CRU

Nomadisme réseau pour la communauté enseignement supérieur-recherche

Projet ARREDU

Christian Claveleira – Vincent Carpier

CRU

CRU

Plan

- Introduction
- Les technologies du nomadisme
  - RADIUS
  - EAP
  - 802.1x
  - 802.11i
  - Méthodes d'authentification
- Le projet eduroam
- Le projet ARREDU

CRU

Introduction

- Les nomades (chercheurs, enseignants, étudiants, invités) ont bessoin d'accès réseau
- Des moyens en place : accès Wi-Fi
- Contrôle de l'accès et de l'usage du réseau
- Minimiser l'administration
- Tout en assurant la sécurité des données

RADIUS
Remote Access Dial-In User Service

Protocole d'authentification avec trois fonctions : AAA

- Authentification : qui demande une connexion ?
- Autorisation : cette personne est elle autorisée ?
- Accounting : temps de connexion , volume

RADIUS

3 acteurs :

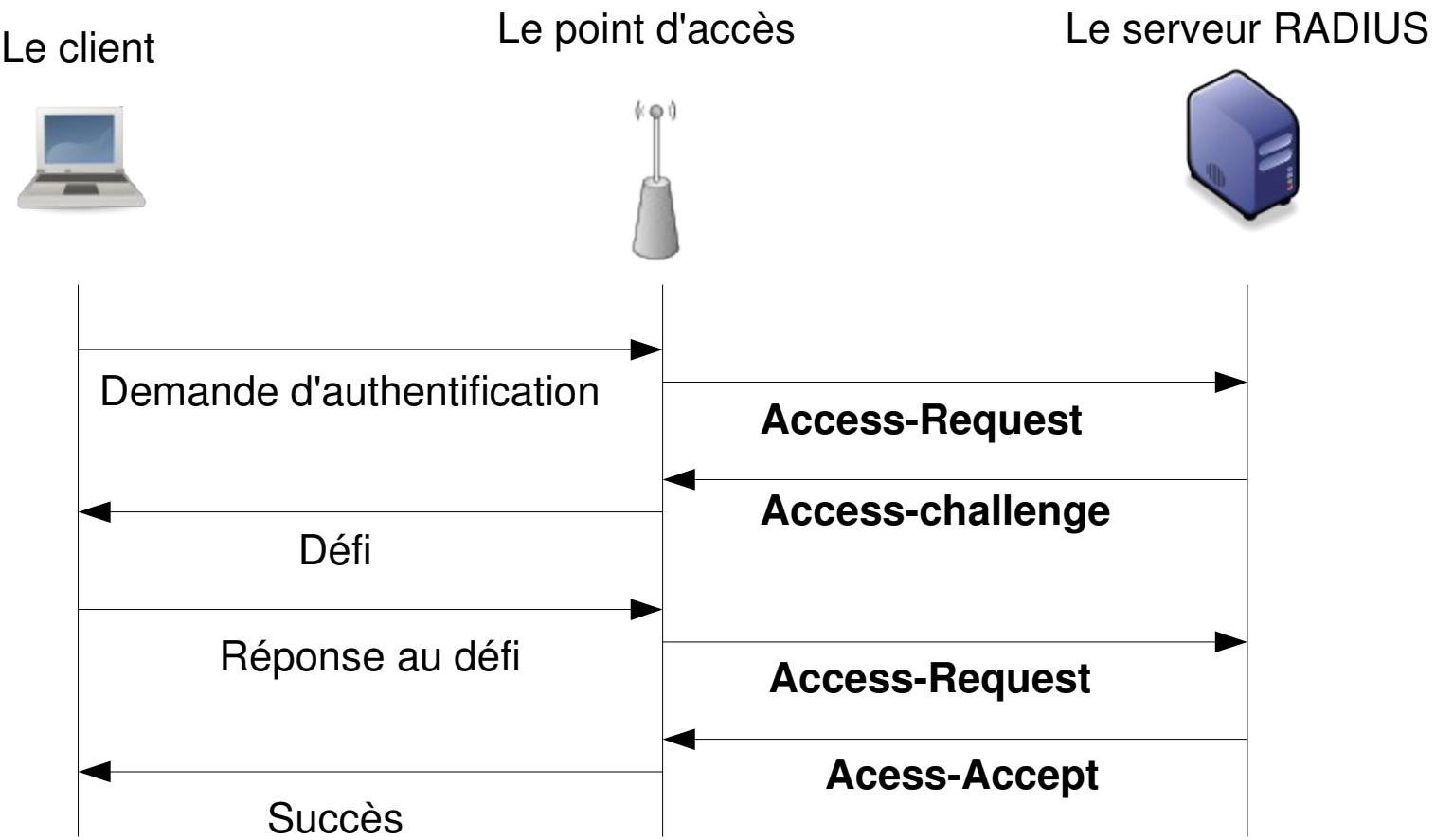
- Client (supplicant) : processus demandant l'authentification pour une connexion au réseau
- Network Access Server : point d'accès au réseau
- Serveur RADIUS : traitement des demandes d'authentification en interrogeant une base de données d'utilisateurs

