

Plan de la présentation

- ➔ Cahier des charges
- ➔ Présentation sommaire de la gamme Aruba
- ➔ Intégration dans notre réseau
- ➔ Choix des SSID diffusés à Subatech
- ➔ Administration du switch au quotidien
- ➔ Possibilités et évolutions
- ➔ Limitations du switch
- ➔ Conclusion

Cahier des charges

- administration simple et centralisée
- forte intégration par rapport au réseau existant
- sécurité optimale
- évolutivité du produit
- simplicité d'architecture
- bonnes performances

Gamme des Switches ARUBA



Aruba 6000 (de 256 à 512 APs, 8000 utilisateurs)



Aruba 5000 (de 48 à 256 APs, 8000 utilisateurs)



Aruba 2400-48 (48 APs, 512 utilisateurs)



Aruba 800-16 (16 APs, 256 utilisateurs)

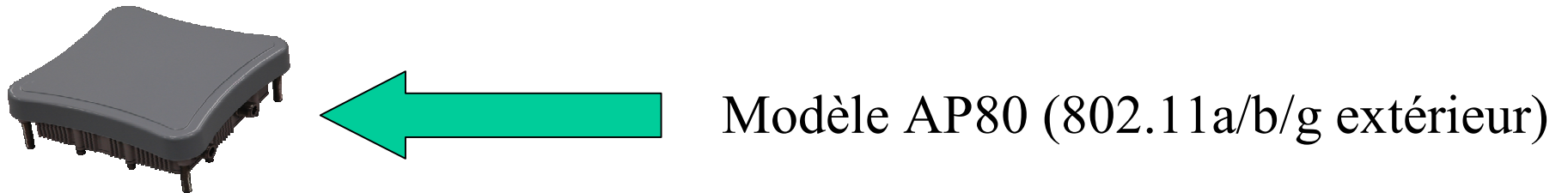
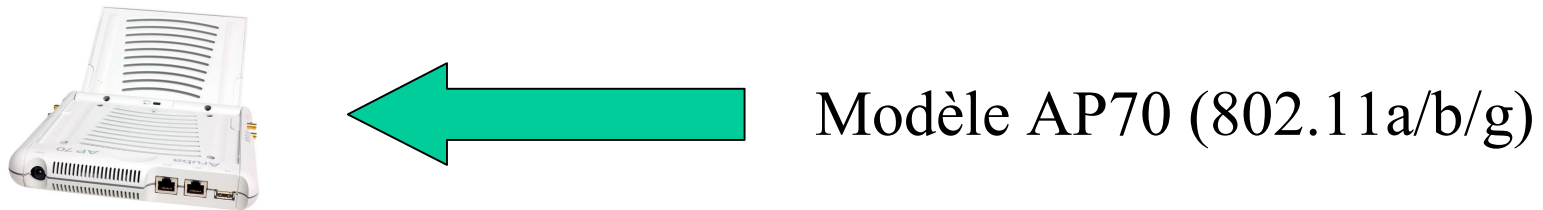
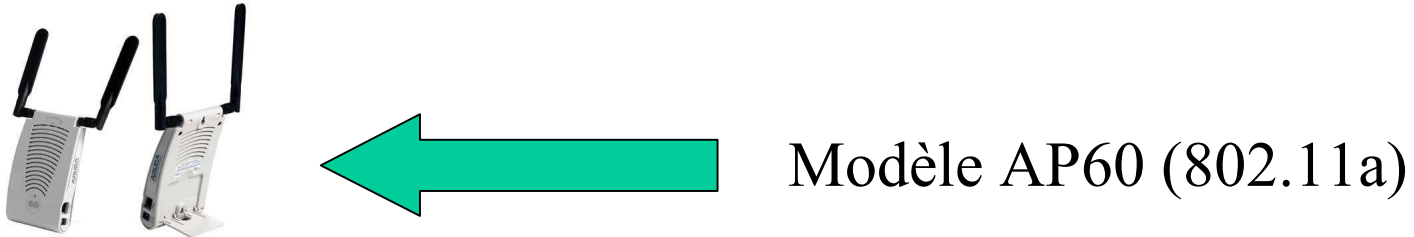
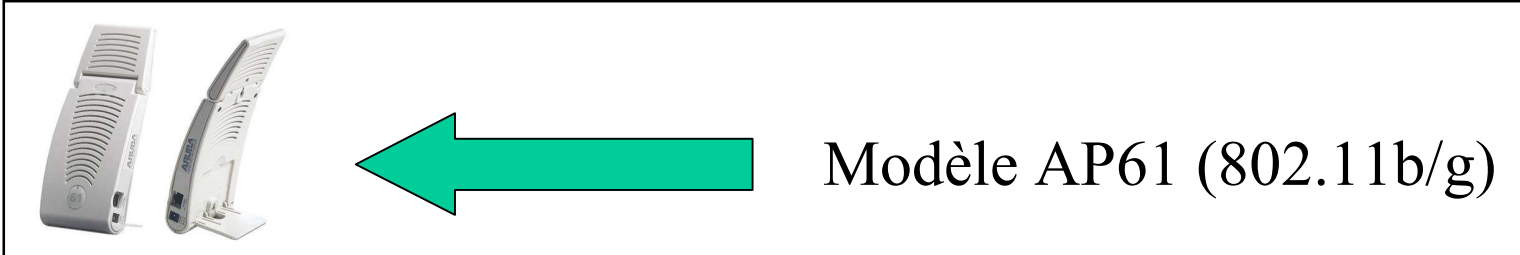


