

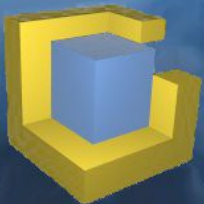


# Redes Wireless bajo Linux



**Centrologic**  
Computational Logistic Center

Ponente: Juan Miguel Taboada Godoy  
[juanmi@centrologic.com](mailto:juanmi@centrologic.com) - <http://www.centrologic.com>





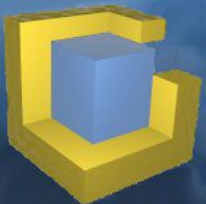
Teoría de redes

Configuración de dispositivos

Asalto y Hackers

Seguridad y protección

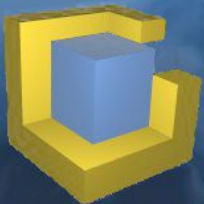
Ingeniería con LinuxAP





# Teoría de Redes

Esquema general  
Dirección IP  
Dirección MAC





## - Esquema General -

### Pesonas:

Nombre  
(Ej: Miguel)

Apellidos  
(Ej: de Cervantes y Saavedra)

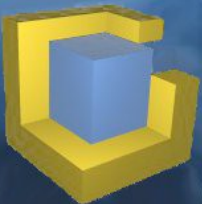
DNI  
(Ej: 12345678-Z)

### Redes:

Nombre de dominio  
(Ej: [www.globatic.com](http://www.globatic.com))

Dirección IP  
(Ej: 212.34.140.103)

Dirección MAC  
(Ej: AC:00:31:46:D3:4E)

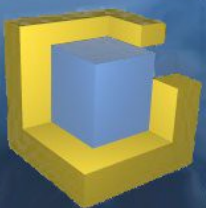




## - Dirección IP -

### Características:

- Única en la red
- Dirección de red: x.y.z.0
- Dirección de broadcast: x.y.z.255
- Máscara de red
- Puerta de enlace
- Ejemplo:  
IP: 192.168.1.254  
Máscara: 255.255.255.0

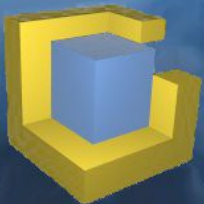
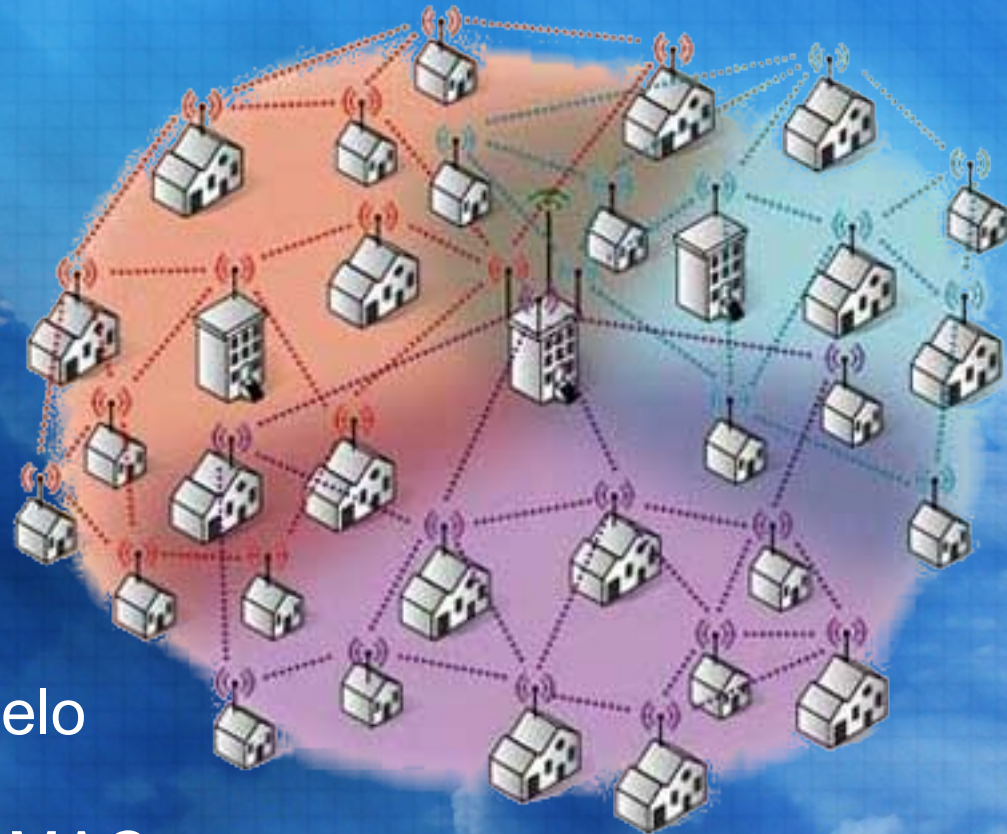




## - Dirección MAC -

### Características:

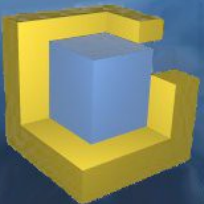
- Única “en el mundo”
- Establecida a nivel físico
- Identifica al fabricante y modelo
- Tabla ARP: relaciona IP con MAC
- Ejemplo: 00:92:3E:DF:24:11





# Configuración de dispositivos

Configurando el hardware  
Configuración física  
Configuración lógica  
El módulo hostap



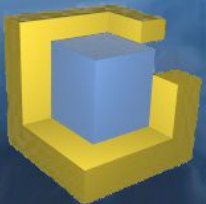
- Configurando el hardware -

¿Está soportada en Linux?

