Lothaire

CRIL

Yet an other Captive Portal

Un portail captif mutualisé pour les Universités et établissements lorrains

JRES 2007

21 novembre 2007

Alexandre.Simon@ciril.fr
Loic.Barreau@ciril.fr
Sebastien.Morosi@ciril.fr

Au programme

- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

Introduction

- Les réseaux gérés couvrent l'ensemble des populations universitaires, grandes Ecoles et établissements de recherche de la Lorraine
  - 4 Universités (UHP, Nancy2, INPL, Paul Verlaine), IUFM, Rectorat, CROUS, CNRS, INRA, INRIA, ...
- Transversalité des populations et nomadisme des utilisateurs
  - un étudiant ou un personnel d'Université a sans doute besoin du réseau sur un autre site que celui de son établissement
  - EPCS : *Nancy-Université*
    - fédération des 3 Universités nancéennes
    - mutualisation de services
    - volonté d'offrir les mêmes services réseaux à toutes les populations
    - volonté de faciliter le nomadisme réseau

Au programme

- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

Historique, besoins et choix

- YaCaP, un peu d'histoire...
  - fin 2004, début 2005
  - les déploiements de bornes et de réseaux *wifi* s'accélèrent
  - ce type de réseaux « ouverts » nécessite un minimum d'authentification avant accès au réseau
  - les solutions de type 802.1X trop contraignantes et trop récentes sont mises de côté
  - une étude sur les portails captifs et leurs fonctionnalités est lancée
  - un cahier des charges est retenu et comparé aux portails captifs existants
  - aucun portail captif existant n'est totalement satisfaisant
  - le développement « maison » de YaCaP débute en février 2005

Historique, besoins et choix

- Les portails captifs étudiés et comparés
  - *m0n0wall*, *chillispot*, *NoCatAuth* et *UCOPIA*
- Besoins et fonctionnalités

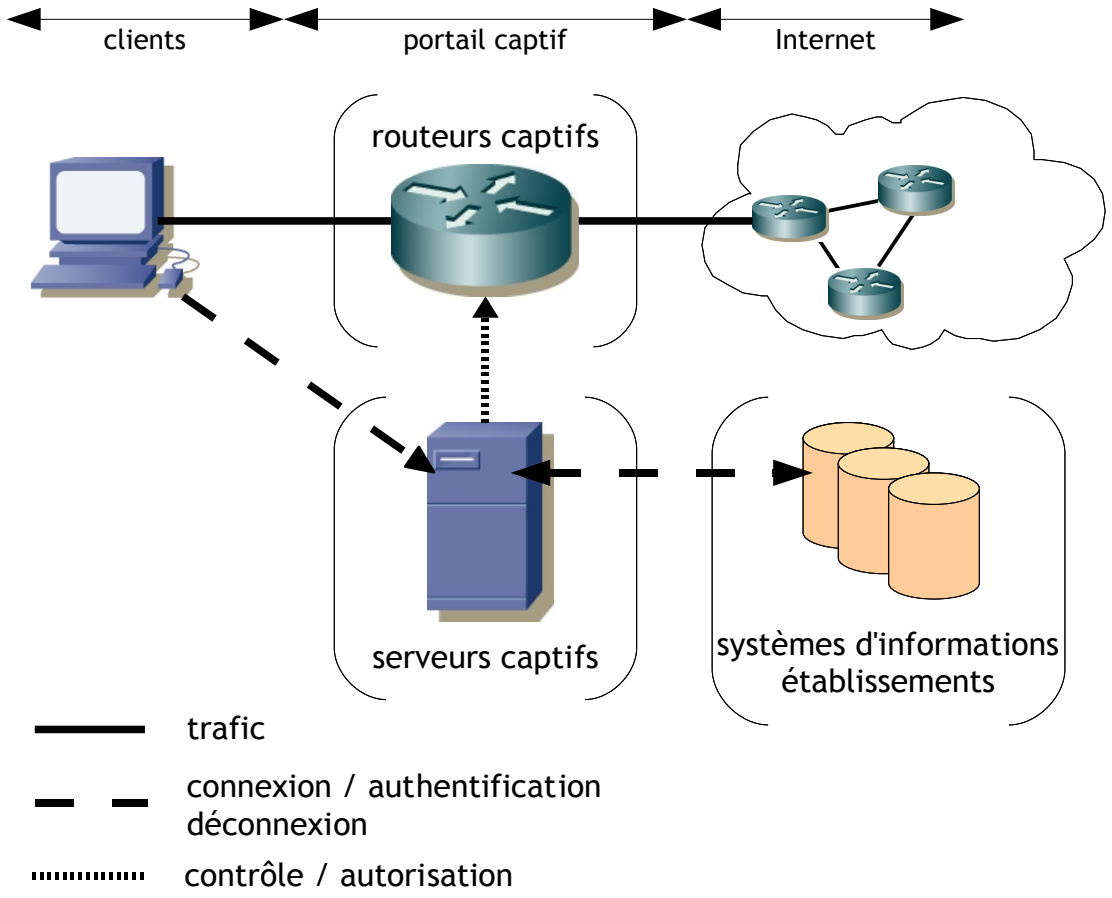
Besoin / Fonctionnalité	Type
Positionnement client/Internet	pas une « simple » machine en « rupture » s'intégrer à l 'existant facilité de passage à l'échelle
Type de réseaux supportés	niveau 3 : filaire et wifi
Technologie de filtrage	matérielle
Authentifications/autorisations	support de CAS / LDAP / RADIUS support authen/authz multi-établissements possibilité de délégation sur SI d'établissement granularité fine des accès
Contraintes côté poste client	limiter les contraintes solution « universelle »
Journaux d'activités	exportation des logs vers établissements possibilité de « croisement » des informations
Haute disponibilité	robustesse évolutivité
Passage à l'échelle	prise en compte de « petites » à « grandes » infrastructures

