Segurança de acesso Redes Wireless e Cabeadas

MUM Brasil – São Paulo – Outubro, 2008

Eng. Wardner Maia

Introdução

Nome: Wardner Maia

→ Engenheiro Eletricista modalidades Eletrotécnica/Eletrônica/Telecomunicações

→ Provedor de Internet Service desde 1995

→ Utilizando rádio frequencia para provimento de acesso desde 2000

→ Ministra treinamentos em rádio frequencia desde 2002 e em Mikrotik desde 2006

→ Certificado pela Mikrotik em Wireless, Roteamento e como Trainer desde 2007

→ Trabalha como engenheiro para a empresa MD Brasil TI & Telecom e para a Rede Global Info – maior rede de provedores independentes do Brasil

Introdução

MD Brasil – TI & Telecom

→ Operador de serviços de Telecom e de Serviços de Valor Adicionado

→ Distribuidora oficial de Hardware e Software Mikrotik

→ Parceira da Mikrotik em treinamentos

www.mdbrasil.com.br / www.mikrotikbrasil.com.br

Porque segurança em Wireless ?

→ Wireless é muitas vezes a única solução para muitas cidades e áreas rurais não cobertas pelas tradicionais e grandes empresas de Telecomunicações.

→ Wireless é a forma mais fácil e rápida de ganhar participação de mercado em provimento de acesso.

→ Boas implementações tem performance similares às de DSL e Cabo.

→ ***Segurança é o Calcanhar de Aquiles para redes Wireless baseadas em equipamentos baseados na tecnologia Wi-Fi (IEEE 802.11).***

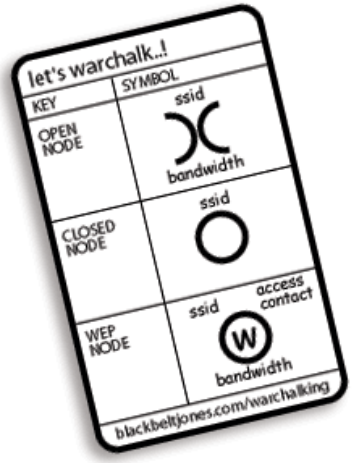
Porque segurança em Redes Ethernet urbanas ?

- Muitos pequenos provedores tem migrado para tecnologia ethernet, lançando cabos UTP, STP e Fibra nas ruas

- A despeito de muito questionamento de técnicos mais tradicionais, esses empreendedores tem conseguido resultados muito expressivos, seja do ponto de vista de clientes atendidos como da própria qualidade do serviço prestado.

- O “mix” Wireless + Wired mostra-se uma alternativa impar na competição com tecnologias tradicionais.

- ***Infelizmente muitas implementações tem sido feitas sem os devidos cuidados podendo comprometer/denegrir a evolução dessa tecnologia.***



Objetivos da Apresentação

→ Dar uma visão geral dos conceitos teóricos envolvidos na segurança de links Wi-Fi e como implementa-las na prática usando o Mikrotik.

→ Fazer uma análise crítica dos modelos de segurança adotados atualmente pelos provedores que usam Wireless e Cabo.

→ Ataques de camada 2, o que são e os desafios para enfrenta-los.

“O poder das batatas”

Dentre 43 Redes sem fio localizadas no mais importante centro financeiro de São Paulo, apenas 8 tinham tomado as medidas de segurança “recomendadas”

Info Exame - 2002

“O poder das batatas”

Em 2002, de acordo com a matéria, as medidas de segurança recomendadas eram:

→ Nome de rede escondido

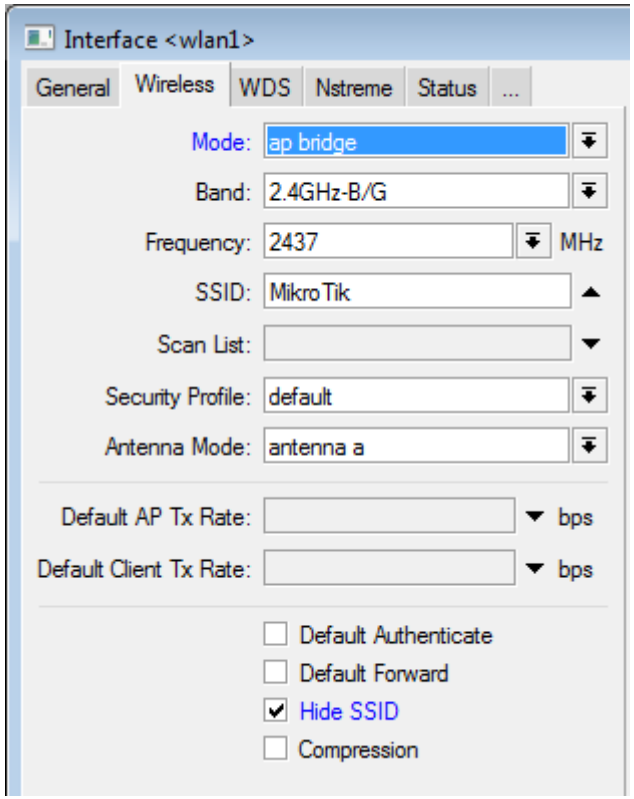
→ Controle de acesso por MAC

→ Criptografia WEP

Segurança “Rudimentar”
(O que não é segurança)

1 – Nome de rede (SSID) escondido

Pontos de Acceso sem fio por padrão fazem o broadcast do seu SSID nos pacotes chamados “beacons”. Este comportamiento puede ser modificado no Mikrotik habilitando a opção Hide SSID.



Fragilidades:

→ SSID tem de ser conhecido pelos clientes

→ Scanners Passivos descobrem facilmente pelos pacores de “probe request”dos clientes.

Segurança “Rudimentar”
(O que não é segurança)

2 – Controle de MAC’s

→ Descobrir MAC’s que trafegam no ar é muito simples com ferramentas apropriadas

→ Airopeek (Windows), Kismet, Wellenreiter, (Linux/BSD)

→ O próprio Mikrotik, com Snooper e Sniffer

`

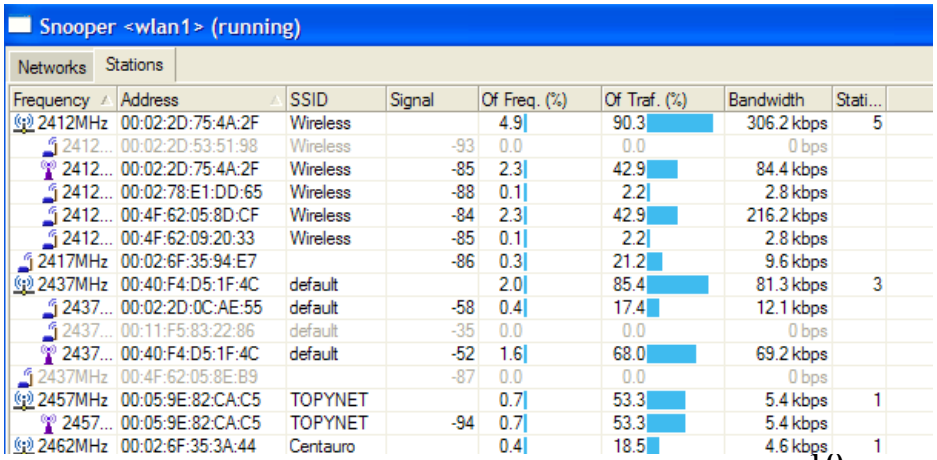
→ “Spoofar” um MAC é muito fácil, tanto em Linux como em Windows.

- FreeBSD :

ifconfig <interface> -L <MAC>

- Linux :

ifconfig <interface> hw ether <MAC>



Frequency	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Stati...
2412MHz	00:02:2D:75:4A:2F	Wireless		4.9	90.3	306.2 kbps	5
2412...	00:02:2D:53:51:98	Wireless	-93	0.0	0.0	0 bps	
2412...	00:02:2D:75:4A:2F	Wireless	-85	2.3	42.9	84.4 kbps	
2412...	00:02:78:E1:DD:65	Wireless	-88	0.1	2.2	2.8 kbps	
2412...	00:4F:62:05:8D:CF	Wireless	-84	2.3	42.9	216.2 kbps	
2412...	00:4F:62:09:20:33	Wireless	-85	0.1	2.2	2.8 kbps	
2417MHz	00:02:6F:35:94:E7		-86	0.3	21.2	9.6 kbps	
2437MHz	00:40:F4:D5:1F:4C	default		2.0	85.4	81.3 kbps	3
2437...	00:02:2D:0C:AE:55	default	-58	0.4	17.4	12.1 kbps	
2437...	00:11:F5:83:22:86	default	-35	0.0	0.0	0 bps	
2437...	00:40:F4:D5:1F:4C	default	-52	1.6	68.0	69.2 kbps	
2437MHz	00:4F:62:05:8E:B9		-87	0.0	0.0	0 bps	
2457MHz	00:05:9E:82:CA:C5	TOPYNET		0.7	53.3	5.4 kbps	1
2457...	00:05:9E:82:CA:C5	TOPYNET	-94	0.7	53.3	5.4 kbps	
2462MHz	00:02:6F:35:3A:44	Centauro		0.4	18.5	4.6 kbps	1

Segurança “Rudimentar” (O que não é segurança)

3 – Criptografia WEP

→ “Wired Equivalent Privacy” – foi o sistema de criptografia inicialmente especificado no padrão 802.11 e está baseada no compartilhamento de um segredo (semente) entre o ponto de Acesso e os clientes, usando o algorítimo RC4 para a criptografia.

→ Várias fragilidades da WEP foram reveladas ao longo do tempo e publicadas na Internet, existindo muitas ferramentas para quebrar a chave, como:

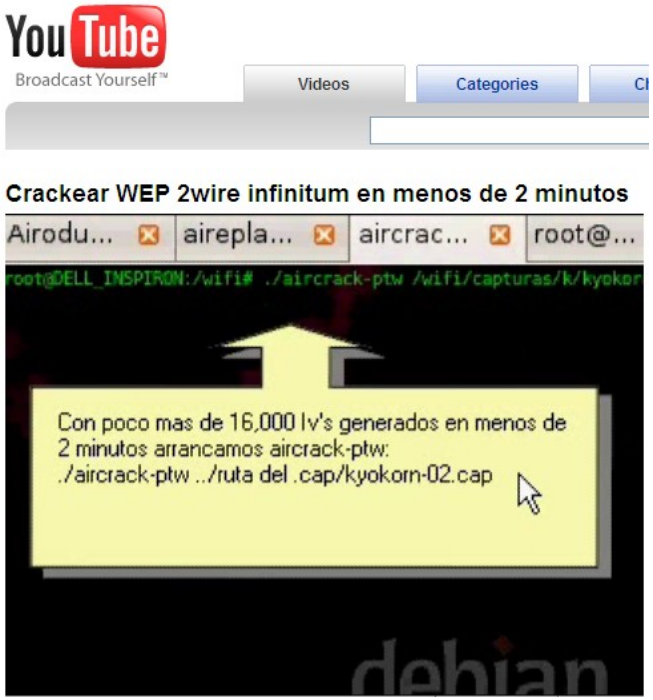
- → Airodump
- → Airreplay
- → Aircrack

→ Hoje é trivial a quebra da WEP que pode ser feita em poucos minutos com técnicas baseadas nas ferramentas acima.

Comprometendo a WEP (em definitivo)

→ Suporte muito vasto para crackear a WEP

You Tube Vídeo (em espanhol)
http://www.youtube.com/watch?v=PmVtJ1r1pmc

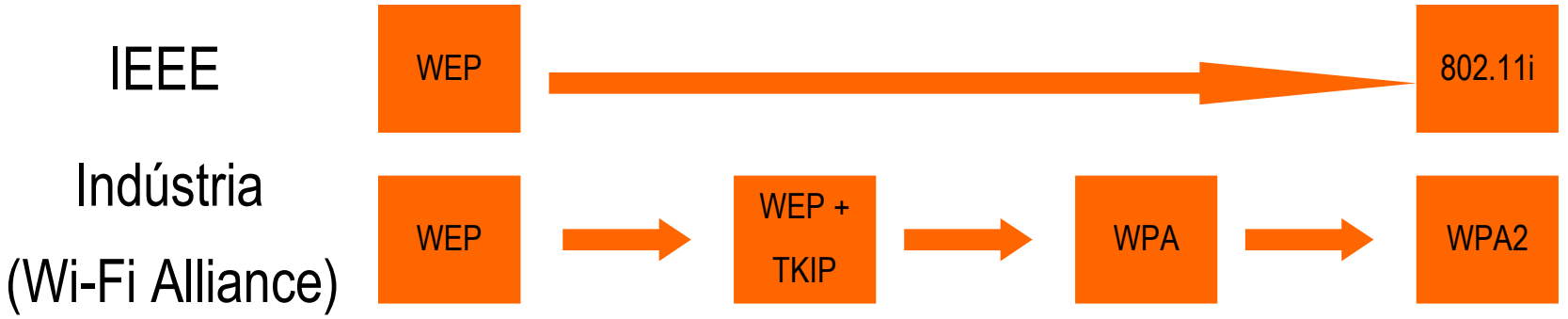


IEEE 802.11i

→ Devido aos problemas apresentados pela WEP o IEEE criou o Grupo de trabalho – 802.11i cuja tarefa principal era fazer a especificação de um padrão de fato seguro.

→ Antes da conclusão do trabalho do grupo 802.11i a indústria lançou padrões intermediários, como o WEP+, TKIP e o WPA (Wireless Protected Access)

→ Em junho de 2004 o padrão foi aprovado e a indústria deu o nome comercial de WPA2.



Fundamentos de Segurança

→Privacidade

→ A informação não pode ser legível por terceiros

→Integridade

→ A informação não pode ser alterada quando em transito.

→Autenticação

AP → Cliente: O AP tem que garantir que o cliente é quem diz ser.

