Projet Nomadisme et réseaux sans fil INPT

Retour d'expérience

RESIST
Avril 2005

Equipe projet:

(Frédérique.COUDRET, Rémi.GOUDIN, Brigitte.SOR) @enseeiht.fr

Objectifs du projet

- Proposer une solution au problème du nomadisme en prenant en compte 2 aspects:
  - réseaux sans fils
  - accès distants (ADSL, câble, UMTS, hot-spot, autre campus, …)
- Valider le modèle proposé par le déploiement d ’un pilote restreint à l’N7 puis généralisation pour tous les sites de l’INPT

Objectifs : services aux utilisateurs

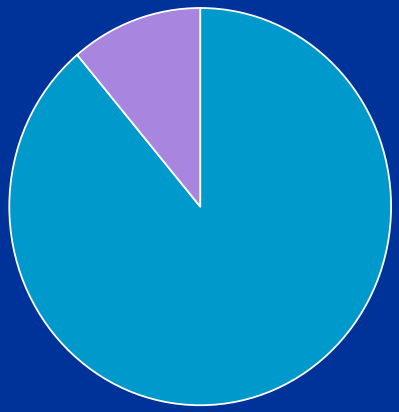
CCF (1/2)

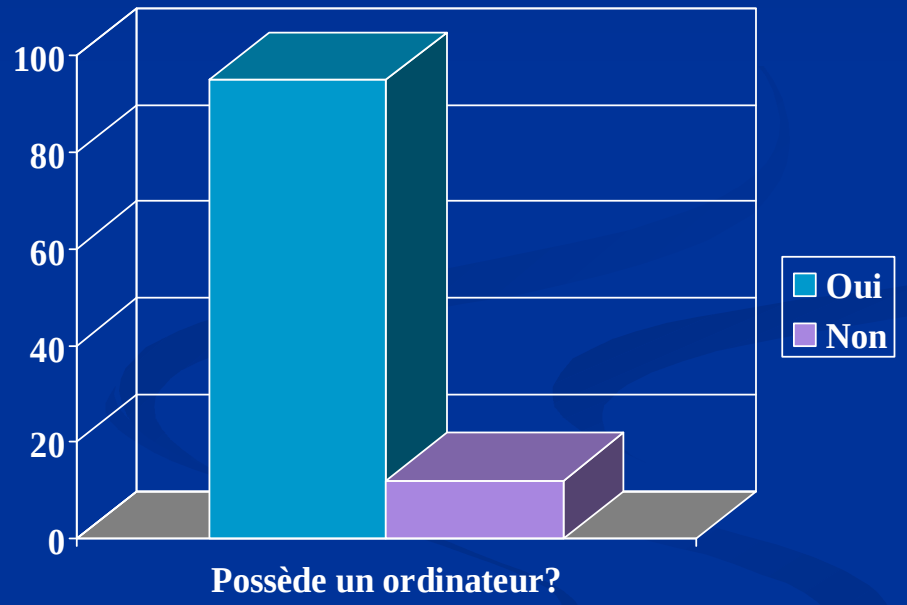
- Cahier des Charges Fonctionnel en bref:
  - Authentification des utilisateurs
  - Cryptage de l'authentification et des échanges de données (VPN)
  - Pas ou peu de contraintes pour les postes clients
  - Facilité d'administration et de maintenance
  - Possibilité de gérer des politiques de sécurité en fonction de communautés d'utilisateurs, de localisation géographique ou plage horaire.

CCF (2/2)

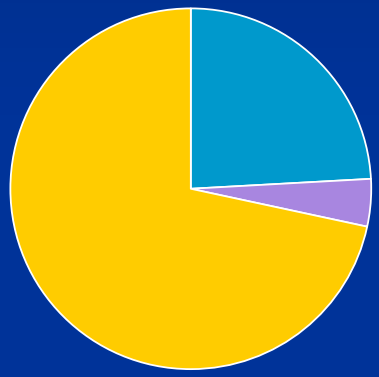
- CCF en bref (suite):
  - Evolutivité de la solution
  - Intégration dans l'architecture actuelle INP et à moyen terme régionale via Remip2000 (projet UNR)
  - Prise en compte des accès sans fils et accès distants
  - Surveillance et détection des anomalies radio

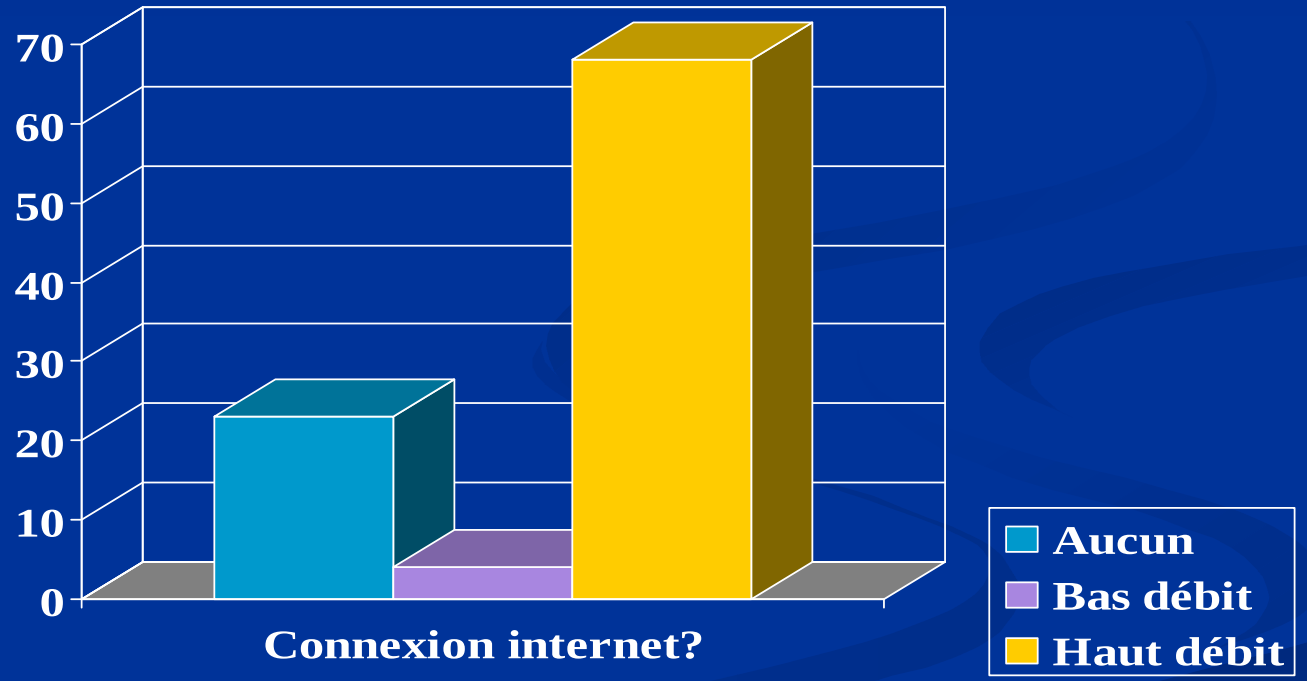
Résultats enquête étudiants (07/04)
Possède un ordinateur?