Aruba 800-4 (4 APs, 60 utilisateurs)

Caractéristiques de l'ARUBA 800

- emplacement 1U
- gère jusqu'à 16 points d'accès
- accepte 256 sessions VPN simultanées (licence)
- débit max. sans chiffrement: 1 Gb/s
- débit max. avec chiffrement: 200 Mb/s
- firewall statefull (licence) par utilisateur et par port
- redondance possible

Gamme des points d'accès

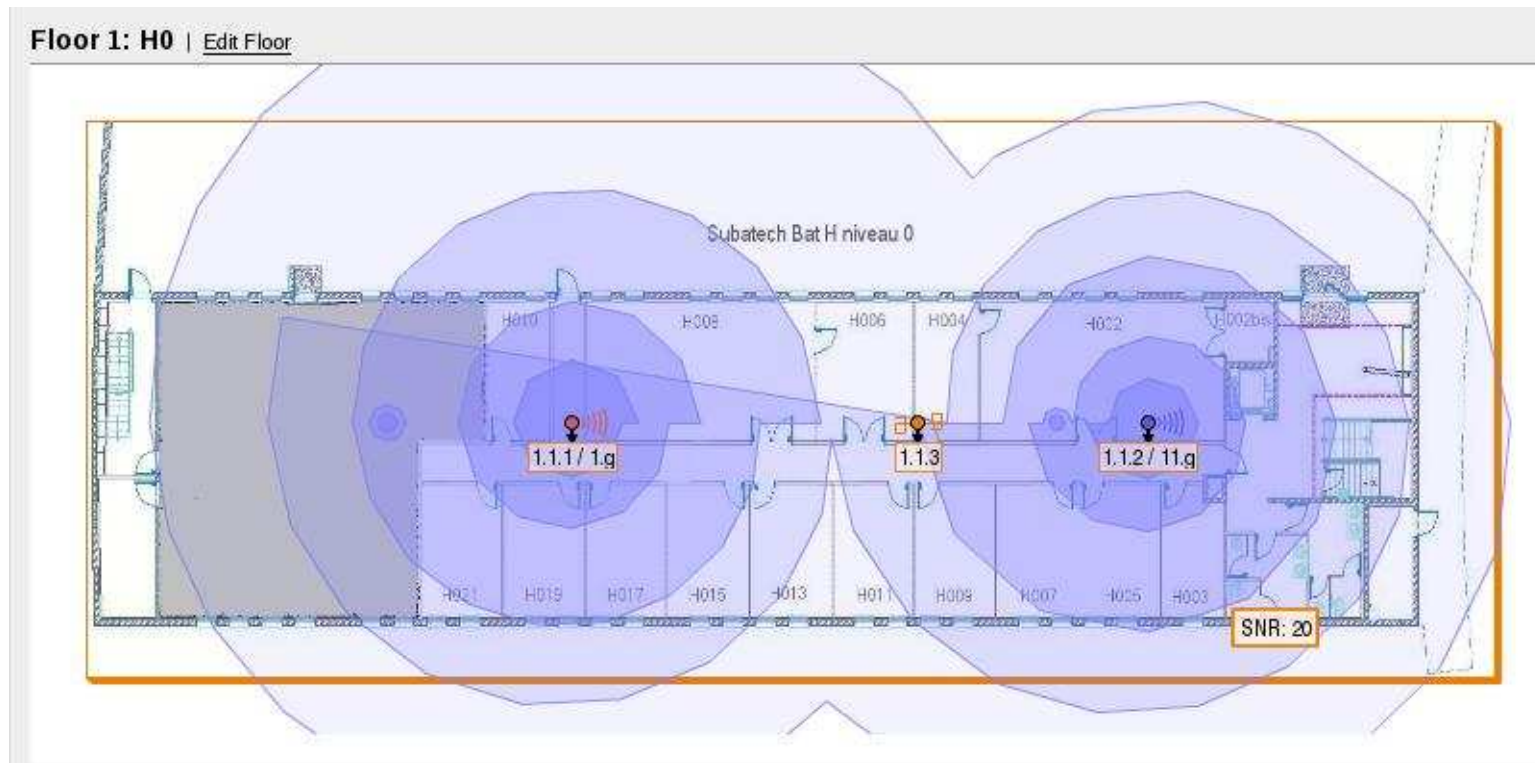


Caractéristiques des bornes WiFi

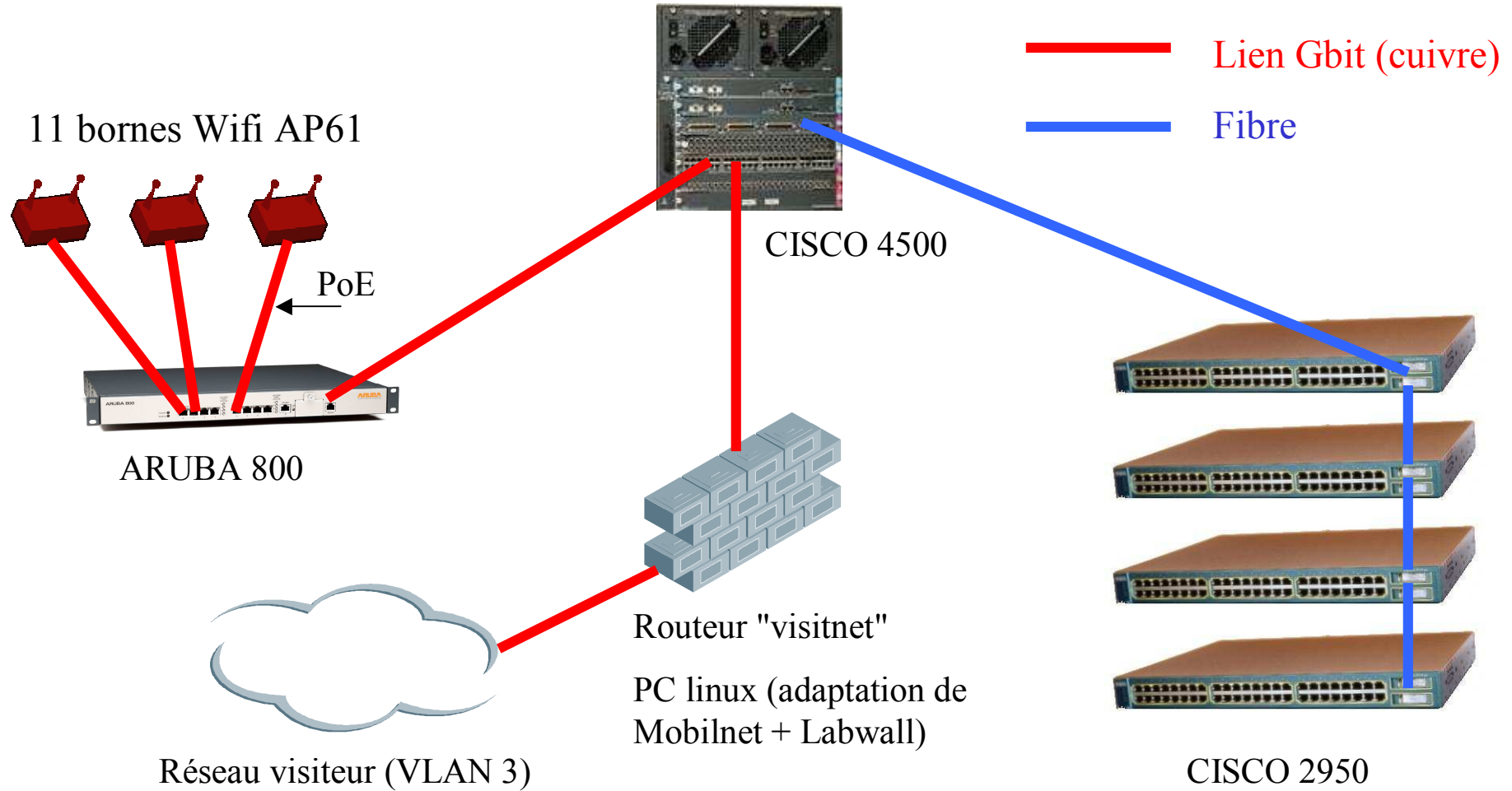
- auto-alimentées (PoE) ———> facilité d'installation
- auto-négociation des puissances d'émission entre les bornes
- auto-négociation des canaux d'émission entre les bornes
- partage de charge dynamique entre les bornes
- aucun paramètre stocké dans les bornes (en cas de vol)
- roaming avec conservation de l'authentification et des droits

Exemple de déploiement des points d'accès (bât. H, RdC)

➔ Étude préalable de l'emplacement des bornes faite par Teldata



Intégration du switch dans notre réseau local



Pré-requis:

- Compatibilité avec le parc de portables Wifi existant
- Maximum de sécurité (parc Windows)

Notre choix:

- Cryptage: WPA/TKIP
- Double authentification:
 - PEAP avec MSCHAPv2 (Login/passwd du domaine Windows)
 - Adresse MAC (base interne Aruba)
- Même adresse IP qu'en filaire (VLAN1) → pas de pont
- Mêmes droits d'accès qu'en filaire
- Double inscription Adresse Mac (wifi + éther) → DHCP