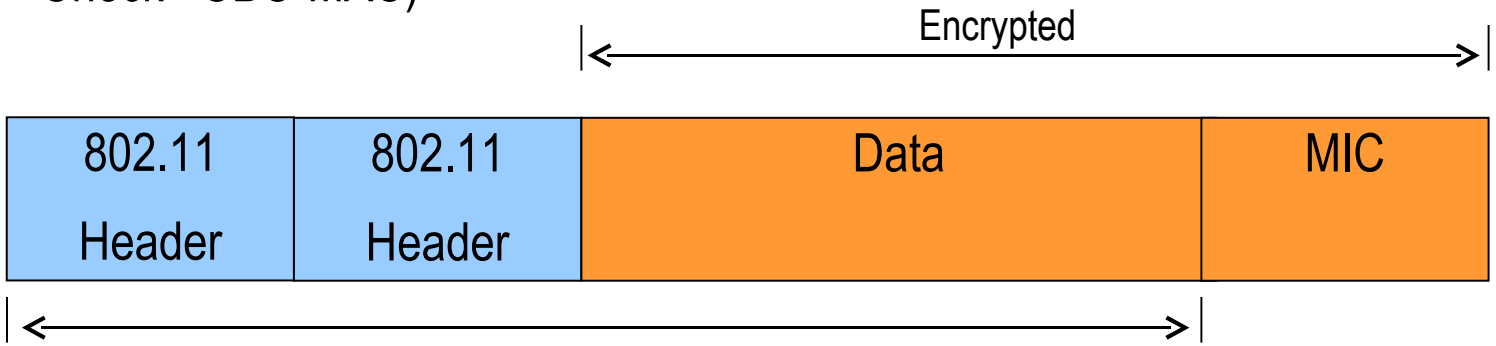
Cliente →AP: O Cliente tem que se certificar que está se conectando no AP verdadeiro. Um AP falso possibilita o chamado ataque do "homem do meio"

Privacidade e Integridade

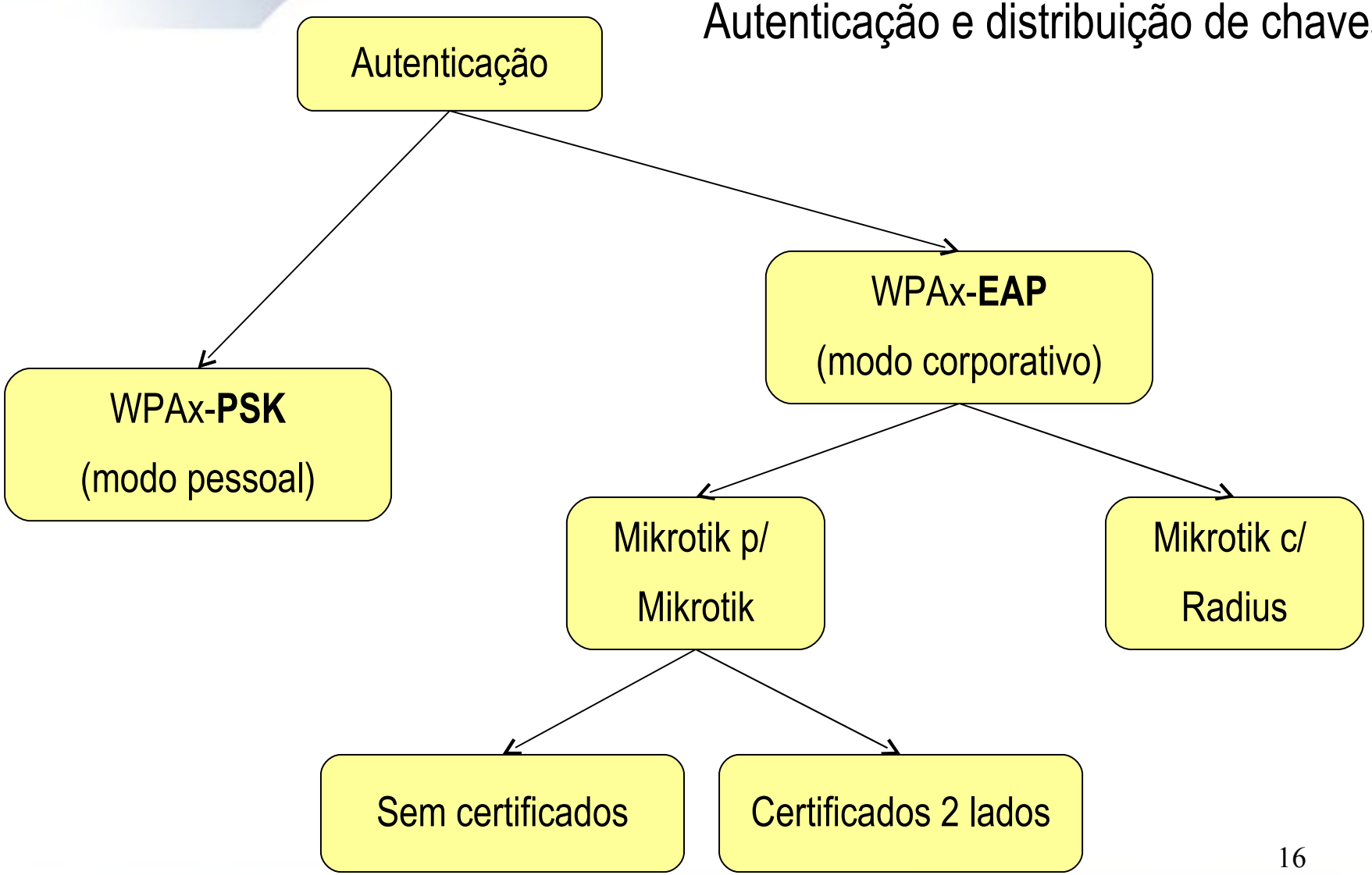
Tanto a privacidade como a integridade são garantidas por técnicas de criptografia.

→ O algorítimo de criptografia de dados em WPA é o RC4, porém implementado de uma forma bem mais segura que na WEP. Na WPA2 utiliza-se o AES.

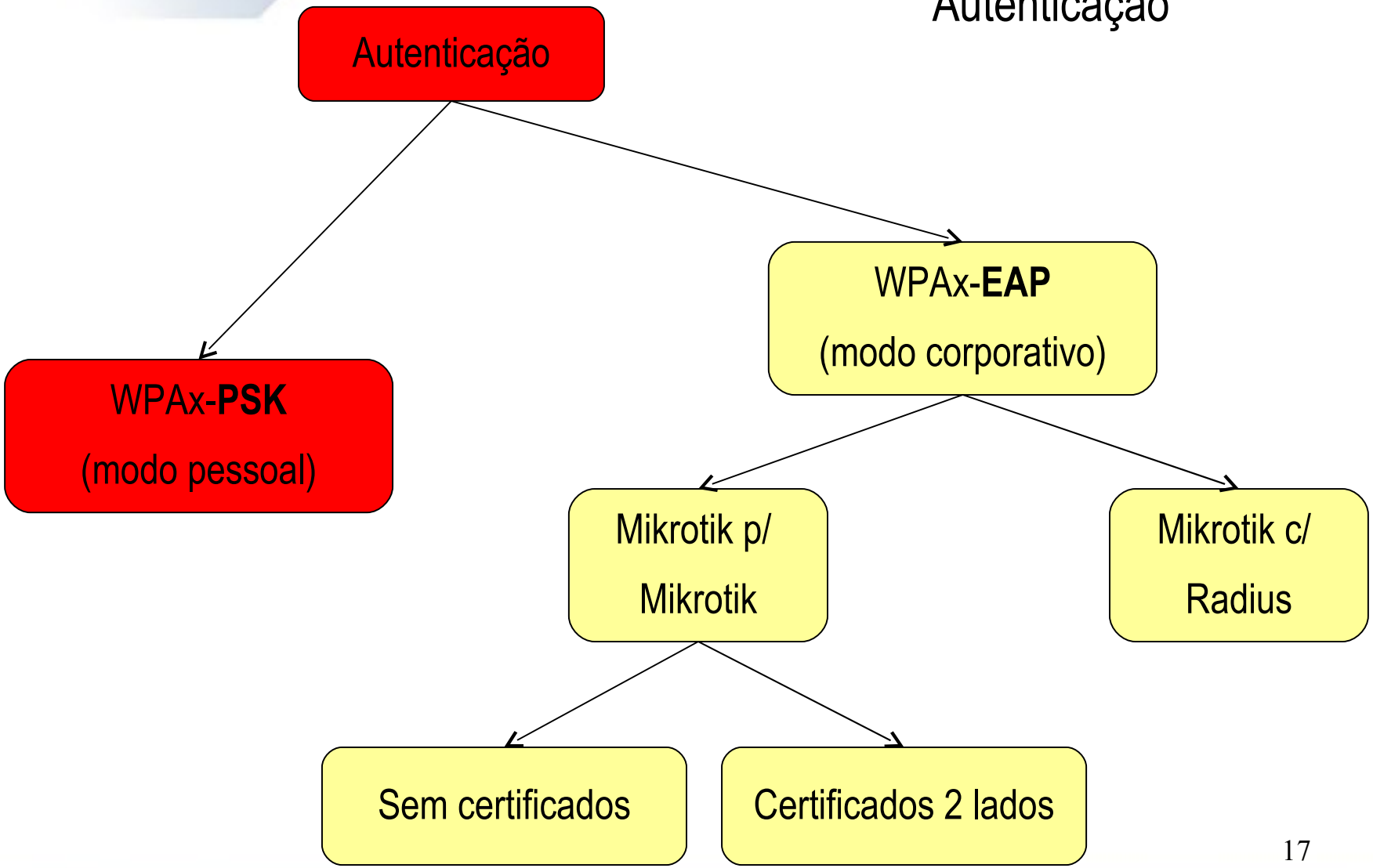
→ Para a Integridade dos dados WPA usa TKIP → Algoritimo de Hashing "Michael" e WPA2 usa CCMP (Cipher Block Chaining Message Authentication Check– CBC-MAC)



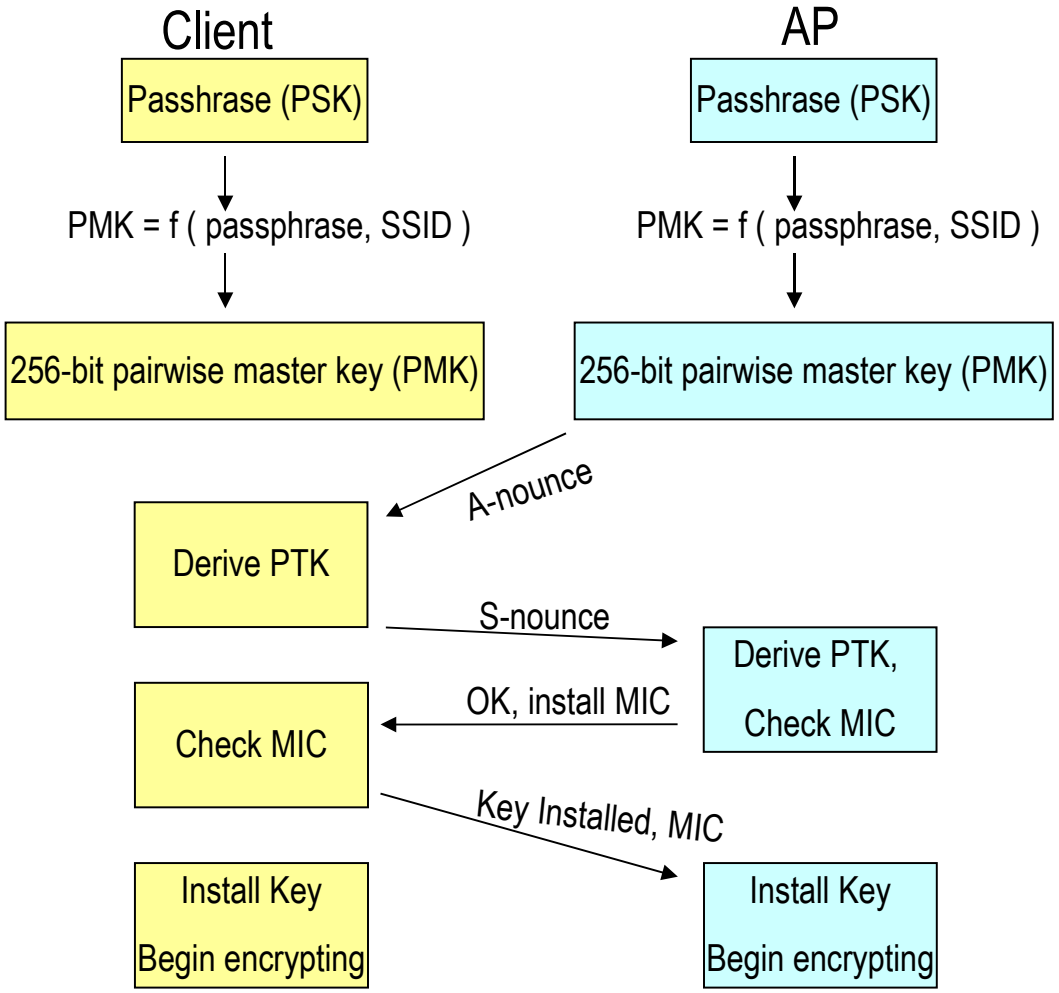
Autenticação e distribuição de chaves



Fundamentos de Segurança WPAx
Autenticação



Como funciona a WPAx-PSK



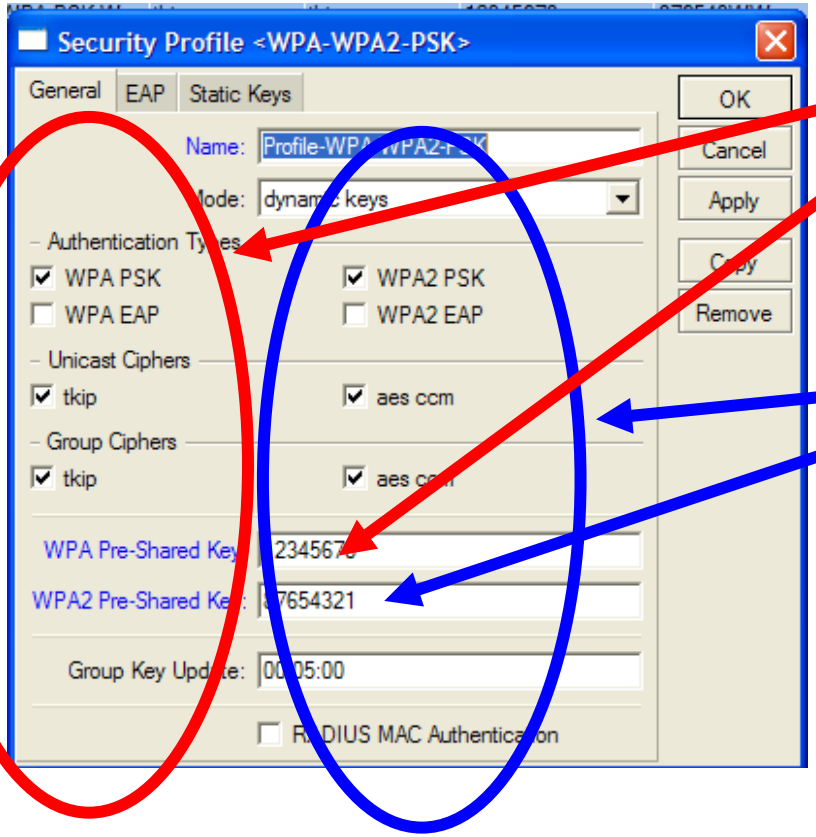
Uma chave “mestra“ chamada PMK – “Pairwise Master Key” é criada por um hash entre a “semente” e o SSID.

A PMK é guardada no Registro do Windows on no arquivo supplicant.conf do Linux

Outra chave chamada PTK - “Pairwise Transient Key” é criada de maneira dinâmica após um processo de handshake de 4 vias. PTK é única por sessão

Utilizando WPA/WPA2 – PSK

É muito simples a configuração de WPA/WPA2-PSK com o Mikrotik



→ **WPA - PSK**

Configure o modo de chave dinâmico,WPA PSK, e a chave pré combinada.

→ **WPA2 – PSK**

Configure o modo de chave dinâmico WPA2, PSK, e a chave pré combinada.

As chaves são alfanuméricas de 8 até 63 caracteres

WPA / WPA2 PSK é segura ?

- A maneira conhecida hoje para quebrar WPA-PSK é somente por ataque de dicionário.
- Como a chave mestra - PMK combina uma contrasenha com o SSID, escolhendo palavras fortes torna o sucesso por ataque de força bruta praticamente impossível.
- Projeto na Internet para estudo de fragilidades da WPA/WPA2 – PSK
  - Cowpatty http://sourceforge.net/projects/cowpatty
- ***A maior fragilidade no entanto da técnica de PSK para WISP's é que a chave se encontra em texto plano nos computadores dos clientes.***

WPA / WPA2 PSK é segura ?