Au programme

- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

Architecture / Infrastructure

- Principe général

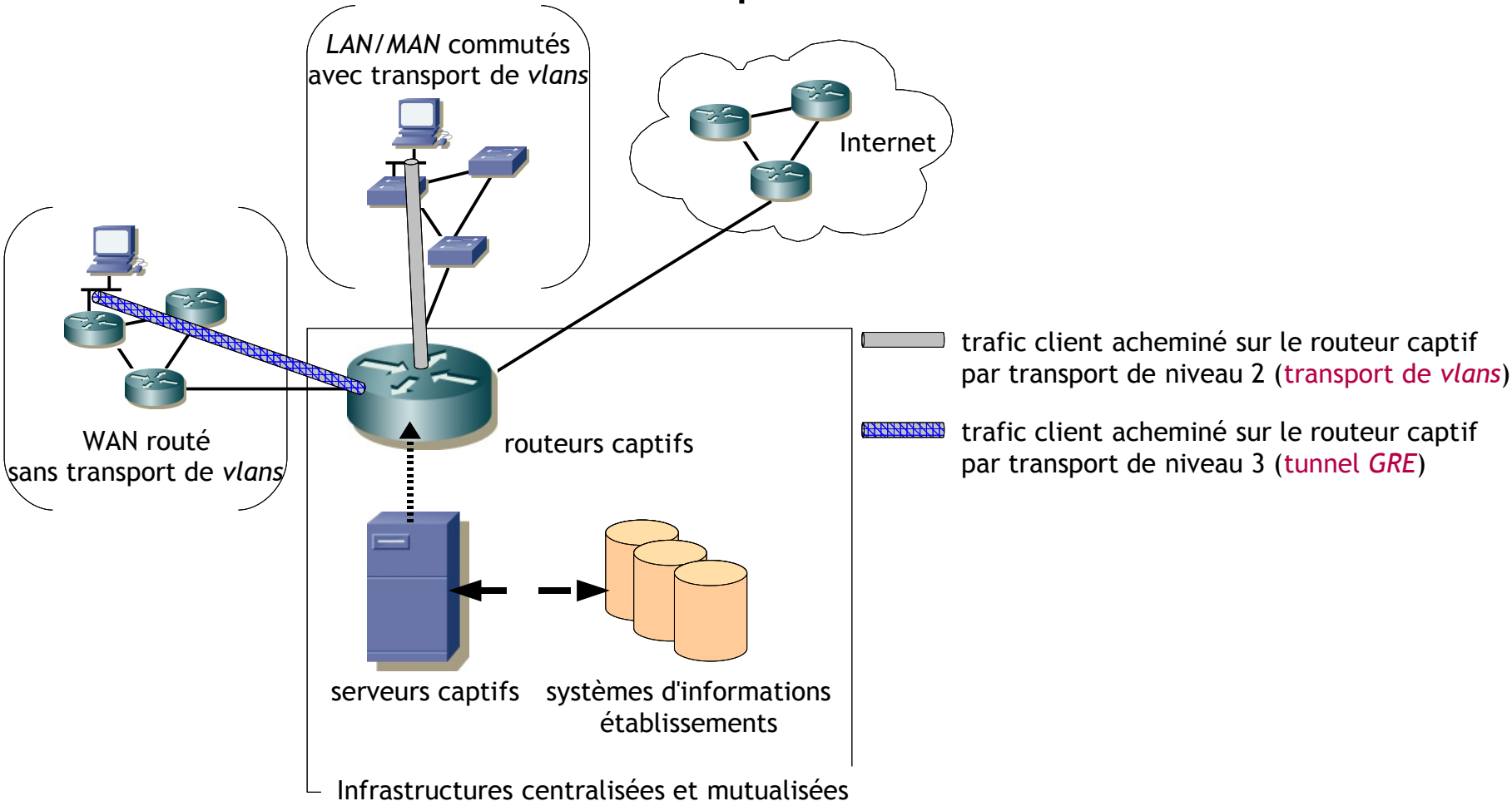


Architecture / Infrastructure

- Principe général
  - utiliser des routeurs matériels (routeurs captifs)
    - pour autoriser
    - et pour router les flux *IP*
  - utiliser des serveurs applicatifs
    - pour authentifier/autoriser les utilisateurs
    - et pour piloter « à la volée » les routeurs captifs
- De l'originalité à la souplesse
  - solution de routage/filtrage matérielle « connue »
  - pas de limitation sur le type/nombre/localisation des routeurs
  - pas de limitation sur le nombre de serveurs captifs
  - interface authen/authz générique pour prise en compte « large » des *SI* d'établissement
  - réseau captif de niveau 3 : possibilité de gestion centralisée

