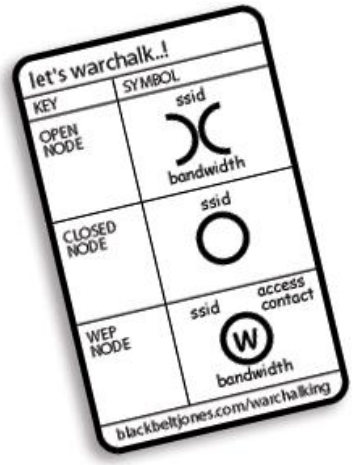
MUM
Argentina
September 7-8th, 2007

Seguridad de redes Inalámbricas



Eng. Wardner Maia

Introducción

MD Brasil – Tecnologia da Informação Ltda
→ Proveedor de Internet desde 1995
→ Redes Inalambricas desde 2000

MD Brasil – Telecomunicações Ltda
→ Sumnistra entrenamientos en Wireless desde 2002
→ Mayorista de Productos Mikrotik
→ Entrenamientos en Mikrotik desde 2007

Red Global Info
→ La más grande red de Proveedores de Brasil. Presente en más de 450 cidades.

Introducción

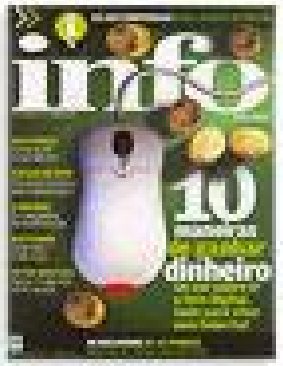
Público-alvo:

→ Proveedores de Servicio de Internet que hacen uso de tecnolgia de acceso inalámbrico fijo baseado en equipos Wi-Fi

Objetivos:

→Abordaje de los aspectos teóricos de seguridad inalámbrica
→Analisis Crítico de los actuales modelos empleados por Proveedores
→Maneras de emplear WPA2-TLS con RouterOS para garantizar la Seguridad
→Ataques de capa 2 e el reto de proteger contra tal tipo de ataques

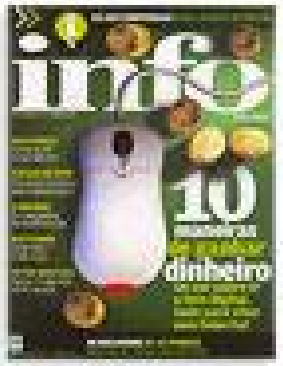
“El poder de las patatas”



Entre 43 redes inalámbricas situadas en la región financiera más importante en Sao Paulo, solamente 8 tenían las configuraciones "recomendadas" de seguridad.

IT Magazine - Info Exame
Articulo publicado en 2002

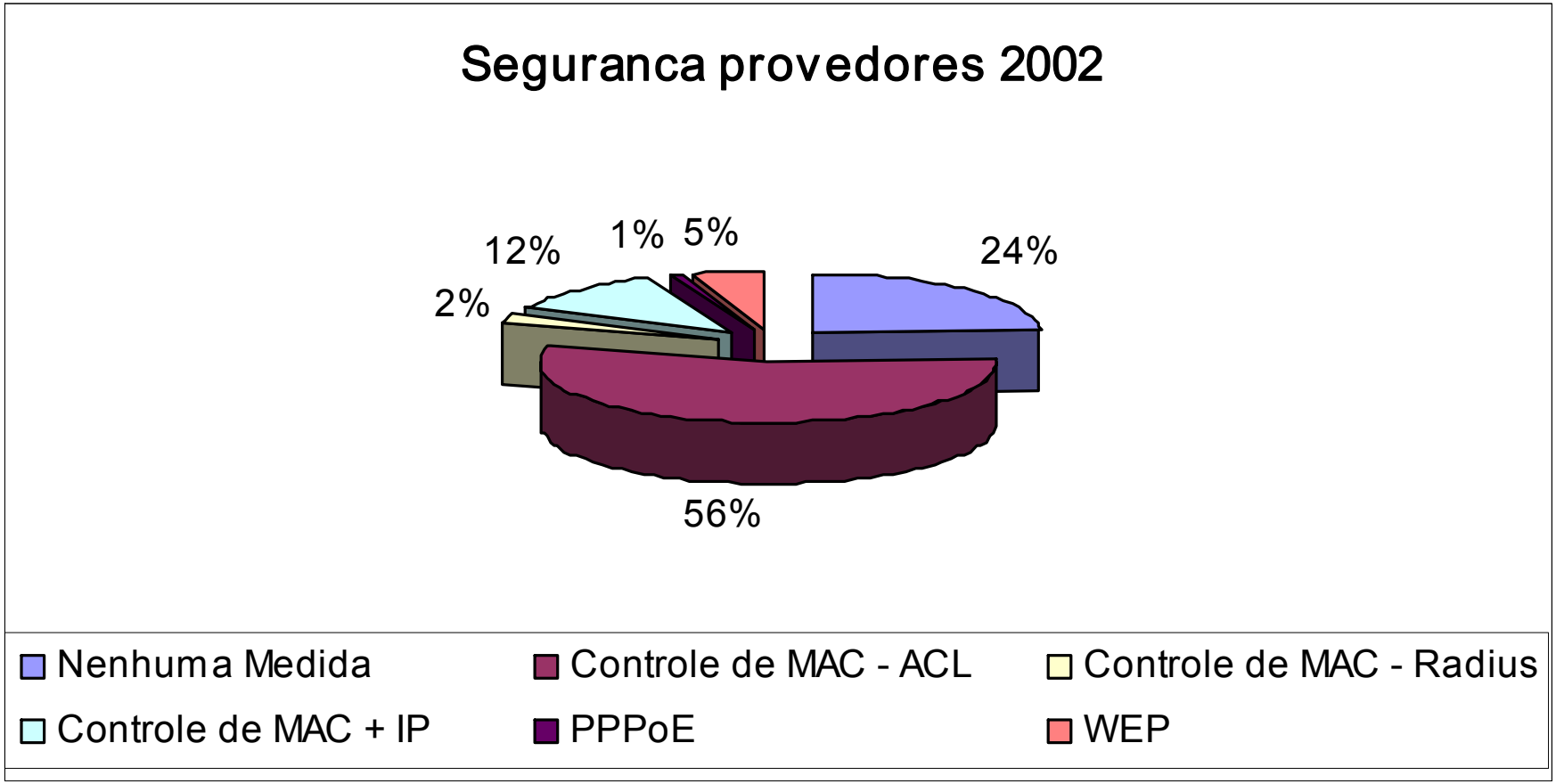
“El poder de las patatas”



Las medidas “recomendadas” de seguridad según el autor eran:

- Nombre de la red escondido
- Control de direcciones MAC
- Encriptación WEP

Encuesta sobre seguridad de WISP's realizada en 2002



Seguridad “Rudimentaria”
(lo que NO és Seguridad)

1 – SSID escondido

Puntos de Acceso Inalámbricos por defecto hacen broadcasts de los SSID em paquetes llamados “Beacons”. Este comportamiento puede ser modificado y el Punto de Acesso configurado para enviar Strings vacías o ninguna informacíón.

Esconder el nombre de la Red ayuda, pero no puede significar seguridad porque

→ SSID’s están presentes en texto plano nas computadoras de los clientes

→ Escaneadores pasivos pueden escuchar las pruebas de los clientes (probe requests) quando buscan su Red y adivinar el SSID

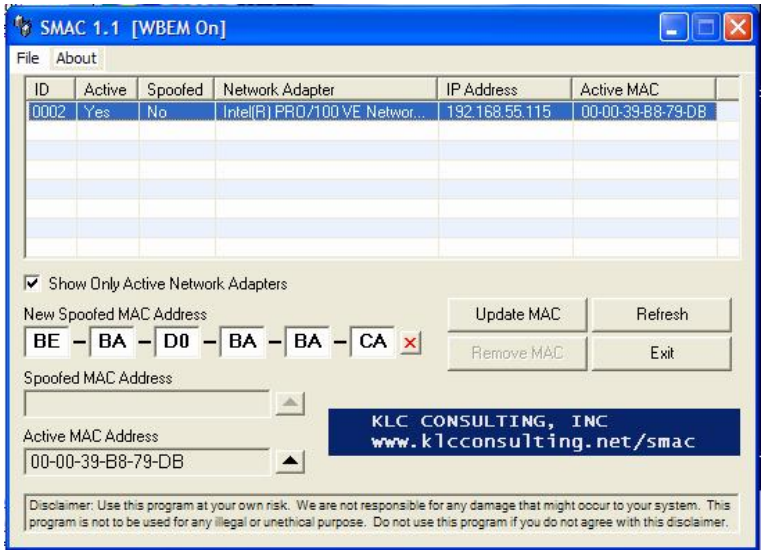
→ Hay equipos que tienen problemas para conectar cuando el AP no hace el broadcast del SSID

Seguridad “Rudimentaria”
(lo que NO és Seguridad)

2 – Filtrado de direcciones MAC

→ Descubrir MAC’s permitidos es posible con escaneadores pasivos
- → Airopeek para Windows
- → Kismet, Wellenreiter, etc for Linux/BSD

→ Falsificar una MAC es muy sencillo con Unix
y lo mismo para Windows



- FreeBSD :

ifconfig <interface> -L <MAC>

- Linux :

ifconfig <interface> hw ether <MAC>

Seguridad “Rudimentaria”
(lo que NO és Seguridad)

3 – Encriptación WEP

→ “Wired Equivalent Privacy” – es un sistema de cifrado estándar de la 802.11 pero su utilizacioin no es mandatoria.

→ Esta basada en un secreto compartido por las partes y encriptacion con el algoritmo RC4 – Pude ser de 40 e 128 bit.

→ 40 bit WEP puede ser crackeada sin hacer uso de técnica sofisticada – solamente un ataque de diccionario quiebra la WEP en menos de 24 horas !

→ 104 bit WEP na práctica no puede ser quebrada por ataque de diccionario solamente. Pero...

Comprometiendo la WEP (en definitivo)

Articulos publicados na Internet justo al comienzo del uso de WEP mostrando las fragilidades existentes

1 – University of Berkeley – “Intercepting Mobile Communications: The insecurity of 802.11”

Borisov, Nikita, Goldberg e Wagner

http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

2 – University of Maryland – “Your 802.11 Wireless Network has no Cloithes.”

Arbaugh, Shankar e Wan

http://www..cs.umd.edu/~waa/wireless.pdf

3 – Security Focus – “Weaknesses in the Key Scheduling Algorithm of RC4”

Fluhrere, Martin e Shamir

http://downloads.securityfocus.com/library/rc4_ksaproc.pdf

Comprometiendo la WEP (en definitivo)

4 – Articulo publicado en 2005 por Andrea Bittau describiendo un ataque basado en Fragmentación y otras técnicas de ataques inductivos – WEP crackeada en menos de 5 minutos !

http://www.toorcon.org/2005/conference.html?id=3www.aircrack-ng.org/doku.php?id=fragmentation&DokuWiki=71f9be8def4d820c6a5a4ec475dc6127

5 – Muy bueno soporte en la net para crackear la WEP

The FEDs can own your WLAN too

http://www.tomsnetworking.com/Sections-article111.php

How to crack WEP

http://www.tomsnetworking.com/Sections-article118.php

Breaking 104 bit WEP in less than 60 seconds

http://eprint.iacr.org/2007/120.pdf

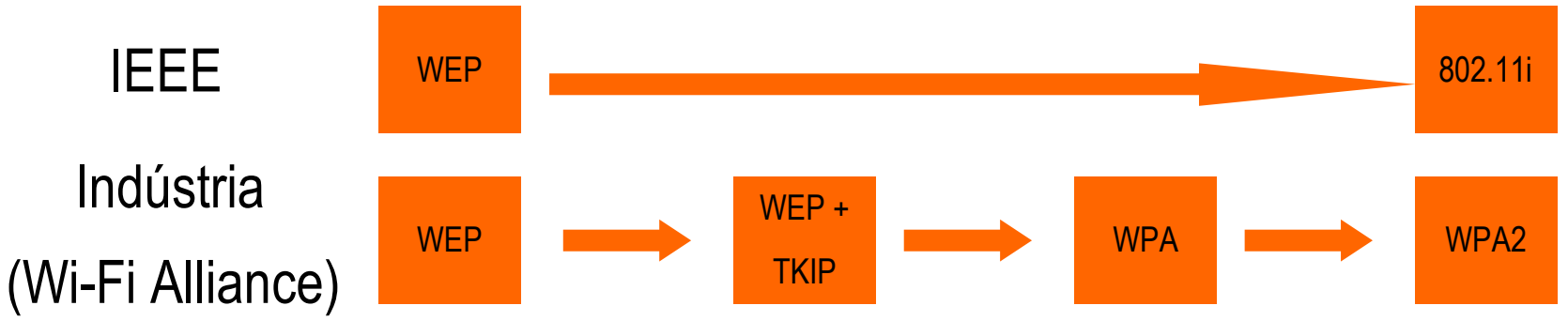
Comprometiendo la WEP (en definitivo)

5 – Muy bueno soporte en la net para crackear la WEP

You Tube Vídeo (en espanõl !!)
http://www.youtube.com/watch?v=PmVtJ1r1pmc

IEEE 802.11i

- Motivado por los problemas de WEP el IEEE ha creado el Grupo de Trabajo – 802.11i cuya tarea principal era hacer una nueva norma de facto segura.
- Antes de la conclusión del grupo 802.11i (que demoró bastante) la Industria creó un estándar propio - el WPA (Wireless Protected Access)
- En junio del 2004 por fin el stándar fue aprobado y la Industria le dio el nombre de WPA2, compatible con 802.11i .y con WPA



Objectivos de 802.11i

→**Autentificación**

AP → Cliente: El AP tiene que garantizar que el cliente es quien dice ser

Client →AP: El Cliente tiene que garantizar que el AP es verdadero y no un AP engañoso (man-in-the-middle attack)

→**Privacidad**

→La información no es legible por terceros.

→**Integridad**

→La información no puede ser alterada en transito.

