Tuto 3 : Wi-Fi et eduroam

30 Janvier 2007
ENSAM – PARIS

Plan de la journée :

http://www.jres.org/tuto/tuto3.php

eduroam.fr

Projet ARREDU en 2004 : buts

- Accès Internet authentifié et sécurisé à des personnels (étudiants) avec mêmes identifiant/mot de passe et procédure sur tous les sites des participants
- Communauté concernée : établissements de recherche et d'enseignement supérieur raccordés à RENATER
- Infrastructure d'authentification répartie utilisant les serveurs RADIUS
- Utilisation principale : accès Wi-Fi
- Intégration à eduroam

Qualité de service

- Les nomades doivent pouvoir utiliser le service avec la même confiance qu'un accès filaire dans leur établissement
- => mot de passe protégé
- => trafic non écoutable
- => accès à un minimum de services/protocoles

Aspects sécurité

- Accès Wi-Fi sujets à écoute, attaques MIM, faux points d'accès, DOS,...
- Sécurisation du trafic :
  - Chiffrement fiable
    - WEP dynamique + rotation fréquente des clés
    - WPA, WPA2
- => portails dits captifs prohibés

Aspects sécurité, suite

- Modèle de sécurité RADIUS : hop-to-hop avec secret partagé
- Protection intrinsèque peu robuste
- => le trafic RADIUS doit être protégé (ex. VLANs dédiés)
- Par défaut les mots de passe sont «déballés» et «ré-emballés» à chaque traversée
- => Sécurisation de l'authentification :
  - Méthodes à base de tunnels SSL bout en bout
  - Authentification mutuelle

Aspects sécurité, suite

- Traçabilité
  - Journalisation des résultats d'authentification
  - Journalisation DHCP, NAT
  - Correspondance @IP <-> utilisateur en cas de besoin (abus)

ARREDU devient eduroam.fr

- Phase pilote jusqu'en avril 2006
- En exploitation depuis
- Intégration à *eduroam* => ARREDU devient la branche française d'*eduroam*

eduroam.fr : solutions techniques

- RADIUS (serveurs et proxies)
- IEEE 802.1x/EAP
- Méthodes d'authentification mutuelle sécurisées
  - PEAP
  - TTLS
  - TLS
- SSID eduroam

eduroam.fr : RENATER au centre des relations de confiance

- Les établissements s'engagent auprès de RENATER
- RENATER s'engage en leur nom auprès de Terena
- -> *trust fabric*

eduroam.fr : engagements de RENATER auprès de Terena

- Ses « clients » doivent s'engager sur de bonnes pratiques et sur l'éducation de leurs utilisateurs
- Au moins un serveur national doit être mis en oeuvre et sécurisé
- Informations sur le service
- Surveillance du service
- Implication du CERT

eduroam.fr : engagements des établissements / RENATER

- Offrir le service conformément aux recommandations
- Administrer et sécuriser un (ou +) proxy RADIUS
- Journaliser les résultats d'authentification
- Faire connaître l'existence du service
- (in)former leurs utilisateurs sur l'utilisation du service et le respect des règles d'utilisation des réseaux visités
- Offrir du support à leurs utilisateurs

eduroam.fr : engagements des établissements / RENATER

- Formalisés via signature de la Charte eduroam.fr/ARREDU associée au service mobilité de RENATER

eduroam.fr : état

- Opérationnel depuis avril 2006
- Un serveur national opéré par le CRU gérant le domaine *fr*
- Un serveur de backup géré par le CRC
- Raccordé à *eduroam* depuis avril 2006
- ~25 établissements raccordés

eduroam.fr

carte des sites raccordés (janvier 2007)