Architecture / Infrastructure

- Mutualisation centralisée / postes clients sur *MAN/WAN*



Au programme

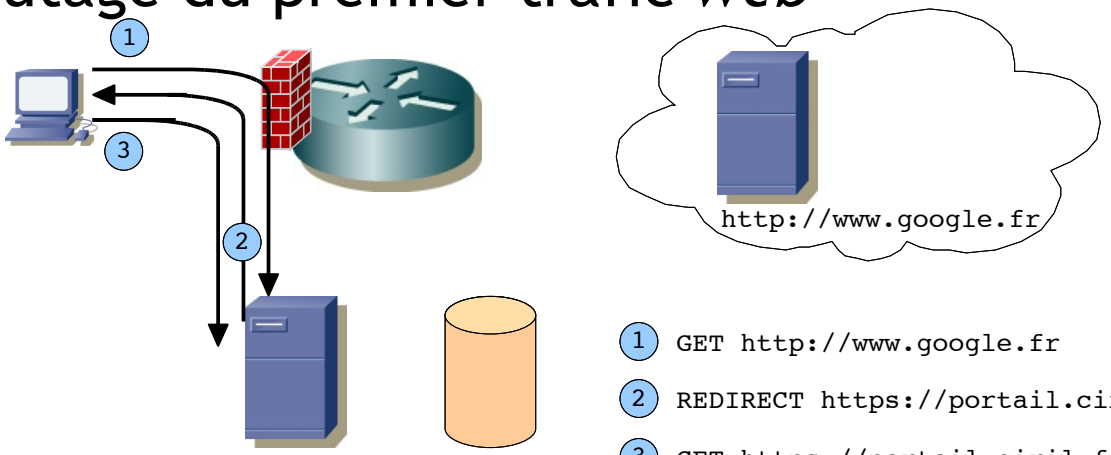
- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

Fonctionnement

- Prérequis
  - réseaux : *IPv4*, pas de protocole ou mécanisme particulier
  - postes clients : pile *TCP/IPv4*, *DHCP*, navigateur web avec support des *popups*, *cookies* et *javascript*
- Sécurisation des échanges entre clients et portail
  - à la charge du portail : tout en *HTTPS*
  - à la charge du réseau de l'établissement : possibilité de sécurisation du médium (*WEP*, *WPA*, *802.1X*, ...)
  - à la charge de l'utilisateur une fois connecté : possibilité d'utilisation de *VPN*, *HTTPS*, ...
- Auto-configuration poste client
  - serveur DHCP central avec « poussage » des paramètres propres au réseau captif utilisé

