# 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)

Aruba800-4 ( 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

Modèle AP61 (802.11b/g)

Modèle AP60 (802.11a)

Modèle AP70 (802.11a/b/g)

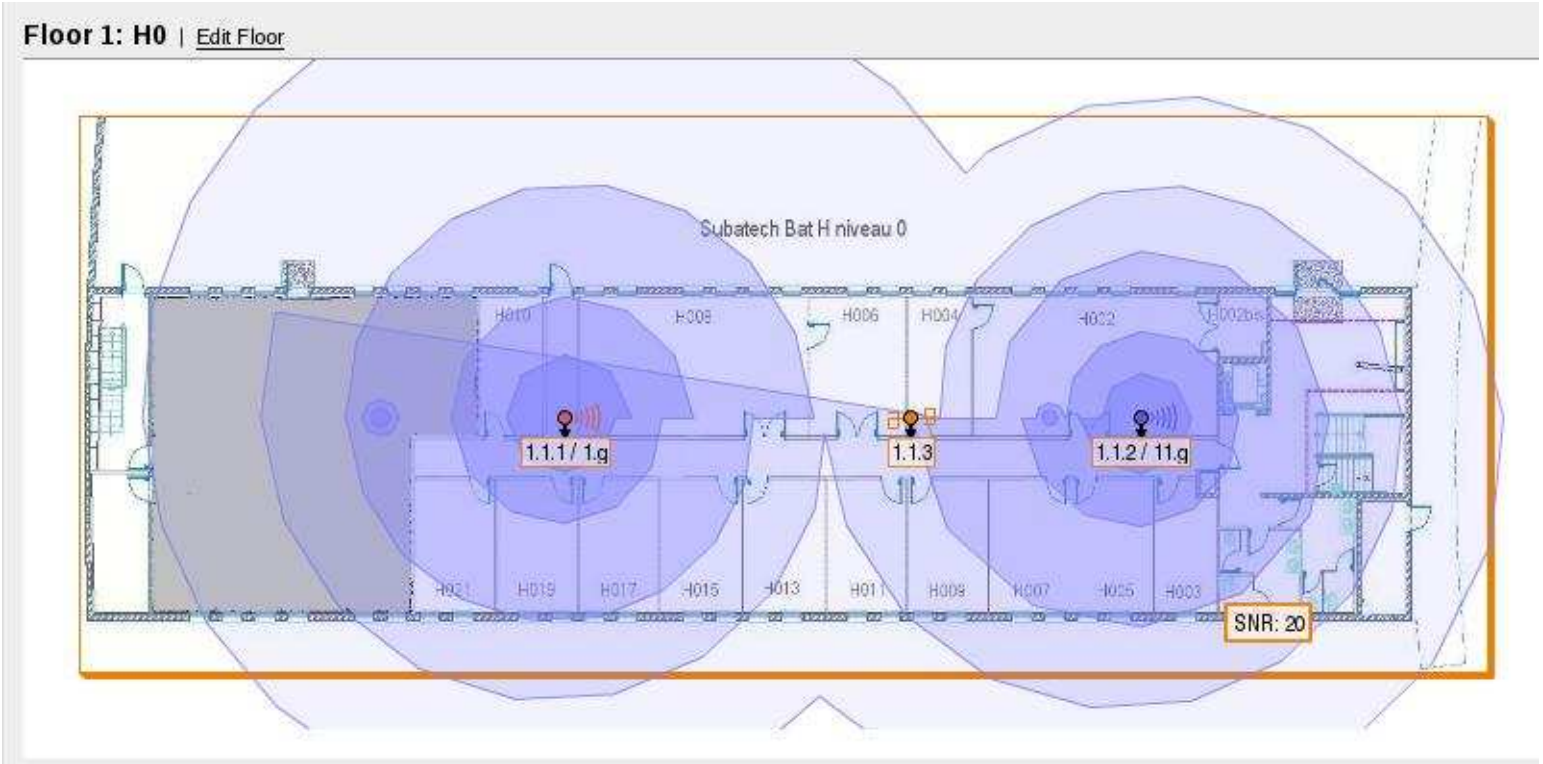
Modèle AP80 (802.11a/b/g extérieur)

