Nomadisme : problématiques et solutions

Eric JULLIEN

Patrick PETIT

David ROUMANET

Plan

- La solution nomade actuelle
- Tests de solutions complémentaires
- La future solution nomade
- Conclusion

Plan

- **- La solution nomade actuelle**
- **- Tests de solutions complémentaires**
- **- La future solution nomade**
- **- Conclusion**

Le contexte académique sur Grenoble

- 5 universités:
  - Université Joseph Fourier
  - Université Pierre Mendès France
  - Université Stendhal
  - Institut National Polytechnique de Grenoble
  - Université de Savoie
- Une population diversifiée (plus de 60000 étudiants, personnels, enseignants, …) aux besoins hétérogènes
- Plusieurs campus communs, des sites distants
- Des bâtiments partagés

⇒ Situation complexe

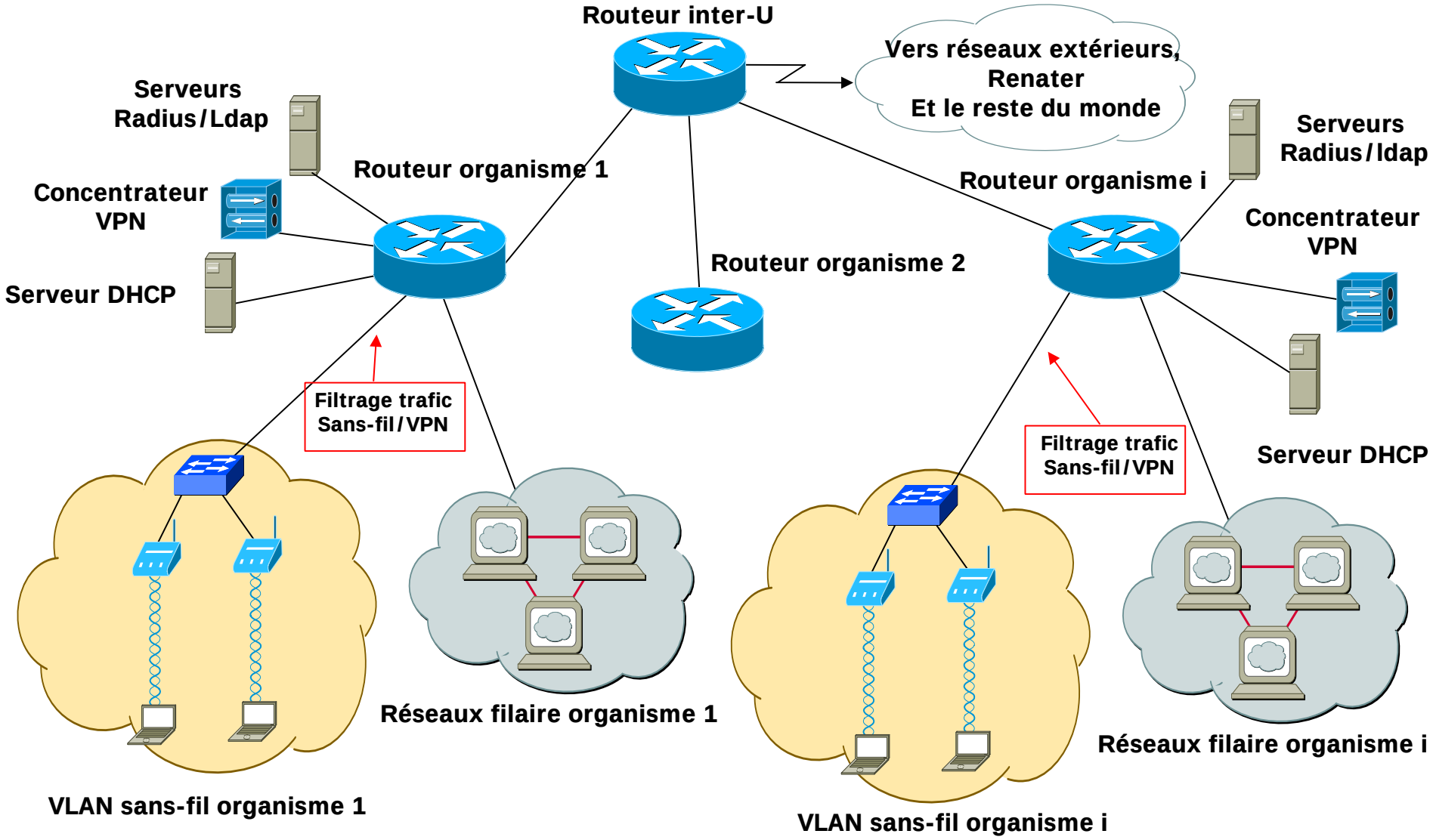
⇒ Nombreux acteurs avec des rythmes, des budgets, des compétences propres