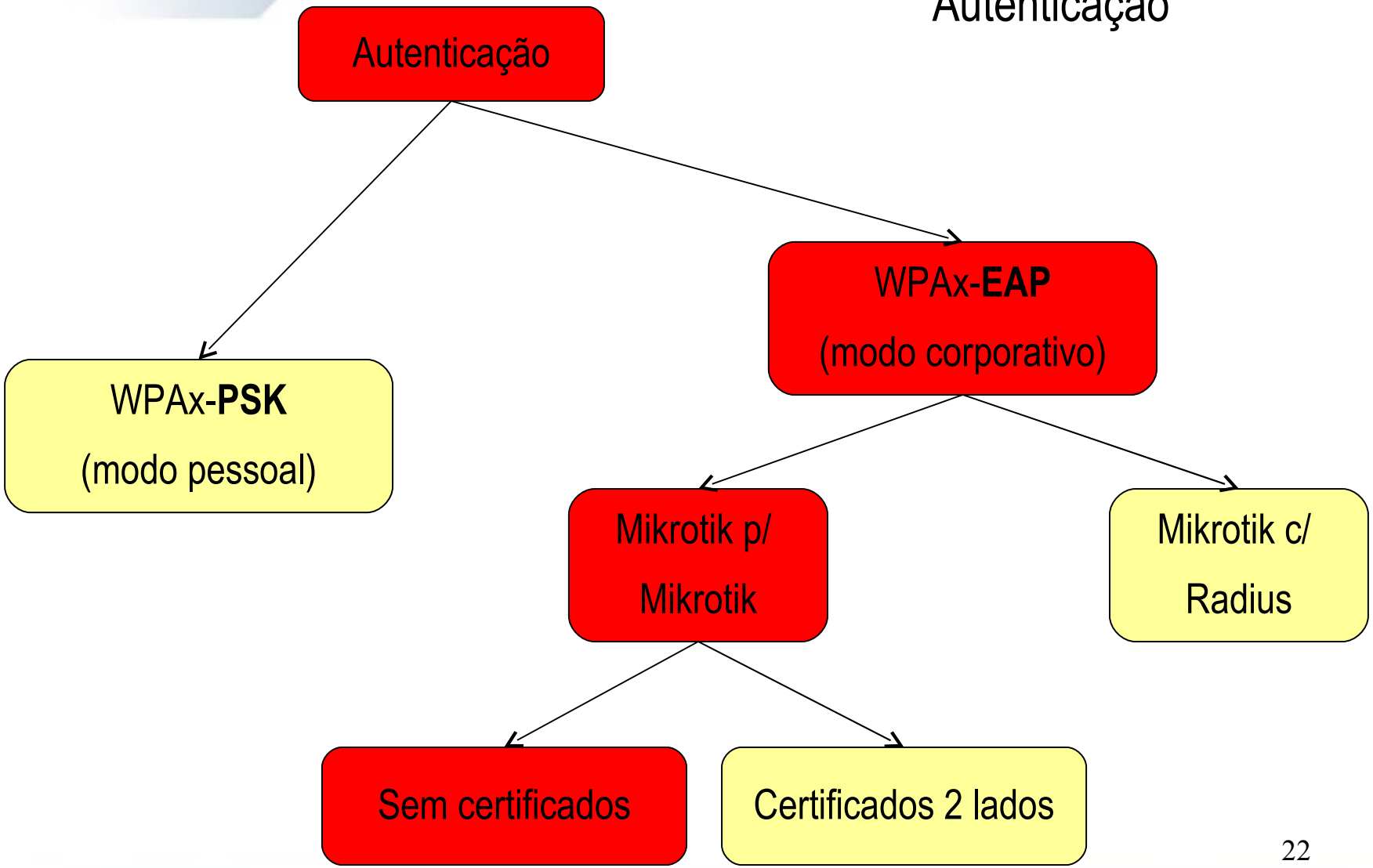
Quando o atacante tem a chave é possível:

- → Ganhar acesso não autorizado
- → Falsificar um Ponto de acesso e fazer o ataque do “homem-do-meio” (man-in-the-middle)

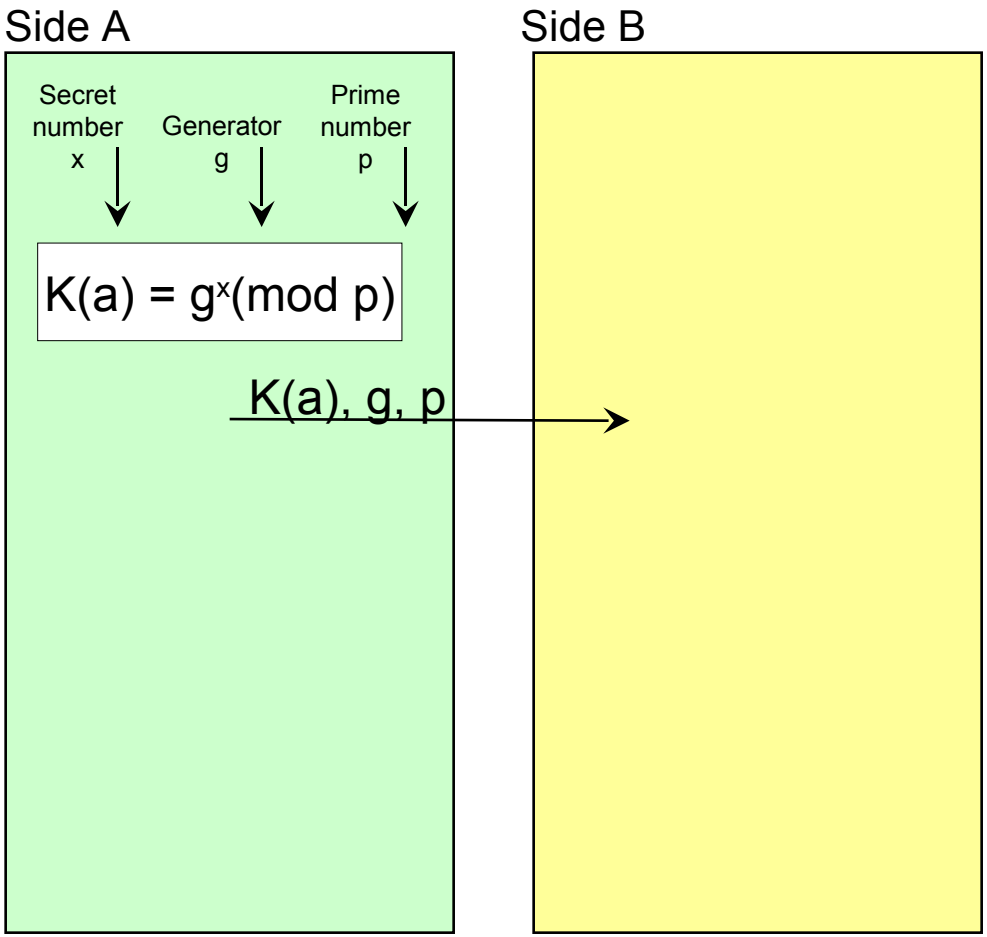
Recomendações para WISP’s

- → Somente use PSK se tem **absoluta certeza** que as chaves estão protegidas (somente tem acesso aos equipamentos dos clientes o próprio WISP)
- → Não se esqueça que as chaves PSK estão em **texto plano** nos Mikrotiks (até para usuários read-only)

Fundamentos de Segurança WPAx
Autenticação



Diffie-Hellmann (Without Certificates)



1. Cada lado escolhe um número secreto x g p.

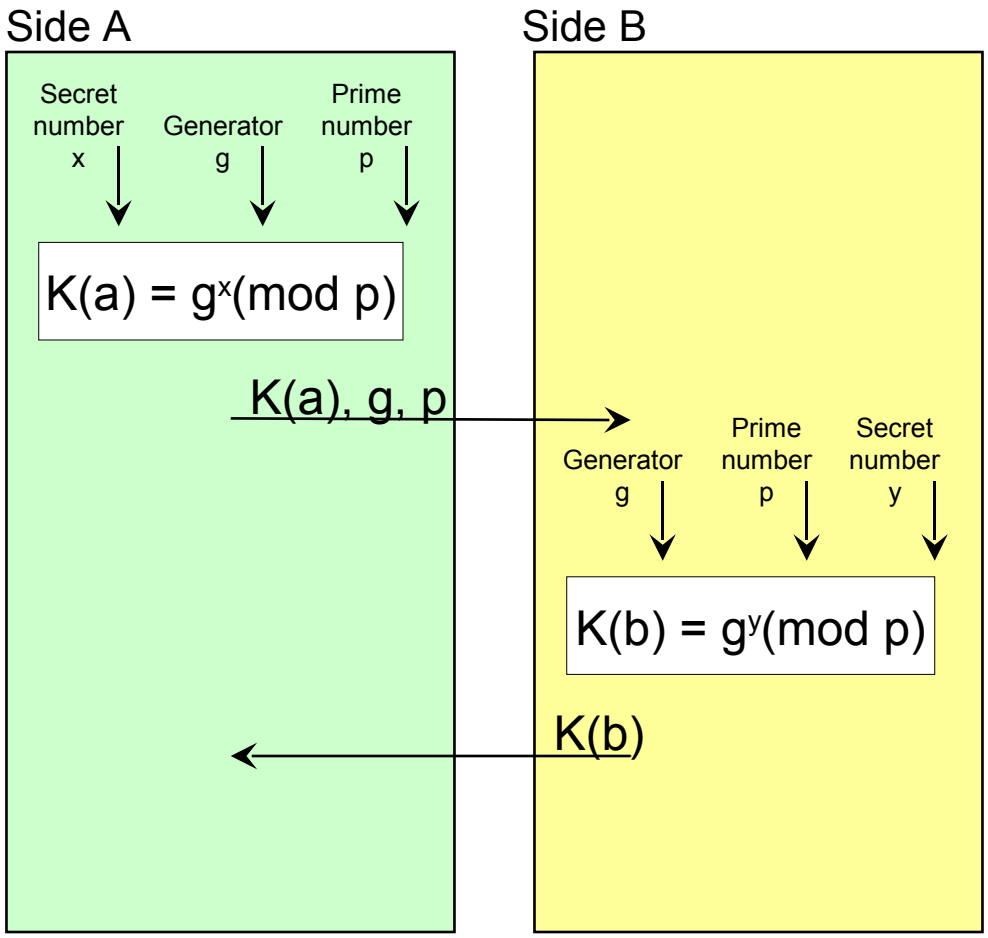
3. Lado A começa selecionando um número primo muito grande (p) e um pequeno inteiro – o gerador (g)

3. Lado A calcula usando aritmética modular a chave pública , K(a):

→ $K(a) = g^{x} \pmod{p}$

6. Lado A manda para o lado B a chave pública e o número primo (p), e o gerador (g)

Diffie-Hellmann (Without Certificates)



1. Lado B faz um cálculo similar com a sua chave secreta e o número primo e o gerador para obter sua chave pública.

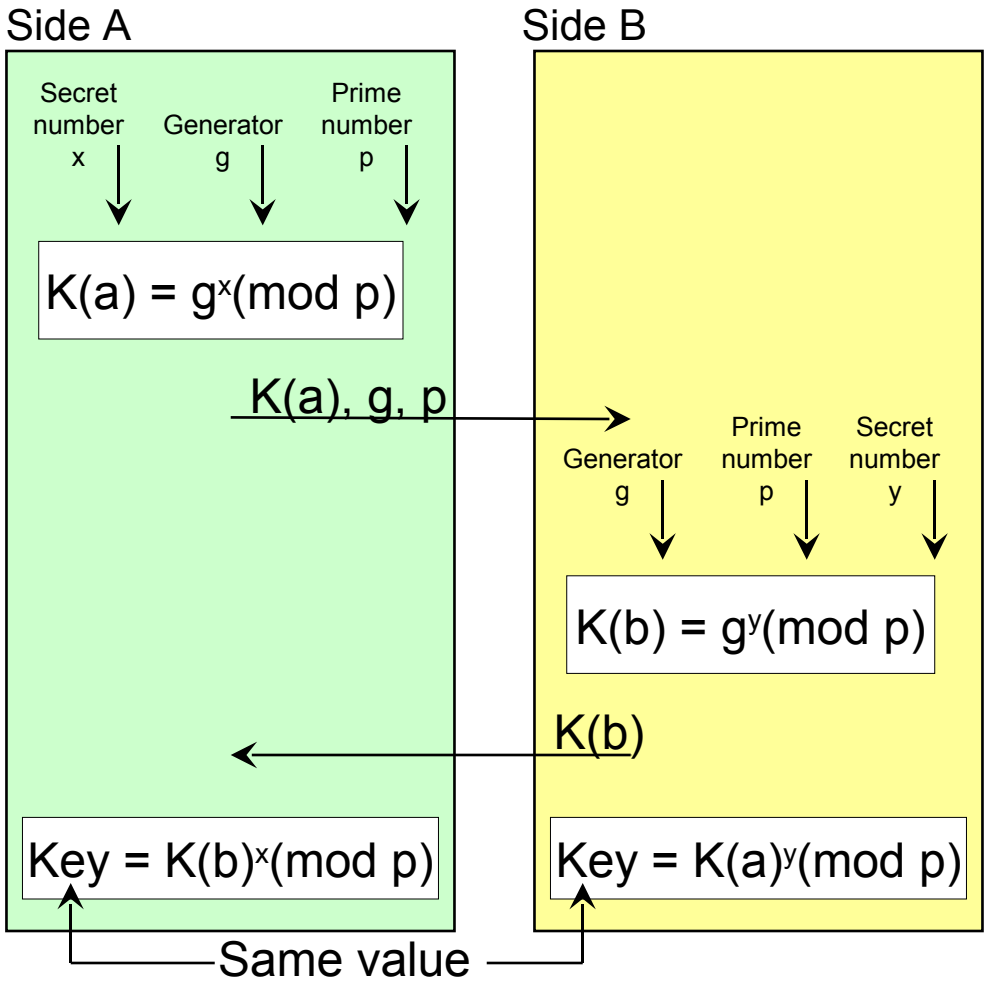
3. Lado B manda para lado A a cahve pública.

7. Agora os dados podem calcular uma mesma chave pré compartilhada (que não circulou pelo meio inseguro)

→ Shared key = $K(b)^x \pmod p$

→ Shared key = $K(a)^y \pmod p$

Diffie-Hellmann (Without Certificates)

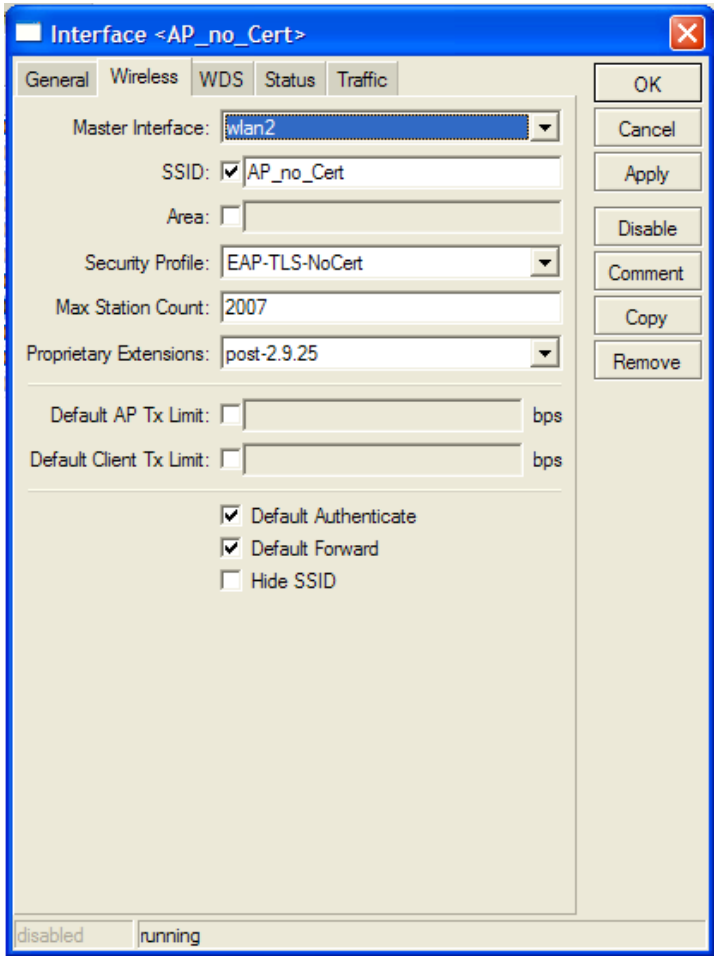


1. Os dois cálculos produzem valores exatamente iguais, graças a propriedade da aritmética modular

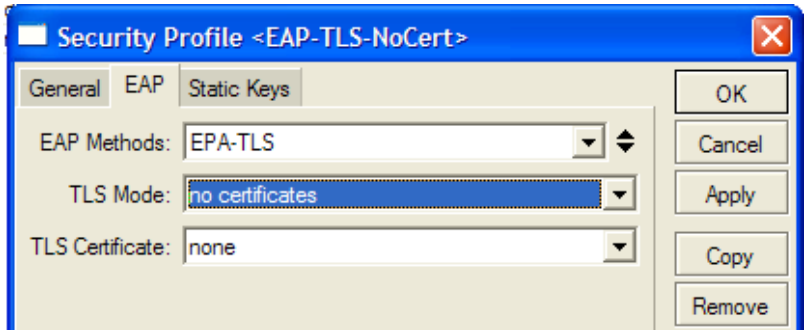
3. A chave calculada é utilizada como PMK e inicia o processo de criptografia normalmente (AES para WPA2 e RC4 para WPA)

