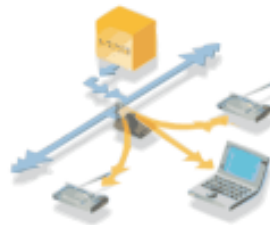


Seguridad en Redes WIRELESS Bajo Linux

Daniel Martínez Ponce dmartinez@bucomsec.com



Seguridad en **Wireless** bajo Linux



Conceptos

Introducción a las Redes Wireless

Redes Wireless: Comunicación sin cables.

Redes Wi-Fi (Wireless Fidelity): Formalmente el término Wi-Fi es aplicable a las redes inalámbricas 802.11b (2,45 Ghz) aunque actualmente se ha extendido abarcando a todas las revisiones 802.11x. Este término ha sido acuñado por la Wi-Fi Alliance.

Componentes principales:

STA: Cliente.

AP: Punto de Acceso.

Topologías de red:

Ad-Hoc (iBSS): Cliente – Cliente.

Infraestructura (BSS): Cliente – AP – Cliente.

Modos de actuación:

Ad-Hoc: Cliente en una red Ad-Hoc.

Managed: Cliente en una red tipo Infraestructura.

Master: Capacidad de algunos interfaces wi-fi para hacer de AP.

Monitor: Capacidad para monitorizar canales.

Típos de Redes Wi-Fi

802.11: Protocolo que proporciona de 1 a 2 Mbps en el rango de frecuencia 2.4GHz, usando: FHSS (Frequency Hopping Spread Spectrum) o DSSS (Direct Sequence Spread Spectrum).

802.11a: Revisión del protocolo 802.11 que proporciona 54 Mbps estandarizado y hasta 72 y 108 Mbps con tecnologías de desdoblamiento no estandarizado en el rango de frecuencia 5GHz, usando: OFDM (Orthogonal Frequency Division Multiplexing), DSSS (Direct Sequence Spread Spectrum).

802.11b: También llamado 802.11 High Rate o Wi-Fi, revisión del protocolo 802.11 que proporciona 11 Mbps con reducciones a 5.5, 2 y 1 Mbps en el rango de frecuencia 2.4 GHz, usando: DSSS (Direct Sequence Spread Spectrum).

802.11g: Protocolo que proporciona 54 Mbps en el rango de frecuencia 2.4 GHz, manteniendo plena compatibilidad con el protocolo 802.11b.

Estándares

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)

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.

Tabla Comparativa de Estándares WLAN

Estándar	Velocidad Máxima	Interface de Aire	Ancho de Banda de Canal	Frecuencia	Disponibilidad
802.11b	11 Mbps	DSSS	25 MHz	2,4 GHz	Ahora
802.11a	54 Mbps	OFDM	25 MHz	5,0 GHz	Ahora
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2,4 GHz	Ahora
HomeRF2	10 Mbps	FHSS	5 MHz	2,4 GHz	Ahora
HiperLAN2	54 Mbps	OFDM	25 MHz	5,0 GHz	Ahora
5-UP	108 Mbps	OFDM	50 MHz	5,0 GHz	Ahora

DSSS: Direct Sequence Spread Spectrum

OFDM: Orthogonal Frequency Division Multiplexing

FHSS: Frequency Hopping Spread Spectrum

5-UP: 5-GHz Unified Protocol (5-UP), Protocolo Unificado de 5 GHz propuesto por Atheros Communications

Terminología

WEP (Wired Equivalent Privacy): Es un protocolo de encriptación a nivel 2 para redes Wireless puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y hasta 256 (208 bits reales) que usan algunas marcas.

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

SKA (Shared Key Authentication):

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

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

SSID (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.



Recomendaciones

Recomendaciones (I)

Cuando hablamos de seguridad, en muchos casos, hablamos también de cierto grado de incomodidad tanto para los usuarios como para los administradores, incomodidad que hoy en día podría considerarse básica y necesaria debido al impulso social y económico que está recibiendo este sector de las comunicaciones.

Estudio de cobertura: Con el fin de radiar de una forma mas restrictiva sobre la localización deseada.

Configuraciones iniciales de STA's y AP's: Evitando configuraciones estandar de fabricante.

Política de actualización de firmwares: Realizando pruebas de funcionalidad en un entorno controlado antes de proceder a su implantación en el sistema en producción.

Política de actualización de drivers: Tanto aquellos proporcionados por el fabricante como los driver desarrollados por terceras personas como HostAP, OrinocoCS, Prism54, Madwifi, etc.

Revisión periódica del estado de los nodos: por si alguno de ellos está bloqueado o no da servicio, esto facilitaría una suplantación de nodo por parte de un atacante.

Recomendaciones (II)

Uso del protocolo de encriptación WEP: Como nivel base de seguridad y complementario a posteriores mecanismos de prevención de intrusiones debido a la fragilidad de dicho protocolo. Se recomienda a su vez una política de cambio periódico de la clave WEP. *(necesarios al menos 200 MB de tráfico o 500.000 paquetes encriptados para romper la encriptación)*

Uso de protocolos seguros en las comunicaciones:

Ssh en lugar de Telnet.

Smtps en lugar de Sntp.

Pops en lugar de Pop.

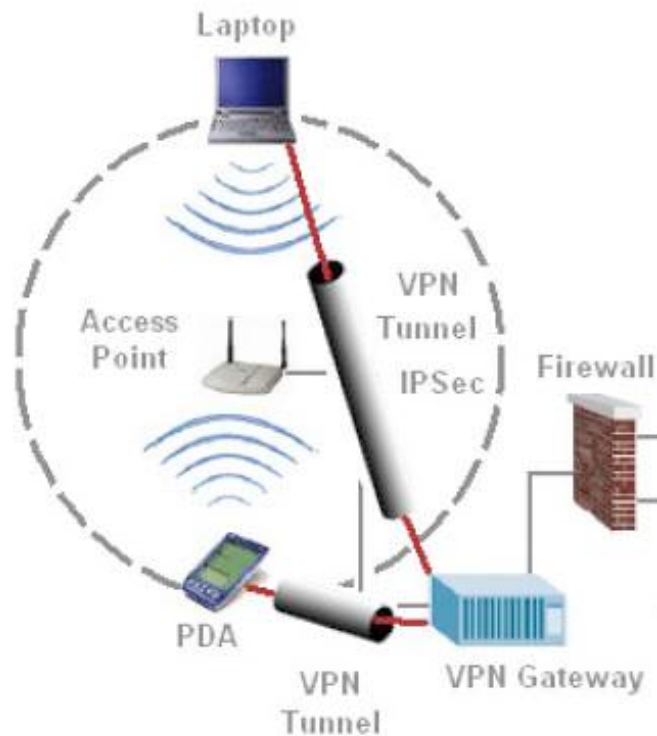
Imaps en lugar de Imap.

Https en lugar de http (páginas con autenticación).

<protocolo>s para todo aquel que lo soporte.

Recomendaciones (III)

Uso de Redes Privadas Virtuales (VPN):



OpenVPN.

vtund.

vpnd.

Freeswan.

CIPE.

IPSec (sin enrutamiento dinámico).

Recomendaciones (IV)

Monización y control de la red: Para no tener nunca la duda de estar sufriendo un posible ataque, es recomendable disponer de una maquina actuando como monitor de red wireless, con herramientas de detección y análisis de tráfico con las que poder hacer comparativas y evitar posibles intrusiones.

Análisis de solapamiento de redes: Para verificar que nuestro diseño de cobertura no se ve dañado por las emisiones radioeléctricas de nuevas redes y de esta forma poder realizar si fuera necesario reajustes en nuestro diseño de cobertura.

Herramientas y Técnicas de Suplantación



Técnicas de Suplantación

Las comunicaciones a través de medios inalámbricos, en concreto 802.11b, presentan un elevado número de deficiencias de seguridad intrínsecas al protocolo así como al medio en el que se realizan las comunicaciones.

Esta es la razón fundamental por la que es posible ejecutar una serie de ataques que hoy en día, en redes cableadas, serían prácticamente imposibles de realizar. Como por ejemplo los ataques DoS (Denegación de servicio).

Un ataque DoS puede tener muchos objetivos pero siempre hay uno común que es el de tratar de inhabilitar la conexión de los diferentes nodos integrantes de la red.

Si un DoS se realiza de forma distribuida se llegaría a lo que se define como inhabilitación del servicio de red.

Creación de Nuevos Nodos de Acceso

Configuraciones aleatorias: Este tipo de ataque implica una modificación en la estructura de red y en su funcionamiento normal. Esto puede derivar en la asociación por parte de los diferentes clientes a estos nuevos nodos siempre y cuando las configuraciones de estos clientes estuvieran realizadas con las opciones por defecto. Particularizando, si el identificador de red (ssid) no es especificado en los clientes, estos se asociarían a aquel nodo de acceso que ofrezca una mejor calidad de señal, esto se deriva en que los diferentes clientes son apartados del marco normal de funcionamiento de la red y se produciría de esta forma una DoS.

Configuraciones similares a los ya existentes: Con este tipo de ataque es posible realizar una modificación real de la estructura de red desplegada, a efecto de la red es totalmente transparente debido a que esta seguirá manteniendo su funcionamiento normal, mientras que los diferentes clientes (a pesar de tener configuraciones específicas) sufrirían una modificación en cuanto a lo que al nodo de acceso se refiere.

La repercusión de ambos ataques en caso de ser efectivos conllevaría a una conexión y desconexión continua de los diferentes clientes de la red, produciendo el DoS en los clientes.

Suplantación de Nodos en la Red (I)

Mediante suplantación de dirección mac e identificador de red: Con esto el atacante consigue anular un nodo en concreto, y asumir todas las conexiones de los clientes que tenía asociados. El cliente al estar asociado al nodo intruso, no puede efectuar ninguna petición de servicio válida y con ello el atacante conseguiría el DoS.

Denegación de servicio a nivel radio: Este tipo de denegación se basa en el anterior, pero en vez de dejar el nodo intruso levantado, mediante un script, se inician y paran sus servicios cada segundo, con ello se consigue, que nunca se llegue a realizar la negociación de enlace entre el dispositivo cliente y el nodo.

Denegación de servicio mediante enlaces dinámicos a otros nodos: Esta denegación se basa en los métodos anteriores expuestos, consiste en una modificación dinámica de la dirección mac del nodo intruso en base a las direcciones mac asignadas a los nodos reales o clientes de la red, manteniéndose activa cada una de ellas el tiempo necesario para que el dispositivo cliente enlace y desenchace con cada uno de las direcciones ficticias que se van generando. Esto es un ataque distribuido desde un punto, y el resultado final es que el nodo ficticio asumirá todas las conexiones clientes de los nodos, no como en los ataques anteriores que afectaban solo a los clientes de un nodo.

Suplantación de Nodos en la Red (II)

Man in the middle: Es uno de los ataques DoS más efectivos por ser bastante complicado de detectar. Consiste en suplantar a un cliente y a un nodo de forma simultánea, de tal forma que todo el tráfico entre el cliente y el nodo real pase primero por el nodo intruso. Al pasar todo este tráfico por un punto ficticio intermedio este salto es totalmente transparente para la red. La repercusión del ataque “man in the middle” es robar o corromper la información, para conseguir un DoS parcial ó total, ocultando la identidad del atacante através de uno de los nodos reales de la red inalámbrica.

Sobre la realización de un “man in the middle” se puede aplicar un ataque de disociación de tramas, que consiste en modificar algunos de los parámetros de la negociación del protocolo y de esta forma, generar tráfico erróneo para producir un error en el hardware del nodo, de un dispositivo cliente concreto o de todos los clientes asociados al nodo.

Herramientas

Existen diversas herramientas para Linux que permiten realizar estos ataques y algunos más:

Airsnort: Herramienta de detección de redes wireless, dispone de una opción para descriptar el algoritmo WEP.

Air Jack: Driver utilizado para gestionar diversas utilidades de seguridad: wlan-jack, essid-jack, monkey-jack, kracker-jack.

Airsnarf: Genera Aps falsos posibilitando la apropiación de información confidencial, passwd de autenticación, etc. Ideal para romper la seguridad de hotspots.