# Caractéristiques des bornes WiFi

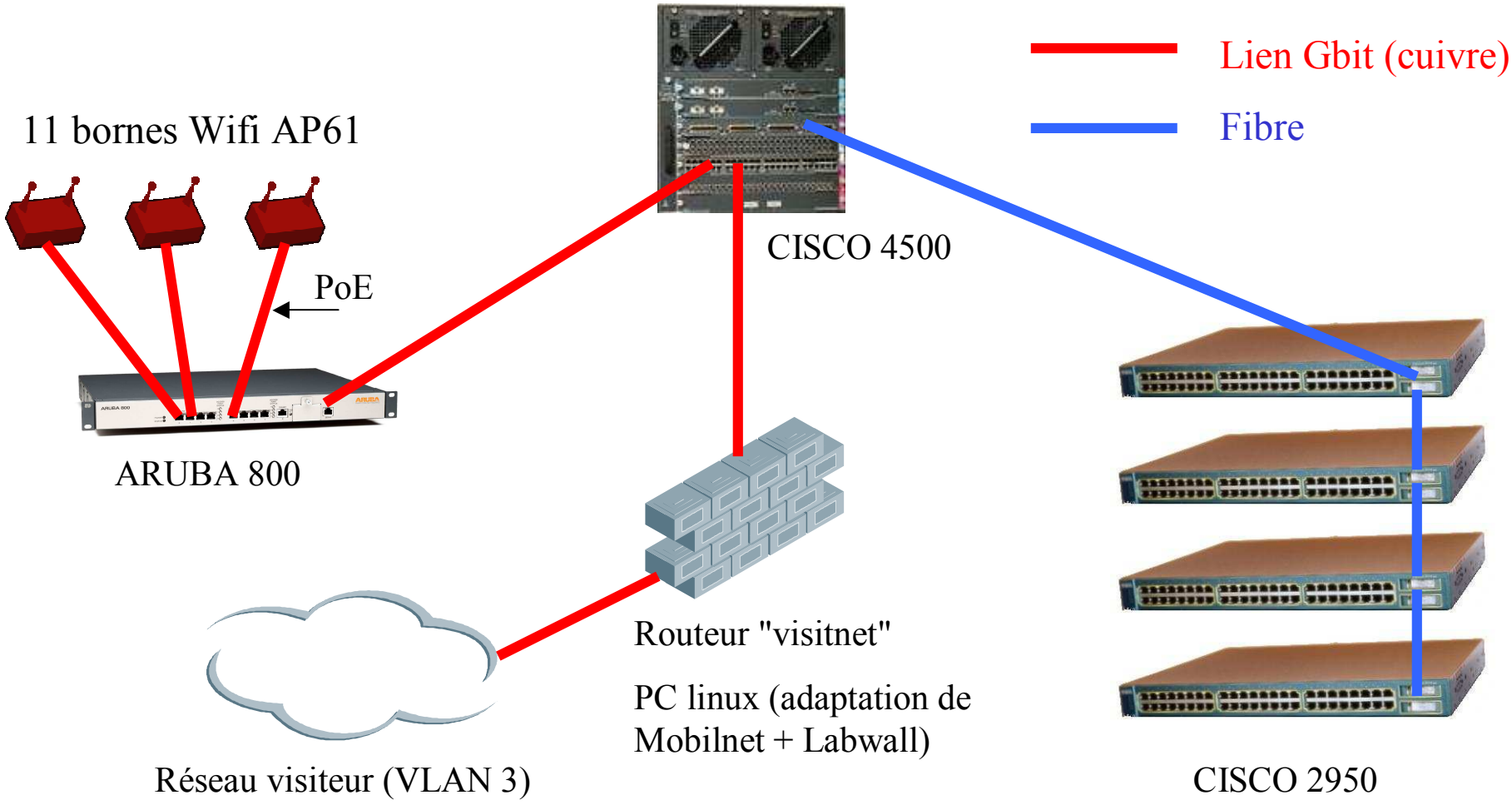
- auto-alimentées (PoE) ⟶ facilité d'installation
- auto-négociation des puissances d'émission entre les bornes
- auto-négociation des canaux d'émission entre les bornes
- partage de charge dynamique entre les bornes
- aucun paramètre stocké dans les bornes (en cas de vol)
- roaming avec conservation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



# SSID Subatech (portable des permanents)

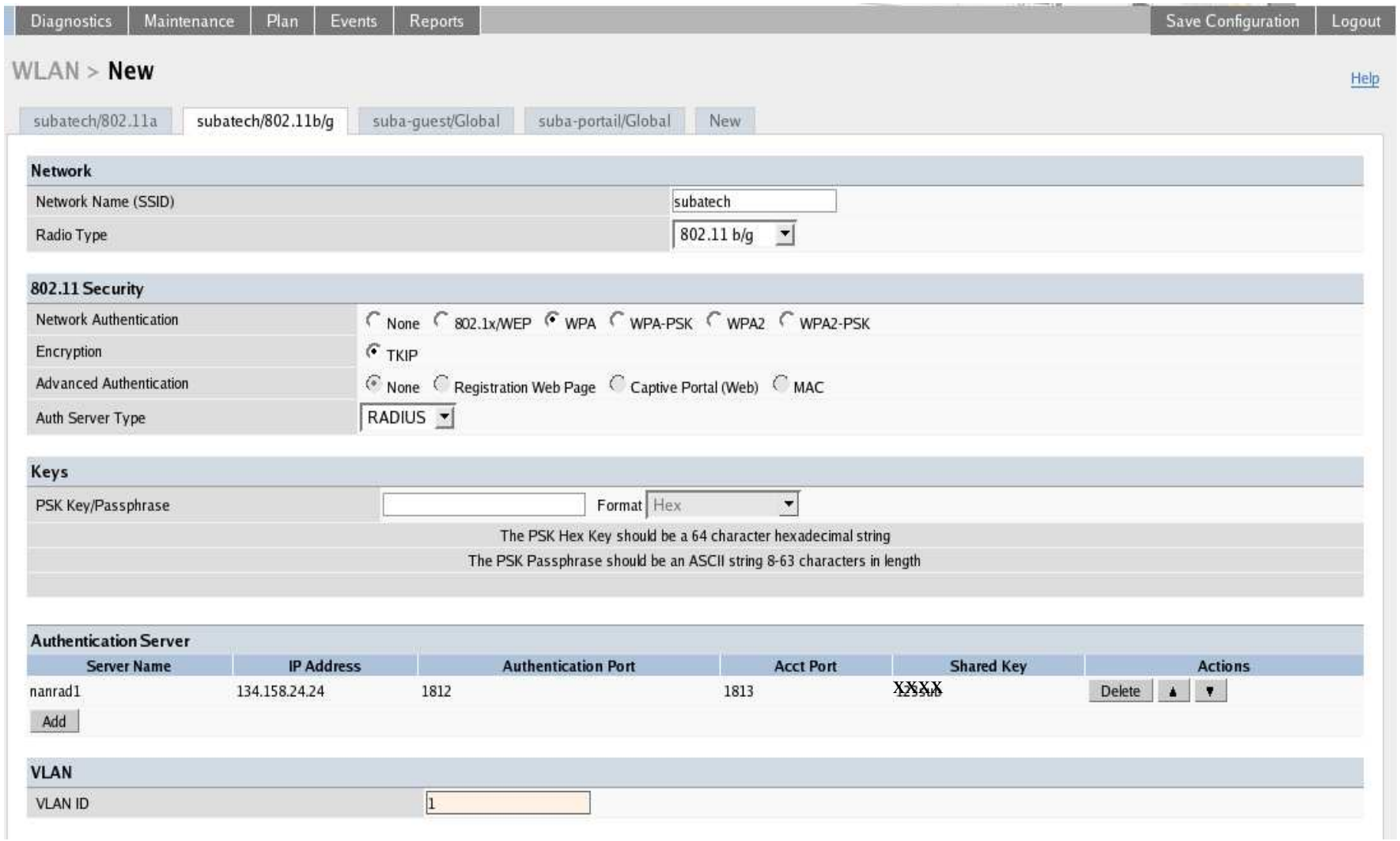
Pré-requis:

- 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

# Configuration du SSID Subatech



# SSID Suba-guest (portable des visiteurs)

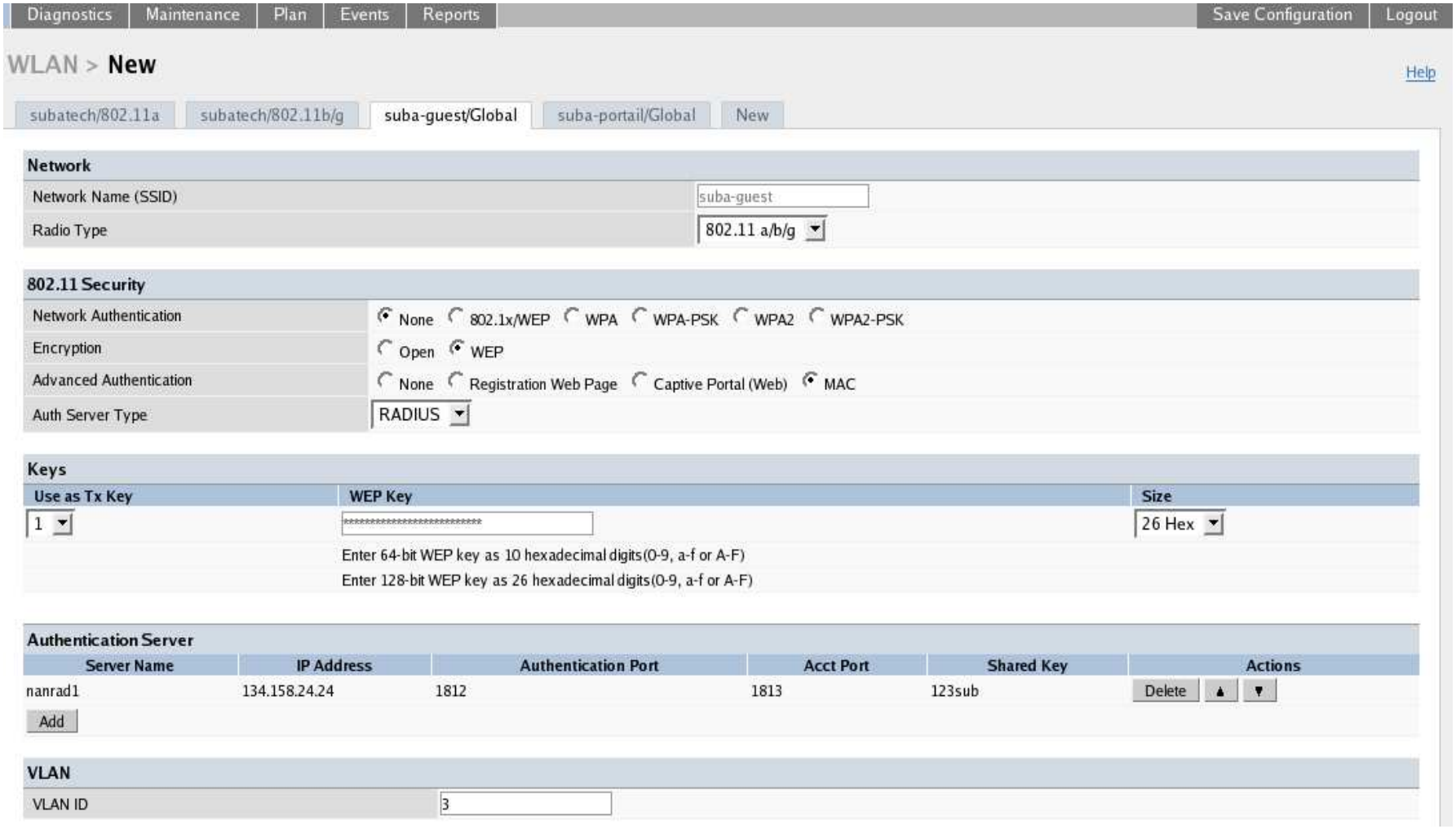
Pré-requis:

- 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, …)