Setup with EAP-TLS – No Certificates

AP Configuration

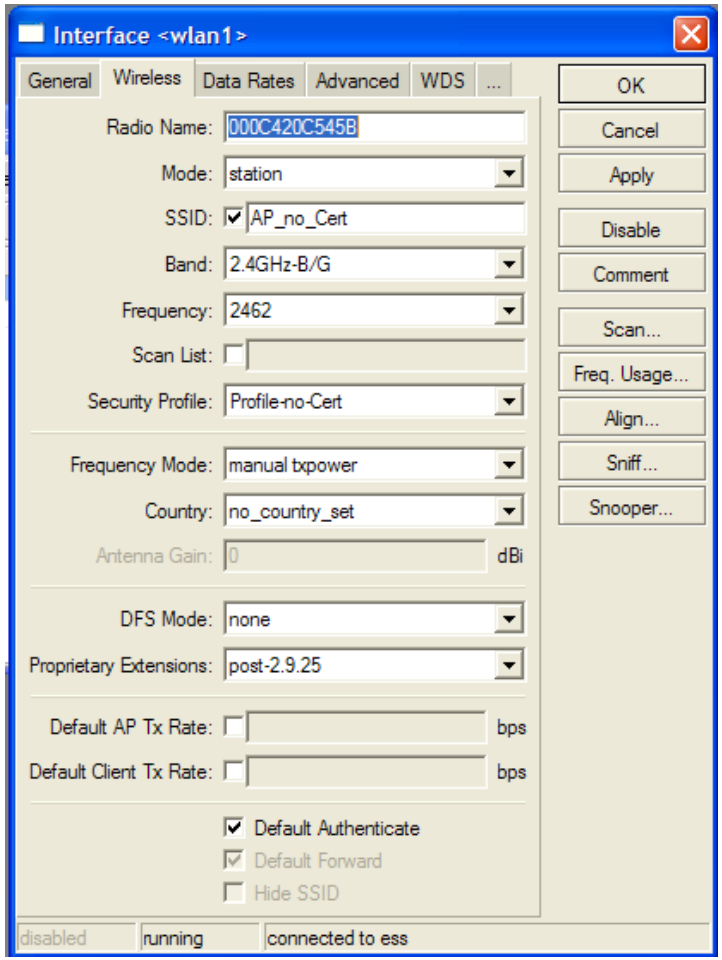


Security Profile

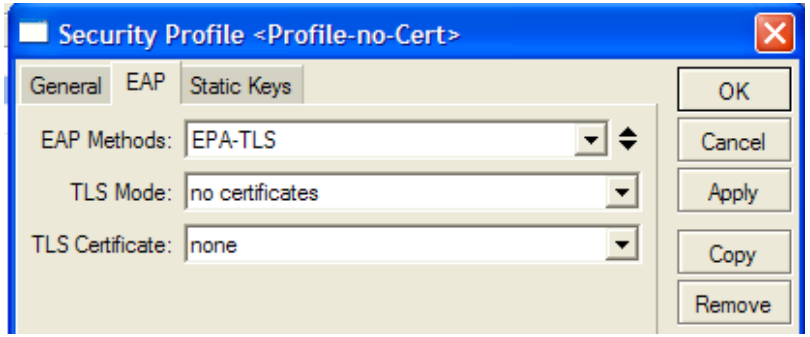


Setup with EAP-TLS – No Certificates

Station Configuration



Security Profile



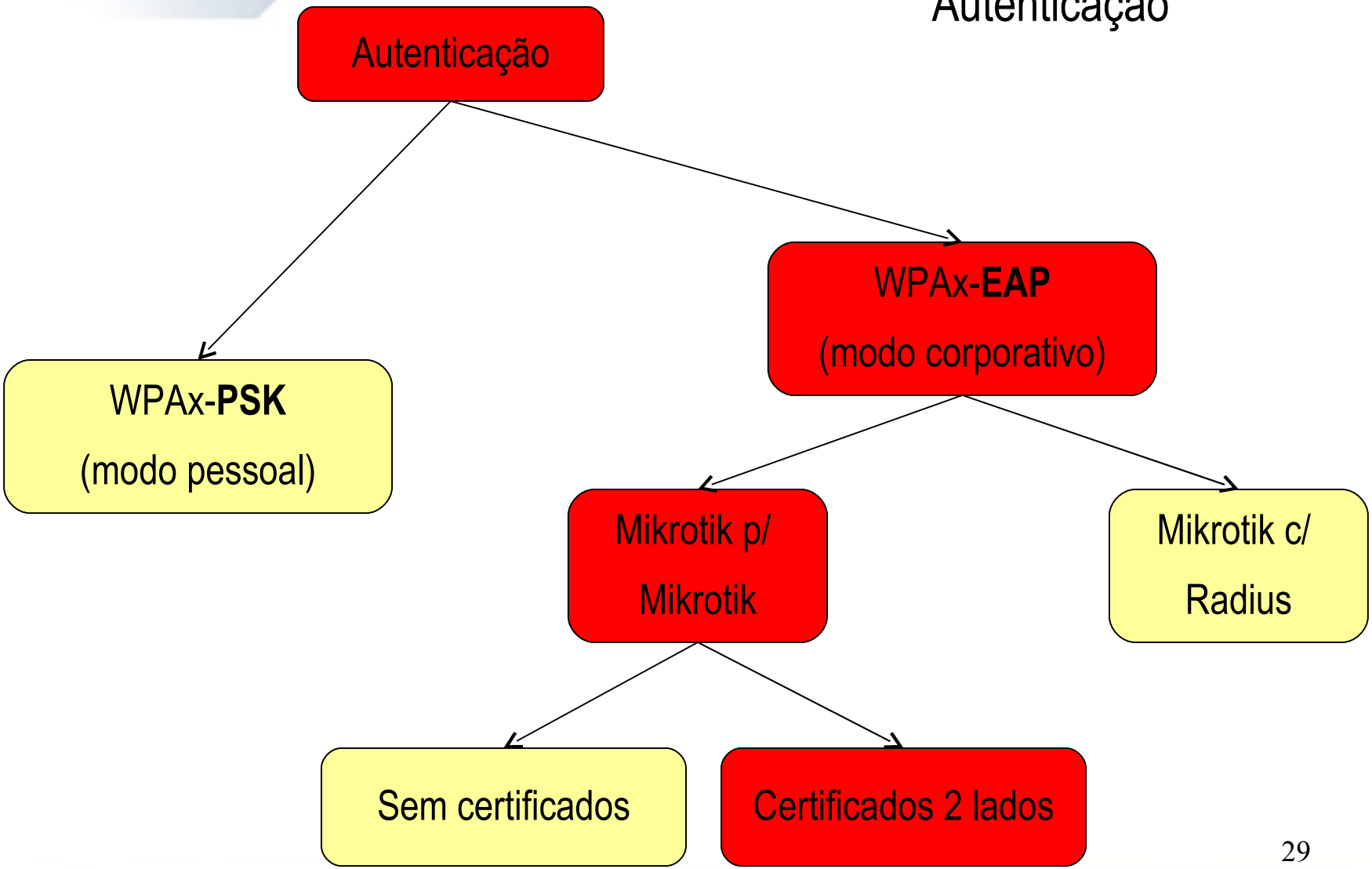
EAP-TLS sem Certificados é seguro ?

- → Como resultado da negociação anonima resulta uma PMK que é de conhecimento exclusivo das duas partes e depois disso toda a comunicação é criptografada por AES (WPA2) o RC4 (WPA)

- → Seria um método muito seguro se não houvesse a possibilidade de um atacante colocar um Mikrotik com a mesma configuração e negociar a chave normalmente como se fosse um equipamento da rede ☹

- → Esse método possui um problema de implementação em multiponto que é o alto consumo de processamento durante o processo de negociação das chaves.

Fundamentos de Segurança WPAx
Autenticação



Trabalhando com Certificados

Un certificado digital é um arquivo que identifica de forma inequívoca o seu proprietário.

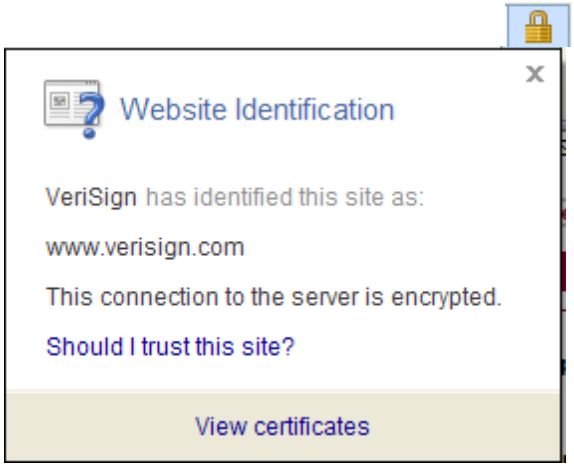
Certificados são criados por instituições emissoras chamadas de CA (Certificate Authorities)

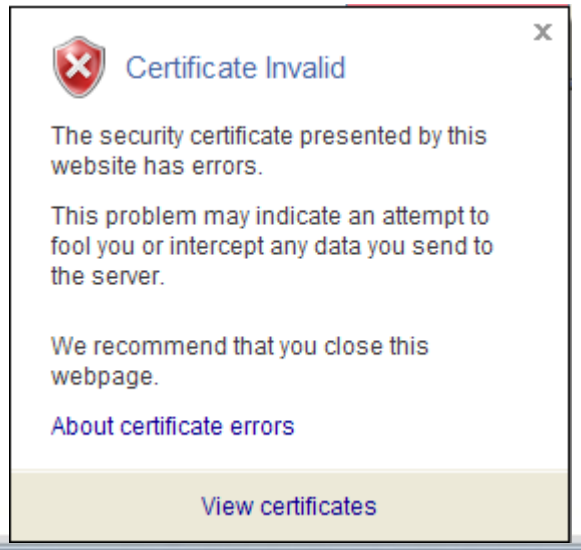
Os Certificados podem ser :

→ Assinados por uma instituição “acreditada” (Verisign, Thawte, etc)

ou

→ Certificados auto-assinados





Passos para implementação de EAP-TLS com Certificados auto assinados

Passo A → Criar a entidade Certificadora (CA)

Passo B → Criar as requisições de Certificados

Passo C → Assinar as requisições na CA

Passo D → Importar os Certificados assinados para os Mikrotiks

Passo E → Se necessário, criar os Certificados para máquinas Windows

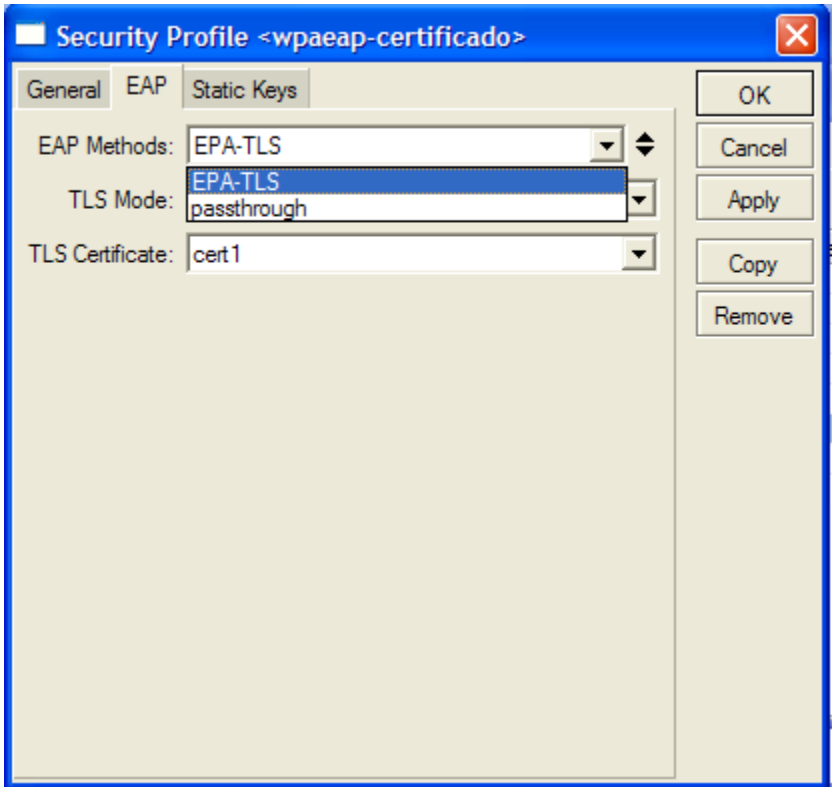
Tutoriais detalhados de como fazer isso:

http://wiki.mikrotik.com/images/2/20/AR_2007_MB_Wireless_security_Argentina_Maia.pdf

http://mum.mikrotik.com/presentations/PL08/mdbrasil.pdf

Método EAP-TLS sem Radius (em AP's e Clientes)

