[MikrotikBrasil]
Routers & Wireless Systems

OLPC & Mikrotik
Providing Digital Inclusion and Broadband connectivity to a whole country

one laptop per child

ROUTING THE WORLD
MikroTik
www.mikrotik.com

Czech Republic MUM - Prague
February, 2009

Eng. Wardner Maia - Brazil

Introduction

Name: Wardner Maia
Country: Brazil

→ Electronic/Telecommunications Engineer

→ In IT & Telecom, market since 1995 – Company MD Brasil

→ Engaged in trainings since 2002

→ Mikrotik Certified Trainer since June, 2007

→ Recent work in cooperation with ServInfo – Uruguay

MD Brasil

MD Brasil – IT & Telecom

→ Internet Service Provider in Sao Paulo State

→ Authorized by Brazilian regulatory agency as Telecom operator to provide Multimedia content all over the country

→ Mikrotik Distributors and Training Partners

→ Consulting Services

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

Servinfo

Servinfo – Uruguay

→ Located in Montevideo and Artigas Uruguay

→ Internet Service Provider, Mikrotik users since 2002

→ Mikrotik Distributors

→ Working on OLPC Network development in Uruguay.

www.servinfo.com.uy

AGENDA

OLPC Project

→ What is OLPC and the XO
→ Mission and Principles
→ OLPC around the World and in Uruguay

The support network in Uruguay

→ The environment
→ How Mikrotik is helping to construct the network

Securing the Laptops and the Network

→ The risks – unauthorized access, eavesdroping, MitM,
→ Main challenges to provide security
→ Proposed solutions

What is OLPC ?

OLPC - One Laptop Per Child Association, was created by an initiative of MIT Massachusetts Institute of technology and is a U.S. non-profit organization set up to oversee the creation of an affordable educational device for use in the developing world.

Mission Statement:

“To create educational opportunities for the world's poorest children by providing each child with a rugged, low-cost, low-power, connected laptop with content and software designed for collaborative, joyful, self-empowered learning”.

The XO

“A small machine with a big mission”

Designed collaboratively the XO is a potent learning tool built especially for children. Some characteristics:

→ projected to support extreme environmental conditions, such as high heat and humidity.

→ Built in wireless with 2 potent antennas

→ Screen that is readable under direct sunlight for children who go to school outdoors.

→ Uses Linux with “Sugar” graphical interface, specially designed for education

Basic Principles

1. The Kids keep the Laptop
2. Focus on early education (6 – 12 years old)
3. No one gets left out
4. Connection to the Internet
5. Free to grow and adapt

OLPC around the world

There are several countries testing and launching OLPC “pilot projects”.

Uruguay was the first country of the world that had adopted for 100% of the children within 6 to 12 years old. It's not a plan, it's reality!

OLPC in Uruguay - “Ceibal Project”

→ 350.000 users total (basic education)

→ 174.000 are already with their XO

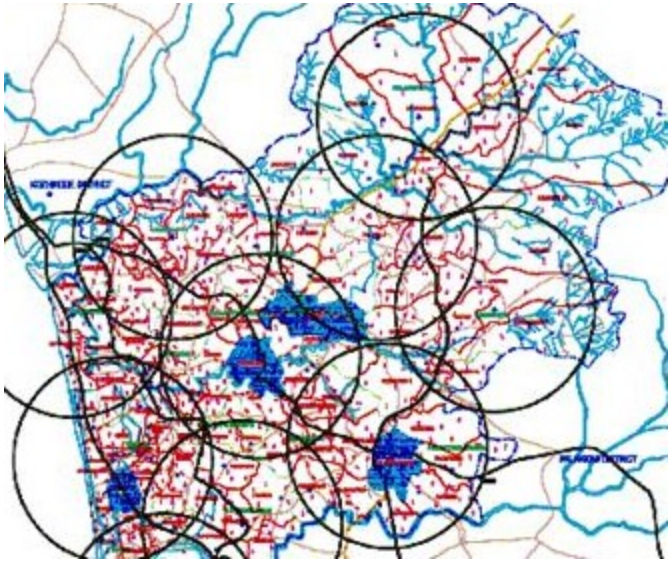
→ until July / 2009 100% of the laptops will be distributed.

→ 50.000 new students go to basic school each year.

→ There are about 3.000 schools all over the country. Most of them with few number of students.

→ Since students go to the second grade and take their Laptops, in 2009 Infra structure should be provided to second grade schools too.

OLPC in Uruguay



→ Internet connectivity is a big challenge for a lot of locations – a lot of kinds of connections are being used like ADSL, Edge. 3G, Satellite, etc.

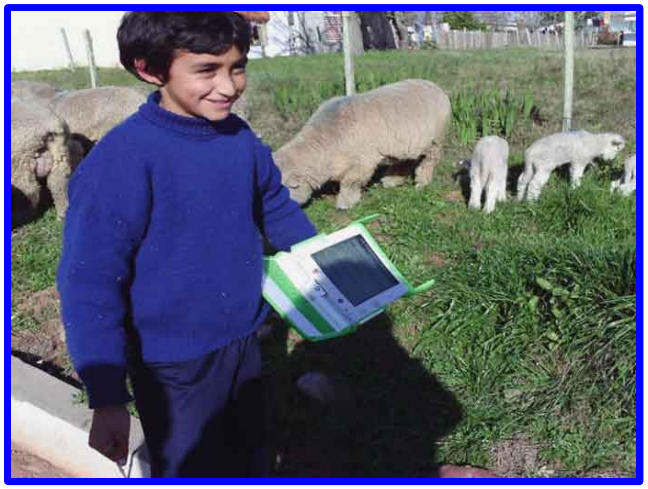
OLPC in Uruguay

How Mikrotik is helping Ceibal project

School with solar energy

Some schools only have satellite access

OLPC in Uruguay



How Mikrotik is helping Ceibal project

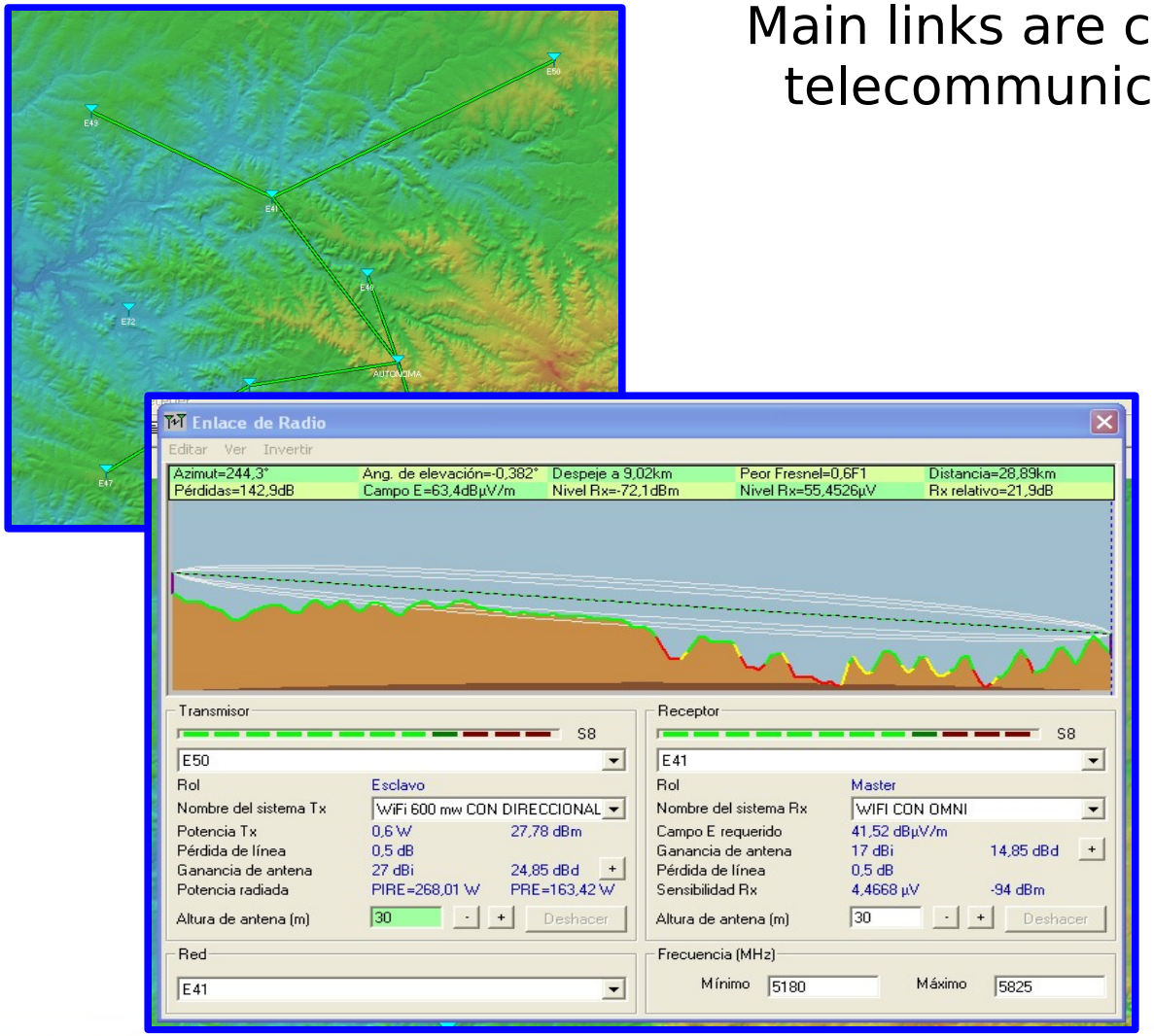
Point to Point links:

