN
192.168.0.100
AP
192.168.1.1
PC
PC
PC
192.168.1.0/24
Gateway: 192.168.1.1

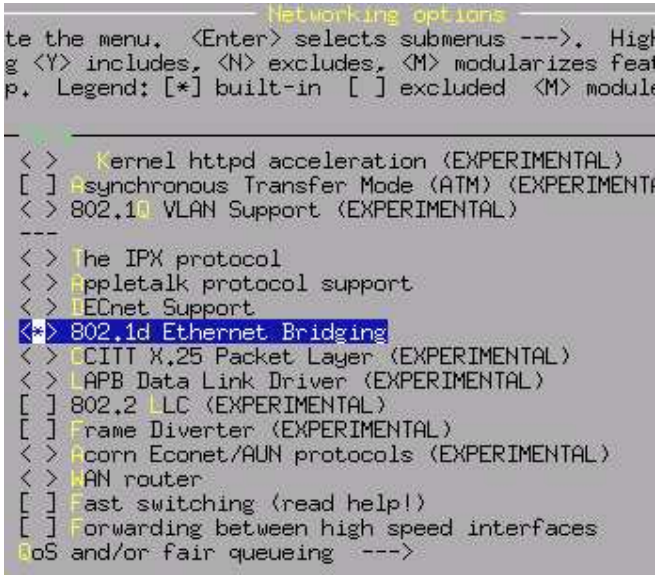
NAT


130.206.33.0/16
Gateway: 130.206.33.7
Internet
130.206.130.100
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 130.206.130.100
AP
192.168.1.1
PC
PC
PC
192.168.1.0/24
Gateway: 192.168.1.1

Bridging



Configuración del bridge




```
#/etc/network/interfaces
auto br0
iface br0 inet static
 address 192.168.0.10
 netmask 255.255.255.0
 network 192.168.0.0
 gateway 192.168.0.1
 bridge_ports eth0 wlan0
```

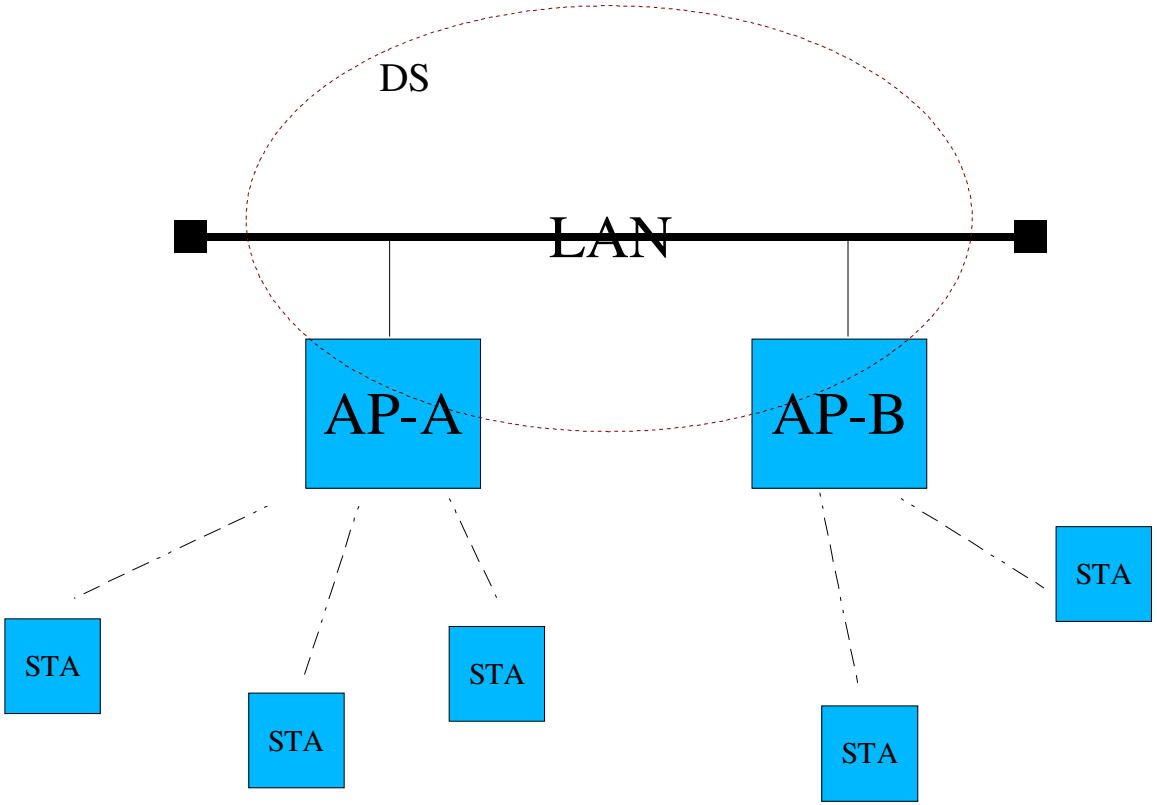
```
[root@ponti root]#
[root@ponti root]# brctl show br0
bridge name     bridge id               STP enabled     interfaces
br0             8000.0050c2019614       no              eth0
                                                        wlan0
[root@ponti root]#
[root@ponti root]#
[root@ponti root]#
[root@ponti root]# brctl showmacs  br0
port no mac addr                is local?       ageing timer
  1     00:04:76:26:96:c7       no                0.04
  2     00:30:65:1d:e6:3a       no              106.18
  1     00:40:43:05:66:00       no               98.57
  2     00:50:c2:01:93:66       no              135.38
  2     00:50:c2:01:96:14       yes               0.00
  1     00:50:da:b0:8a:d6       no              173.22
  1     00:60:08:b3:6c:b7       yes               0.00
[root@ponti root]#
[root@ponti root]#
[root@ponti root]#
New  Konsole  Shell  Shell No 2
```