Fake AP : FakeAP es un script en perl que permite enviar beacons frames con diferentes ESSIDs y diferentes direcciones MACs a la red. De esta forma posibilita la generación de un alto número de redes wireless falsas en cuestión de minutos.

Monitorización y Control



Monitorización y Control

En cualquier red wireless, al igual que en cualquier red ethernet convencional, es necesario llevar una monitorización y control periódico del estado de la red.

En entornos wireless habría que realizar dos diferenciaciones:

- ❖ **Monitorización y control de red:** Análisis de la cantidad de tráfico, tipo de protocolos, direcciones origen/destino, etc.
- ❖ **Monitorización y control a nivel radio:** Análisis del espectro radioeléctrico en el que se encuentren alojadas nuestras comunicaciones.



Monitorización y Control de Redes (I)

En esta sección utilizaremos analizadores específicos de tráfico tales como TCPDUMP, IPTRAF, ETHEREAL, etc. Este último, bastante práctico, ya que reconoce el tráfico generado en las redes wireless diferenciando entre diversos protocolos como puedan ser WEP, WPA, etc.

Dicha monitorización se contrastaría con muestreos MRTG para poder realizar gráficas comparativas.

The screenshot shows the Ethereal network analyzer interface. The top pane displays a list of captured packets with columns for No., Time, Source, Src Port, Destination, Dst Port, Protocol, and Info. The bottom pane shows a detailed view of a selected packet, including its sequence length, profile ID, endianness, and various flags.

No.	Time	Source	src port	Destination	dst port	Protocol	Info
11	0.013301	craig.laptop	1029	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 LocateRequest 1
13	0.020141	craig.laptop	12345	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 LocateReply 1
15	0.020366	craig.laptop	1029	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Request 2 (two-usage): bind_new_context
17	0.020546	craig.laptop	12345	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Reply 2: No Exception
18	0.020379	craig.laptop	1029	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 LocateRequest 3
19	0.027152	craig.laptop	12345	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 LocateReply 3
20	0.027305	craig.laptop	1029	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Request 4 (two-usage): bind
21	0.028488	craig.laptop	12345	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Reply 4: No Exception
22	0.028773	craig.laptop	1029	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Request 5 (two-usage): bind_new_context
23	0.031111	craig.laptop	12345	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Reply 5: No Exception
24	0.031346	craig.laptop	1029	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 LocateRequest 5
25	0.031481	craig.laptop	12345	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 LocateReply 6
26	0.031613	craig.laptop	1029	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Request 7 (two-usage): bind
28	0.032002	craig.laptop	12345	craig.laptop	127.0.0.1	OSNMWING	GIOP 1.0 Reply 7: No Exception
33	26.212009	craig.laptop	1030	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 Request 1 (two-usage): get
35	26.212363	craig.laptop	12345	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 Reply 1: No Exception
40	26.214951	craig.laptop	1031	craig.laptop	127.0.0.1	GIOP	GIOP 1.0 LocateRequest 1

Packet 23 details:

- Sequence Length: 1
- Profile ID: 166_INTERNET_LOP (0)
- Sequence Length: 30
- Endianness: Little Endian (1)
- IIOP Major Version: 1
- IIOP Minor Version: 0
- String Length: 10
- IIOP:Profile_host: 127.0.0.1
- IIOP:Profile_port: 12345
- Sequence Length: 6
- Object Key 9:....

Monitorización y Control de Redes (II)

Es recomendable utilizar analizadores de tráfico específicos para redes wireless.

En sistemas Linux uno de los más recomendables es AIRTRAF, éste no sólo monitoriza tráfico sino que permite la selección de un punto de acceso específico sobre cualquier red wireless para su monitorización.

```
AirTraf: 0.4.0 '02
- Statistics for eth0

BSSID: 00022d28dc25  SSID: MaveLAN Network  WEP: opensystem  CHANNEL: 8

Management Frames:
Beacon: 2456
Disassoc: 0
Other: 12
Total Packets: 2468
Total Bytes: 167752
Bandwidth: 5.44 Kbps

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

Data Frames:
External Packets: 22924
External Bytes: 3363679
Internal Packets: 141479
Internal Bytes: 16413129
Total Packets: 164403
Total Bytes: 20376708
Bandwidth: 0.1160 Mbps

Corrupt Frames: (count) (bytes)
Bad MAC addr: 0 0
Bad IP checksum: 688 79808
FCS error: 0 0
Filtered data: 41 4872
Overall: 729 84680

OVERALL ACTIVITY:
Total Packets: 165871
Total Bytes: 20544460
Bandwidth: 0.1215 Mbps

Link Quality Analysis:
Link Utilization: 1.10 %
Background Noise: 95.52 %
Packet Loss: 0.41 %

Connected Nodes
MAC address 0: 00022d28dc25 - AP  IP: (Unknown)
incoming packets: 0 outgoing packets: 2468
incoming bytes: 0 outgoing bytes: 167752
avg_signal strength: 210.37
Bandwidth: 0.0054 Mbps

MAC address 1: 00022d0040e5 - STA  IP: (192.168.239.210)
incoming packets: 72224 outgoing packets: 69267
incoming bytes: 8378333 outgoing bytes: 8035540
avg_signal strength: 203.87
Bandwidth: 0.0000 Mbps

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
Active
```

Monitorización y Control a Nivel Radio

Para realizar este análisis utilizaremos herramientas específicas en entornos wireless tales como AirSnort, Netstumbler, Kismet, etc.

Son las herramientas utilizadas normalmente en “wardriving” pero también pueden ser muy útiles a la hora de monitorizar el estado de los puntos de acceso de una red wireless:

- ❖ Verificar la activación de WEP, WPA.
- ❖ Uniformidad de los ESSID.
- ❖ Detección de nodos suplantados.
- ❖ Etc.

Todos los logs de registro creados con estas herramientas podrán ser útiles a la hora de realizar análisis forense en caso de “desastre” en nuestra red de comunicaciones.

Herramientas de Control Adicionales

Como medida de seguridad y herramienta de monitorización y control adicional, a parte de los firewalls respectivos de una red ethernet tradicional, se recomienda la utilización de un firewall en el punto de comunicación con la red wireless, con su correspondiente IDS para la monitorización del tráfico generado.

Entre la diversas herramientas podemos destacar para entornos Linux:

SNORT+Parche actualización wireless: Tradicional IDS de redes ethernet con un módulo de ampliación para redes wireless ya disponible.

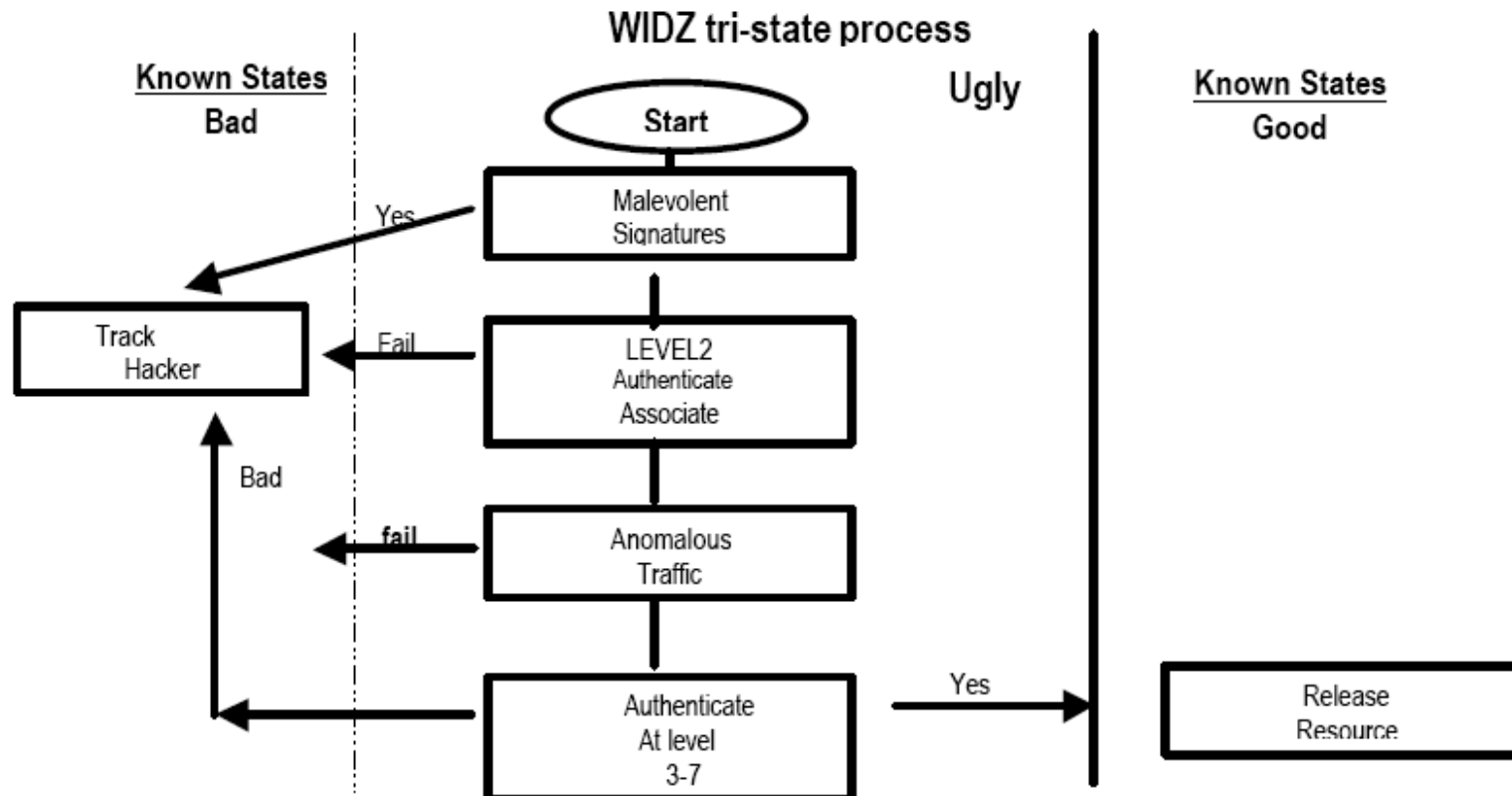
AirShang: 802.11 IDS que basa su monitorización en direcciones MAC.

Widz: 802.11 IDS que en su ultima versión es capaz de detectar AP's falsos, Monkey-Jacks, Flouds entre otros e incorpora una "Mac Black-List" es uno de los mas completos ya que no basa su funcionamiento solo en las direcciones MAC.

Wids: 802.11 IDS no implementa todas las opciones de Widz pero es una alternativa muy fiable.

Dentro de los IDS comerciales podemos mencionar Isohair, red-m y airdefence.

Diagrama de Estados del Software WIDZ



Diseño y Cobertura



Diseño de Cobertura

Prerrequisitos para un correcto diseño de cobertura:

- ❖ Caracterización de las necesidades.
- ❖ Diseño radio sobre plano acotado.
- ❖ Pruebas de radiación.

En Linux tenemos herramientas para realizar estudios reales de radiación, WAVEMON es una de ellas.