¿Recompilar el Kernel?

Cargar módulos (opcional)

Comprobar con ndiswrapper





## - Configuración física -

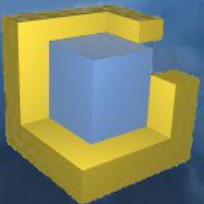


### Obtención de datos:

- ESSID
- Canal
- WEP
- WPA

### Wireless-tools (iwconfig):

- iwconfig wlan0 essid any
- iwconfig wlan0 channel 7
- iwconfig wlan0 key "clave\_wep"





## - Configuración lógica -



### Obtención de datos:

- IP
- Máscara
- Puerta de enlace
- DNS

### Route:

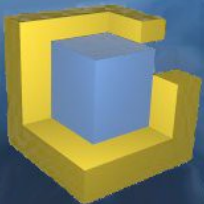
- route del default
- route -n
- route add default gw 192.168.1.254

### Ifconfig:

- ifconfig wlan0 up/down
- ifconfig wlan0 192.168.1.32
- ifconfig wlan0 netmask 255.255.255.240

### resolv.conf:

- vi /etc/resolv.conf





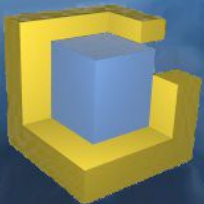
## - El módulo HostAP -

### Efectos:

- Comportamiento como cliente
- Comportamiento como AP
- Modo WDS soportado (cliente-AP)

### Características:

- Sólo chipset PRISM (todas las gamas)
- WEP, WPA y WPA2
- ACL (Listas de acceso)
- Roaming
- Usado por LinuxAP



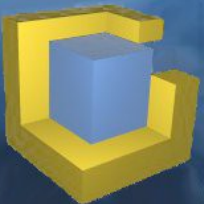


## - El módulo HostAP -

### Proceso para usarlo:

- 1) Creamos los módulos (make)
- 2) Instalamos los módulos (make install)
- 3) Cargamos los módulos:
  - modprobe hostap
  - hostap\_cs: tarjetas PCMCIA
  - hostap\_pci: tarjetas PCI
  - hostap\_plx: adaptadores PLX pci-pcmcia
  - hostpa\_crypt: módulos de encriptación

Soporte normal en Debian: /etc/networks/interfaces





Tira cómica gracias a:

**es.comp.os.linux.\***

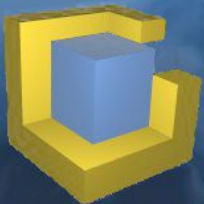


<Pausa>



# Asalto y Hackers

Conexión inalámbrica  
Control del tráfico

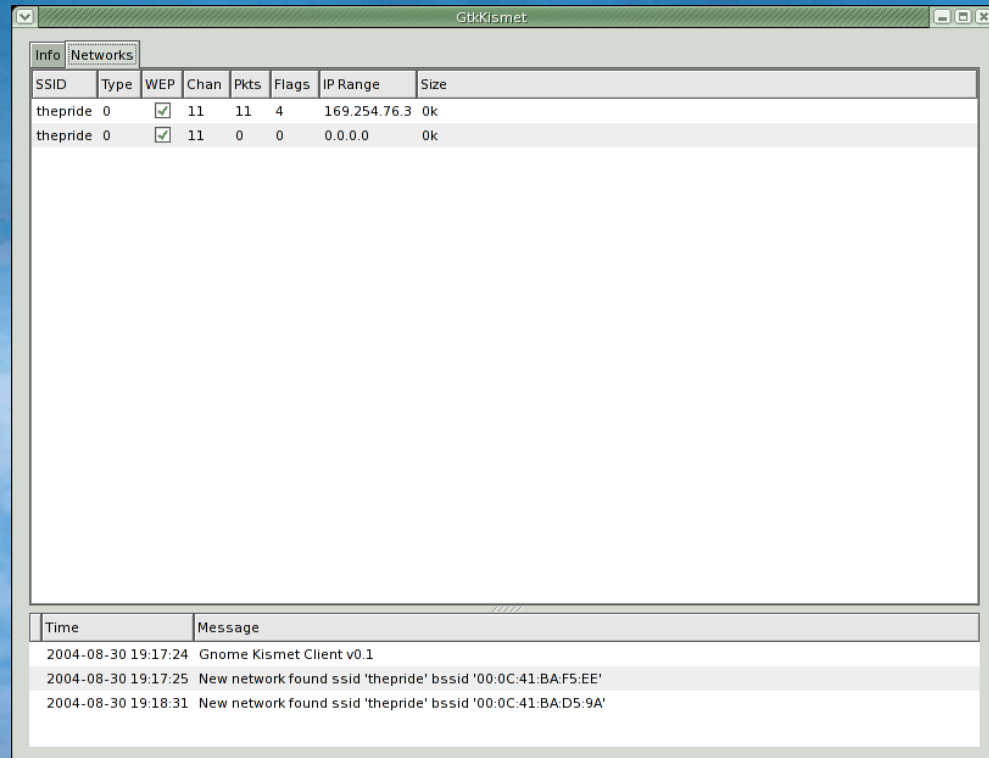




## - Conexión inalámbrica -

Wavemon

Kismet



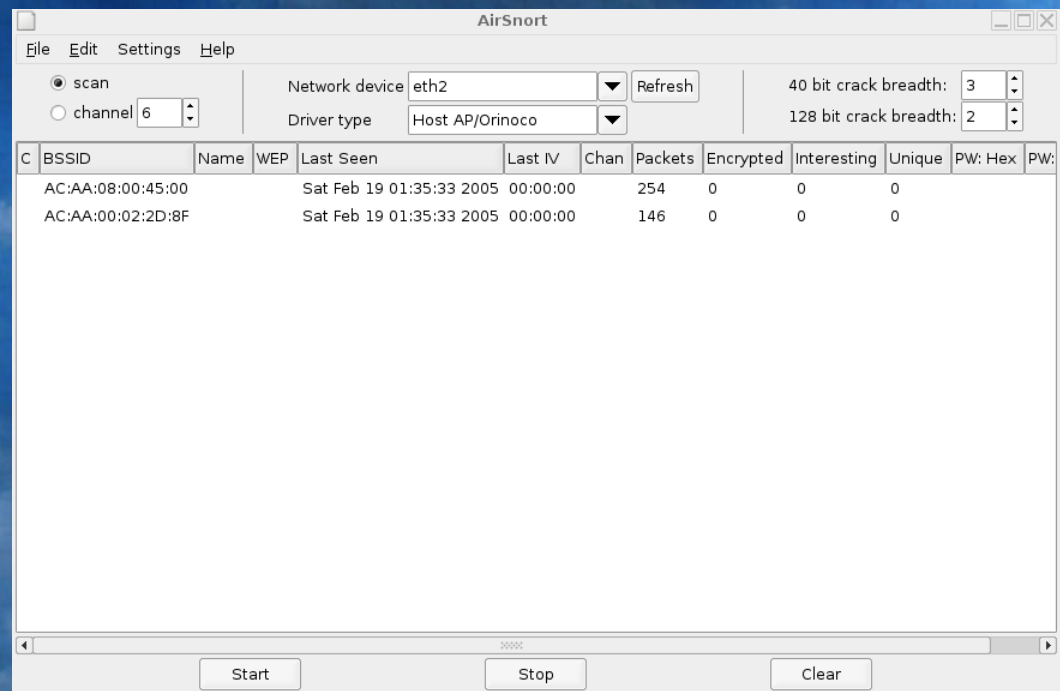
GBKismet

SSID	Type	WEP	Chan	Pkts	Flags	IP Range	Size
thepride	0	<input checked="" type="checkbox"/>	11	11	4	169.254.76.3	0k
thepride	0	<input checked="" type="checkbox"/>	11	0	0	0.0.0.0	0k

Time	Message
2004-08-30 19:17:24	Gnome Kismet Client v0.1
2004-08-30 19:17:25	New network found ssid 'thepride' bssid '00:0C:41:BAF5:EE'
2004-08-30 19:18:31	New network found ssid 'thepride' bssid '00:0C:41:BAD5:9A'

```

Interface
eth2 (IEEE 802.11-DS), ESSID: "www.globatic.com", nick: "HERMES I"
Levels
link quality: 68/92
=====
signal level: -28 dBm (1.58 uW)
=====
noise level: -96 dBm (0.00 uW)
=====
signal-to-noise ratio: +68 dB
=====
Statistics
RX: 246761 (284322590), TX: 154237 (23917564), inv: 0 nwid, 0 key, 64 misc
Info
frequency: 2.4420 GHz, sensitivity: 1/3, TX power: 15 dBm (31.62 mW)
mode: managed, access point: 00:12:17:C4:FF:82
bitrate: 11 Mbit/s, RTS thr: off, frag thr: off
encryption: n/a
power management: off
Network
if: eth2, hwaddr: 00:02:2D:8F:9B:26
addr: 192.68.0.1, netmask: 255.255.255.0, bcast: 192.68.0.255
    
```



AirSnort

File Edit Settings Help

☒ scan ☐ channel 6

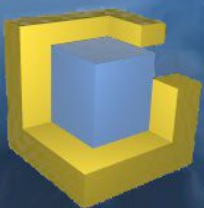
Network device: eth2  Driver type: Host AP/Orinoco

40 bit crack breadth: 3 128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW:
	AC:AA:08:00:45:00			Sat Feb 19 01:35:33 2005	00:00:00		254	0	0	0		
	AC:AA:00:02:2D:8F			Sat Feb 19 01:35:33 2005	00:00:00		146	0	0	0		