Como trabaja 802.11i

802.11i tiene 3 partes

→Supplicant (Solicitante, Cliente)
→Authenticator (Autenticador, AP)
→Authentication Server (Servidor de Autenticación, RADIUS)

Y es hecha por una combinación de protocolos:

→ 802.1X – A Port Based Network Access Control
→ EAP – Extensible Authentication Protocol
→ RADIUS – Remote Access Dial In User Service

Variantes de 802.11i

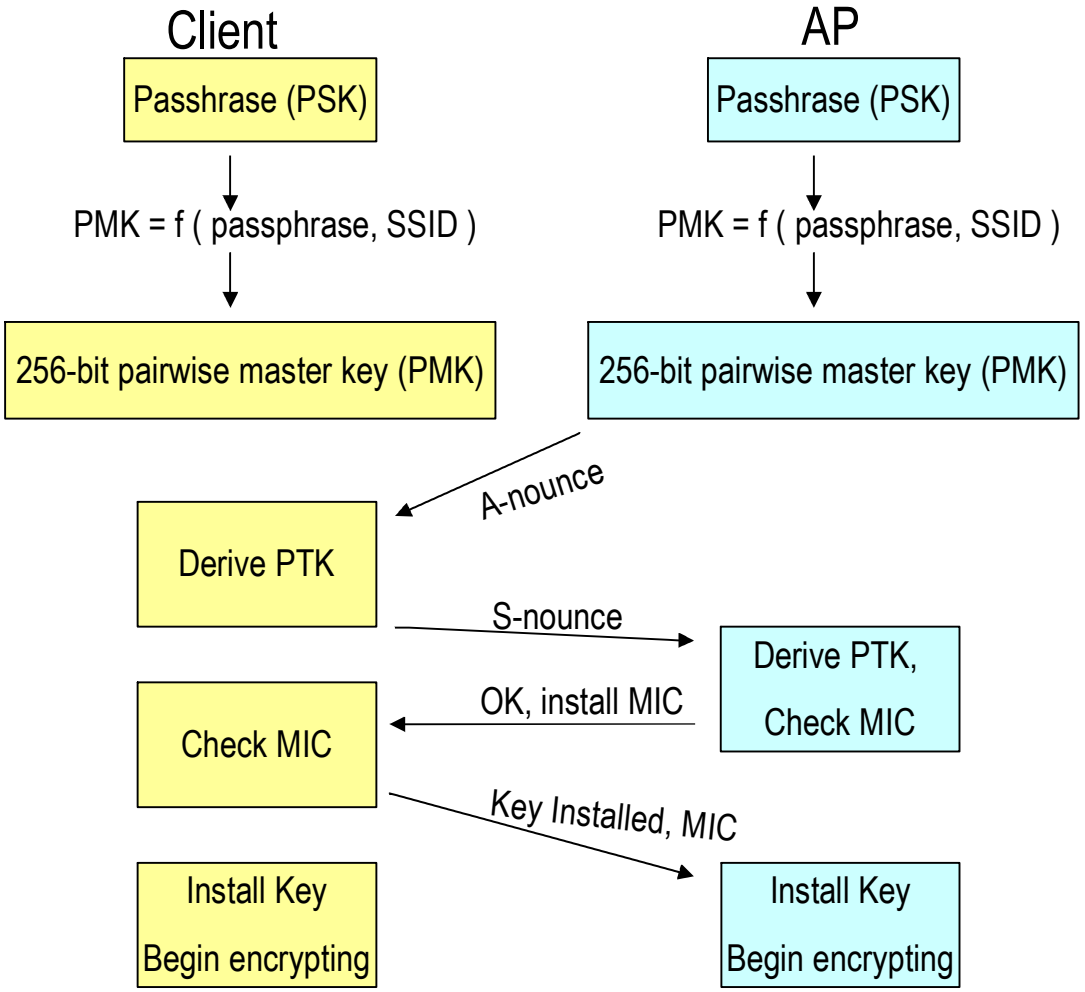
El proceso de autenticación puede ser de 2 maneras:

→ Home Mode: (modo casero, personal)
→ Pre Shared Key (PSK)

→ Enterprise Mode: (modo corporativo)
→ 802.1X/EAP

		WPA	WPA2
Modo Corporativo	Autenticación	802.1X / EAP	802.1X / EAP
	Cifrado	TKIP/MIC	AES-CCMP
Modo Personal	Autenticación	PSK	PSK
	Cifrado	TKIP/MIC	AES-CCMP

802.11i PSK



Una “llave Maestra” llamada PMK – Pairwise Master Key es creada por un hash entre la Passphrase y el SSID. La PMK es guardada en el Registro de Windows on en supplicant.conf en Linux.

Otra llave llamada PTK - Pairwise Transient Key es creada de manera dinámica despues de un proceso de handshake de 4 vias. PTK es única a cada sessión.

Privacidad con 802.11i

Privacidad

→ Después de la autenticación, los dos lados – AP y Cliente tienen la misma PMK – Pairwise Master Key que se mantiene durante toda la sesión

→ Para la transmisión de datos, es hecha una derivación de la PMK y una PTK – Pairwise Transient Key ***única para cada cliente*** es utilizada para encriptación.

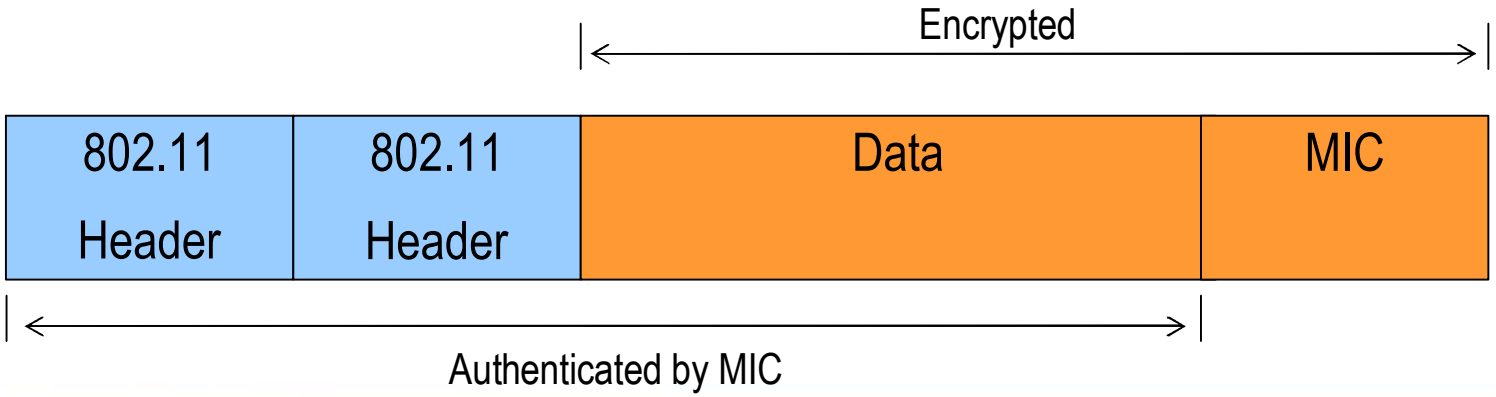
Integridad con 802.11i

Una parte de la PTK tiene la función de proteger los datos para que no sean alterados cuando en transito – es el MIC - Message Integrity Check (MIC). Con el MIC, para todo paquete el transmissor calcula un hash de los datos con una llave secreta – Temporal Integrity Key.

MIC = hash(packet, temporal integrity key)

WPA usa TKIP → Algoritimo de Hashing “Michael”

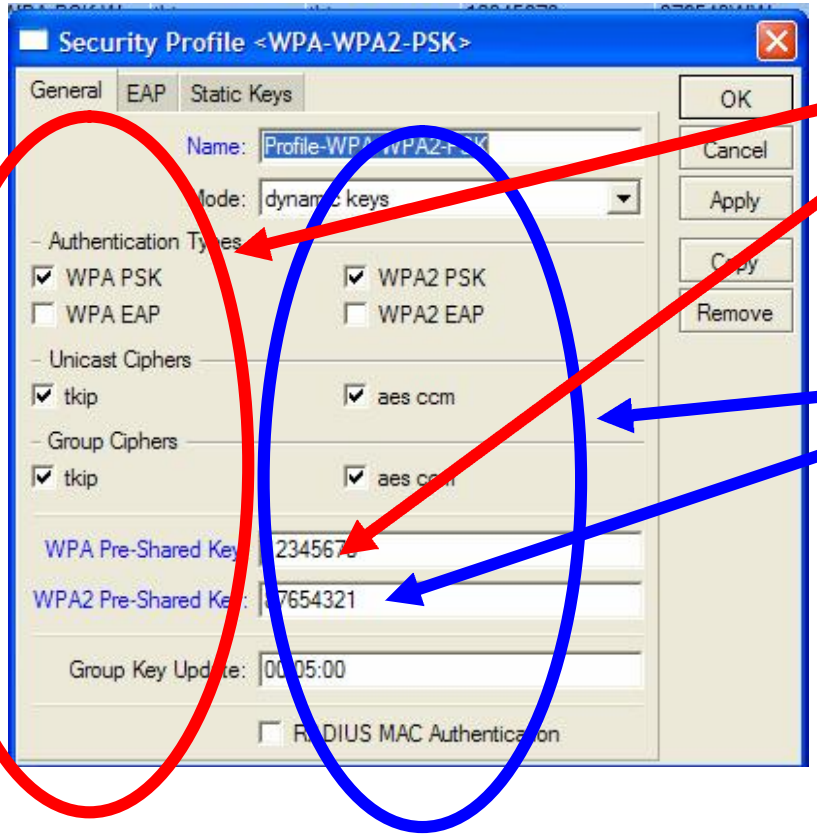
WPA2 uses CCMP → Cipher Block Chaining Message Authentication Check– CBC-MAC



Utilizando WPA/WPA2 – PSK con Mikrotik RouterOS

Utilizando WPA/WPA2 – PSK

Es muy sencilla la configuraccion de WPA/WPA2-PSK con Mikrotik



→WPA - PSK

Configure el modo de llave dinámico, WPA PSK, y la llave compartida.

→ WPA2 – PSK

Configure el modo de llave dinámico, WPA PSK, y la llave compartida.

Las llaves son alfanumericas de 8 hasta 63 caracteres

¿ Cuanto segura es WPA / WPA2 PSK ?

- La manera conocida hoy de crackear WPA-PSK es solamente por un ataque de diccionario.
- Como la llave maestra - PMK combina una contraseña con el SSID, escogiendo dos palabras fuertes, hace ineficientes los diccionarios precompilados
- No hay diferencias en la manera y nivel de dificuldad para crackear WPA-PSK o WPA2-PSK, porque el mecanismo que genera la PMK es el mismo. Solamente cambia el MIC.
- Herramienta para quiebra de WPA/WPA2 – PSK
  - Cowpatty http://sourceforge.net/projects/cowpatty
- La mayor fragilidad de PSK para WISP's es que la llave se encuentra em texto plano nas computadoras dos clientes

¿ Cuán segura es WPA / WPA2 PSK ?

Cuando el atacante tiene la llave PMK es possible:

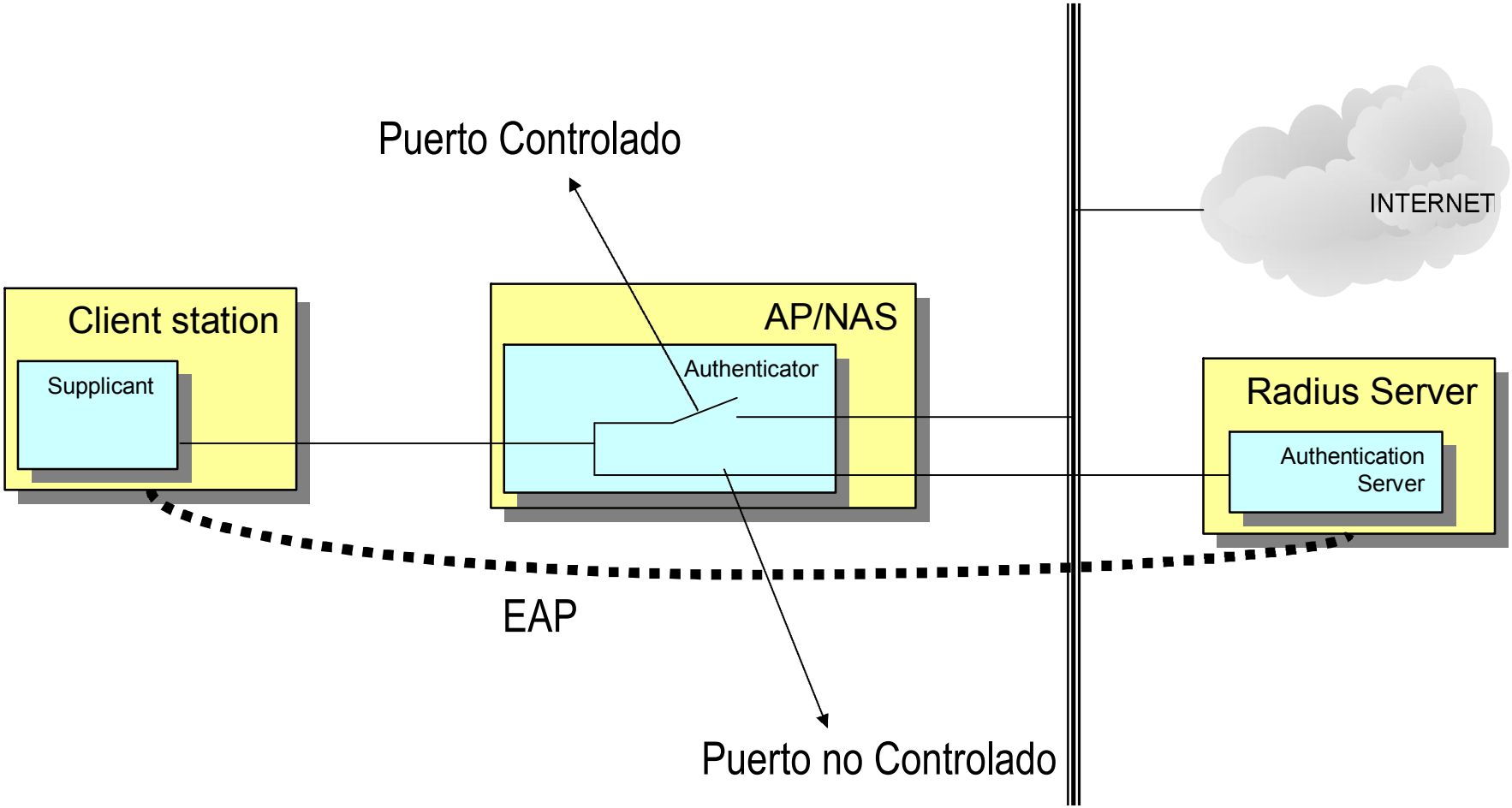
- → Ganar acceso no autorizado
- → Falsificar um Punto de acesso y hacer el ataque del “hombre del medio” (man-in-the-middle)

Recomendaciones para WISP’s

- → Solo use PSK se tiene **absoluta certeza** que las llaves están protegidas (equipos clientes del proveedor)
- → No olvides que las llaves PSK están em **texto plano** dentro de los boxes Mikrotik (hasta para read-only user)

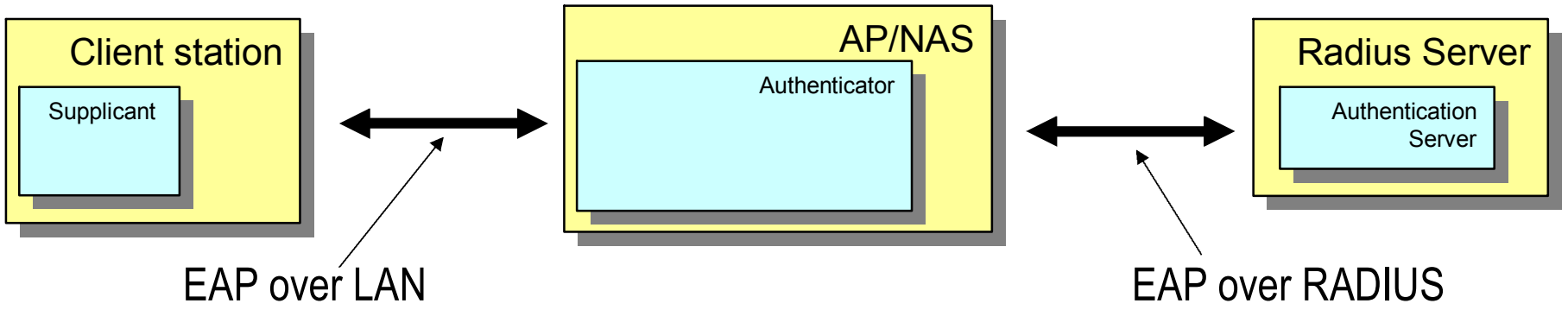
Seguridad 802.11i
Modo Corporativo

Autenticación via 802.1X



EAP

EAP es un protocolo para identificación de usuarios o hosts originalmente diseñado para Protocolo Punto a Punto (PPP)



Soporta diferentes tipos de autenticacción. Los más comunes son: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-LEAP, EAP-MD5 etc

Tipos de EAP

EAP Type	Open/ Proprietary	Mutual Auth	Authentication Credentials		Key Material	User Name In Clear
			Supplicant	Authenticator		
TLS	Open	Yes	Certificate	Certificate	Yes	Yes
TTLS	Open	Yes	Username/Pwd	Certificate	Yes	No
PEAP	Open	Yes	Username/Pwd	Certificate	Yes	No
LEAP	Proprietary	Yes	Username/Pwd		Yes	Yes

Tipos de EAP

LEAP: (Lightweight EAP)

Es un protocolo propietario de Cisco patentado antes mismo de 802.11i and WPA. Es basado en nombre de usuario y contraseña que se envía sin protección.

Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.

Trabaja con variados tipos de clientes pero solo con AP Cisco.

→ Tool to crack LEAP: Asleap - http://asleap.sourceforge.net/

OBS: Mikrotik no soporta LEAP

Tipos de EAP

PEAP: (Protected EAP) and EAP-TTLS (EAP tunneled TLS)

PEAP y TTLS son parecidos- TTLS es compatible con otros protocolos como LEAP y hacen uso de Certificados de Autenticidad en lado del Servidor y usuario contraseña en lado cliente. Autenticación sigue la orden:

1 – El Servidor manda un EAP request

2 – Cliente manda una identidade (lo que sea) - un Tunel TLS es creado

3 – Dentro del tunel, el cliente pasa usuário y contraseña

El problema con TTLS y PEAP es el “hombre del medio”

OBS: Mikrotik no soporta TTLS y PEAP

Tipos de EAP

EAP-TLS (EAP – Transport Layer Security)

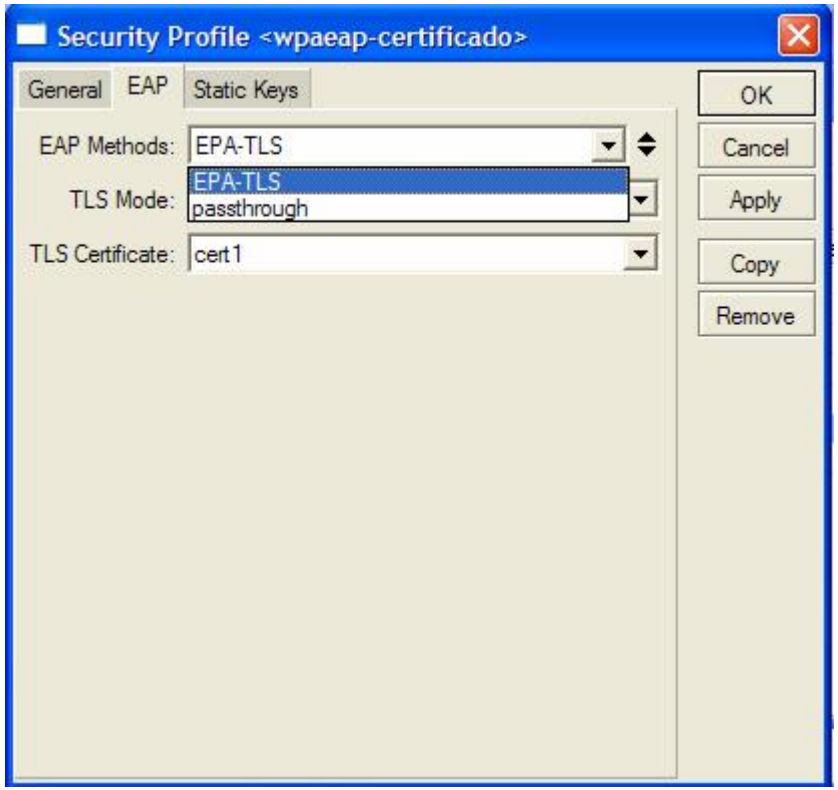
→ Es el tipo de EAP que Mikrotik soporta

Provee mayor nivel de seguridad y necesita certificados en los dos lados – Cliente y Servidor.

Los Certificados pueden ser instalados:

- → En AP y Clientes
- → Em Clientes y Servidor Radius
- → Sin Certificados !

Security Profiles – EAP Methods



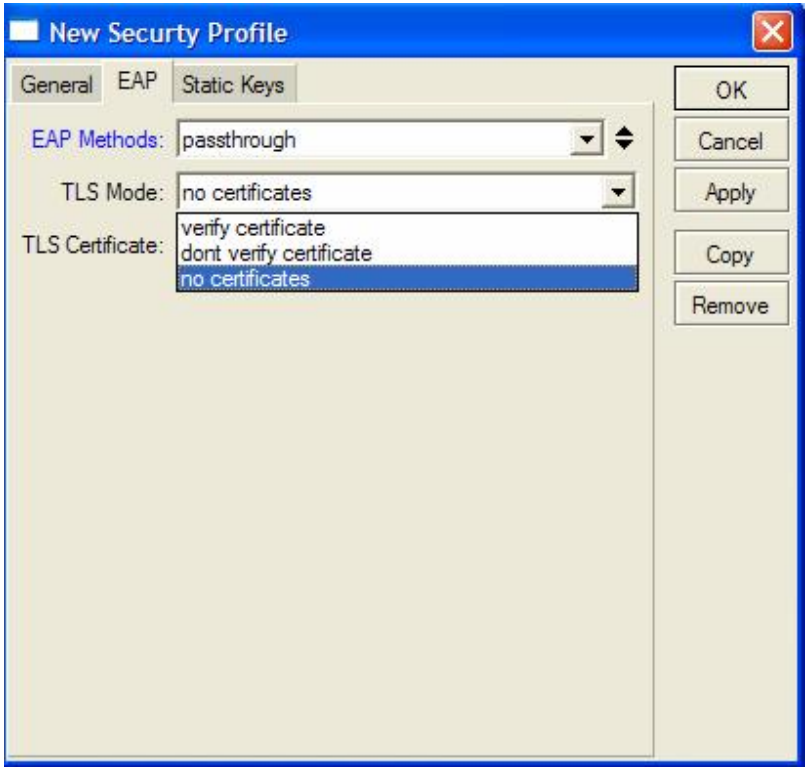
→EAP-TLS

Usa Certificados

→ passthrough

Manda para un Servidor Radius (funciona como dispositivo 802.1X) – solo para Puntos de Acceso.

Security Profiles – TLS Mode



→ verify certificates

Requiere un certificado y verifica si fue firmado por una Certificadora

→ don't verify certificates

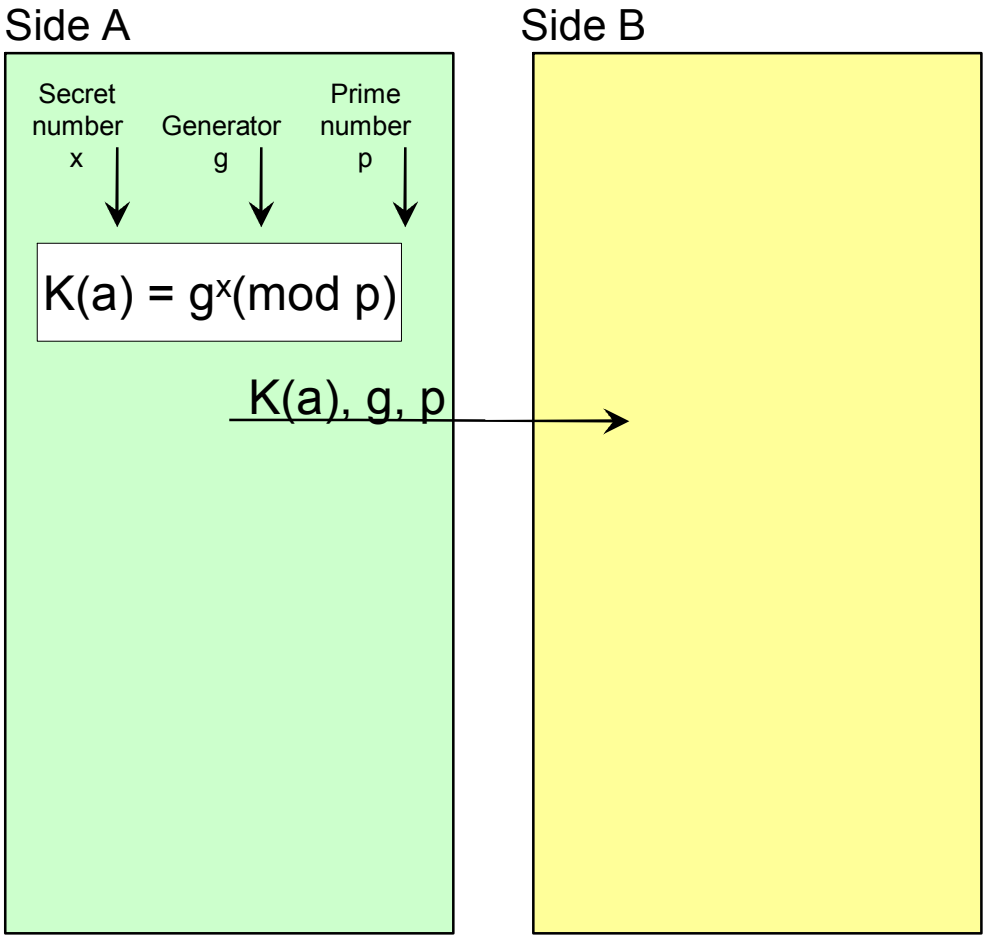
Requiere un certificate, pero no verifica

→ no certificates

Certificados son negociados dinámicamente con el algoritmo de Diffie-Hellman (explicado adelante)

¿¿ Trabajar con EAP-TLS pero sin Certificados ??

Diffie-Hellmann (Without Certificates)



1. Cada lado escoge un número secreto x y y – llaves privadas.

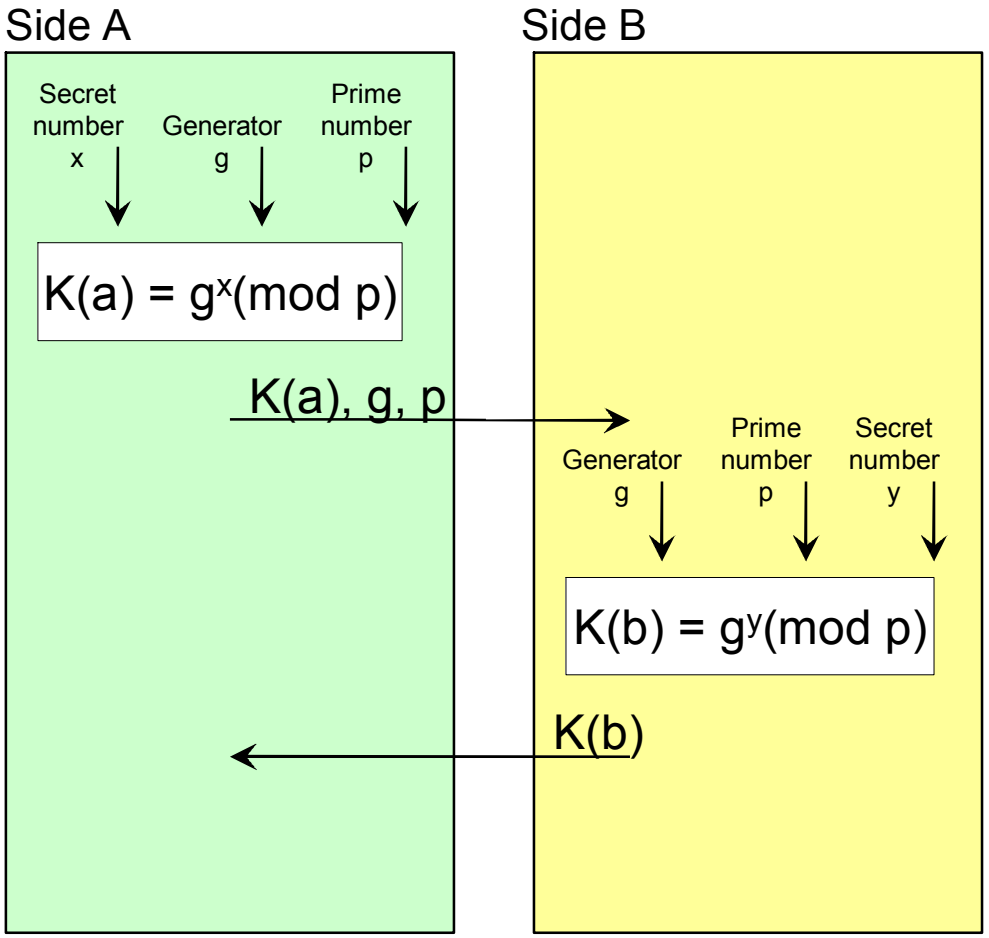
2. Lado A empieza seleccionando un número primo muy alto (p) y un pequeño entero – el generador (g)

3. Lado A calcula usando aritmética modular la clave publica, K(a):

   → $K(a) = g^{x} \pmod{p}$

4. Lado A manda para o lado B la clave publica, el número primo (p), y el generador (g)

Diffie-Hellmann (Without Certificates)