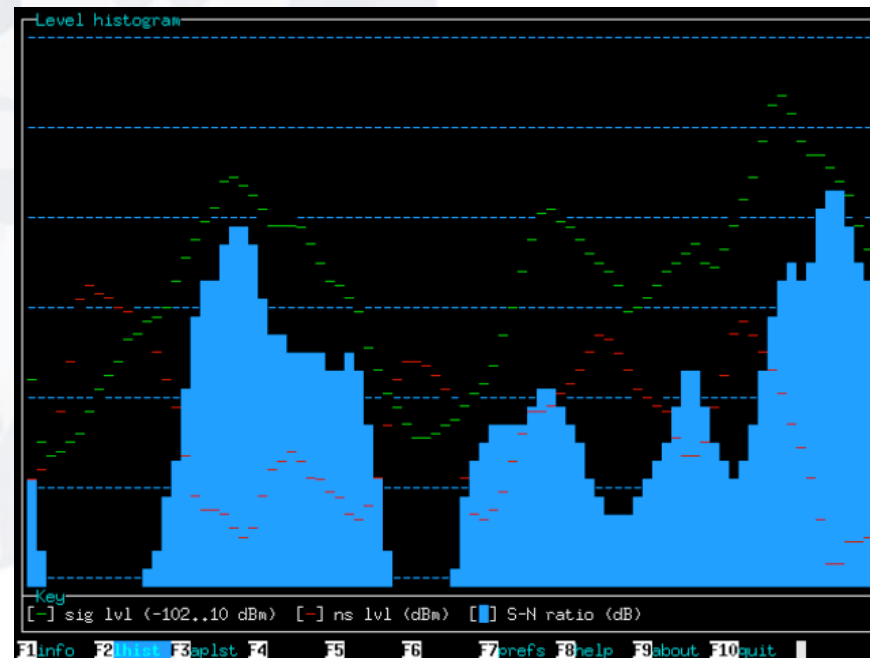
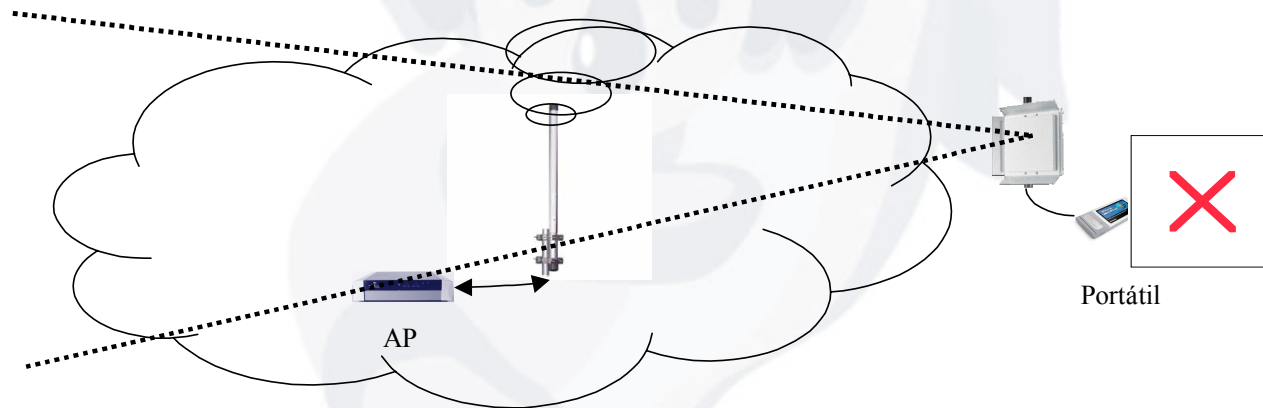


Diagrama de Radiación

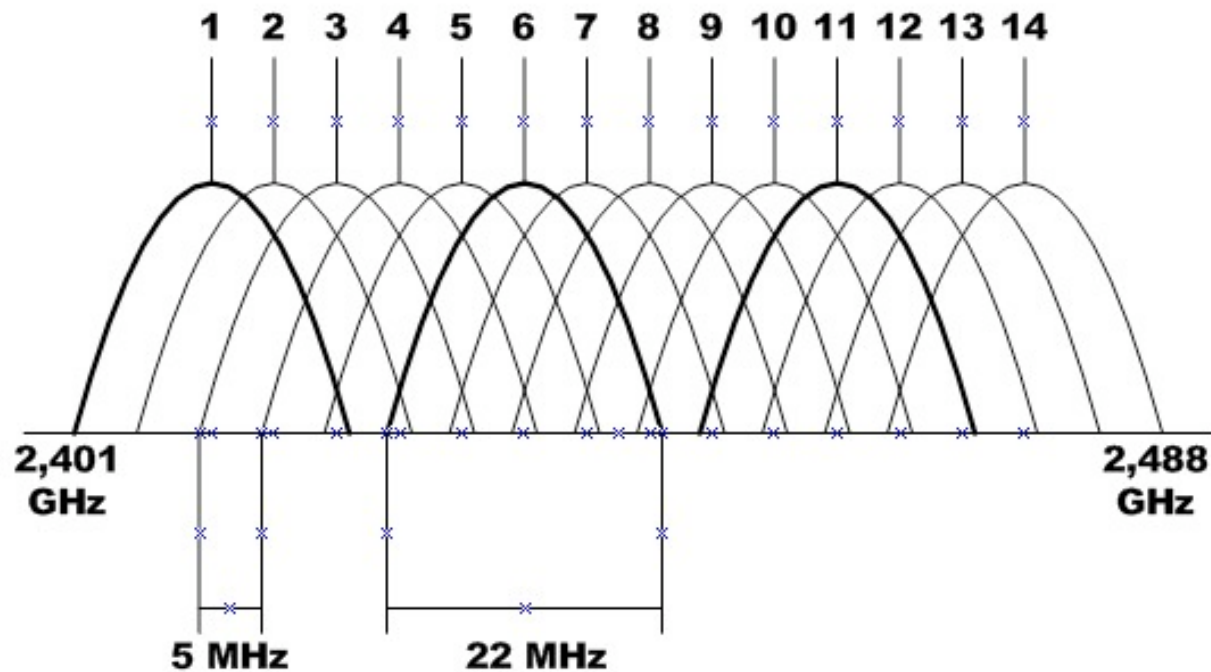
Con la herramienta Wavemon y una antena direccional es posible realizar estudios de cobertura mediante técnicas de triangulación.



Con una buena planificación y coordinación de este tipo de pruebas se puede realizar un buen estudio de cobertura sobre plano.

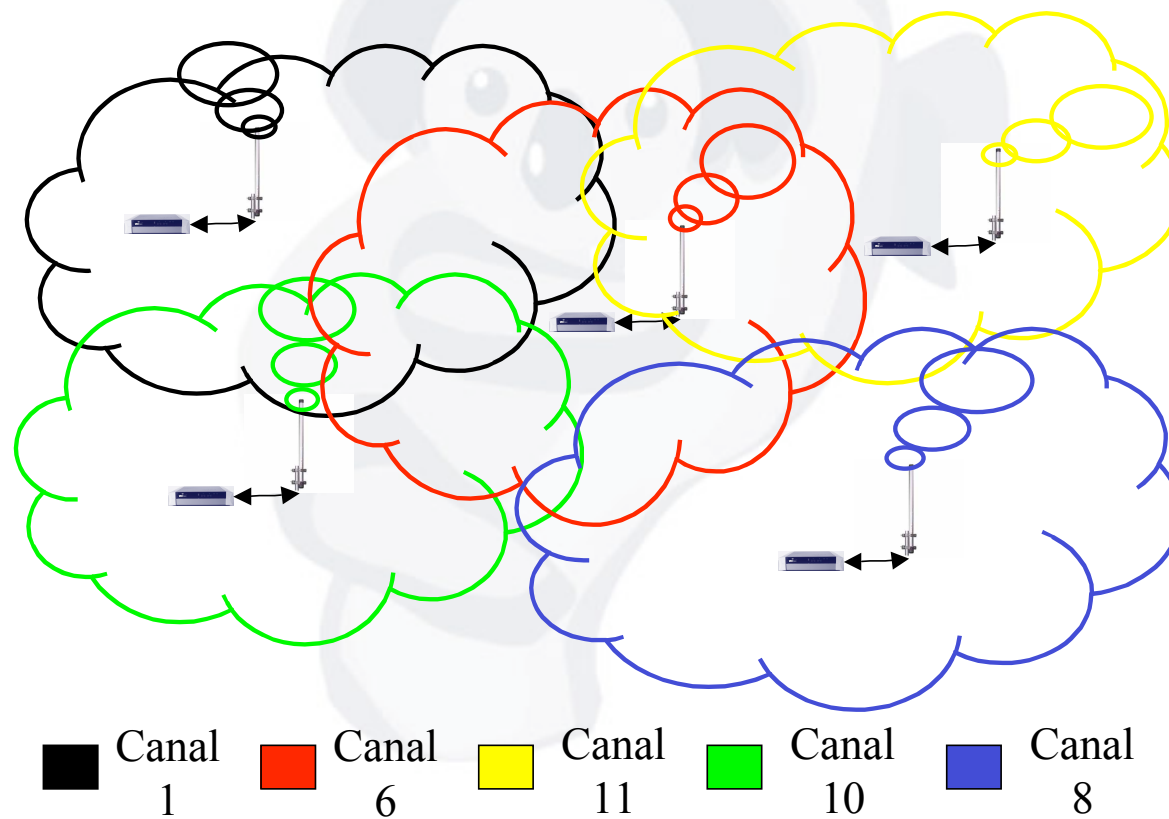
Solapamientos de Canal (I)

Una vez reflejadas sobre plano las zonas de radiación de cada uno de los Ap's se procederá a realizar un estudio de los solapamientos de canal sobre el terreno.



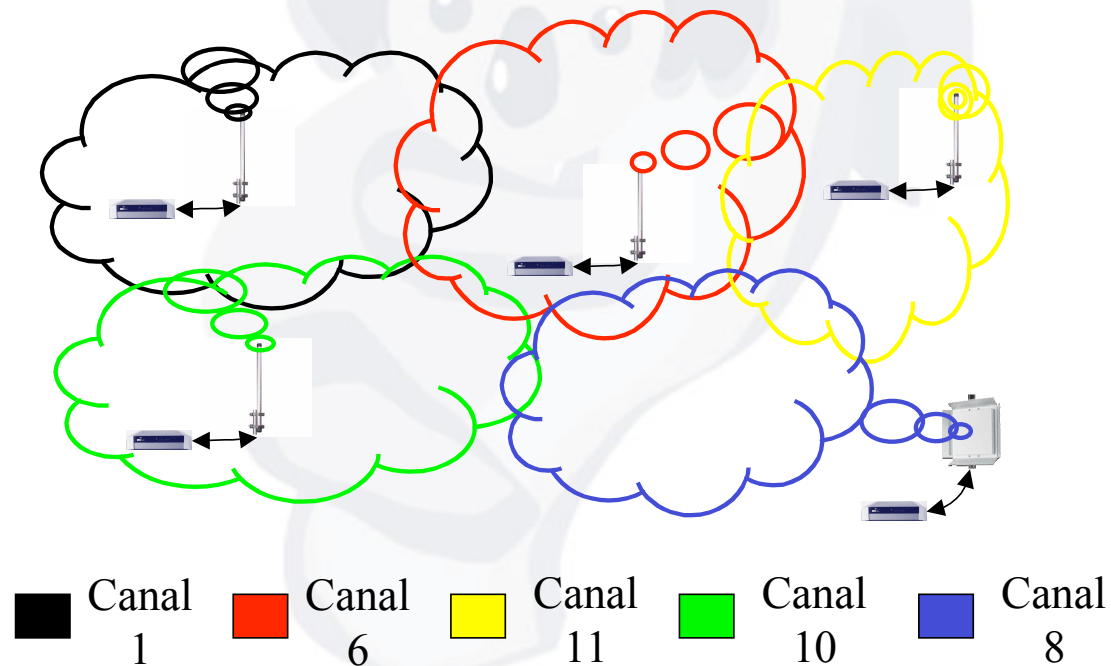
Solapamientos de Canal (II)

Con este estudio conseguiremos una idónea planificación de cobertura minimizando en la medida de lo posible la solapación entre canales.