There are more than 100 Point-to-Point links connecting schools. All PtP links are using Mikrotik. Depending on the distance and other conditions, the equipments used are:

→ typically for outdoor access R52H / R5H cards are employed.

OLPC in Uruguay

Main links are connected to government telecommunication company - ANTEL



OLPC in Uruguay

Use of government buildings

Some schools are used as repeaters

OLPC in Uruguay

How Mikrotik is helping Ceibal project

Access Points:

→ 95% of the Access Points installed at the schools are Mikrotik powered

→ About 5.000 RB433 are installed

→ RB230 used in locations where only 3G is available. We are looking forward for RB433 with USB support !

→ R52 cards for indoor access, R52H for outdoor access.

OLPC in Uruguay

School Access Points - RB433

Securing the Network

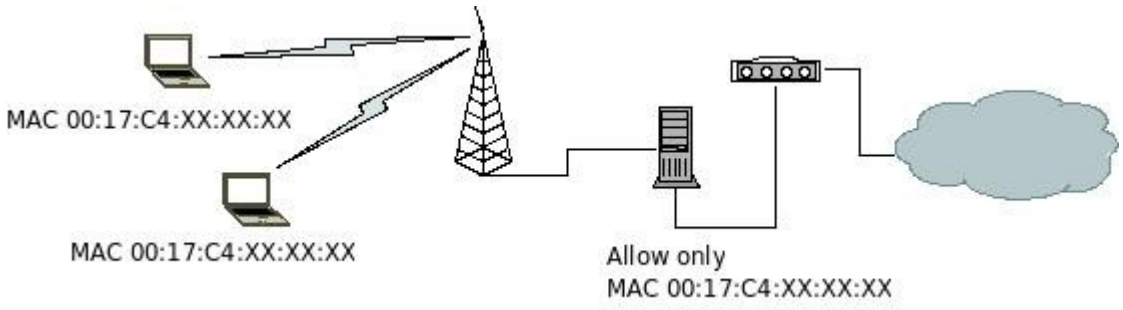
Securing the network

The project was launched with only one “security” method:

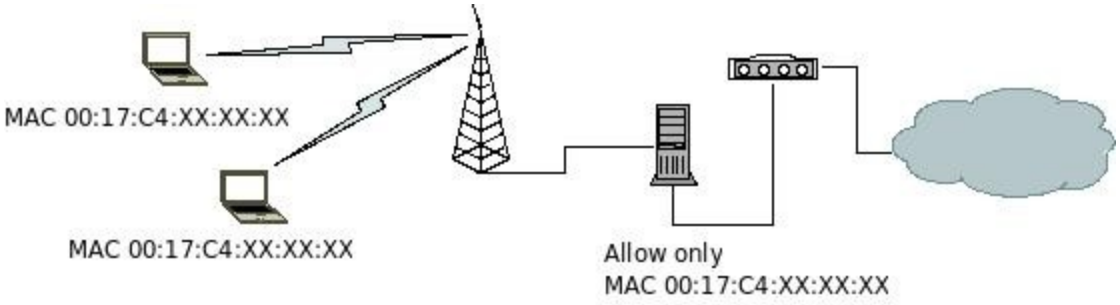
MAC access control lists

→ Running at the Servers, not at the AP

→ In order to allow roaming, only the 3 first pairs of MAC (Vendor's identification) were used.



Securing the network



The ***minor*** risks:

→ Only blocks external navigation. Do not deny association.

→ Subject to MAC spoofing

→ Even without MAC spoofing machines with Marvell chipset could use the network.

Securing the network

The ***major*** risks:

→ **Eavesdropping** – anyone with a Wireless card in promiscuous mode could “hear” the traffic – no privacy.

→ **Data injection/modification** – anyone with a appropriate card/software could inject or modify data, sending wrong information to the students.

→ **Rogue Access Point** – just configuring the same SSID an attacker could catch stations to his/her own structure.

→ **Man-in-the-Middle (MitM) attack** - trivial with a Rogue AP and DHCP server. Possible without Rogue AP too, using some arp spoofing tool (dsniff for instance)

Wireless security implementations at Ceibal
The challenges

→ There are 174.000 laptops in operation with the Children

→ A “recall” for installation would be very time consuming and unpractical.

→ The implementation should be transparent and without human intervention.

→ The solution should be compatible with the graphical environment the kids are using today.

→ All the process must be 100% secure but we should consider that initially the informations will travel over a today insecure network.

Tools we have to facilitate our job

→ OLPC has a process to secure update the XO's

→ This process can be used to install some scripts that can run with root privileges on the laptops.

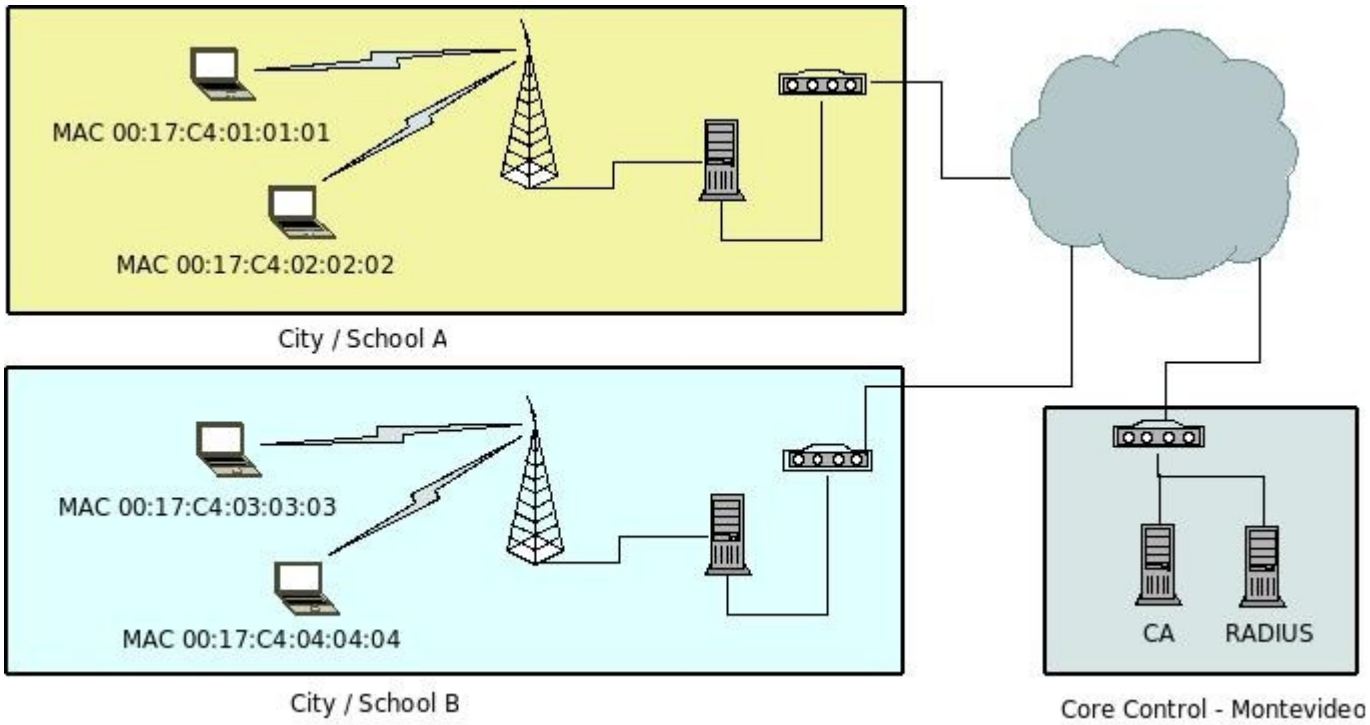
→ SFTP (secure ftp) is available at the XO's