Solution nomade Unique mutualisée sur tous les campus

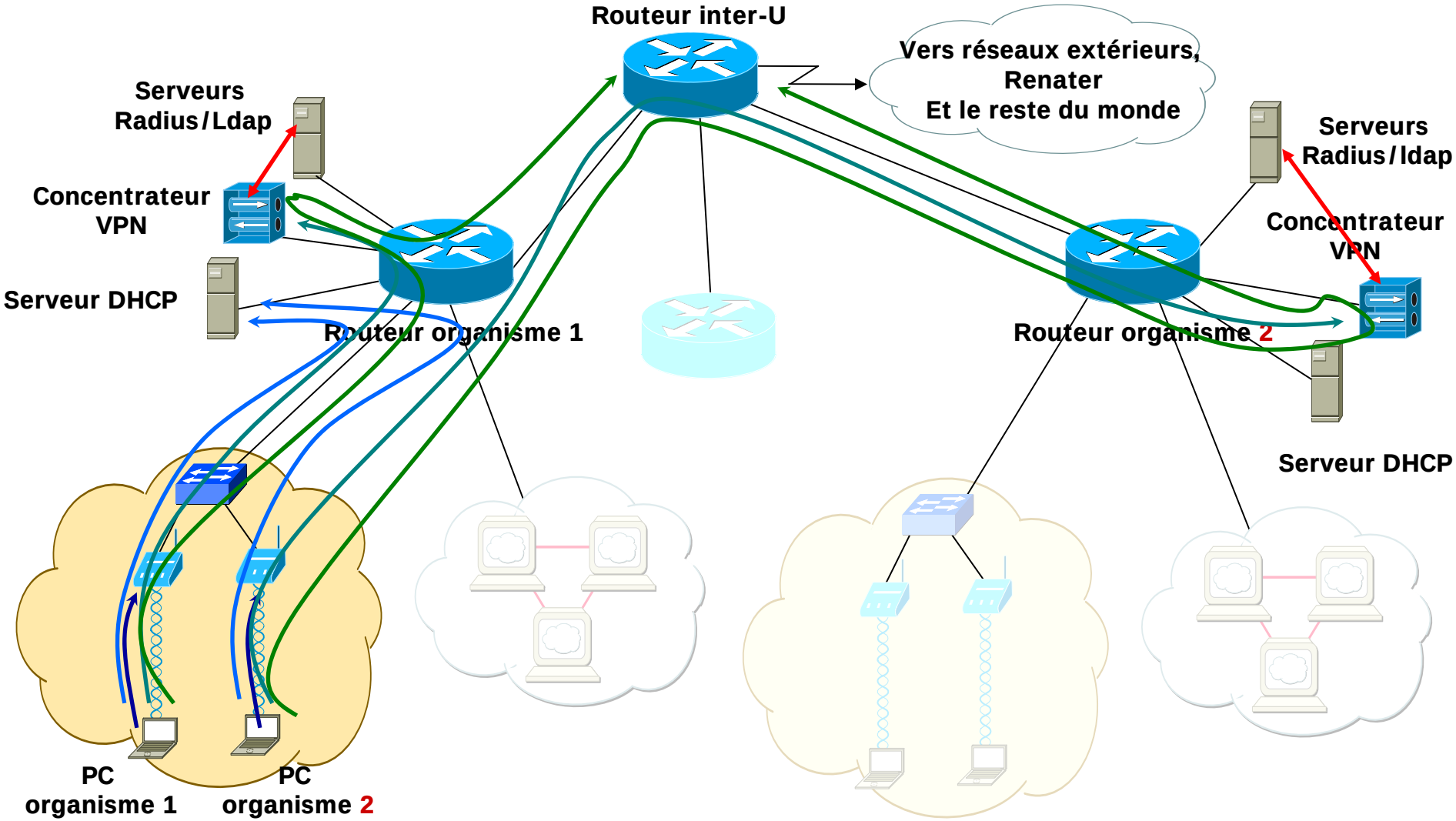
Solution retenue : VPN-IPSec

- Des bornes sans fils qui présentent un SSID ouvert avec des adresses de classes privées (10.X.X.X)
- Accès restreints vers les concentrateurs VPN et le site Web de diffusion du logiciel client VPN-IPSec
- Chaque établissement
  - déploie son architecture VPN
  - réalise l'identification/authentification de ses utilisateurs