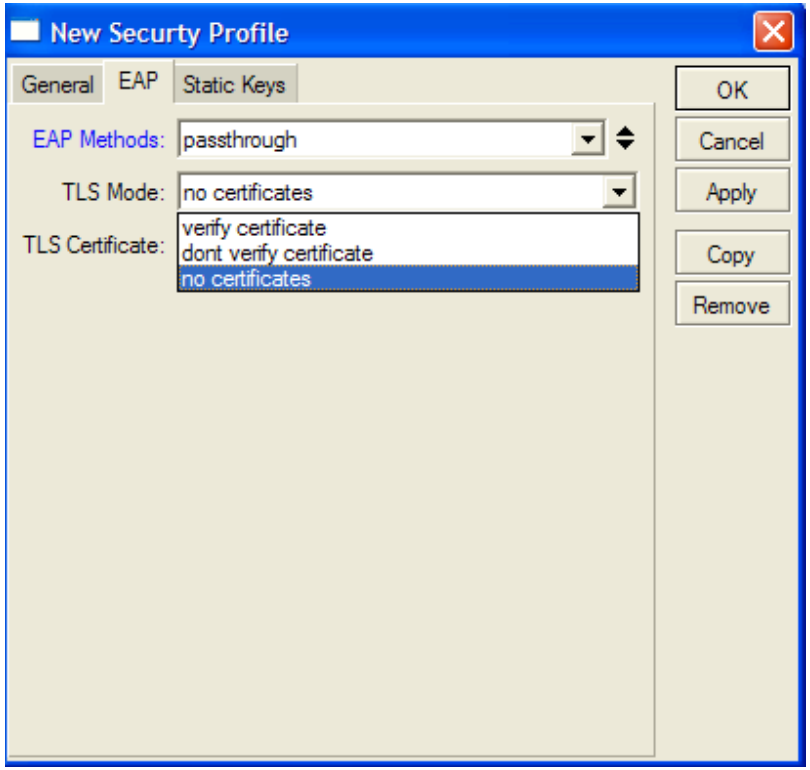
Security Profiles – Métodos de EAP



→EAP-TLS

Usa Certificados

Security Profiles – TLS Mode



→ **verify certificates**

Requer um certificado e verifica se foi firmado por uma ~CA

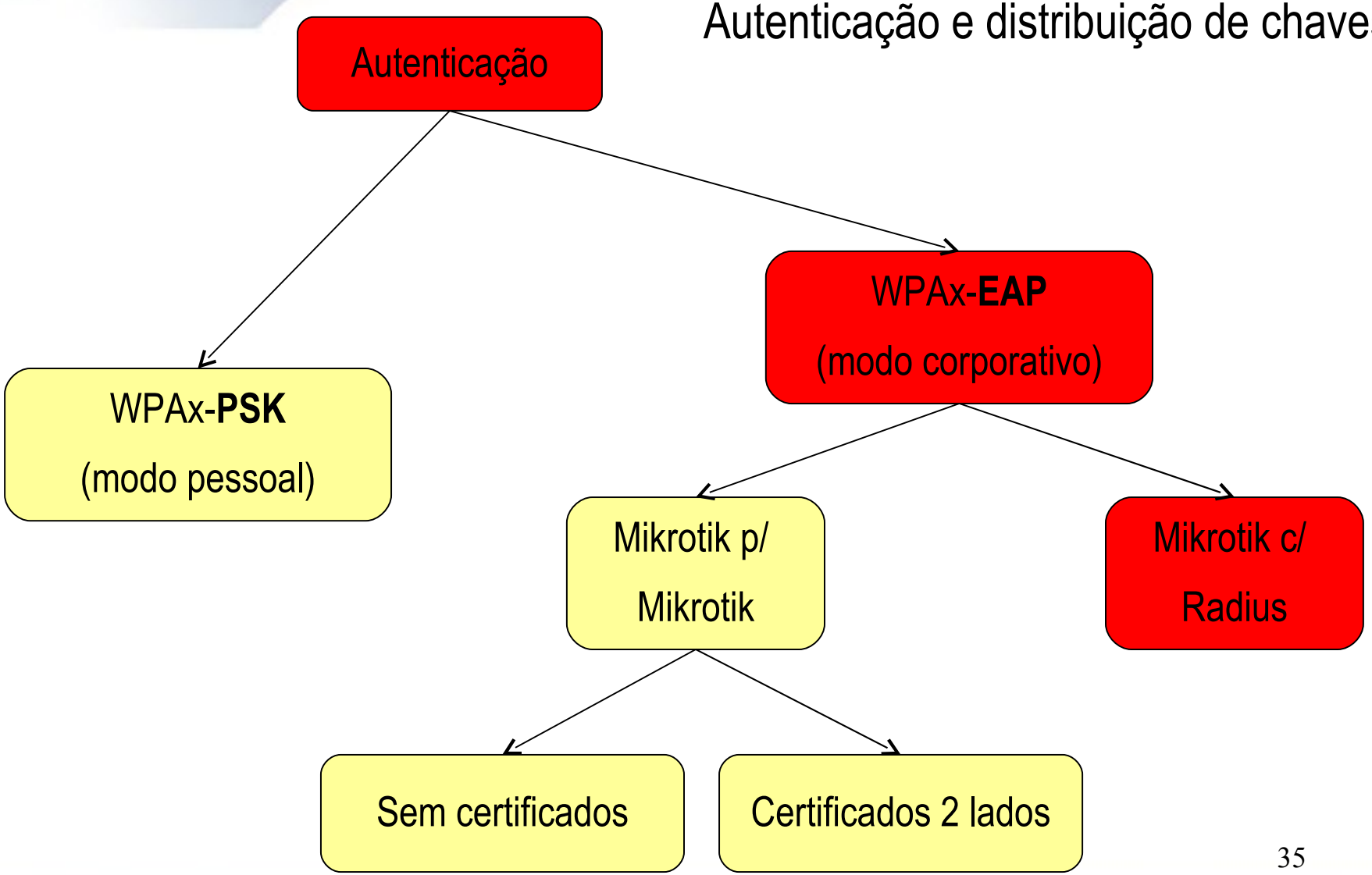
→ **don't verify certificates**

Requer um Certificado, porém não verifica

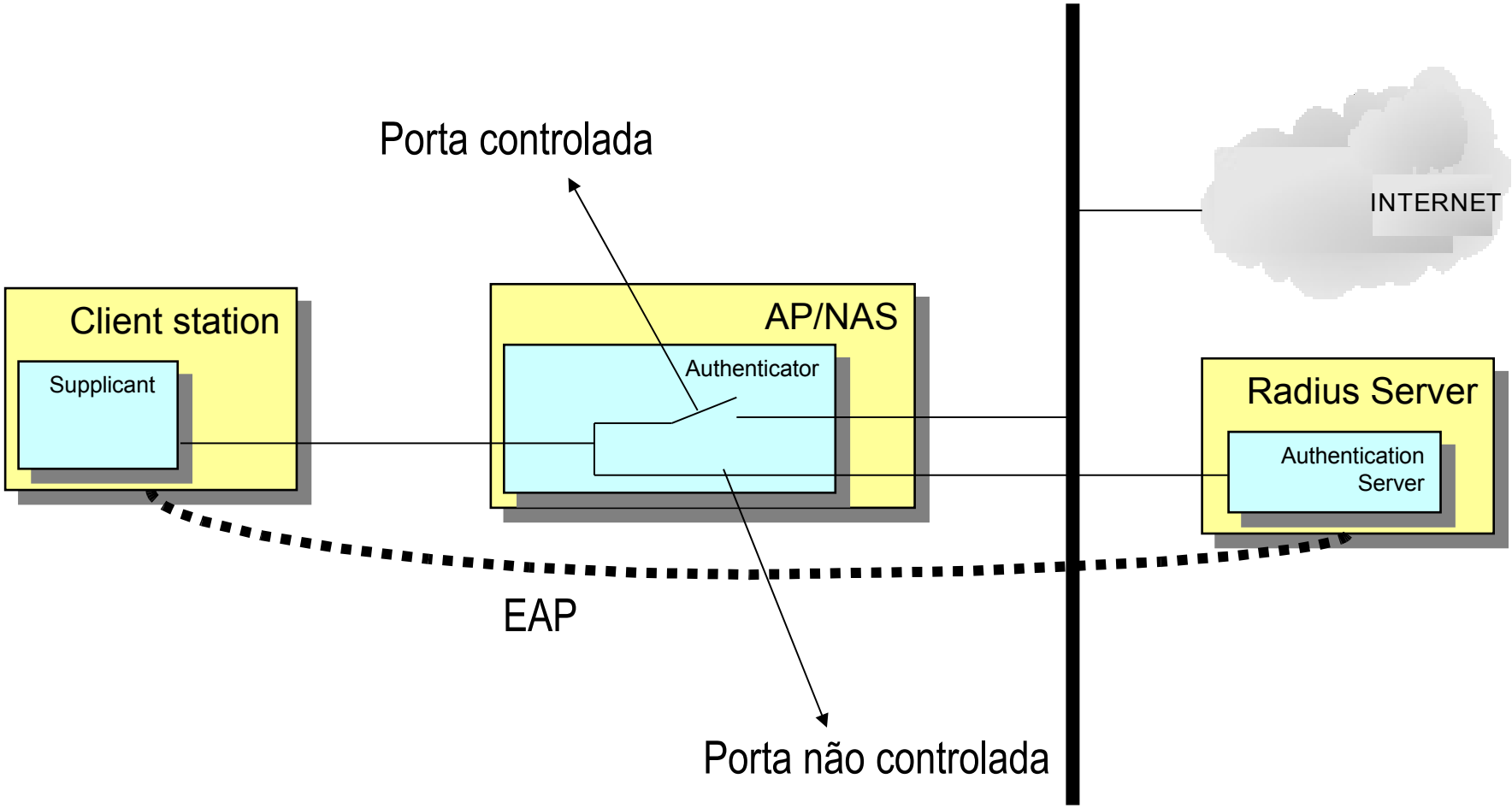
→ **no certificates**

Certificados são negociados dinâmicamente com o el algorítmo de Diffie-Hellman (explicado anteriormente

Autenticação e distribuição de chaves

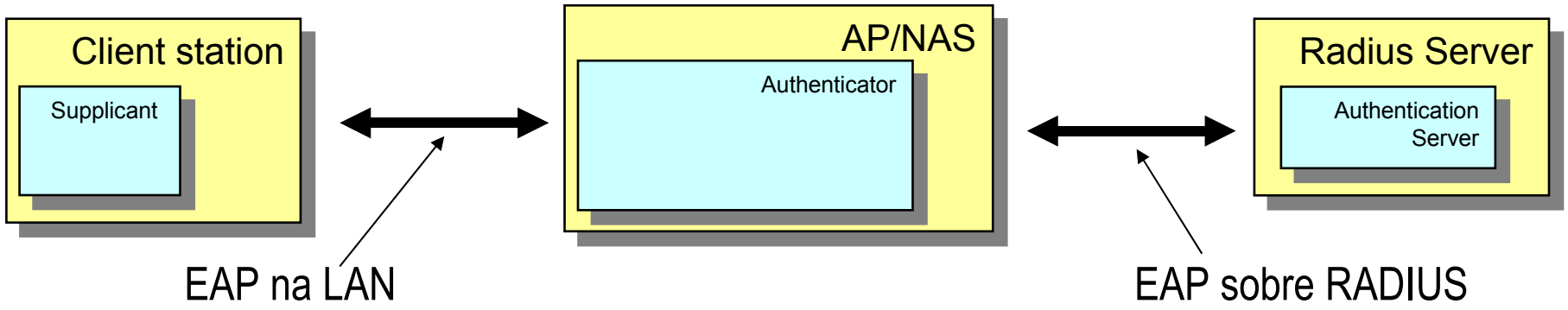


WPAx com Radius



EAP

EAP é um protocolo para identificação de hosts ou usuários originalmente projetado para Protocolo Ponto a Ponto (PPP)



Suporta diferentes tipos de autenticação. Os mais comuns são:

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)

É um protocolo proprietário da Cisco patenteado antes mesmo da 802.11i e WPA/ é baseado em nome de usuário e senha que se envia sem proteção.

Este método não cuida da proteção das credenciais durante a fase de autenticação do usuário com o servidor.

Trabalha com variados tipos de clientes, porém somente com AP's da Cisco.

→ Ferramente para crackear LEAP: Asleap - http://asleap.sourceforge.net/

OBS: Mikrotik não suporta LEAP.

Tipos de EAP

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

PEAP y TTLS são dois mét*odos bastante parecidos –e fazem uso de Certificados* Digitais do lado do Servidor e usuário e senha no lado cliente.

O processo segue a seguinte ordem:

1 – O Servidor manda uma requisição EAP

2 – É Criado um túnel criptografado através do envio do Certificado

3 – O usuário e senha é passado de forma criptografada

O problema com TTLS e PEAP é que é possível o ataque do “homem-do-meio”

OBS: A diferença entre TTLS e PEAP é que PEAP é compatível com outros protocolos como LEAP

Tipos de EAP

EAP-TLS (EAP – Transport Layer Security)

→ O Mikrotik suporta EAP-TLS tanto como cliente como AP e ainda repassa esse método para um Servidor Radius

Provê o maior nível de segurança e necessita de Certificados nos lados do Cliente e do Servidor Radius

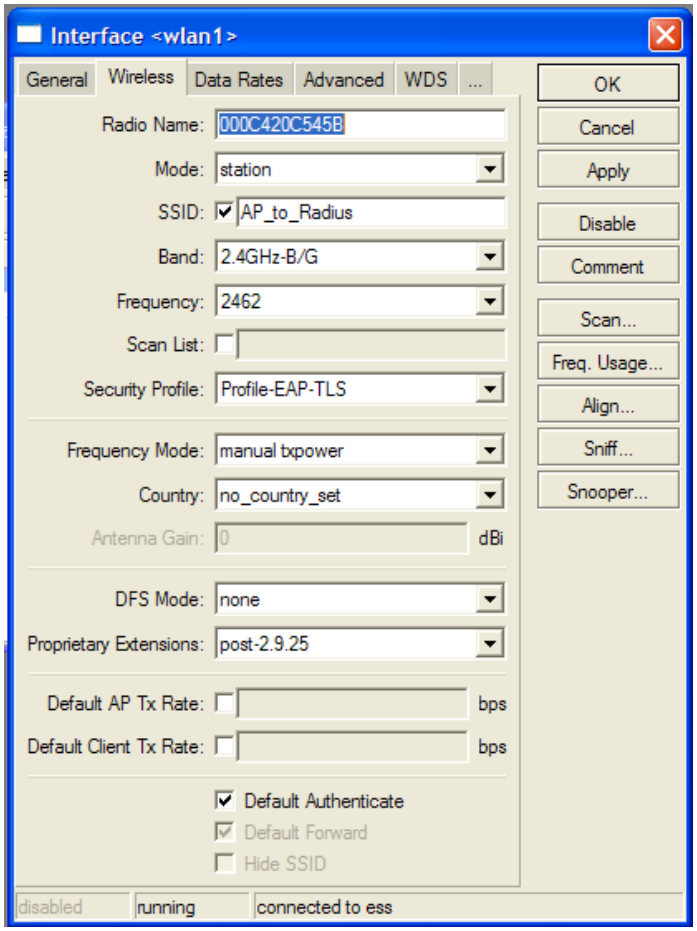
Os passos de como configurar e instalar certificados em um Servidor RADIUS podem ser obtidos em:

http://wiki.mikrotik.com/images/2/20/AR_2007_MB_Wireless_security_Argentina_Maia.pdf

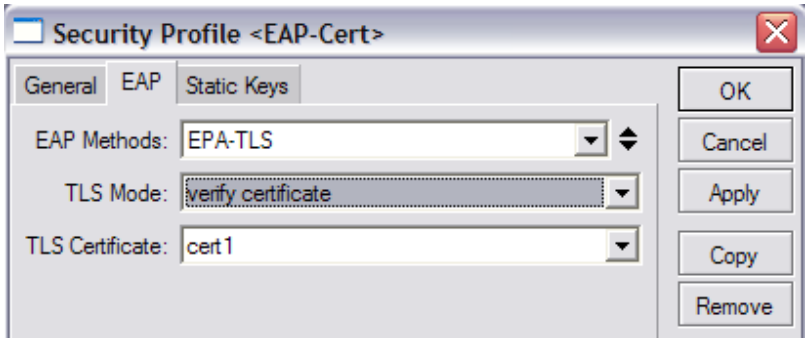
http://mum.mikrotik.com/presentations/PL08/mdbrasil.pdf