→ Fortunately XO's Linux has full support for openssl for generating certificate requests securely.

Preparing the environment

Typically schools have at least one Access Point and one server (PC based) that makes NAT, Firewall, wiki, etc.

To deploy the security framework we are proposing a core router in Montevideo to control all the schools.



Preparing the environment

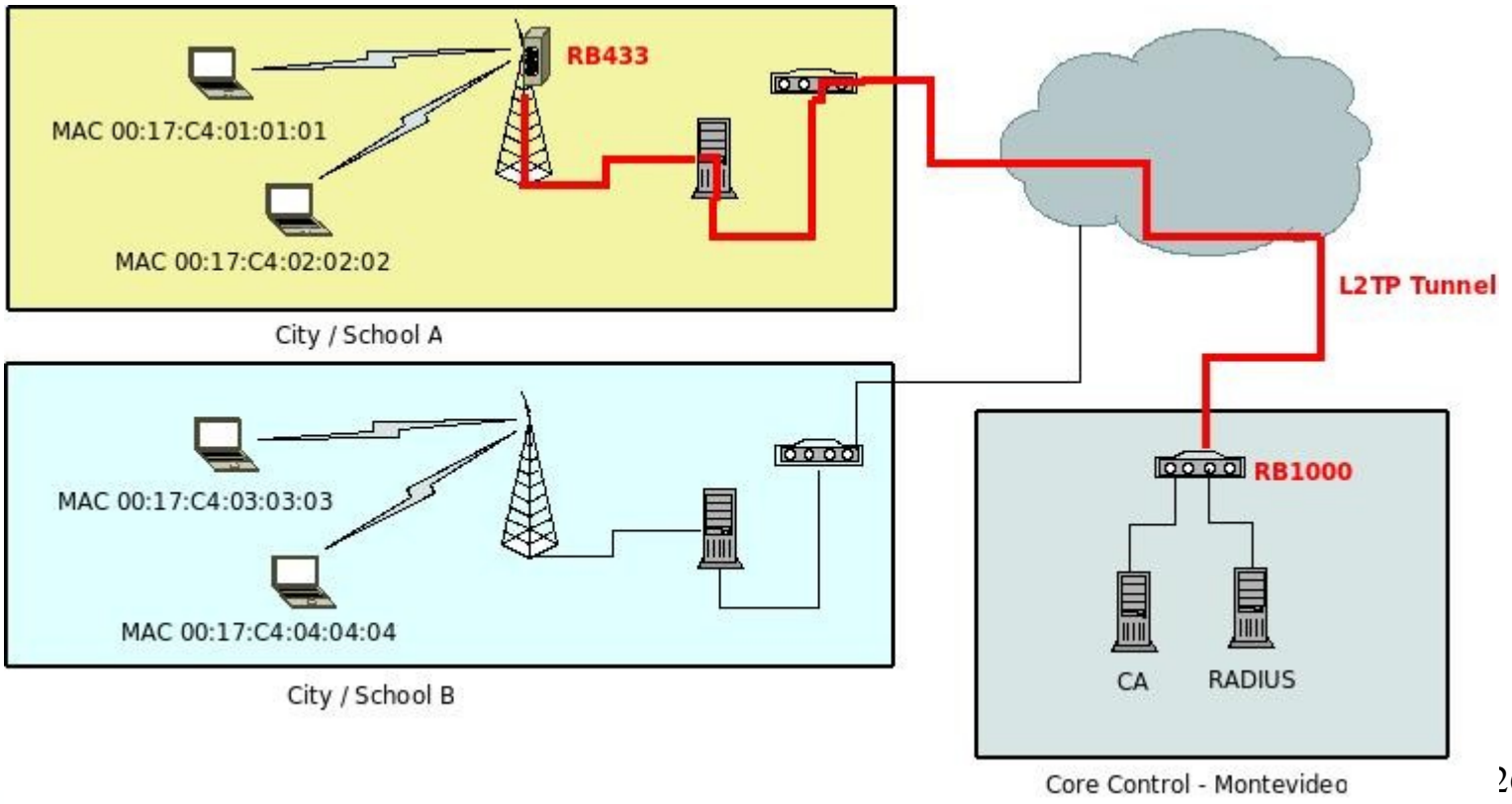
Despite having sftp at XO, we cannot ensure a secure communication over the Internet because of the possibility of a Man-in-the-middle attack (XO's have no means to authenticate the server)

On the other hand, it is necessary to access remotely the Access Points from the core side and most of them are behind a NAT made by server (PC) present in many schools.

To achieve these 2 goals (security and transparency), L2TP tunnels with IPSec between all AP's and the main core should be configured.

Preparing the environment

Security and transparency made by L2TP tunnel with IPSec between all AP's (typically RB433) and core router.



Securing the Access Points

First Proposed solution:

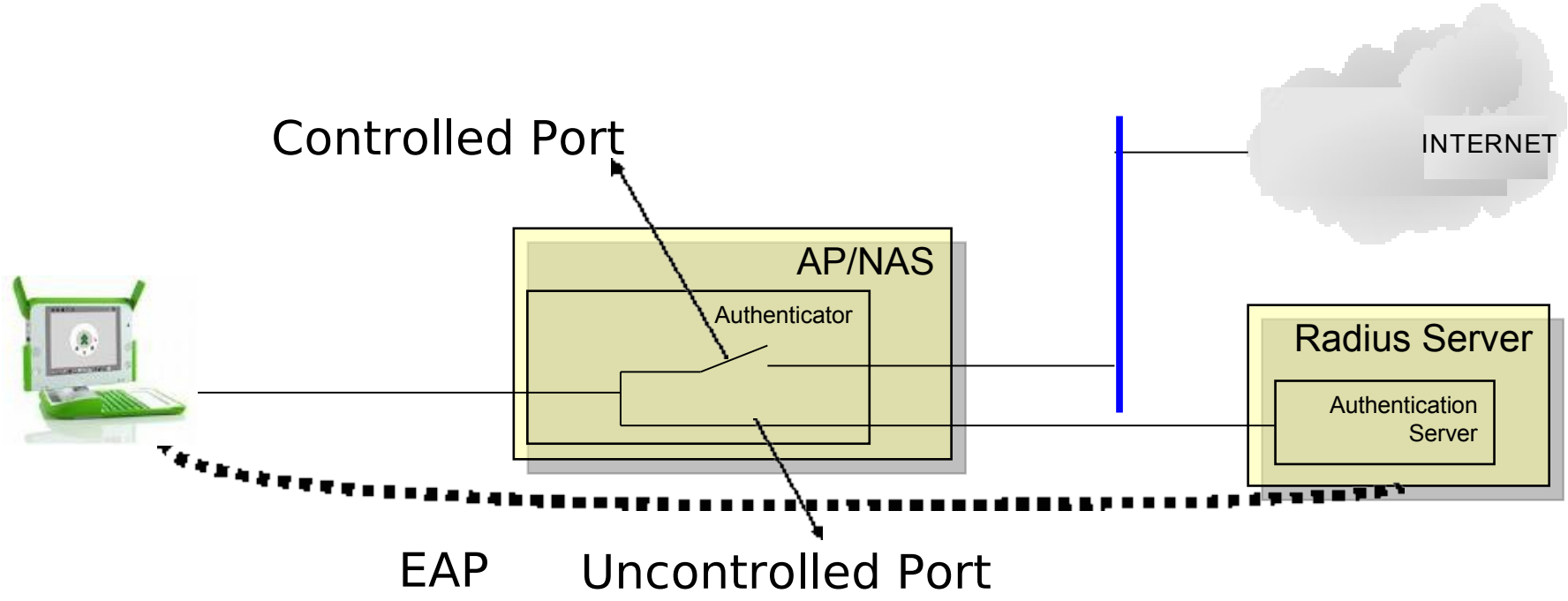
802.11i (WPA2) Enterprise mode

OBS:

WEP – were not considered because it is insecure and obsolete.