Start Stop Clear

AirSnort





## - Control del tráfico -

```
root@Naru: /root
Archivo  Editor  Ver  Terminal  Solapas  Ayuda
ck=280 Win=1448 Len=877 TSV=979259317 TSER=41709326
5.284820 192.68.0.1 -> 192.68.0.10 TCP 48244 > 5901 [ACK] Seq=280 Ack=17317
7 Win=18824 Len=0 TSV=41709348 TSER=979259308
5.285521 192.68.0.1 -> 192.68.0.10 TCP 48244 > 5901 [PSH, ACK] Seq=280 Ack=
173177 Win=18824 Len=10 TSV=41709349 TSER=979259308
5.290879 192.68.0.10 -> 192.68.0.1 TCP 5901 > 48244 [ACK] Seq=173177 Ack=29
0 Win=1448 Len=0 TSV=979259340 TSER=41709349
5.361256 192.68.0.10 -> 192.68.0.1 TCP 5901 > 48244 [ACK] Seq=173177 Ack=29
0 Win=1448 Len=1448 TSV=979259408 TSER=41709349
5.362949 192.68.0.10 -> 192.68.0.1 TCP 5901 > 48244 [ACK] Seq=179691 Ack=30
0 Win=1448 Len=1448 TSV=979259408 TSER=41709349
5.362987 192.68.0.1 -> 192.68.0.10 TCP 48244 > 5901 [ACK] Seq=300 Ack=18113
3 Win=18824 Len=0 TSV=41709427 TSER=979259408
5.874441 192.68.0.10 -> 192.68.0.1 TCP 5901 > 48244 [ACK] Seq=181130 Ack=29
0 Win=1448 Len=1448 TSV=979259918 TSER=41709432
5.876092 192.68.0.10 -> 192.68.0.1 TCP 5901 > 48244 [ACK] Seq=181130 Ack=29
5.876132 192.68.0.1 -> 192.68.0.1 TCP 5901 > 48244 [ACK] Seq=181130 Ack=29
5 Win=18824 Len=0 TSV=41709940 TSV=41710000 TSER=41710000
5.879797 192.68.0.1 -> 192.68.0.10 TCP 48244 > 5901 [ACK] Seq=181130 Ack=29
194813 Win=18824 Len=10 TSV=41710044 TSER=97926000
5.984468 192.68.0.10 -> 192.68.0.1 TCP 5901 > 48244 [ACK] Seq=181130 Ack=29
0 Win=1448 Len=0 TSV=979260033 TSER=41710044
```

tetherreal

iptraf

IPtraf		Nmap run completed -- 1 IP address (1 host up) scanned in 32				
Statistics for		root@Naru:~ #				
	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
Total:	1208	808203	768	776895	440	31308
IP:	1208	791291	768	766143	440	25148
TCP:	1191	788887	751	763739	440	25148
UDP:	18	3904	18	3904	0	0
ICMP:	0	0	0	0	0	0
Other IP:	0	0	0	0	0	0
Non-IP:	0	0	0	0	0	0
Total rates:		26.1 kbytes/sec	Broadcast packets:		8	
		41.8 packets/sec	Broadcast bytes:		810	
Incoming rates:		24.9 kbytes/sec	IP checksum errors: 0			
		26.2 packets/sec				
Outgoing rates:		1.2 kbytes/sec				
		15.6 packets/sec				

Ethereal: Capture - Interface eth	
Captured Packets	
Total	629
SCTP	0
TCP	612
UDP	16
ICMP	0
ARP	1
OSPF	0
GRE	0
NetBIOS	0
IPX	0
VINES	0
Other	0
Running	00:00:15
[X] Detener	

The Ethernet Network Analyzer					
File Edit View Go Capture Analyze Statistics Help					
Filter: [ ] Expression... Limpia Aplicar					
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [ACK]
2	0.000769	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [PSH]
3	0.000788	192.68.0.1	192.68.0.10	TCP	48244 > 5901 [ACK]
4	0.001097	192.68.0.1	192.68.0.10	TCP	48244 > 5901 [PSH]
5	0.003423	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [ACK]
6	0.103960	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [ACK]
7	0.105771	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [ACK]
8	0.105926	192.68.0.1	192.68.0.10	TCP	48244 > 5901 [ACK]
9	0.105904	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [PSH]
10	0.106229	192.68.0.1	192.68.0.10	TCP	48244 > 5901 [PSH]
11	0.108503	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [ACK]
12	0.509189	192.68.0.10	192.68.0.1	TCP	5901 > 48244 [ACK]
1 (1514 bytes on wire, 1514 bytes captured)					
et II, Src: 00:01:02:6a:ac:aa, Dst: 00:02:2d:8f:9b:26					
et Protocol, Src Addr: 192.68.0.10 (192.68.0.10), Dst Addr: 192.68.0.1 (192.68.0.1)					
02 2d 8f 9b 26 00 01 02 6a ac aa 08 00 45 00 ...&...j....E					
dc 5f 83 40 00 40 06 55 05 c0 44 00 0a c0 44 ...@.@.U...D					
01 17 0d bc 74 1f 43 c6 11 e7 de e6 0b 80 10 ....t.C.....					
a8 d4 64 00 00 01 01 08 0a 3a 5c bc 00 02 7a ...d....z					
capture P: 629 D: 629 M: 0					