Fonctionnement

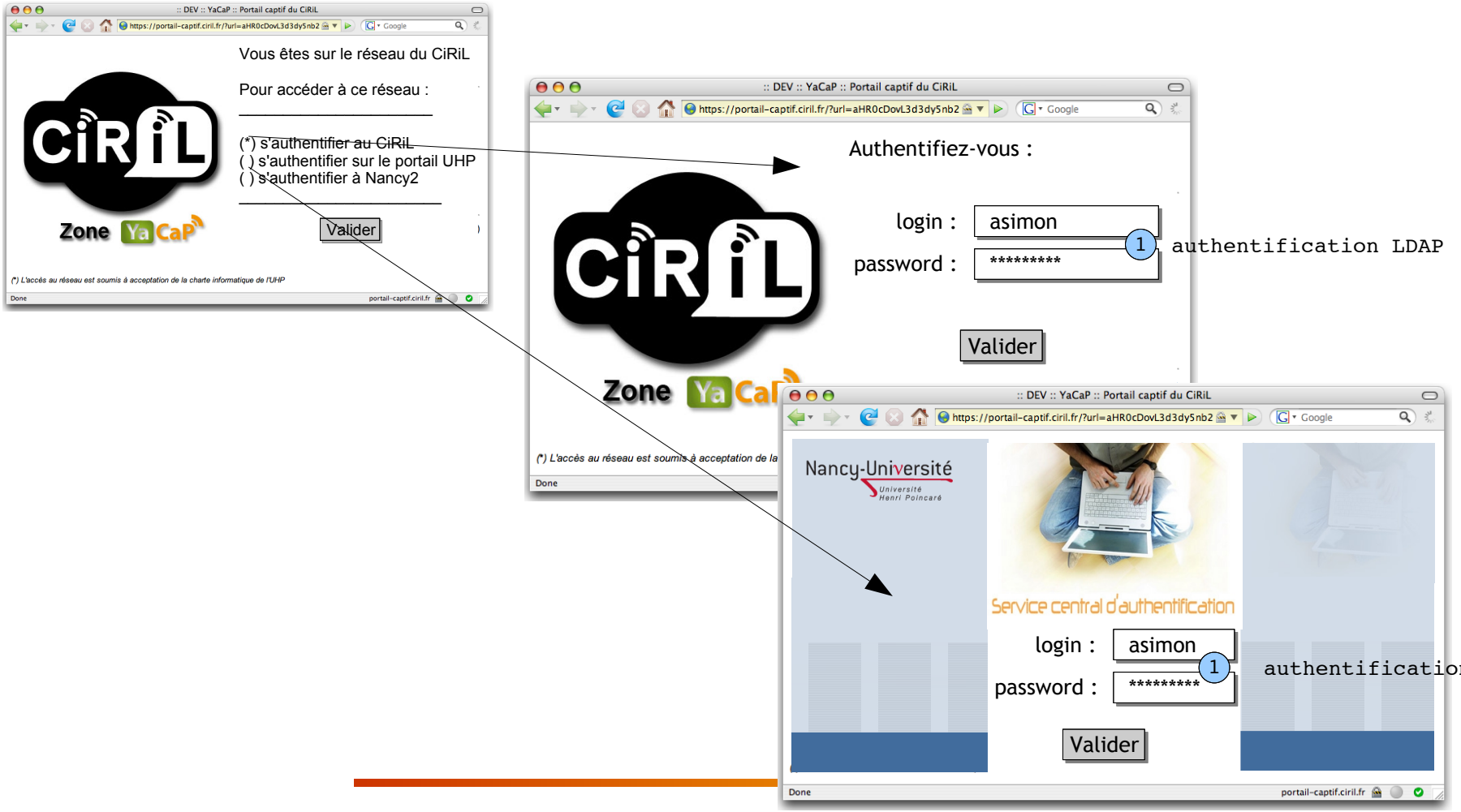
- Déroutage du premier trafic *web*



1. `GET http://www.google.fr`
2. `REDIRECT https://portail.ciril.fr`
3. `GET https://portail.ciril.fr`