WPA – was not considered because all XO's support WPA2.

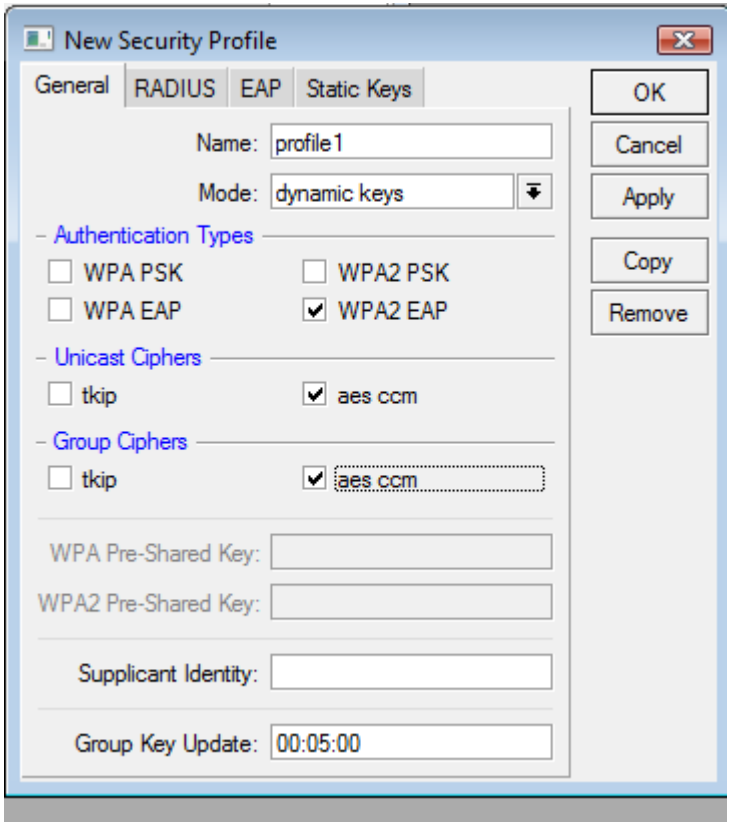
802.11i – Enterprise mode

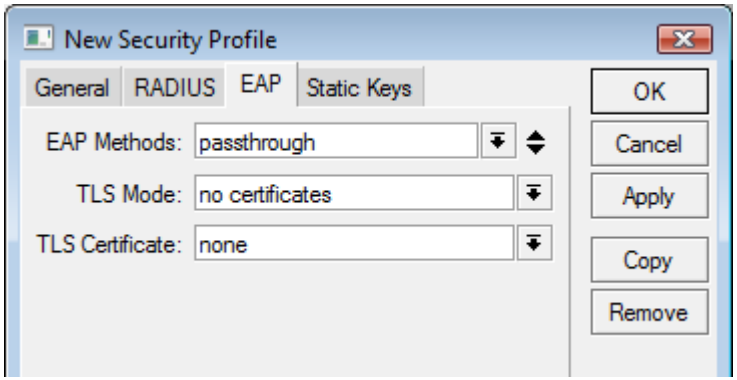


→ The negotiation between Station and Radius results in a PMK that is installed in station and AP.

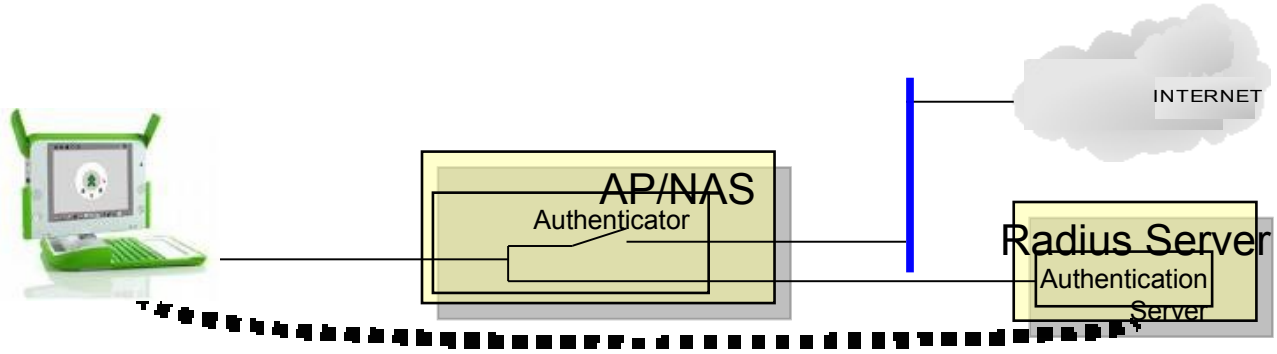
→ PMK is used start encryption/integrity check process.

802.11i – Enterprise mode





802.11i – Enterprise mode



There are several EAP methods. The method chosen for Ceibal project was EAP-PEAP.

With this method we have:

→ Certificates installed both in Clients and Radius

→ username and password on Client side

→ Mikrotik AP in passthrough mode (802.1x compatible)

802.11i implementation

1 – CA Creation

→ CA private key hard locked for security

2 – Certificate requests and random username/passwords generation

3 – CA signature

4 – XO Installation

Before starting the process

XO

CA

XO Identity (i)

XO MAC (i)

XO Identity (1...n)

XO MAC (1...n)

Scripts running at the XO and CA side

XO

CA

XO(i) generate cr(i), pk(i) ppk(i), peapuser(i), peappass(i)

XO send data via sftp

Check Integrity

No

Yes

My first homework is concluded.

CA looks up in an upcoming dir.

Are there new Req's ?