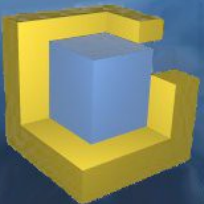
ethereal





# Seguridad y protección

Prevención  
Mantenimiento





## - Prevención -

iptables: protege de posibles olvidos

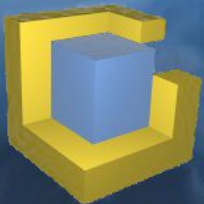
tbfirewall: front-end para iptables (tablas de reglas)

DMZ: Desmilitarized Zone

SSL: usar servicios que soporte conexiones SSL

Túneles seguros: entre máquinas lejanas y distintas redes

Radius: autenticación para acceso a la red





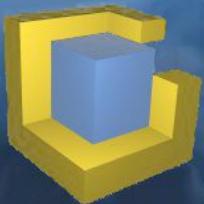
## - Prevención -

iptables: protege de posibles olvidos

```
iptables -A INPUT -s 192.168.1.2 -j DROP
iptables -A INPUT -s 80.28.98.53 -d 150.214.40.3 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 8080 -j DROP
iptables -A PREROUTING -s 192.168.1.0/24 -j MASQUERADE
```

tbfirewall: front-end para iptables (tablas de reglas)

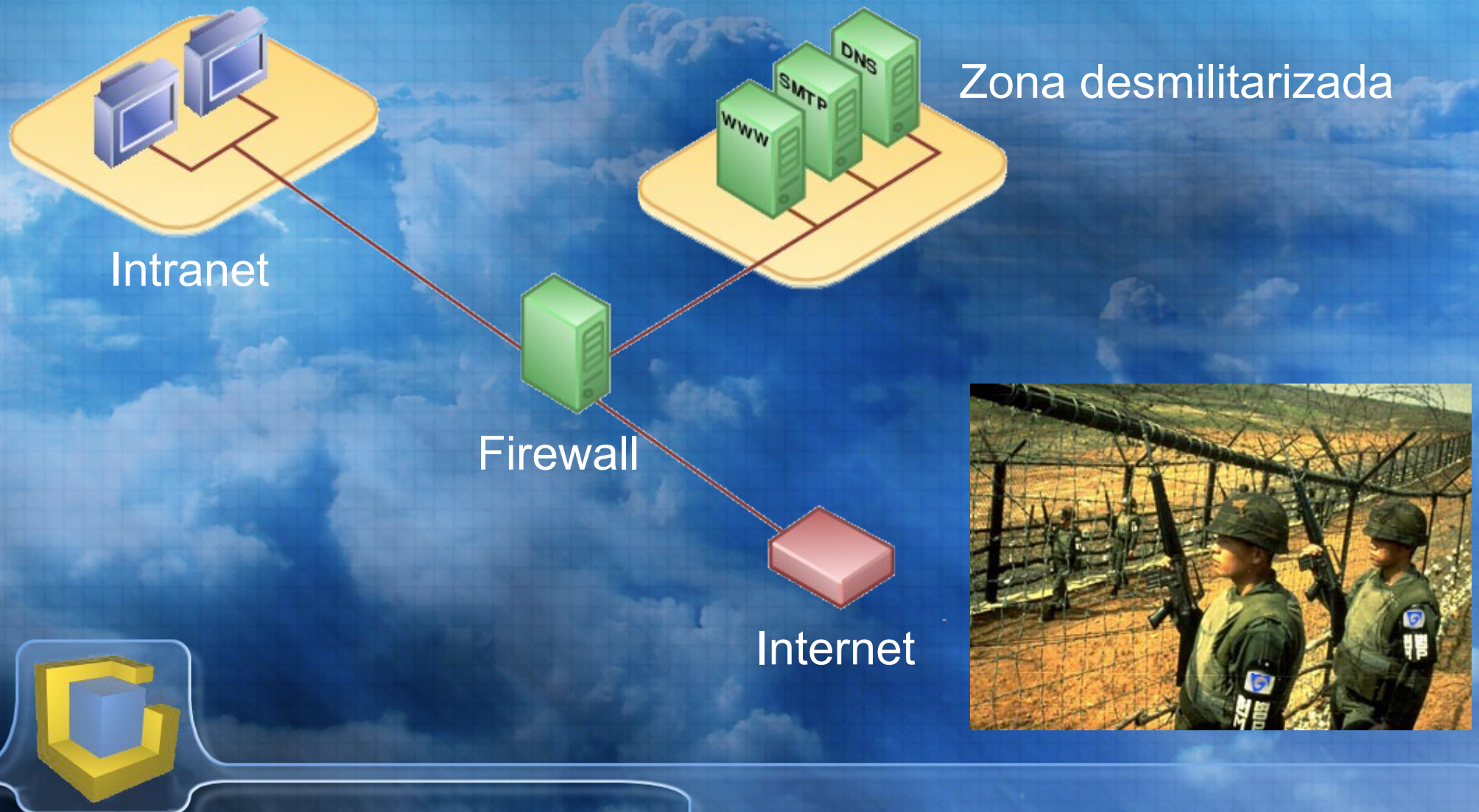
```
eth0 icmp 0 3 8 11
eth0 tcp auth ssh ftp ftp-data microsoft-ds
eth0 udp ssh microsoft-ds
eth0 tcp netbios-ns netbios-dgm netbios-ssn
eth0 udp netbios-ns netbios-dgm netbios-ssh
```