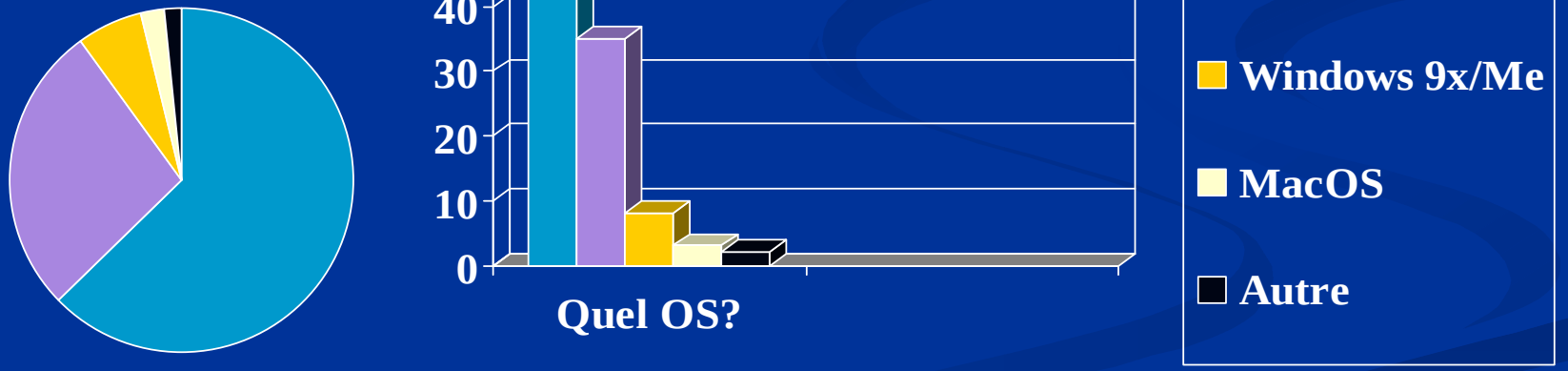


Résultats enquête étudiants
Connexion internet?





Premiers résultats enquête étudiants
Quel système d'exploitation?



Les objectifs du projet

- Gestion similaire des accès sans-fils et des accès distants
- Sécurité
- Simplicité pour l'utilisateur final
- Facilité d'administration de la solution
- Intégration dans l'architecture existante
- Evolutivité

Types d'utilisations

- Portable et sans fil sur le site
  - Invité avec son portable (internet)
  - Salles de TP mobile
  - Étudiant avec son portable
  - Personnel avec son portable
- Accès distant :
  - Étudiant
  - Personnel

Etat de l'art - Accès sans-fil

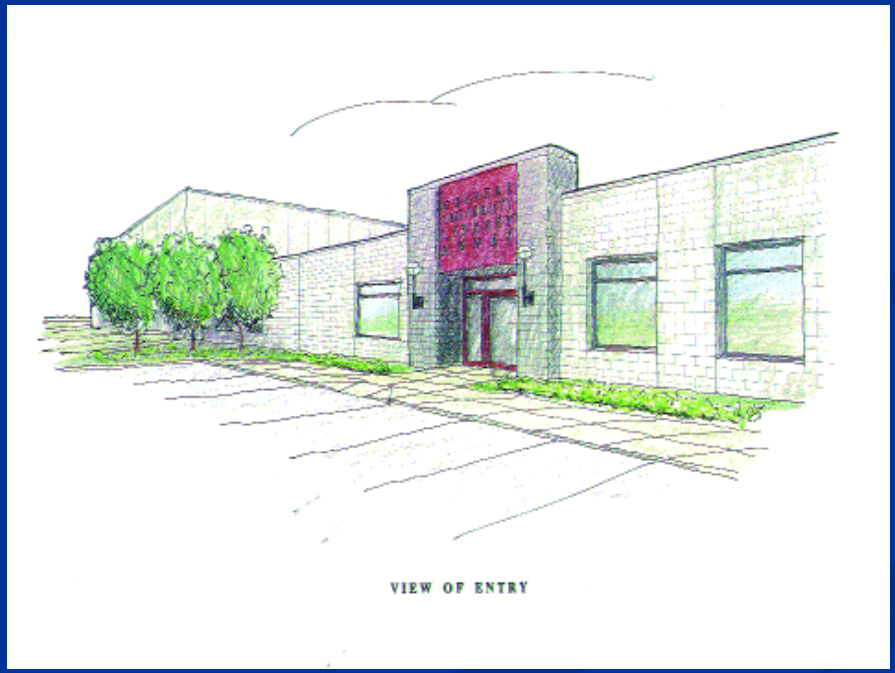
- *Sécurisation au niveau 2*
- *Sécurisation au niveau 3 et plus*