Les paquets RADIUS

Pour remplir ses fonctions, le protocole RADIUS dispose de 9 types de paquet :

- 4 pour l'authentification
- 2 pour l'accounting
- 1 code pour le status client
- 1 code pour le status serveur
- 1 code reservé

Principe de demande d'authentification avec RADIUS



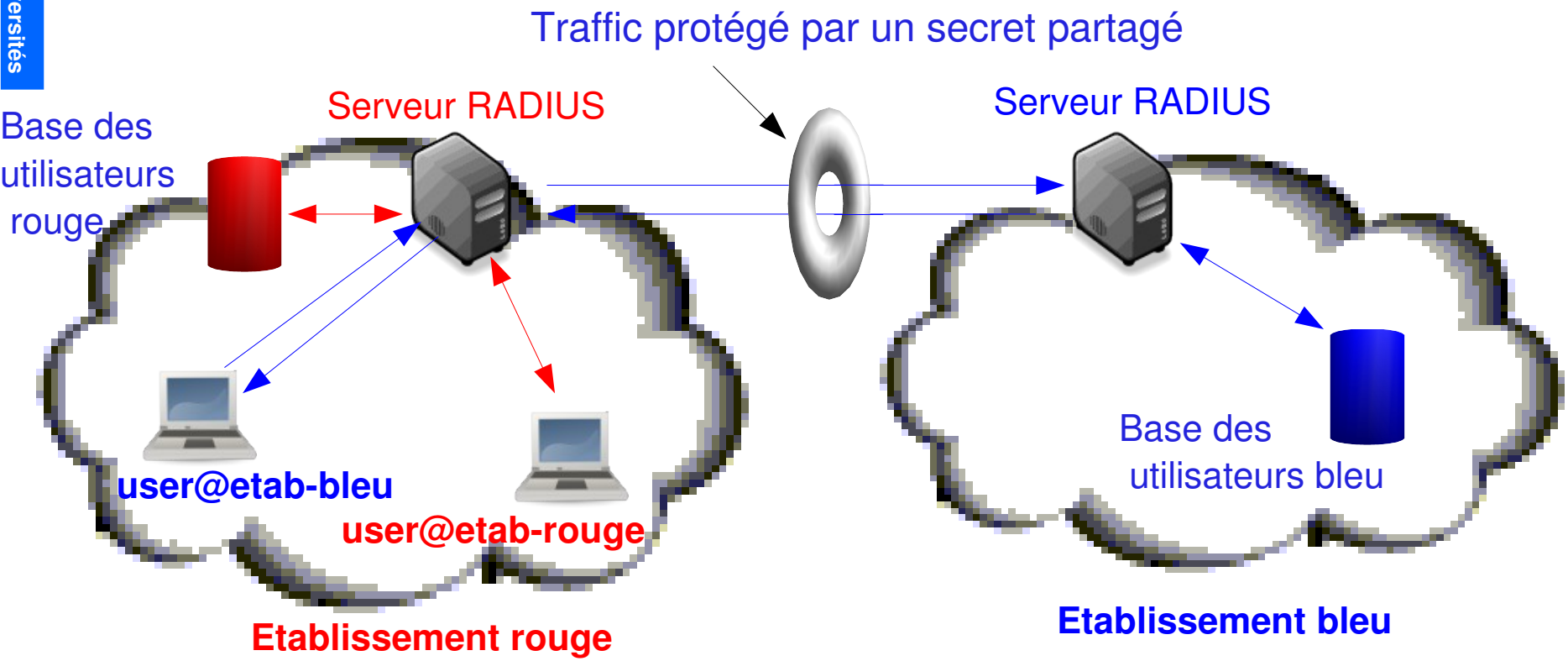
Relayage RADIUS

Délégation de l'authentification à un autre serveur RADIUS, fonction aussi appellée proxy-RADIUS

A qui doit-on adresser la demande ?