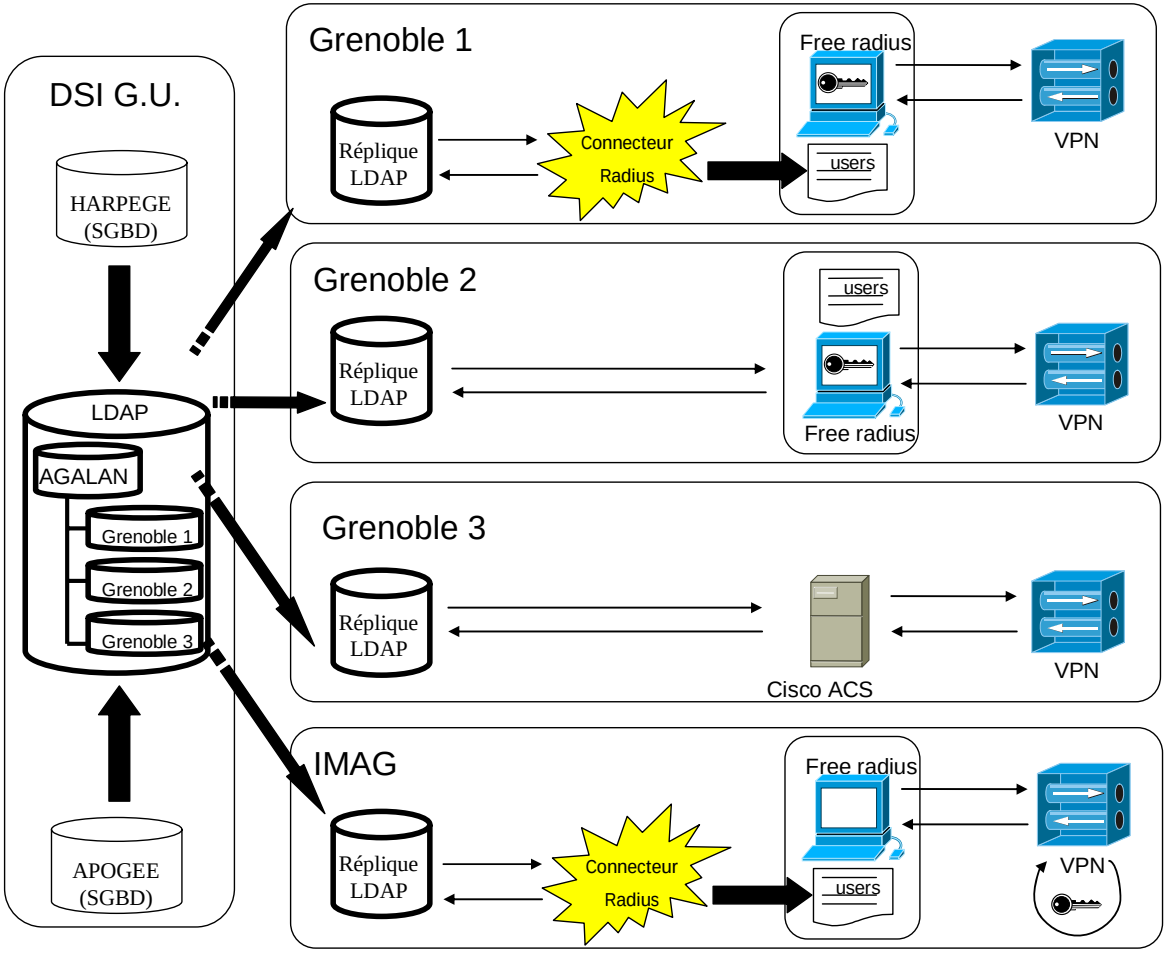
Principe d'architecture solution VPN



Scénario de connexion VPN-IPSec



Principe d'authentification



Avantages de la solution

- Homogénéité
  - Solution unique sur tous les campus
- Confidentialité des échanges
  - Chiffrement robuste inclus
- Respect des chartes
  - Gestion des traces
- Solution utilisable « en nomade »
  - Les connexions utilisables sont nombreuses (maison, étranger, …).
- Gestion des accès par type de population

Contraintes de la solution

- Solution centralisée
- Le chiffrement grève les performances
- Téléchargement et configuration d'un logiciel client
  - Nécessité d'avoir un serveur Web commun
- Gestion des visiteurs
  - Certains scénarios sont difficiles à gérer (congrès, invitations, visites).

Retours d'expérience : solution de + en + utilisée

MAIS…

- **Problématique de téléchargement et d'installation du client VPN-IPsec**
- **Les usagers ne sont pas toujours dans les annuaires**
- **Apparition de problèmes liés à l'utilisation du sans fils (vol de portable, password,…).**
- **Apparition de l'utilisation de portables personnels et ennuies qui vont avec :**
  - **Postes non à jour (patchs, spywares, virus)**
  - **Problème de responsabilité des CRI**
  - **=> expérimentation en cours : cellule d'assistance basée sur des étudiants formés par les CRIs.**

Plan

- La solution nomade actuelle
- **Tests de solutions complémentaires**
- La future solution nomade
- Conclusion

Tests de solutions complémentaires

« cahier des charges précis » : « 90 % des besoins des nomades sont de type web pur »

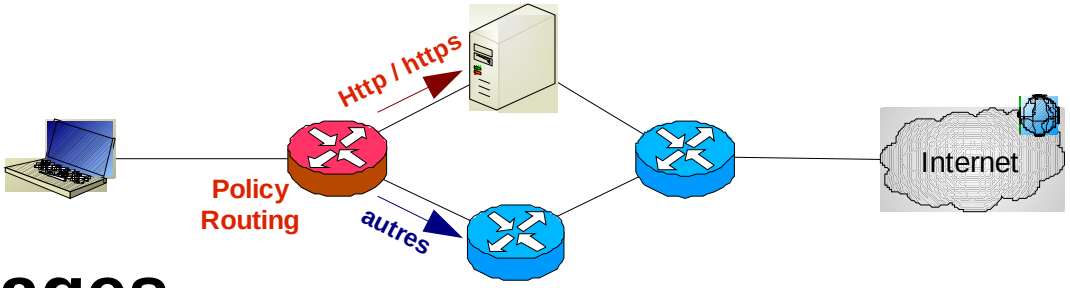
- **Plusieurs types de solutions ont été étudiés dans ce cadre :**
  - **Simple en manipulation**
  - **Accès web pur**
  - **Trace des utilisateurs**
  - **Taxonomie propriétaire des solutions testées :**
    - **L'approche Proxy avec Auto détection (sans client)**
    - **L'approche Proxy Transparent (sans client)**
    - **L'approche VPN-SSL (client léger)**
    - **L'approche « portail captif » (sans client)**
- **En parallèle de ces tests, étude d'une architecture basée sur la norme 802.11i**