Características adicionales del hostap

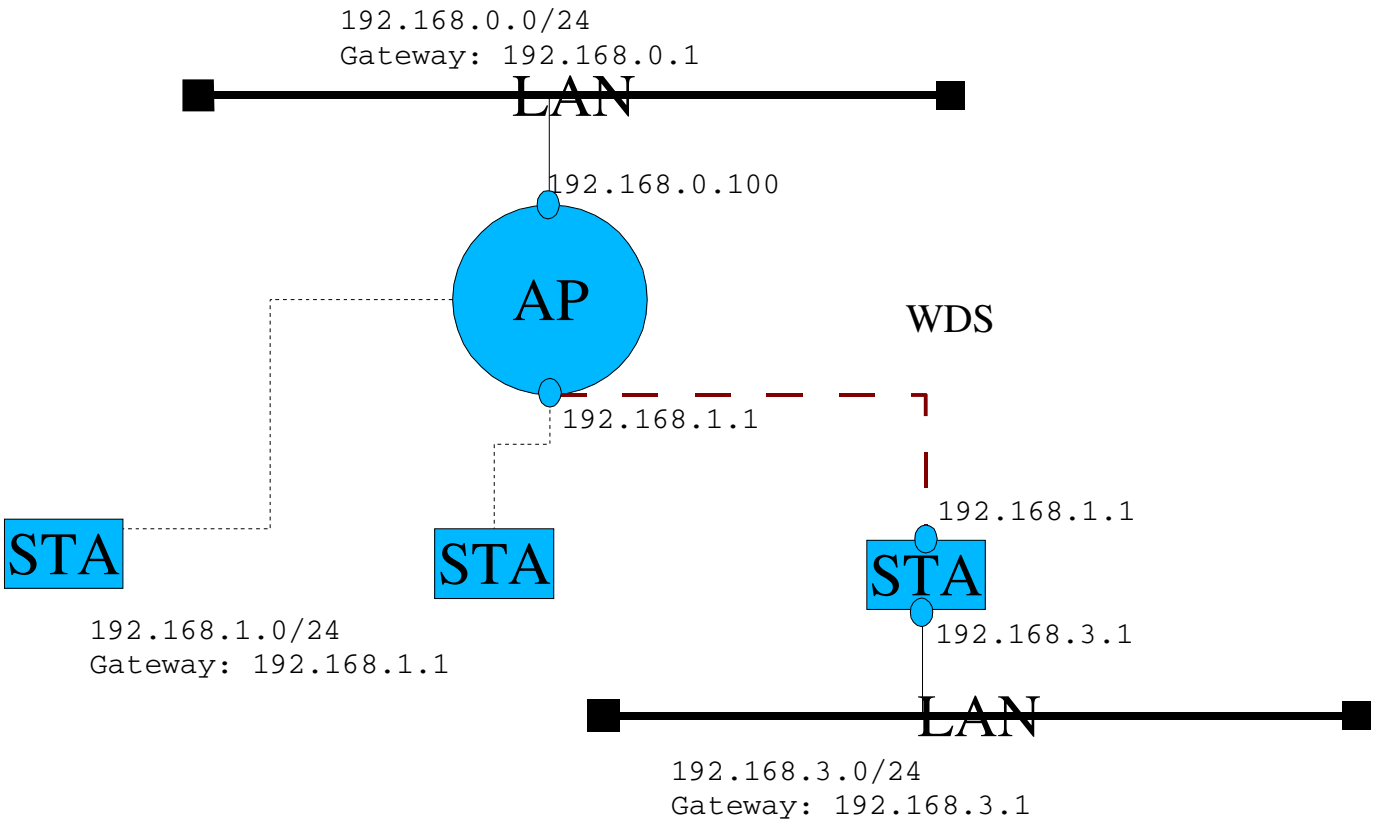
- Soporte de listas de acceso por MACs
- Soporte del WDS (wlan0wds0)
  - Bridiging entre varias LANs distintas
- Autentificación 802.1X-2001
- Monitorización de otros AP
  - Enlaces automáticos con wds#
- Monitorización de 802.11