Introduction de la notion de domaine (realm) lors de la demande d'authentification

Proxy RADIUS



Suivant la valeur du domaine le premier serveur RADIUS rencontré sait si il doit traiter l'authentification ou relayer la demande à un autre serveur

EAP
Extensible Authentification Protocol

Protocole de transport de méthodes d'authentification telles que :

OTP, TTLS, PEAP, SIM ...

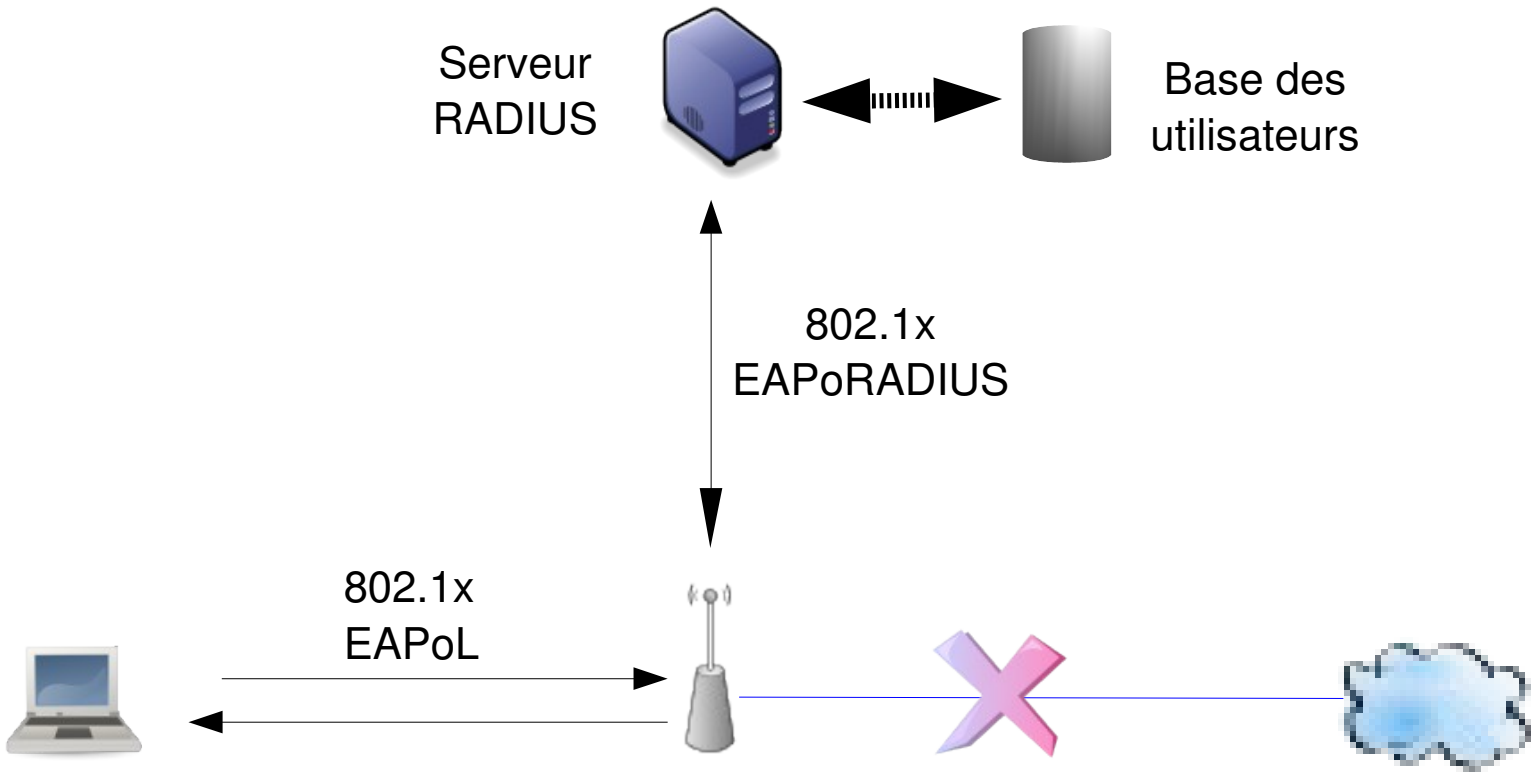
Ce protocole ne sert que dans la phase d'authentification