Workflow de gestion du service

NB : Service activé à réception de l'agrément signé

=> Possibilité de test de l'infrastructure au préalable

Les spécifications techniques

www.cru.fr/wiki/eduroam/specifications_techniques

Service de mobilité pour la communauté RENATER

Interface SAGA

1

Demande d'inscription par le correspondant technique RENATER

2

Renseignement par le correspondant eduroam des informations du compte

Base d'enregistrement des établissements adhérants

Monitoring des clients RADIUS assuré par le CRU

3 – Configuration du RADIUS d'établissement

Proxies national et son backup

Les nomades

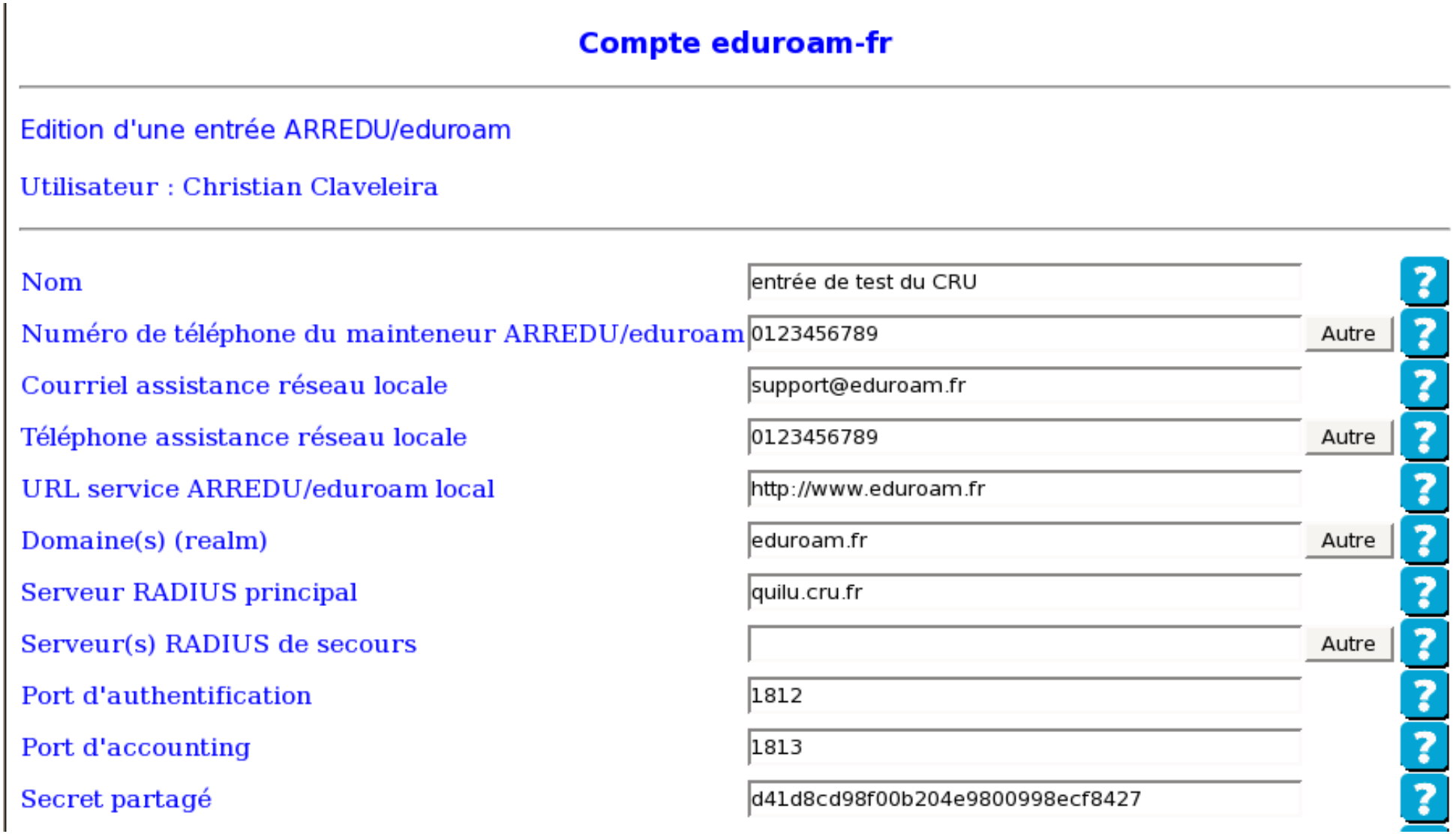
RENATER / CRU

Etablissement

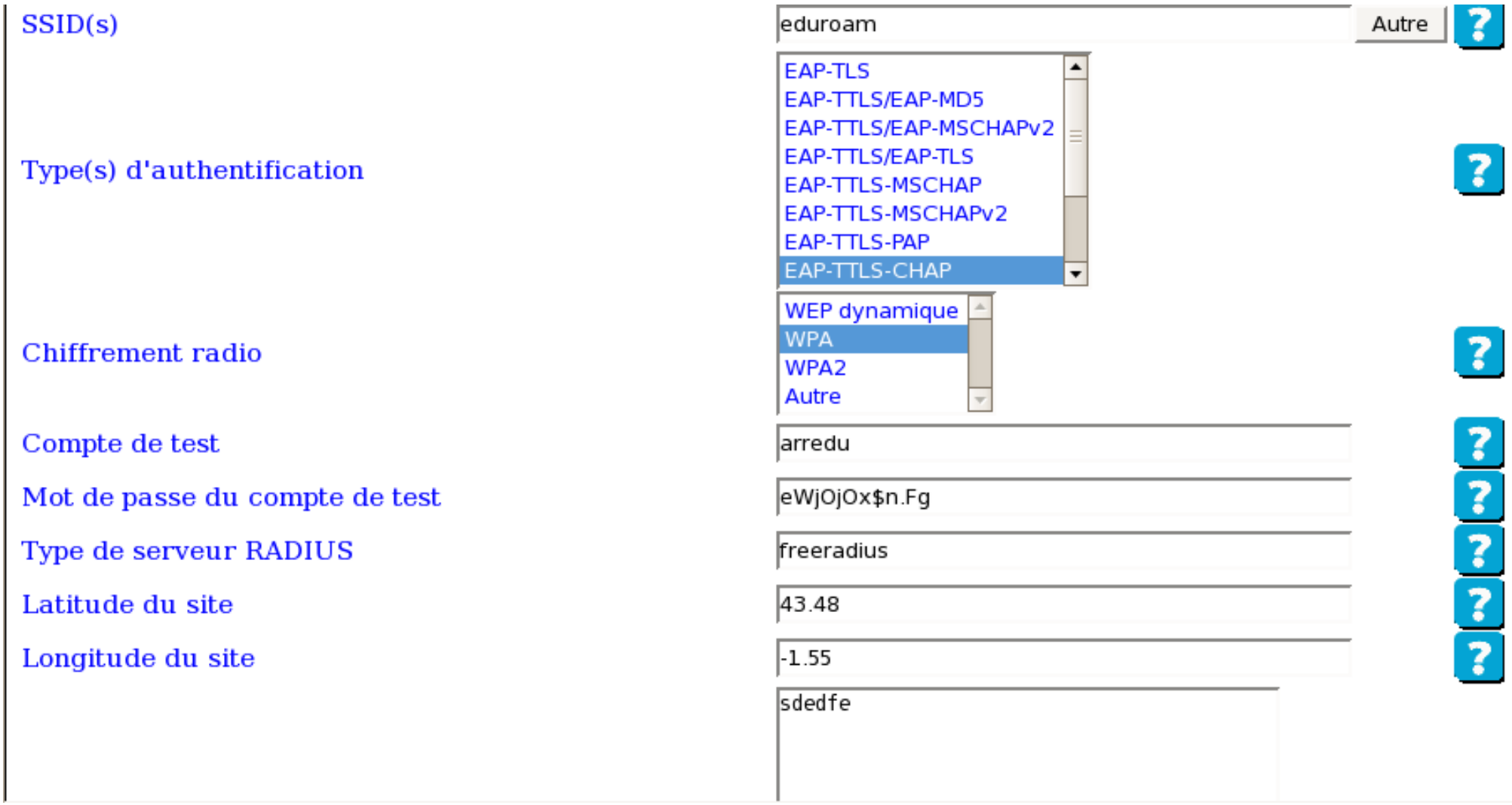
Interface de configuration du compte (1)

- interface Web de gestion de son compte
  http:arredu.cru.fr/admin
  => accès authentifié X509 ou Sympa

Interface de configuration du compte (2)



Interface de configuration du compte (3)



