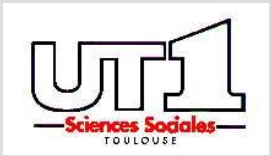
Eduroam

- Xavier Marty
- xavier.marty@univ-tlse1.fr
- Université Toulouse 1 Sciences Sociales



Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

Rappels

- TutoJRES n°3
  - http://www.jres.org/tuto/tuto3.php
  - Remerciements : C. Claveilera / V. Carpier

Constat

- L'accès à l'internet se démocratise.
- La mobilité devient un enjeu, un besoin, une nécessité !

Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

Eduroam : Projet

- Initiative de la TF Mobility de Terena en 2003
- Etude des problèmes de sécurité des réseaux sans fil
- Recommandations pour les solutions de nomadisme international pour les utilisateurs de réseaux académiques (NRENs)

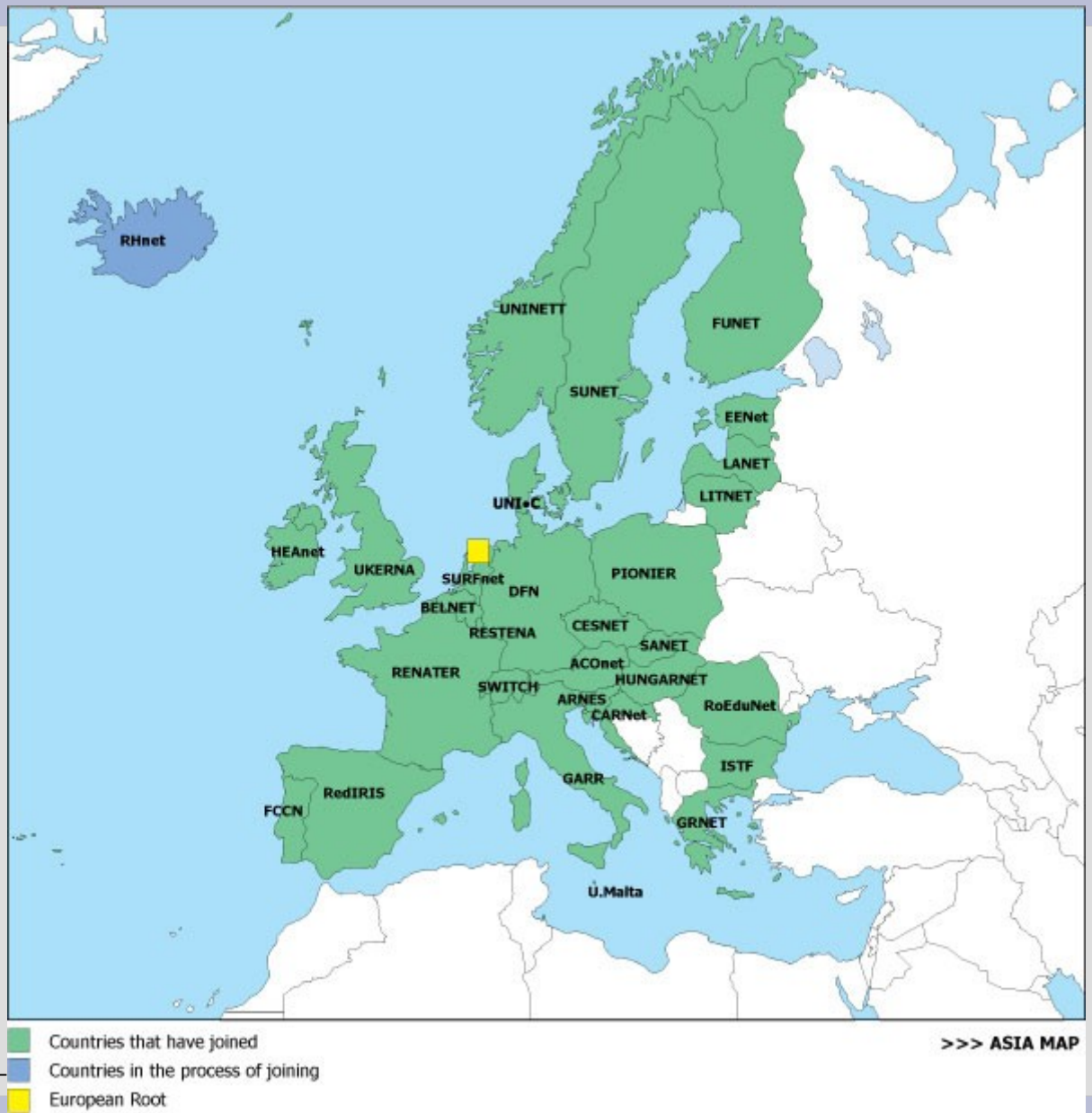
Eduroam : Buts

- Donner un accès internet aux utilisateurs nomades de l'Education et de la Recherche
  - Simplement
  - Sans surcroît d'administration
  - Sécurisé
  - Contrôlé
  - Facilement mis en oeuvre

Eduroam : Solution

- 802.1X + Radius
- Hiérarchie de serveurs Radius gérés par les NRENs ayant signé un agrément avec Terena
- Serveur racine géré par Terena

