

Autenticación e Integridad en redes Wireless

Campus-Party 2003
Valencia 14 de Agosto'03

Toni dIF. Diaz
toni@madridwireless.net

<http://madridwireless.net>

<http://blyx.com>

<http://vklab.sinroot.net>

Contenido (I)

- 1.- Conceptos.
- 2.- Buenos hábitos.
- 3.- FakeAP: Evasion y ¿victoria?
- 4.- Monitorización y control.
- 5.- Necesidades.

Autenticando accesos.

- 6.- ¿Qué es 802.11i?
- 7.- Entendiendo 802.1X
- 8.- Implementación de 802.1X

Contenido (II)

9.- Software

9.1.- Captive portal

9.2.- Otros

9.3.- NoCat Auth

9.3.1.- Características

9.3.2.- Modos de funcionamiento

9.3.3.- Componentes

9.3.4.- Estructura y funcionamiento

9.3.5.- Implementaciones del gateway

9.3.6.- Gestión del ancho de banda

9.3.7.- Análisis

9.3.8.- El cliente

9.3.9.- Servicios y Software necesario

9.3.10.- Warchalking + NoCatAuth

Referencias

1-Conceptos (I)

Redes wireless: comunicación sin cables

Redes Wi-Fi: 802.11*

La diferencia entre las redes inalámbricas y otras está en los niveles mas bajos de la pila OSI, nivel físico y nivel de enlace. Se definen en el estandar 802.11 del IEEE

Tipos:

802.11a: 54 Mbps estandarizado, y hasta 72 y 108 Mbps con tecnologías de desdoblamiento no estandarizado. 5 Ghz. En teoría hasta 64 usuarios por AP. Dispositivos caros.

802.11b: *11 Mbps estandarizado, y hasta 22 Mbps por desdoblamiento de la velocidad no estandarizado. 2.4 Ghz. En teoría hasta 32 usuarios por AP.*

802.11g: 54 Mbps, compatible con 802.11b. 2.4 Ghz.

1-Conceptos (II)

Deficiencias:

- Seguridad
- No integra QoS
- 2.4Ghz es una frecuencia muy concurrida.
- Dispositivos de 5 Ghz son caros.

Componentes principales: Cliente (STA) y punto de acceso (AP)

Topologías de red:

Ad-Hoc (iBSS): Cliente – Cliente

Infraestructura (BSS): Cliente – AP – Cliente

Modos de actuación de los dispositivos.

Ad-Hoc: dispositivo cliente en una red Ad-Hoc

Managed: dispositivo cliente en una red tipo Infraestructura

Master: capacidad de algunos interfaces wi-fi para hacer de AP

1-Conceptos (III)

Terminología usada en redes wireless:

WEP: Significa Wired Equivalet Privacy, puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y hasta 256 que usan algunas marcas

OSA: (Open System Authentication), cualquiera puede formar parte de la red.

SKA: Shared Key Authentication.

ACL: significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC.

CNAC: significa Closed Network Access Control, no permite el enlace si no se conoce el SSID.

SSID: significa Service Set IDentifier, cadena de 32 caracteres como máximo, necesario conocer para unir un cliente a la red.

SOHO: small office/home office networks

Beacon Frames: paquetes que transmite un AP para anunciar su disponibilidad y características.

1-Conceptos (IV)

Estándares: (sindominio.net/suburbia/article.php3?id_article=22)

802.11a (5 Ghz)

802.11b (2.4 Ghz)

802.11c Define características de AP como bridges.

802.11d Permite el uso de 802.11 en países restringidos por el uso de las frecuencias.

802.11e Define el uso de QoS.

802.11f Define el enlace entre STA y AP. Roaming

802.11g (2.4 Ghz a más velocidad que 802.11b)

802.11h Superior al 802.11a permite asignación dinámica de canales (coexistencia con el HyperLAN). Regula la potencia en función de la distancia.

802.11i *Estándar que define la encriptación y la autenticación para complementar completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del WPA con su Temporal Key Integrity Protocol (TKIP).*

802.11j Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.

802.11m Propuesto para mantenimiento de redes inalámbricas.

2-Buenos hábitos (I)

Uso de protocolos seguros en las comunicaciones:

Ssh en lugar de Telnet

Smtps en lugar de Sntp

Pop-ssl en lugar de Pop

Imap-ssl en lugar de Imap

Https en lugar de http (al menos para páginas con autenticación)

Uso de Redes Privadas Virtuales (VPN):

OpenVPN

vtund

vpnd

Freeswan

CIPE

IPSec (no soporta enrutamiento dinámico)

2-Buenos hábitos (II)

Uso de WEP:

Es mejor que no usar nada, necesitamos al menos 200Mb de tráfico o 500.000 paquetes encriptados para reventar la encriptación.

Uso de un firewall para separar las diferentes redes.

¡¡Cuidado con los bridges!!

Usar QoS

Usar AP redundantes para solventar ataques DoS

Disponer de un falso Punto de Acceso: FakeAP

3-FakeAP: Evasión y ¿victoria?

Un falso punto de acceso wireless que molesta (I)

FakeAP es un script en perl que envia beacons con diferentes ESSID y diferentes direcciones MAC a la red con o sin wep utilizando el driver hostap.

No es un AP válido sino uno falso que no sirve para dar servicio.

Probado en RedHat Linux y OpenBSD (port)

Requisitos: Tener una máquina con hostap al menos del 31/7/2002 instalado y funcionando.

3-FakeAP: Evasión y ¿victoria?

Un falso punto de acceso wireless que molesta (II)

1-Descargar, descomprimir y desempaquetar.

[Http://www.blackalchemy.to/project/fakeap/](http://www.blackalchemy.to/project/fakeap/)

2-Instalar los siguientes modulos de perl:

Getopt::Long, Time::HiRes, (# perl -MCPAN -e shell
cpan> install nombre::modulo)

3-Añadir a fakeap.pl la primera linea con el path de donde este el binario de perl (#!/usr/bin/perl) y hacerlo ejecutable.

3-FakeAP: Evasión y ¿victoria?

Un falso punto de acceso wireless que molesta (III)

4-Ejecución:

```
[root@moon fakeap-0.3.1]# ./fakeap.pl --interface wlan0 --channel 10 --words
lists/stefan-wordlist.txt --sleep 2 -vendors lists/stefan-maclist.txt --power
15
fakeap 0.3.1 - Wardrivring countermeasures
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved
```

```
Using interface wlan0:
Sleeping 2 sec
Static channel 10
Generating ESSIDs from lists/stefan-wordlist.txt
Vary Tx power up to 15
Using 53068 words for ESSID generation
Using 20 vendors for MAC generation
```

```
-----
3: ESSID=pompey          chan=10 Pwr=12  WEP=N MAC=00:04:E2:39:31:F3
4: ESSID=straub         chan=10 Pwr=1   WEP=N MAC=00:02:2D:C0:B2:35
7: ESSID=galois         chan=10 Pwr=14  WEP=N MAC=00:80:0F:5F:B7:1E
-----
```

Run complete

5-Conclusion: FakeAP no es la panacea pero molesta

3-FakeAP: Evasión y ¿victoria?

Un falso punto de acceso wireless que molesta (IV)