# Configuration du SSID Suba-guest



# SSID Suba-portail

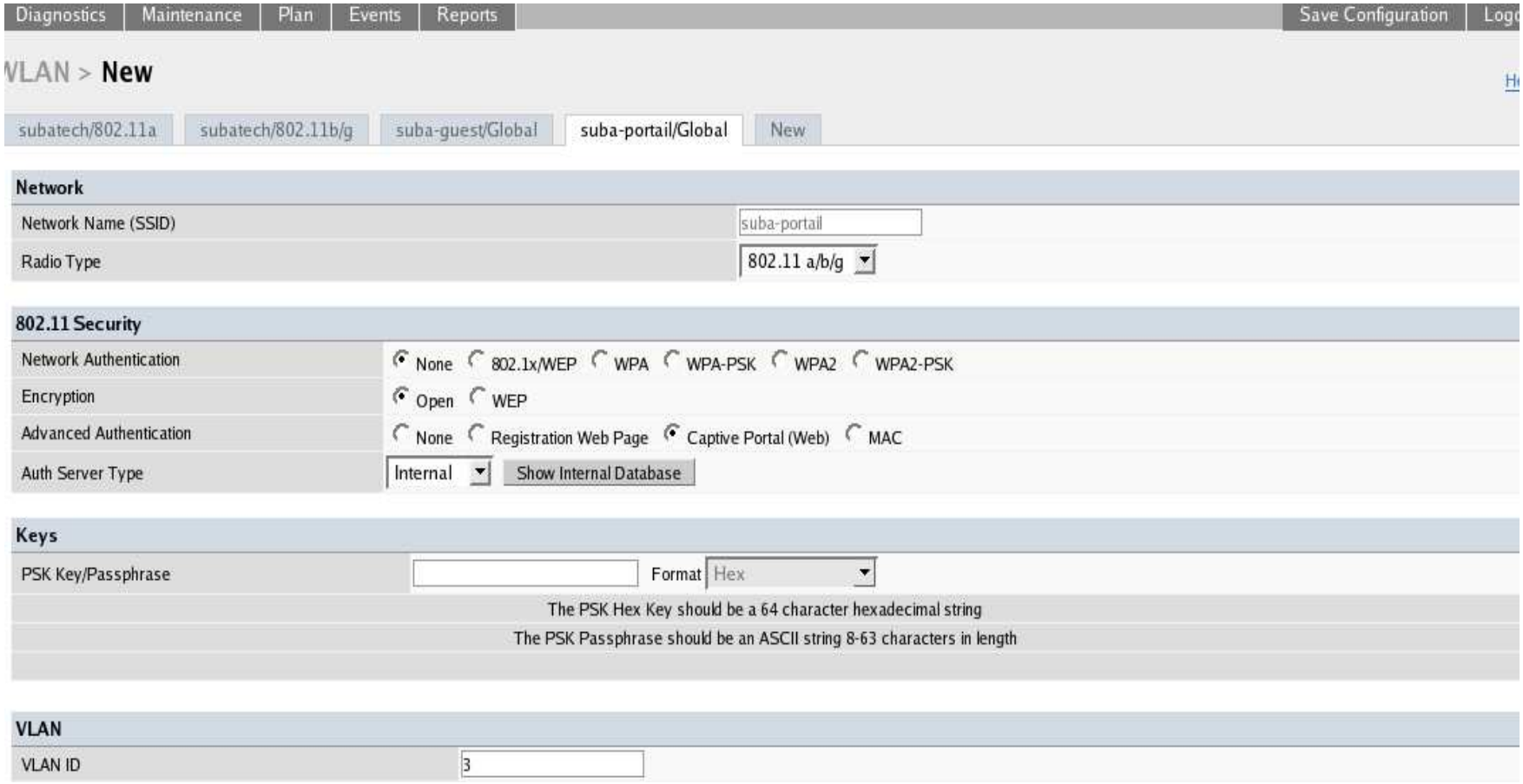
Pré-requis:

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

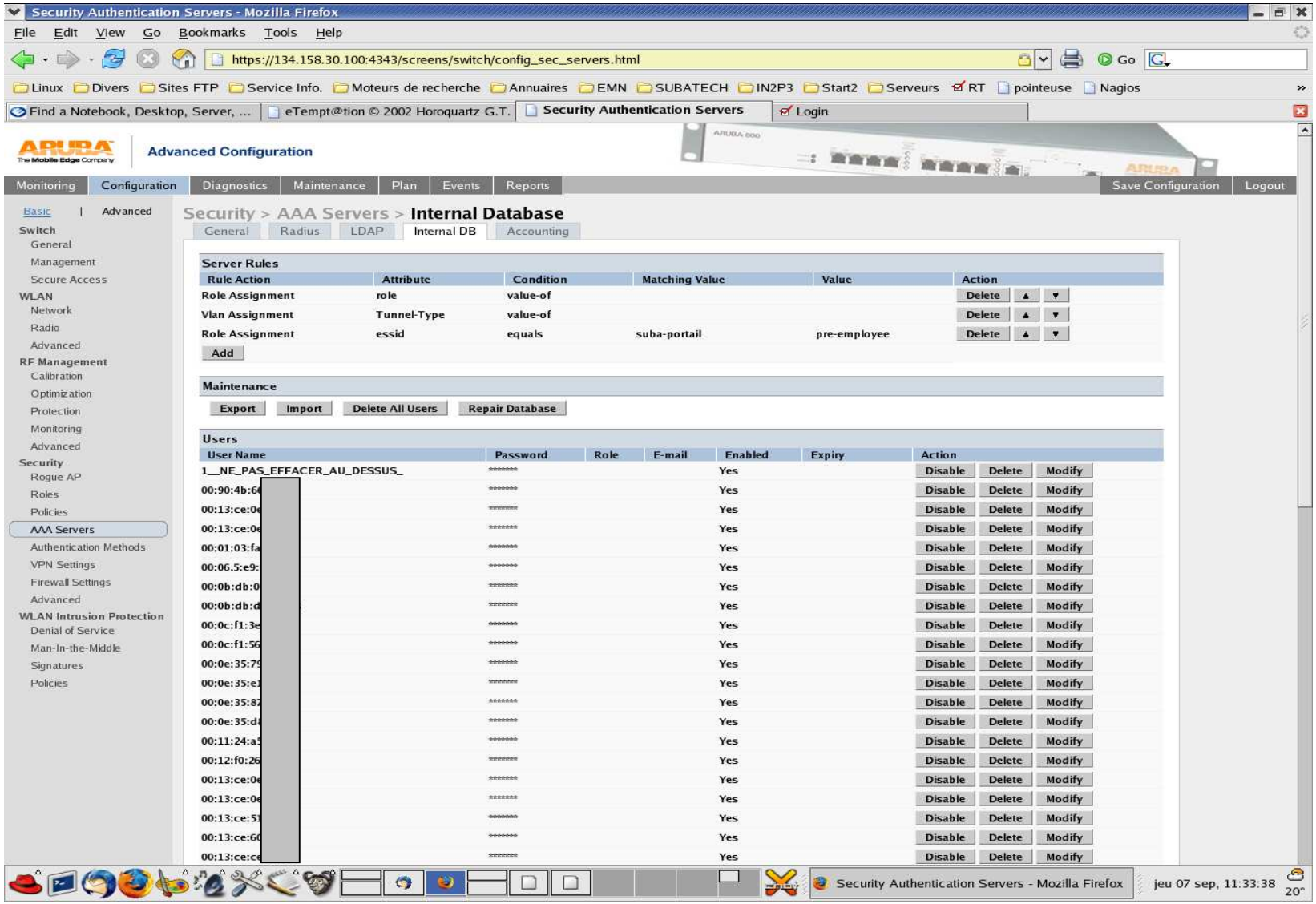
Notre choix:

- 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

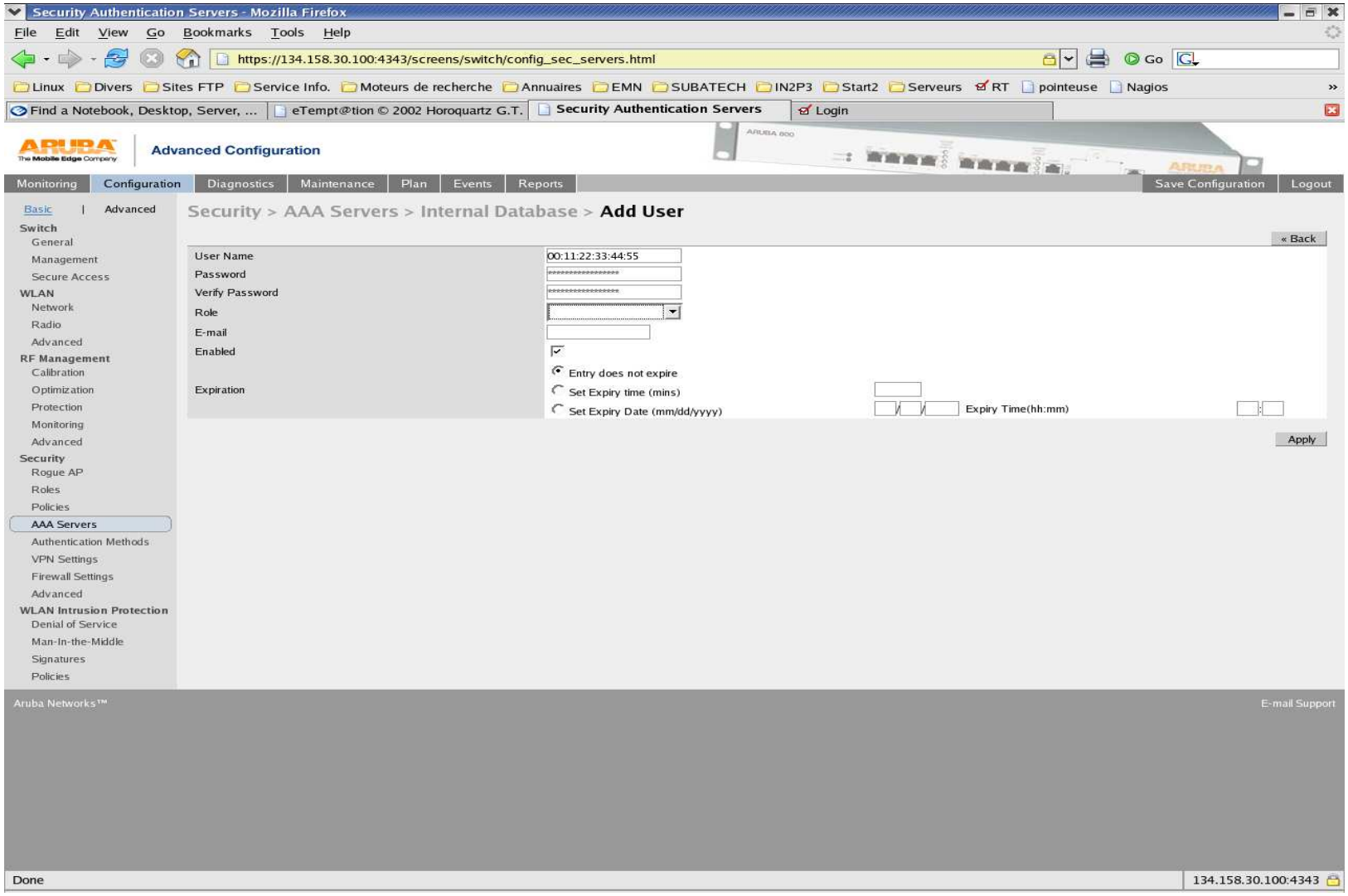
# Configuration du SSID Suba-portail



# Admin: enregistrement d'un portable sur le réseau permanent



# Admin: enregistrement d'un portable sur le réseau permanent



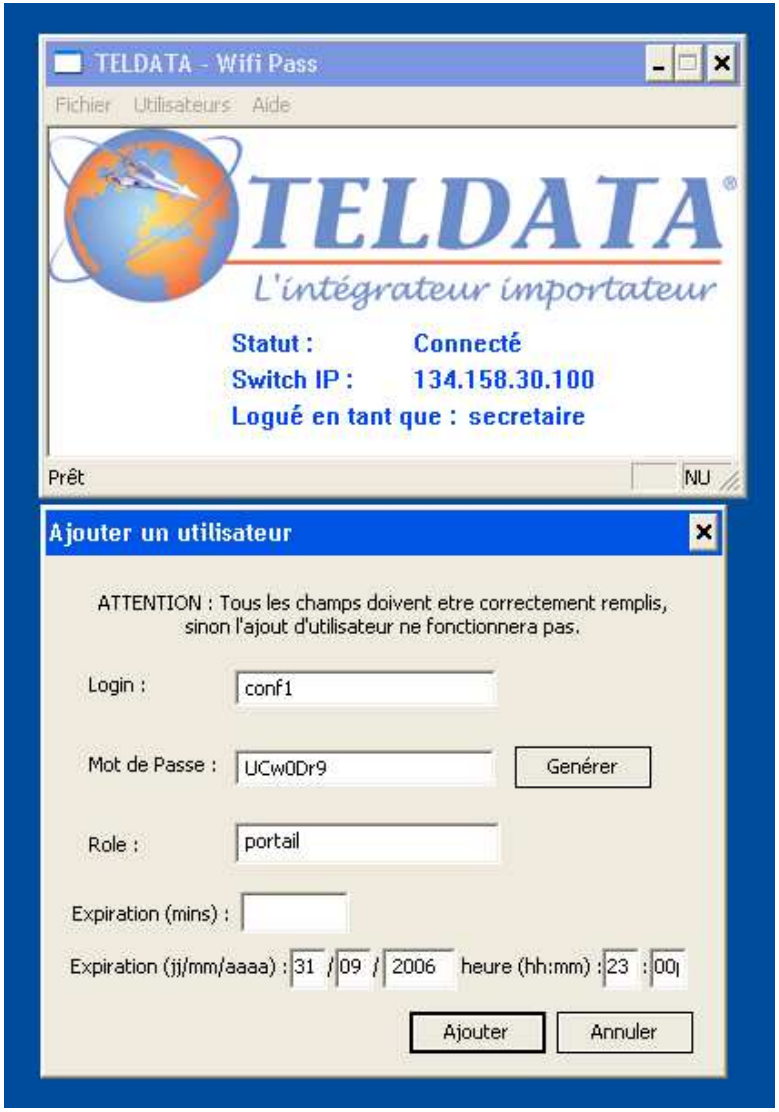
# Admin: enregistrement d'un portable sur le réseau visiteur