Auto détection de Proxy

- La solution
  - L'implémentation de l'auto détection de proxy en DHCP n'a été validée que sous Windows avec IE
  - L'implémentation de l'auto détection de proxy par DNS a été vérifiée
    - sous Windows avec IE et Firefox,
    - sous linux avec Firefox,
    - sous Mac avec Firefox. (Sous Mac OS X 10.3 Safari et IE n'implémentent pas cette méthode).
- Avantages
  - on peut facilement prendre en compte d'autres protocoles que le http et le https, la gestion des authentifications est prise en compte, trace des utilisateurs complète
  - Possibilité de gérer des « crédits temps » avec SurfPass pour Squid (à valider)
  - Le navigateur s'exploite naturellement
- Inconvénients
  - L'auto détection n'est pas vraiment transparente pour les utilisateurs (il faut avoir coché la case si elle existe!!!)
  - Elle n'est pas prise en compte par tous les systèmes et tous les navigateurs
  - Pas de sécurisation des données

Proxy transparent

- **Pré-requis : policy routing**



- **Avantages**
  - **L'usage du navigateur reste inchangé (on peut exploiter ses favoris)**
- **Inconvénients**
  - **Pas de sécurisation des données**
  - **Moins modulable qu'un proxy normal**

Proxy Transparent

Solution testée	Avantages	Inconvénients
Squid v2.5 en mode transparent	• Solution libre	• Pas d'authentification à l'heure actuelle donc pas de trace des utilisateurs
WinGate	• Solution peu onéreuse • Trace utilisateurs complète	• Le client doit accepter les « pop-up », • Interpréteur java indispensable, • Problèmes de fonctionnement avec certains sites (bureau virtuel Rhône-Alpes) • Authentification en Active directory uniquement
BlueCoat	• Authentification ldap, radius,…, • Trace des utilisateurs complète, • Respect des sessions https, • Gestion des sessions http par cookie	• Https géré via une période de temps et avec adresse IP • Ftp en mode transparent OK mais obligation de forcer le client en mode passif si non automatique

VPN-SSL (client léger)

- **Avantages**
  - **Sécurisation des données**
- **Inconvénients**
  - **Le champ d'url du navigateur n'est plus exploitable,**
  - **Les favoris du navigateur ne le sont plus non plus,**
  - **Il faut disposer d'un interpréteur Java ou autre (activeX)**

VPN-SSL (client léger)

Solution testée	Avantages	Inconvénients
Cisco VPN 30xx	• Solution incluse sur les boîtiers VPN en standard • Authentification identique à la solution VPN • Fonctionne avec tous les sites web	• Interface • Gourmant en ressources (facteur 3 par rapport à du VPN IPSec en théorie, facteur 10 en pratique) • Traces utilisateurs insuffisantes dans notre contexte
Array Network SPX 3000	• performances • Traces utilisateurs complètes	• La version testée ne fonctionne pas avec certains sites (hotmail.com par exemple)

« portails captifs »

- La solution Monowall (pf-sense)
  - Portail de « niveau 2 »
  - Se substitue à la passerelle par défaut
- Avantages
  - Peut proposer plus que du http et https
- Inconvénients
  - Se comporte comme un NAT/PAT : pas de sécurisation des données (usurpation d'adresse MAC possible)
  - Difficultés de déploiement dans notre environnement (1 portail par Vlan de bornes) lié a son fonctionnement : filtrage par adresses MACs

« portails captifs »

- La solution Talweg
  - Portail de niveau « applicatif »
  - Pré-requis : avoir déployé du Policy-routing
- Avantages
  - Logiciel libre développé par le Crium (Université de Metz)
  - Gestion des logs complète
  - Facilité de déploiement dans notre contexte
  - Authentification et transport sécurisé des données sur le sans fil
  - Le mode de fonctionnement permet d'utiliser son navigateur naturellement, cependant la redirection ne permet pas de sauvegarder des URLs proprement dans ses favoris
- Inconvénients
  - La réécriture d'adresse a un coût

Autres solutions sans client et client léger

- **Il en existe bien d'autres !**
  - **Certaines éliminées d'office (ne correspondant pas à notre contexte)**
    - **Chilispot, nocatauth, Aventail, Symantec 4400, Ucopia, Bluesocket, AEP networks Netilla, Permeo Technologies (ActiveX), SSL Explorer, OpenVPN, NuFW …**
  - **Certaines n'ont pas été testées par manque de ressources**
    - **Juniper Netscreen, Menlo logic, Net Swift, iGate Safenet SSL-VPN, eGAP SSL-VPN, Arkoon, CyberGuard, ovisGate SSL, CheckPoint, F5 Networks Firepass 1000…**