EAP et 802.1x

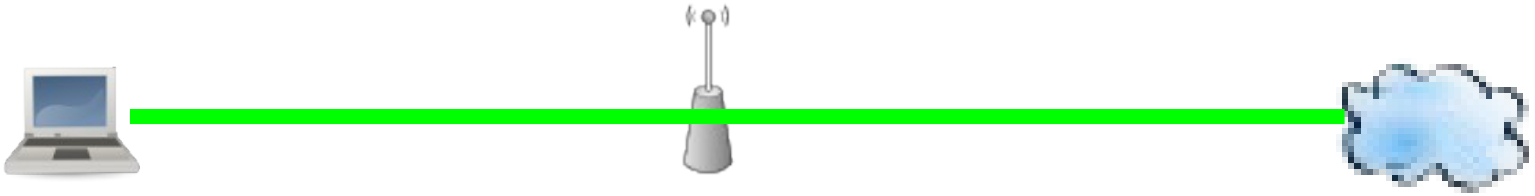
802.1x décrit le transport des méthodes d'authentification sur EAP entre le client et un serveur RADIUS

Un point d'accès utilisant la norme 802.1x se comporte comme un interrupteur

EAP et 802.1x


Serveur
RADIUS
Base des
utilisateurs
802.1x
EAPoRADIUS
802.1x
EAPoL

EAP et 802.1x



Début de 802.11i

Faiblesses du WEP (MIM et Hijacking)

=> GT IEEE début de la norme 802.11i

2002, ne voyant rien aboutir, la Wi-Fi Alliance publie une version allégée de 802.11i

=> WPA (chiffrement TKIP)

WPA est utilisable sur les bornes d'accès de type 802.11a et 802.11b moyennant un upgrade du firmware

Naissance de 802.11i

2004, IEEE ratifie la norme 802.11i

En parallèle, la Wi-Fi Alliance crée la certification WPA2 (chiffrement AES) pour les produits implémentant entièrement la norme 802.11i

WPA2 implique l'utilisation de borne d'accès de type 802.11g (puce crypto dédiée)