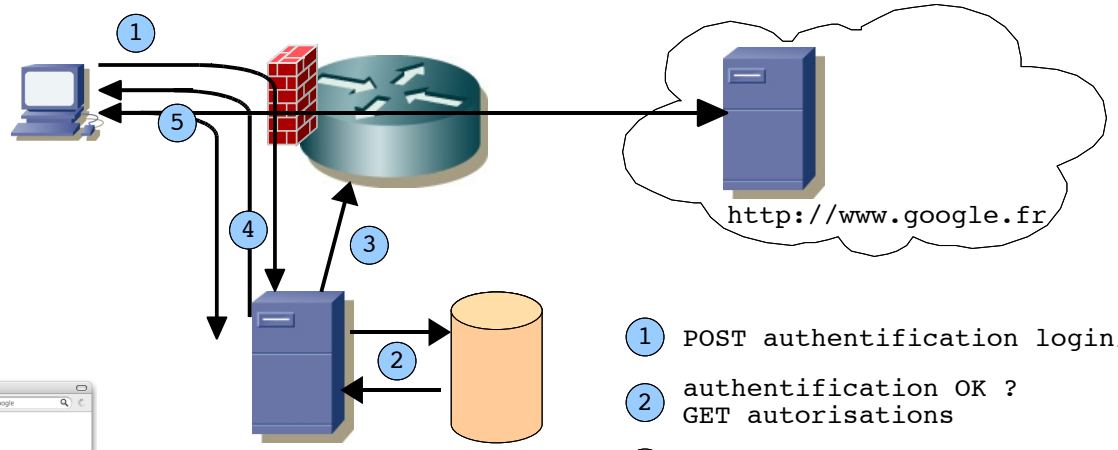
Fonctionnement

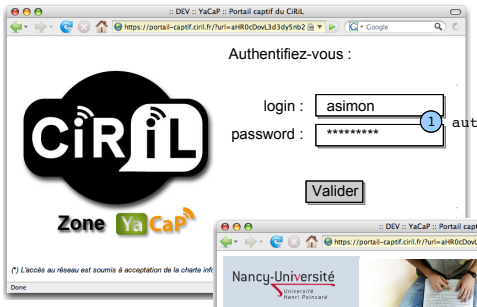
- Qui suis-je ? Où dois-je m'authentifier ?



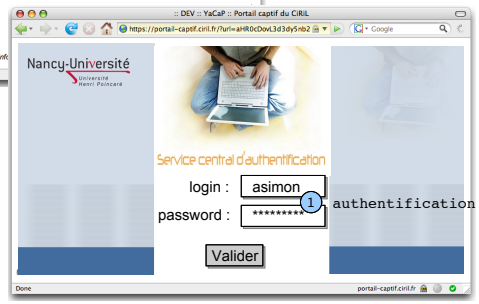
Fonctionnement

- Authentification, autorisation et utilisation





1 authentification LDAP

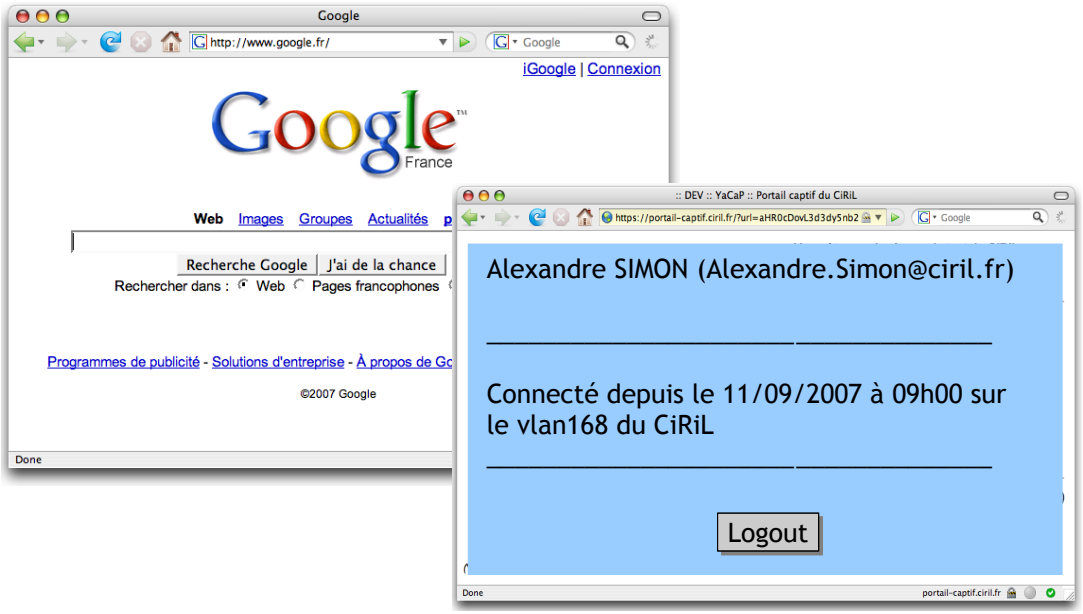


1 authentification CAS

1. POST authentification login/password
2. authentification OK ?
   GET autorisations
3. SET autorisations
4. SET cookie + popup
5. trafic <-> http://www.google.fr
   REFRESH popup