Etat de l'art - Accès sans-fil

Au niveau 2

- 802.1X
- WPA
- 802.11i (WPA 2)

Aucun accès au réseau sans authentification



Etat de l'art - Accès sans-fil

Au niveau 3 +

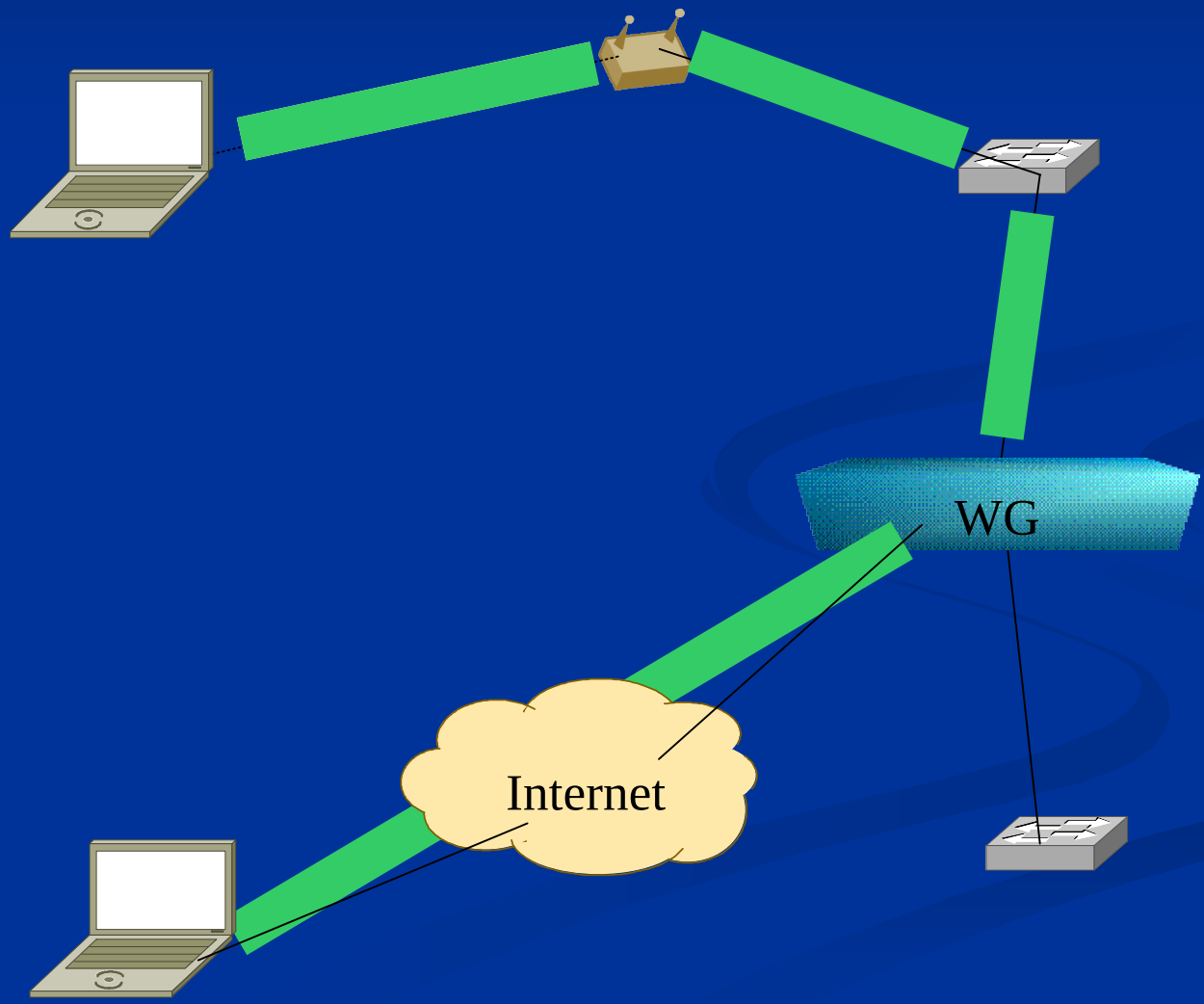
- firewall dynamique
- VPNs

Accès «libre» à un réseau isolé avant authentification

Etat de l'art - Accès distants

- VPNs basés sur IPSec
  (IPSec, L2TP/IPSec, Xauth/IPSec)
- VPNs basés sur SSL

Problématique



Solutions testées