## - Prevención -

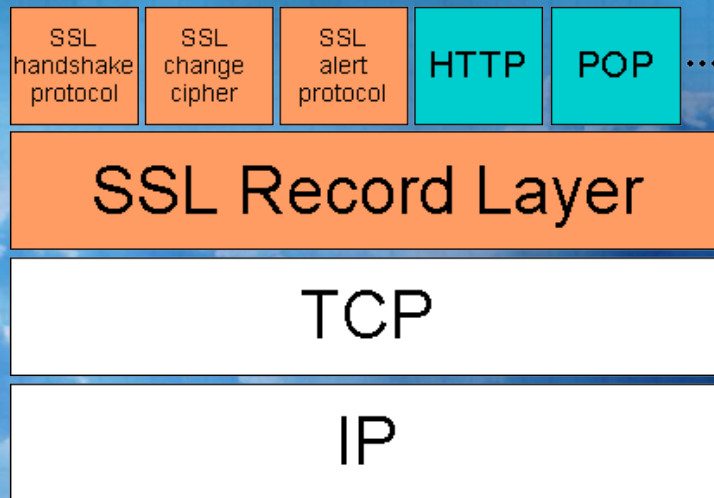
DMZ: Desmilitarized Zone (Zona Desmilitarizada)



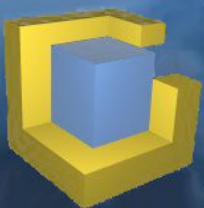
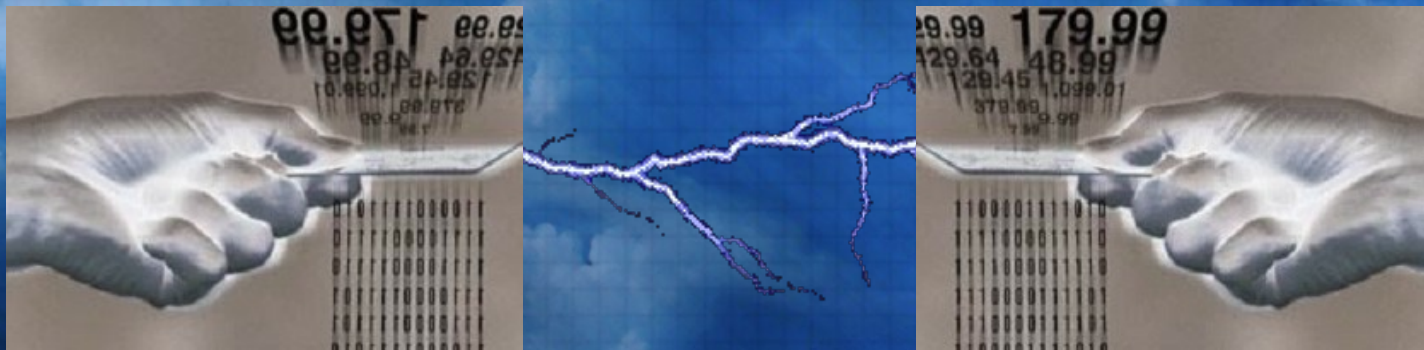


## - Prevención -

SSL: usar servicios que soporte conexiones SSL



Túneles seguros: entre máquinas lejanas y distintas redes

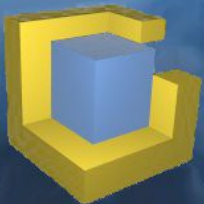
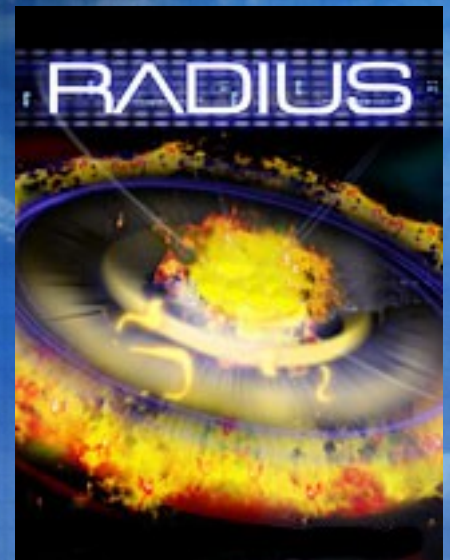




## - Prevención -

Radius: autenticación para acceso a la red

- 1) Intento de acceso a la red
- 2) Pantalla de autenticación
- 3) Envío de datos de autentiación
- 4) Comprobación de credenciales
- 5) Creación de reglas de acceso
- 6) Acceso a la red