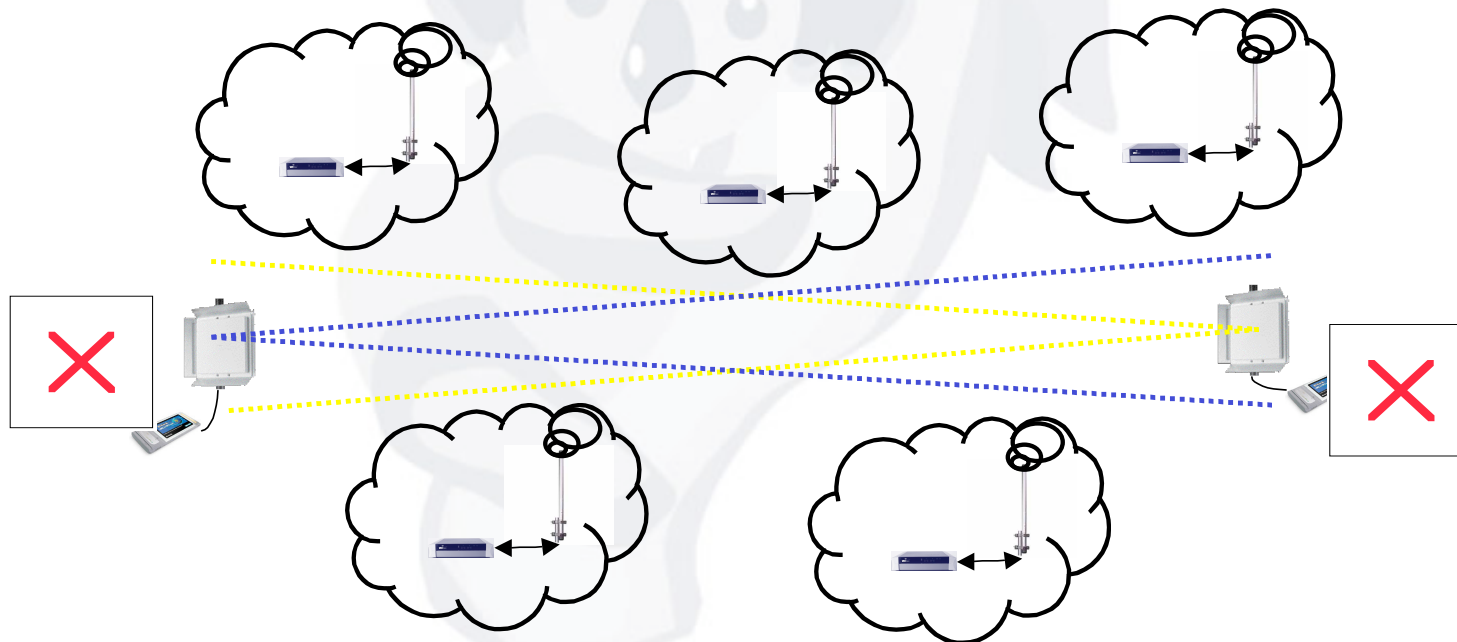
Ajuste de Radiación y Potencia

Una vez implantado el diseño de cobertura se procederá a realizar una revisión de potencia emitida, orientación de las antenas y ubicación de Ap's con el fin de ajustar en la medida de lo posible la radiación a la zona deseada.



Enlaces P2P

En el caso de realizar enlaces P2P se recomienda el uso de antenas lo más directivas posibles con el fin de evitar la radiación de señal sobre zonas no deseadas. De esta forma se minimiza las posibles interferencias y se aumenta la seguridad del sistema.



Autenticación



Autenticación, Autorización y Control de Acceso

Autenticación: Es el proceso por el que se verifica que una entidad es quien dice ser. Suele incluir unas credenciales (usuario/contraseña, certificados, tokens opacos, ...).

Autorización: Es el proceso de decidir si la entidad, una vez autenticada, tiene permiso para acceder al recurso. Se suele realizar comprobando pertenencias de usuarios a grupos, niveles o si dicha entidad pertenece a una lista de suscripción.

Control de Acceso: Es el proceso de conceder el permiso definitivo. Incluso una vez autorizado, un usuario puede tener restringido el permiso a partes del recurso, o un número de veces, o un intervalo de tiempo determinado. Con frecuencia se implementa usando ACLs (Listas de Control de Acceso) o máscaras.

Por regla general, los tres componentes suelen estar fuertemente entrelazados en un modelo de seguridad concreto.

Sistemas de Autenticación

En Linux se suele usar PAM, una implementación modular que permite adaptar un gran conjunto de métodos y bases de datos de autenticación:

- ❖ Ficheros (shadow) passwd, group
- ❖ HTTP (Basic, Digest)
- ❖ LDAP
- ❖ Dominio NT
- ❖ NIS
- ❖ Kerberos

Radius

Remote Authentication Dial In User Service

- ❖ Es un servicio (servidor) para autenticación remota, estándar de facto.
- ❖ Compatible con SNMP.
- ❖ Se compone de un servidor y un cliente.
- ❖ Admite varios tipos de bases de datos de contraseñas, y usar varios tipos de esquemas de autenticación, por ejemplo PAP y CHAP (se integra prácticamente con cualquier bbdd y SO).
- ❖ Algunos incorporan protección contra "sniffing" y ataques activos.
- ❖ Permite administración centralizada.
- ❖ La Autorización viene definida en el RFC 2865.
- ❖ Los servicios de Accounting están disponibles en el RFC 2866.

RSA

Con esta solución, válida para cualquier método de autenticación en Linux, podemos incrementar la seguridad, y facilitar a los administradores la implementación de políticas de seguridad.

RSA es un servidor de autenticación de doble factor integrable con Linux mediante pam, válido para utilizar con cualquier sistema de autenticación en Linux.

El servicio de autenticación “RSA secure id”, solo puede ser integrado, actualmente, sobre sistemas Windows y Unix.

Se prevé que en pocos meses RSA Security disponga de este servicio para sistemas Linux.



Key Fob

Versión más conocida de RSA (Token).

RSA Token

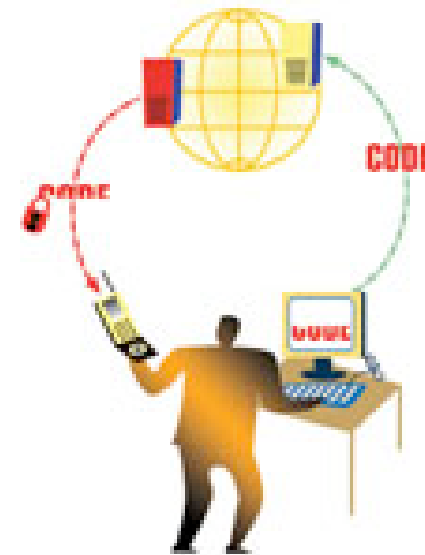
Los token también pueden funcionar con otros formato, como por ejemplo tarjetas tipo calculadora, por software en un pda o el móvil (muchos móviles actuales ya lo soportan).



Hardware Token



iPAQ Pocket PC
Software Token



Otros Sistemas de Autenticación

Por último podemos utilizar como sistema de autenticación, aunque no sea una autenticación real, el conocido port-knocking (apertura de puertos bajo demanda de petición.)

Consiste en realizar intentos de conexión mediante una secuencia de acceso a puertos predefinidos para que el sistema reconozca tu identidad y de esta forma active un perfil de reglas al firewall (iptables). De esta forma se garantizan accesos restringidos a servicios de máquinas concreta:

- ❖ Ssh
- ❖ Vpns
- ❖ Telnet

Una vez finalizada la sesión es posible cerrar los puertos previamente utilizados mediante una secuencia de terminación.

El demonio del sistema encargado de esto es Knockd.

Configuración de Knockd

```
#Abrir SSH
[openSSH]
sequence = 2222,3333,4444
protocol = tcp
timeout = 15
command = /usr/sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
#Cerrar SSH
[closeSSH]
sequence = 4444,3333,2222
protocol = tcp
timeout = 15
command = /usr/sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

Como se puede ver, esto es francamente útil para establecer conexiones en la administración de servidores.

Es posible crear scripts de apertura y cierre automático de puertos para usuarios de forma que el firewall modifique sus perfiles de reglas bajo demanda.



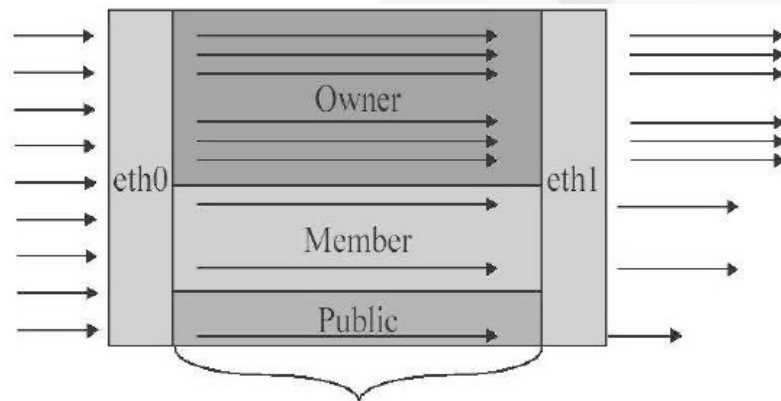
QoS

Calidad de Servicio

- ❖ Consiste en un conjunto de técnicas utilizadas para aumentar la eficiencia de las comunicaciones.
- ❖ Parte crítica de las redes de comunicaciones, tanto para el nivel de servicios de Internet como para el de intranet.
- ❖ Gestión de ancho de banda, caudal eficaz etc.
- ❖ Entre las diferentes técnicas conocidas de QoS destacan por su simplicidad y eficiencia los “Traffic Shapper” y la utilización de proxys (Squid) para diferentes tipos de servicios.

QoS (I) Implementación de NocatAuth

- ❖ Distinción de tres Class Based Queue (Clases Owner, Member y Public)
- ❖ Muy restrictiva.



Paquetes marcados con la clase del usuario

- 1.- Propietario/s
- 2.- Usuarios con login.
- 3.- Guest mínimo ancho de banda.
- 4.- Sin login (skip)

QoS (II) Configuración del Kernel

“Networking options - QoS and/or fair queueing” hay que activar las siguientes opciones:

- [*] QoS and/or fair queueing
- <*> CBQ packet scheduler
- <*> HTB packet scheduler
- <*> CSZ packet scheduler
- <*> The simplest PRIO pseudoscheduler
- <*> RED queue
- <*> SFQ queue
- <*> TEQL queue
- <*> TBF queue
- <*> GRED queue
- <*> Diffserv field marker
- <*> Ingress Qdisc
- [*] QoS support
- [*] Rate estimator
- [*] Packet classifier API
- <*> TC index classifier
- <*> Routing table based classifier
- <*> Firewall based classifier
- <*> U32 classifier
- <*> Special RSVP classifier
- <*> Special RSVP classifier for IPv6
- [*] Traffic policing (needed for in/egress)

QoS (III) Traffic Shapper

DOWNLINK=10000 → Valor mas bajo del teórico ancho de banda.

UPLINK=10000 → Lo mismo que con el download, pero ahora para upload.

DEV=wlan0 → Dispositivo de control.

NOPRIOHOSTSRC= → Hosts fuente a los que queremos dar una prioridad inferior.

NOPRIOHOSTDST= → Hosts destinos a los que queremos dar una prioridad inferior.

NOPRIOPORTSRC=4662 → Puertos fuente a los que queremos dar una prioridad inferior.

NOPRIOPORTSRC=21

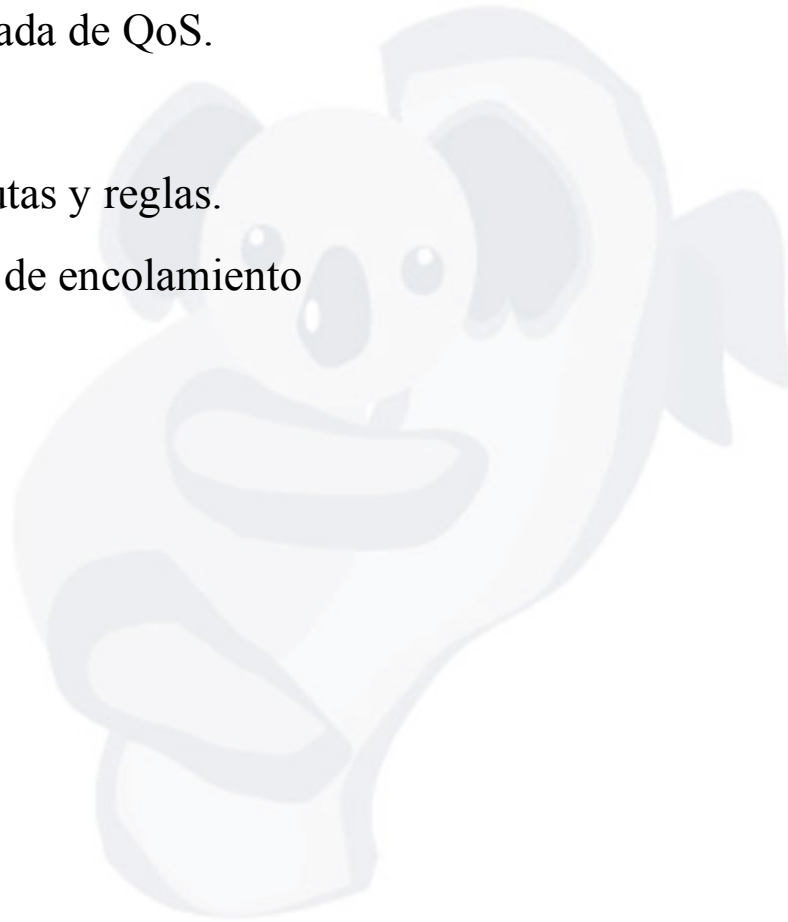
NOPRIOPORTSRC=80

NOPRIOPORTDST=4662 → Puertos destino a los que queremos dar una prioridad inferior.

NOPRIOPORTDST=20

NOPRIOPORTDST=21

QoS (IV)

- ❖ Configuración avanzada de QoS.
 - ❖ Herramienta IP.
 - ❖ Múltiples tablas de rutas y reglas.
 - ❖ Múltiples algoritmos de encolamiento
 - ❖ Etc.
- 

Aplicación Práctica (I)

Supongamos que queremos mantener las conexiones ssh sin cortes en la salida a Internet mediante una máquina con hostap, una línea adsl de 512kbps y realizando masquerading (iptables).