No

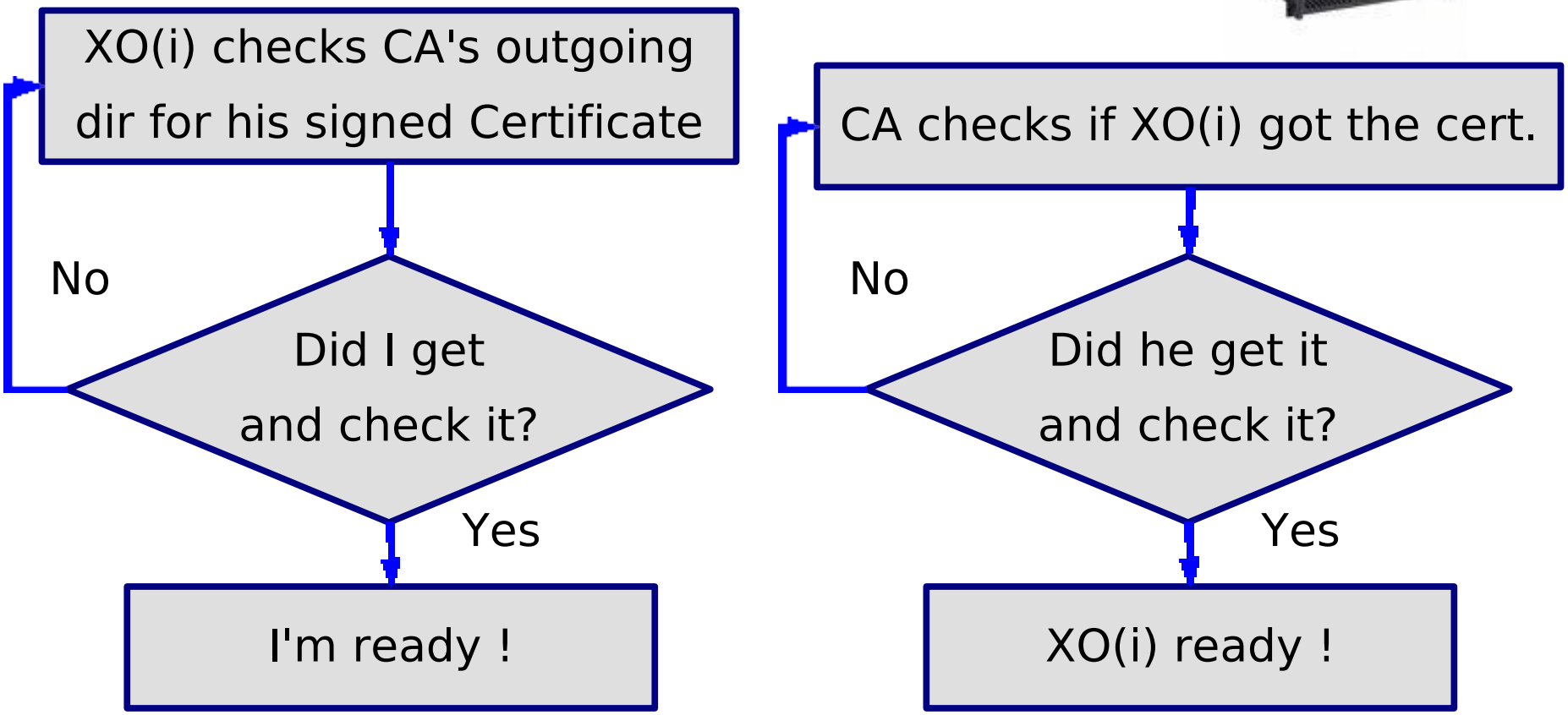
Yes

Sign reqs and put at outgoing dir.

Scripts running at the XO and CA side

XO

CA



After the scripts have run

XO

CA

XO Identity (i)

XO MAC (i)

→ Signed Certificate (i)

→ Private Key (i)

→ Private Key passphrase (i)

→ CA public Certificate (i)

→ Peap Username (i)

→ Peap password (i)

XO Identity (1...n)

XO MAC (1...n)

→ Signed Certificate (1...n)

→ Private Key (1...n)

→ Private Key pass (1...n)

→ CA public Certificate (1...n)

→ Peap Username (1...n)

→ Peap password (1...n)

Securing the Access Points

First Proposed solution:

802.11i (WPA2) Enterprise mode

Ready to run ?

Unfortunately NOT :-(

→ 802.11i EAP-PEAP runs fine with WPA supplicant, but...

→ Current version of OLPC Network Manager (Graphical Interface) is not able to manage 802.1x.

→ Network Manager developers are working in 802.1x supportable version, but no time frame is clearly assumed.

→ Laptops should be able to connect in home open networks also and we cannot ask children to open a terminal an run Unix commands.

Securing the Access Points

Second Proposed solution:

802.11i (WPA2)
1 PSK per client

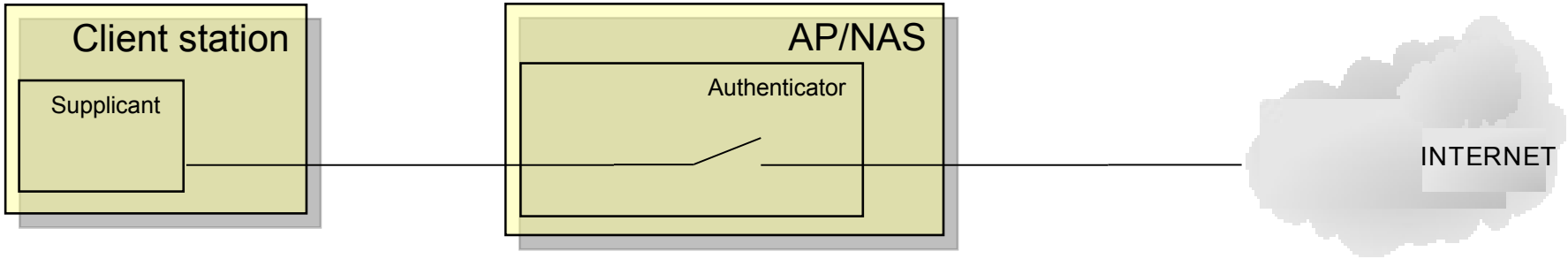
.

How WPA2 – PSK works

→ SSID and PSK generate a PMK (Pairwise Master Key)

→ PMK is used to generate a PTK (Pairwise Transient Key) that is unique per client and per session.

SSID = linksys; PSK = 12345678 (bad idea)



maia@maia-laptop:~$ wpa_passphrase linksys 12345678

PMK=9f2c39e00c30c1efec5fb12fe3c51f4bb7c75a6d9dc7e8541d0e3cfade0ad17c

Enterprise x PSK

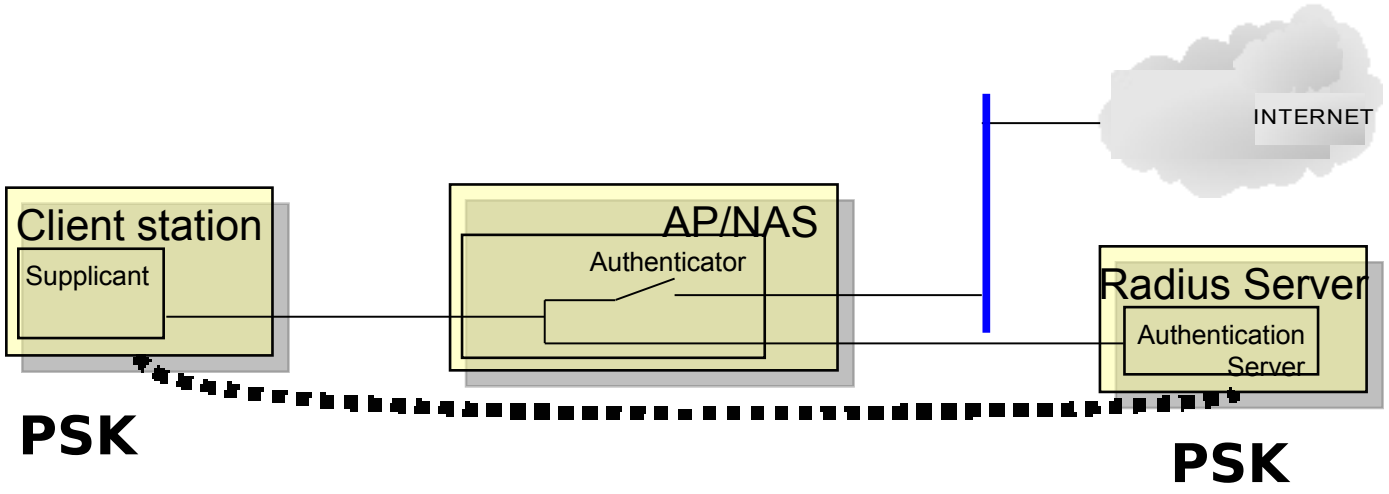
Is PSK less secure than Enterprise Mode ?

In terms of **Privacy** and **Integrity**, the answer is **NO** because both techniques use:

→ for encryption: **AES (Advanced Encryption Standard)**
→ for integrity: **CBC-MAC (Cipher Block Chaining Message Authentication Check)**

The problem is how the Keys are distributed:
→ If you have one PSK for the whole network and the key got compromised, all security has gone...