## - Mantenimiento -

### chkrootkit

```
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for Optickit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for LOC rootkit ... nothing found
Searching for Romanian rootkit ... nothing found
Searching for Suckit rootkit ... nothing found
Searching for Volc rootkit ... nothing found
Searching for Gold2 rootkit ... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... You have 50 process hidden for readdir command
You have 50 process hidden for ps command
Warning: Possible LKM Trojan installed
Checking `rexedcs'... not found
Checking `sniffer'... lo: not promisc and no packet sniffer sock
eth0: not promisc and no packet sniffer sockets
Checking `w55808'... not infected
Checking `wted'... nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... nothing deleted
root@Naru:~ #
```

- 1) apt-get update/upgrade
- 2) chkrootkit
- 3) nmap localhost
- 4) John the Ripper
- 5) Cisilia

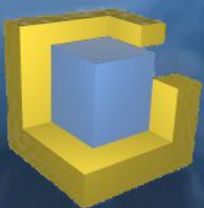
john

```
root@Naru:/etc # john -users:topo shadow
Loaded 1 password (FreeBSD MD5 [32/32])
glob (topo)
guesses: 1 time: 0:00:02:22 (3) c/s: 5159 trying: glob
root@Naru:/etc # john -users:topo shadow
Loaded 0 passwords, exiting...
root@Naru:/etc # john -users:topo shadow
Loaded 0 passwords, exiting...
root@Naru:/etc # john -users:okercho shadow
Loaded 1 password (FreeBSD MD5 [32/32])
guesses: 0 time: 0:00:00:11 46% (2) c/s: 4616 trying: gnicaR
session aborted
root@Naru:/etc #
```



USER	PRI	NI	SIZE	RSS	SHARE	STAT	N#	%CPU	%MEM	TIME	COMMAND
root	19	0	5520	5520	168	S	7	99.9	1.0	107:01	john-mm
root	14	0	632	632	44	S	7	99.9	0.1	85:02	cisilia
root	18	0	632	632	44	S	6	99.9	0.1	58:34	cisilia
root	15	0	632	632	44	S	1	71.0	0.1	50:38	cisilia
root	15	0	632	632	44	S	1	70.2	0.1	51:32	cisilia
root	14	0	632	632	44	S	1	70.0	0.1	48:26	cisilia
root	15	0	632	632	44	R	0	69.4	0.1	65:01	cisilia
root	19	0	632	632	44	R	0	68.9	0.1	57:15	cisilia
root	16	0	1072	1072	1008	R	0	68.3	0.2	56:21	cisilia
root	15	0	632	632	44	S	13	53.0	0.1	49:10	cisilia
root	18	0	632	632	44	S	31	52.8	0.1	52:59	cisilia
root	14	0	632	632	44	S	31	52.6	0.1	53:26	cisilia
root	14	0	632	632	44	S	13	52.4	0.1	53:13	cisilia
root	11	0	892	892	704	R	0	0.3	0.1	0:13	mtop
root	9	0	1024	1024	968	S	0	0.1	0.1	0:06	cisilia
root	9	0	440	412	384	S	0	0.0	0.0	0:43	init

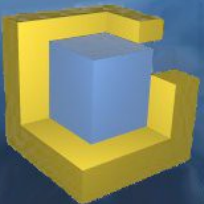
cisilia





# Ingeniería con LinuxAP

Historia  
Firmwares  
Modelos de Aps  
Configuración WEB  
Configuración Telnet/SSH





## - Firmwares : Linux AP 1 -

Distribución de Linux (también llamada OpenAP)

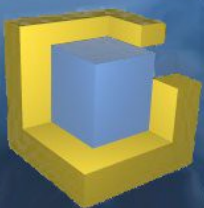
Sólo para algunos Aps

Muchas opciones EXTRAS frente a firmware original

Código libre bajo licencia GNU/GPL

Podemos compilar nuestro propio firmware

Soporta WDS





## - Firmwares : Linux AP 2 -

Iniciado por Linksys (Cisco Systems)

Linksys viola la GPL

Gracias a la FSF se consiguen las fuentes

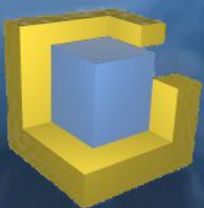
Aumenta el rendimiento del AP

Mejora las posibilidades

Soporte de WDS

### Ramas del firmware original:

- Satori (Sveasoft)
- OpenWRT
- HyperWRT
- Samadhi2 (Valencia Wireles)
- Busybox





## - Modelos de APs -



SMC 2682W

USRobotics USR2450



Linksys WRT54G





## - Configuración WEB -

Setup - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://192.168.1.250/

Barrapunto Google AltaVista - Babel Fis... El Callejero de Pagin... AlltheWeb.com PHP: Índice de funcio...

**LINKSYS®**  
A Division of Cisco Systems, Inc.

Firmware Version: Satori-4.0 v2.07.1.7sv

**Wireless-G Broadband Router** **Esperanza03**

**Setup** | **Wireless** | **Security** | **Access Restrictions** | **Applications & Gaming** | **Administration** | **Status**

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

**Internet Setup**

**Internet Connection Type** Automatic Configuration - DHCP

**Optional Settings (required by some ISPs)**

Router Name:

Host Name:

Domain Name:

MTU:

Size:

**Network Setup**

**Router IP**

Local IP Address:  .  .  .