Sniffer, kismet:

```
Eterm Font Background Terminal
Network List (Autofit)
Name      T W Ch Packts Flags IP Range      Size
osan-milnet-tac  A N 10      1    0.0.0.0      0B
mk         A N 10      1    0.0.0.0      0B
dreamers   A N 10      1    0.0.0.0      0B
kellsie    A N 10      1    0.0.0.0      0B
farrukh    A N 10      1    0.0.0.0      0B
ramothgilead A N 10      1    0.0.0.0      0B
ergok      A N 10      1    0.0.0.0      0B
kandor     A N 10      1    0.0.0.0      0B
crayola    A N 10      1    0.0.0.0      0B
whitaker   A N 10      1    0.0.0.0      0B
reused     A N 10      1    0.0.0.0      0B
macis      A N 10      1    0.0.0.0      0B
dcomm1643  A N 10      1    0.0.0.0      0B
boasters   A N 10      1    0.0.0.0      0B
Wingolfia  A N 10      1    0.0.0.0      0B
clappeth   A N 10      1    0.0.0.0      0B
fornicators A N 10      1    0.0.0.0      0B
greywood   A N 10      1    0.0.0.0      0B
lufferlang A N 10      1    0.0.0.0      0B
cerberus   A N 10      1    0.0.0.0      0B
glenfield  A N 10      1    0.0.0.0      0B
remitha    A N 10      1    0.0.0.0      0B
bugw       A N 10      1    0.0.0.0      0B
vinitha    A N 10      1    0.0.0.0      0B
kipper     A N 10      1    0.0.0.0      0B
brilliant  A N 10      1    0.0.0.0      0B
agee       A N 10      1    0.0.0.0      0B
. halli    A N 10      1    0.0.0.0      0B
. wengyik  A N 10      1    0.0.0.0      0B
! csd4     A N 10      1    0.0.0.0      0B

Info
Ntwrks    40
Pckets    40
Cryptd    0
Weak      0
Noise     0
Discrd    0
Pkts/s    0

Elapsed 000214

Status
Found new network "prevailed" bssid 00:05:86:D1:77:F8 WEP N Ch 10 @ 11.00 mbit
Found new network "csd4" bssid 00:40:33:71:8D:B5 WEP N Ch 10 @ 11.00 mbit
Found new network "wengyik" bssid 00:80:C8:D7:0B:39 WEP N Ch 10 @ 11.00 mbit
Found new network "halli" bssid 00:04:5A:70:24:D9 WEP N Ch 10 @ 11.00 mbit
Battery: AC 100% 6h0m0s
```

4-Monitorización y control (I)

Linux: Airtraf, Kismet, Ethereal + parche 802.11

FreeBSD: wicontrol, bsd-airtools (dstumbler)

Software de control basado en sondas distribuidas:

- Supervisar correcto uso de WPA, WEP, LEAP, PEAP, 802.1x así como VPNs.

- Detectar otros AP o redes ad-hoc para evitar Man In The Middle attacks o comunicación Peer-to-peer.

- Evita asociaciones accidentales con redes similares.

Software disponible: AirMagnet, RogueGuard, AirDefense

IDS:

- Snort, Demarc, Ntop (red)

- Tripwire, logcheck, logwatch, cops, portsenry (host)

4-Monitorización y control (II)

Airtraf 1.1: IDS de redes wireless

- Captura y analiza el tráfico 802.11b
- Controla el uso de ancho de banda
- Monitoriza la potencia de la señal del AP
- Busca APs y sus correspondientes SSID, canal, tráfico, etc.
- Almacena toda la información para ser procesada.
- Interpreta métodos de autenticación y asociación
- Añadiendo otras características IDS.

Web: <http://www.elixar.com>

4-Monitorización y control (III)

```
AirTraf: 1.0.0 '02
- Statistics for eth1 -
BSSID: 00022d28dc25  SSID: WavelAN Network  WEP: opensystem  CHANNEL: 8  TIME: 00:00:44

Management Frames:
  Beacon: 636
  Disassoc: 0
  Other: 22
  Total Packets: 658
  Total Bytes: 44612
  Bandwidth: 5.39 Kbps

Control Frames:
  Acknowledgement: 0
  Other: 0
  Total Packets: 0
  Total Bytes: 0
  Bandwidth: 0.00 Kbps

Data Frames:
  External Packets: 23
  External Bytes: 5946
  Internal Packets: 708
  Internal Bytes: 423433
  Total Packets: 731
  Total Bytes: 429379
  Bandwidth: 0.3520 Mbps

Corrupt Frames: (count) (bytes)
  Bad MAC addr: 0 0
  Bad IP chksum: 0 0
  FCS error: 0 0
  Filtered data: 0 0
  Overall: 0 0

OVERALL ACTIVITY:
  Total Packets: 1389
  Total Bytes: 473991
  Bandwidth: 0.3574 Mbps

Connected Nodes
MAC address 0: 00022d28dc25 - AP  IP: (Unknown)
  incoming packets: 0  outgoing packets: 658
  incoming bytes: 0  outgoing bytes: 44612
  avg.signal strength: 0.00
  Bandwidth: 0.0054 Mbps

MAC address 1: 00409635e0b7 - STA  IP: (192.168.0.7)
  incoming packets: 392  outgoing packets: 321
  incoming bytes: 366071  outgoing bytes: 57672
  avg.signal strength: 0.00
  Bandwidth: 0.3520 Mbps

Active

CHANNEL STATUS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14
Up/Down/PgUp/PgDn-scroll window  Left/Right-change channels  P-pause  X-exit
```


4-Monitorización y control (IV)

Drivers HostAP:

/proc/net/hostap/wlanN/

ap_control – Access Control List

Ejemplos de instalación de ACLs con HostAP

```
# allow policy
```

```
iwpriv wlan0 maccmd 1
```

```
iwpriv wlan0 addmac 00:11:22:33:44:55
```

```
iwpriv wlan0 addmac 00:12:34:56:78:9a
```

```
# deny policy
```

```
iwpriv wlan0 maccmd 2
```

```
iwpriv wlan0 addmac 00:11:22:33:44:56
```

```
iwpriv wlan0 addmac 00:12:34:56:78:9b
```

5-Necesidades

Autenticación.

Privacidad y encriptación (Confidencialidad).

-Es posible capturar el tráfico.

Integridad:

-Alteración del tráfico.

QoS: gestión del ancho de banda.

Escalabilidad.

Alta disponibilidad de servicio.

Autenticando accesos

6- ¿Qué es 802.11i? (I)

Standard de seguridad para redes 802.11

Surgió a raíz de las vulnerabilidades del 802.11b y sera aplicable a redes 802.11a (54Mbps), 802.11b (11Mbps) y 802.11g (22Mbps).

Actualmente es un borrador de la IEEE (Institute of Electrical and Electronics Engineers). Se prevee que sea definitivo a finales del 2003.

Lo desarrolla (comite): Cisco, VDG, Trapeze, Agere, IBM, Intersil y otros.

Ya se han extraido partes que se han desarrollado completamente:

- Se prevee que use parte del standard IEEE 802.1X (EAPoL).
- WPA (Wi-Fi Protected Access) y TKIP (Temporal Key Integrity Protocol).

6- ¿Qué es 802.11i? (II)

TKIP (Temporal Key Integrity Protocol), codifica las claves mediante un algoritmo de "hashing", con verificaciones de integridad adicionales para evitar manipulaciones.

Implica modificaciones en el firmware del actual hardware.

Probablemente se especifiquen modificaciones de hardware en el standard.

Información sobre el estado del proyecto:

http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

7-Entendiendo 802.1X (I)

Mecanismo estándar para autenticar centralmente estaciones y usuarios.

Estándar abierto, soporta diferentes algoritmos de encriptación.

Se apoya en el protocolo de autenticación EAP (Extensible Authentication Protocol), en realidad es EAPoL (EAP over LAN) de forma que se puede usar en redes ethernet, 802.11, Token-Ring y FDDI

Requiere cliente (Xsuplicant), Punto de Acceso y servidor de autenticación.