Tests solution 802.11i

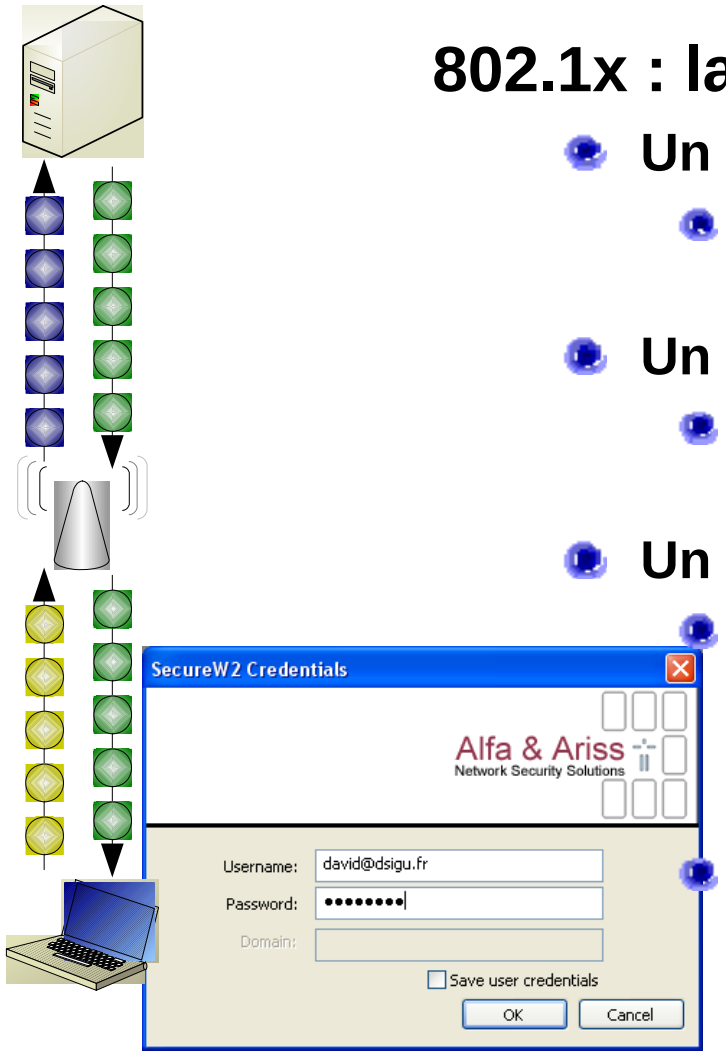
- 802.11 : la révolution sans fil MAIS…

  => Erreur de conception : WEP
  - … une mauvaise implémentation de RC4 menace le déploiement du standard 802.11

- Les solutions : WPA
  - WPA : 802.1x + TKIP
  - WPA2 : 802.1X + CCMP

802.1x est un « vieux » standard (PPP)

Tests solution 802.11i



802.1x : la sécurité en 3 points

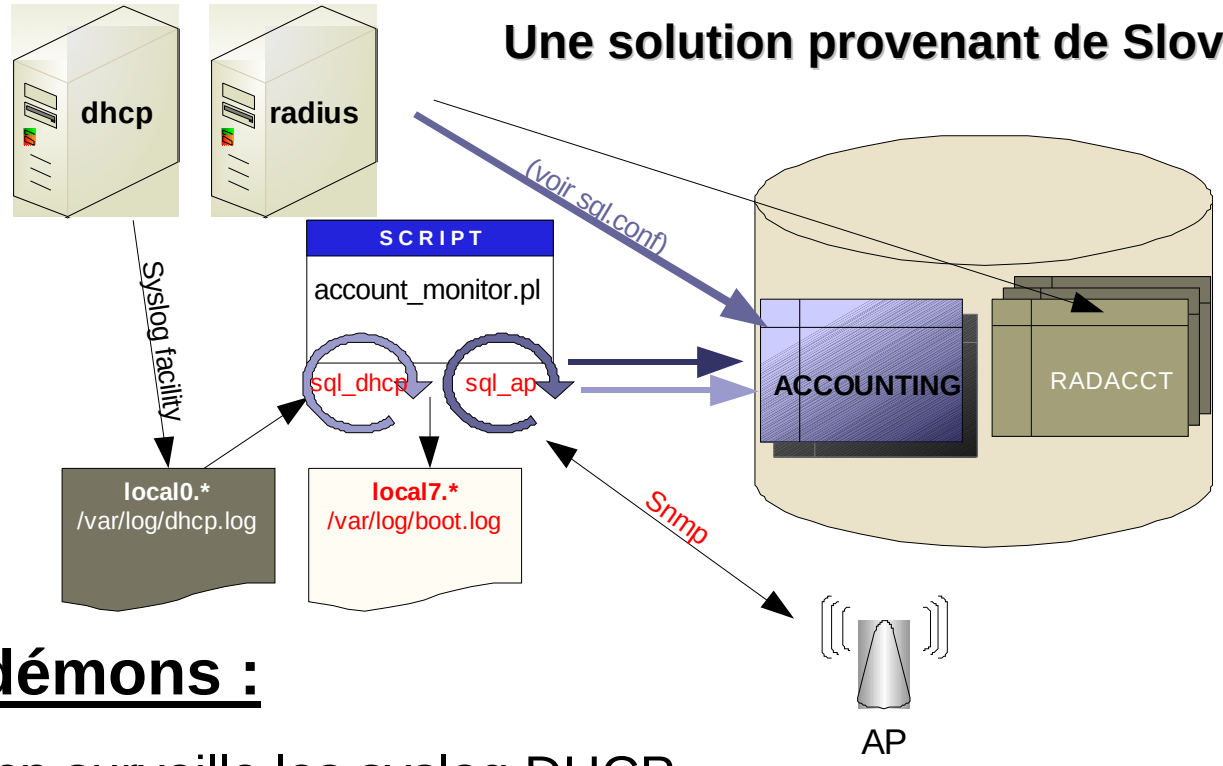
- Un serveur d'authentification (AAA)
  - Nous avons conservé FreeRADIUS : complet, gratuit, open-source, RADIUS
- Un point d'accès (AP)
  - Nous avons utilisé Cisco AP1100 : compatible WPA & WPA2 (même SSID)
- Un supplicant
  - Nous avons choisis SecureW2 pour Windows : simple à mettre en œuvre, gratuit et open-source (support GINA en cours de développement)
  - WPASupplicant pour les postes linux.