5. Lado B hace un calculo similar con su clave secreta, el primo y el generator para obtenir su clave publica.

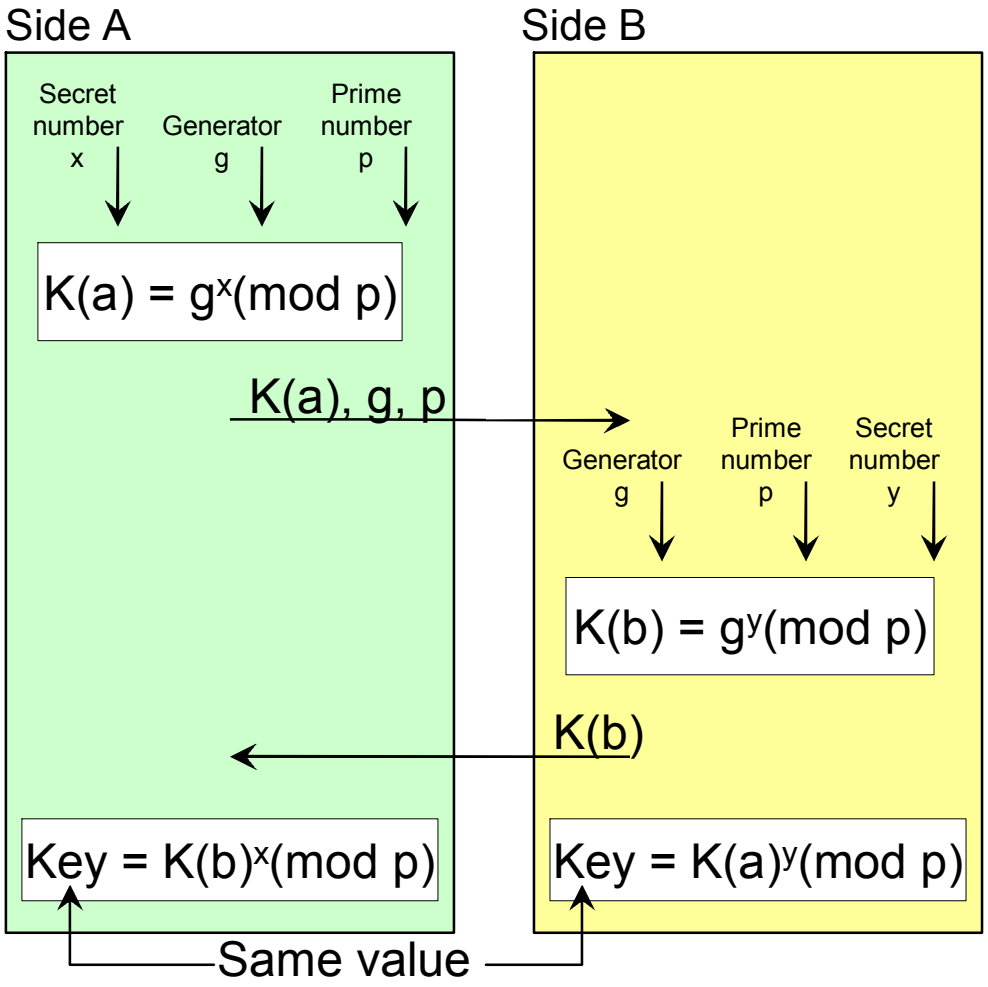
6. Lado B manda para lado A la clave publica.

7. Ahora los dos lados pueden calcular una misma clave compartida

→ Shared key = $K(b)^x \pmod p$

→ Shared key = $K(a)^y \pmod p$

Diffie-Hellmann (Without Certificates)

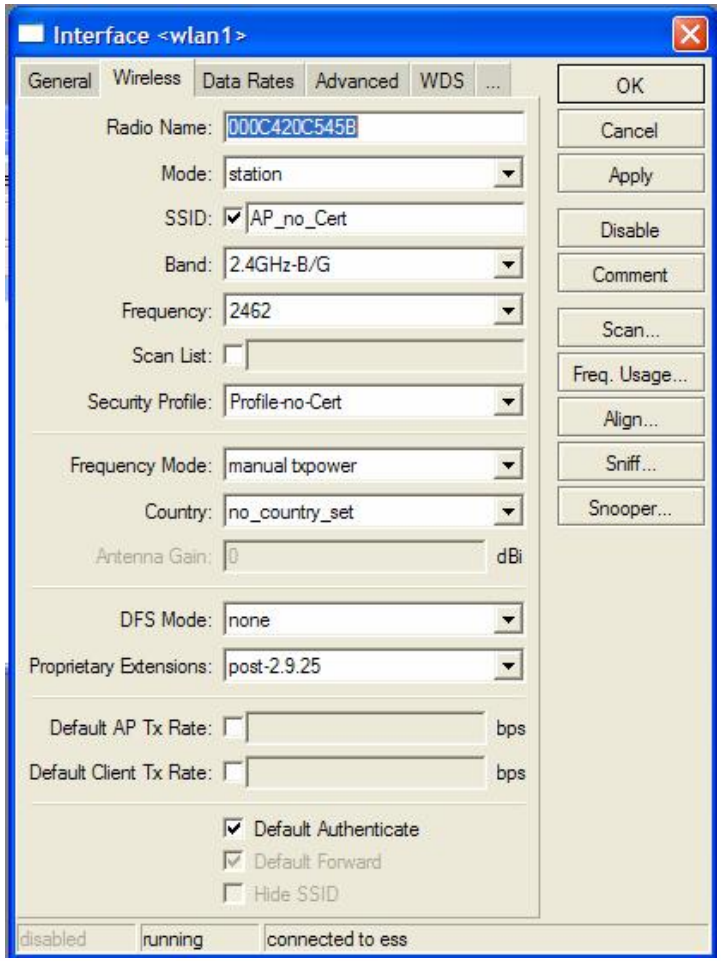


8. Los dos cálculos producen valores exatamente iguales – propiedad de aritmética modular

9. La clave calculada es usada como PMK e inicia el proceso de encriptación

Setup with EAP-TLS – No Certificates

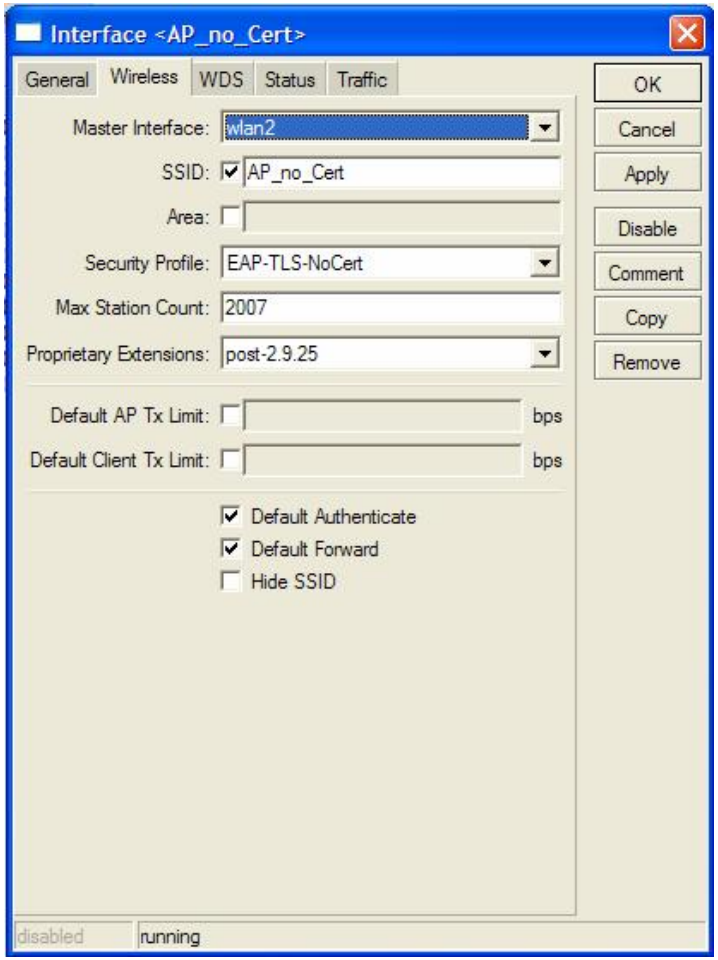
Station Configuration



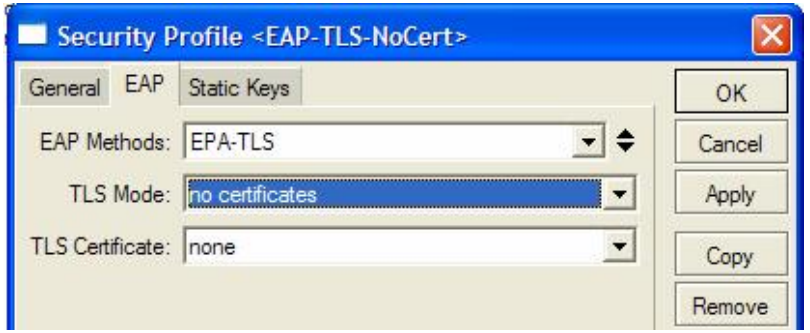
Security Profile

Setup with EAP-TLS – No Certificates

AP Configuration



Security Profile



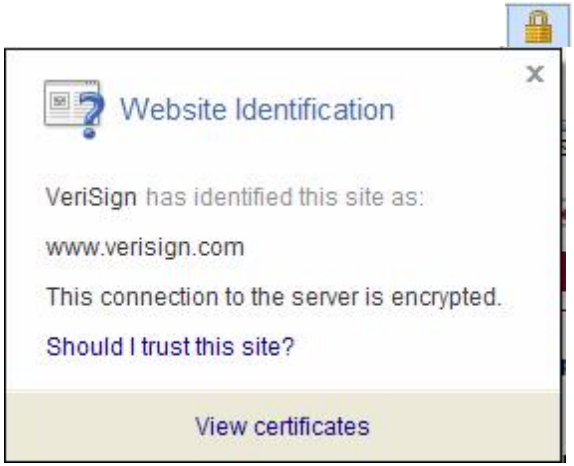
¿ Cuanto seguro es EAP-TLS sin Certificados ?

- Como resultado de la negociacion anónima resulta una PMK y después toda la comunicacción es encriptada por AES (WPA2) o RC4 (WPA)
- Sería todo muy seguro si no hubiera la posibilidad de un hacker meter un Mikrotik con la misma configuracción y negociar la clave normalmente ☹
- Una idea para hacer esa configuración de forma segura es después de cerrar el enlace, hacer un tunel PPtP o L2TP entre los equipos.

Implantando EAP-TLS con Certificados

Implantando EAP-TLS con Certificados

Un certificado digital es un fichero que identifica su propietario de manera única. Certificados son creados por instituiciones emisoras llamadas de CA (Certificate Authorities)

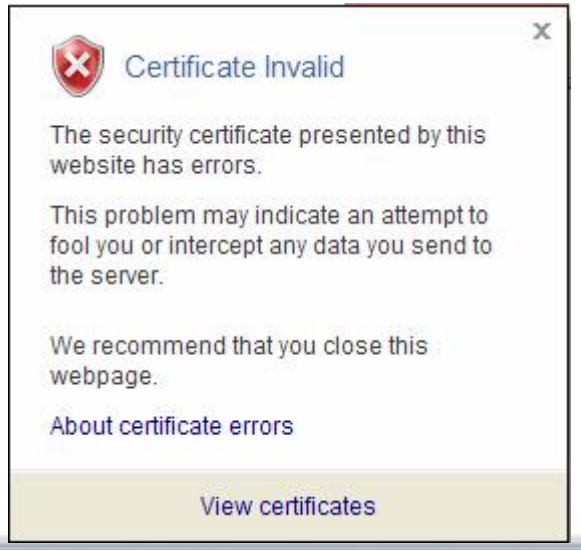


Certificados pueden ser :

→ Firmados por una instituición “acreditada” (Verisign, Thawte, etc)

o

→ Certificados auto-firmados



Implantando EAP-TLS con Certificados

Creando la CA - Certificate Authority

→En una máquina Linux con OpenSSL modifique el fichero openssl.conf con los datos que se usarán en los Certificados que serán generados

/etc/ssl/openssl.conf

```
dir                                 = ./MikrotikBrasil_CA

countryName_default                 = BR
stateOrProvinceName_default         = Sao Paulo
organizationName_default            = MikrotikBrasil_Private_Network
```

Implantando EAP-TLS con Certificados

Creando la CA - Certificate Authority – cont.

→ Modifique el script creador de la CA (CA.sh) para el mismo directorio.

```
CATOP=./MikrotikBrasil_CA
```

→Corra el con la opcion –newca

```
root@wlanbrasil:/etc/ssl# ./misc/CA.sh –newca
CA certificate filename (or enter to create)
```

→Pressione <enter> e contesta a las preguntas

Implantando EAP-TLS con Certificados

Creando la CA - Certificate Authority – cont.

→ El Certificado fue creado y se encuentra en:

/etc/openssl/MikrotikBrasil_CA/cacert.pem

→ Una Clave protegida con DES también está en:t:

/etc/openssl/MikrotikBrasil_CA/cakey.pem

Implantando EAP-TLS con Certificados

Creando las requisiciones de Certificados

Puedem ser creadas en propio Mikrotik con :
/ certificates create-certificate-request

```
[admin@MikroTik] certificate>
create-certificate-request  decrypt  edit  find  get  import  print  remove  reset-certificate-cache  set
[admin@MikroTik] certificate> create-certificate-request
certificate request file name: certificate-request-01.pem
file name: private-key-01.pem
passphrase: ******
verify passphrase: ******
rsa key bits: 1024
country name: BR
state or province name: Sao Paulo
locality name: Bebedouro
organization name: Mikrotik Brasil Corp.
organization unit name: Wireless Security
common name: hotspot.mikrotikbrasil.com.br
email address: maia@mikrotikbrasil.com.br
challenge password: ******
unstructured address: www.mikrotikbrasil.com.br
[admin@MikroTik] certificate>
```

Implantando EAP-TLS con Certificados

Creando las requisiciones de Certificados – cont..