Diagnostics Maintenance Plan Events Reports Save Configuration Logout

WLAN > New [Help](#)

subatech/802.11a subatech/802.11b/g suba-guest/Global suba-portail/Global New

Network

Network Name (SSID)

Radio Type

802.11 Security

Network Authentication None 802.1x/WEP WPA WPA-PSK WPA2 WPA2-PSK

Encryption TKIP

Advanced Authentication None Registration Web Page Captive Portal (Web) MAC

Auth Server Type

Keys

PSK Key/Passphrase Format

The PSK Hex Key should be a 64 character hexadecimal string
 The PSK Passphrase should be an ASCII string 8-63 characters in length

Authentication Server

Server Name	IP Address	Authentication Port	Acct Port	Shared Key	Actions
nanrad1	134.158.24.24	1812	1813	XXXX	Delete ▲ ▼

VLAN

VLAN ID

Pré-requis:

- Visiteurs longue durée (> 1 semaine)
- Minimum de sécurité
- Facilité de configuration (Linux)

Notre choix:

- Cryptage: WEP (clé 128 bits stockée dans le switch et renouvelée 1 fois/mois)
- Authentification: Adresse MAC (Freeradius)
- Même adresse IP qu'en filaire (VLAN3) délivrée par le serveur DHCP de Visitnet (pas de pont)
- Mêmes règles de filtrage qu'en filaire (accès à nos imprimantes, intranet, ...)

[Diagnostics](#) | [Maintenance](#) | [Plan](#) | [Events](#) | [Reports](#) | [Save Configuration](#) | [Logout](#)

WLAN > New [Help](#)

[subatech/802.11a](#) | [subatech/802.11b/g](#) | [suba-guest/Global](#) | [suba-portail/Global](#) | [New](#)

Network

Network Name (SSID)
 Radio Type

802.11 Security

Network Authentication None 802.1x/WEP WPA WPA-PSK WPA2 WPA2-PSK
 Encryption Open WEP
 Advanced Authentication None Registration Web Page Captive Portal (Web) MAC
 Auth Server Type

Keys

Use as Tx Key	WEP Key	Size
1	<input type="text" value="*****"/>	26 Hex

Enter 64-bit WEP key as 10 hexadecimal digits(0-9, a-f or A-F)
 Enter 128-bit WEP key as 26 hexadecimal digits(0-9, a-f or A-F)

Authentication Server

Server Name	IP Address	Authentication Port	Acct Port	Shared Key	Actions
nanrad1	134.158.24.24	1812	1813	123sub	Delete ▲ ▼

[Add](#)

VLAN

VLAN ID

Pré-requis:

- Visiteurs courte durée (< 1 semaine): séminaires, conf, ...
- Zéro configuration
- Accès authentifié (différent d'un hotspot)

Notre choix:

- Aucun cryptage
- Authentification via portail sécurisé (HTTPS): couple login/passwd défini directement dans la base interne du switch
- VLAN3: adresse IP délivré par Visitnet
- Filtrage Visitnet + filtrage Aruba: accès au HTTP(S) et SSH uniquement

Diagnosics Maintenance Plan Events Reports Save Configuration Log

VLAN > New

subatech/802.11a subatech/802.11b/g suba-guest/Global suba-portail/Global New

Network

Network Name (SSID) suba-portail

Radio Type 802.11 a/b/g

802.11 Security

Network Authentication None 802.1x/WEP WPA WPA-PSK WPA2 WPA2-PSK

Encryption Open WEP

Advanced Authentication None Registration Web Page Captive Portal (Web) MAC

Auth Server Type Internal Show Internal Database

Keys

PSK Key/Passphrase Format Hex

The PSK Hex Key should be a 64 character hexadecimal string
The PSK Passphrase should be an ASCII string 8-63 characters in length

VLAN

VLAN ID 3

Admin: enregistrement d'un portable sur le réseau permanent

The screenshot shows the Aruba Advanced Configuration web interface in Mozilla Firefox. The browser address bar displays the URL: https://134.158.30.100:4343/screens/switch/config_sec_servers.html. The interface is titled "Security Authentication Servers" and shows the "Internal Database" configuration for "AAA Servers".

The "Server Rules" section contains the following table:

Rule Action	Attribute	Condition	Matching Value	Value	Action
Role Assignment	role	value-of			Delete ▲ ▼
Vlan Assignment	Tunnel-Type	value-of			Delete ▲ ▼
Role Assignment	ssid	equals	suba-portail	pre-employee	Delete ▲ ▼

The "Maintenance" section includes buttons for "Export", "Import", "Delete All Users", and "Repair Database".