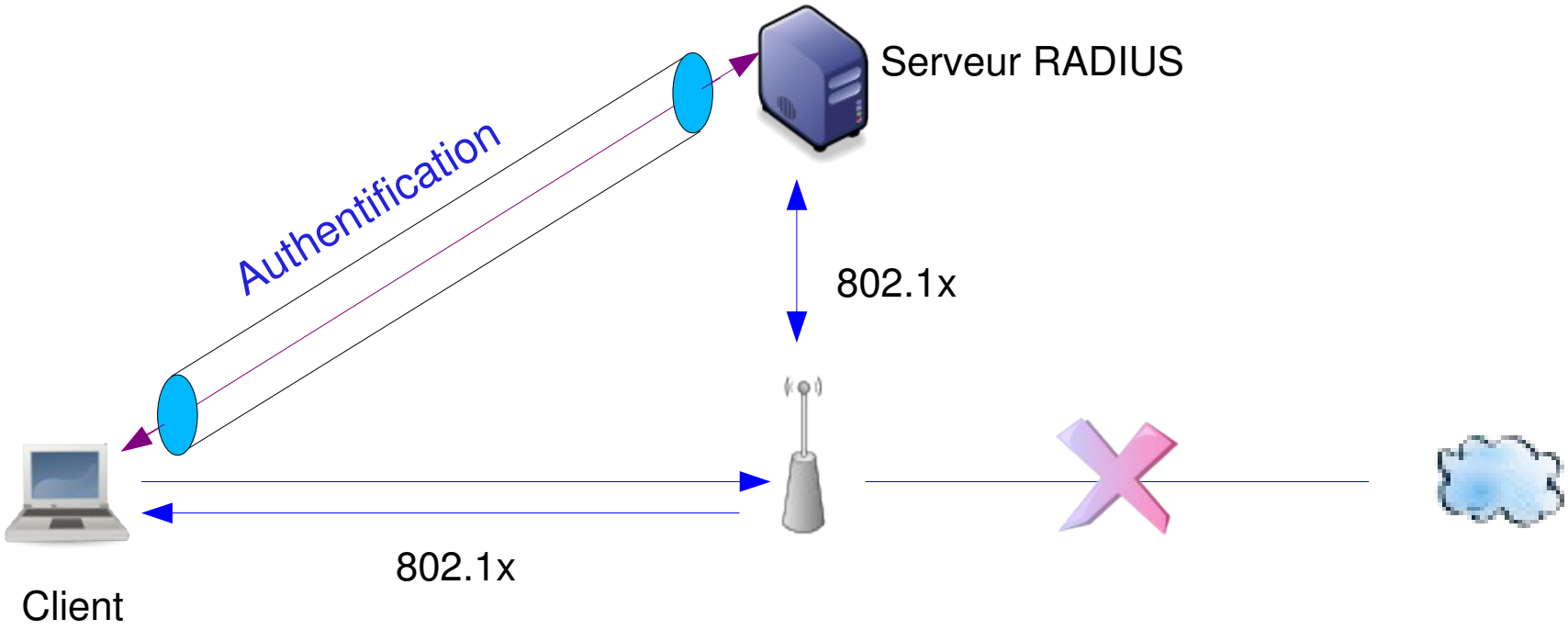
Méthodes d'authentification

EAP – PEAP

EAP – TTLS

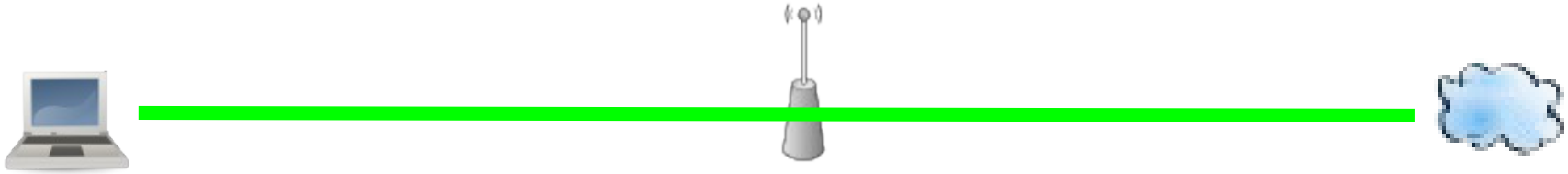
EAP - TLS

Points communs à PEAP – TTLS - TLS



Etablissement d'un tunnel TLS avec authentification du serveur RADIUS, puis utilisation de ce tunnel pour transmettre l'authentification

Points communs à PEAP – TTLS - TLS



Client

Accès au LAN

PEAP
Protected Extensible Authentication Protocol

Méthode d'authentification : MS-CHAP(v2) ou TLS transitant dans le tunnel TLS

Pour s'affranchir d'une distribution de certificat client, on préférera une authentification MS-CHAP(V2)

TTLS
Tunneled Transport Layer Security

Même principe que PEAP avec authentification du serveur RADIUS, mais on dispose d'un choix de méthode d'authentification plus large :

MD5, PAP, MS-CHAP(v2), LEAP, TTLS, TLS, FAST, GTC, OTP, AKA, SIM

TLS

Transport Layer Security

Authentification mutuelle du serveur et du client par certificats X.509

Utilisation d'une IGC obligatoire

Solution la plus sûre et la plus robuste

Néanmoins penser à protéger correctement la clé privé : utilisation de carte à puce cryptologique