Los niños llaman la atención

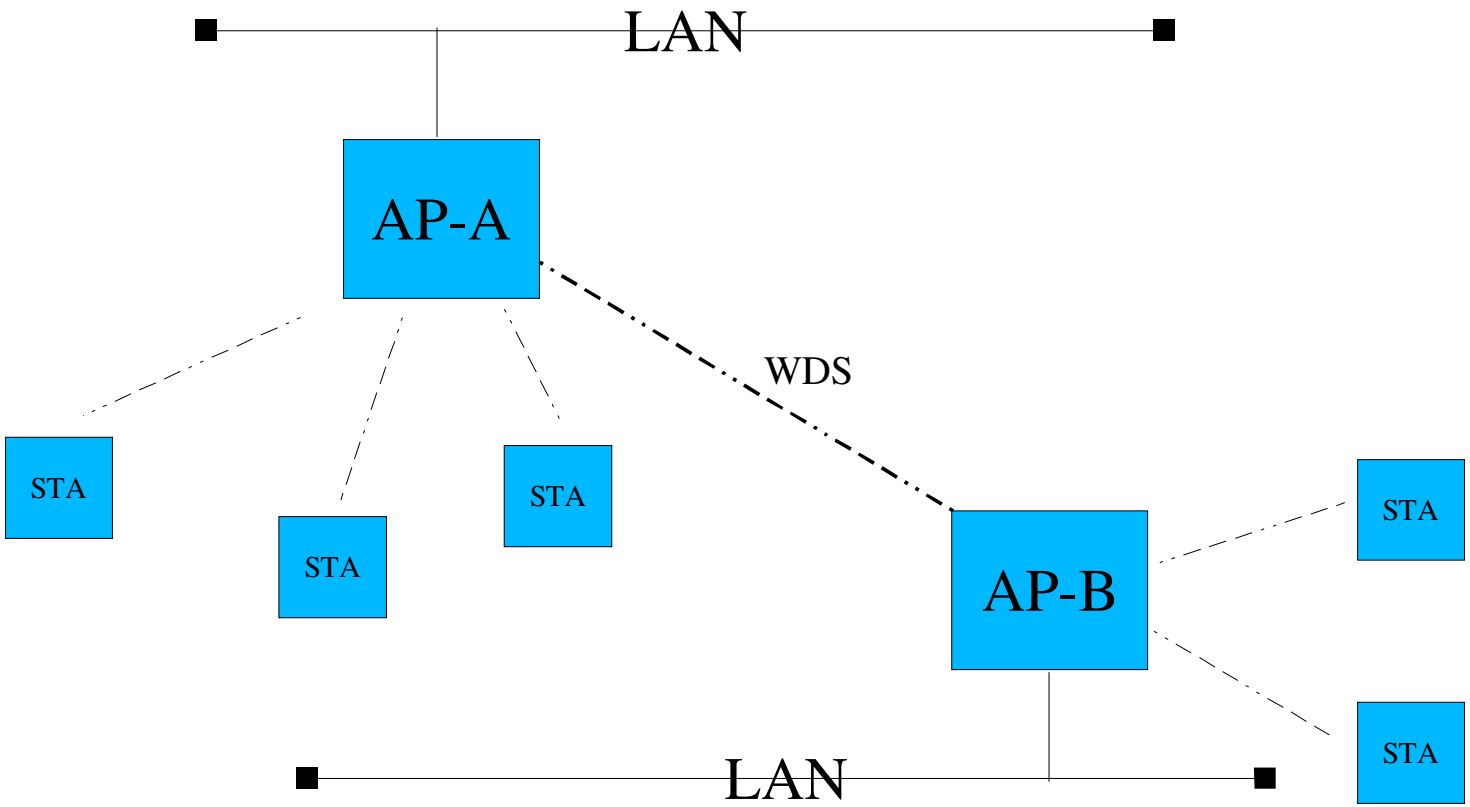
El Sistema de Distribución



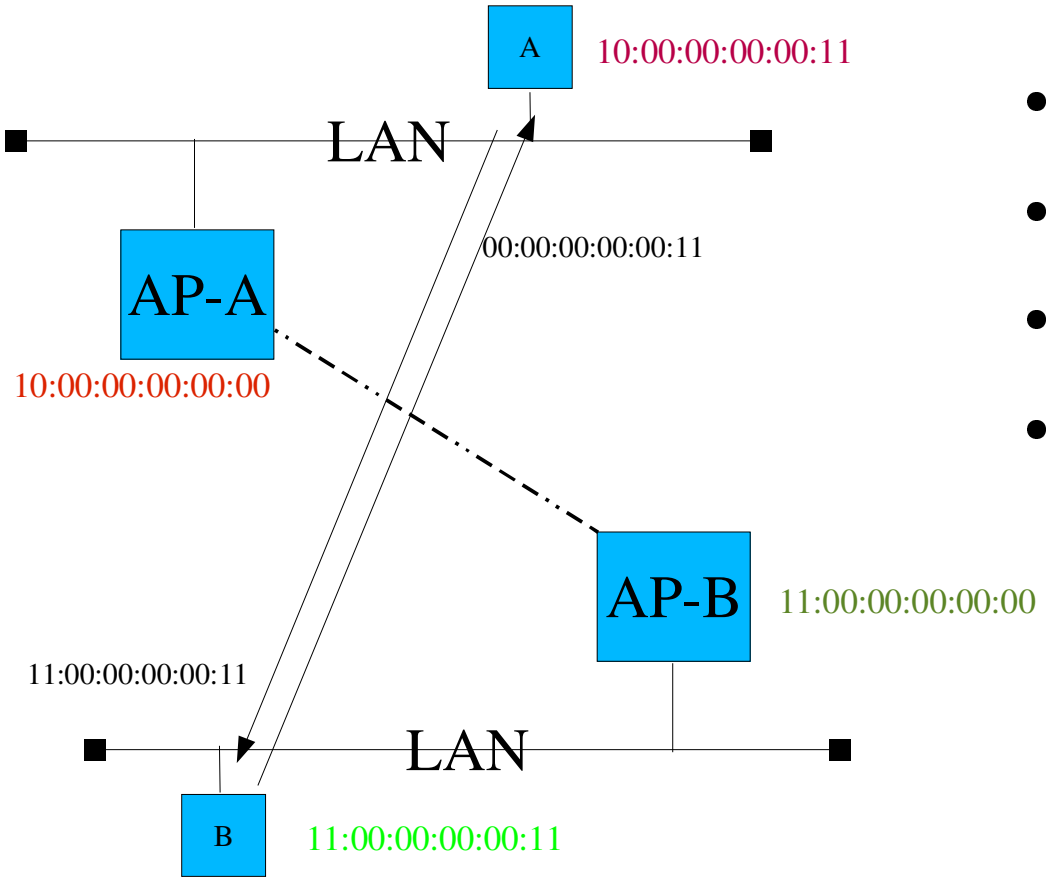
WDS con enrutado IP



Interconexión LAN con WDS



Bridging transparente



- RA: 11:00:00:00:00:00
- TA: 10:00:00:00:00:00
- DA: 11:00:00:00:00:11
- SA: 10:00:00:00:00:11

Enlace Manual

Configuración AP-A

```
iwpriv wlan0 wds_add 11:00:00:00:00:00
ifconfig wlan0wds0 0.0.0.0
brctl addif br0 wlan0wds0
```

Configuración AP-B

```
iwpriv wlan0 wds_add 10:00:00:00:00:00
ifconfig wlan0wds0 0.0.0.0
brctl addif br0 wlan0wds0
```

Enlace Automático

```
# la primera interfaz wds
iwpriv wlan0 wds_add 00:00:00:00:00:00
ifconfig wlan0wds0 0.0.0.0
brctl addif br0 wlan0wds0
# la segunda interfaz wds
iwpriv wlan0 wds_add 00:00:00:00:00:00
ifconfig wlan0wds1 0.0.0.0
brctl addif br0 wlan0wds1
# habilitamos en enlace automático
prism2_param wlan0 autom_ap_wds 1
prism2_param wlan0 other_ap_policy 1
# agregamos ambas interfaces al bridge
brctl addif br0 wlan0wds0
brctl addif br0 wlan0wds1
```

... wlan0: adding automatic WDS connection to AP 00:50:c2:01:96:14
... wlan0: using pre-allocated WDS netdevice wlan0wds0