```
# Creación del árbol de clases
```

```
tc qdisc add dev eth1 root handle 1: htb default 20 # Por defecto toda la información irá a la banda 20
```

```
tc class add dev eth1 parent 1: classid 1:1 htb rate 512kbps ceil 512kbps
```

```
tc class add dev eth1 parent 1:1 classid 1:10 htb rate 300kbps ceil 512kbps
```

```
tc class add dev eth1 parent 1:1 classid 1:20 htb rate 200kbps ceil 512kbps prio 1 # Esta banda tiene menor prioridad y menor ancho de banda mínimo
```

```
# Asociación de colas con sfq
```

```
tc qdisc add dev eth1 parent 1:10 handle 10: sfq
```

```
tc qdisc add dev eth1 parent 1:20 handle 20: sfq
```

```
# Asociación de la marca 1 con la banda 10
```

```
tc filter add dev eth1 protocol ip parent 1: handle 1 fw classid 1:10
```

```
# Reglas de filtrado (se marca con un 1 los paquetes destinados a un ssh)
```

```
iptables -A FORWARD -i wlan0 -o eth1 -p tcp -dport 22 -t mangle -j MARK --set-mark 1
```

Aplicación Práctica (II)

Ampliación funcional para mldonkey:

```
tc filter add dev $DEV parent 1:0 protocol ip prio 10 u32 \  
match ip protocol 17 0xff \  
match ip sport 4666 0xffff \  
flowid 1:30
```

La razón de esta particularización es que los paquetes del mldonkey son demasiado pequeños y utiliza mucho tráfico udp por lo cual es mas difícil de controlar.



802.11i

¿Qué es 802.11i?

Standard de seguridad para redes 802.11 que surgió a raíz de las vulnerabilidades del 802.11b y será aplicable a redes 802.11a (54Mbps), 802.11b (11Mbps) y 802.11g (22Mbps).

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

WPA (Wi-Fi Protected Access) es una versión “pre-standard” de 802.11i que usa TKIP (Temporal Key Integrity Protocol) el cual soluciona los problemas de WEP (Wired Equivalent Privacy) incluyendo el uso de claves dinámicas.

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

Implica modificaciones en el firmware del actual hardware.

Probablemente se especifiquen modificaciones de hardware en el Standard para incluir **Advanced Encryption Standard (AES)** próxima generación de algoritmos criptográficos que sustituirá a DES y 3DES

Entendiendo 802.1x



Entendiendo 802.1x (I)

Es un mecanismo estándar para autenticar centralmente estaciones y usuarios.

Es un estándar abierto que soporta diferentes algoritmos de encriptación.

Se apoya en el protocolo de autenticación EAP (Extensible Authentication Protocol), aunque 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).

Entendiendo 802.1x (II)

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 EAPTTLs

Portales Cautivos



Portales Cautivos

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/>

Otros:

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

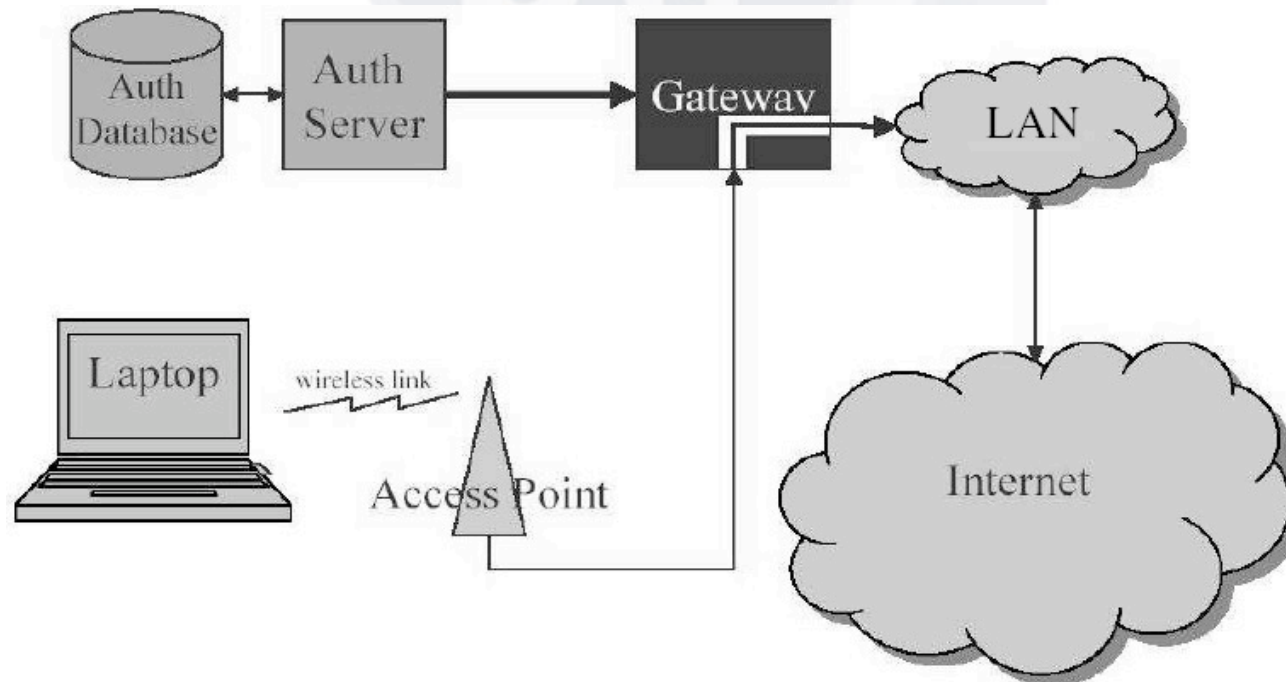
WARTA Proyect - www.hpi.net/whitepapers/warta/warta.pdf

-Autenticación, routing, QoS.

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

Funcionamiento

La mayoría de los portales cautivos implementan este diseño.



Avances en tecnologías inalámbricas



BROADBAND WIRELESS



Glosario

LAN: Local Area Network

MAN: Metropolitan Area Network

BWA: Broadband Wireless Access

SILS: Standard for Interoperable LAN/MAN Security”

SDE: Secure Data Exchange

KM: Key Management

PKM: Privacy Key Management Protocol

TEK: Traffic Encryption Key

Accesos Wireless de Banda Ancha

Los accesos Wireless de banda ancha (BWA) se han convertido en la opción más eficiente a la hora de implantar conectividad en el ámbito empresarial.

Los BWA permiten integrar una elevada variedad de servicios, tales como:

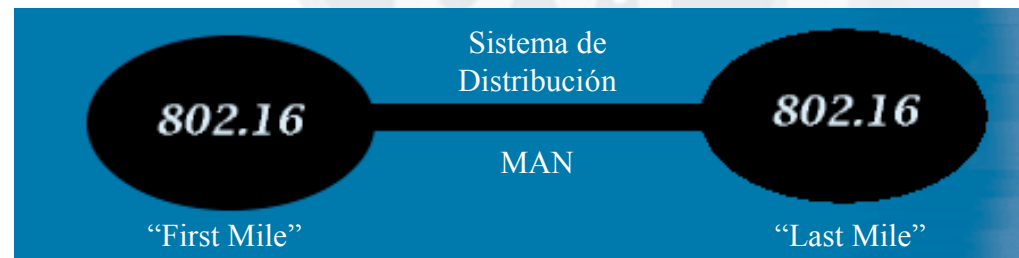
- ❖ Acceso a recursos locales / inet.
- ❖ Servicio integrado de datos/voz.
- ❖ Vídeo bajo demanda, etc.

Por otra parte los accesos WBA ofrecen un alto grado de escalabilidad y movilidad, siendo estas, características que convierten a este tipo de sistemas en un medio de comunicación ideal, permitiendo de esta forma extender de manera fiable y eficiente la conectividad ofrecida por otros medios que pudieran estar ya implantados:

- ❖ Sistemas opticos
- ❖ Sistemas XDSL
- ❖ ATM, FRAME RELAY, etc

IEEE 802.16 WirelessMAN (I)

802.16 es el standard desarrollado por el IEEE-SA en un intento por hacer más accesibles los accesos wireless de banda ancha (BWA).



En este standard el IEEE define una interfaz inalámbrica que entre sus diversas funcionalidades destaca la de poder crear enlaces metropolitanos (WirelessMAN).

IEEE 802.16 WirelessMAN (II)

802.16 especifica una interfaz inalámbrica (WirelessMAN-SC) dotada de un esquema de modulación basado en una única portadora (Single Carrier), diseñado inicialmente para operar en las bandas situadas entre 10 -66 GHz y posteriormente migrado también a las comprendidas entre 2 - 11 GHz.

Esta interfaz inalámbrica permite establecer comunicaciones con un ancho de banda de 10 MHz, siendo posible ofrecer una eficiencia espectral que garantiza flujos de varios cientos de Mbits.

802.16 está diseñado en base a las últimas técnicas de tratamiento digital, soporte simultáneo para FDD y TDD, modulación adaptativa, balanceo diferenciado de flujos, calidad de enlace y otras muchas características que permiten ajustar instantáneamente los esquemas de transmisión para obtener siempre la máxima eficiencia en la transferencia de datos.

El soporte de FDD permite la implantación de redes full-duplex celulares con un alto grado de escalabilidad, facilitando el crecimiento de las mismas de manera sencilla y progresiva.