CRU

Comparaison sur les méthodes d'authentification

Méthodes	Authentification	Tunnel	IGC nécessaire	Client natif	Client Disponible
MD5	Non	Non	Non	Win, MacOS	Linux
LEAP	Non	Non	Non	MacOS	Win, Linux
PEAP	Serveur	Oui	Non	Win, MacOS	Linux
TTLS	Serveur	Oui	Non	MacOS	Win, Linux
TLS	Client & serveur	Oui	Oui	Win, MacOS	Linux
FAST	Serveur	Oui	Non	Non	Win, Linux

eduroam

- Initiative de la TF Mobility de Terena en 2003
- Étude des problèmes de sécurité des réseaux sans fil
- Recommandations pour solution(s) de nomadisme international pour les utilisateurs de réseaux académiques (NREN

eduroam : buts

- accès Internet aux utilisateurs nomades
  - Aisés mais contrôlés
  - Entraînant peu de surcroît d'administration
  - Sécurité comparable à un accès filaire
  - Facilement déployable à grande échelle

eduroam : solutions étudiées

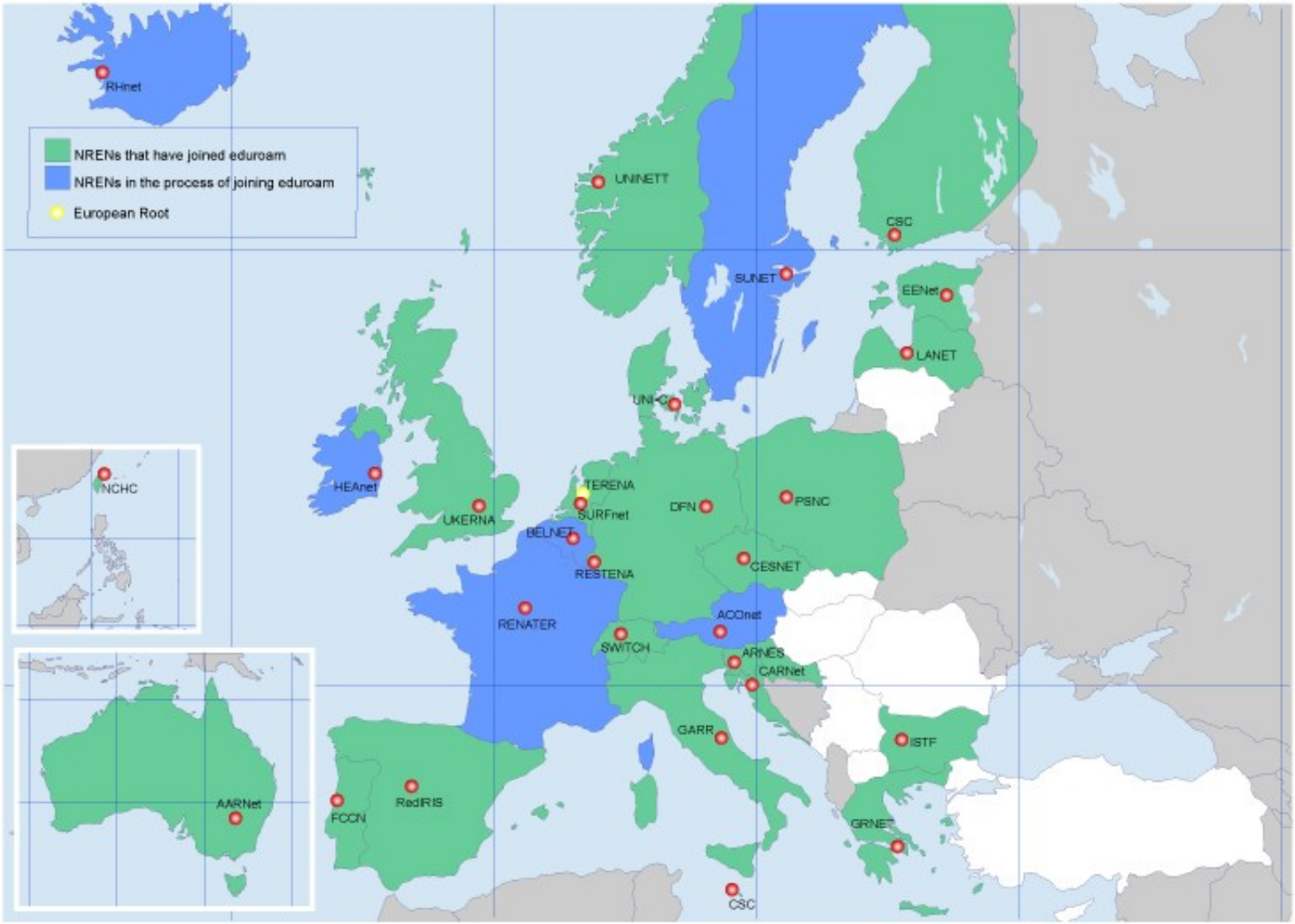
- Authentification Web + Radius
  - déploiement facile
  - Déjà utilisé
  - Problèmes de sécurité
- VPN
  - Déploiement laborieux à grande échelle
  - Déjà utilisé
  - Sûr
- IEEE 802.1x + Radius