Eduroam : Europe

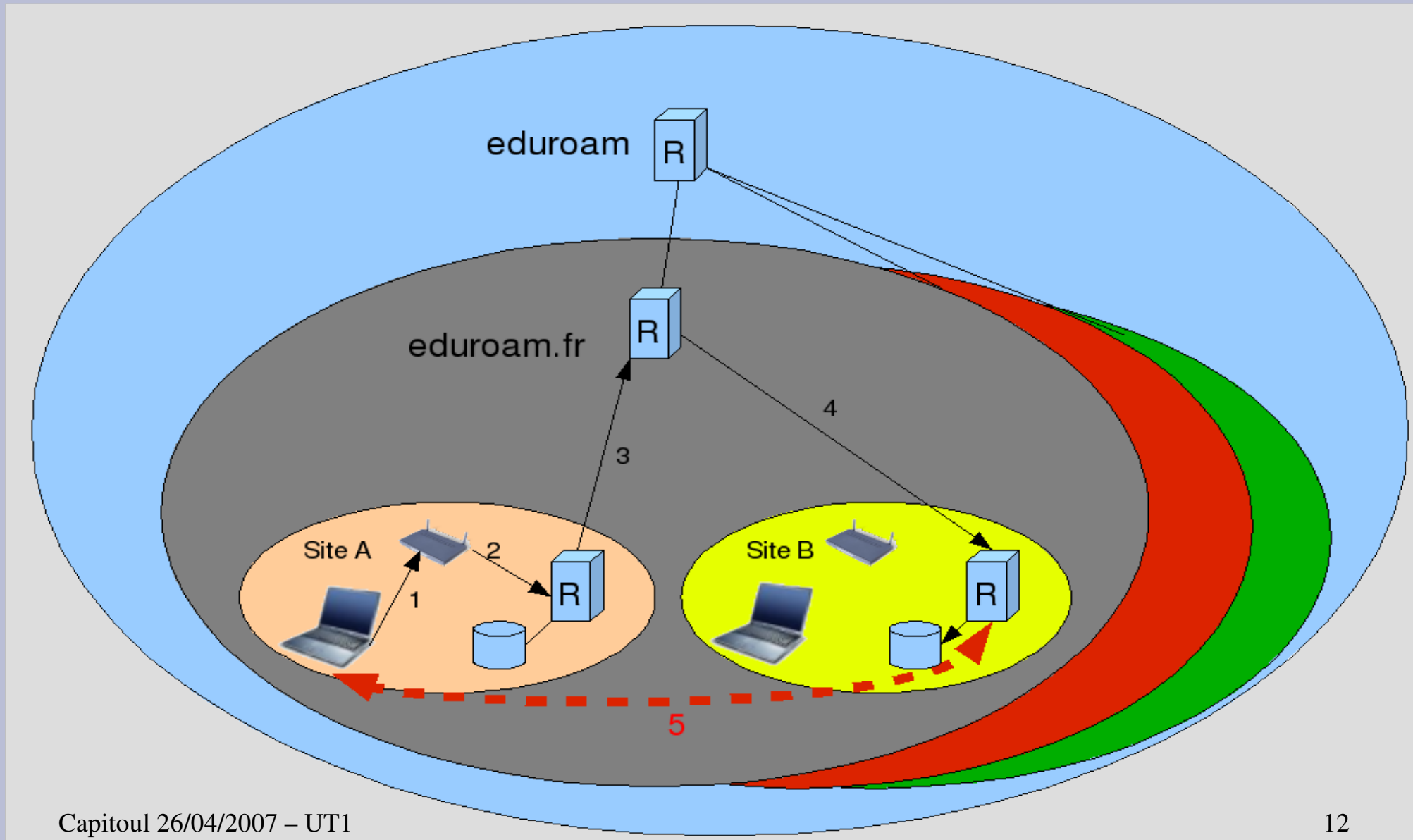


Eduroam : Asie/Pacifique

Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

Eduroam : Architecture



Eduroam : Méthode 1/3

- SSID
  - eduroam
- Authentification
  - 802.1X / EAP
  - Serveur Radius et proxy
- Portails captifs prohibés

Eduroam : Méthode 2/3

- Chiffrement
  - WEP dynamique avec rotation fréquente des clés
  - WPA ou WPA2
- Méthodes d'authentification sécurisées
  - PEAP
  - TTLS
  - TLS

Eduroam : Méthode 3/3

- Services à offrir
  - HTTP, HTTPs, DNS, ICMP (echo/reply), IPSec, OpenVPN, SSH, POPs, IMAPs, NTP, SMTP/AUTH, SMTP Local
- Monitoring
  - Création d'un compte de test pour le CRU

Eduroam : Engagements

- Offrir le service conformément aux recommandations
- Administrer et sécuriser le ou les proxy Radius
- Loguer
- Faire connaître le service en informant les utilisateurs sur le respect des règles d'utilisation des réseaux visités
- Offrir du support à leurs utilisateurs

Eduroam : Renater

- Les établissements s'engagent auprès de Renater
  - Signature de la Charte eduroam.fr/ARREDU associé au service mobilité
- Renater s'engage en leur nom auprès de Terena

Eduroam : France 1/3

- Service opérationnel depuis avril 2006
- Serveur national opéré par le CRU gérant le domaine fr
- Serveur de backup géré par le CRC

Eduroam : France 2/3

- Site dédié : http://www.eduroam.fr
- Carte :

Eduroam : France 3/3

- Monitoring

Surveillance nationale du service eduroam.fr

Surveillance du fonctionnement de l'infrastructure eduroam.fr, le 20/04/07 à 14:30:01 :

Nom	TTLS	PEAP	RADIUS
CIRIL / Centre Interuniversitaire de Ressources Informatiques de Lorraine	OK (0.31 s)	OK (0.40 s)	OK (implicite)