The "Users" section contains the following table:

User Name	Password	Role	E-mail	Enabled	Expiry	Action
1_NE_PAS_EFFACER_AU_DESSUS_	*****			Yes		Disable Delete Modify
00:90:4b:60:00:00	*****			Yes		Disable Delete Modify
00:13:ce:0e:00:00	*****			Yes		Disable Delete Modify
00:13:ce:0e:00:00	*****			Yes		Disable Delete Modify
00:01:03:fa:00:00	*****			Yes		Disable Delete Modify
00:06:5e:90:00:00	*****			Yes		Disable Delete Modify
00:0b:db:00:00:00	*****			Yes		Disable Delete Modify
00:0b:db:d0:00:00	*****			Yes		Disable Delete Modify
00:0c:f1:3e:00:00	*****			Yes		Disable Delete Modify
00:0c:f1:56:00:00	*****			Yes		Disable Delete Modify
00:0e:35:79:00:00	*****			Yes		Disable Delete Modify
00:0e:35:e1:00:00	*****			Yes		Disable Delete Modify
00:0e:35:87:00:00	*****			Yes		Disable Delete Modify
00:0e:35:d0:00:00	*****			Yes		Disable Delete Modify
00:11:24:a5:00:00	*****			Yes		Disable Delete Modify
00:12:f0:26:00:00	*****			Yes		Disable Delete Modify
00:13:ce:0e:00:00	*****			Yes		Disable Delete Modify
00:13:ce:0e:00:00	*****			Yes		Disable Delete Modify
00:13:ce:51:00:00	*****			Yes		Disable Delete Modify
00:13:ce:60:00:00	*****			Yes		Disable Delete Modify
00:13:ce:c0:00:00	*****			Yes		Disable Delete Modify

Admin: enregistrement d'un portable sur le réseau permanent

The screenshot shows a Mozilla Firefox browser window displaying the Aruba Advanced Configuration web interface. The address bar shows the URL: `https://134.158.30.100:4343/screens/switch/config_sec_servers.html`. The browser's bookmark bar contains several folders like 'Linux', 'Divers', 'Sites FTP', etc. The page title is 'Security Authentication Servers'. The interface has a top navigation bar with tabs: 'Monitoring', 'Configuration', 'Diagnostics', 'Maintenance', 'Plan', 'Events', 'Reports'. The 'Configuration' tab is active, and the breadcrumb path is 'Security > AAA Servers > Internal Database > Add User'. On the left, there is a sidebar menu with categories: 'Switch', 'WLAN', 'RF Management', 'WLAN Intrusion Protection', and 'Security'. The 'AAA Servers' option is selected. The main content area contains a form for adding a user with the following fields and options:

- User Name:
- Password:
- Verify Password:
- Role:
- E-mail:
- Enabled:
- Expiration: Entry does not expire (selected), Set Expiry time (mins) [input type="text" value=""], Set Expiry Date (mm/dd/yyyy) [input type="text" value=""] [input type="text" value=""] Expiry Time(hh:mm) [input type="text" value=""] [input type="text" value=""]

Buttons for '< Back' and 'Apply' are visible. The footer of the page shows 'Aruba Networks™' on the left and 'E-mail Support' on the right. The status bar at the bottom indicates 'Done' and the IP address '134.158.30.100:4343'.

