



Wifi labo pour tous ? vs IHP

Anne ALVAREZ – IHP Paris

Journées Mathrice Marseille 31/03/2015

PLAN


- 1 – Le wifi à l'IHP
- 2 – Où est le problème ?
- 3 – Etat des lieux
- 4 – Une solution possible ?
- 5 – Critiques - Réflexions
- 6 – Des idées ... ?


Le wifi à l'IHP

11 bornes Cisco AP1142N : 2 par étage, 3 au RDC

Pas de centralisation de la configuration : telnet sur chaque borne

2 réseaux pour tout le bâtiment :

 **eduroam** : authentification par le serveur radius de l'UPMC
protocole de chiffrement AES-CCM
adresses IP attribuées publiques, vlan 134.157.87.128/25

 **IHP** : pas d'authentification
mot de passe de type WPA changé tous les 3 mois
protocole de chiffrement TKIP
adresses IP attribuées publiques, vlan 134.157.88.0/24

Où est le problème ?

CE QUE DISENT LA LOI ET LE CNRS :

- en cas de délit, les traces doivent permettre d'identifier l'auteur du délit (décret n°2006-358 du 24 mars 2006, article 1)
- conserver nom de famille, prénoms, adresse postale, adresses électroniques, coordonnées téléphoniques, adresse de l'installation téléphonique de l'abonné (décret n°2010-236, article 2, annexe)
- conserver pendant un an des traces conformes à la loi informatique et libertés (www.cil.cnrs.fr/CIL/IMG/pdf/Po_gest_traces.pdf)

CE QU'ON RISQUE :

- sanctions pénales pour le DU (amende, contrainte pénale, emprisonnement...)
- sanctions disciplinaires pour l'ASR s'il n'a pas respecté les préconisations de son administration (avertissement → révocation)

PERSONNES SUSCEPTIBLES DE SE CONNECTER

- 1 - personnel IHP => eduroam
/etc/passwd
- 2 - invités ayant un bureau à l'IHP
/etc/passwd
- 3 - invités sans bureau
- 4 - lecteurs de la bibliothèque
- 5 - personnel et visiteurs des
sociétés savantes et associations
- 6 - visiteurs de l'enseignement
supérieur et la recherche => eduroam
- 7 - autres visiteurs :
personnes du secteur privé, retraités

RESSOURCES DEMANDEES

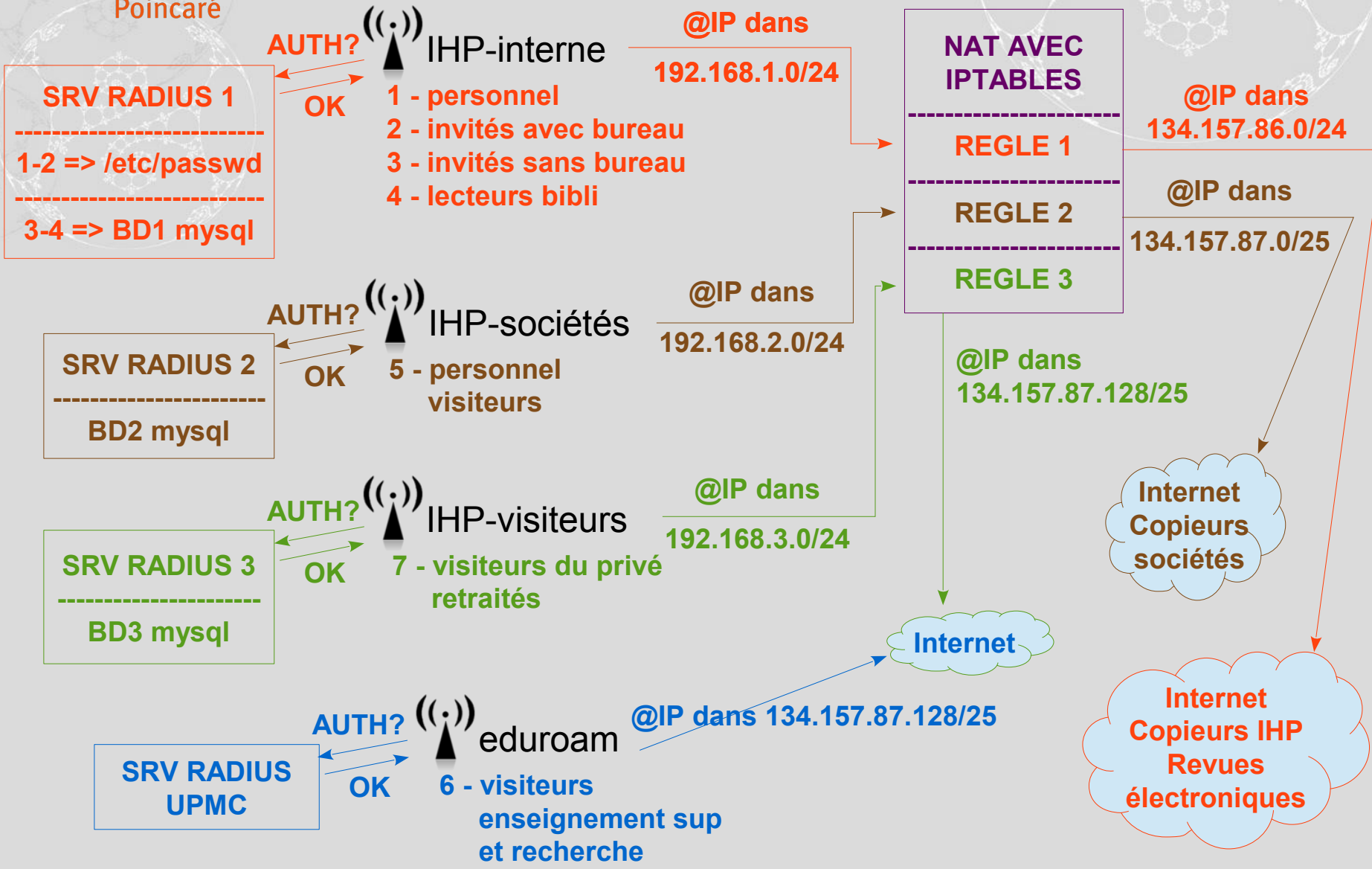
Internet/messagerie

Impression réseau IHP

Impression réseau sociétés

Revue électronique

Une solution possible ?



INCONVENIENTS DE LA SOLUTION :

- architecture complexe et fragile
- n'intègre pas les postes en libre service
- nécessite le développement d'interfaces de saisie des comptes
- demande une réorganisation des services pour la création des comptes

LES QUESTIONS QUE JE ME POSE :

- intégrer dans l'architecture un portail captif ?
- pour les comptes non Unix, choisir ldap ou mysql comme base d'authentification ?
- existerait-il une solution plus simple, peu contraignante pour les utilisateurs, permettant d'identifier les personnes connectées ?

Des idées ...?

A VOUS LA PAROLE ...

Merci de votre attention :-)