CRIHAN / Centre de Ressources Informatiques de Haute-Normandie	RADIUS_NOT_AVAIL		NOK
CROUS de Poitiers	NOP	NOP	NOP
CRU	OK (0.27 s)	OK (0.20 s)	OK (implicite)
Chancellerie des Universites de Paris - Sorbonne	OK (0.26 s)	OK (0.36 s)	OK (implicite)
ENS LSH		RAD_REJECT (3.23 s)	Reject (2.05 s)
Université de Toulouse 1	OK (0.32 s)		OK (implicite)

Eduroam : Sécurité

- Traçabilité
  - Journalisation des résultats d'authentification
  - Journalisation DHCP, NAT
  - Correspondance @IP / Utilisateur

Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

Contexte

- « Petit service réseau » :-)
- Etude WiFi préalable
- Validation du projet
  - CHS
  - CA
- Solution clé en main
  - Portail captif
  - Bornes
  - Equipement de management des bornes

Contexte : Pourquoi eduroam ?

- Mobilité accrue
- Simplicité d'a ccès
- Sécurité renforcée
- Visibilité de l'Univ ersité sur le plan international

Contexte : Mobilité pour qui ?

- Initialement
  - Tout le monde
- En pratique
  - Etudiants suivant une formation dans plusieurs établissements
  - Enseignants / Chercheurs qui se déplacent et interviennent dans plusieurs lieux

Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

Mise en oeuvre : Adhésion

- Ouverture d'un compte Saga
- Acceptation de l'agrément Renater
- Déclaration du correspondant
- Accès et personnalisation via l'interface web du CRU

Mise en oeuvre : Radius

- Deux radius (FreeRadius)
  - Un radius pour l'authentification en Portail Captif et en 802.1X interne
  - Un radius frontal pour l'authentification eduroam permet le filtrage du Portail Captif
- Modification du proxy.conf
  - Configuration fournies par eduroam