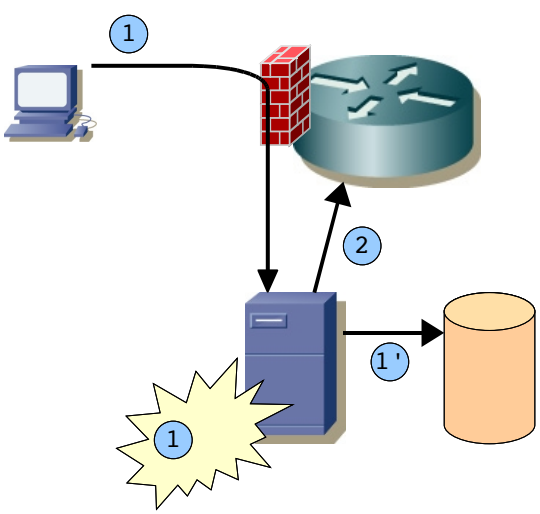
Fonctionnement

- Utilisation du réseau et maintient de session par *popup*



Fonctionnement

- Déconnexion



1 POST logout ou time-out

1' SET logout (si CAS)

2 DEL autorisations

Au programme

- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

Systèmes d'information

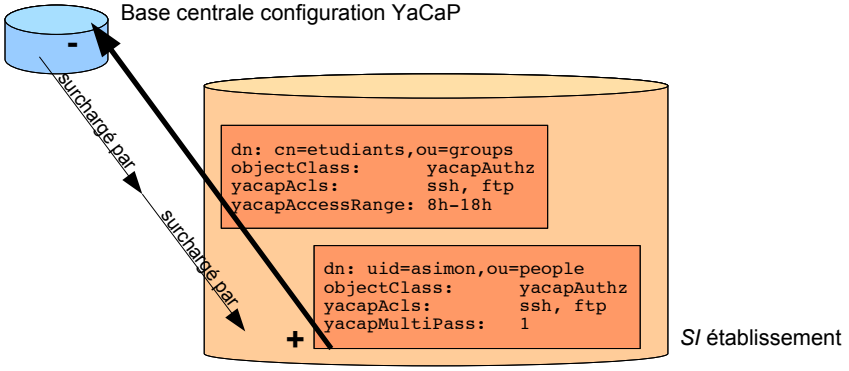
- YaCaP a été conçu pour déléguer les authentifications/autorisations aux établissements et pour supporter les interrogations *CAS*, *LDAP/AD*, *Shibboleth* et *Radius*
- Implémentations réalisées :
  - authentification
    - *CAS* : ok
    - *LDAP/AD* : ok
    - *Radius* : partielle
    - *Shibboleth* : non
  - autorisation
    - *LDAP/AD* : ok
    - *Radius* : partielle
    - *CAS* : non applicable
    - *Shibboleth* : non

Systèmes d'information

- Paramètres de configuration d'un *vlan* captif
  - non-surchargeables, définis uniquement en central
    - routeur / interface / *subnet*
    - paramètres *DHCP*
    - *templates HTML*
    - *URL* de déroutage du premier trafic *web*
    - *access-list* avant authentification
  - surchargeables, définis en central et en option dans le *SI* de l'établissement
    - *access-list* après authentification
    - horaires d'accès autorisés
    - *soft timeout*
    - *hard timeout*
    - *URL* de redirection, une fois le client connecté
    - *multipass* : connexion multiple d'un même login

Systèmes d'information

- Délégation de l'authentification
  - gestion autonome et maîtrise totale des utilisateurs par les établissements
- Possibilité de surcharge et délégation des autorisations
  - les paramètres par défaut en central peuvent être surchargés dans les *SI* des établissements
  - gestion autonome et maîtrise totale des accès et de la sécurité par les établissements
  - granularité fine et hiérarchisation des surcharges



Systèmes d'information

- Scénarii multiples d'authentification/autorisation : mutualisation inter-établissement et authentifications traversales
  - un réseau captif peut proposer plusieurs sources d'authen/authz
    - réseaux BU, proposer l'ensemble des *SI* des universités
    - réseaux CROUS, proposer l'ensemble des *SI* des universités + *SI* du CROUS
  - autorisation du mécanisme de surcharge
    - possibilité d'autoriser ou non la surcharge sur le couple [réseau/*SI*]
    - idée :
      - n'autoriser les surcharges à partir du *SI* de l'établissement U1 que sur les réseaux de l'établissement U1
      - n'autoriser que les paramètres par défaut des réseaux U1 pour les clients s'authentifiant sur l'établissement U2