Admin: enregistrement d'un portable sur le réseau visiteur

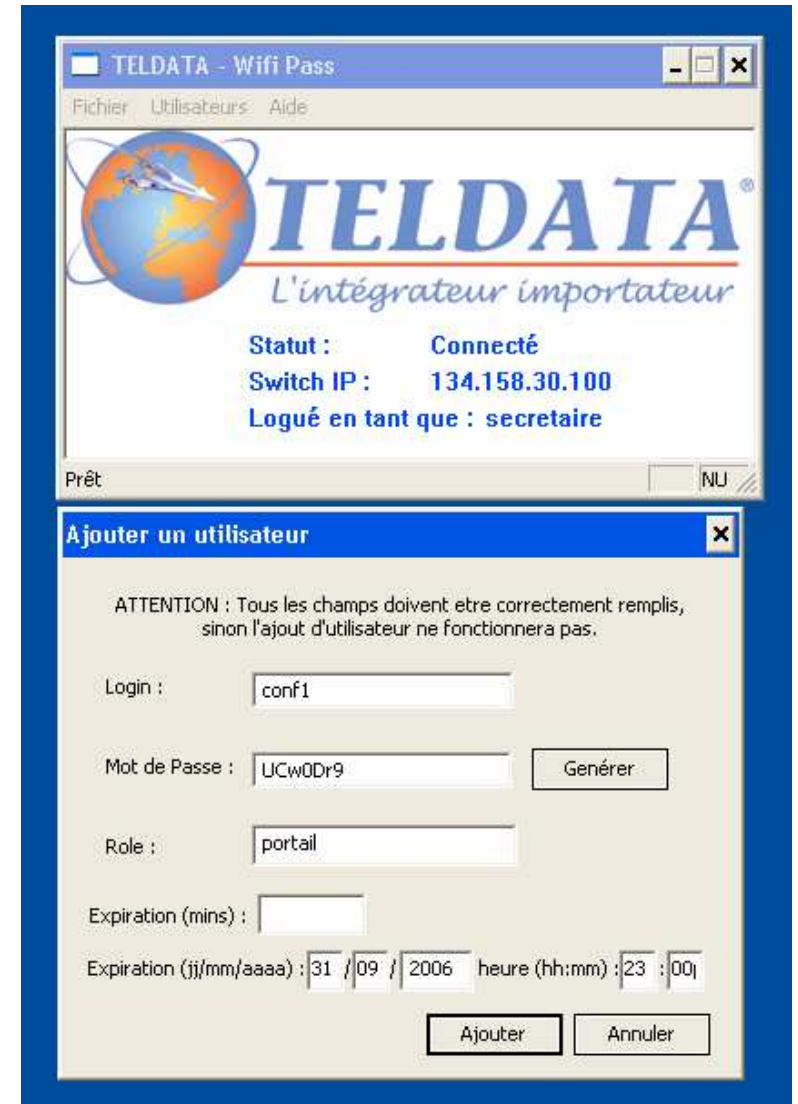
Inscription de l'adresse Mac sur le serveur Radius dans le fichier /etc/raddb/users:

```
123456789abc auth-type := local, user-password == "123456789abc"  
004096a6xxxx auth-type := local, user-password == "004096a6xxxx"  
0014a557xxxx auth-type := local, user-password == "0014a557xxxx"  
0013d467xxxx auth-type := local, user-password == "0013d467xxxx"  
000b5d23xxxx auth-type := local, user-password == "000b5d23xxxx"  
00023fb2xxxx auth-type := local, user-password == "00023fb2xxxx"  
00003935xxxx auth-type := local, user-password == "00003935xxxx"  
001143f1xxxx auth-type := local, user-password == "001143f1xxxx"  
000fb08bxxxx auth-type := local, user-password == "000fb08bxxxx"  
00404507xxxx auth-type := local, user-password == "00404507xxxx"  
0050eb10xxxx auth-type := local, user-password == "0050eb10xxxx"  
000d938axxxx auth-type := local, user-password == "000d938axxxx"  
000cf10exxxx auth-type := local, user-password == "000cf10exxxx"  
000fb039xxxx auth-type := local, user-password == "000fb039xxxx"  
000e3573xxxx auth-type := local, user-password == "000e3573xxxx"  
000fb0eexxxx auth-type := local, user-password == "000fb0eexxxx"
```

Admin: création d'un accès au portail avec l'application WifiPass



Admin: création d'un accès au portail avec l'application WifiPass



Admin: renouvellement de la clé Wep 128 Bits pour Suba-guest

The screenshot shows the Aruba Advanced Configuration web interface. The browser window title is "Access Point Configuration - Mozilla Firefox". The address bar shows the URL: https://134.158.30.100:4343/screens/switch/config_ap.html?mode=NetworkEditSSID&loc=0.0.0&ssid=suba-guest&phytype=Glob. The page title is "Advanced Configuration". The navigation menu includes: Monitoring, Configuration, Diagnostics, Maintenance, Plan, Events, Reports, Save Configuration, and Logout. The left sidebar shows a tree view with categories like Switch, Management, WLAN, RF Management, Security, and WLAN Intrusion Protection. The main content area is titled "WLAN > Network > Edit SSID".

Edit SSID

SSID: suba-guest Forward Mode: Tunnel

Radio Type: 802.11 a/b/g

Hide SSID:

SSID Default VLAN: 3 << None Encryption Type: WEP

Ignore Broadcast Probe Request:

DTIM Period: 1

Encryption Type: NULL WEP TKIP AES-CCM Mixed TKIP/AES-CCM

Static WEP Dynamic WEP

WEP Keys

Inherit from Global Location (0.0.0)

S. No	Use as Tx Key	WEP Key	Size
1	<input checked="" type="radio"/>	*****	26 Hex
2	<input type="radio"/>		26 Hex
3	<input type="radio"/>		26 Hex
4	<input type="radio"/>		26 Hex

Enter 64-bit WEP keys as 10 hexadecimal digits(0-9, a-f or A-F)
Enter 128-bit WEP keys as 26 hexadecimal digits(0-9, a-f or A-F)

