Authentification sur Osiris

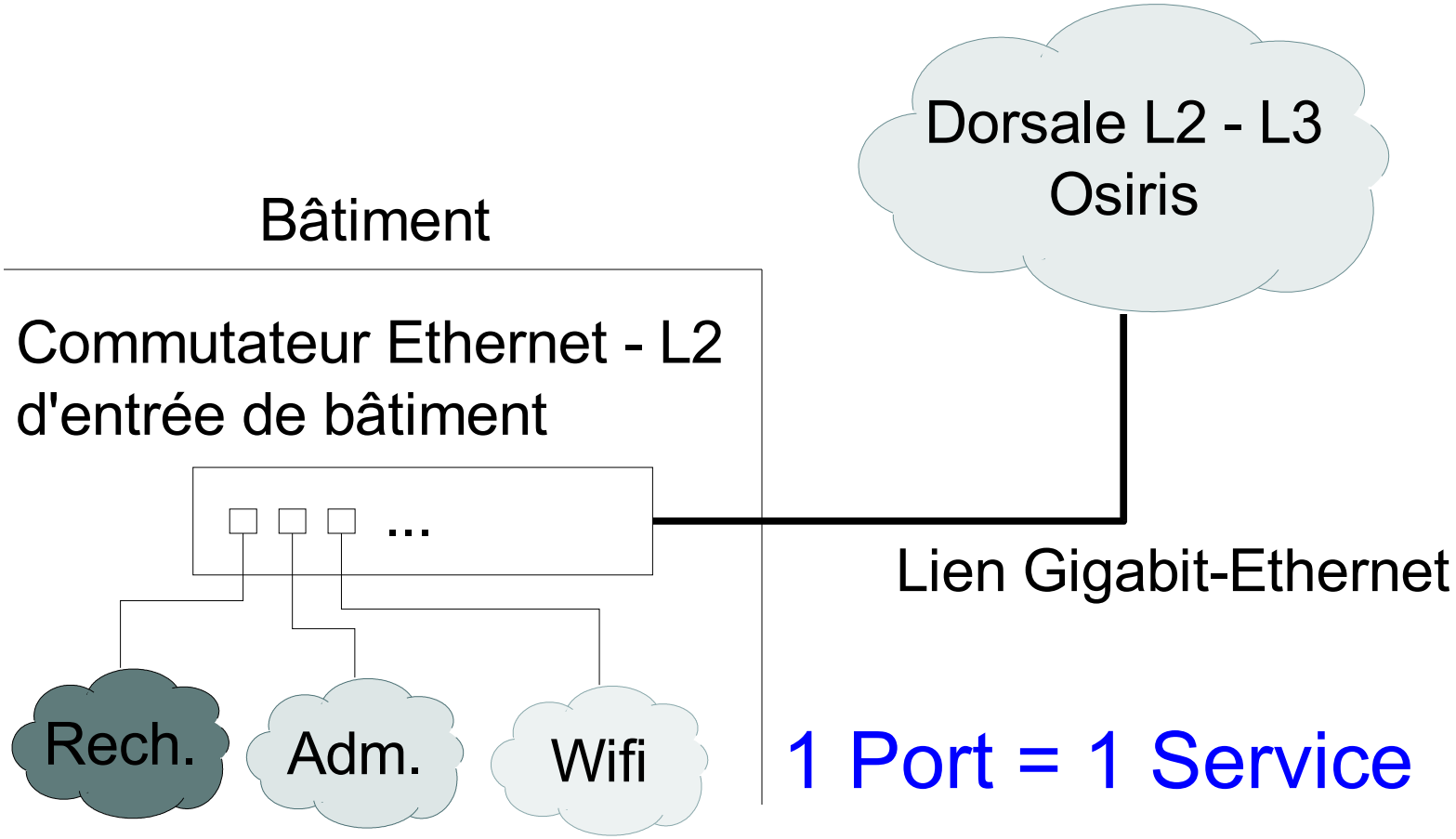
Centre Réseau Communication
Jean Benoit, Alain Zamboni, Pierre David

Introduction – Contexte

- Le réseau *Osiris* strasbourgeois, c'est :
  - 17 établissements
  - ~110 bâtiments raccordés
  - ~20 000 ordinateurs
  - ~50 000 utilisateurs potentiels
- Un long historique de mutualisation
  - Un opérateur de réseau : le CRC
  - Osiris est « le réseau d'établissement » de la plupart des établissements
  - Centralisation de services (routage IP, filtrage, relayage mail, hébergement mail, etc.)