Mise en oeuvre : LDAP

- Rajout de champs pour définir les vlans des utilisateurs
  - Chercheurs
  - Enseignants / Personnels
  - Etudiants

Mise en oeuvre : Paramétrage des bornes

- Mise en places des SSIDs
  - Ouvert
    - Pour le portail captif
    - Pour les documentations en ligne
  - Sécurisé (mais non visible)
- Gestion des vlans
  - Pour chaque groupe d'utilisateurs pour des autorisations spécifiques
- Actions journalières
  - Arrêt du service WiFi la nuit

Mise en oeuvre : Test

- Test avec le CRU
  - Mise à disposition d'un user par le CRU
    - Test avec radtest et client EAP
  - Vérification du blocage du portail captif
  - Mise à disposition d'un user local pour le monitoring
- Test avec un autre établissement
  - Même principe de test

Mise en oeuvre : Spécificité UT1

- SSID eduroam non broadcasté
  - Contrainte technique
- Méthode EAP / TTLS
  - Encryption en WPA et WPA2
  - Authentification sur l'annuaire ldap via le radius
  - Vlan spécifique pour les personnes extérieures
- Choix des clients
  - SecureW2
  - Intel ProWireless

Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

Informations : Signalisation

- Panneaux indicateurs des zones
  - Zone WiFi eduroam
  - Lieu de passage et de travail
    - Bibliothèques
    - Cafétérias
    - Halls / Salles de réunion

Informations : Documentation

- Pages Web
  - Authentification
  - Charte
  - Aide et documentation sur les méthodes et mise oeuvre possible du service
  - Recommandations (Charte, Sécurité, ...)
  - Horaires d'ouverture du service
  - FAQ
- Document papier mis à disposition par le service pédagogique

Informations : Support 1/2

- Moniteur
  - Pour les étudiants
  - 4 demi-journées par semaine
  - Enrichissement FAQ
  - Travail quotidien
    - Entre 4 et 8 étudiants par jour
    - Entre 15 et 30 minutes pour résoudre un problème
- Service informatique
  - Pour les personnels
  - Pour les étudiants après avoir vu le moniteur

Informations : Support 2/2

- Difficultés rencontrées
  - Problèmes pour l'activation de la carte WiFi
    - Matériels et logiciels
    - Conflit avec les configurations personnelles
  - Problèmes de pilotes
    - Mise à jour
  - Problèmes spécifiques de certaines cartes
    - Désactivation automatique
  - Infections de poste
    - Virus
  - Code d'accès inconnus

Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

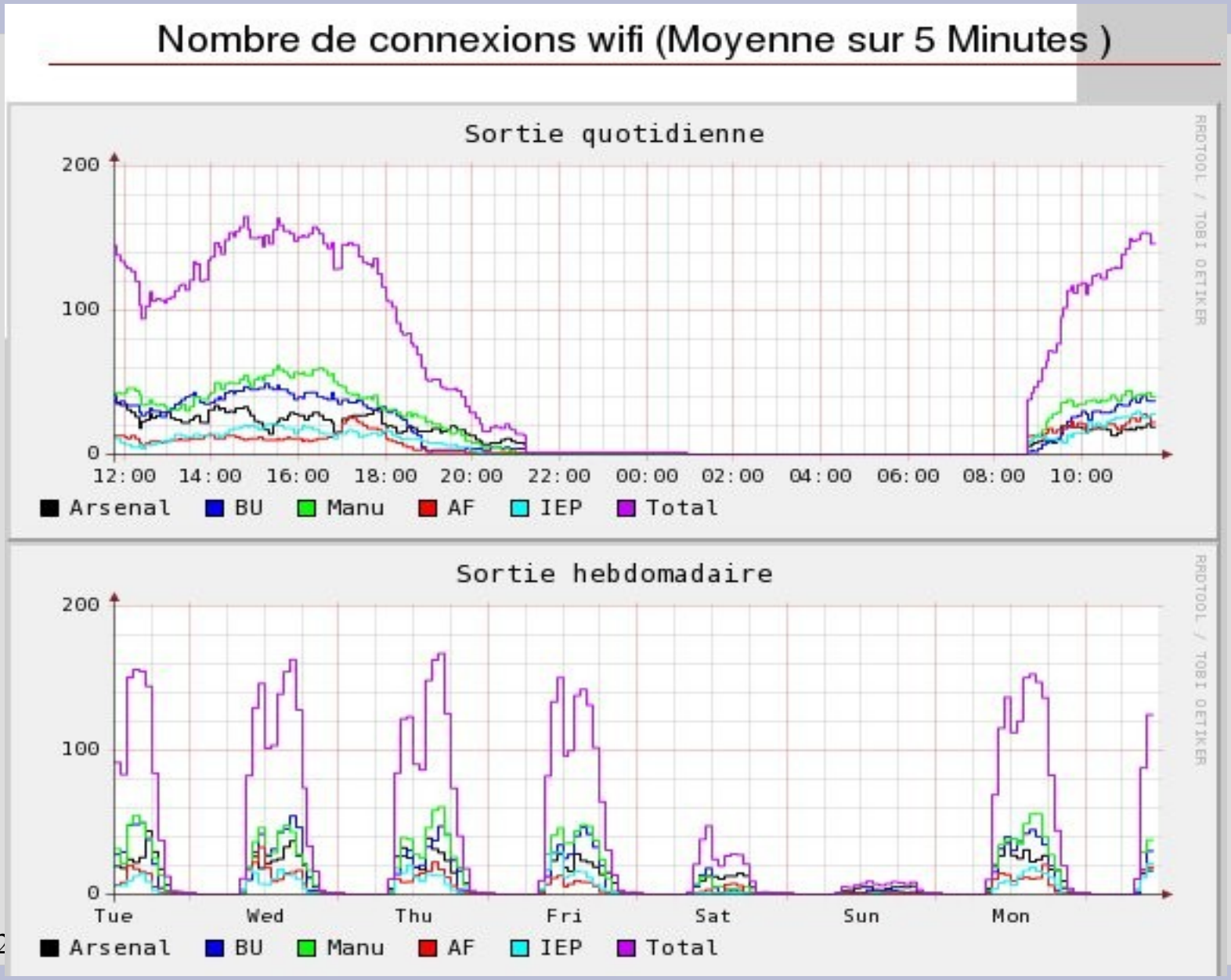
Quotidien : Exploitation

- Vérification de l'état des bornes
- Activation du service
- Déploiement de bornes supplémentaires
  - Bornes temporaires
- Création de comptes temporaires