IEEE 802.16 WirelessMAN (III)

802.16 debe su eficiencia a una meticulosa descripción de sus capas física y de acceso al medio, proporcionando esta última mecanismos para garantizar un alto grado de calidad de servicio (QoS) en la comunicación .

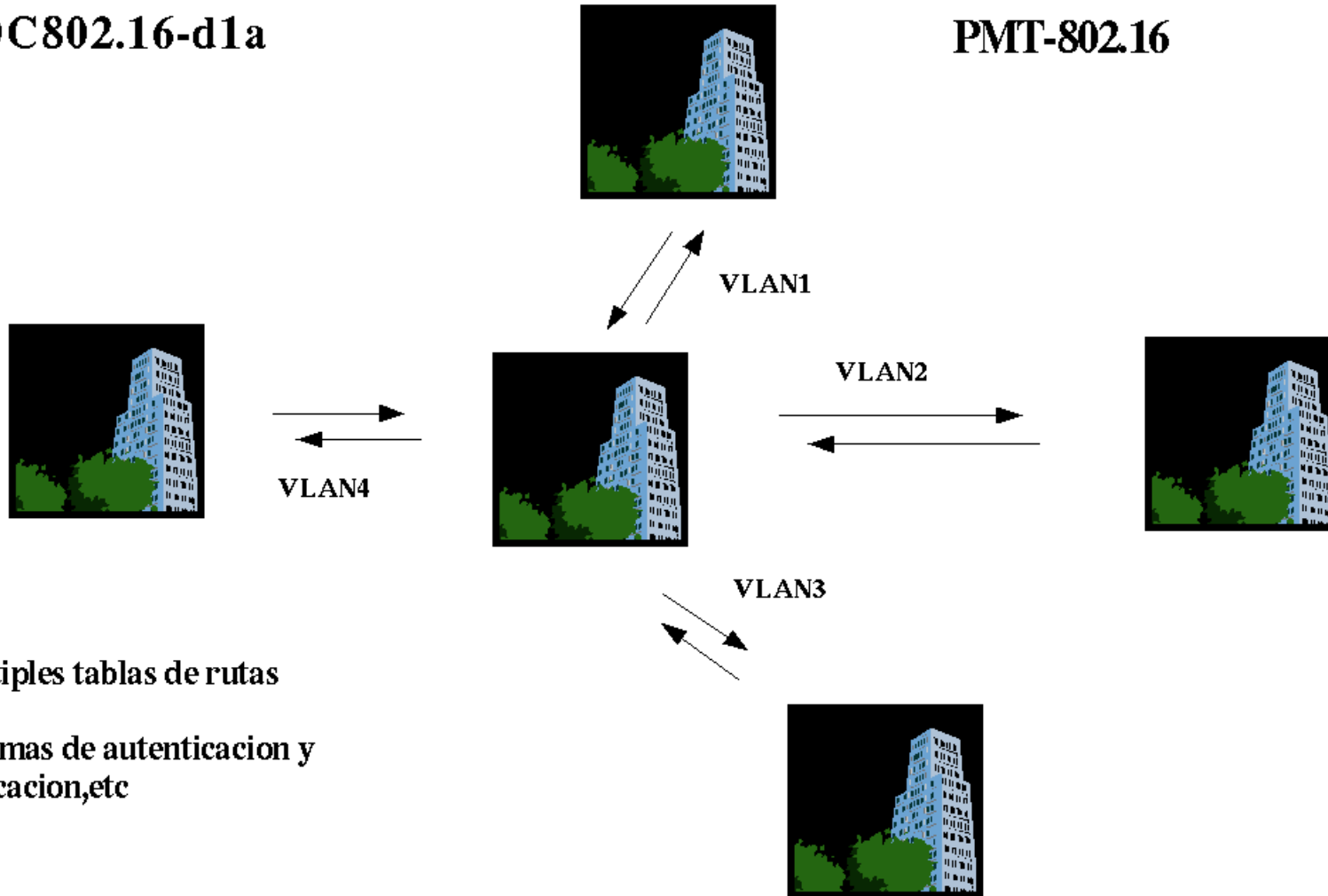
La última capa descrita en el protocolo (WirelessMAN-MAC) está definida de tal forma que permite acomodar fácilmente protocolos de niveles superiores así como diferentes servicios de voz-video asegurando en todo momento un total control sobre el flujo de datos cursado.

Los enlaces de 802.16 diseñados para operar en las bandas comprendidas entre los 2 y los 11 GHz no tienen necesidad de ser dotados de visión directa , y se caracterizan por tener rangos de cobertura cercanos a los 50 Km.

A su vez el protocolo ofrece diversos mecanismos para paliar los errores asociados a las transmisiones en el espacio libre facilitando de esta forma la posibilidad de implantación de múltiples enlaces punto - multipunto de banda ancha (PMP-BWA) y pudiendo asegurar en cada momento un mínimo BER (Bit Error Rate) asociado a las comunicaciones cursadas.

BWDC802.16-d1a

PMT-802.16



- Múltiples tablas de rutas
- QoS
- Sistemas de autenticación y tarificación, etc

MOBILE BROADBAND WIRELESS



802.16e Vs 802.20

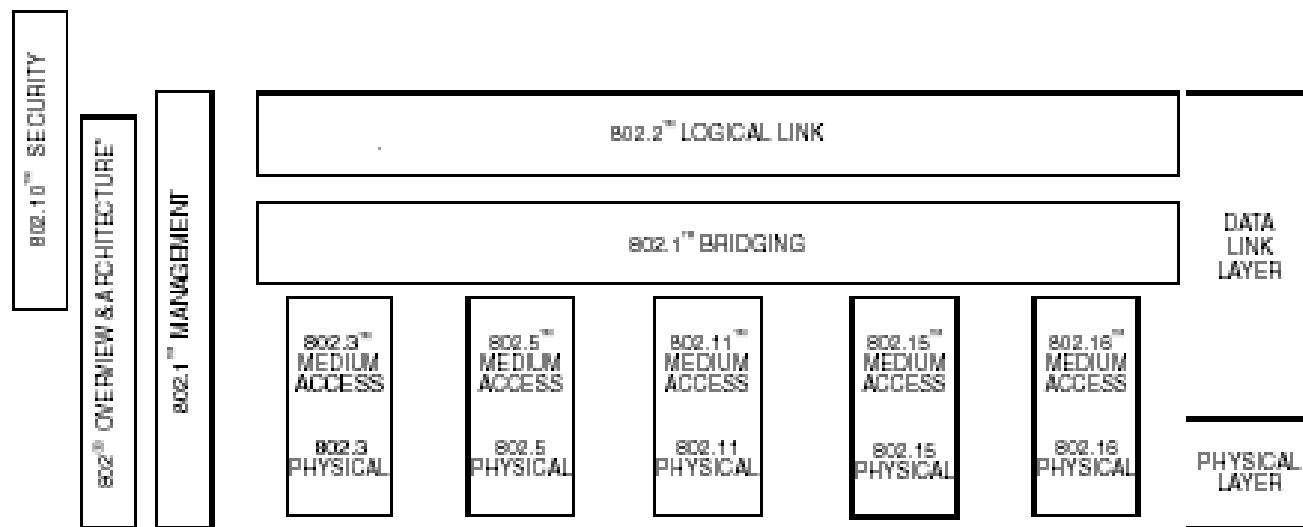
- ❖ Nuevas definiciones de la interface radio y enlace para accesos de banda ancha móviles.
- ❖ 802.16e opera en el rango de 2/6 GHz mientras que 802.20 lo hace por debajo de 3,5 GHz
- ❖ 802.16e es una evolución de 802.16a, mientras que 802.20 es un estándar desarrollado desde cero.
- ❖ 802.16e está actualmente aprobado por IEEE y aparecerá un draft a mediados del 2004 mientras que 802.20 se encuentra en desarrollo a día de hoy.
- ❖ 802.16e soportará clientes con velocidades entre 120 y 150 km/h, mientras que 802.20 soportará hasta 250 km/h, con células de unos 15 km.
- ❖ Ambos estándares son tecnológicamente muchos más evolucionados que la 3G móvil.

Niveles de Seguridad 802.16a



Niveles de Seguridad en 802.16a (I)

Como se muestra a continuación puede observarse que la arquitectura de protocolos que incorpora el estándar 802.16a.



* Formerly IEEE Std 802.1A™.

Niveles de Seguridad en 802.16a (II)

Como se muestra en la Figura 1.1, 802.16 basa su seguridad en el protocolo de comunicaciones 802.10, “Standard for Interoperable LAN/MAN Security” (SILS).

802.10 es un estándar desarrollado por el IEEE para proporcionar un nivel elevado de seguridad en los accesos a Redes de Área Local y Redes Metropolitanas. Este estándar incorpora funcionalidades tales como el intercambio seguro de datos (SDE), así como un sistema para el intercambio y control de claves (KM), siendo este totalmente independiente del sistema de intercambio de datos

Entre los diferentes servicios ofrecidos por el SDE se encuentran:

- ❖ Transparencia con respecto a otros niveles de jerarquía.
- ❖ Confidencialidad de datos.
- ❖ Integridad de las conexiones.
- ❖ Autenticación por origen de datos.
- ❖ Control de acceso.

Niveles de Seguridad en 802.16a (III)

El sistema de intercambio de datos en 802.16 se basa en un algoritmo de TEK's dinámicas siendo la negociación de estas realizadas por los diferentes nodos de la red y en base a periodos de tiempo predefinidos. A su vez el sistema de manejo de claves (KM) es implementado a través del protocolo PKM, este último basa su seguridad en la previa configuración de un conjunto de claves privadas.

Los niveles de seguridad anteriormente comentados PKM, TEK variaran en función de la complejidad y el tamaño de las claves que puedan ser preconfiguradas en los diferentes enlaces, dicho valor será definido en cada caso por las características particulares de cada fabricante y/o producto.

Diseños de radio seguros

WDS Inseguro o Muy Seguro



WIRELESS DISTRIBUTION SYSTEM

Drivers soportados por WDS

HostAP: Es el driver mas conocido por ser el primero que se desarrollo para poner las tarjetas en modo master

Doc de instalación en Madridwireless (<http://madridwireless.net/docs.shtml>)

HermesAP: Este driver no se puede utilizar con una simple orinoco (se ha hecho ingeniería inversa) para que fuera legal habría que utilizar la tarjeta interna de algún AP comercial de Lucent, entonces tendríamos licencia del driver.

Doc de instalación Mío ;) (<http://madridwireless.net/docs/hermesap/hermesap.html>)

PrimsGT:

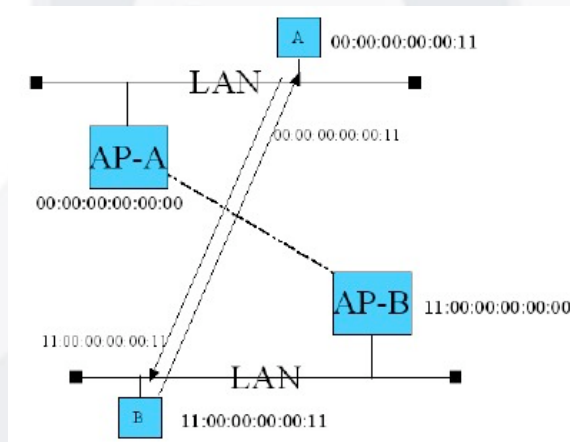
Doc de instalación del driver en Prism54 (<http://prism54.org>)

ETC.....

Diseño WDS (Mismo Canal)

Lo Bueno

- ❖ Difícil de rastrear al trabajar con 4 direcciones Mac .

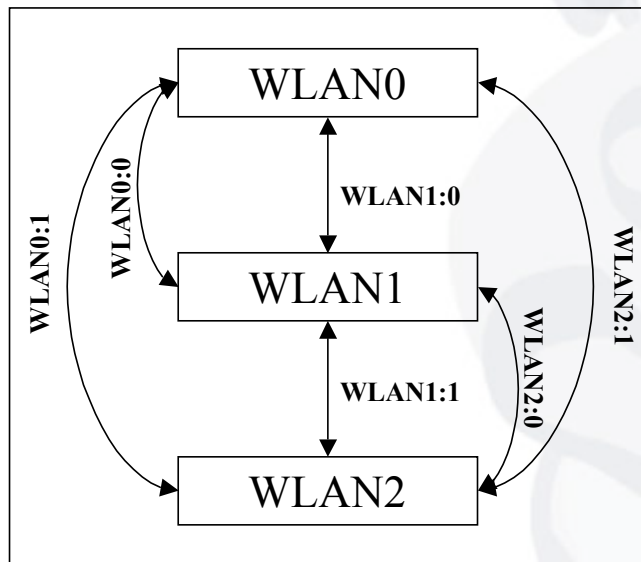


Lo Malo

- ❖ Porque se anuncia todo a toda la red.
- ❖ Denegación de servicio sobre un canal (se tira nube WDS entera).

Diseño WDS (Misma Máquina con 3 Canales)

Sobre una misma máquina montar con 3 tarjetas Wireless en modo master en 3 canales distintos, (más de tres generan ruido entre ellas) sobre estas 3 tarjetas se montan túneles WDS a nivel interno.



- ❖ Alta Disponibilidad
- ❖ Mas usuarios sobre un punto de acceso
(pruebas reales en una concentración 70-80 clientes sin perder servicio sobre un mismo nodo).
- ❖ Balanceo de carga sobre el punto de acceso

Diseño WDS (Misma Máquina con 3 Canales) Configuración (I)