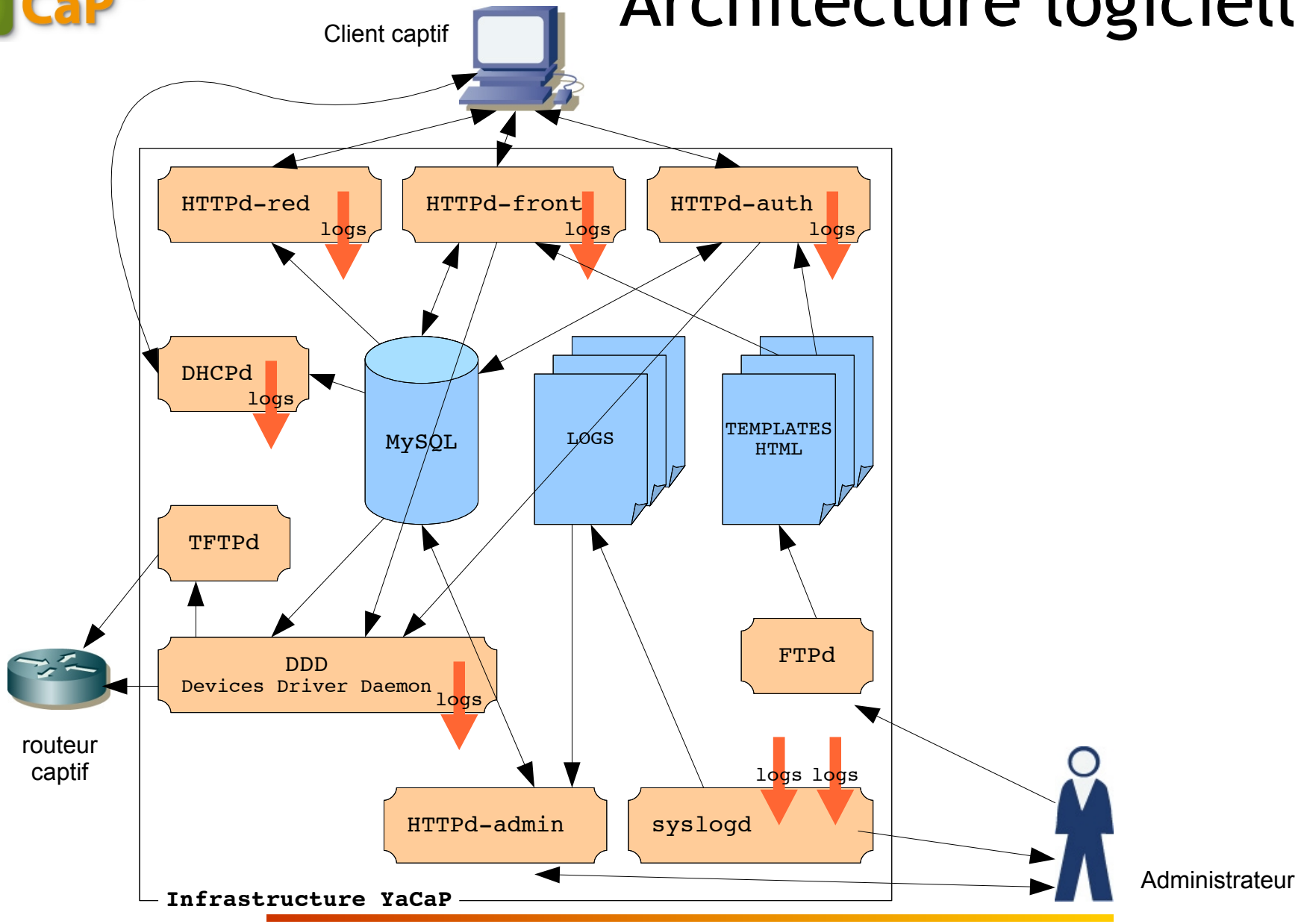
Au programme

- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

Architecture logicielle

- Infrastructure centralisée = point unique de panne *SPoF*
  - mise en oeuvre de toutes les techniques nécessaires pour rendre le service *performant*, *robuste et hautement disponible*
- Philosophie de développement
  - découpage en « briques fonctionnelles »
  - optimisations spécifiques de chaque brique
    - optimisation du code
    - spécialisation et optimisation des configurations
    - pré-chargement des informations statiques au démarrage
    - pré-calcul et factorisation « au plus tôt » des informations dynamiques
  - rendre possible la redondance de chaque brique
    - choix des outils
    - choix de développement « redondable »