Renseignements fournis

- Type d'authentification de vos utilisateurs -> monitoring
- Chiffrement radio -> informations à mettre à disposition des utilisateurs
- User / mot de passe du compte test -> monitoring
- Type de serveur RADIUS -> informatif
- Latitude / Longitude (pré-remplie) -> affichage carte www.eduroam.fr

Authentification RADIUS

- Configuration proxy et client
- N'utiliser que EAP / {TLS – TTLS ou PEAP}
- Mettre en place le nécessaire pour la traçabilité
- Pas de trafic venant de portail web dit captifs

Services à offrir

- Offrir le DHCP
- Préconisations : pas de filtrage de protocole en sorti (et dans tous les cas, au minimum : HTTP et HTTPS, DNS, ICMP (echo/reply), IPSec, OpenVPN, SSH, POPs, IMAPs, NTP, SMTP/AUTH, SMTP local)
- Diffusion de l'information
- Formation et support pour ses utilisateurs

eduroam.fr

Monitoring de l'infrastructure nationale

Buts

- Surveiller la disponibilité et les temps de réponse des serveurs RADIUS d'établissement
- Permettre aux administrateurs de voir comment est vu leur serveur
- Aller au-delà de la surveillance des serveurs RADIUS
- Offrir aux utilisateurs de vérifier la disponibilité de l'infrastructure là où ils en ont besoin

Méthode

- Simuler une utilisation réelle
  - Utiliser un compte d'utilisateur
  - Utiliser la méthode d'authentification retenue par l'établissement
  - N'utiliser l'authentification RADIUS (qui expose les *credentials*) qu'en secours