Subnet Mask:

Gateway:  .  .  .

**Network Address Server Settings (DHCP)**

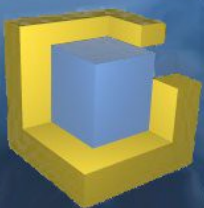
DHCP Server: ☒ Enable ☐ Disable

Starting IP:

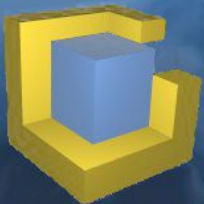
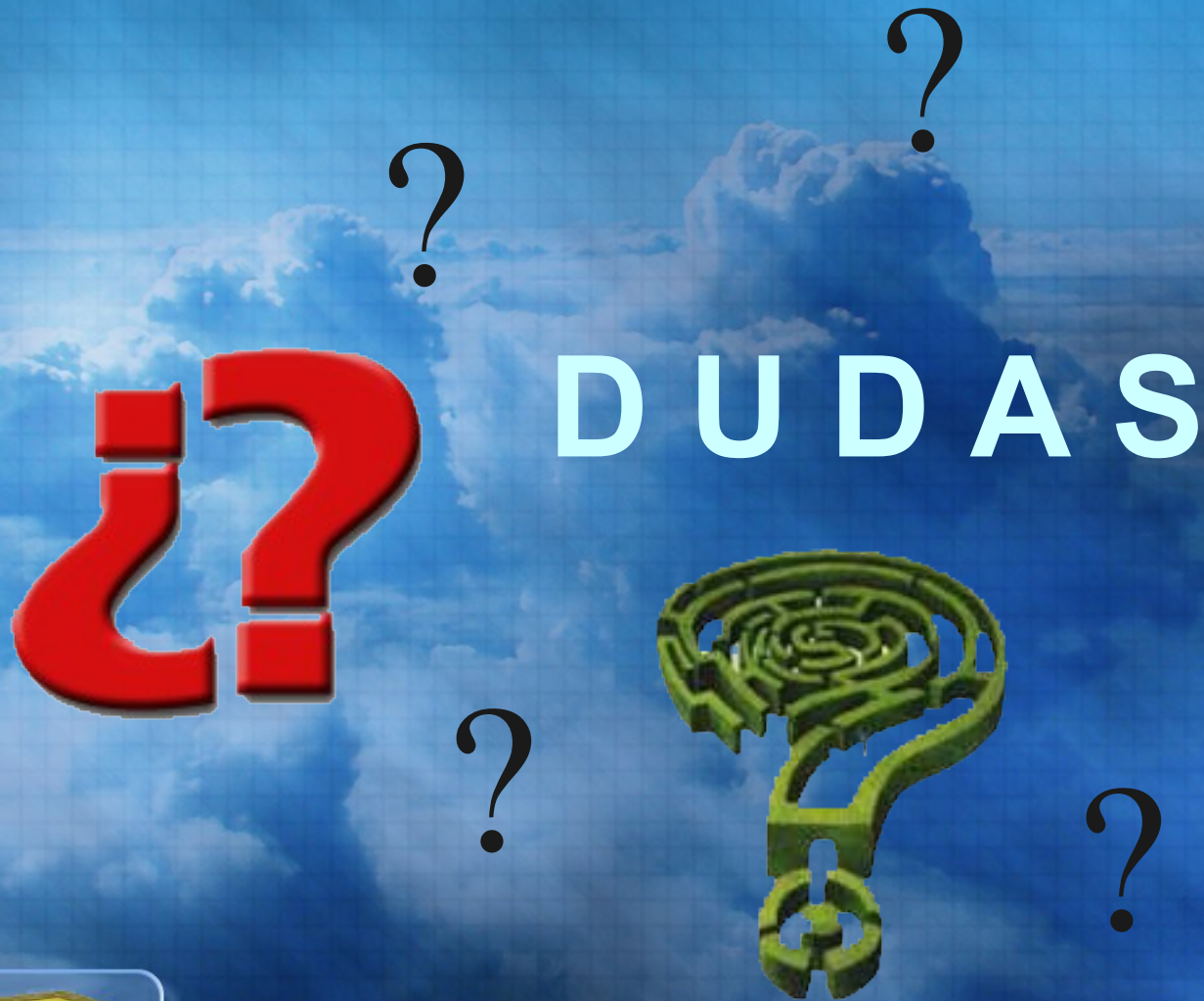
More...

Done

Interfaz web de WRT54G: fácil de configurar

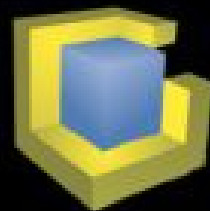








GRACIAS



**Centrologic**  
Computational Logistic Center

Ponente: Juan Miguel Taboada Godoy  
juanmi@centrologic.com - <http://www.centrologic.com>