eduroam : conclusion

- 802.1x + Radius retenu
- Première expérience de mobilité inter-NREN
- Pilote européen appelé EduRoam (devenu eduroam)
- Hiérarchie de serveurs Radius gérés par les NRENs ayant signé un agrément avec Terena
- Serveur racine géré par Terena

CRU

eduroam : couverture actuelle



ARREDU : contexte en 2004

- Besoins d'accès à l'Internet en déplacement chez des collègues
- Maîtrise de l'utilisation des réseaux d'établissements
- Démocratisation des portables
- Incitation au déploiement du Wi-Fi dans les établissements en marge de l'opération MIPE en 2004
- Groupe de travail *gt-sans-fil*

ARREDU : 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

ARREDU : 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

CRU

Aspects sécurité, suite

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

Aspects sécurité, suite

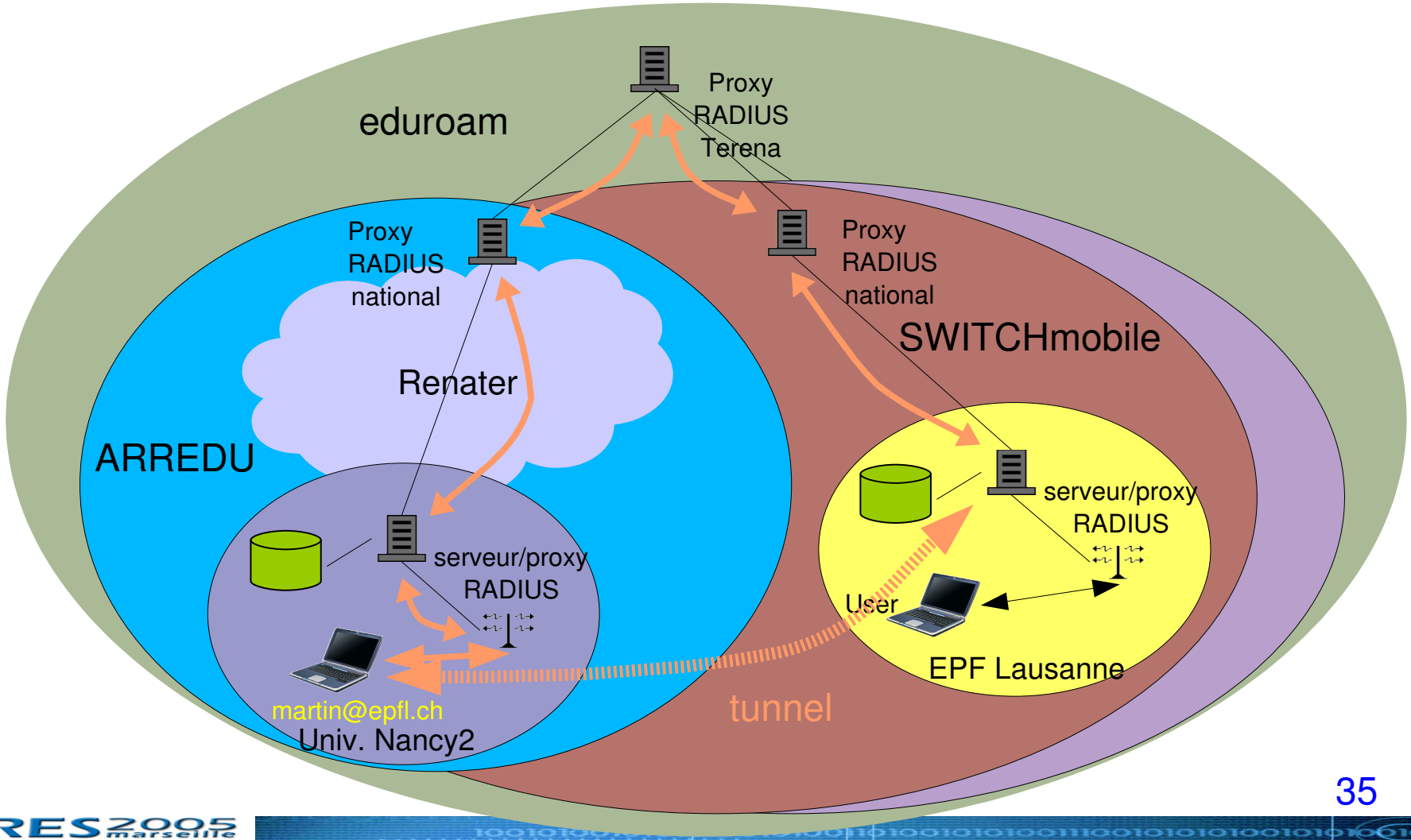
- Traçabilité
  - Journalisation des résultats d'authentification
  - Journalisation DHCP, NAT
  - Correspondance @IP <-> utilisateur en cas de besoin (abus)