Setup with EAP-TLS + Radius Client Configuration

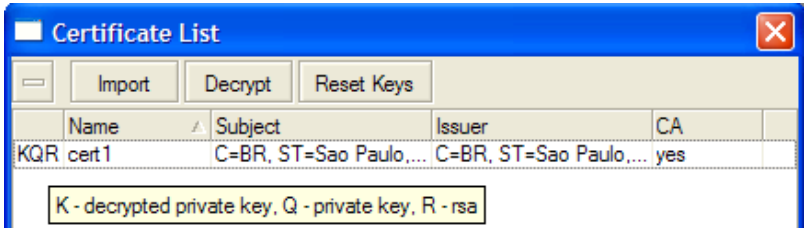
Station Configuration



Security Profile

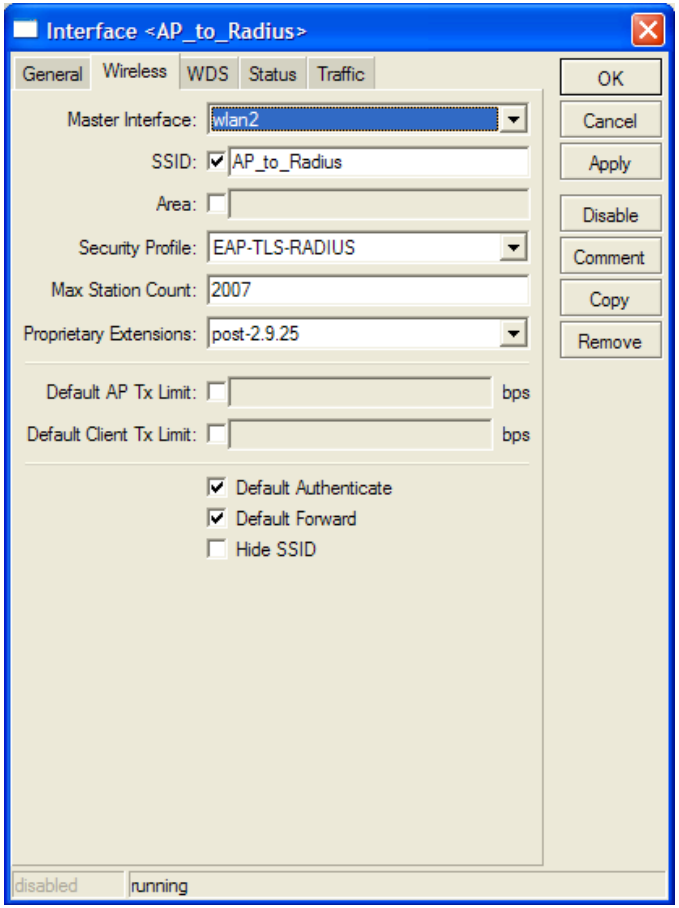


Certificate

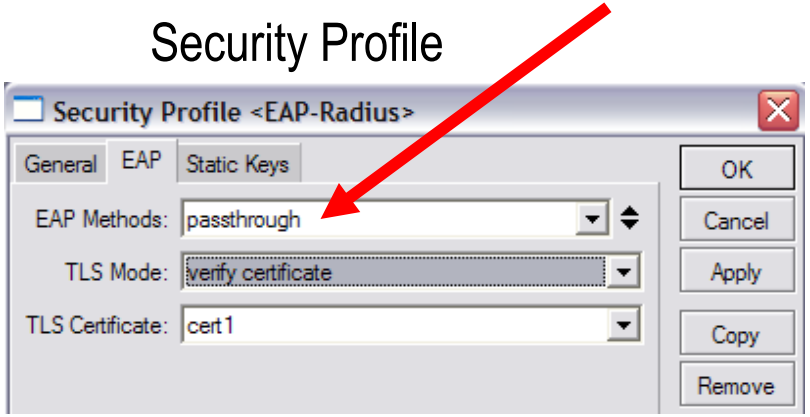


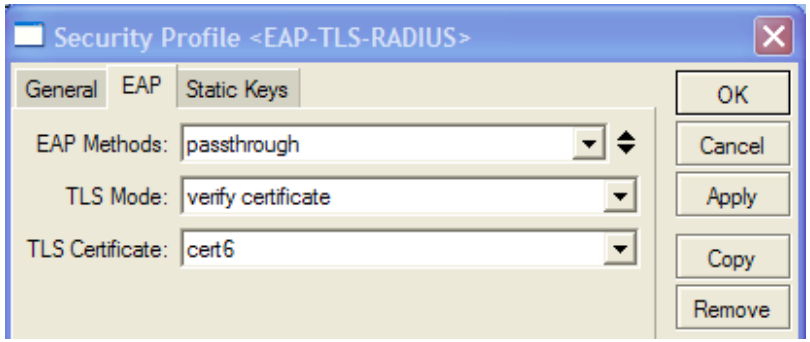
Setup with EAP-TLS + Radius
AP Configuration

AP Configuration



Security Profile

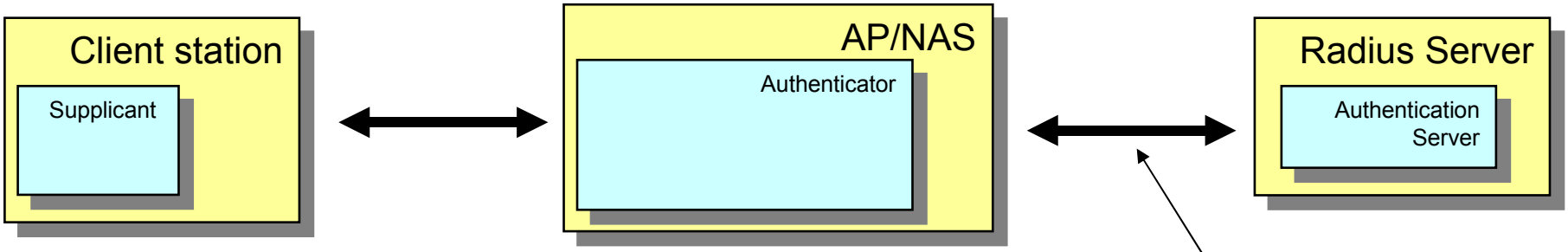




O método EAP-TLS + Radius é seguro ?

No se discute que o EAP-TLS é o método mais seguro que se pode obter, porém há

Um ponto que se pode levantar como uma possível fragilidade:



Existem ataques conhecidos contra o protocolo Radius.

Se um atacante tem acesso físico ao link entre o AP e o Radius

ele pode fazer ataque de força bruta para descobrir a PMK.

→ Para evitar isso há várias formas como proteger esse trecho com um tunel L2TP ou PPtP

Resumo dos métodos possíveis de implantação e seus problemas

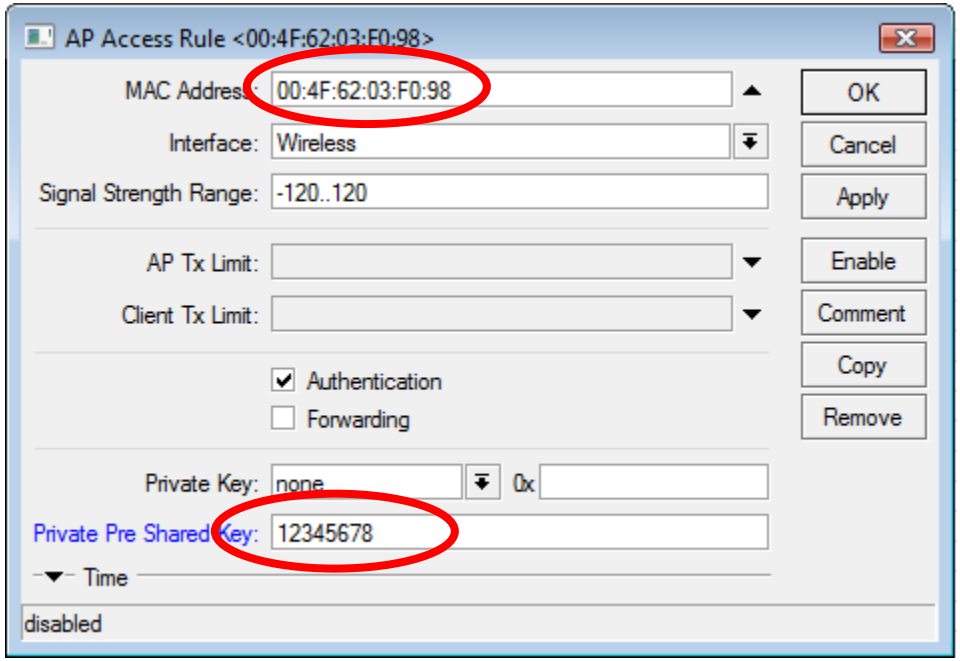
- **WPA-PSK:**
  - Chaves presentes nos clientes e acessíveis aos operadores
- **Método Sem Certificados:**
  - Passível de invasão por equipamento que tambem opere desse modo
  - Problemas com processamento
- **Mikrotik com Mikrotik com EAP-TLS**
  - Método seguro porém inviável economicamente e de implantação praticamente impossível em redes existentes.

Resumo dos métodos possíveis de implantação e seus problemas

- **Mikrotik com Radius:**
  - EAP-TTLS e EAP-PEAP:
    - Sujeito ao “homem do meio” e pouco disponível nos atuais equipamentos.
  - EAP-TLS
    - Método seguro, porém também não disponível na maioria dos equipamentos. Em “plaquinhas” é possível implementa-los.

Método alternativo Mikrotik

→ O Mikrotik na versão V3 oferece a possibilidade de distribuir uma chave WPA2 por cliente . Essa chave é configurada no Access List do AP e é vinculada ao MAC address do cliente, possibilitando que cada cliente tenha sua chave.



→ Cadastrar porém nos access lists, voltamos ao problema da chave ser visível a usuários do Mikrotik !

Método alternativo Mikrotik

→ Felizmente porém o Mikrotik permite que a chave seja atribuída por Radius o que torna muito interessante esse método.

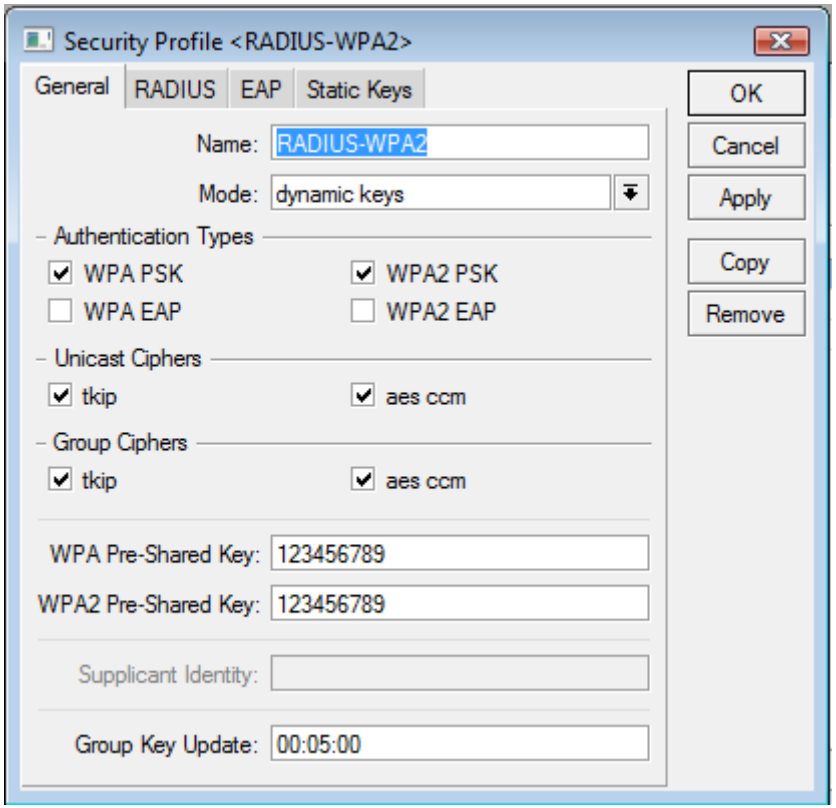
Para configurar precisamos:

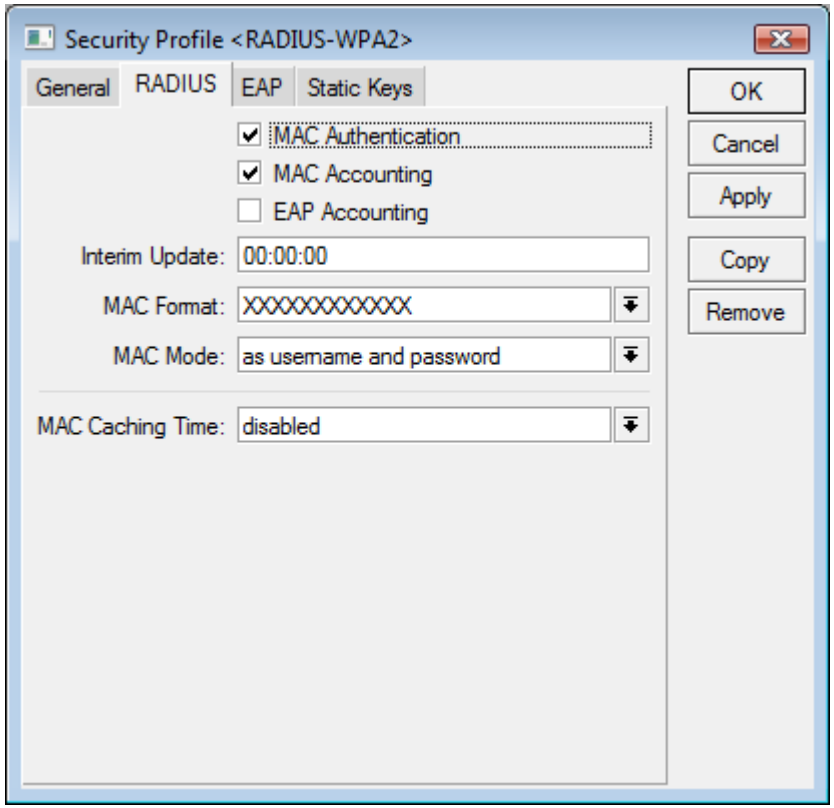
→ Criar um perfil WPA2 qualquer

→ Habilitar a autenticação via MAC no AP

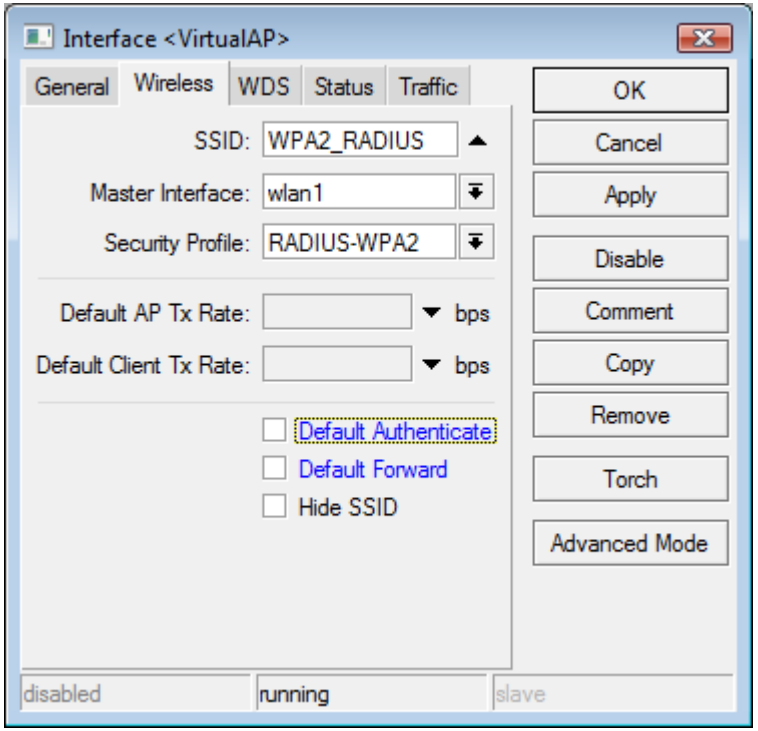
→ Ter a mesma chave configurada tanto no cliente como no Radius.