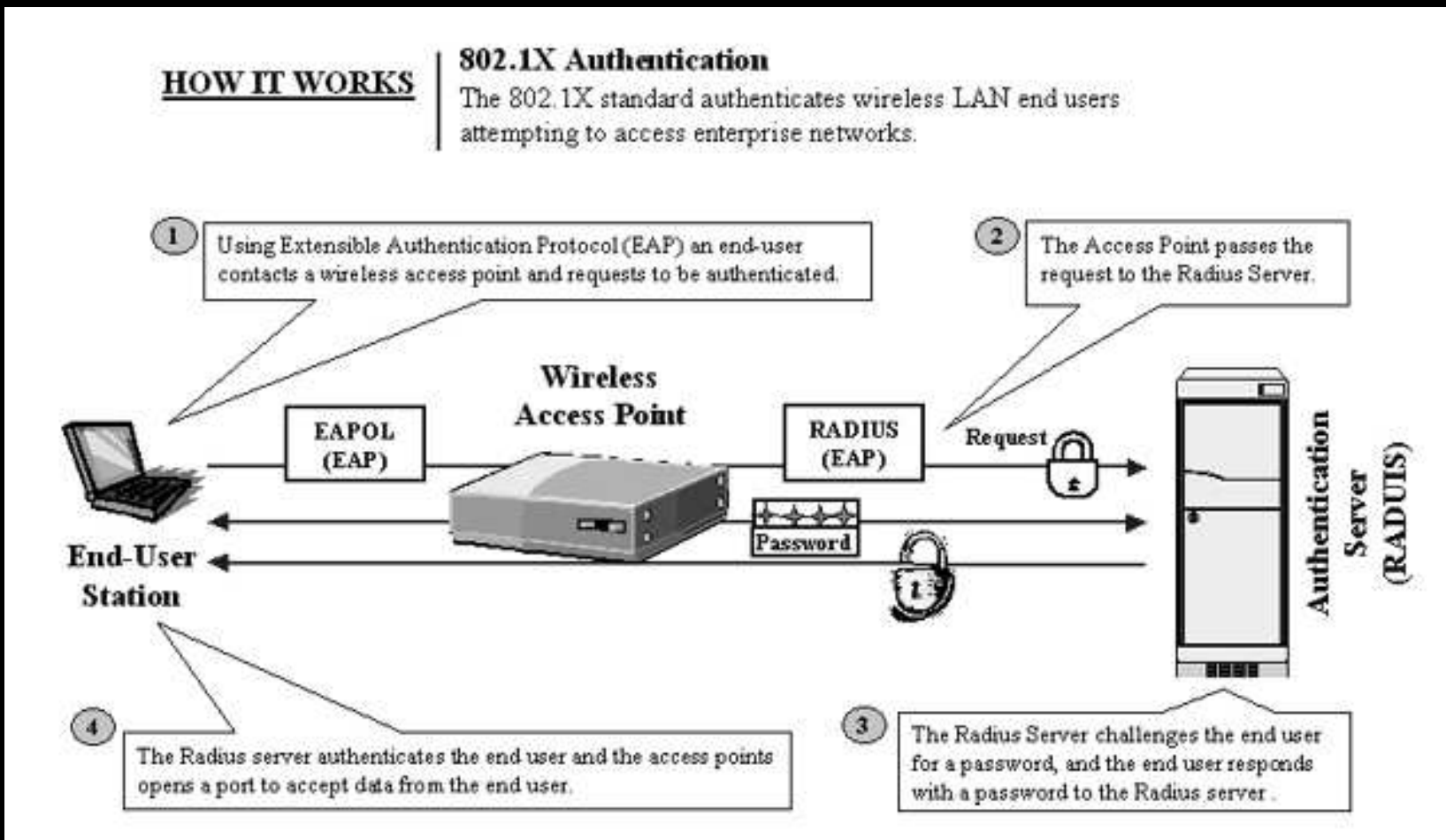
EAP es soportado por muchos Puntos de Acceso y por HostAP

Antes de la autenticación sólo se permite tráfico 802.1X (petición de autenticación)

7-Entendiendo 802.1X (II)

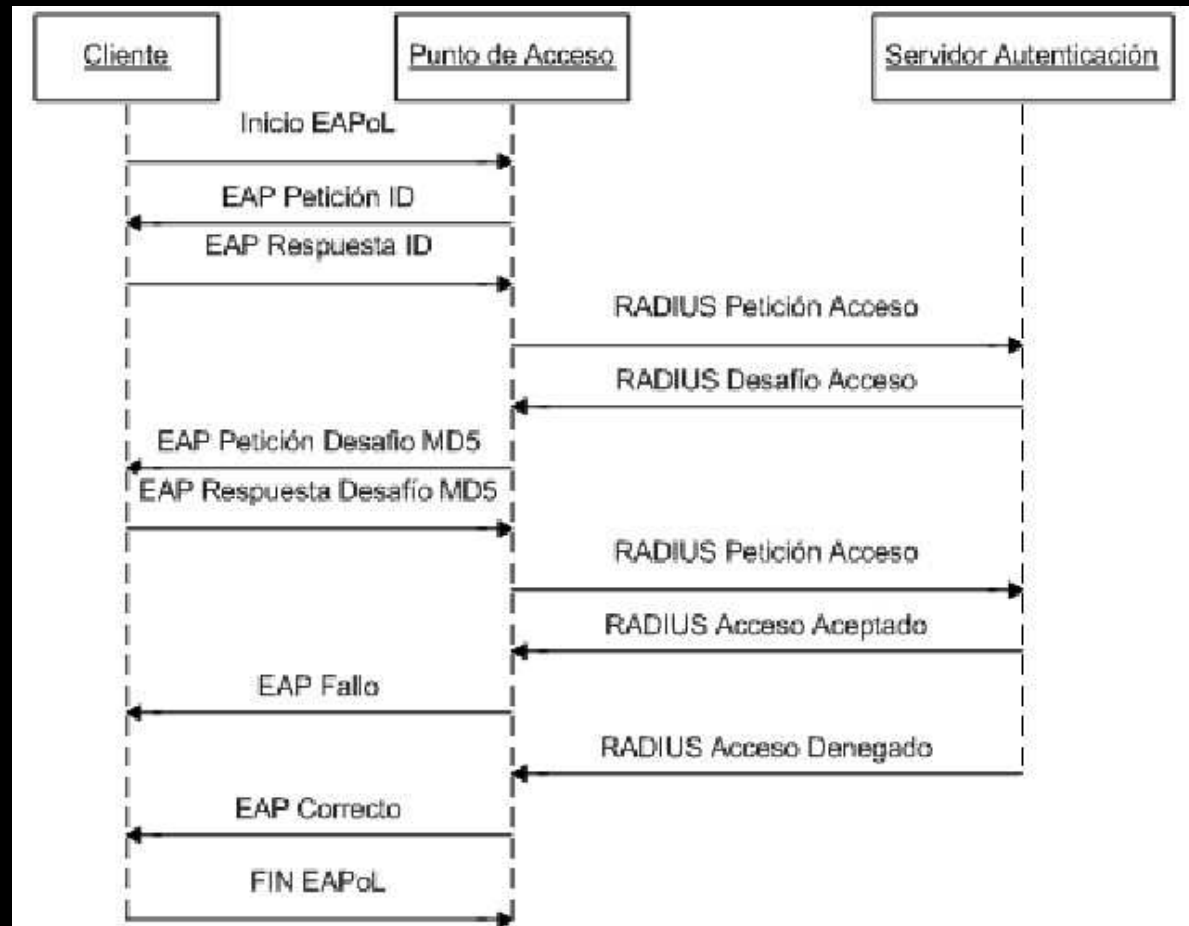
EAP en acción:

El cliente (supplicant) envía un mensaje de inicio al AP este le pide identificación y cierra todo el tráfico excepto 802.1X, el cliente le envía su identidad, el AP la pasa al servidor de autenticación, éste envía un paquete de aceptación al AP y el AP le devuelve la autorización para comenzar la transmisión.



7-Entendiendo 802.1X (III)

Proceso de autenticación con EAP detallado:



7-Entendiendo 802.1X (IV)

Variantes de EAP (Extensible Authentication Protocol):

EAP-TLS (EAP – Transport Level Security)

Autenticación mutua, cifrada y depende de certificados de una CA. Soportado por hostapd.

EAP-TTLS (EAP Tunned TLS)

No necesita ambos certificados, solo el de el servidor para crear un tunel. Usado en redes wireless.

EAP-MD5

El servidor envia un mensaje desafío al cliente y este contesta con otro mensaje MD5 o no autentica. Fácil de implementar pero menos fiable.

LEAP (Lightweigth EAP)

Implementacion de Cisco, autenticación mutua, permite el uso dinámico de WEP.

PEAP (Protected EAP): desarrollado por M\$, Cisco y RSA, similar a EAP-TTLS

8-Implementación de 802.1X (I)

802.1X en la vida real con Software libre.

HostAP está capacitado para implementar 802.1X “for testing”

Requisitos:

-Compilar el demonio hostapd (incluido en el paquete hostap) en el AP:

```
#cd hostapd  
#make  
#hostapd /etc/hostapd.conf
```

-Servidor RADIUS Freeradius

-Cliente linux Xsupplicant (<http://www.open1x.org>) para autenticación EAP-TLS

HostAP soporta envío aleatorio de WEP a las estaciones (la misma a todas las estaciones o diferente a cada una)

8-Implementación de 802.1X (II)

Mas información en la documentación de HostAP

Otra implementación con AP Cisco en lugar de HostAP:
<http://www.missl.cs.umd.edu/wireless/eaptls/>

- OpenSSL
- LibNet
- FreeRADIUS
- Xsupplicant

8-Implementación de 802.1X (III)

Captura de configuración EAP para el Cisco AP340:

MISSL340AP Authenticator Configuration

Cisco AP340 11.10T

Uptime: 00:21:27

802.1X Protocol Version (for EAP Authentication): Draft 10

Server Name/IP	Server Type	Port	Shared Secret	Timeout (sec.)
192.168.5.200	RADIUS	1812	*****	20
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input checked="" type="checkbox"/> MAC Address Authentication				
192.168.5.200	RADIUS	1812	*****	20
Use server for: <input type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication				
	RADIUS	1812	*****	20
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication				
	RADIUS	1812	*****	20
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication				

Apply OK Cancel Restore Defaults

[Map][Login][Help]

Cisco AP340 11.10T © Copyright 2001 Cisco Systems, Inc. [credits](#)

9-Software (I)

Aplicaciones que proporcionan autenticación, encriptación y privacidad (o alguna de estas premisas) con Software Libre sin usar EAP.