Las requisiciones también pueden ser generadas en la máquina Linux:

root@wlanbrasil:/etc/ssl# openssl req –new clave_privada.pem –out Requisicion_de_certificado.pem –days dias_de_validad

Serán creados 2 ficheros: la clave privada e la Requisición de Certificado

A continuación debemos **firmar el Certificado**

Implantando EAP-TLS con Certificados

Asignando las requisiciones de Certificados

Las requisiciones creadas en RouterOS o en la máquina Linux se firma con

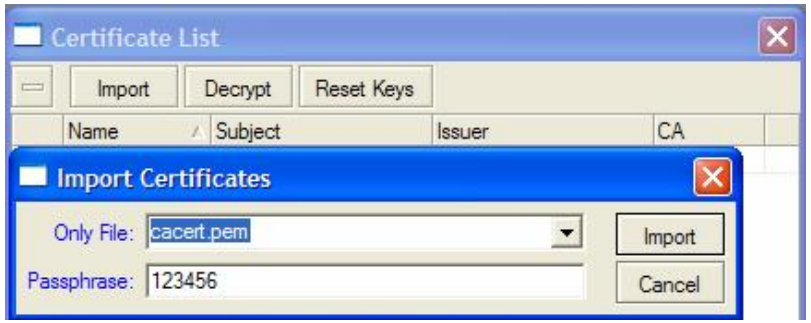
root@wlanbrasil:/etc/ssl# openssl ca –config ./openssl.conf –policy policy_anything –out /certificado_asignado.pem –infiles /requisicion_de_certificado.pem

Ähora el fichero de requisición puede ser deletado porque será utilizado solo el certificado_assinado.pem

Implantando EAP-TLS con Certificados

Importando el Certificado para Mikrotik

via Winbox



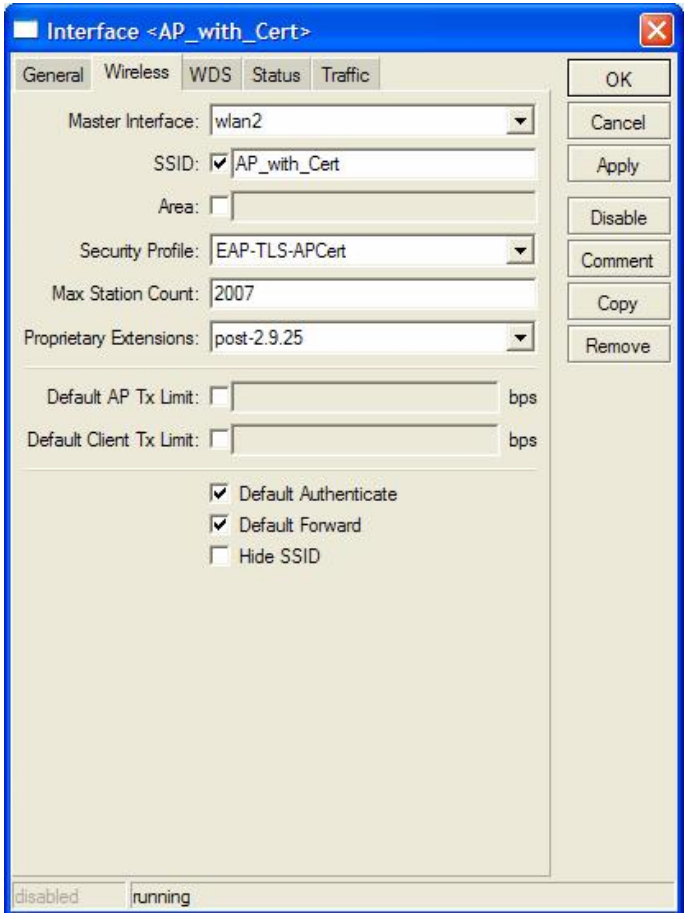
Después de la Importación

Para importar la clave es necesaria la misma contraseña que se utilizó en la creación

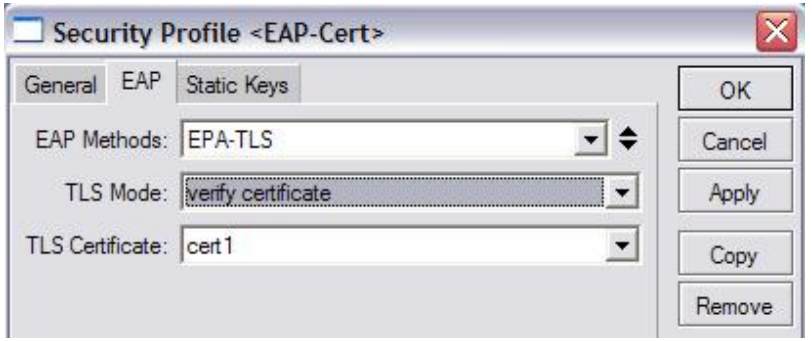
Utilización de EAP-TLS con Certificados en AP y Clientes

Utilización de EAP-TLS (AP con Certificado)
Configuración del AP

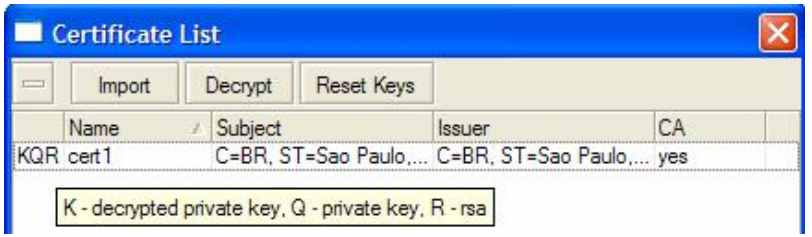
AP Configuration



Security Profile

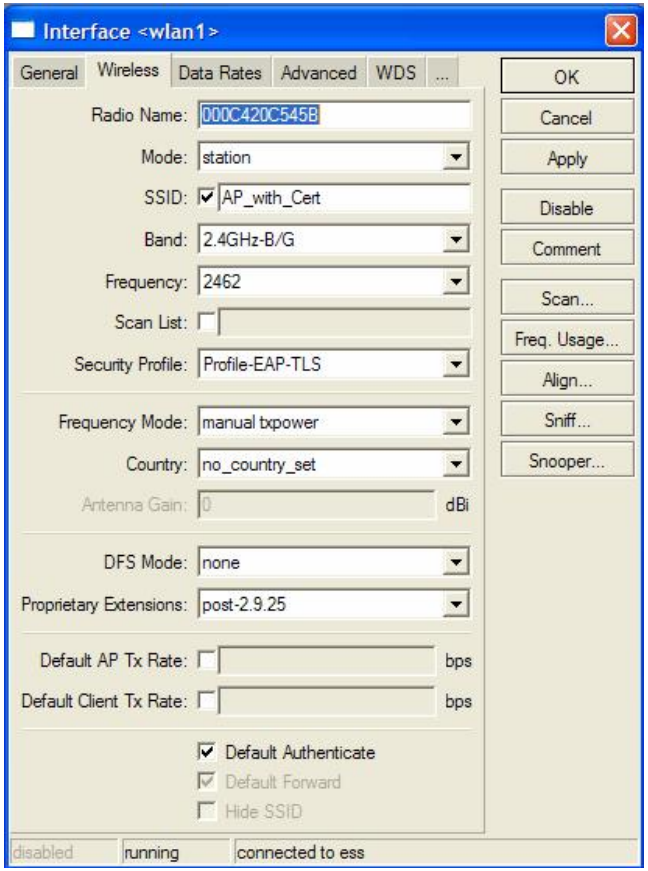


Certificate

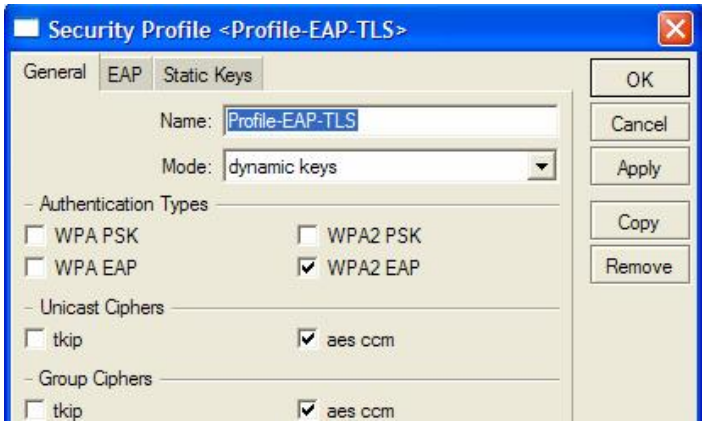


Utilización de EAP-TLS (AP con Certificado)
Configuración del Cliente

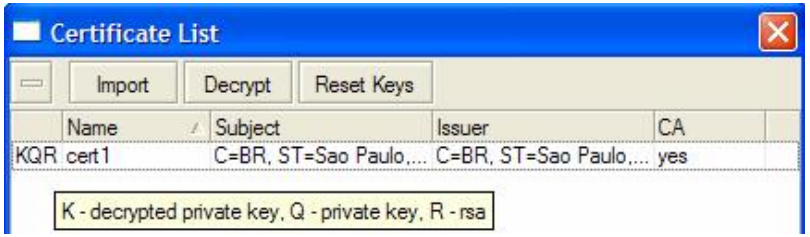
Station Configuration



Security Profile



Certificate



Implantando EAP-TLS + Radius

Implantando EAP-TLS + Radius

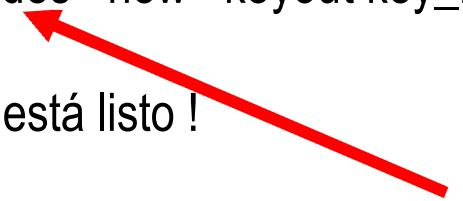
Creando Certificado para instalar en el Servidor RADIUS (1/1)

El Certificado para Radius puede ser creado de la misma manera que otros certificados, pero es mejor que se utilize la opcción –nodes

Se no se utiliza la opcción –nodes toda vez que se inicia Radius tiene que digitar la clave privada.

openssl req –nodes –new –keyout key_file.pem –out req_file.pem –days 365

Se firma como los otros y está listo !



Implantando EAP-TLS + Radius

Instalando el Certificado en el Servidor RADIUS (1/1)

→Ponga las cosas en sus lugares correctos:

```
root@radius:/usr/local/etc/raddb# mv certs certs.old
root@radius:/usr/local/etc/raddb# mkdir certs
root@radius:/usr/local/etc/raddb# mv /root/radius_cert_key.pem ./certs
root@radius:/usr/local/etc/raddb# mv /root/cacert.pem ./certs
```

→Crea el parámetro de Diffie-Hellman:

```
root@radius:/usr/local/etc/raddb# dd if=/dev/random of=./certs/random count=2
root@radius:/usr/local/etc/raddb# openssl dhparam –check –text -5 -512 –out
./certs/dh
```

→Chequea si tudo se encontra en su lugar

```
root@radius:/usr/local/etc/raddb# ls ./certs
cacert.pem dh radius_cer_key.pem random
```

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (1/4)

→Edite el fichero clients.conf con la lista de AP's (NAS's) que utilizarán el Radius

```
root@radius:/usr/local/etc/raddb# aee clients.conf
client 192.168.100.1/32     {
                            secret              = 123456
                            shortname           = AP1
                            }
```

→Edit radiusd.conf

```
root@radius:/usr/local/etc/raddb# aee radiusd.conf

user = nobody
group = nogroup
```

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (2/4)

Editing radiusd.conf - cont

```
authorize       {
                preprocess
                chap
                mschap
                suffix
                eap
                files
                }
```

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (3/4)

Configure el fichero users

root@radius:/usr/local/etc/raddb# aee radiusd.conf

```
DEFAULT         Auth-Type = EAP
                Tunnel-Type = 13,
                Tunnel-Medium-Type = 6,
                Tunnel-Private-Group-Id = 1
```

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (4/4)

→ Edite eap.conf

root@radius:/usr/local/etc/raddb# aee eap.conf

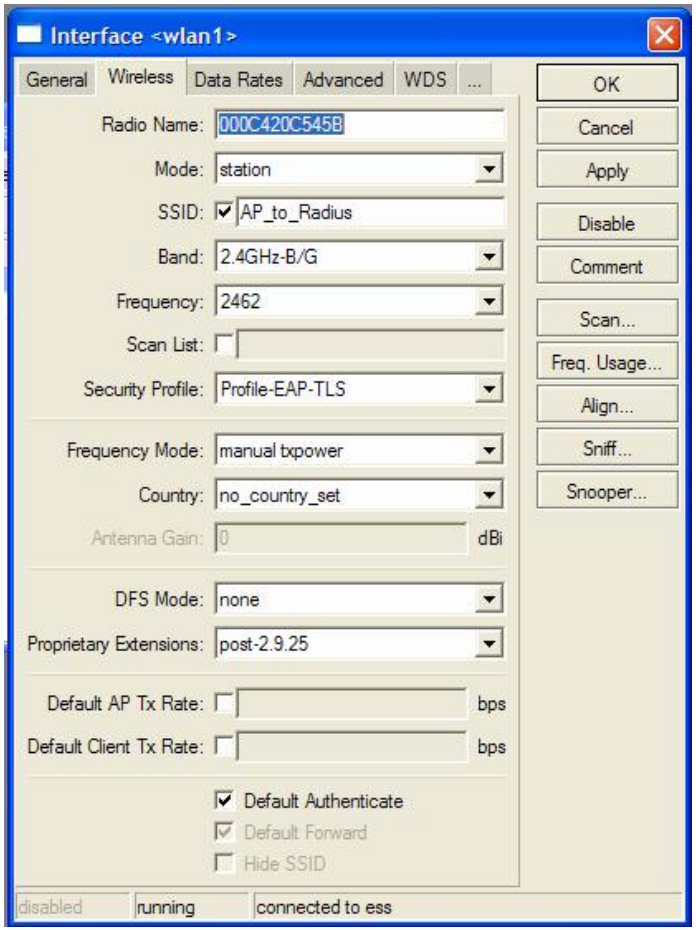
```
default_eap_type = tls
tls                     {
        private_key_file = ${raddbdir}/certs/radius_cert_key.pem
        certificate_file = ${raddbdir}/certs/radius_cert_key.pem
        CA_file = ${raddbdir}/certs/cacert.pem
        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/cacert.pem
        }
```

→Finalmente inicia el Radius Server

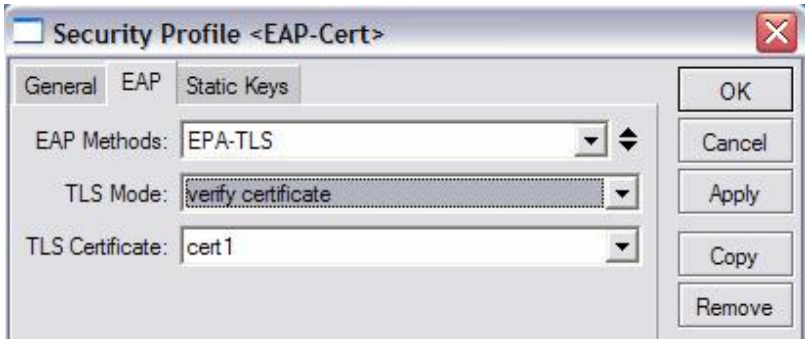
root@radius:/usr/local/etc/raddb# ./radiusd -X