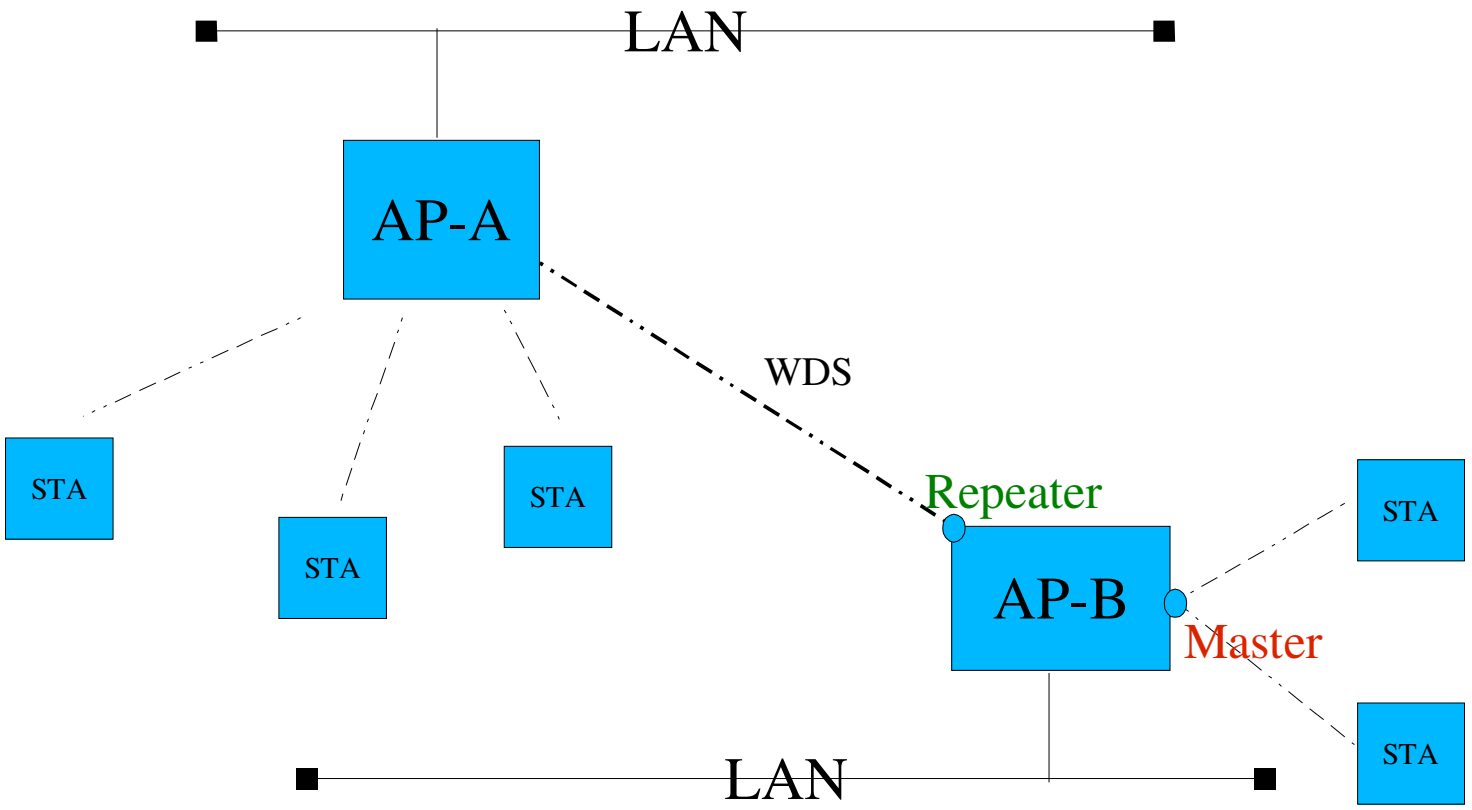
/etc/network/interfaces

```
auto br0
iface br0 inet static
    address 192.168.0.3
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
    gateway 192.168.0.1
    bridge_ports none
    bridge_stp on

iface eth0 inet static
    address 192.168.0.2
    netmask 255.255.255.0
    up /usr/sbin/brctl addif br0 eth0
```

```
Iface wlan0 inet static
    address 192.168.0.2
    netmask 255.255.255.0
    wireless_essid Antoli
    wireless_mode Master
    wireless_key s:poner_tu_clave
    wireless_channel 6
    up ifconfig wlan0 0.0.0.0
    up /usr/sbin/brctl addif br0 wlan0
    up iwpriv wlan0 wds_add 00:00:00:00:00:00
    up ifconfig wlan0wds0 0.0.0.0
    up prism2_param wlan0 autom_ap_wds 1
    up prism2_param wlan0 other_ap_policy 1
    up /usr/sbin/brctl addif br0 wlan0wds0
    down ifconfig wlan0wds0 down
```

Configuración ideal con *Repeater*



Consideraciones finales

- En modo bridging de dos *Master* se tiene que usar el mismo canal.
- A poca distancia hay muchas interferencias.
- Problema del *hidden-node*.
- Hay problemas para enlazar un *Master* y un *Repeater*.
- En versiones anteriores al 1.5 del firmware, no son compatibles con el estándar. Las nuevas sí.

Preguntas...

http://hostap.epitest.fi/

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/DISTRIBUTIONS.txt

http://bulmalug.net/body.phtml?nIdNoticia=1309

http://bulmalug.net/body.phtml?nIdNoticia=1624