WPA2-PSK “Mikrotik Powered”

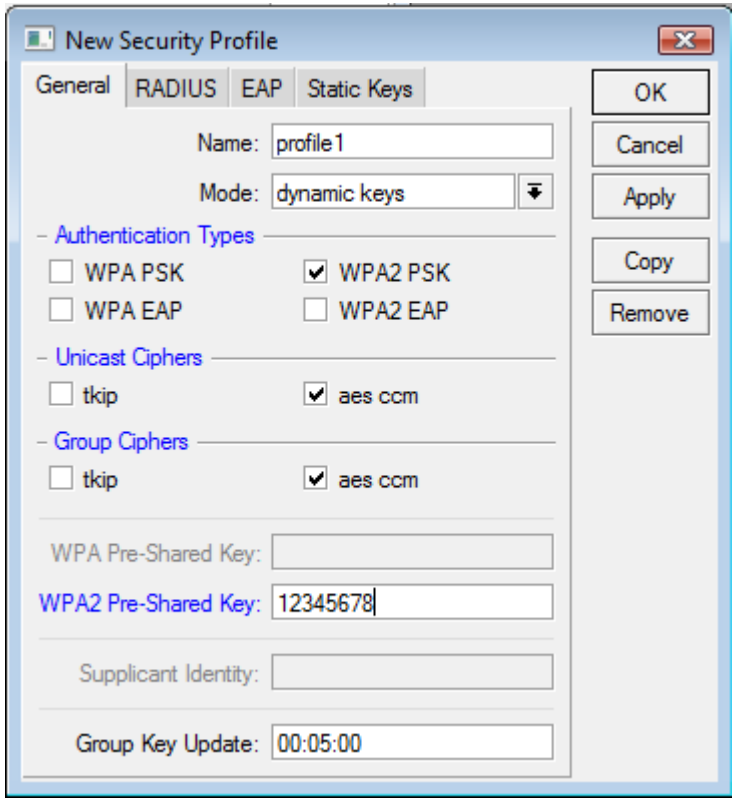


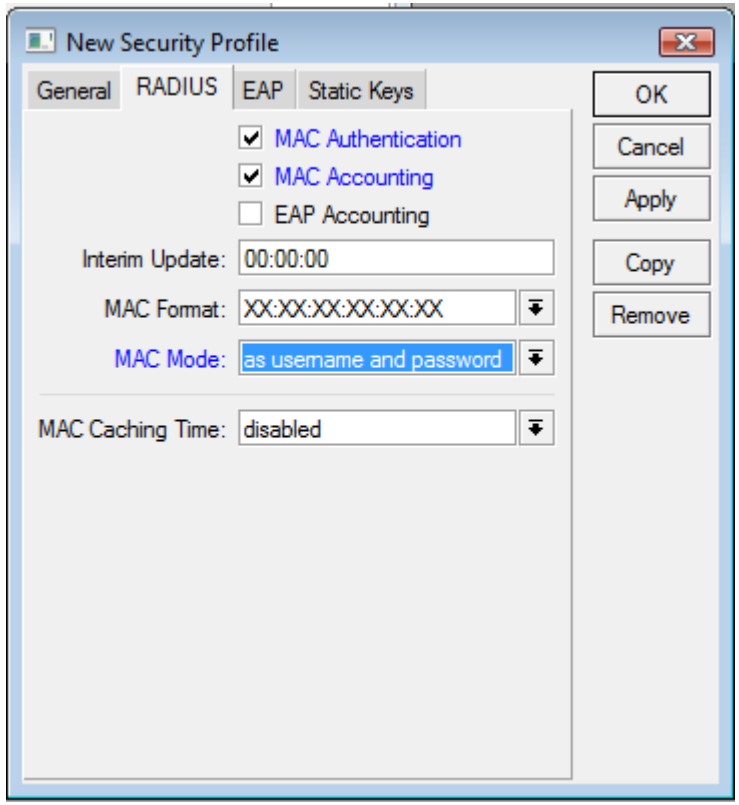
Mikrotik allows to configure 1 PSK per Client (MAC) using Access Lists

→ The Keys can be stored at the Radius Server, tying MAC + PSK

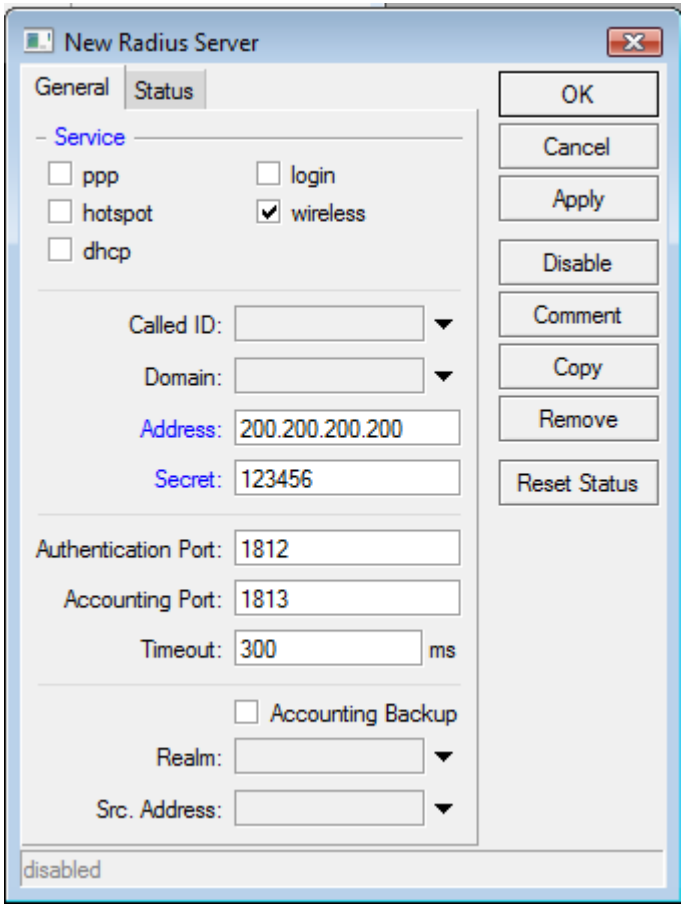
→ No PSK will stay in the AP.

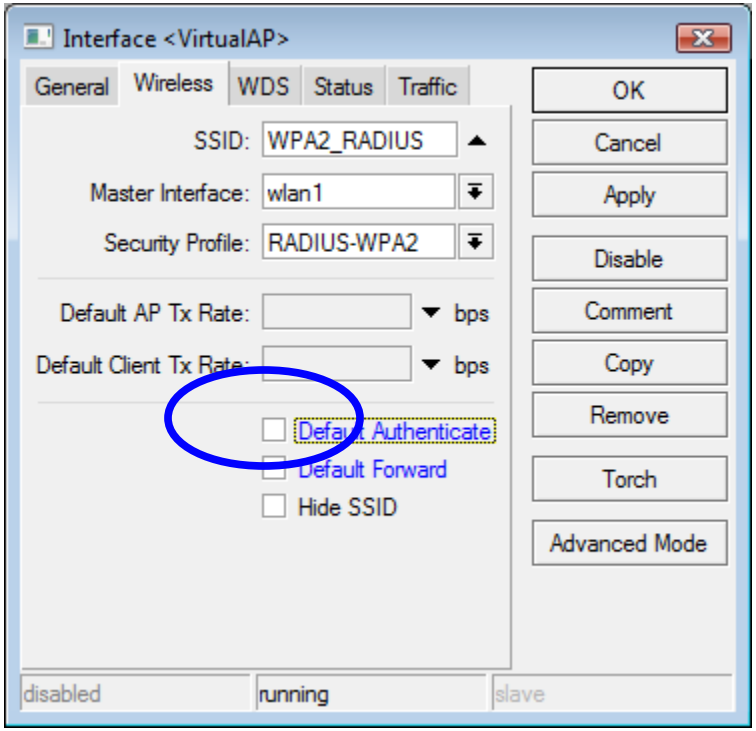
Configuring the Security Profile





Configuring the Wireless Interface





Radius (users)

/etc/freeradius/users

```
# Syntax
# MAC           Cleartext-Password := “MAC“
# Mikrotik-Wireless-Psk =”key_from_8_to_63_characters“


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
```

After the scripts had ran

XO

Radius

XO Identity (i)

XO MAC (i)

…

…

→ PSK (i)

XO Identity (1…n)

XO MAC (1…n)

…

…

→ PSK (1…n)

Is WPA2-PSK “Mikrotik Powered” 100% secure ?