Tests solution 802.11i

- EAP : quel mécanisme choisir ?
  - MD5 ? LEAP ? Pas assez robuste…
  - PEAP ? Pas sous Linux
  - TLS ? Nécessite une autorité de certification
  - TTLS ? Un bon compromis dans notre contexte !
- AAA : Authentication, Autorization and Accounting
  - Respect de la charte Renater ➔ Accounting obligatoire

Tests 802.11i : l'accounting

Une solution provenant de Slovénie (ARNES)

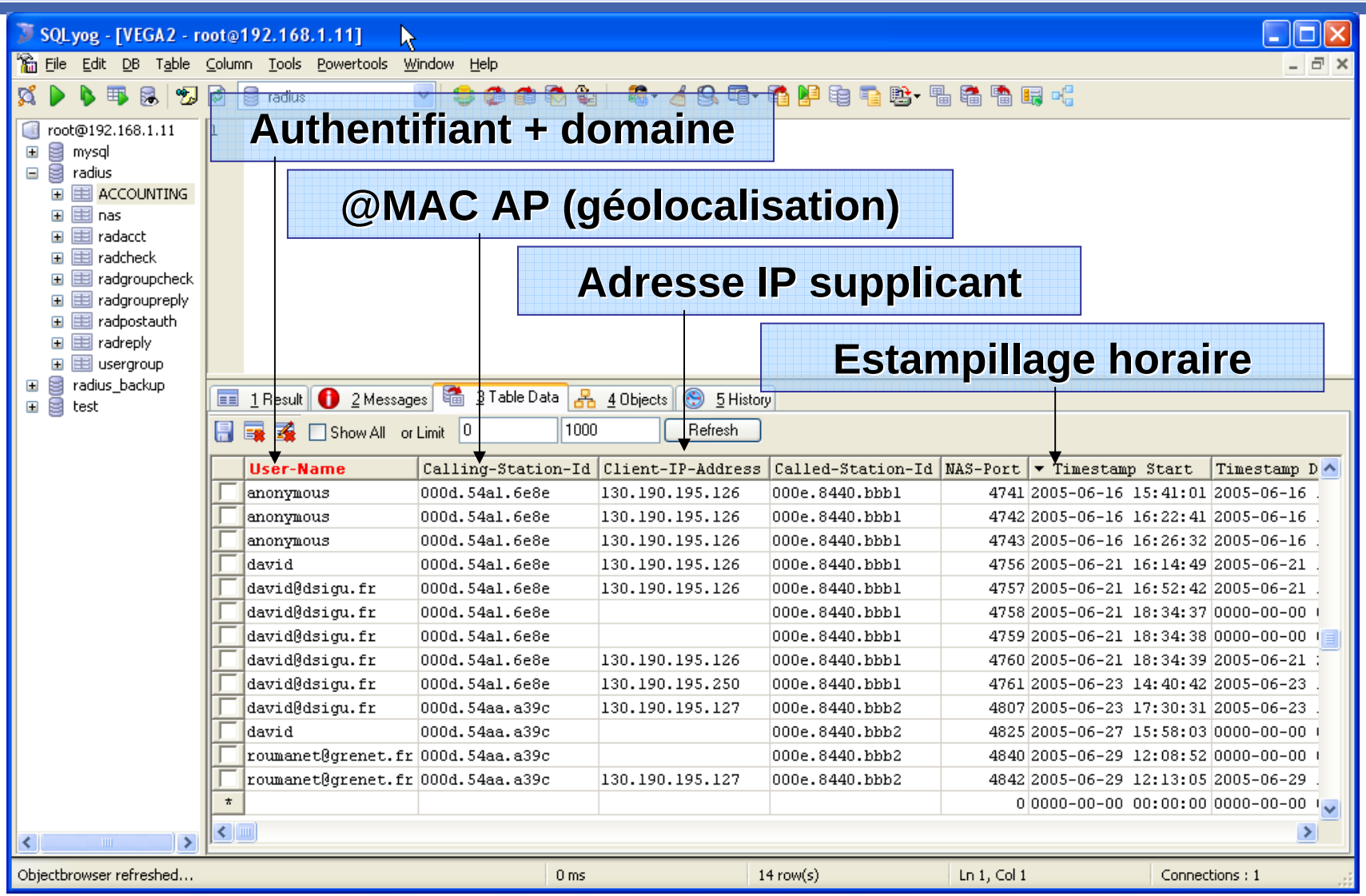


Deux démons :

- sql_dhcp surveille les syslog DHCP
- sql_ap surveille par SNMP les associations avec l'AP