Configurando o Perfil





Configurando a Interface Wireless



Arquivo users: (/etc/freeradius)

```
# Sintaxe:
# MAC     Cleartext-Password := “MAC“
#             Mikrotik-Wireless-Psk = “Chave_PSK_de_8_a_63_caracteres“


001DE05A1749      Cleartext-Password := "001DE05A1749“
                        Mikrotik-Wireless-Psk = "12345678912“
001B779ADD5D    Cleartext-Password := "001B779ADD5D"
                        Mikrotik-Wireless-Psk = "12345678911“
001B77AF82C9      Cleartext-Password := "001B77AF82C9"
                        Mikrotik-Wireless-Psk = "12345678911"
```

Radius (dictionary)

/usr/share/freeradius/dictionary.mikrotik

```
# MikroTik Attributes

VENDOR          Mikrotik        14988

ATTRIBUTE       Mikrotik-Recv-Limit             1       integer         Mikrotik
ATTRIBUTE       Mikrotik-Xmit-Limit             2       integer         Mikrotik
ATTRIBUTE       Mikrotik-Group                  3       string          Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Forward       4       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Skip-Dot1x    5       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Enc-Algo      6       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Enc-Key       7       string          Mikrotik
ATTRIBUTE       Mikrotik-Rate-Limit             8       string          Mikrotik
ATTRIBUTE       Mikrotik-Realm                  9       string          Mikrotik
ATTRIBUTE       Mikrotik-Host-IP                10      ipaddr          Mikrotik
ATTRIBUTE       Mikrotik-Mark-Id                11      string          Mikrotik
ATTRIBUTE       Mikrotik-Advertise-URL          12      string          Mikrotik
ATTRIBUTE       Mikrotik-Advertise-Interval     13      integer         Mikrotik
ATTRIBUTE       Mikrotik-Recv-Limit-Gigawords   14      integer         Mikrotik
ATTRIBUTE       Mikrotik-Xmit-Limit-Gigawords   15      integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Psk           16      string          Mikrotik

# MikroTik Values

VALUE           Mikrotik-Wireless-Enc-Algo      No-encryption           0
VALUE           Mikrotik-Wireless-Enc-Algo      40-bit-WEP              1
VALUE           Mikrotik-Wireless-Enc-Algo      104-bit-WEP             2
```

Laboratório de PSK por cliente

O aluno que quiser participar, crie um arquivo texto no formato abaixo e coloque no FTP com a identificação XY-PSK, onde XY é seu número.

Sintaxe:
MAC Cleartext-Password := “MAC“
Mikrotik-Wireless-Psk = “Chave_PSK_de_8_a_63_caracteres“

#Exemplo:
001DE05A1749 Cleartext-Password := "001DE05A1749“
Mikrotik-Wireless-Psk = "12345678912“

Criptografia

x

WISP's

Pesquisa realizada em setembro de 2007

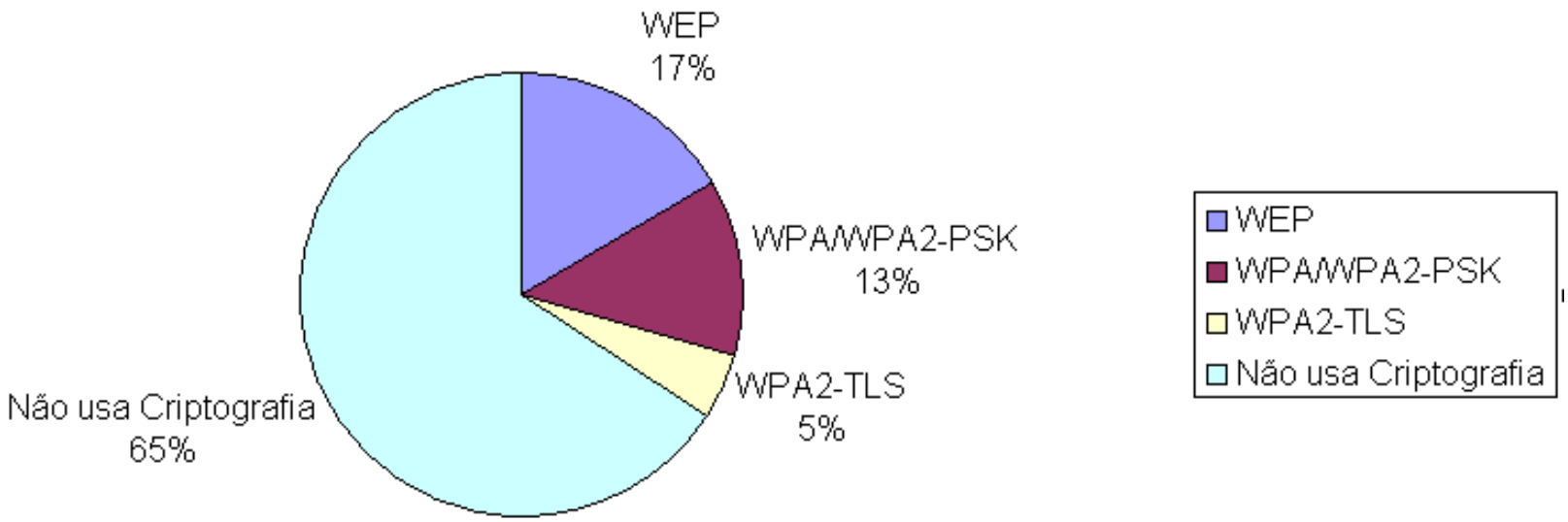
Provedores que responderam à Pesquisa: 74

Número de Clientes atendidos: 52.385

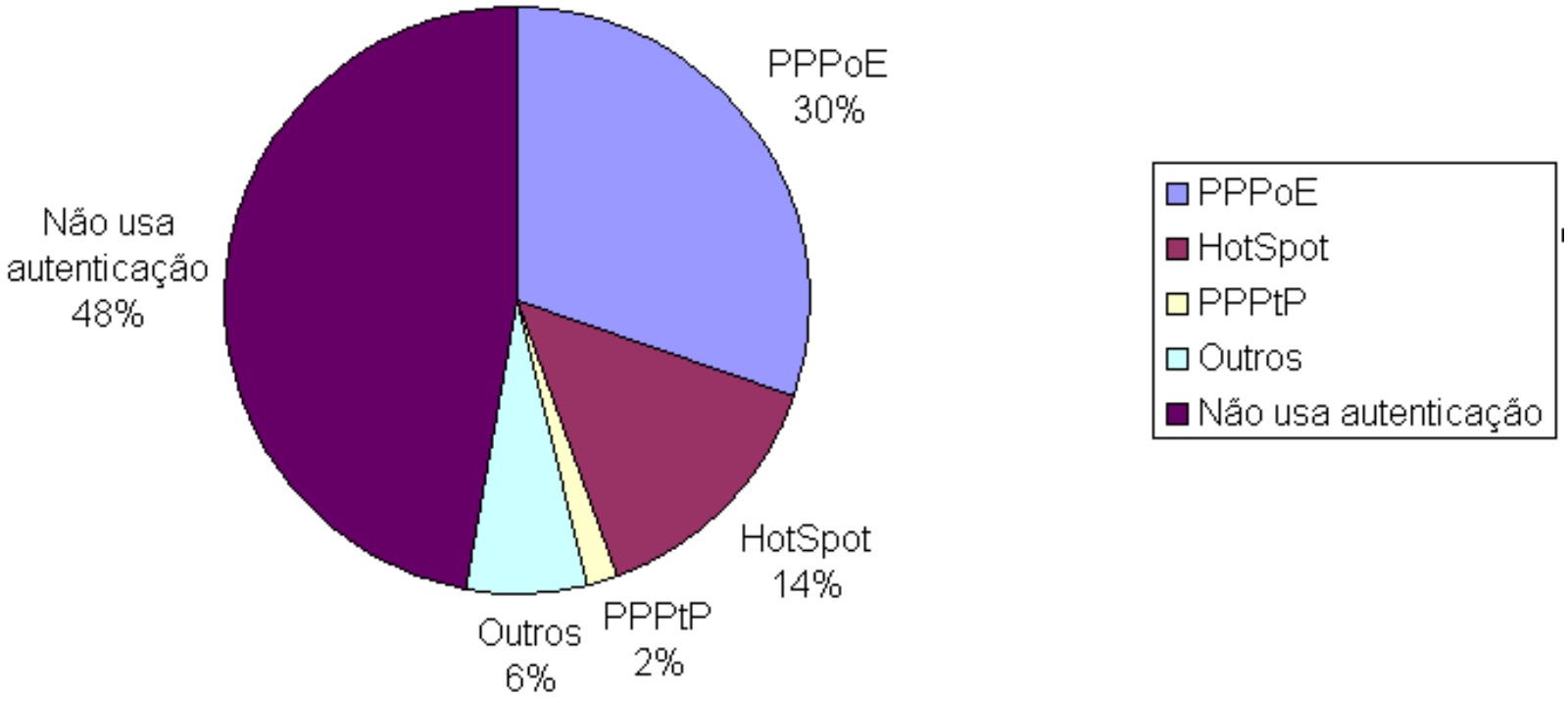
Total de Link contratado: 585.6 mbps

Os resultados foram compilados de maneira ponderada resultados foram compilados de manera ponderada utilizando o critério do número de clientes atendidos.

Pesquisa realizada en setembro de 2007
Criptografia

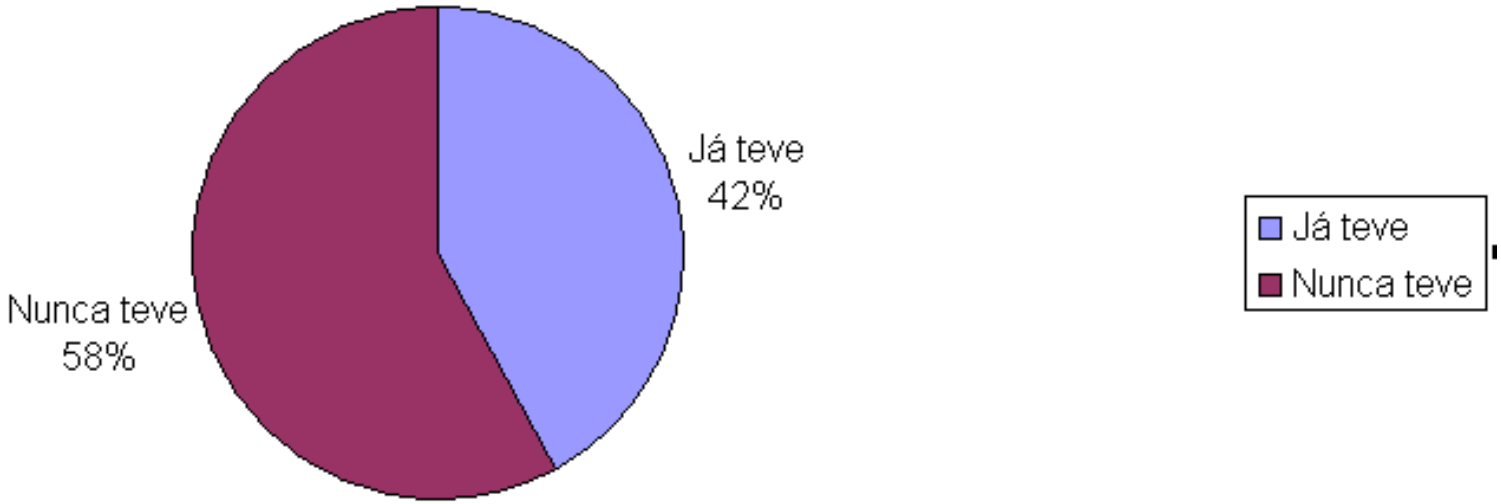


Pesquisa realizada en setembro de 2007
Autenticação



OBS: De todos que usam autenticação PPPoE ou Hotspot somente 4% usam também criptografia (96% usam somente PPPoE ou Hotspot como medida de segurança)

Spoof de MAC e ou IP



Soluções (não 80211i) para a última milha

A conclusão da pesquisa é que a grande maioria tenta dar segurança a suas redes com as soluções:

→Túneis PPPoE

→Autenticação Hotspot

Vamos fazer a seguie uma análise crítica desses modelos em particular com relação à segurança

Considerações acerca de PPPoE e Hotspot
quando utilizados por provedores para “segurança”

Tuneis PPPoE
aspectos gerais

→ PPPoE : originalmente desenvolvido para redes cabeadas

→ O PPPoE Server (PPPoEd) escuta as requisições de clientes PPPoE que por sua vêz utilizam o protocolo PPPoE discovery – tudo é feito na camada 2

→ PPPoE por padrão não é criptografado – pode ser configurado com criptografia MPPE se o cliente suporta esse método.

→ O método CHAP protege apenas o nome de usuário e senha e nada além disso.

Túneis PPPoE
aspectos gerais

- A interface que “escuta” as requisições PPPoE não deve ter configurado Ip que seja “roteado” ou para o qual esteja sendo feito NAT. Se isso ocorre é possível burlar a autenticação PPPoE.
- Como outros túneis os valores de MTU e MRU devem ser modificados.
- PPPoE é sensivel a variações de sinal.
- Em máquinas Windows é necessário a instalação de um discador, o que representa trabalho administrativo.

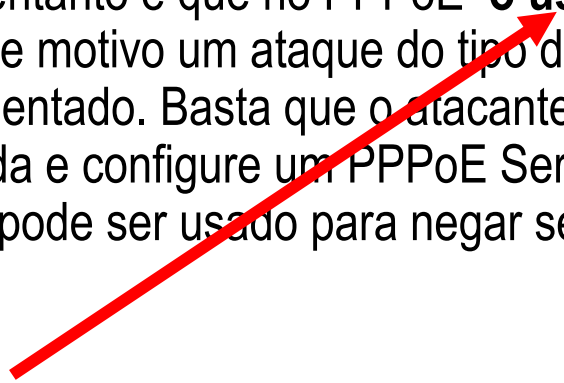
PPPoE e Segurança

→ Un atacante que falsifique um endereço MAC em uma planta onde se rode PPPoE não consegue navegar, porem causa muitos problemas aos usuários verdadeiros.

.

→ Existem ataques a PPPoE quando falsos clientes disparam sucessivas requisições de conexão (PPPoE discovery) causando negação de serviço.

→ O mais grave no entanto é que no PPPoE **o usuário não autentica o Servidor**. Por esse motivo um ataque do tipo do "homem-do-meio" pode ser facilmente implementado. Basta que o atacante ponha um AP falso em uma posição privilegiada e configure um PPPoE Server para capturar as requisições dos clientes. Isso pode ser usado para negar serviço ou para capturar senhas.



Hotspots
aspectos gerais

- Originalmente foram desenvolvidos para dar serviço de conexão à Internet em Hotéis, Shoppings, etc. Com o tempo tem sido utilizados como plataforma para autenticar usuários de WISP's.

- A interface configurada para "ouvir" o hotspot captura a tentativa de navegação e pede usuário e senha.

- Existem vários métodos de autenticação, inclusive com Certificados digitais é possível fazea a autenticação por HTTPS.

Hotspots e Segurança

- Uma vez que um usuário tenha sido autenticado e seu par IP + MAC seja descoberto e falsificado por um atacante, este ganha acesso sem usuário e senha. O ponto de acesso não “vê” os dois, porém somente um usuário. O serviço fica precário mas há a navegação de ambos.

- Usar DHCP reduz o trabalho dos hackers a menos da metade, pois descoberto o MAC, o DHCP “dá o IP de presente”

- O método de criptografia MD5 presente na autenticação chap somente protege o momento da autenticação, de nada adiantando para o tráfego da sessão que pode ser sniffado

- Trabalhando com Certificados Digitais e HTTPS, dár-se-ia ao usuário a possibilidade deste “autenticar” o ponto de acesso, evitando assim o ataque do “homem-do-meio”. No entanto dificilmente o usuário estará devidamente orientado para tanto e a maioria deles aceitará um Certificado falso.

PPPoE & Hotspot & segurança - conclusões

→ PPPoE tem muitas vantagens porque elimina uma série de problemas comuns de redes wireless como broadcasts, trafegos causados por vírus, etc.

→ Hotspots apresentam muitas facilidades interessantes como mandar mensagens, criar rotas, etc.

→ Ambos são excelentes ferramentas para auxiliar na administração e controle de rede, pricipalmete quando implementados em conjunto com Radius.