Setup with EAP-TLS + Radius Client Configuration

Station Configuration



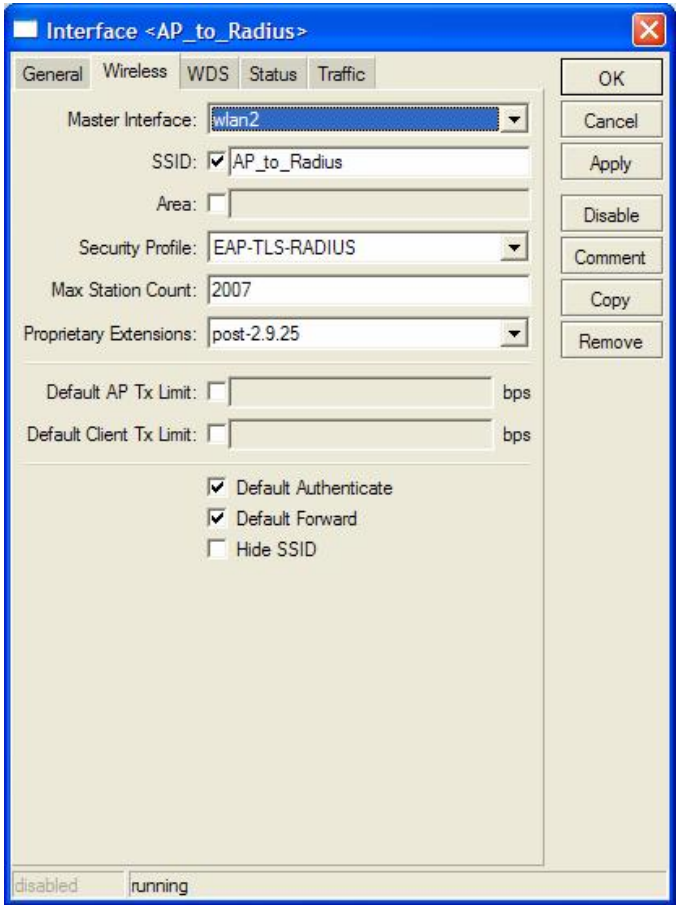
Security Profile



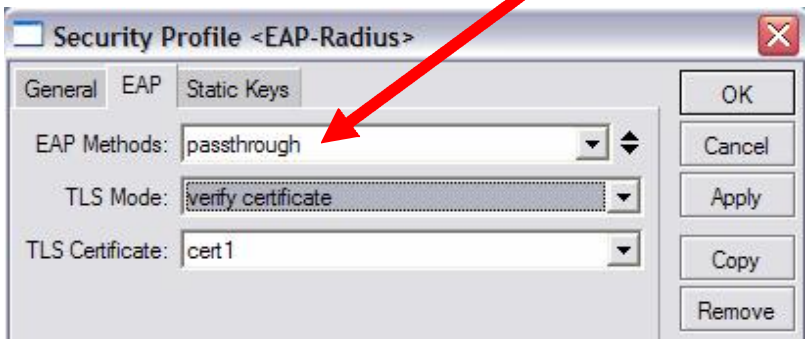
Certificate

Setup with EAP-TLS + Radius AP Configuration

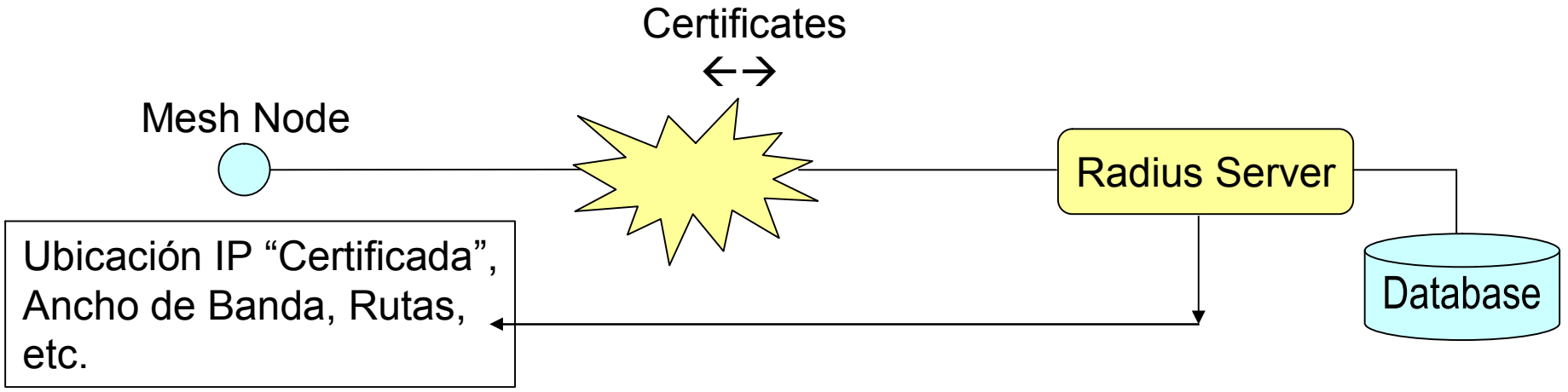
AP Configuration

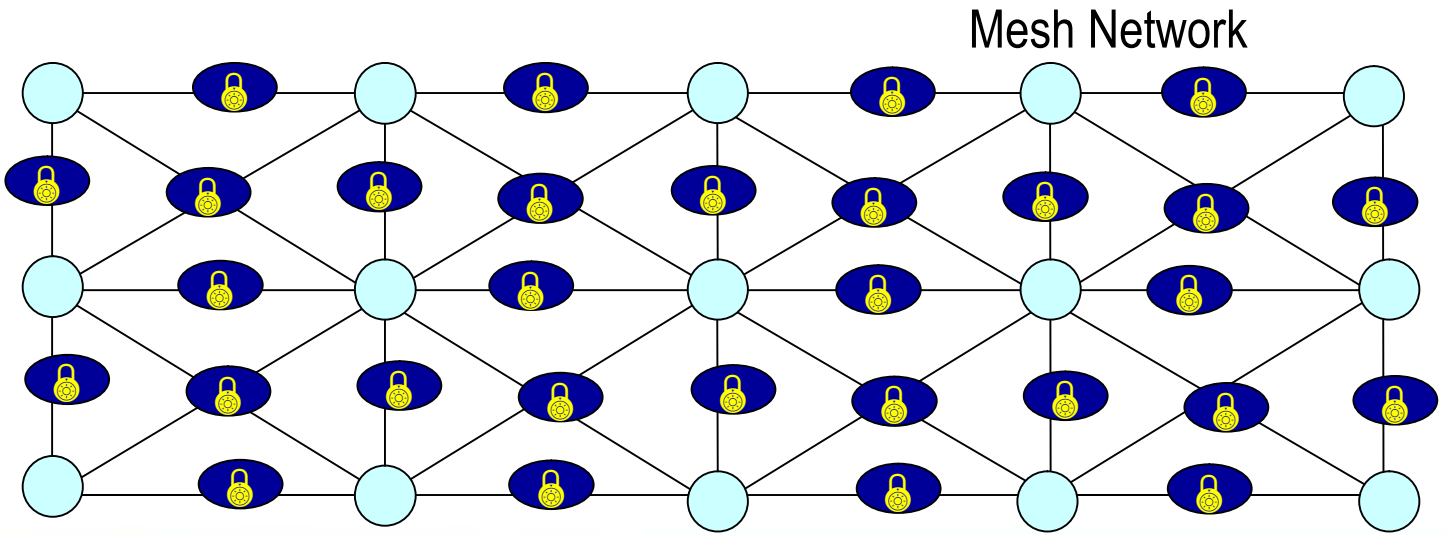


Security Profile



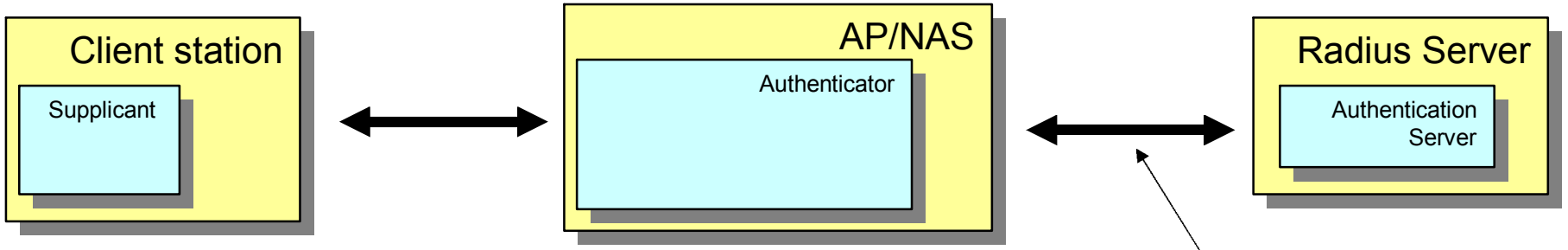
Backbone con EAP-TLS +Radius





¿ Cuanto seguro es EAP-TLS + Radius ?

No se discute que EAP-TLS es el método más seguro, pero la única cosa que se podría argumentar es cuanto al link entre AP y Radius.



→ Hay ataques conocidos contra Radius. Si un atacante tiene Acceso físico a el link entre AP y Radius, el puede hacer un ataque de diccionario para descobrir la PMK.

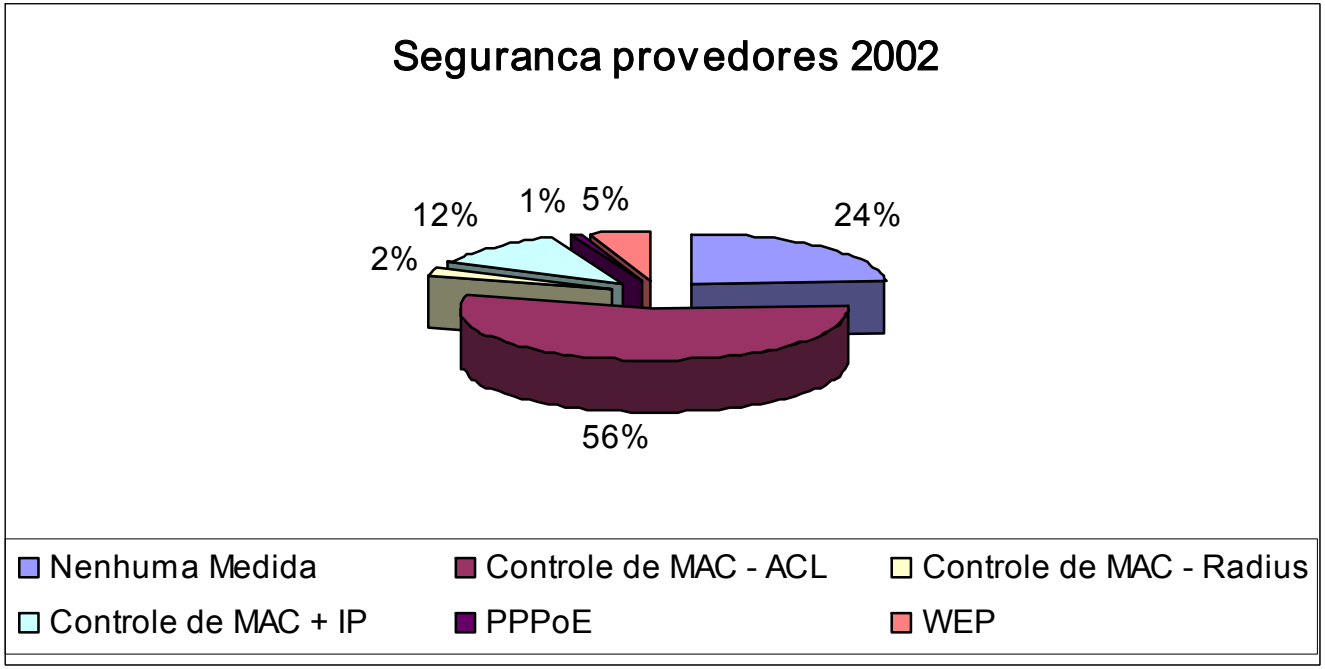
→ Para evitar pude-se proteger de muchas maneras, como con un tunel L2TP con IPSec entre Radius y AP.

802.11i

x

WISP's

Volviendo al pasado – En 2002 Los WISP's en Brasil Con las medidas "apropiadas"



Se consideraban muy seguros…

Soluciones para ultima milla

Para tratar de asegurar el servicio en la última milla, muchos proveedores utilizan las soluciones:

→Túneles PPPoE

→Autenticación Hotspot

A continuacción vamos a hacer un analisis crítico de los dos modelos cuando empleados con objetivos de seguridad.

Encuesta realizada en septiembre de 2007

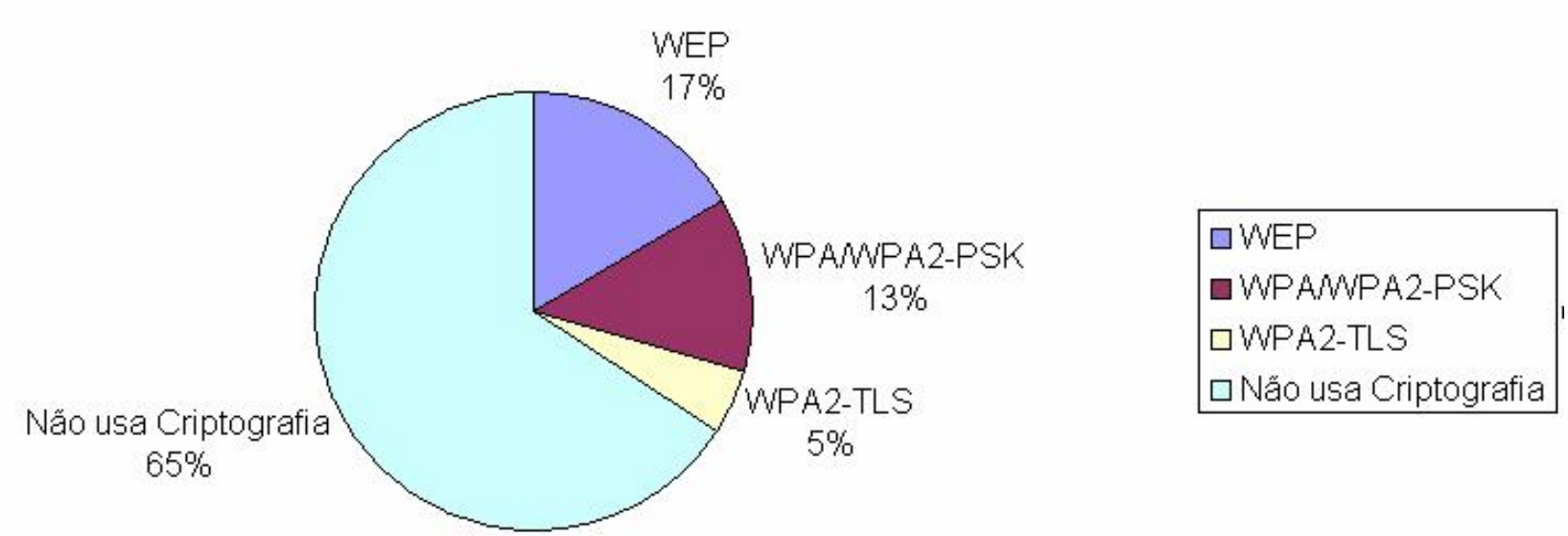
Proveedores que responderan a la Encuesta: 74