CRU

ARREDU : solutions techniques

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

ARREDU/eduroam : architecture



ARREDU : une question de confiance

- Intervenants : utilisateurs, sites d'origine, sites visités, NRENs, Terena
- Confiance des visiteurs dans les sites visités :
  - Disponibilité du service
  - Infrastructure réseau
  - Administration réseau
  - Administration des serveurs Radius
  - Chiffrement des liaisons sans fil

Une question de confiance, suite

- Confiance des sites visités dans les sites d'origine :
  - Validation, choix et sécurisation de l'authentification
  - Information de leurs utilisateurs
  - Configuration de leurs équipements
  - support
- Confiance dans les NRENs, à commencer par Renater
  - Fiabilité et sécurisation de leurs réseaux

ARREDU : 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*

ARREDU : 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

ARREDU : engagements des établissements / Renater

- Ils doivent offrir le service conformément aux recommandations
- Administrer et sécuriser au moins un 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

ARREDU : état

- Phase pilote
- Un groupe de travail
- Un serveur national opéré par le CRU gérant le domaine *fr*
- Un serveur de backup géré par le CRC
- ~30 domaines

CRU

ARREDU : en cours

- Finalisation de la charte ARREDU
- Offrir les modifications d'agrément de Renater pour la mobilité
- Signer l'agrément Terena
- Mettre à disposition les procédures d'inscription des établissements
- Élaborer les spécifications techniques

ARREDU/eduroam : procédure d'adhésion

- Modification de l'agrément Renater
  - Nouveau service mobilité associé à une charte
  - Accessible dans SAGA
  - Désignation d'un « correspondant »
- Ouverture d'un « compte » ARREDU à la signature pour ce service
- Renseignements donnés par le correspondant via interface Web
- Échange secret partagé

Eduroam : en discussion

- Choix de SSID (en plus de *eduroam*)
- Réécriture des *policies* eduroam
- Eduroam-in-a-box
  - PA 802.1x
  - Serveur Radius
  - Interface de configuration
- Supplicant dédié eduroam
  - Basé sur wpa_supplicant
  - GUI

Perspectives

- GEANT2 : Joint Research Activity 5 (JRA5) :
  - Groupe de travail sur le nomadisme
  - Champ plus large que *TF Mobility*
  - Beaucoup de recoupements avec TF Mobility
- -> eduroam-NG

Eduroam-NG

- Défauts actuels :
  - Peu ou pas de notion d'autorisation
  - Toute une chaîne à traverser
  - Chaîne statique (pas de découverte dynamique)
  - Confiance basée sur secret partagé
- Pistes en cours d'exploration :
  - DIAMETER (standard, PKI, DNS)
  - RadSec (propriétaire, PKI, DNS)
  - Radius DNSSEC (DNSSec, pas de PKI)

Conclusion

- ARREDU/eduroam permettent un meilleur partage des infrastructures réseau
  - Avec une qualité de service garantie
  - Sans changer les habitudes des utilisateurs
  - à moindre coût
  - Au sein et au-dela du périmètre de Renater

Ressources

- Site ARREDU : http://www.cru.fr/nomadisme-sans-fil/arredu/index.html
- Liste de diffusion arredu@cru.fr : http://listes.cru.fr/wws/info/arredu
- Projet eduroam : http://www.eduroam.org/

CRU

Questions ?