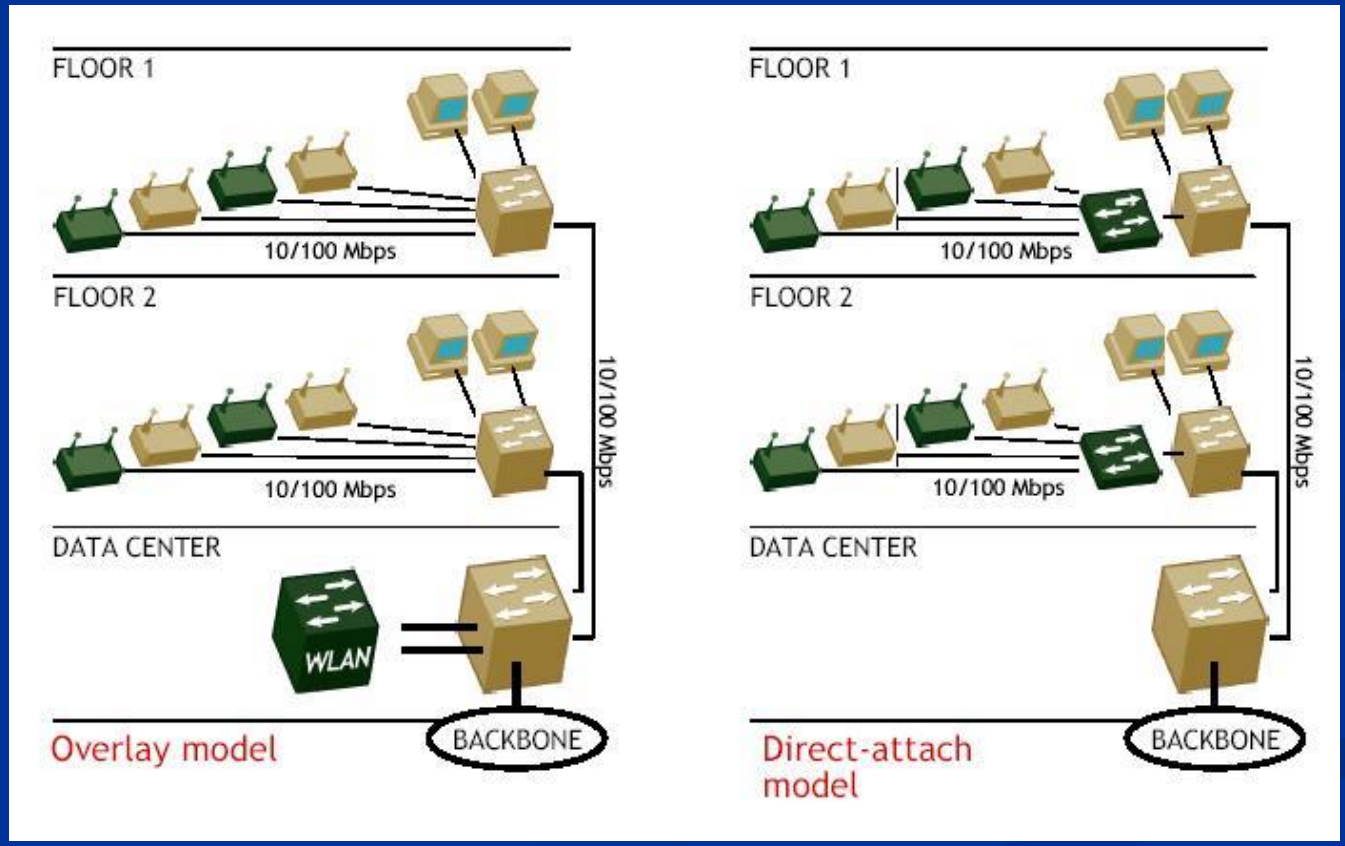
- 802.1X + FreeRadius
  (www.freeradius.org)
- Bluesocket
  (www.bluesocket.com)
- Cisco
  (www.cisco.com)
- Aruba
  (www.arubanetworks.com)

Aruba

- Solution complète: switchs + APs
- Authentification web
- Filtrage dynamique
- VPNs
- Gestion radio
- Sécurité avancée
- ...

Aruba

Type d'architecture



Solution Aruba

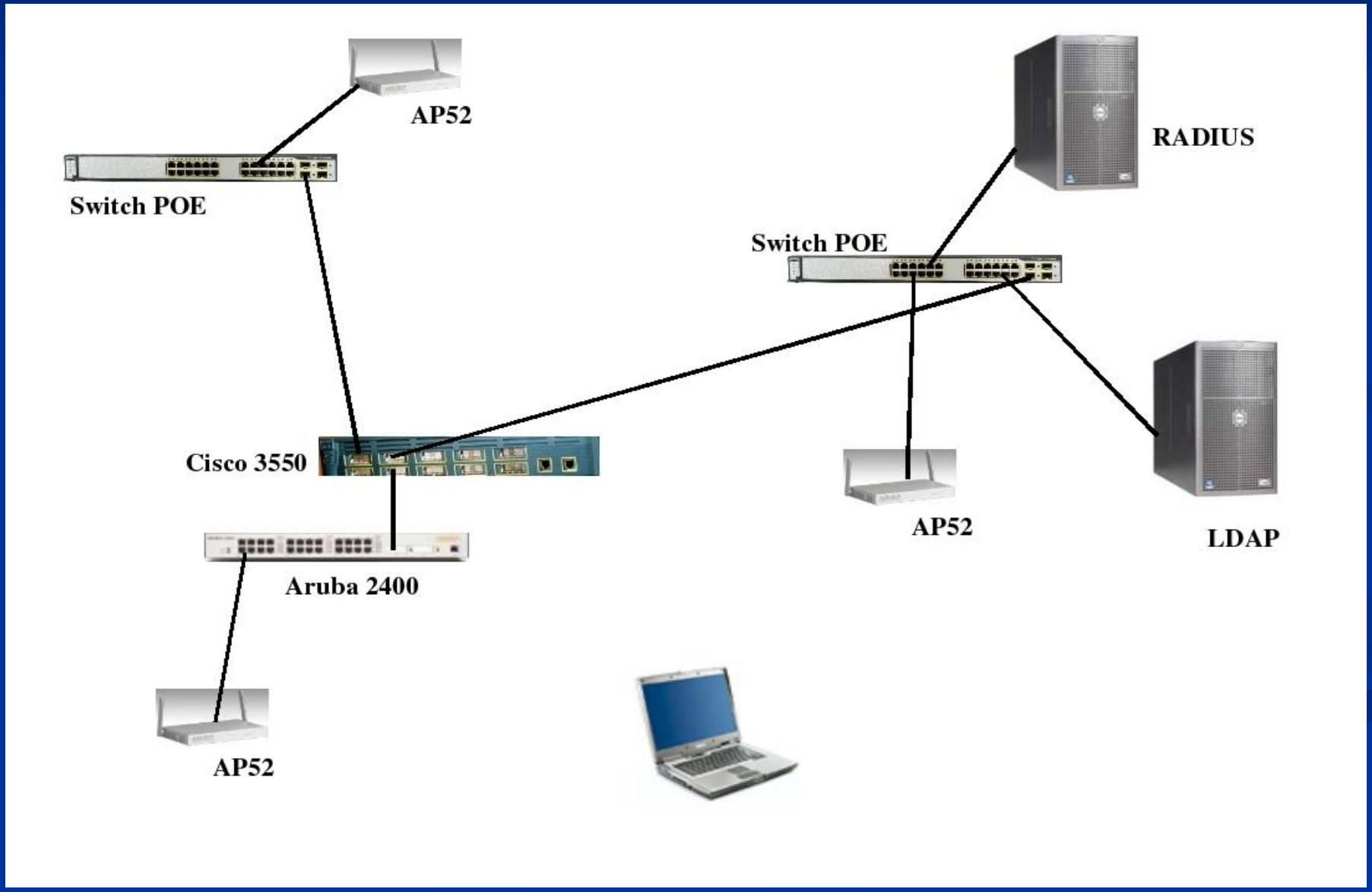
Caractéristiques techniques du switch 2400:

- *jusqu'à 48 bornes Aruba supportées*
- *capacité maxi: 2 Gbps*
- *400 Mbps de bande passante en crypté (3DES)*
- *24 ports 10/100 Mbps POE + 2 uplinks gigabit*
- *jusqu'à 256 sessions VPN simultanées*

Architecture physique

- *Un switch Aruba 2400 connecté par un lien gigabit sur le coeur de réseau*
- *24 bornes AP52 (802.11a|b|g), dont 5 dédiées à la surveillance radio, réparties sur 3 batiments*
- *Utilisation de la technologie 802.3af (POE) pour l'alimentation électrique des bornes*

Architecture physique

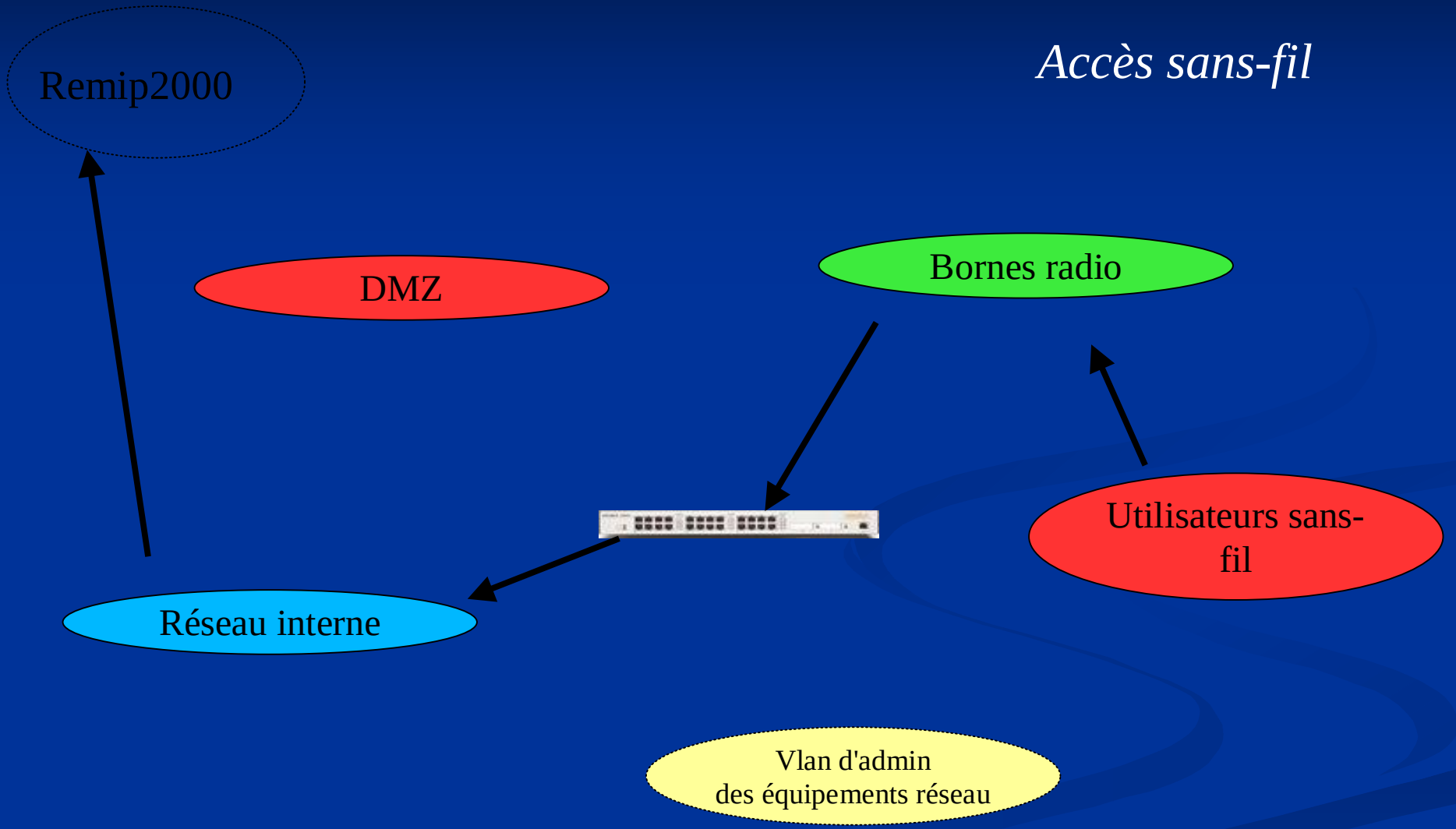


Architecture logique

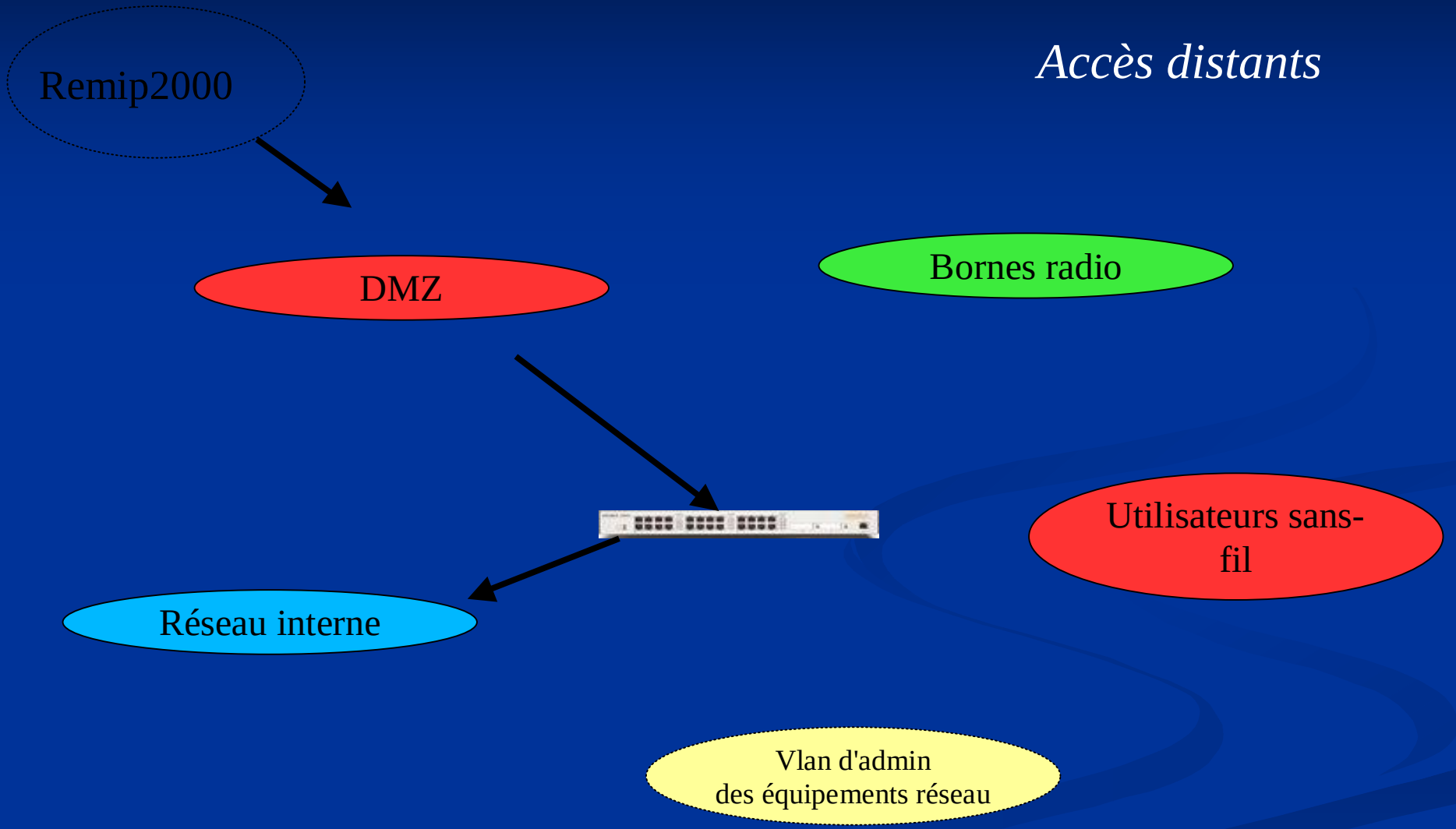
Utilisation des VLAN:

- *un vlan dédié pour les bornes radio*
- *un (ou plusieurs) vlans pour les utilisateurs sans-fil*
- *seul le switch Aruba (multi-vlans) permet l'interconnexion entre les utilisateurs, sans-fil ou distants, et le réseau local*