→ **PPPoE e Hotspot ajudam muito, porém não podem ser encarados como plataformas de segurança como tem sido até então !**

→ **Segurança em Wireless se faz somente com criptografia bem implementada e em redes cabeadas com dispositivos com isolação de portas.**

Porque os WISP's não utilizam Criptografia em Wireless ?

WISP's dizem que não utilizam Criptografia pelos seguintes motivos:

- → Muita Complexidade
  - → **Não é fato. Com Mikrotik as implementações são muito fáceis**
- → Equipamentos antigos não aceitam criptografia.
  - → **É verdade, mas no Mikrotik é possível ter diversos perfis, com vários tipos de criptografia.**
- → Antigos problemas da WEP fazem WPA não confiável
  - → **As técnicas empregadas são muito diferentes e não há comparação.**
- → Problemas de performance com a criptografia
  - → **Novos Chipsets Atheros fazem criptografia em hardware – não há problemas de performance**

Segurança – conclusões (quase) finais

Segurança em meio wireless que cumpra os requisitos de:

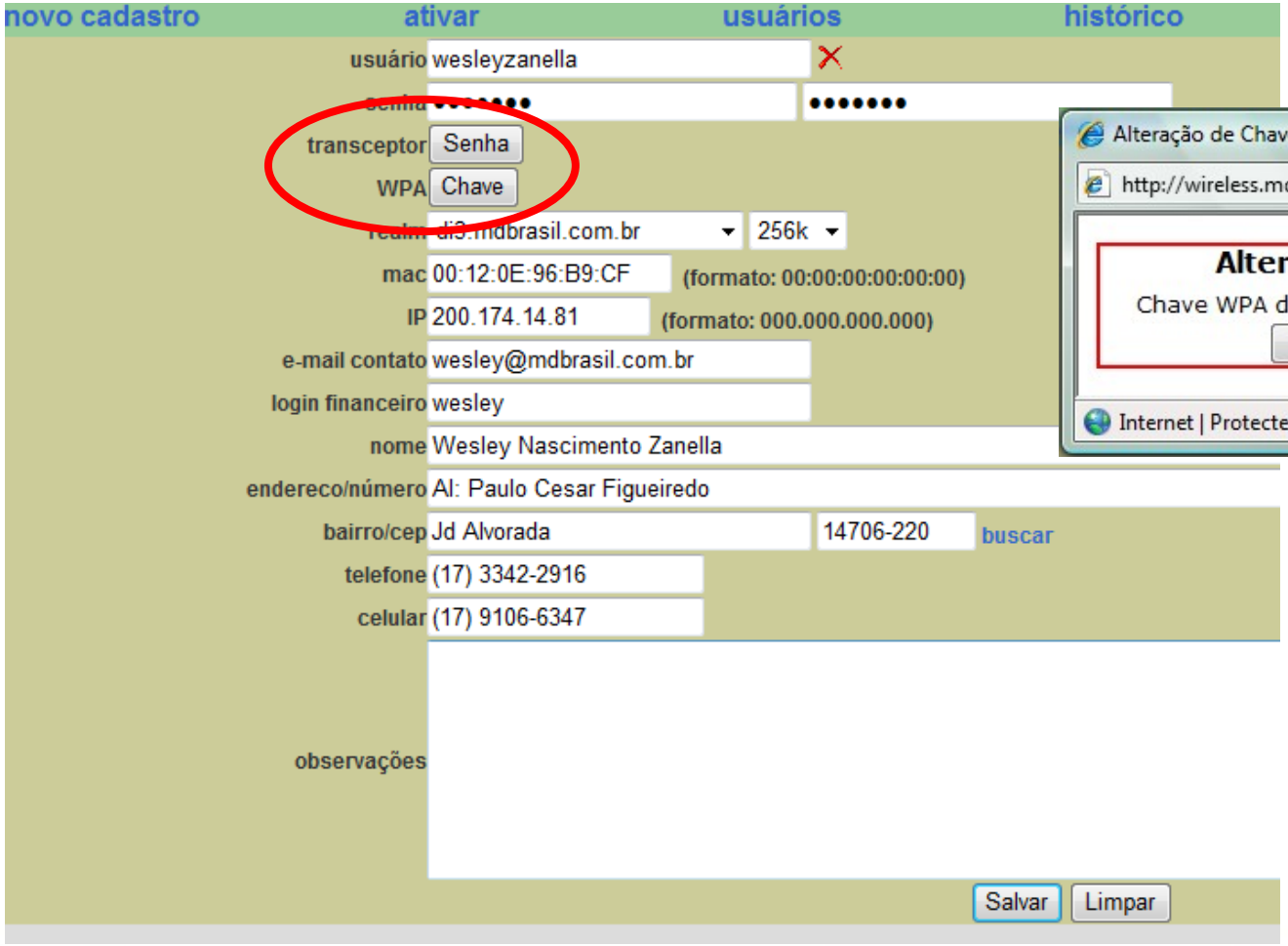
- Autenticação mútua
- Confidencialidade
- Integridade de dados

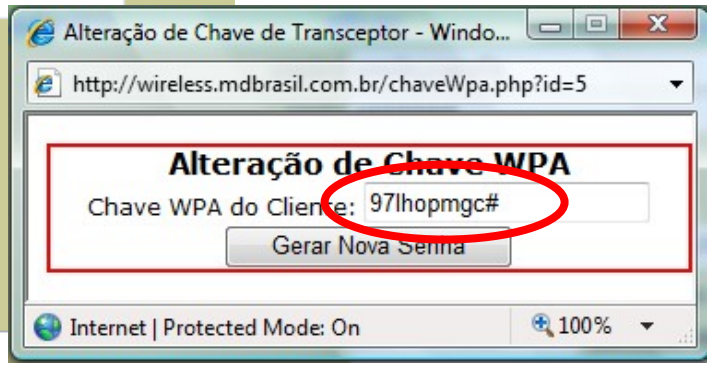
→**Somente se consegue com a utilização de uma estrutura baseada em 802.11i (WPA2) com EAP-TLS implementada con Certificados Digitais + Radius.**

→ **Um excelente "approach" é a utilização de chaves Privadas WPA2-PSK quando distribuidas pelo Radius.**

Outras implementações como a formação de VPN's entre os clientes e um concentrador antes que seja dado o acesso à rede é tambem uma solução possível que não foi abordada aqui pois em escala sua implementação pode se mostrar inviável.

Implementação de WPA2 por cliente com Radius na MD Brasil



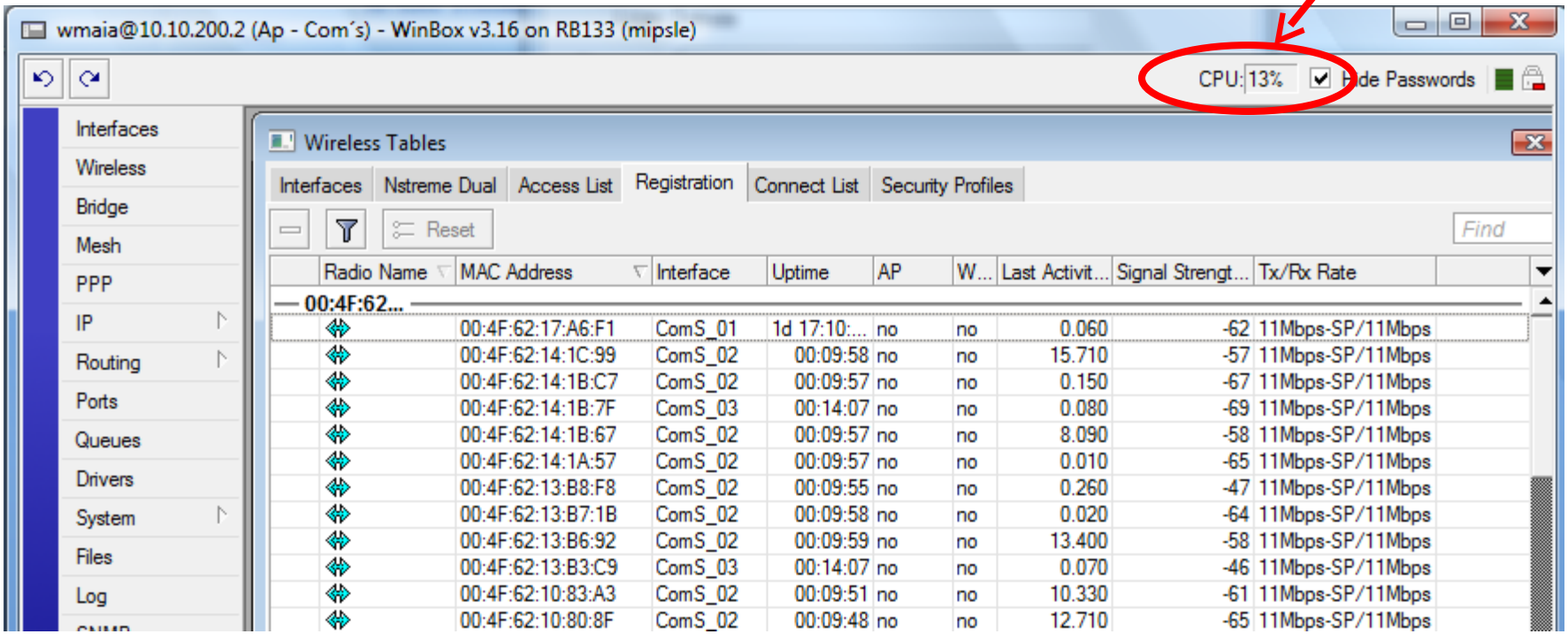


Case MD Brasil

Pontos de acesso:

→Mikrotik RB133 somente como AP Bridge c/ 3 cartões R52, média 25 clientes p/ cartão

→ 100% clientes com WPA2 atribuída por Radius

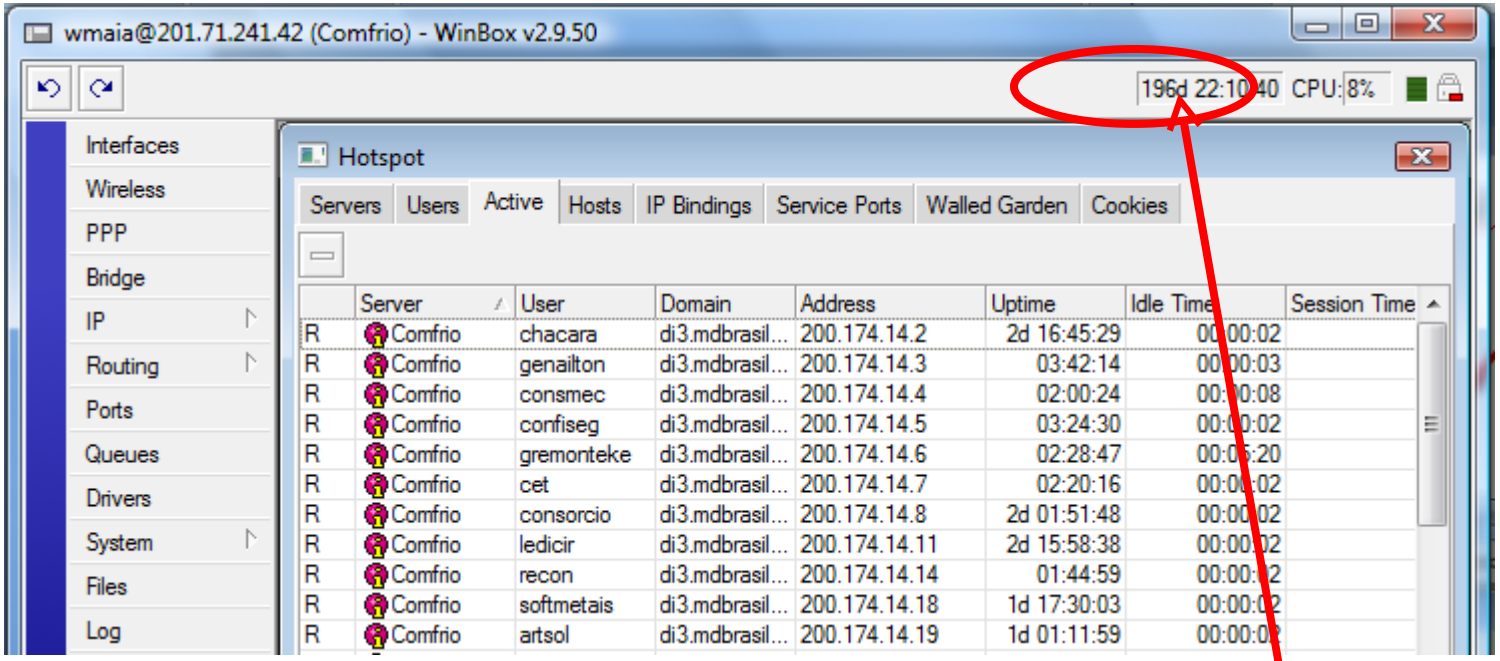


Case MD Brasil

→ Clientes primeiro autenticam-se por MAC + PSK individual (transaparente p/ cliente

→ Em seguida é pedida autenticação Hotspot para cada cliente.

→ A opção por Hotspot nada tem a ver com a segurança. É somente uma opção de negócio



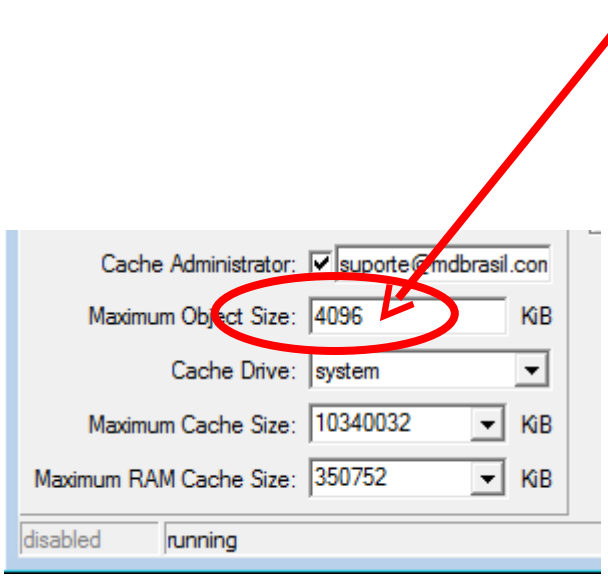
OBS → destaque para o uptime !

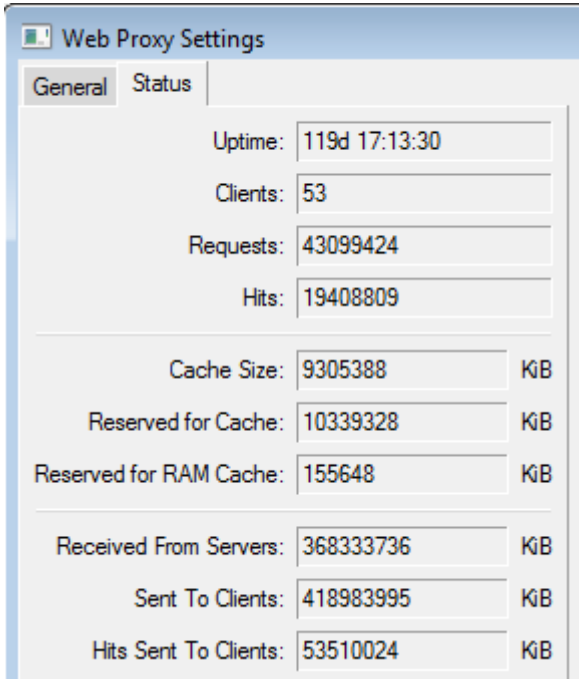
Case MD Brasil

→Hotspot + Web Proxy rodam localmente em todos pontos de acesso com mais concentração de clientes.

→ Web-Proxy's dos pontos de acesso armazenam objetos pequenos

→ Web-Proxy central (não Mikrotik) armazena objetos grandes.





Obrigado !

Wardner Maia – maia@mikrotikbrasil.com.br