```
# /etc/network/interfaces -- configuration file for
# ifup(8), ifdown(8)
# The loopback interface
auto lo
iface lo inet loopback

# The first network card - this entry was created
# during the Debian installation
# (network, broadcast and gateway are optional)
auto br0
iface br0 inet static
    address 10.64.2.5
    netmask 255.255.255.224
    network 10.64.2.0
    broadcast 10.64.2.31
    #gateway 192.168.0.1
    bridge_ports none
    bridge_stp on

auto eth0
iface eth0 inet static
    address 192.168.0.5
    netmask 255.255.255.224
    network 192.168.0.0
    broadcast 192.168.0.31
    gateway 192.168.0.3
```

Diseño WDS (Misma Máquina con 3 Canales) Configuración (II)

```
auto wlan0
iface wlan0 inet static
    address 10.64.2.5
    netmask 255.255.255.224
    network 10.64.2.0
    broadcast 10.64.2.31
    #gateway 192.168.0.3
    wireless_mode "Master"
    wireless_essid "BUCOMSEC"
    wireless_nick "BuKoBoX"

up ifconfig wlan0 0.0.0.0
up /usr/sbin/brcctl addif br0 wlan0
up iwpriv wlan0 wds_add 00:90:D1:08:19:28
up ifconfig wlan0wds0 0.0.0.0
#up prism2_param wlan0 autom_ap_wds 0
#up prism2_param wlan0 other_ap_policy 1
up /usr/sbin/brcctl addif br0 wlan0wds0
# down ifconfig wlan0wds0 down

up iwpriv wlan0 wds_add 00:02:6F:01:85:34
up ifconfig wlan0wds1 0.0.0.0
up prism2_param wlan0 autom_ap_wds 0
up prism2_param wlan0 other_ap_policy 1
up /usr/sbin/brcctl addif br0 wlan0wds1
# down ifconfig wlan0wds1 down
```

Diseño WDS (Misma Máquina con 3 Canales) Configuración (III)

```
auto wlan1
iface wlan1 inet static
    address 10.64.2.6
    netmask 255.255.255.224
    network 10.64.2.0
    broadcast 10.64.2.31
    #gateway 192.168.0.3
    wireless_mode "Master"
    wireless_essid "BUCOMSEC"
    wireless_nick "BuKoBoX"

up ifconfig wlan1 0.0.0.0
up /usr/sbin/brcctl addif br0 wlan1
up iwpriv wlan1 wds_add 00:90:D1:08:18:FA
up ifconfig wlan1wds0 0.0.0.0
#up prism2_param wlan1 autom_ap_wds 1
#up prism2_param wlan1 other_ap_policy 1
up /usr/sbin/brcctl addif br0 wlan1wds0
# down ifconfig wlan1wds0 down

up ifconfig wlan1 0.0.0.0
up /usr/sbin/brcctl addif br0 wlan1
up iwpriv wlan1 wds_add 00:02:6F:01:85:34
up ifconfig wlan1wds1 0.0.0.0
up prism2_param wlan1 autom_ap_wds 0
up prism2_param wlan1 other_ap_policy 1
up /usr/sbin/brcctl addif br0 wlan1wds1
# down ifconfig wlan1wds0 down
```

Diseño WDS (Misma Máquina con 3 Canales) Configuración (IV)

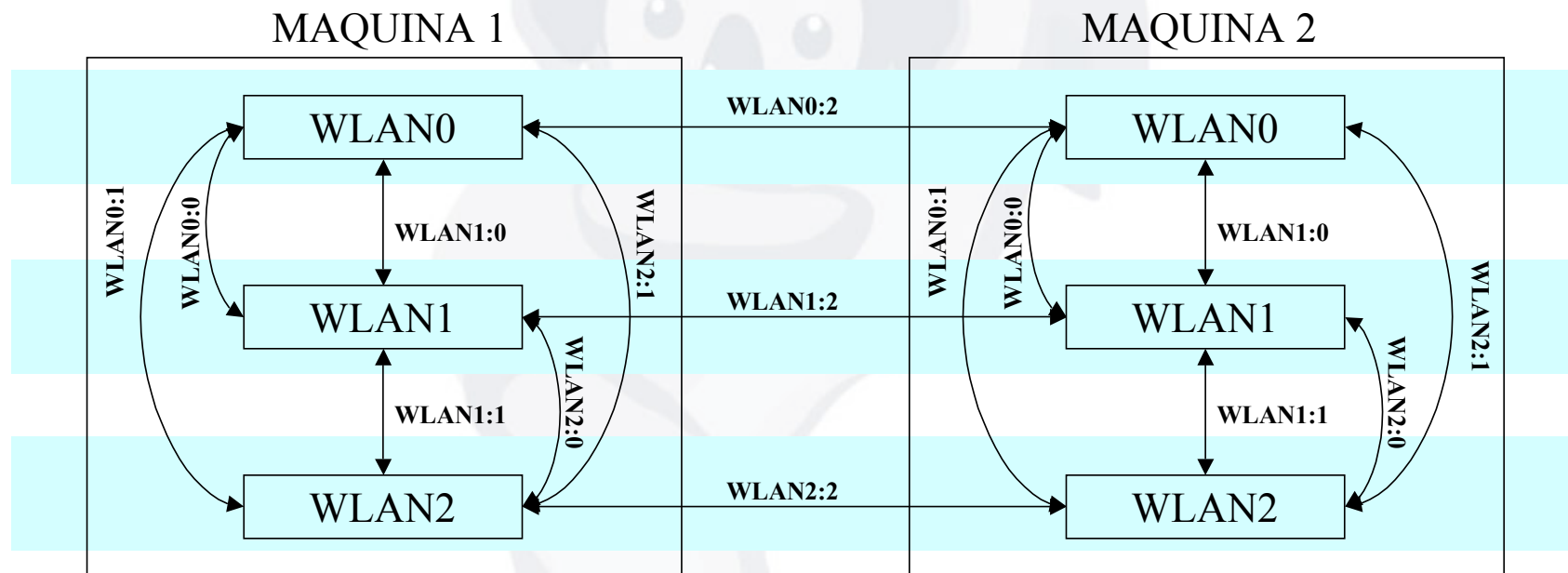
```
auto wlan2
iface wlan2 inet static
    address 10.64.2.7
    netmask 255.255.255.224
    network 10.64.2.0
    broadcast 10.64.2.31
    #gateway 192.168.0.3
    wireless_mode "Master"
    wireless_essid "BUCOMSEC"
    wireless_nick "BuKoBoX"

up ifconfig wlan2 0.0.0.0
up /usr/sbin/brcctl addif br0 wlan2
up iwpriv wlan2 wds_add 00:90:D1:08:18:FA
up ifconfig wlan2wds0 0.0.0.0
#up prism2_param wlan2 autom_ap_wds 0
#up prism2_param wlan2 other_ap_policy 1
up /usr/sbin/brcctl addif br0 wlan2wds0
# down ifconfig wlan2wds0 down