➔ La corrélation @IP dynamique / identifiant RADIUS est faite

Tests 802.11i : résultats d'accounting sous forme SGBD

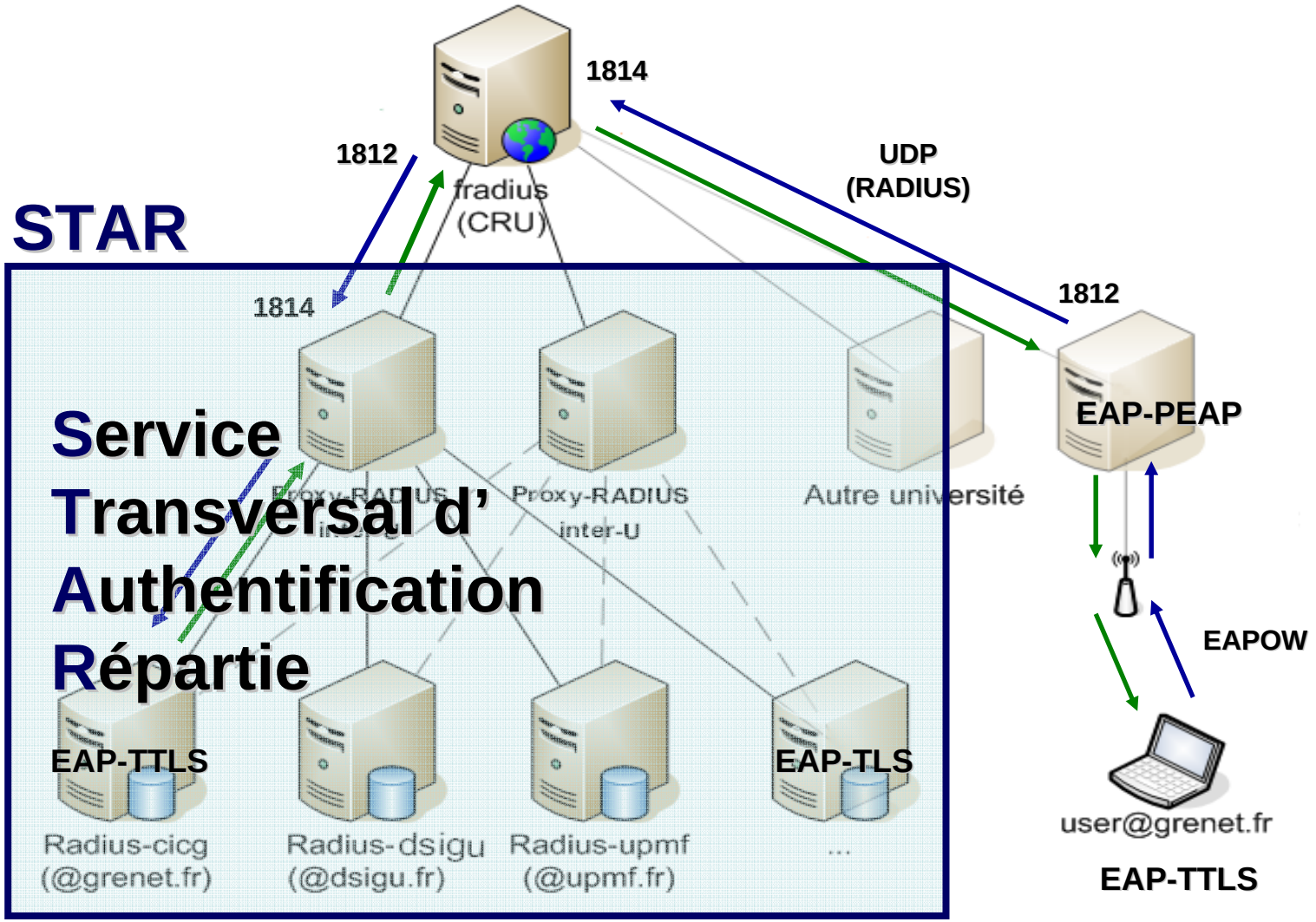


Tests 802.11i : Radius

La fonction de « Proxyfication » :

- Les serveurs RADIUS peuvent échanger des informations
- Le mécanisme d'authentification employé n'est pas dépendant du serveur RADIUS le plus proche de l'AP
- Il est possible d'envisager une authentification décentralisée ➔ ARREDU et portail captif !

Tests 802.11i : Proxy radius, Architecture et cinématique



Plan

- La solution nomade actuelle
- Etude de solutions complémentaires
- **La future solution nomade**
- Conclusion

La nouvelle solution nomade

A partir de toutes ces briques, nouvelle architecture proposée :

- On conserve le VPN pour tout accès nomade de nos utilisateurs
- Pour les accès sans-fil :
  - Adjonction d'une solution de simple accès web à la solution VPN de base pour « nos » utilisateurs
  - Création en parallèle d'une possibilité de se connecter en sans-fil dans le cadre du scénario ARREDU / EDUROAM