Introduction – Contexte

- Le modèle « Osiris »



Introduction – Contexte

- Des projets numériques
  - Un des 4 projets d'ENT (EPPUN)
  - Une UNR (UNERA) pour 7 des 17 établissements
  - Niveau d'utilisation des briques variable
    - Ex: l'INSA n'utilise pas aujourd'hui Univ/R
- EPPUN
  - Socle géré par le SIIG (Service Interuniversitaire d'Informatique de Gestion)
  - Constitution d'un méta-annuaire, utilisé pour l'authentification des applications EPPUN
- D'autres établissements ont leur annuaire

Nouveaux services du CRC

- Trois nouveaux services majeurs
  - VPN
  - Wifi
  - Hébergement de boîtes aux lettres (enfin, c'est pas vraiment nouveau, on en gérait déjà ~3 000)
- Population cible : ~50 000 utilisateurs
  - Potentiellement : tous les établissements, étudiants y compris

Nouveaux services du CRC

- VPN
  - Objectif premier : faire la peau aux modems tout en offrant l'accès aux ressources Osiris (SCD)
  - Validation par le comité de pilotage Osiris
  - Ouverture du service : depuis 2004
  - Évolution depuis mai 2005 : accès dans un VLAN spécifique par composante ou labo
  - Cisco 3725 + IPSec/XAuth + FreeRadius

Nouveaux services du CRC

- Accès sans-fil
  - Initiative ULP, prolongée par l'Unera, à laquelle se joignent d'autres établissements
  - Une seule infrastructure Wifi : réseau transversal inter-établissements, gestion centralisée par le CRC
    - Le CRC « rentre » à l'intérieur des bâtiments
    - Validé par le Comité de Pilotage Osiris (la plupart des établissements y adhèrent)
  - Actuellement : 100 AP, 200 AP à la rentrée 2005
  - Deux types d'accès (IPv4 et IPv6)
    - Avec client IEEE 802.1X + EAP/TTLS + FreeRadius
    - Avec browser Web + portail captif (maison) + FreeRadius

Nouveaux services du CRC

- Accès sans-fil (suite)
  - SSID « osiris » : portail captif (droits restreints) + accueil 802.1X
  - SSID « osiris-sec » : accès 802.1X
    - 1 grand VLAN par défaut
    - 1 VLAN spécifique par composante