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

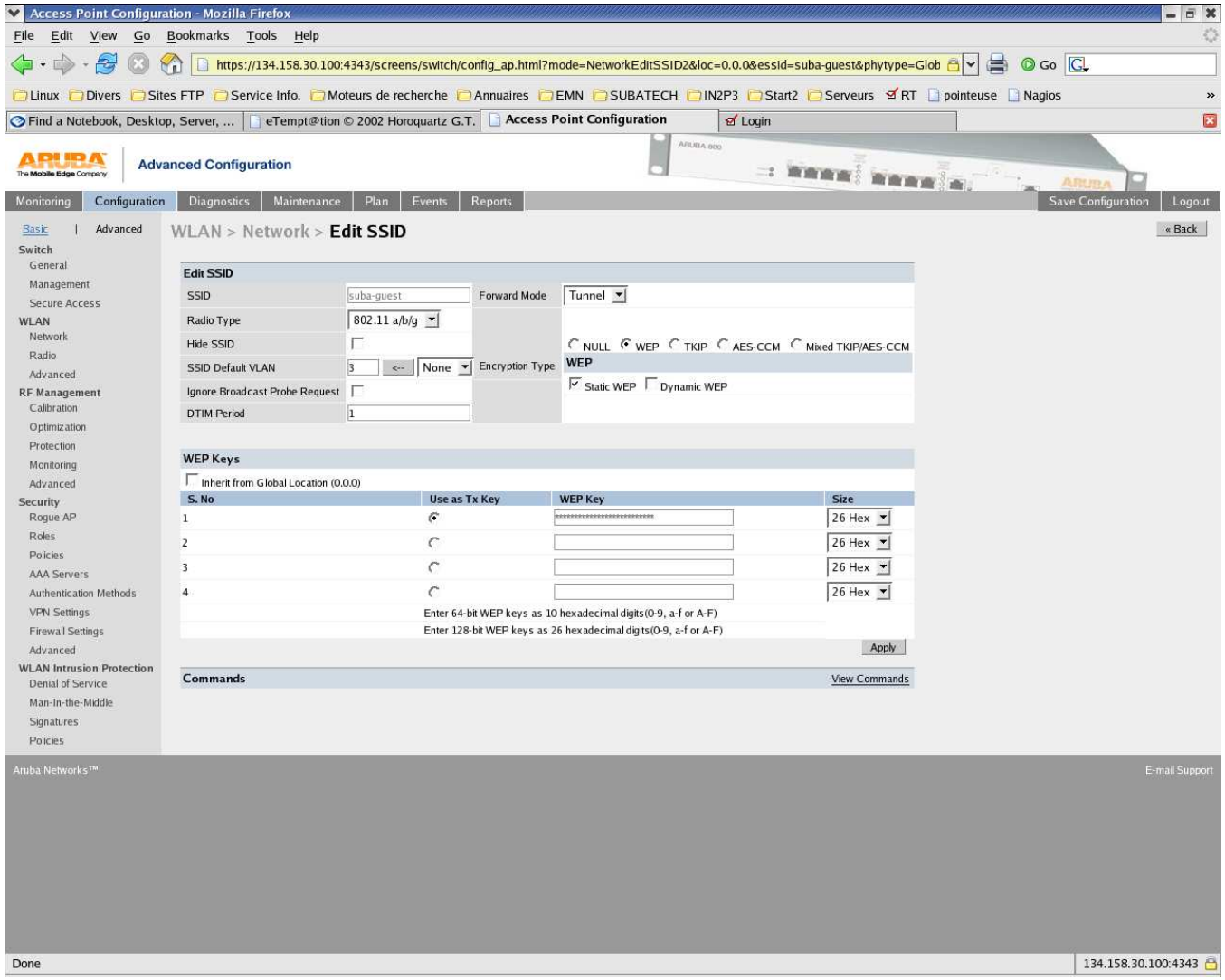
```
123456789abc auth-type := local, user-password == "123456789abc"
004096a6xxxx auth-type := local, user-password == "004096a6xxxx"
0014a557xxxx auth-type := local, user-password == "0014a557xxxx"
0013d467xxxx auth-type := local, user-password == "0013d467xxxx"
000b5d23xxxx auth-type := local, user-password == "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

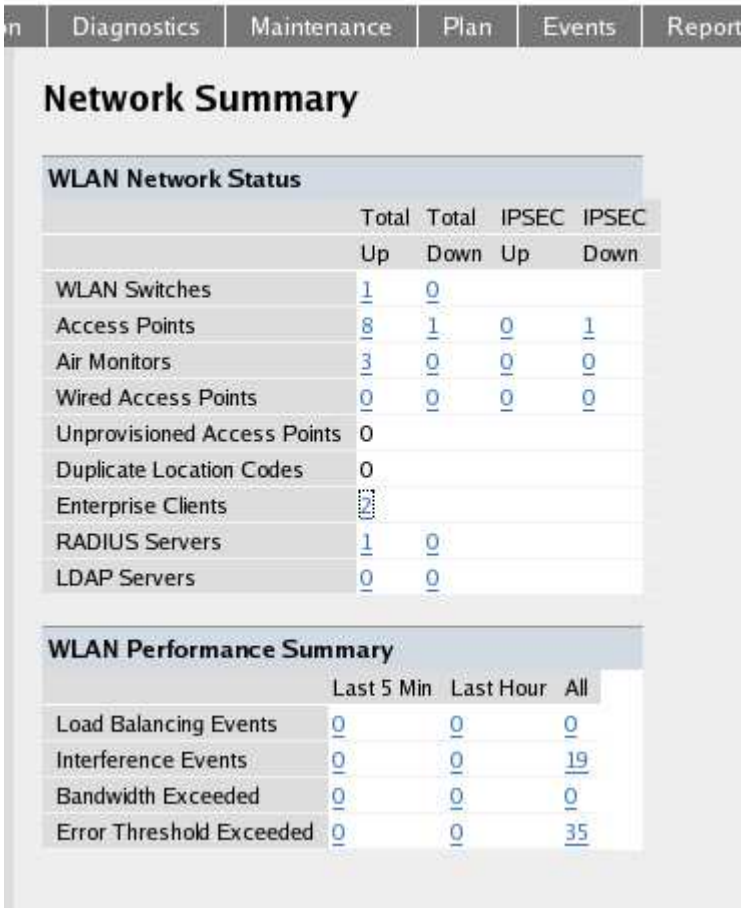
# Admin: création d'un accès au portail avec l'application WifiPass

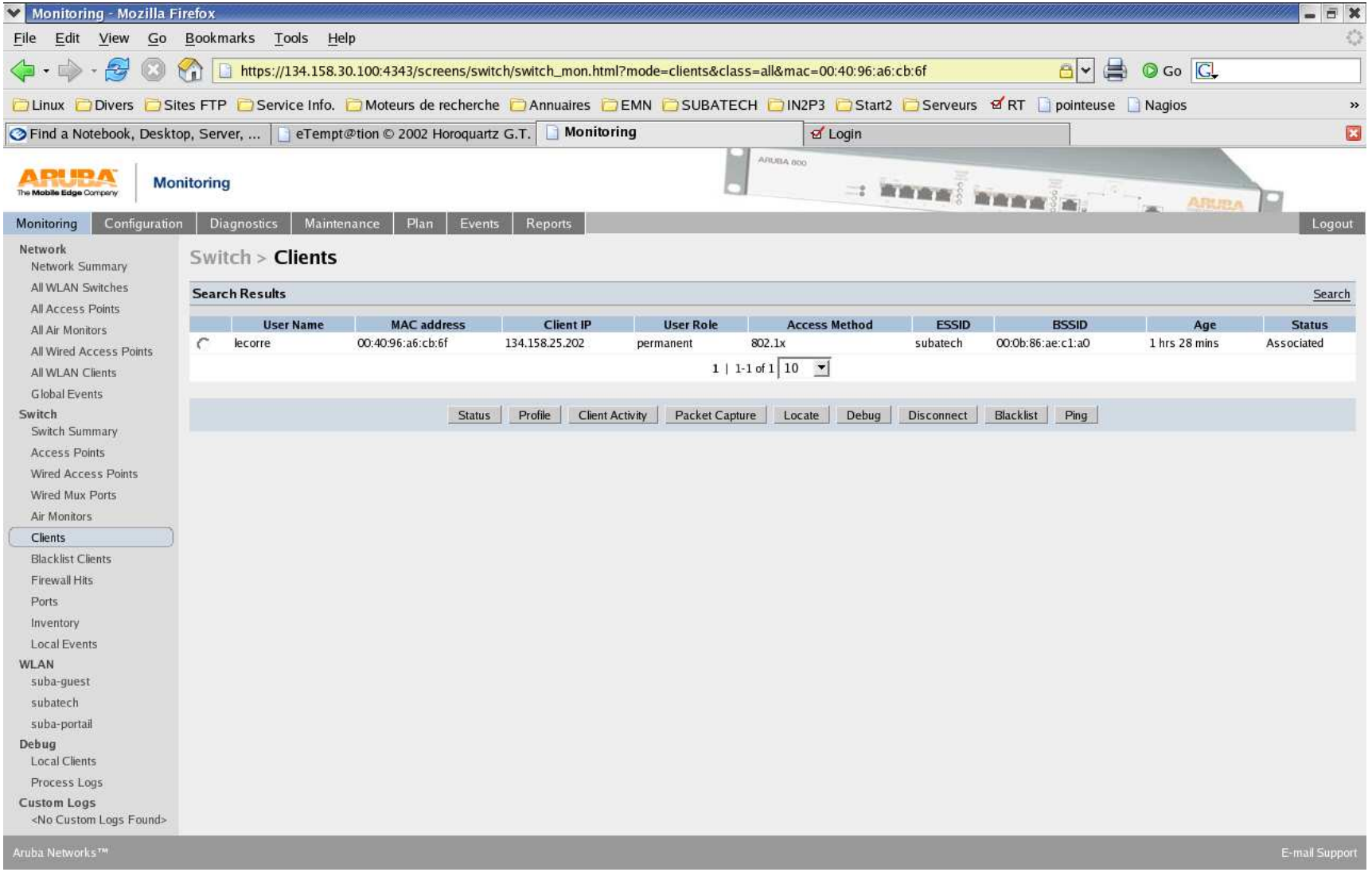