Numero de Clientes atendidos: 52.385

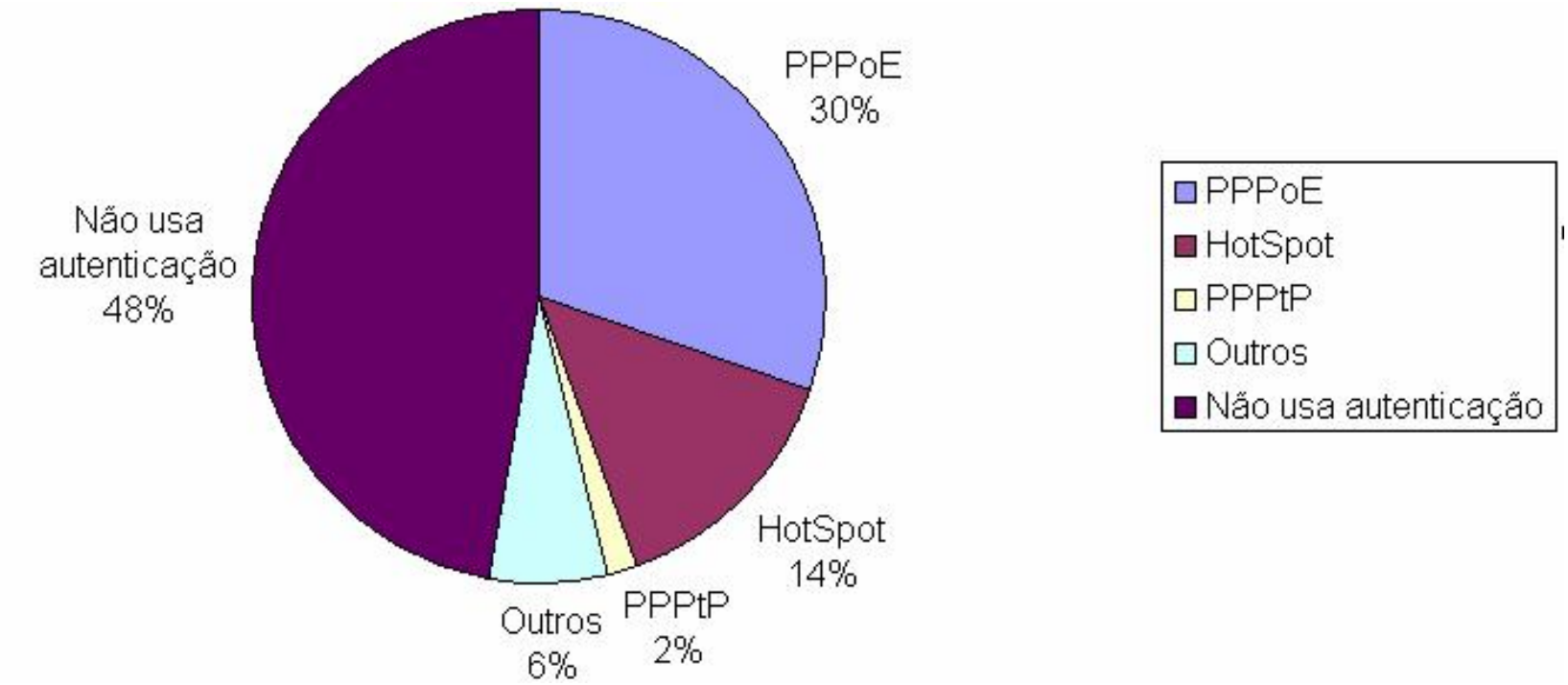
Total de Link contratado: 585.6 mbps

Los resultados fueran compilados de manera ponderada por ele numero de clientes atendidos. Por ejemplo, la respuesta de un proveedor que tiene 1000 clientes vale 10 veces a de un que tiene 100 clientes.

Encuesta realizada en septiembre de 2007
Encriptacción



Encuesta realizada en septiembre de 2007
Autenticacción



OBS: De todos que usan autenticación PPPoE o Hotspot solamente 4% usan tambien encriptación. (96% usan solamente PPPoE o Hotspot como medida de seguridad)

Spoof de MAC y o IP

Soluciones (no 80211i) para la última milha

Para tratar de asegurar el servicio en la última milla, muchos proveedores utilizan las soluciones:

→Túneles PPPoE

→Autenticación Hotspot

A continuacción vamos a hacer un analisis crítico de los dos modelos cuando empleados con objetivos de seguridad.

Tuneles PPPoE
aspectos generales

→ PPPoE : originalmente desarollado para redes alambradas .

→ El PPPoE Server (PPPoEd) escucha las requisiciones de PPPoE clients que utilizan el protocol PPPoE discovery.

→ PPPoE por defecto no es encriptado – puede ser configurado si el cliente soporta encriptación.

→User/password puede ser protegido empleando de método CHAP authentication. PAP passes in plain text.

Tuneles PPPoE
aspectos generales

→ La interface que “escucha” las requisiciones PPPoE no deben tener configurado IP “roteado”. Se lo tiene es posible pasar a largo de la autenticación PPPoE configurando de forma manual um IP de la grade.

→ Como otros tuneles, los valores de MTU and MRU deben ser modificados.

→ PPPoE es sensible a variaciones de señal

→ En máquinas Windows es necessario a instalación de un marcador, lo que representa trabajo administrativo.

PPPoE y Seguridad

→ Un atacante que falsifique una dirección MAC no logra navegar, pero causa muchos problemas para el usuario verdadero.

.

→ Quando el concentrador PPPoE está corriendo en la misma máquina del AP, un MAC falso causa la negación de servicio al usuario verdadero quando este intenta conectarlo.

→ Lo más grave que tiene PPPoE es que **el usuario no autentica el Servidor**. Por esse motivo un ataque del tipo “hombre del medio” puede facilmente ser implementado. Basta que un atacante ponga un AP falso en una posición privilegiada y accione um PPPoE Server para capturar las requisiciones PPPoE discover de los clientes y aceptar qualquier usuario/contraseña que sea.

Hotspots
aspectos generales

→ Originalmente fueram desarollados para dar servicio de conexión a Internet en Hoteles, Shoppings, etc. Con el tiempo, WISP's hacen uso de Hotspots como medio para autenticar usuarios.

→ La interface configurada como Hotspot escucha las requisiciones de navegación y pide usuario/contraseña.

→ Mikrotik puede autenticar en la base local o en un Radius externo.

→ Con Certificados digitais en el box Mikrotik se puede configurar un Hotspot com https.

Hotspots y Seguridad

→ Una vez que un usuario se ha autenticado y su par IP + MAC sea descobierto y falsificado por un atacante, el atacante gana acceso sin tener usuario/contraseña. El punto de acesso no “ve” dos, pero solo un usuario. El servicio se queda malo para los dos (pero lo atacante sabe el motivo) y no hay conflicto.

→ Cuando se trabaja sin Certificados, el ataque del “hombre del medio” puede ser hecho como en PPPoE porque el cliente no autentica el Hotspot.

→ Trabajando con Certificados se puede en el primer acceso instalar en la máquina del cliente el Certificado y enseñar al Cliente los riscos de aceptar un Certificado diferente.

PPPoE x Hotspot & seguridad - conclusiones

→ PPPoE tiene muchas ventajas porque trabaja en capa 2 y no hay tráfico IP. Muchos problemas como vírus. broadcasts, etc no existen en una planta basada en PPPoE

→ El ataque del “hombre del medio” es muy sencillo de implementar contra los WISP’s que usan PPPoE. No hay mucho por hacer para evitar esto..

→ Hotspots tambien son vulnerables pero si son bien configurados e instalados con Certificados digitales pueden evitar el “hombre del medio” pero los usuarios tienen que tener conocimiento de una serie de prácticas.

→Los dos son excelentes herramientas de ayuda para la administración de la Red, principalmente cuando trabajando en conjunto com Radius.

→ **PPPoE y Hotspot ayudan, pero no significan seguridad !!!**

Seguridad – conclusiones (casi) finales

Seguridad en el medio Inalámbrico que cumpla los princípios básicos de

- Autenticación
- Confidencialidad
- Integridad de datos

Solo se consigue con la utilización de una estrutura basada en 802.11i con EAP-TLS implementada con Certificados Digitales + Radius.

Otras implementaciones como la formación de VPN's entre los clientes y un Concentrador son eficaces pero en escala de implementación pueden mostrarse inefectivas.

¿ Porque los WISP's no utilizan 802.11i ?

WISP's dicen que no utilizan 802.11i por los motivos abajo:

- → Mucha Complejidad
  - → **(con Mikrotik todo es muy sencillo!!)**
- → Por ser un padrón abierto se esperan problemas de seguridad para el futuro
  - → **(puede ser una verdad, pero la realidad es hoy)**
- → Equipos antigos no permitem encriptacción.
  - → **(Mikrotik permite varios profiles. Hasta WEP puede ser una buena salida)**
- → Antiguos problemas de Wep hacen criptografia no creíble
  - → **(Las diferencias son muchas. No hay comparación)**
- → Problemas de performance cuando se usa encriptacción.
  - → **(Nuevos Chipsets Atheros tienen encriptación por hardware, no hay problemas de performance)**

Servicio afectado por ataques de capa 2

Servicio afectado por ataques de capa 2

IEEE 802.11i se preocupó con

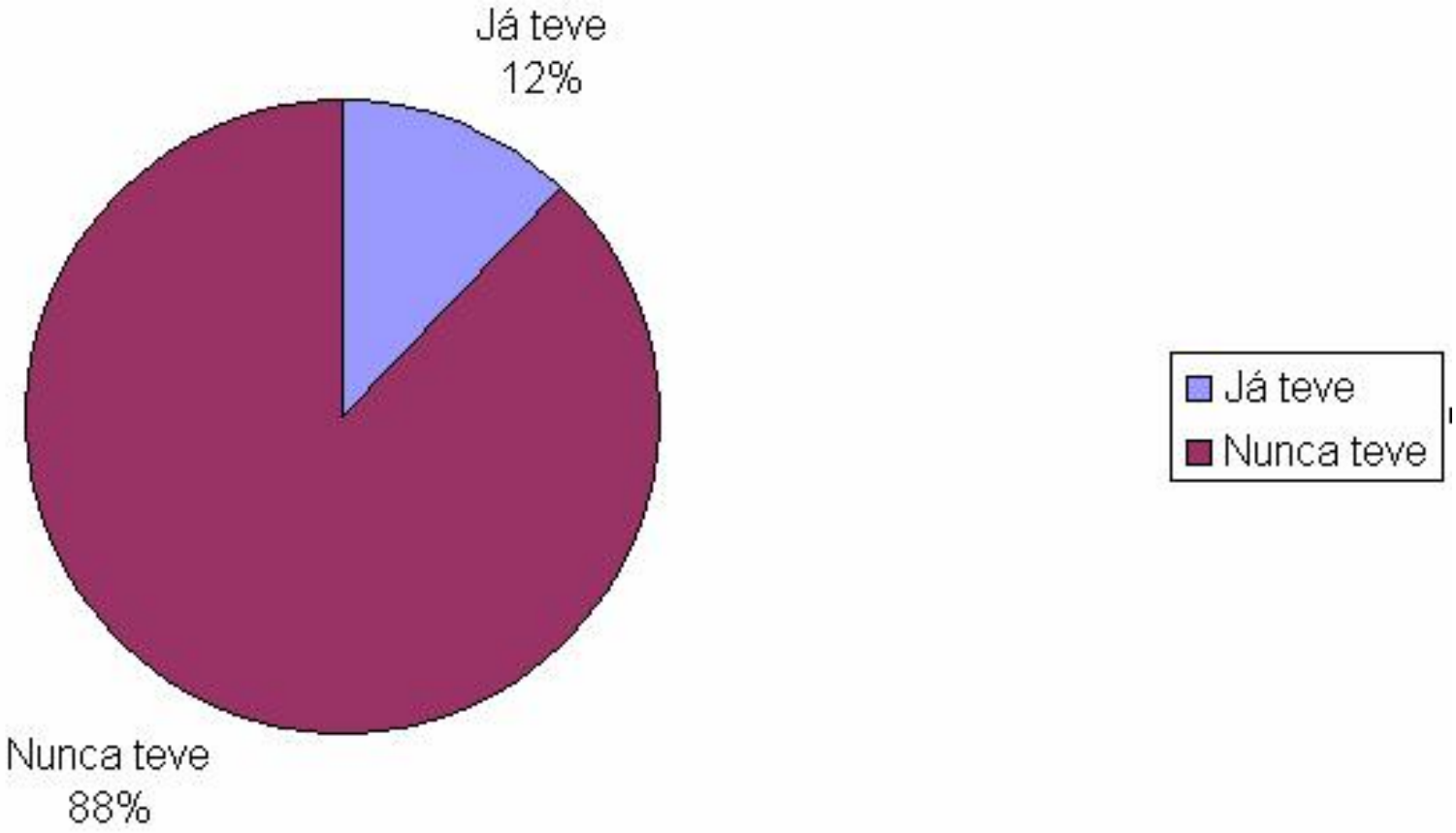
- → Autenticación
- → Confidencialidad
- → Integridad

Desafortunadamente 802.11i no se preocupó con la ***disponibilidad*** del servicio.

El Servicio Wi-Fi puede ser comprometido con dos tipos de ataque:

- → Basados en alto poder de RF (verdaderamente un ataque de capa 1)
- → Basados nel protocol 802.11

Ataque al medio fisico



Servicio afectado por ataques de capa 2

→ Basados en alto poder de RF (Jamming)

No hay nada que hacer en Mikrotik. La única medida posible es llamar las autoridades responsables por el espectro radioelectico.

Un buen projecto de RF puede ayudar mucho.

→ Basados en el protocol 802.11

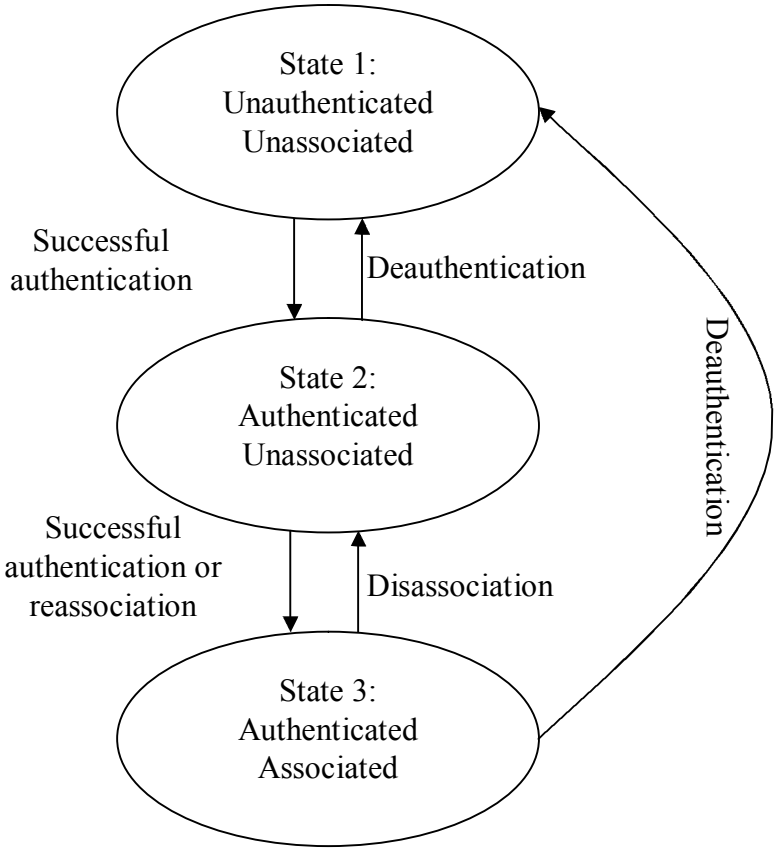
Son basados en debilidades del protocol 802.11 muy dependente de MAC address

Hay muchas herramientas disponibles en la Internet que pueden ser usadas para Ataques com. Void11, airreplay, etc.