9-Software (II)

Captive portal:

NoCat Auth - <http://nocat.net>

LANRoamer – <http://www.lanroamer.net>

Wireless Heartbeat - <http://www.river.com/tools/authhb/>

NetLogon - Linköping University

FisrtSpot (PatronSoft) – <http://www.patronsoft.com/firstspot/>

WiCap (OpenBSD) - <http://www.geekspeed.net/wicap/>

9-Software (III)

Otros:

SLAN - <http://slan.sourceforge.net/>

WARTA Project - www.hpi.net/whitepapers/warta/warta.pdf

- Autenticación, routing, QoS.

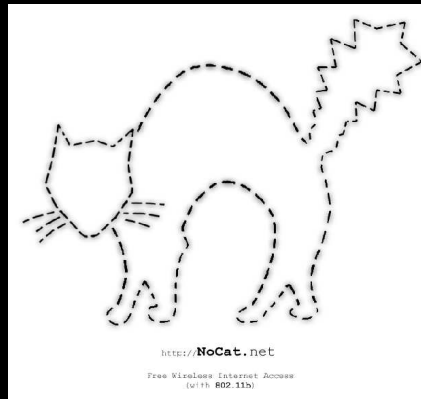
- FreeBSD, PPPoE, IPFW, RADIUS, Hardware, red.

9-Software (IV)

NoCat Auth

Sistema de **validación de clientes** para nodos wireless, según el tipo de usuario asigna **ancho de banda** y da **acceso a servicios** disponibles.

Lo desarrolla la **comunidad wireless de Sonoma County** -Schuyler Erle-, California (E.E.U.U.). Colaboran **SeattleWireless, PersonalTelco, BAWUG, Houston WUG** además de personas y grupos de todo el mundo.



9-Software (IV)

NoCat Auth

Características:

- Autenticación segura basada en SSL (navegador).
- Autoriza mediante usuario y contraseña.
- Informa de la entrada y salida del usuario en la red.
- Añade la implementación de QoS por usuarios y grupos.

9-Software (IV)

NoCat Auth

Modos de funcionamiento:

Captive Portal (Portal Cautivo):

- Captura las peticiones de usuarios a una web.
- Comprueba los credenciales del usuario y máquina contra una base de datos.
- Login obligatorio para el usuario.
- Mantiene la sesión mientras está logeado.

9-Software (IV)

NoCat Auth

Otros modos de funcionamiento:

Passive Portal:

-Como **Captive** pero se usa cuando hay un Firewall entre AP y NoCat-GW.

Open Portal:

-Simplemente muestra una web con las condiciones de uso, no requiere credenciales.

9-Software (IV)

NoCat Auth

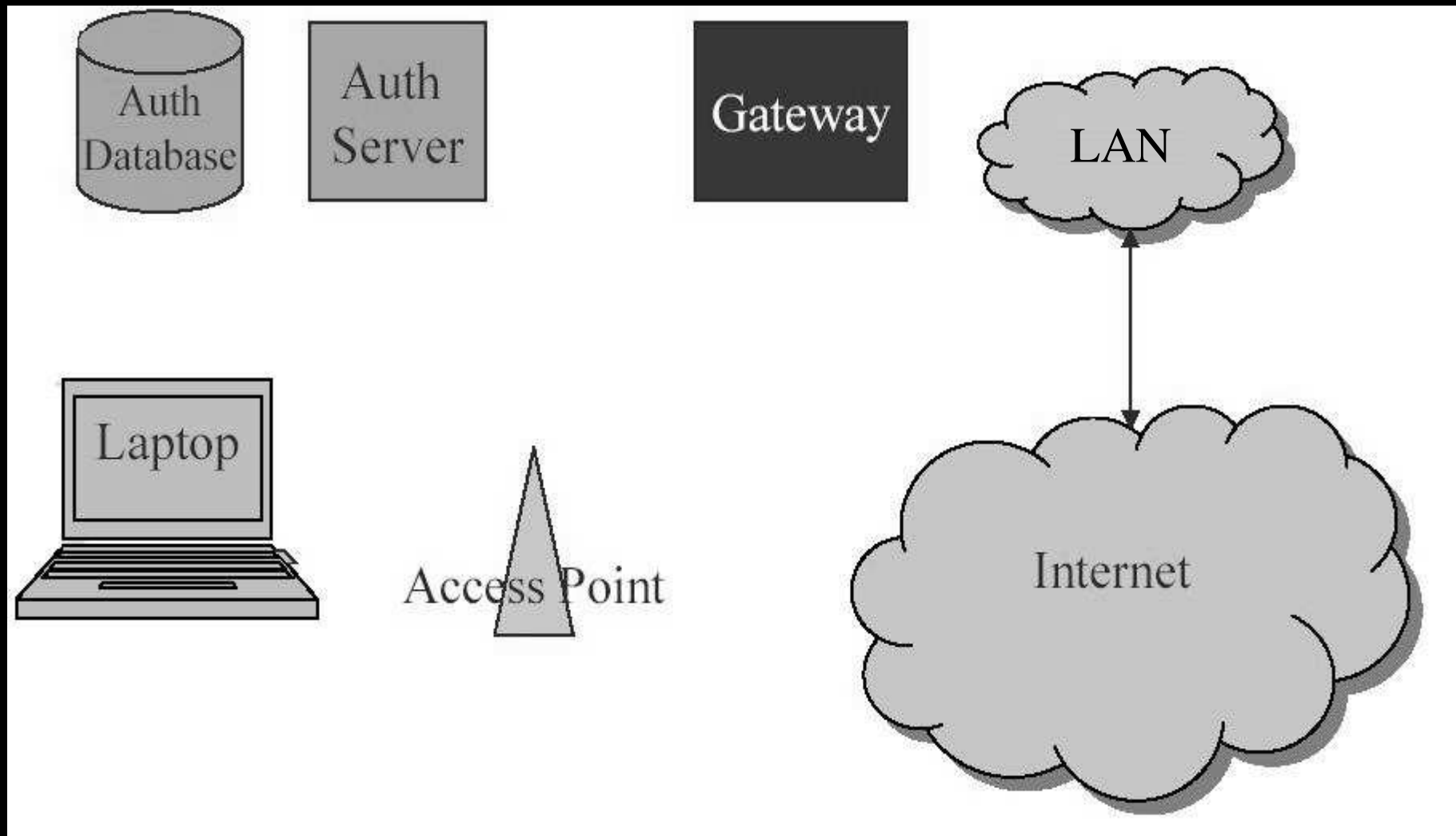
Componentes:

- NoCat Auth**: Servicio de autenticación
- NoCat Gateway**: Servicio de redirección y FW.
- Auth Database**: Fichero propio (MD5), Base de Datos, Ldap, Radius, PAM, Samba, IMAP.
- Access Point**

9-Software (IV)