Apply

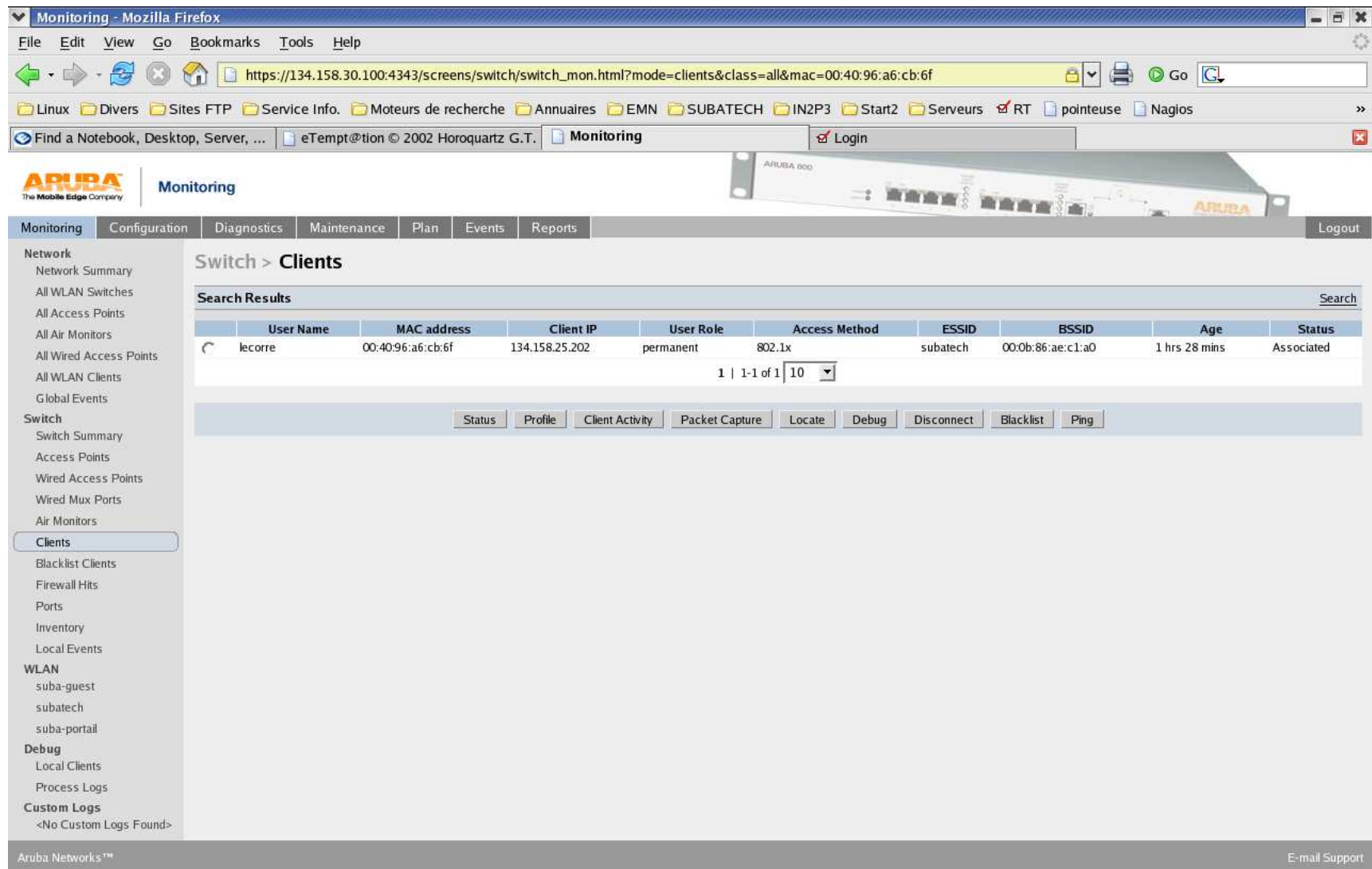
Commands View Commands

Aruba Networks™ E-mail Support

Done 134.158.30.100:4343

	Total	Total	IPSEC	IPSEC
	Up	Down	Up	Down
WLAN Switches	1	0		
Access Points	8	1	0	1
Air Monitors	3	0	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	0			
Duplicate Location Codes	0			
Enterprise Clients	2			
RADIUS Servers	1	0		
LDAP Servers	0	0		

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	19
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	35



The screenshot shows a web browser window with the URL `https://134.158.30.100:4343/screens/switch/switch_mon.html?mode=clients&class=all&mac=00:40:96:a6:cb:6f`. The page title is "Monitoring" and it features the Aruba logo. The main content area is titled "Switch > Clients" and displays search results for a specific MAC address. The results table is as follows:

User Name	MAC address	Client IP	User Role	Access Method	ESSID	BSSID	Age	Status
lecorre	00:40:96:a6:cb:6f	134.158.25.202	permanent	802.1x	subatech	00:0b:86:ae:c1:a0	1 hrs 28 mins	Associated

Below the table, there are navigation buttons: Status, Profile, Client Activity, Packet Capture, Locate, Debug, Disconnect, Blacklist, and Ping. The footer of the page includes "Aruba Networks™" and "E-mail Support".