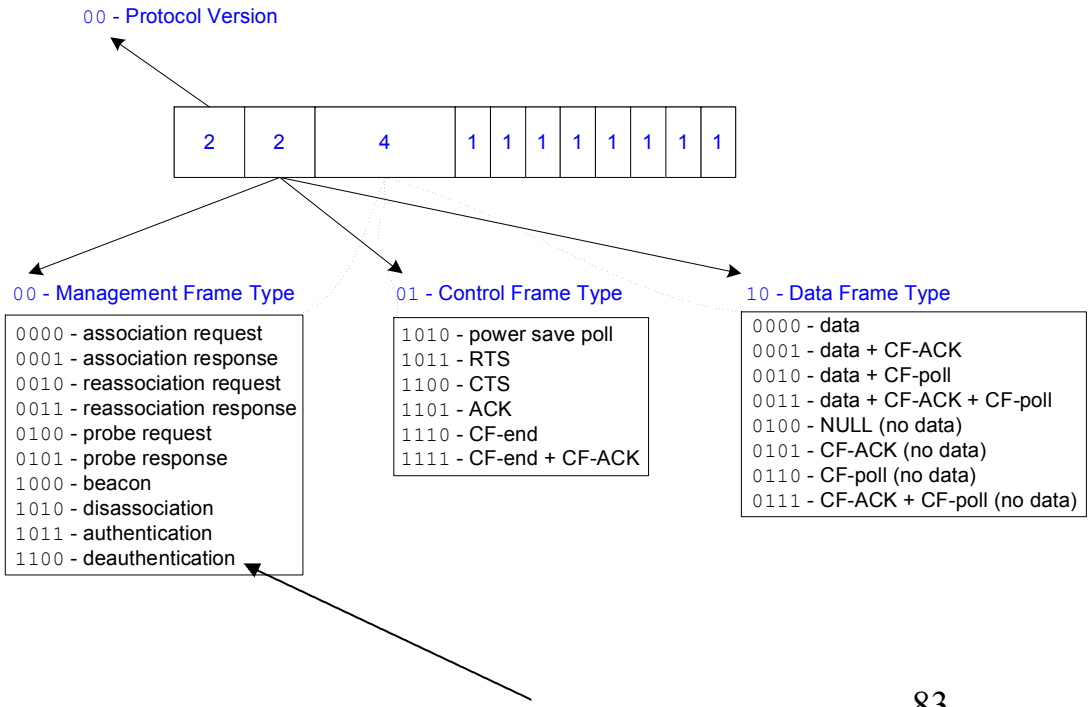
www.wlanbrasil.com.br/donwloads/seguranca/cd1.iso

www.wlanbrasil.com.br/donwloads/seguranca/cd2.iso

Proceso de association



802.11 Types and Subtypes



Ataque de Deauth

1 – El atacante utiliza alguna herramienta como airopeek, kismet, wellenreiter, para descubrir :

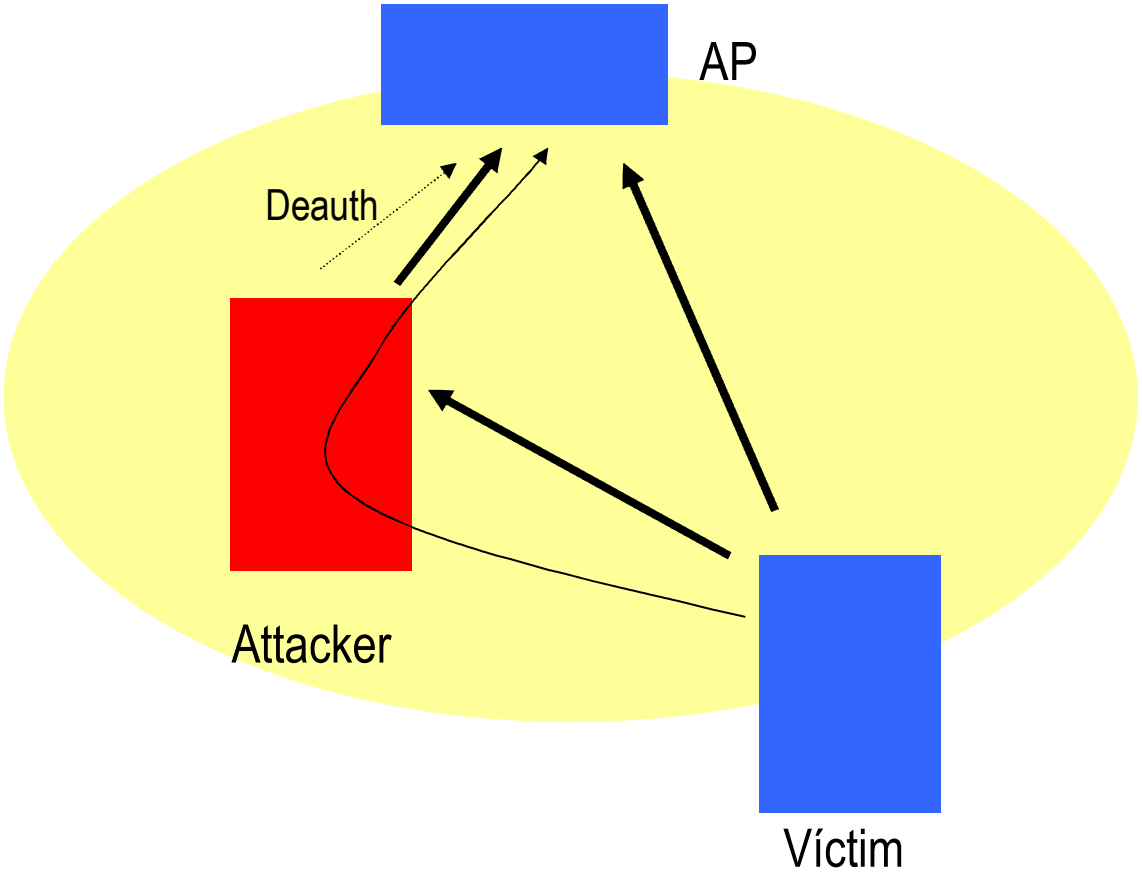
→ El MAC del AP
→ El MAC del Cliente
→ Canal de RF

2 – Lanza paquetes de deauth en el aire

→ NO necesita de potencia alta
→ NO necessita asociación
→ NO necesita estar en la tabla de MAC's

Solo tiente que tener una targeta inalámbrica apropiada que permite inyeción de paquetes, como Prism, Atheros, Ralink, etc y el driver apropiado.

Hombre del medio “in aire” (Monkey Jack attack)



Contramedidas para De-auth Attack con Mikrotik

Modificación del Protocol

- → Con una modificación del protocol 802.11 este tipo de ataque puede ser evitado.
- → La idea es basada en que los equipos no obedezan paquetes de deauth
- → Hay que ver se la modificación tiene impactos para otras cosas
- → Teniendo en cuenta que Nstreme es un protocolo propietário quiza Mikrotik pueda pueda implementar

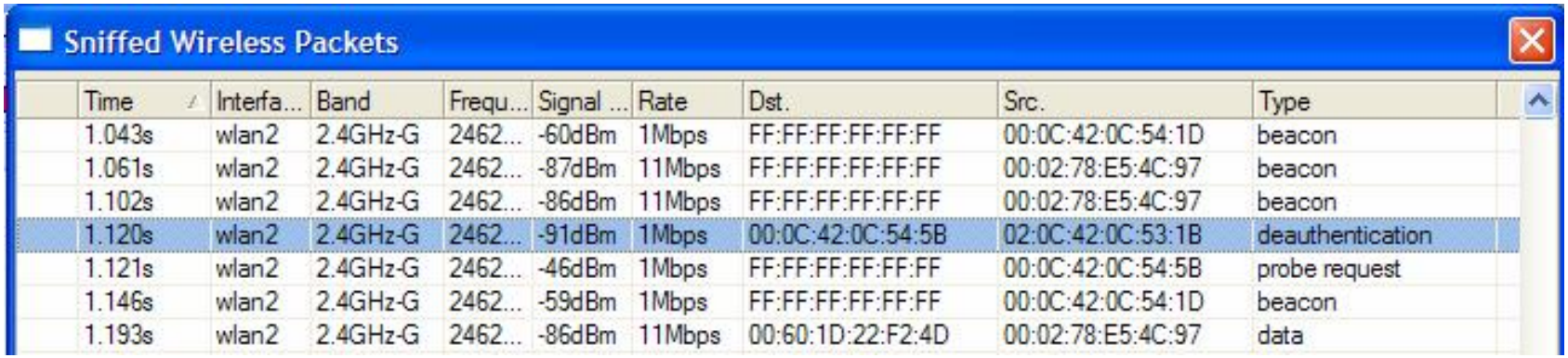
- → Abajo hay un link para un articulo que describe los problemas y propone soluciones

http://sysnet.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-slides.pdf

Contramedidas para De-auth Attack con Mikrotik

La primera cosa que tiene que hacer es estar seguro que estás con este tipo de ataque

Los paquetes inalámbricos pueden ser sniffados em /interface/wireless/sniffer



Time	Interfa...	Band	Frequ...	Signal ...	Rate	Dst.	Src.	Type
1.043s	wlan2	2.4GHz-G	2462...	-60dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:0C:42:0C:54:1D	beacon
1.061s	wlan2	2.4GHz-G	2462...	-87dBm	11Mbps	FF:FF:FF:FF:FF:FF	00:02:78:E5:4C:97	beacon
1.102s	wlan2	2.4GHz-G	2462...	-86dBm	11Mbps	FF:FF:FF:FF:FF:FF	00:02:78:E5:4C:97	beacon
1.120s	wlan2	2.4GHz-G	2462...	-91dBm	1Mbps	00:0C:42:0C:54:5B	02:0C:42:0C:53:1B	deauthentication
1.121s	wlan2	2.4GHz-G	2462...	-46dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:0C:42:0C:54:5B	probe request
1.146s	wlan2	2.4GHz-G	2462...	-59dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:0C:42:0C:54:1D	beacon
1.193s	wlan2	2.4GHz-G	2462...	-86dBm	11Mbps	00:60:1D:22:F2:4D	00:02:78:E5:4C:97	data

El paquete de tipo “deauthentication” principalmente en gran número muestra que la red esta sufriendo un ataque deauth

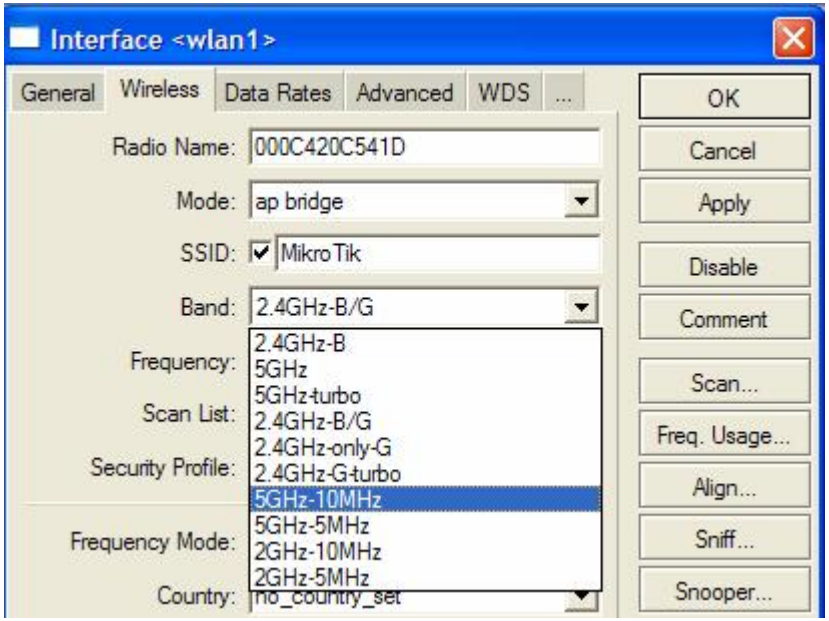
Verifique principalmente los MAC’s de origen y destino.

Contramedidas para De-auth Attack con Mikrotik

Los modos de operación que emplean ancho de 10 y 5 Mhz. no son afectados por las herramientas de deauth

Nosotros testamos en la práctica con Void11 y air-replay.

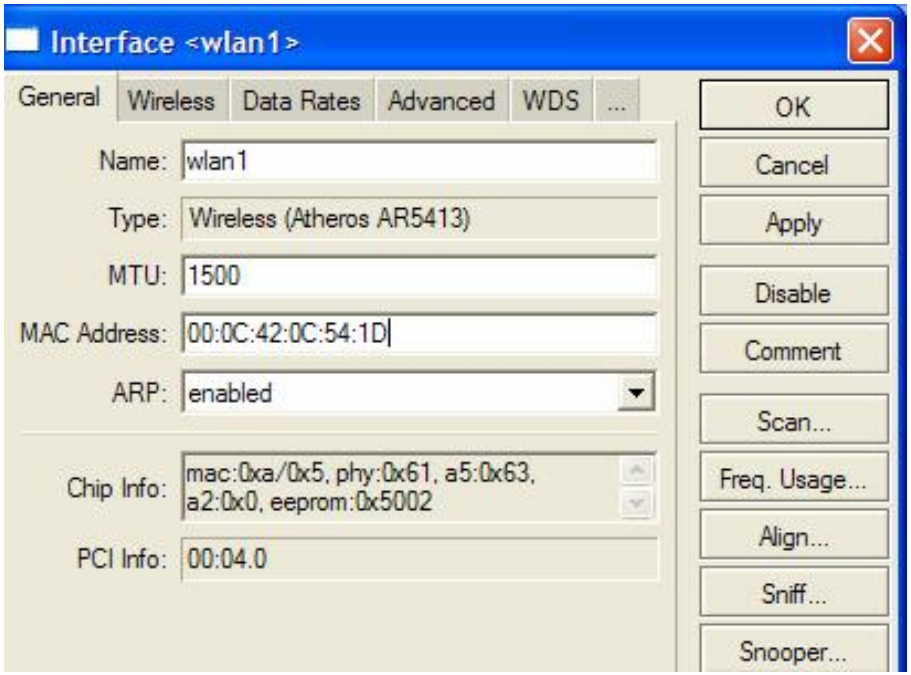
Si el ataque esta siendo hecho en un link Punto a Punto cámbialo para 10 o 5 Mhz puede ser una buena solución.



Contramedidas para De-auth Attack con Mikrotik

Como los ataques son hechos utilizando el AP MAC, una salida es cambiar el MAC en el Mikrotik

Esta puede no ser considerada una mediada elegante de seguridad, pero un trabajo puede ayudar que el atacador descubra el nuevo MAC.



Contramedidas para De-auth Attack con Mikrotik

Seguridad por “obscuridad”

Utilizando AP’s Virtuales que no hacen nada, pero so lanzan broadcasts con SSID’s y MAC’s puedes crear un ambiente muy dificil de ser sniffado.

- → Con Mikrotik puedes tener AP’s virtuales con diferentes direcciones MAC
- → Puedes con scripts adicionales crear, habilitar y desabilitar dinamicamente muchas más AP’s virtuales con muchos MAC’s.

OBS: La idea es parecida con que lo hace el Script Perl llamado “Fake AP”

http://www.blackalchemy.to/project/fakeap

Muchas Gracias !

Paldies !

Obrigado !

Wardner Maia
maia@mikrotikbrasil.com.br