NoCat Auth

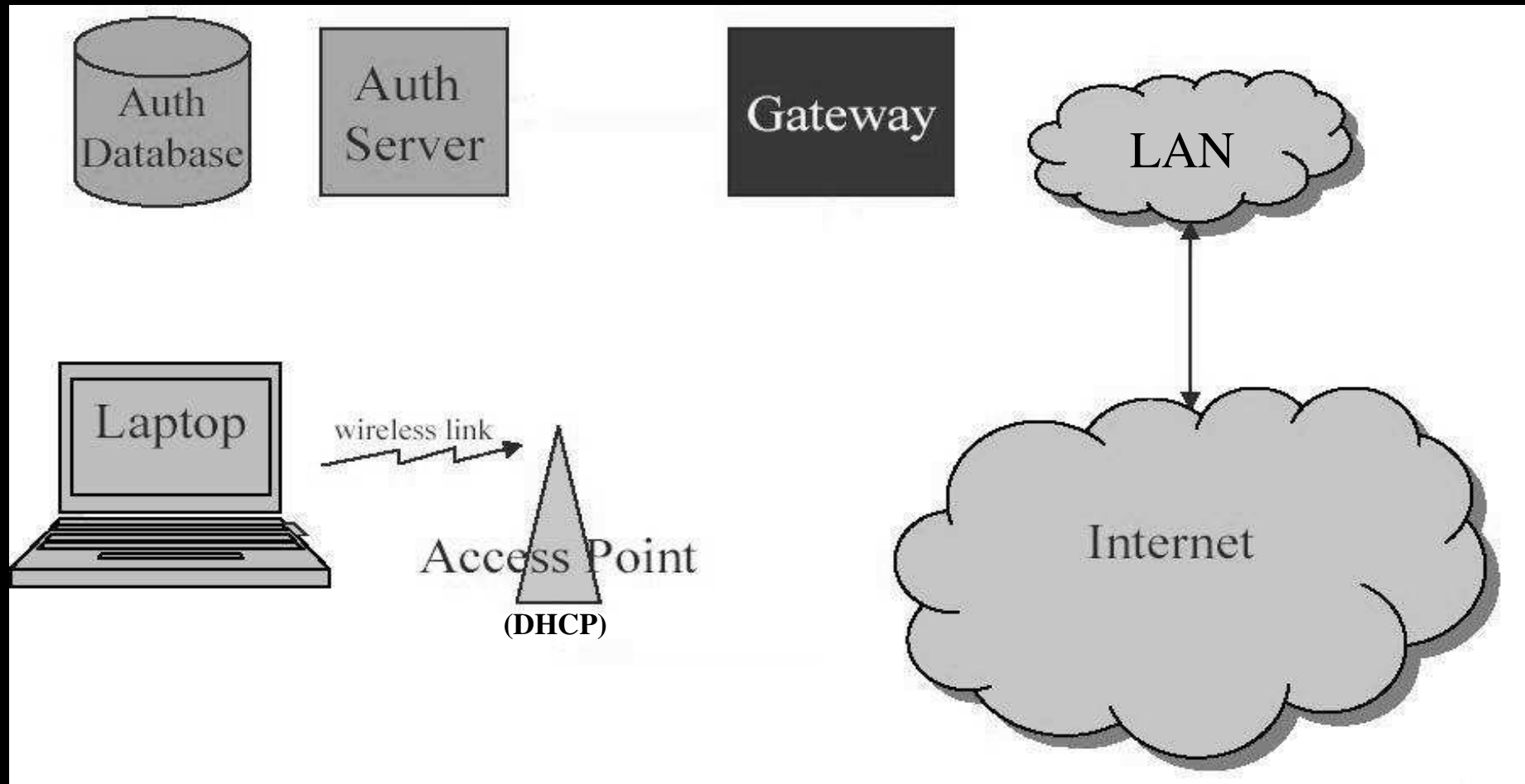
Estructura y funcionamiento



9-Software (IV)

NoCat Auth

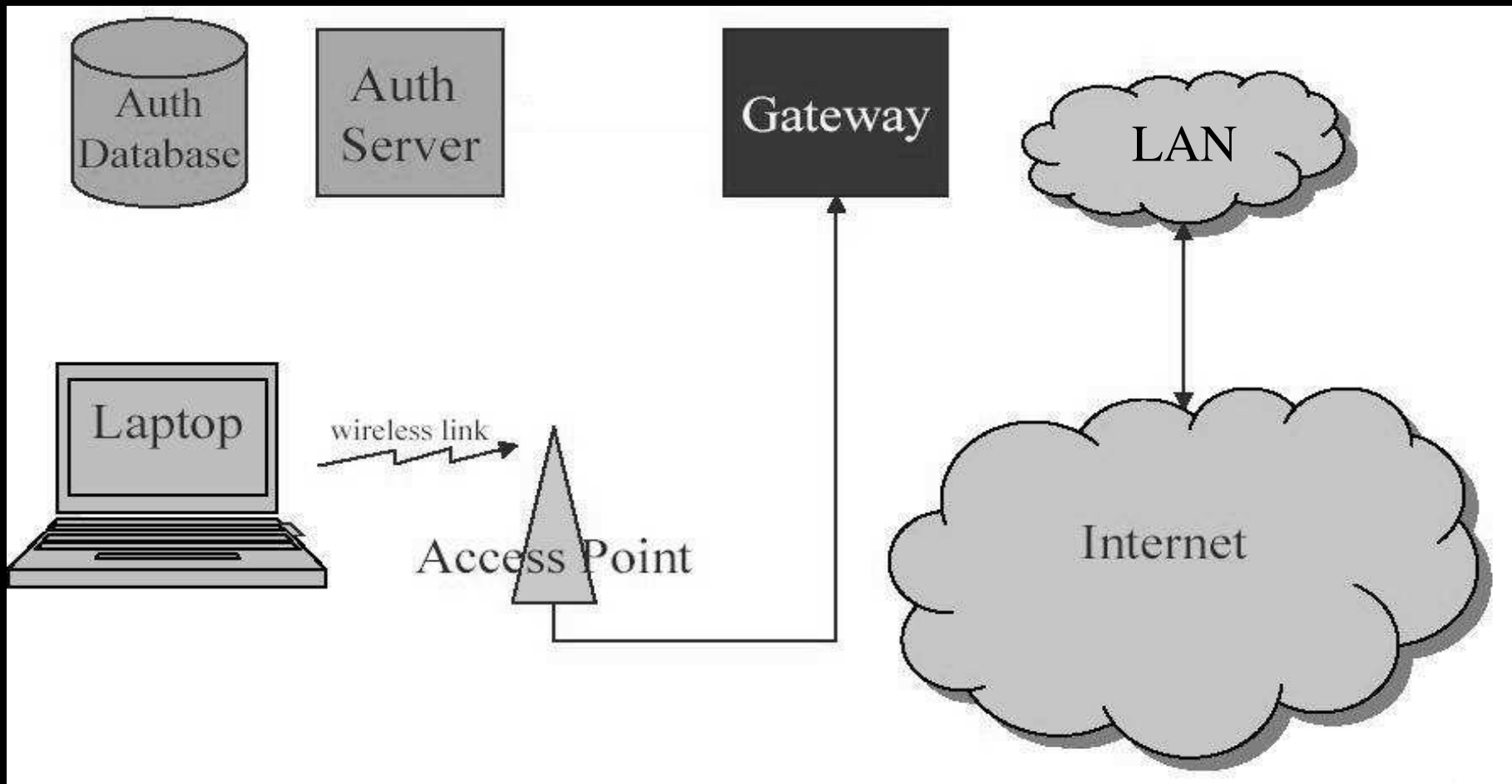
El cliente se asocia con un AP y le asigna una IP:



9-Software (IV)

NoCat Auth

El AP reenvía las peticiones al GW:

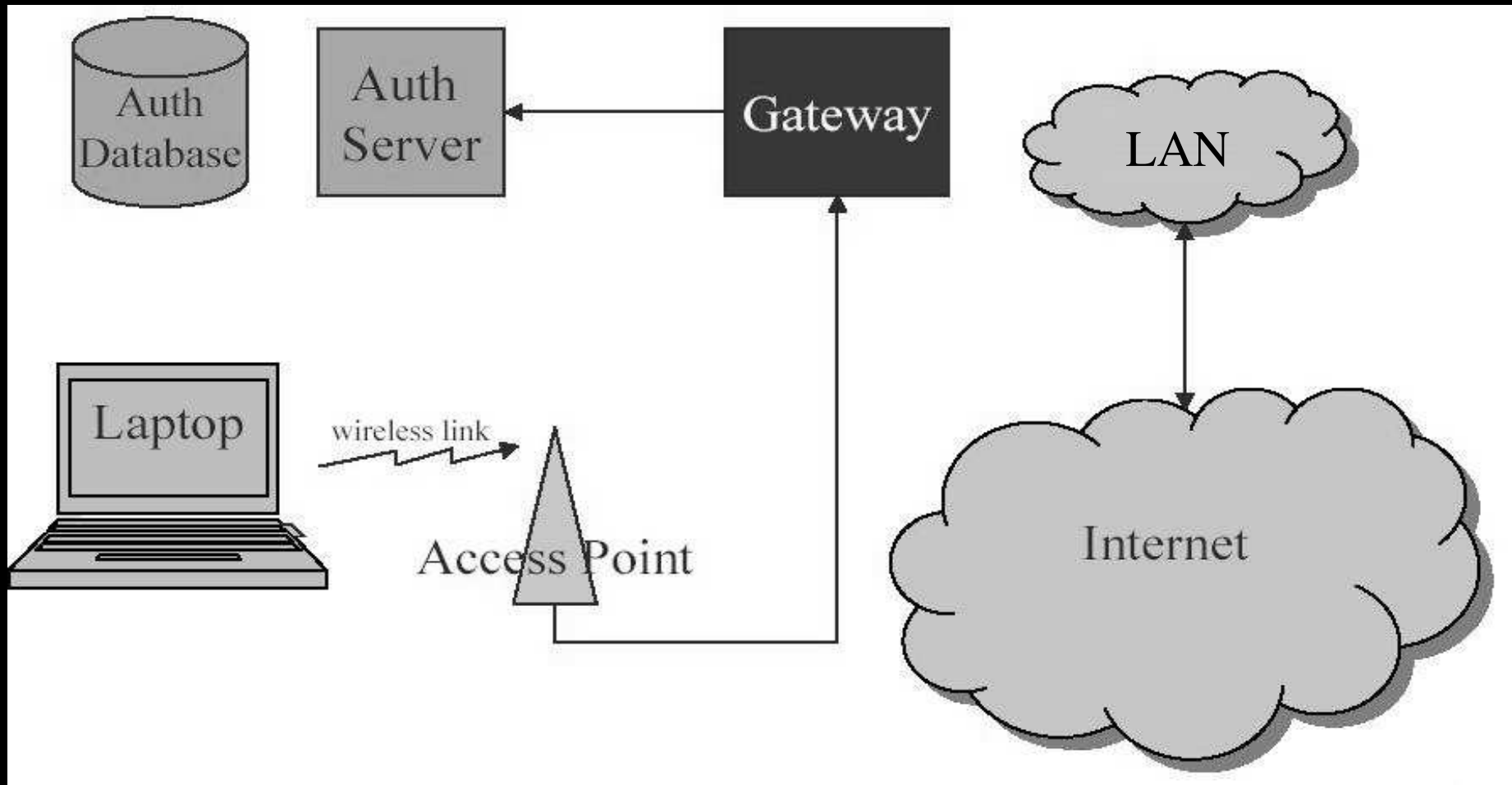


9-Software (IV)

NoCat Auth

El GW redirige a la página de login del Auth Server:

```
iptables -t nat -A PREROUTING -s 10.10.21.0/24 -p tcp --dport 80 -j  
REDIRECT -d 10.10.21.2 --to-port 443
```



9-Software (IV)

NoCat Auth


Página de login:

Greetings! Welcome to the NoCat Network.

Login:

Password:

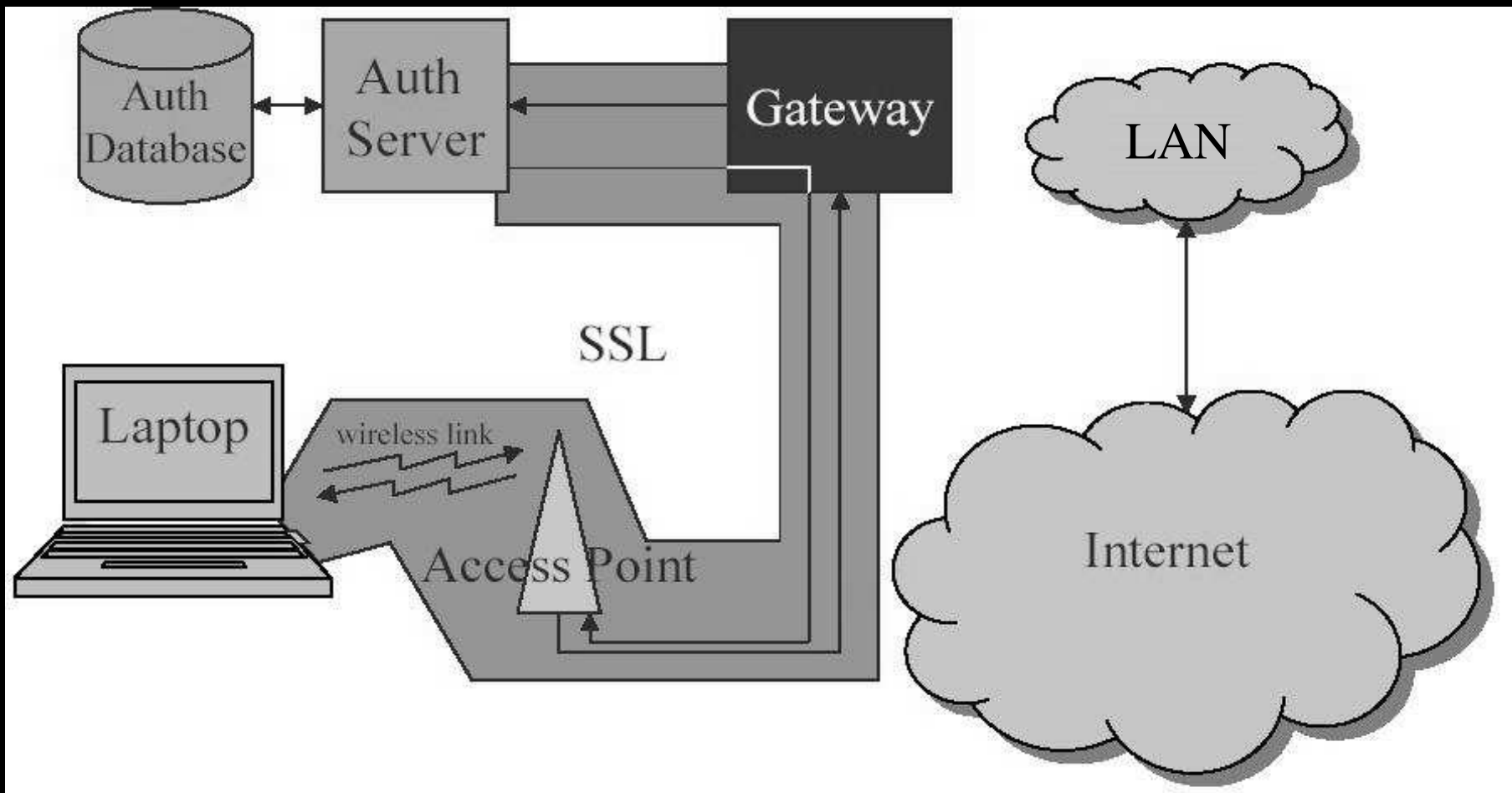
Don't have an account? [Register here!](#)

 nocat
AUTHENTICATION

9-Software (IV)