Security Summary

WLAN Attack Summary			
	Last 5 Min	Last Hour	All
Denial of Service Attacks	<u>0</u>	<u>4</u>	<u>488</u>
Man in the Middle Attacks	<u>0</u>	<u>0</u>	<u>109</u>
Signature Pattern Matches	<u>0</u>	<u>0</u>	<u>24</u>
Policy Violations	<u>1</u>	<u>2</u>	<u>58</u>

Rogue AP Classification Summary			
	Last 5 Min	Last Hour	All
Rogue APs Detected	<u>0</u>	<u>0</u>	<u>0</u>
Rogue APs Disabled	<u>0</u>	<u>0</u>	<u>0</u>
Interfering APs Detected	<u>0</u>	<u>2</u>	<u>3</u>
Known Interfering APs	<u>0</u>	<u>3</u>	<u>4</u>

Client Classification Summary			
	Last 5 Min	Last Hour	All
Valid Clients	<u>0</u>	<u>0</u>	<u>0</u>
Interfering Clients	<u>0</u>	<u>4</u>	<u>4</u>
Disabled Rogue Clients	<u>0</u>	<u>0</u>	<u>0</u>

- Détection (IDS) des :
 - attaques DOS
 - man in the middle
 - outils de scan de réseau (netstumbler, air_jack, ...)
 - violation des règles de filtrage
 - bornes sauvages (action manu ou auto possible)
 - réseau adhoc (action manu ou auto possible)
- génération d' alertes SNMP ou syslog

Admin: localisation d'un portable ou d'une borne WIFI pirate (par triangulation)

Locate > Batiment H - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://134.158.30.100:4343/screens/wmsi/plan.html?locator=true&campus-id=1&building-id=1&mac=00:40:96:a6:cb:6f

Linux Divers Sites FTP Service Info Moteurs de recherche Annuaires EMN SUBATECH IN2P3 Start2 Serveurs RT pointeuse Nagios

Laboratoire SUBATECH eTemp@tion © 2002 Horoquartz G.T. Locate > Batiment H Login

Keep data for 3 minutes Send NULL Packets Refresh Heat Map

Target Devices

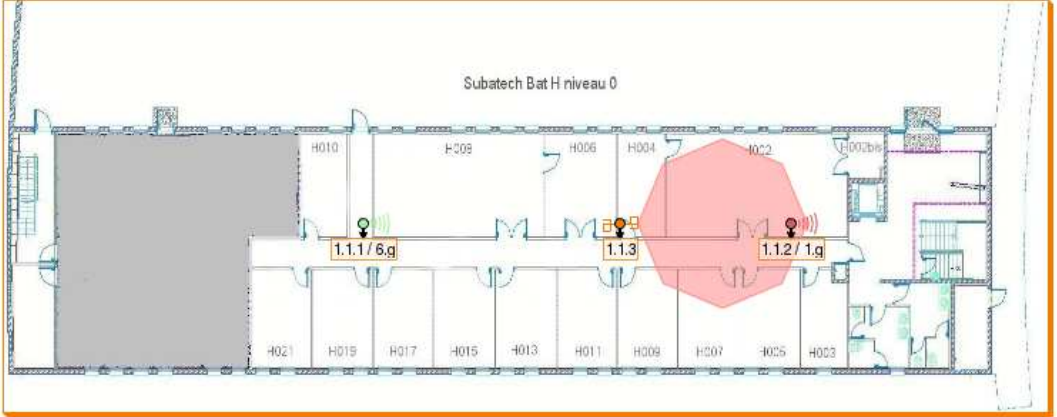
DEV	Manufacturer	MAC	Coord.	Type	CH	User	SSID	BSSID	Active
STA	Cisco Systems, Inc.	00:40:96:a6:cb:6f	N/A	VALID	g 1	lecorre	subatech	00:0b:86:ae:c1:a0	Active

Listening Air Monitors / Access Points

Loc.	RSSI	Dist.	X	Y	Flr	IP	AP Type	Radio	Type	BSSID	Count	Duration
1.1.3	15	19	36	10	1	134.158.30.113	61	802.11a/g	Air Monitor	00:0b:86:ac:5b:10	26	190 sec
1.1.2	13	22	46	10	1	134.158.30.112	61	802.11g	Access Point	00:0b:86:ae:c1:a0	249	165 sec

Add Device Choose Devices... Remove Device

Floor 1: H0



Subatech Bat H niveau 0

- Remote AP (testé mais pas divulgué)
- VPN
- VoIP
- Remédiation (Zone Labs)
- QoS
- 802.11i

- double interrogation Radius impossible (pour l'instant ?). C'est à dire que pour le SSID Subatech, nous avons:
 - vérification login/passwd du domaine sur Radius → ntlm_auth → Contrôleur de domaine Active Directory
 - vérification de l'adresse MAC dans la base interne du switch.

Alors qu'avec la borne Cisco Aironet 1100 utilisée pour nos tests préliminaires, les adresses MAC étaient stockées également sur Radius.

- le switch ne peut pas envoyer des mails d'alerte directement

CONCLUSION

- ➔ Réclamé fort mais peu utilisé par les permanents
- ➔ Facilité d'accueil des visiteurs (délégation possible pour le portail)
- ➔ Diminution du travail de câblage
- ➔ Bonne prestation de la part de Teldata

Réf: <http://www.teldata.fr>