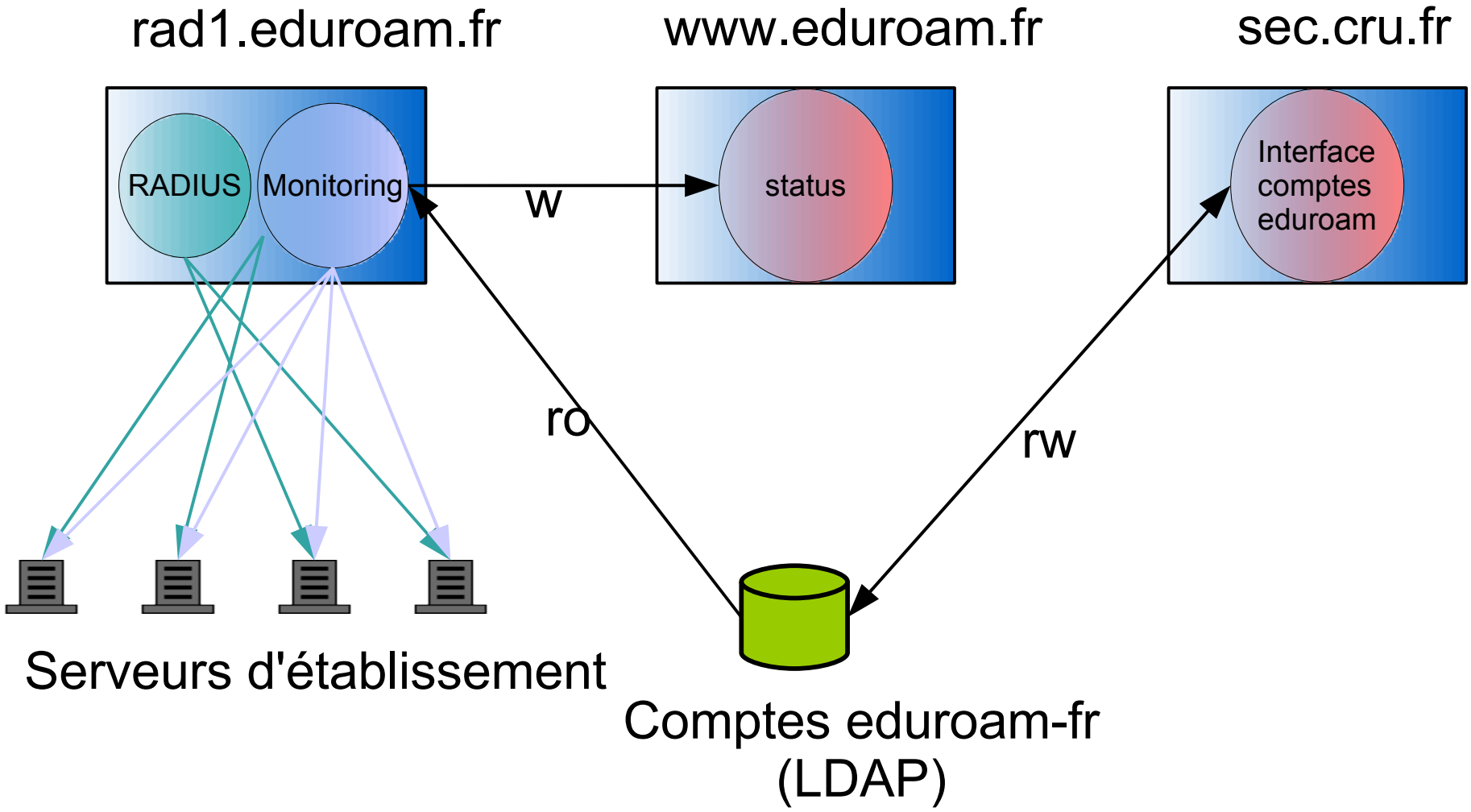
Problèmes

- Simuler un supplicant 802.1x + EAP
- Minimiser les intermédiaires
- Afficher les résultats

Choix

- Tests effectués depuis le proxy national *rad1.eduroam.fr*
  - Autorisé sur tous les serveurs d'établissement
  - Aucun serveur intermédiaire
    - Pas de trafic inutile sur le proxy
    - Pas d'aléa introduit par d'autres serveurs
- Affichage effectué sur www.eduroam.fr
  - Pas de http sur *rad1.eduroam.fr*
- Couplage avec la carte géographique

Architecture



Implémentation

- Basée sur la commande *eapol_test* de *wpa_supplicant* et sur *radtest* de FreeRADIUS
- Des scripts génèrent les configurations nécessaires à *eapol_test* pour tester chaque établissement et analysent les résultats d'exécution
- Affichage texte ou html
- Peut être utilisé pour faire du debugging sur un *realm* particulier