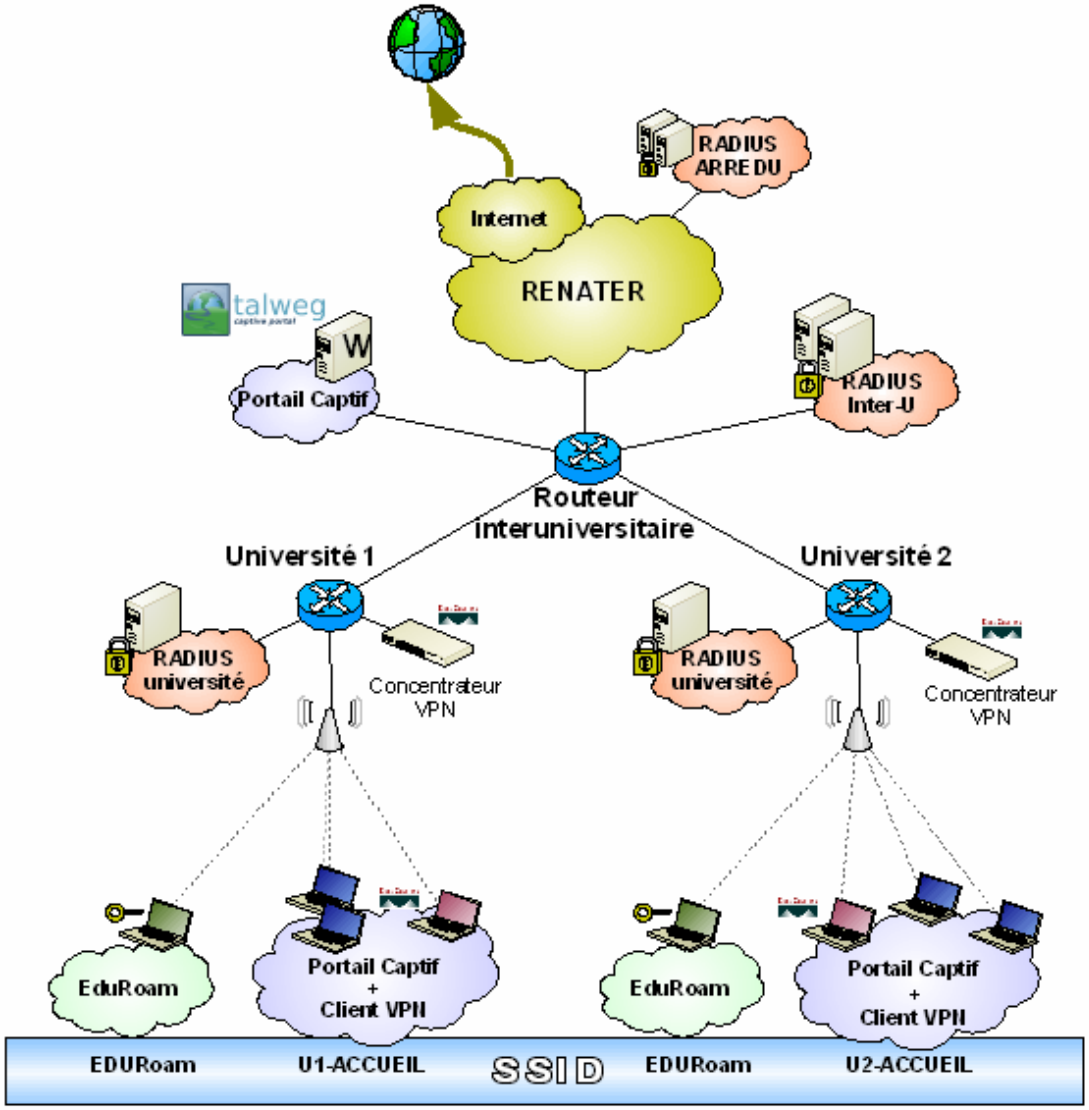
Aspects techniques pour le sans-fil

- **Conservation du SSID ouvert**
  - **pour accueillir informer les usagers des services sans-fil offerts**
  - **offrir un accès web simplifié,**
  - **Disposer d'un accès polyvalent sécurisé au moyen des tunnels VPN-IPSec**
- **Création d'un nouveau SSID pour le scénario ARREDU/eduroam**
  - **Solution valide pour tout scénario EAP TLS/TTLS/802.11i**
- **Ajout d'un SSID pour la téléphonie sur IP**

Authentification et gestion des logs

- **Nécessité des proxy radius**
  - **Pour l'accès au « web simplifié » par nos utilisateurs**
    - **Utilisable également à terme par les boîtiers VPN (sûreté de fonctionnement)**
  - **Pour le scénario ARREDU/EDUROAM**
    - **Utilisable par tout nomade dépendant d'un établissement ayant adhéré au projet**
- **Pour la gestion des logs**
  - **Déjà en fonction pour les accès VPN**
  - **Disponible sur le portail captif**
  - **Introduction des scripts de géo localisation pour la solution ARREDU/EDUROAM**

Synthèse de l'architecture



Plan

- La solution nomade actuelle
- Etude de solutions complémentaires
- La future solution nomade
- **Conclusion**

Nomadisme : problématiques et solutions

- Les scénarios couverts sont de + en + vastes
- Il faut travailler sur la salubrité des postes
- A moyen terme : Attente…
  - D'un Client 802.11i inclus dans les systèmes d'exploitation
  - De la mobilité IPv6 pour s'affranchir de la solution de type VPN.

    (pilote en cours et en fonction pour certains scénarios à la DSI Grenoble Universités)