Architecture logique



Architecture logique



Architecture logique

Remip2000

Administration

DMZ

Bornes radio

Utilisateurs sans-fil

Réseau interne

Vlan d'admin
des équipements réseau

Sécurité

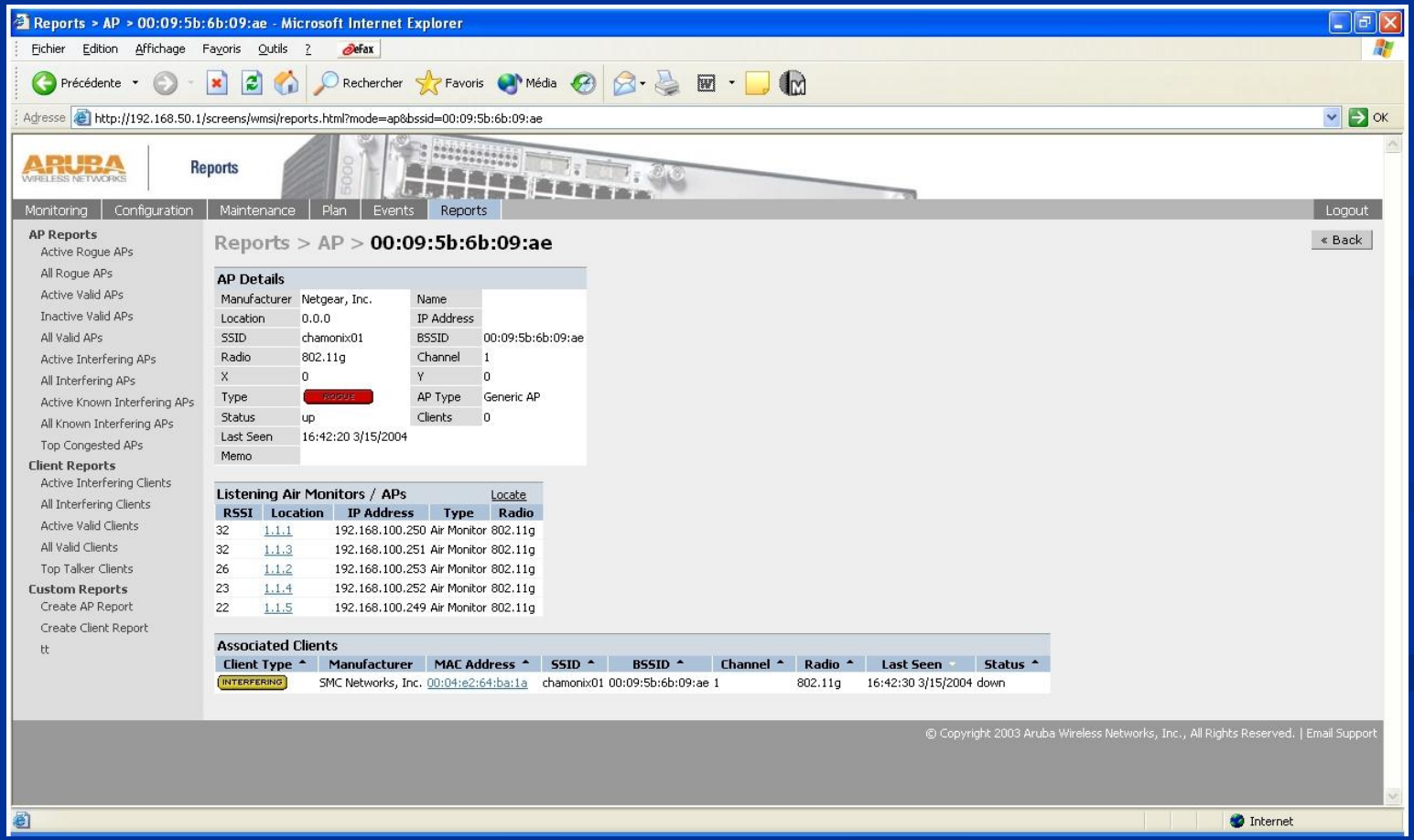
- Définition de 3 profils utilisateurs (étudiant, personnel, visiteur) et de leurs droits d'accès associés
- Authentification obligatoire sur LDAP ou RADIUS+LDAP
- Plusieurs méthodes d'authentification et de cryptage des communications proposées (portail captif +WEP 128, VPN, WPA)
- Filtrage dynamique + NAT
- Segmentation réseau par VLAN

Sécurité

- Plusieurs réseaux radio (SSID non diffusés)
- Désactivation radio en dehors des heures d'ouverture
- Bornes dédiées à la surveillance (détection d'anomalies radio, d'intrusions, de points d'accès «rogues»...)
- Protection contre certains types d'attaques radio (DoS...)

Administration de la solution

Interface web d'administration :



Plan > Batiment B > Planning - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://chaussette-2/screens/wmsi/plan.html?campus-id=1&building-id=2

Firefox Help Firefox Support Plug-in FAQ

Building Specification
- Dimension
- Modeling: AP
- Modeling: AM

Planning
- Floors
  - Floor 1
  - Floor 2
  - Floor 3
  - Floor 4
- AP Plan
- AM Plan

Deployed
- Floors
  - Floor 1
  - Floor 2
  - Floor 3
  - Floor 4

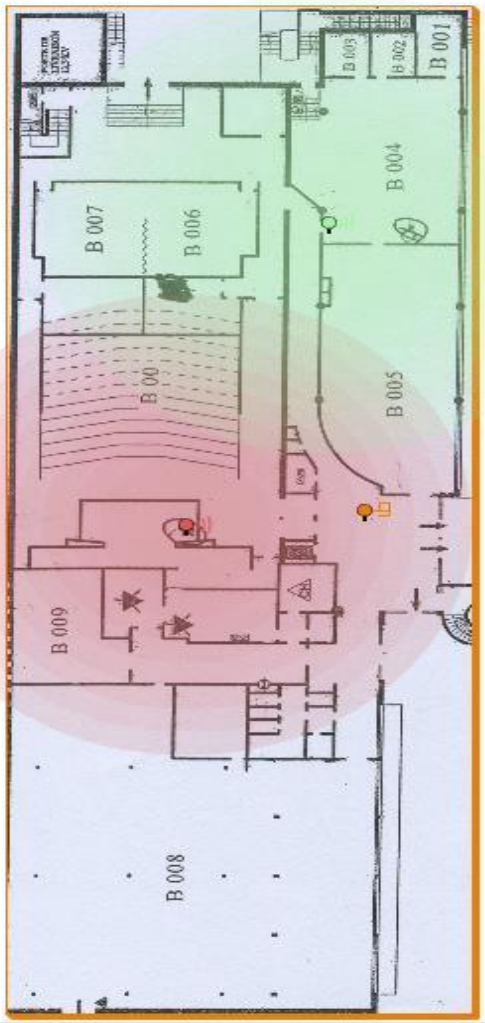
Plan > Batiment B > Planning

Save | Add New Floor | AP Planning »