Will MAC spoofing work ?

→ No, because an attacker could spoof the MAC but not guess the PSK.

What about a stolen Laptop ?

→ It will not work anymore because we will deny its association in the Radius server. Stolen MAC and PSK become useless informations.

Is WPA2-PSK “Mikrotik Powered” 100% secure ?

What if the attacker launches a Rogue AP to “hear” the claimed PSK's ?

→ Commercial AP's including Mikrotik do not log wrong PSK tries. Note that we said commercial - the hacker light at the end of the tunnel could be here...

What if the attacker launches a Rogue AP + a Hacked Radius Server to “hear” the claimed PSK's ?

→ Radius uses a symmetrical cryptography hashing the requests and replies using the secret configured at Radius and the AP.

Radius in 'promiscuous' mode

maia@maia-laptop:/etc/freeradius/radiusd.conf

....

Log authentication requests to the log file.

allowed values: {no, yes}

log_auth = yes

Log passwords with the authentication requests.

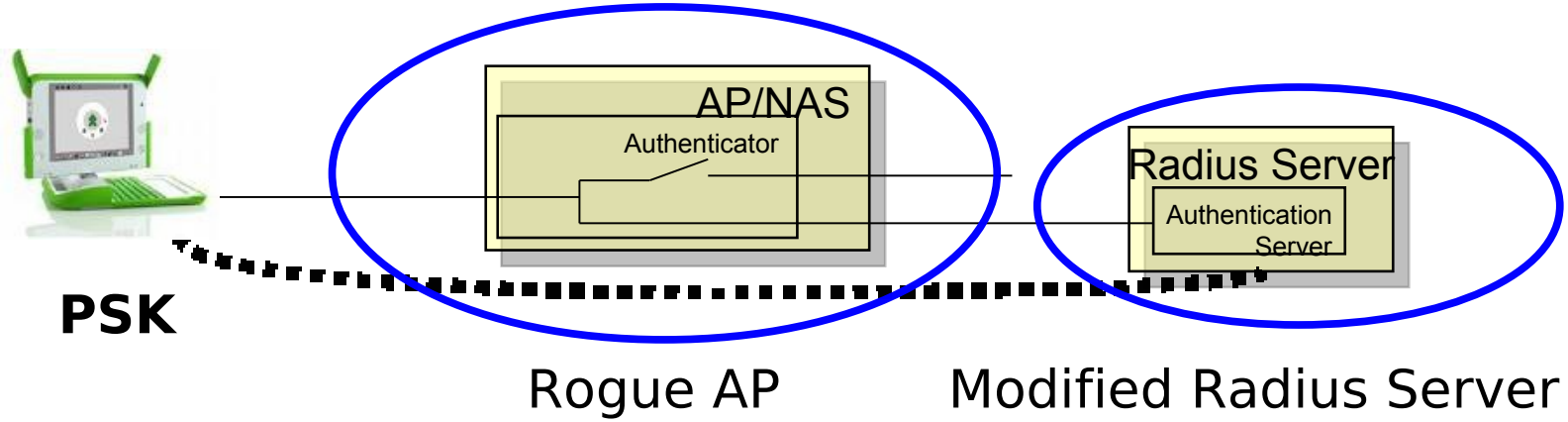
allowed values: {no, yes}

log_auth_badpass = yes

log_auth_goodpass = yes

...

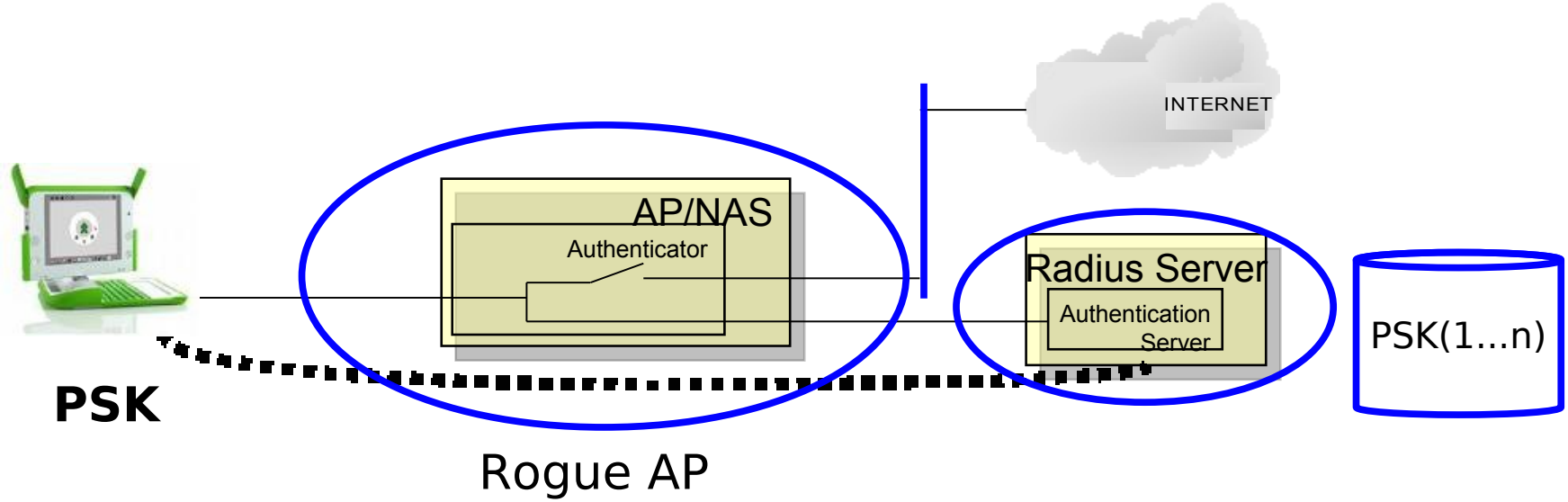
Hacking
WPA2-PSK “Mikrotik Powered”



Hacked Radius Server means a server prepared to de-hash the Radius requests to show them in plain text.

After some time, the hacker discovered all PSK that tried to connect in that AP.

Hacking
WPA2-PSK “Mikrotik Powered”



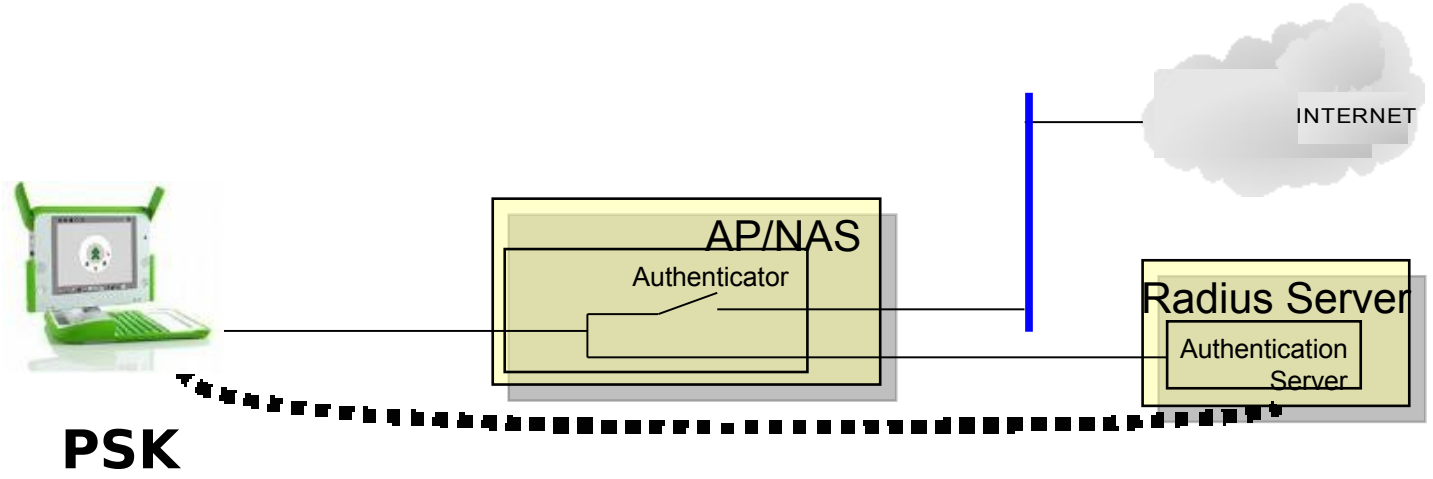
Rogue AP

Now, we have 2 problems related to the XO's with PSK discovered

→ The hacker could launch MitM for all XO's that the key was discovered.