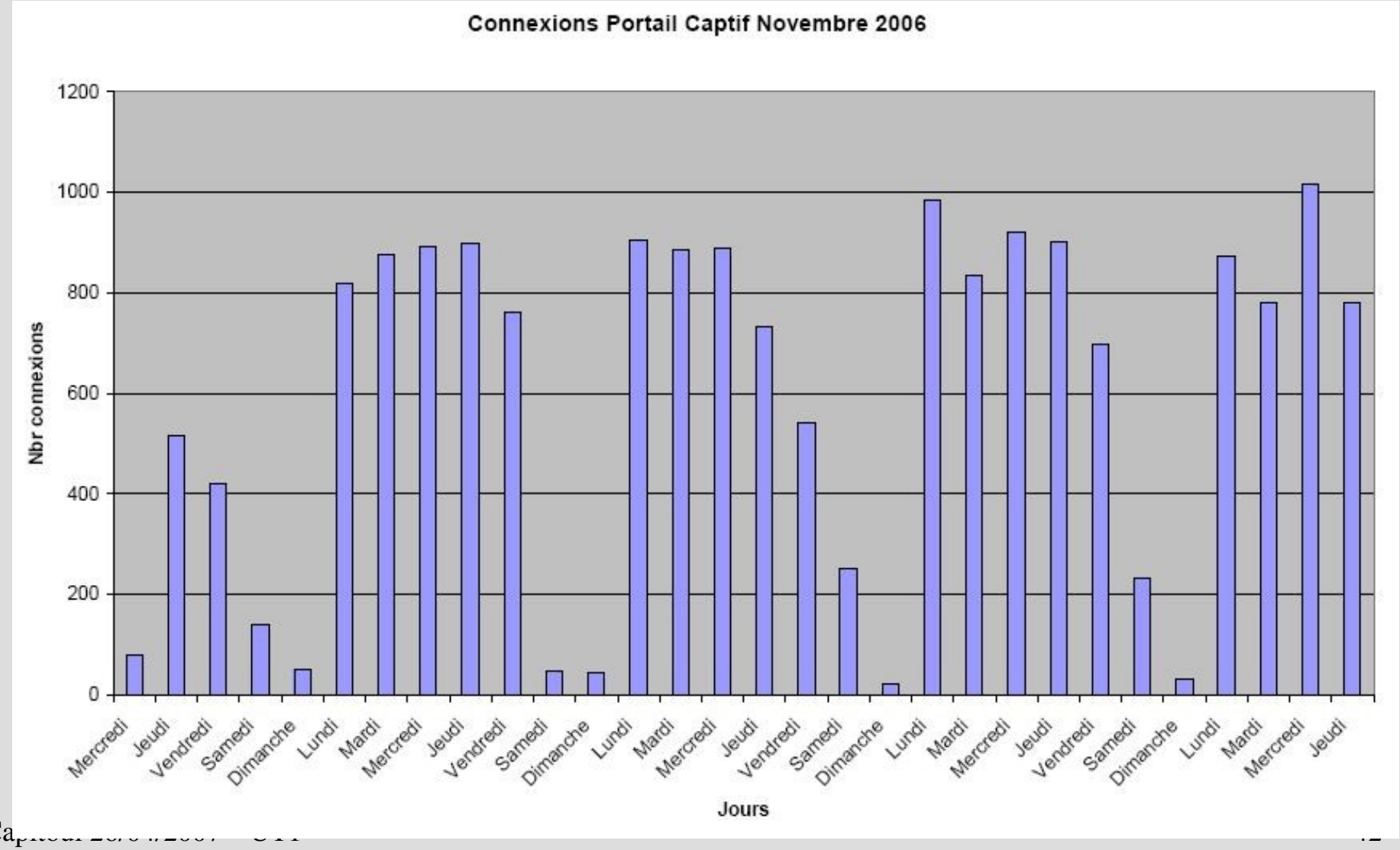
Quotidien : Surveillance

- Détection de bornes ou ordinateurs parasites
  - Rogues AP
  - Ordinateurs configurés en ad hoc
- Blocage des postes infectés
  - Mise en quarantaine
  - Information
- Journalisation des connexions
- Statistiques

Quotidien : Statistiques 1/2



Quotidien : Statistiques 2/2



Problèmes rencontrés

- Propagation de multiples SSID et affectation automatique de vlan
- Propagation du user de test du service
- Opération de maintenance ou mise à niveau du service
  - Si possible la nuit, pour des mises à jour de configuration des bornes
  - Mise en place d'un 2nd radius suite aux directives d'eduroam

Problèmes rencontrés

- Horaire d'ouverture du service WiFi
  - Problème pour les concierges pour faire sortir les étudiants lors de la fermeture des locaux
  - Modification des plages d'ouvertures durant les vacances

Plan

- Eduroam : Présentation
  - Présentation générale
  - Aspects techniques
- Eduroam : UT1
  - Contexte
  - Mise en oeuvre
  - Informations sur le WiFi
  - Quotidien
  - Bilan

Bilan : Service WiFi

- Déploiement
  - Opérationnel depuis avril 2005
- Utilisation
  - Augmentation constante
    - Plus de 800 connexions / jour
    - Plus de 100 connexions / week-end
  - Nécessité d'avoir une personne dédié pour le support

Bilan : Eduroam

- Déploiement
  - Rapide pour nous
    - Système d'information opérationnel
    - 802.1X déjà présent
  - Opérationnel depuis début 2006
- Service
  - Fonctionnement simple s'il s'agit de l'unique utilisation
  - Intervention contraignantes sur les postes étudiants
  - Contexte local : Mobilité à l'échelle régionale
    - Problématique : Peu d'entités raccordées à eduroam en Midi-Pyrénées
    - Solution : Service complémentaire de mobilité régionale MIP-WiFi

Bilan : Avenir

- Augmentation du nombre de bornes
- Réflexion sur un déploiement du 802.1X sur les prises filaires
- Changement de Portail Captif
  - Shibboleth
  - NoCatAuth
  - cf Echo du CRU n°6

Conclusion

- Quels sont les pré-requis pour mettre en place eduroam ?
  - Un radius opérationnel
  - Une gestion du 802.1X
- Quel avenir pour la mobilité
  - Eduroam se démocratisera dès que :
    - Le nombre d'entités ainsi que le nombre de points d'accès seront conséquents
    - L'utilisation sera simplifié

Questions ?