Control

Zoom 900 900 % | Approx. Coverage AP - 802.11b|g | Coverage Rate 48 Mbps

Floor 1: Rdc | Edit Floor



Read chaussette-2

Administration de la solution

- Administration centralisée des bornes depuis le switch
- Suivi en temps réel des connexions et du trafic
- Utilisation de l'accounting Radius
- Configuration du switch par Web ou CLI (un seul fichier de conf)

Retour d'expérience sur la période de tests

- *Tests ouverts à tous les utilisateurs volontaires (étudiants et personnels)*
- *Création d'une liste de diffusion dédiée*
- *Nombre d'utilisateurs: environ 40 au début, 60 à la fin*
- *Durée des tests:*
  - *un mois pour le sans-fil*
  - *deux semaines pour les VPN*

Aujourd’hui

- *50 sessions en moyenne par jour (max 120)*
- *33h de connexion par jour   (max 92h)*
- *Forte demande service VPN*

Retour d'expérience exploitation

- Systèmes validés: Windows XP/2000, Linux 2.4 ou supérieur, MacOS X
- Pbs rencontrés liés essentiellement aux cartes clientes => utiliser drivers les plus récents
- Nombre de bornes de surveillance insuffisant => minimum 3 par batiment pour pouvoir faire de la localisation

(à vérifier avec nouvelle version AirOS 2.3)

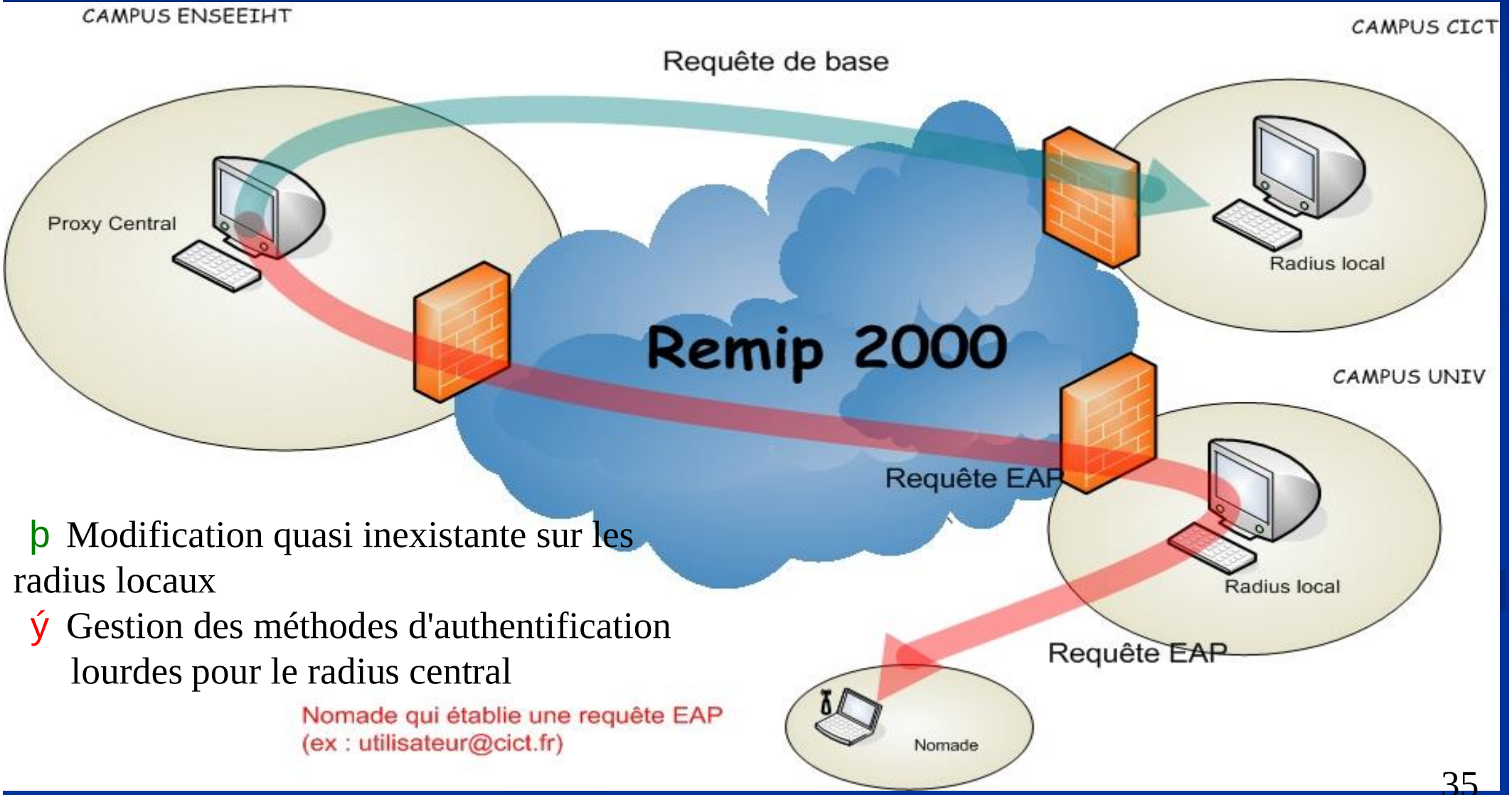
La suite,

- Nomadisme inter-sites INP :
  - Déploiement à l'étude ENSAT, Labège services centraux
- Nomadisme inter-universitaire
  maquette en cours (CICT/UPS, UT1,N7)
- IPv6 et mobilité

  AO DR: LAAS, CICT, IRIT/UPS, IRIT/N7

  démo décembre 2005 : JRES 2005
- Le grid wifi pour les labos en reconstruction?

Nomadisme régional



- Modification quasi inexistante sur les radius locaux
- Gestion des méthodes d'authentification lourdes pour le radius central

Merci pour votre attention, questions?