Résultats de monitoring

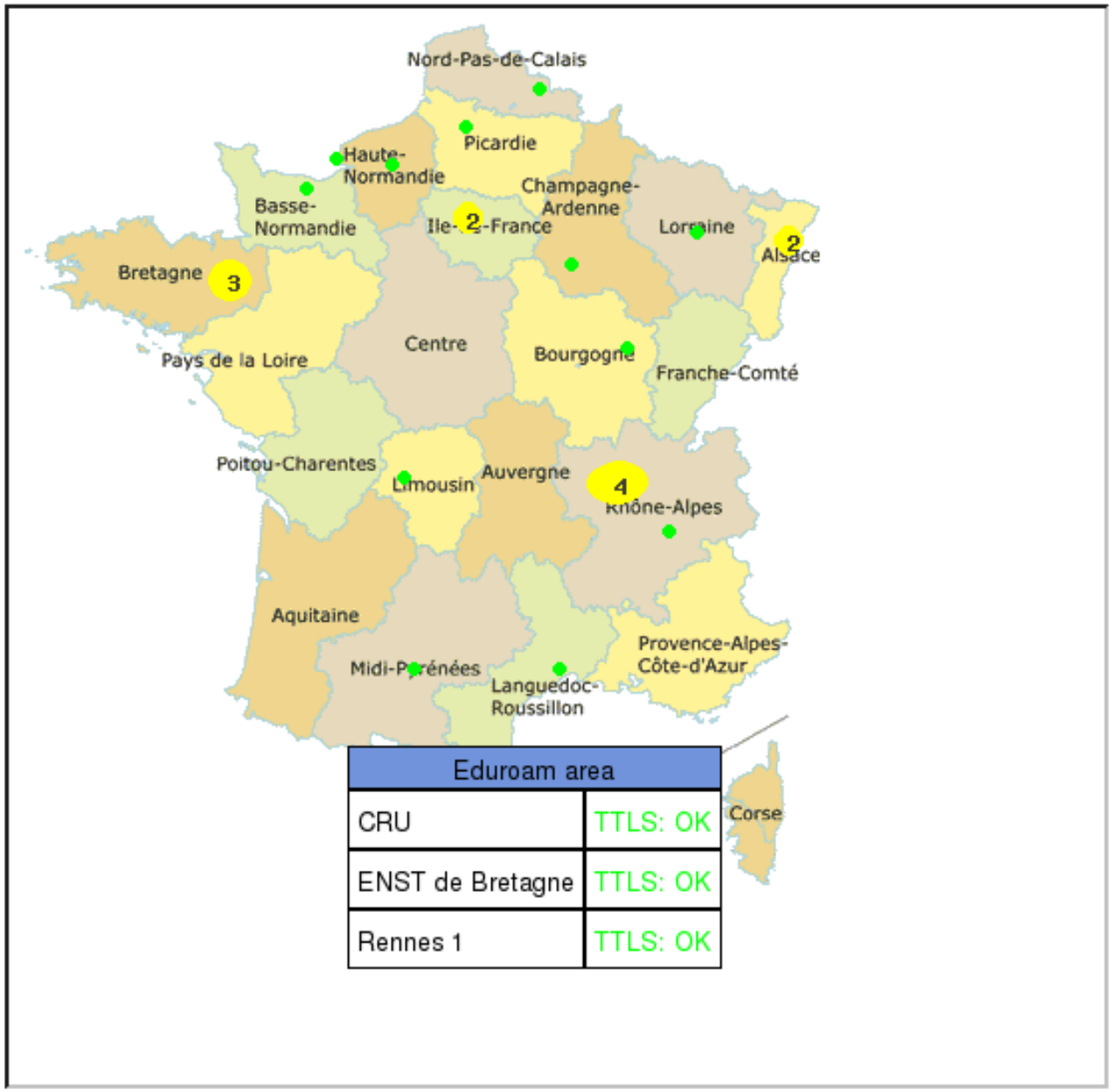
eduroam.fr Monitoring

Surveillance du fonctionnement de l'infrastructure eduroam.fr, le 22/01/07 à 16:45:01 :

Nom	TTLS	PEAP	RADIUS
CRU	OK (0.24 s)	OK (0.51 s)	OK (implicite)
INSA de Lyon	OK (0.34 s)		OK (implicite)
ENST de Bretagne	OK (0.24 s)		OK (implicite)
Université de Technologie Troyes		OK (0.61 s)	OK (implicite)
Chancellerie des Universites de Paris - Sorbonne	OK (0.27 s)	OK (0.37 s)	OK (implicite)
Université de Toulouse 1	OK (0.32 s)		OK (implicite)
Rennes 1	OK (10.01 s)	RADIUS_NOT_AVAIL (10.01 s)	NOK
Université de Valenciennes	OK (0.43 s)	OK (0.56 s)	OK (implicite)
Université de Nancy 2	OK (0.30 s)	OK (0.41 s)	OK (implicite)
Université de Dijon	OK (1.51 s)	OK (2.09 s)	OK (implicite)
Université d'Amiens	OK (0.37 s)		OK (implicite)
ENS de Lyon		OK (0.58 s)	OK (implicite)
Université de Rouen	NOP	NOP	NOP
IRD	NOP	NOP	NOP
Université de Le Havre	OK (10.01 s)		OK (implicite)
Institut IMAG (Informatique et Mathétiques Appliquées de Grenoble)	NOP	NOP	NOP
ENS LSH		OK (0.58 s)	OK (implicite)
CRIHAN / Centre de Ressources Informatiques de Haute-Normandie	NOP	NOP	NOP
Université de Strasbourg 1	RADIUS_NOT_AVAIL (10.01 s)		NOK
Université de Strasbourg 2	NOP	NOP	NOP
INRP - Institut National de Recherche Pédagogique	NOP	NOP	NOP
GIP RENATER	RADIUS_NOT_AVAIL (10.01 s)		NOK
Université de Montpellier 3	RADIUS_NOT_AVAIL (10.01 s)		NOK
Université de Limoges	RADIUS_NOT_AVAIL (10.01 s)		NOK

Done

Couplage avec la carte géographique



À faire

- Adapter l'affichage à l'augmentation des adhérents
- Trier
- Alertes automatiques des correspondants ?