→ Spoofing the MAC(i) and knowing the PSK(i), hacker could use the network

Better protecting WPA2-PSK “Mikrotik Powered”



To create mutual authentication we'll need more 3 symmetrical parameters:

→ KRS1(i) and KRS2(i): Key Radius Server credentials exclusive for XO(i) – XO will expect to see those keys at Radius Server.

→ KXO(i): Key XO credential exclusive for XO(i) – Radius Server will expect to see this key from the XO

After the scripts had ran

XO

Radius

XO Identity (i)

XO MAC (i)

...

...

PSK (i)

→ KXO(i)

→ KRS1(i)

→ KRS2(i)

XO Identity (1...n)

XO MAC (1...n)

...

...

PSK (1...n)

→ KXO(1...n)

→ KRS1(1...n)

→ KRS2(1...n)

Better protecting WPA2-PSK “Mikrotik Powered”

PSK(i) →

← Radius Reply OK

Connection Established

XO 

← Radius sends KRS1(i)

Radius

If KRS1(i) is OK, XO sends KXO(i) →

← If KXO(i) is received Radius sends KRS2(i)

XO can access the internet

Better protecting WPA2-PSK “Mikrotik Powered”

To hack this setup, the attacker should:

→ Install a Rogue AP and a hacked Radius Server

→ Stay a long time “hearing” the requisitions

Theoretically is possible to obtain MAC(i), PSK(i) and even KRS1(i) but, because of he won't have KXO(i), he won't obtain KRS2(i). In practice it means:

→ He could not use Network Resources

→ He cannot perform MitM attack against anyone

All keys are useless information for the hacker !

Conclusions about the proposed solutions

→ No matter of fact that EAP PEAP is more elegant and a more secure solution.

→ With EAP-PEAP Network Manager integration is a problem though.

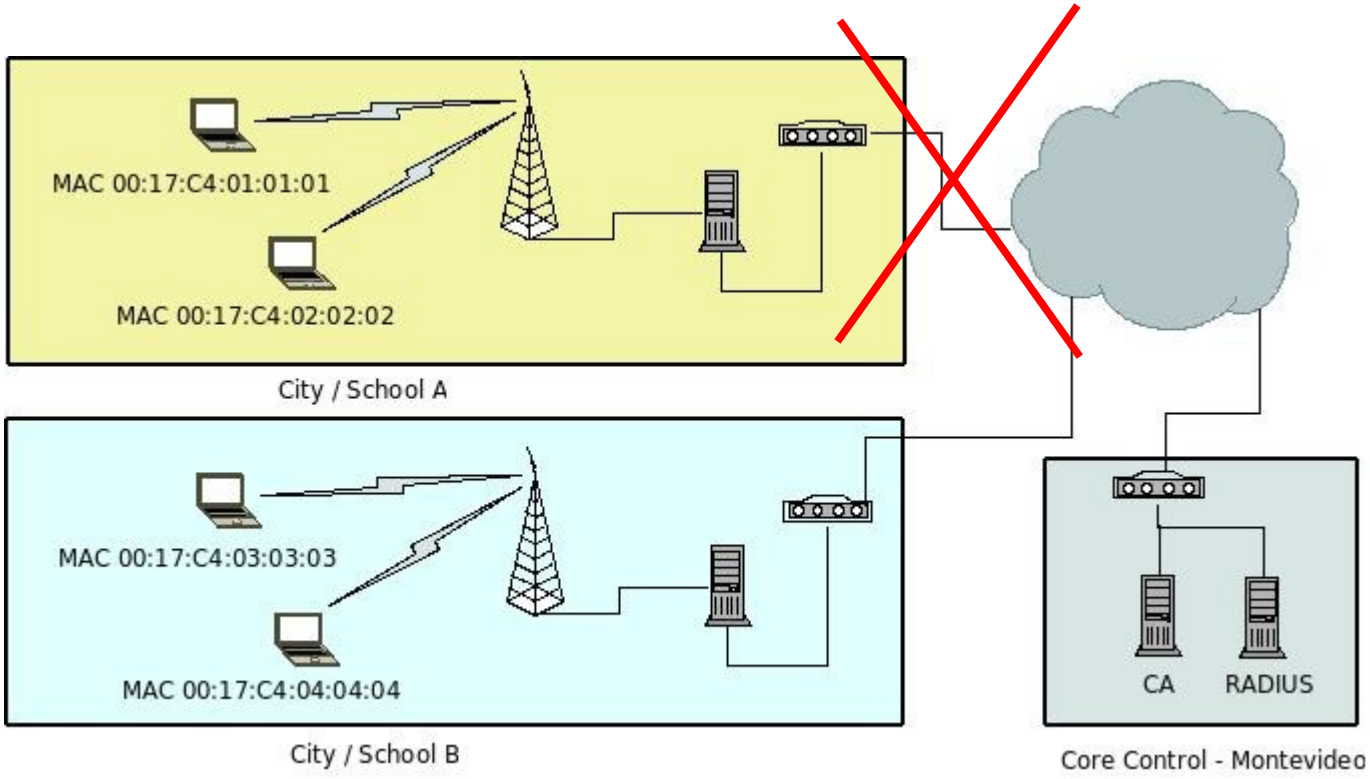
→ “Mikrotik Powered PSK” could be deployed with a high grade of security.

→ The good news are that the algorithms to generate all the parameters are the same for PSK or for Certificates.

Proyecto Ceibal

Network Reliability

What if Internet connection fails ?



There are activities other then Internet, like local wiki, etc

Children should be able to access them !

One parameter more...

XO

CA

XO Identity (i)

XO MAC (i)

...

PSK (i)

KXO(i)

KRS(i)

PSK2(i)

XO Identity (1...n)

XO MAC (1...n)

...

PSK (1...n)

KXO(1...n)

KRS(1...n)

PSK2(1...n)

What if Internet connection fails ?

Server maintain a list of the XO that had connected in Every AP during the last 5 days

→ Mikrotik AP fetches the list and maintain a disabled access list with XO_MAC(i), PSK2(i)

tool fetch address=201.14.21.253 user=ceibal_AP password=xxxxxxxxxxxxx dst-path=xoi_directory

What if Internet connection fails ?

→ Server connectivity is monitored with netwatch

→ If connection fails, default profile is disabled and an alternative profile is launched

→ A new secure profile with one PSK per XO becomes available.

→ Children click on the new icon and get connectivity :-)

Conclusions

→ Ceibal project is a good example of digital inclusion for other developing countries.

→ It is possible to provide a high level of security, despite the limitations explained. Uruguay case can be used for other similar projects and even for deploying security to large networks.

→ Mikrotik reach features and flexibility is helping a lot to make things easier and economically feasible.

OLPC & Mikrotik

Our special thanks for

– OLPC project and LATU – the government department responsible for the project management.

– Our Latin America Partners - Servinfo, which gave us the chance to participate in this wonderful project.

– Our European Partners FMS Internetservice (Germany) and Wireless Connect (Ireland), for a lot of useful information exchanged.

Děkuji

Na zdraví!

Wardner Maia
maia@mikrotikbrasil.com.br