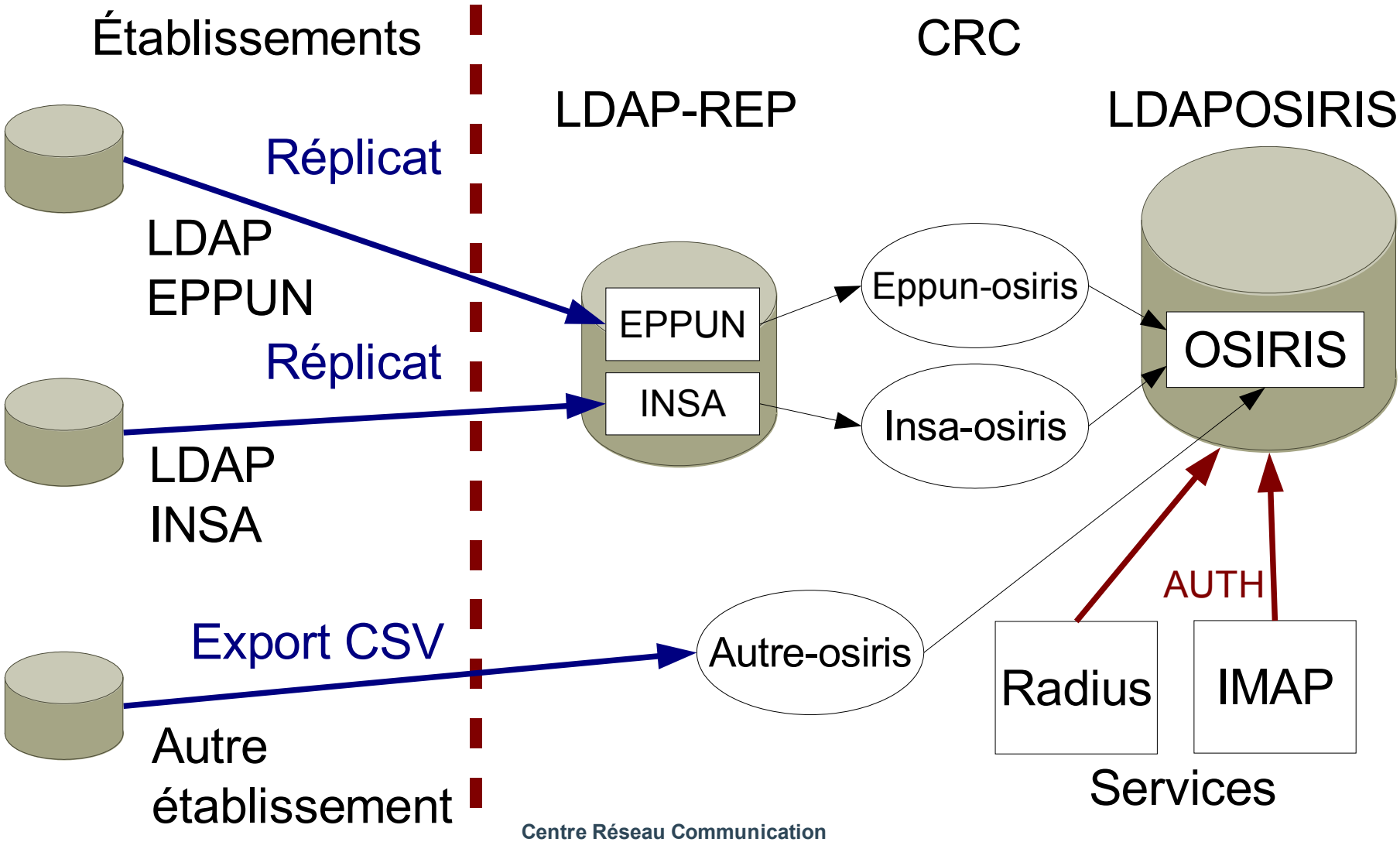
Nouveaux services du CRC

- Hébergement de messagerie
  - Volonté de quelques établissements de rationnaliser la gestion de leur messagerie
  - Objectif : pleine charge à la rentrée 2005
  - Changement d'échelle
  - Sendmail + Courier-imap + IMP + OpenLDAP

Architecture – Objectifs

- Services tous authentifiés (pas de Wifi ouvert)
- Disponibilité : 99,9 % (comme le reste d'Osiris)
- Même login/mot de passe (pas de « realm »)
  - Base de comptes centralisée
  - Unicité du login dans l'espace de nommage Osiris
- Utilisation des annuaires d'établissements...
  - ... quand ils existent
  - ... complétés par des informations additionnelles
    - Ex : VLAN Wifi, IP fixe pour le VPN, adresses mail supplémentaires, etc., via une interface Web

Architecture



Divers – Wifi

- Comptes « invités »
  - CDD (Comptes à Durée Déterminée) ouverts à la demande (via le Web) par les correspondants réseaux
  - VLAN paramétrable par le correspondant (VLAN de la composante ou VLAN par défaut)
- Mode « conférence »
  - CDD ouvert avec :
    - Autorisation de login multiple
    - Validité : 1 jour
    - Login et passwd = nom de la conf
  - VLAN par défaut

Conclusion

- Système en cours de mise en place
  - Les fondations sont là
  - Montée en charge progressive
  - Pas encore beaucoup de recul
  - Reste à réaliser : fiabilisation/redondance (FreeRadius + OpenLDAP)
- Architecture
  - Pensée dès le départ pour ~50 000 utilisateurs
  - Extensible : nouveaux établissements et services
  - Extensible : projet Arredu