NoCat Auth

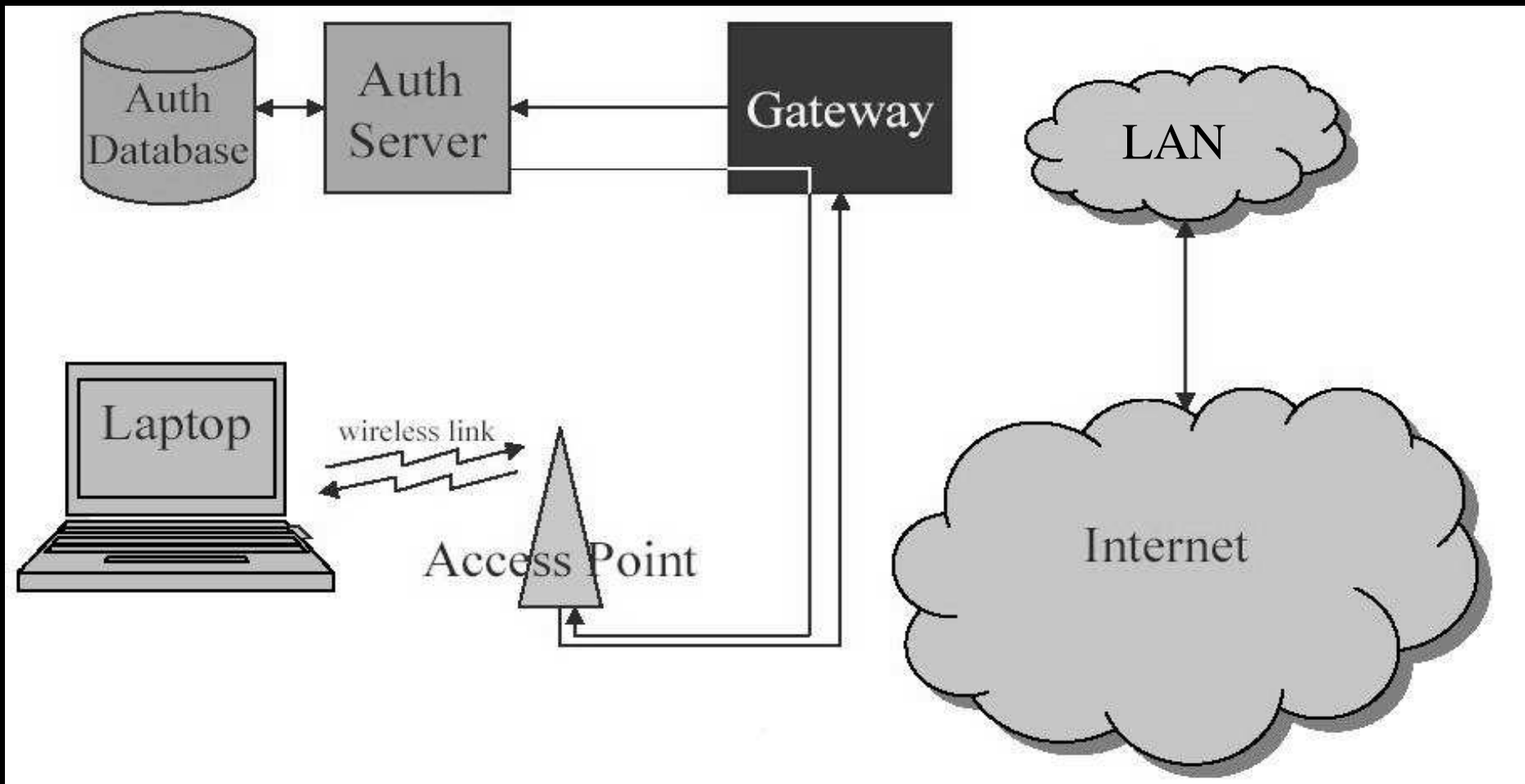
La conexión es autenticada vía SSL:



9-Software (IV)

NoCat Auth

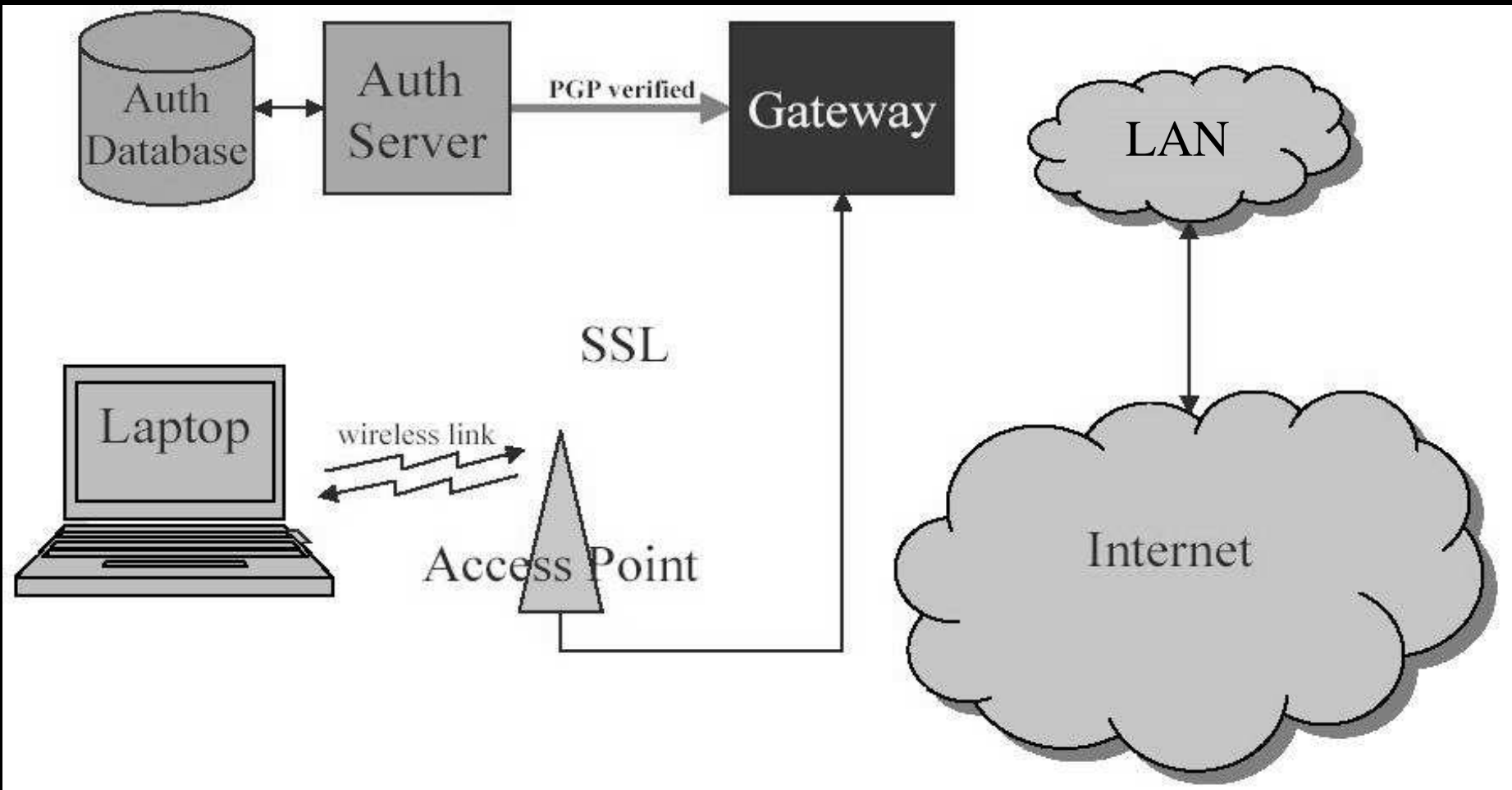
El Auth Server pide usuario y contraseña al cliente (via SSL) y la comprueba con la Auth Database:



9-Software (IV)

NoCat Auth

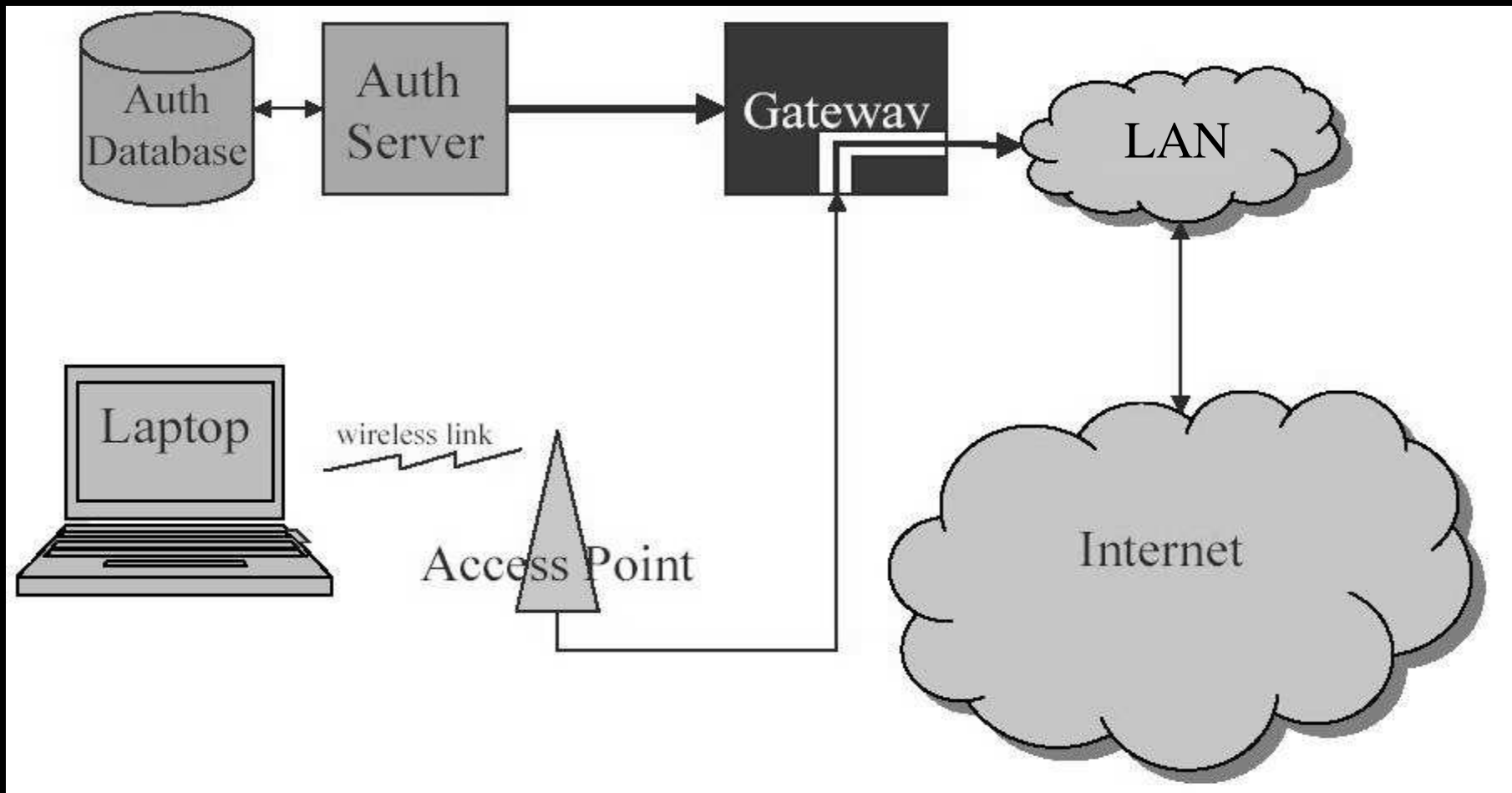
Los mensajes de autorización van firmados con PGP/GnuPG, el GW utiliza la clave pública del Auth Server:



9-Software (IV)

NoCat Auth

Si la autenticación ha sido satisfactoria el GW redirige el tráfico a la LAN y/o Internet:



9-Software (IV)

NoCat Auth

Implementaciones del Gateway:

IPTables: linux 2.4

IPChains: linux 2.2

IPFilter: *BSD

IPFW2: FreeBSD (patch)

Modos:

(1) Aceptar - Denegar

(2) Excluir - Incluir puertos

(3) Control de Ancho de Banda

(1), (1)+(2), (1)+(2)+(3)

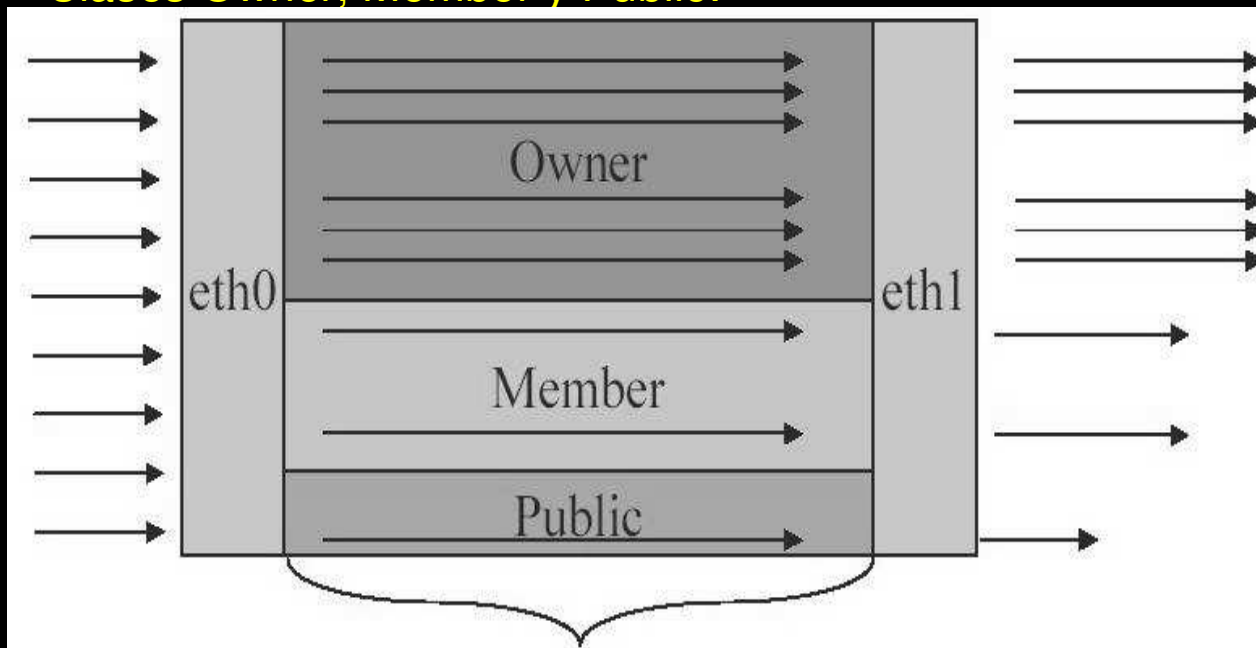
9-Software (IV)

NoCat Auth

Gestión del Ancho de Banda (QoS):

Class Based Queue
Clases Owner, Member y Public:

Paquetes
marcados
con la clase
del usuario



Propietario/s

Usuarios con
login pero no
son propietarios

Sin login (skip)
mínimo ancho de
banda. Guest

Los valores por defecto de NoCatAuth están en throttle.fw y son Owner=3mbit, Member=1mbit y Public=128kbit

9-Software (IV)

NoCat Auth

LO BUENO

- Autenticación (en modo Captive)
- Administración sencilla
- Traffic Shaping (QoS con CBQ)
- Fácil Acceso
- User Friendly: aprendizaje rápido y fácil para los usuarios.
- Bajo coste
- Software Libre: modificar según necesidades.

9-Software (IV)

NoCat Auth

LO MALO

- Comunicación no cifrada (por defecto).
- Implementar VPN: el cliente necesita software específico.
- Spoofing.

9-Software (V)

NoCat Auth

Necesidades del cliente

-Navegador (Mozilla, Netscape, Opera, Galeon, Konqueror o M\$IE).

- Independiente del SO

- No necesita plugins

- Opera en Zaurus no funciona

-Tarjeta wireless.

-Cuenta de acceso (para Captive mode).

9-Software (V)

NoCat Auth





Servicios de red y software necesarios:

- Servidor web (Apache)
- OpenSSL
- GnuPG
- Perl y modulos de perl correspondientes.
- Servidor DNS
- Servidor DHCP (en AP o en el GW)
- Servidor para centralizar cuentas de usuarios.


9-Software (VI)

NoCat Auth

¡Warchalking!

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid  bandwidth
WEP NODE	ssid access  bandwidth contact
NOCAT NODE	ssid  probability

blackbeltjones.com/warchalking

KEY	SYMBOL
NoCatAuth Node	ssid  public bandwidth member bandwidth

Referencias

[Http://www.google.com](http://www.google.com)

<http://nocat.net>

<http://www.missl.cs.umd.edu/wireless/eaptls>

<http://www.cs.umd.edu/~mvanopst/8021x/howto>

<http://www.blackalchemy.to/Projects/fakeap/fake-ap.html>

<http://www.open1x.org>

<http://www.saunalahti.fi/~asokan/research/mitm.html>

<http://www.missl.cs.umd.edu/wireless/eaptls>

<http://www.airdefense.net/>

<http://gsyc.escet.urjc.es/actividades/ati-wifi-feb-2002/wifi-2up.pdf>

http://escert.upc.es/_se_cursos/Curso_Seguridad_WLAN_30h_v02.pdf

<http://www.ugr.es/Informatica/redes/CVI-UGR.pdf>

<http://www.gcr.tsc.upc.es/downloads%5Cdoctorado%5Cwlan.pdf>

<http://www.nwfusion.com/news/tech/2001/0924tech.html>



Preguntas ¿?



Gracias

**Autenticación e Integridad
en redes Wireless**

Toni dIF. Diaz
toni@madridwireless.net

<http://blyx.com>
<http://vklab.sinroot.net>
<http://madridwireless.net>

Se autoriza la copia o distribución por cualquier medio y la traducción a otros idiomas, siempre que se cite al autor y se incluya esta nota.

Para versiones más actualizadas del documento:
<http://blyx.com>