# Admin: renouvellement de la clé Wep 128 Bits pour Suba-guest



# Admin: suivi des connexions



# Admin: suivi des connexions



# Admin: statistiques de connexions aux SSID

# Admin: sécurité du réseau Wifi

## Security Summary

### WLAN Attack Summary

| | Last 5 Min | Last Hour | All |
|---|---|---|---|
| Denial of Service Attacks | 0 | 4 | 488 |
| Man in the Middle Attacks | 0 | 0 | 109 |
| Signature Pattern Matches | 0 | 0 | 24 |
| Policy Violations | 1 | 2 | 58 |

### Rogue AP Classification Summary

| | Last 5 Min | Last Hour | All |
|---|---|---|---|
| Rogue APs Detected | 0 | 0 | 0 |
| Rogue APs Disabled | 0 | 0 | 0 |
| Interfering APs Detected | 0 | 2 | 3 |
| Known Interfering APs | 0 | 3 | 4 |

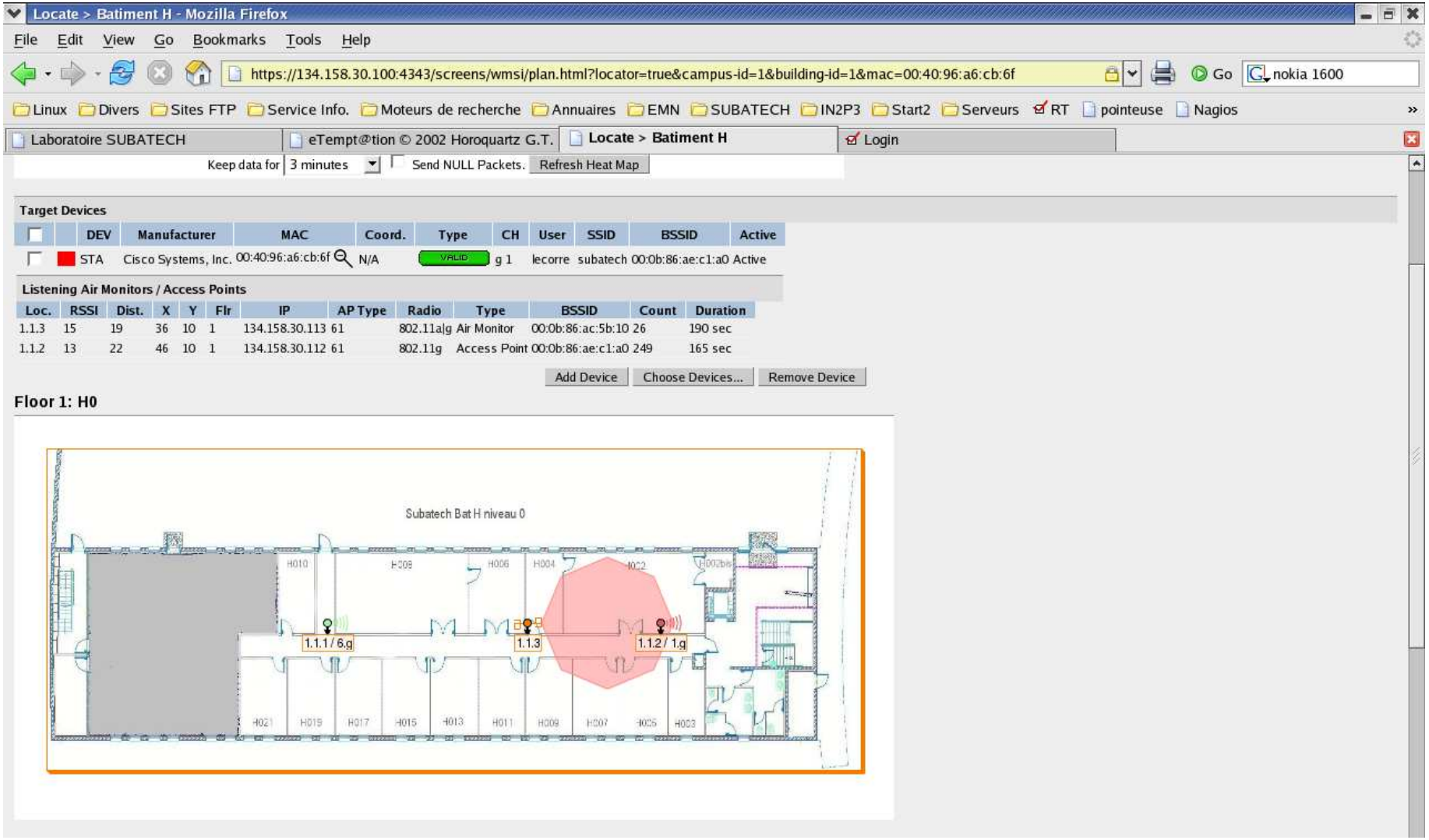
### Client Classification Summary

| | Last 5 Min | Last Hour | All |
|---|---|---|---|
| Valid Clients | 0 | 0 | 0 |
| Interfering Clients | 0 | 4 | 4 |
| Disabled Rogue Clients | 0 | 0 | 0 |

- 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)



# Possibilités et évolutions

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

# Limitations du produit

• 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