up ifconfig wlan2 0.0.0.0
up /usr/sbin/brcctl addif br0 wlan2
up iwpriv wlan2 wds_add 00:90:D1:08:19:28
up ifconfig wlan2wds1 0.0.0.0
up prism2_param wlan2 autom_ap_wds 0
up prism2_param wlan2 other_ap_policy 1
up /usr/sbin/brcctl addif br0 wlan2wds1
# down ifconfig wlan2wds0 down
```

Diseño WDS (2 Máquinas con 3 Canales) (I)

Si unimos varias máquinas con tres interfaces wireless se obtiene una alta disponibilidad.



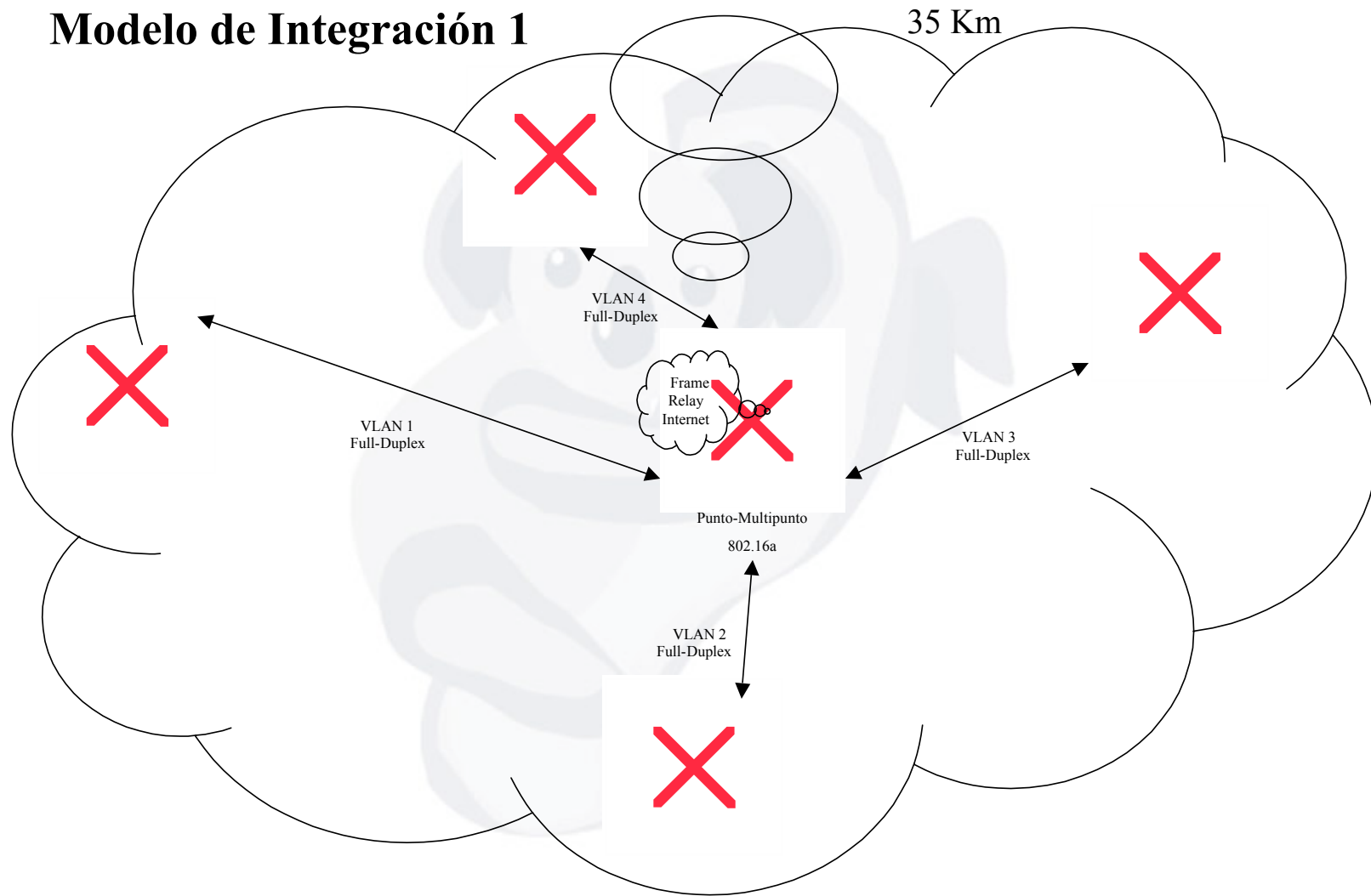
Diseño WDS (2 Máquinas con 3 Canales) (II)

- ❖ Dificultad a la hora de realizar una denegación.
- ❖ Para conseguir una DoS tendríamos que hacer un ataque distribuido a nivel radio.
- ❖ El seguimiento de las tramas de red capturando tráfico conlleva un análisis muy complejo llegando incluso a bloquear las herramientas de captura (usando este sistema AirTraf resistió tan solo 2 minutos).
- ❖ Balanceo de carga entre nodos, posible gracias al cambio de canales en los túneles WDS entre nodos.

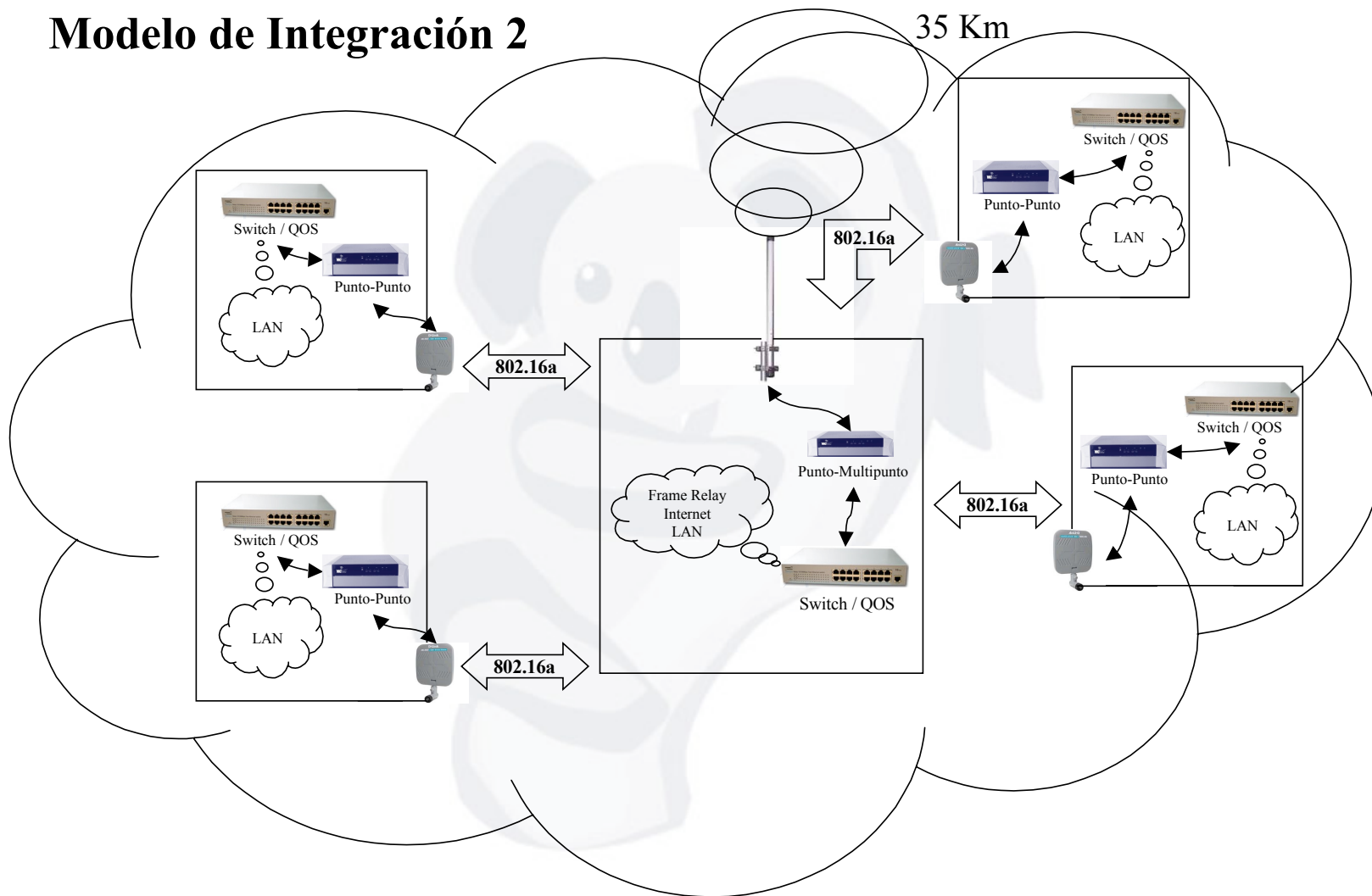
Integraciones Seguras de Redes Inalámbricas



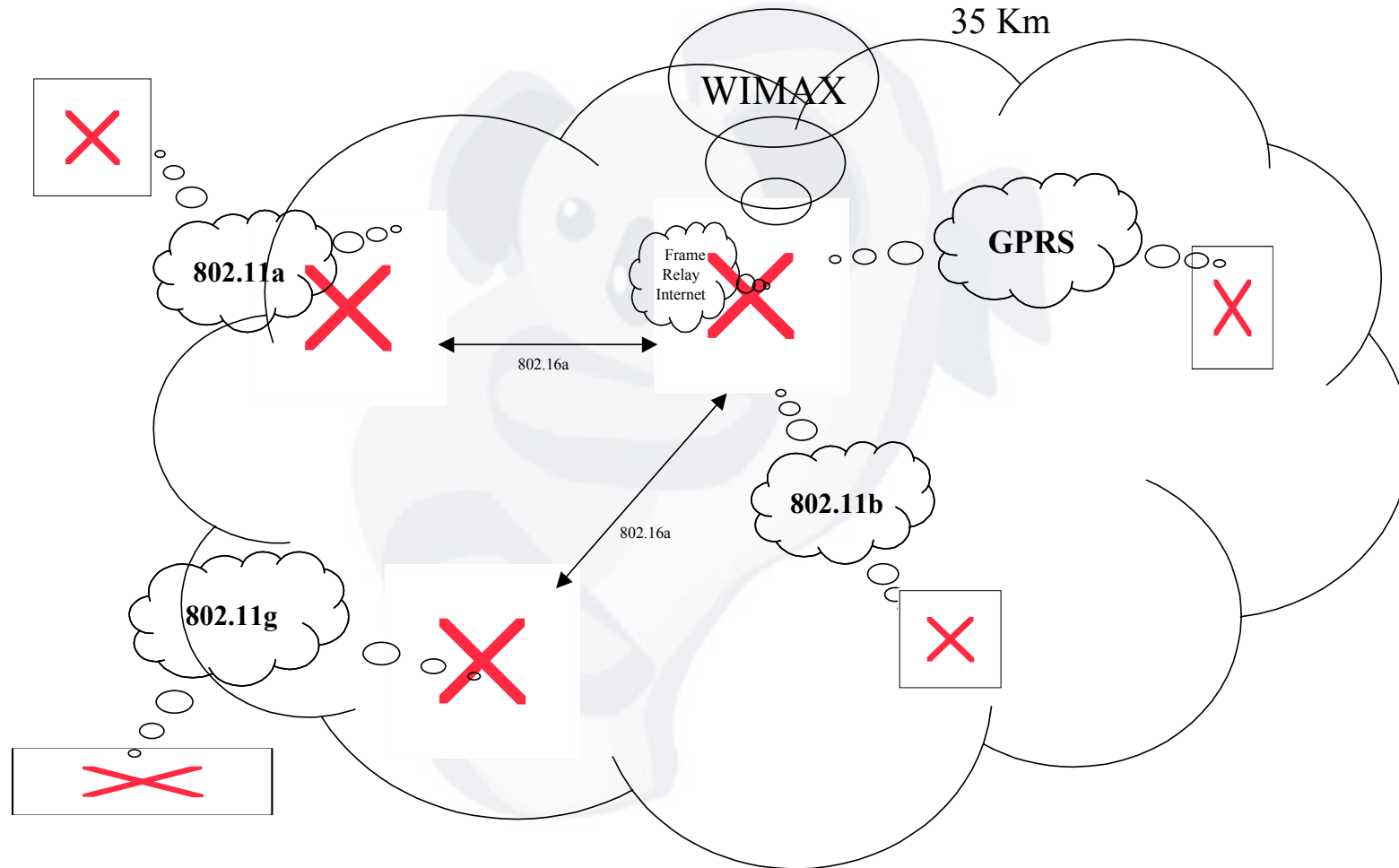
Modelo de Integración 1



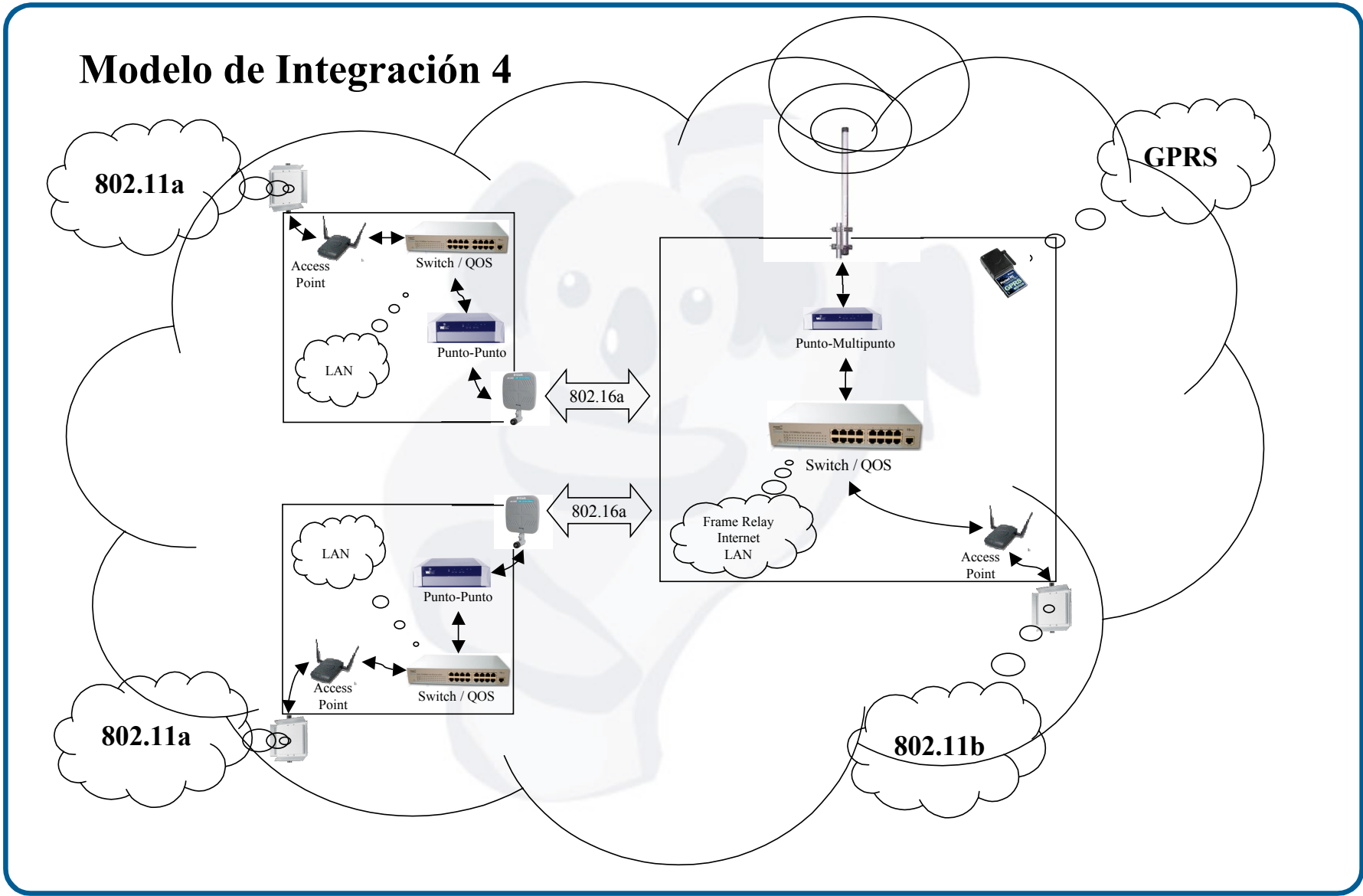
Modelo de Integración 2



Modelo de Integración 3



Modelo de Integración 4



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>

AGRADECIMIENTOS

SECO

Pablo Vaquero

Antonio de la Fuente

Víctor Fernández

Eduardo Martín

Público asistente

MUCHAS GRACIAS