Architecture logicielle



Au programme

- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

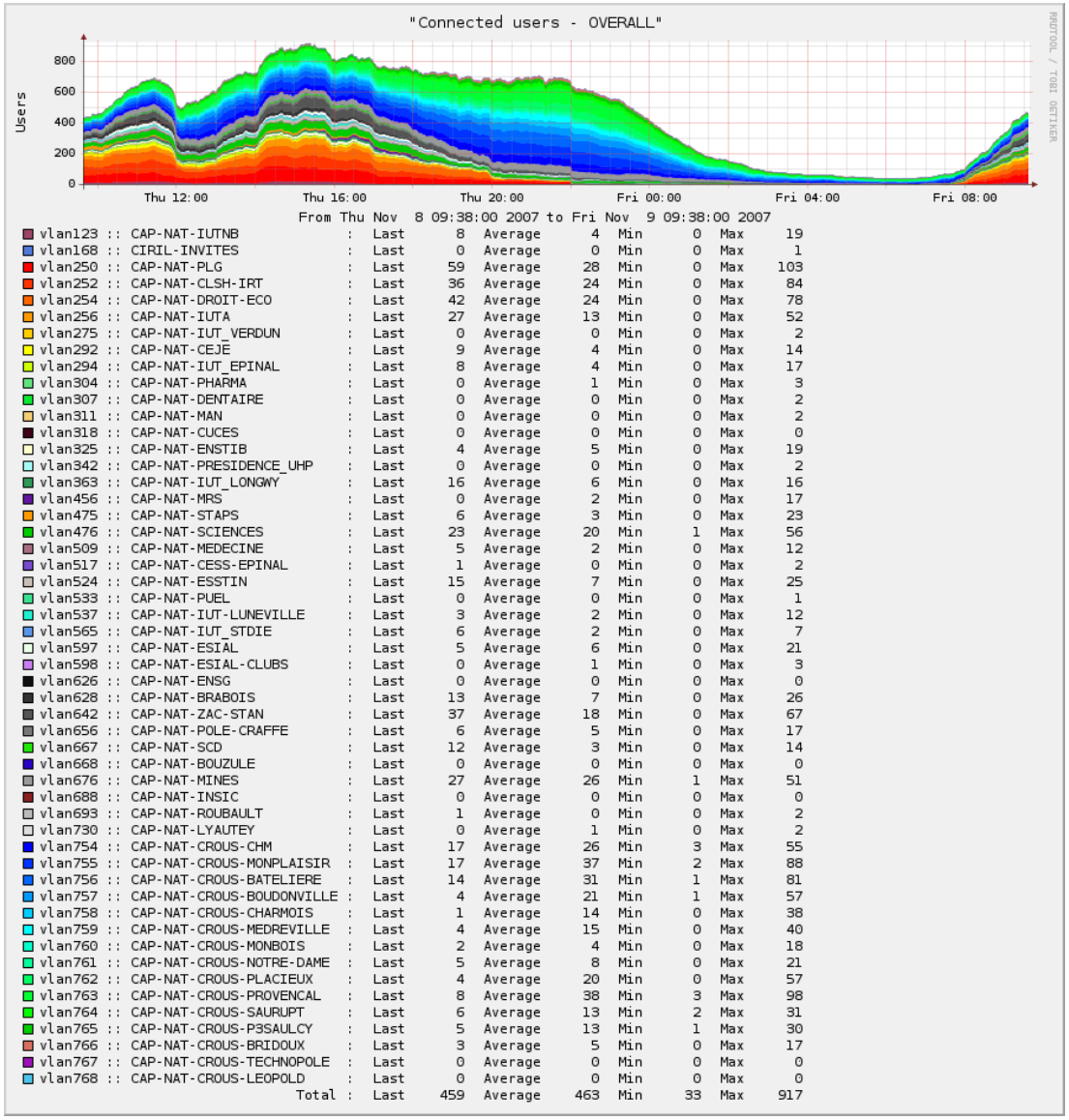
YaCaP et Lothaire

- Depuis le printemps 2006, YaCaP est en production sur Lothaire pour :
  - les trois Universités nancéennes (Nancy2, UHP et INPL)
  - l'IUFM de Lorraine
  - et le CROUS de Nancy-Metz
- L'infrastructure compte
  - 6 serveurs et 3 routeurs captifs
  - 39 *vlans* métropolitains
  - 13 *vlans* WAN distants
- L'infrastructure est théoriquement dimensionnée pour supporter
  - 1500 (utilisateurs universitaires) + 8000 (utilisateurs CROUS) = ***9500 utilisateurs simultanés***

YaCaP et Lothaire

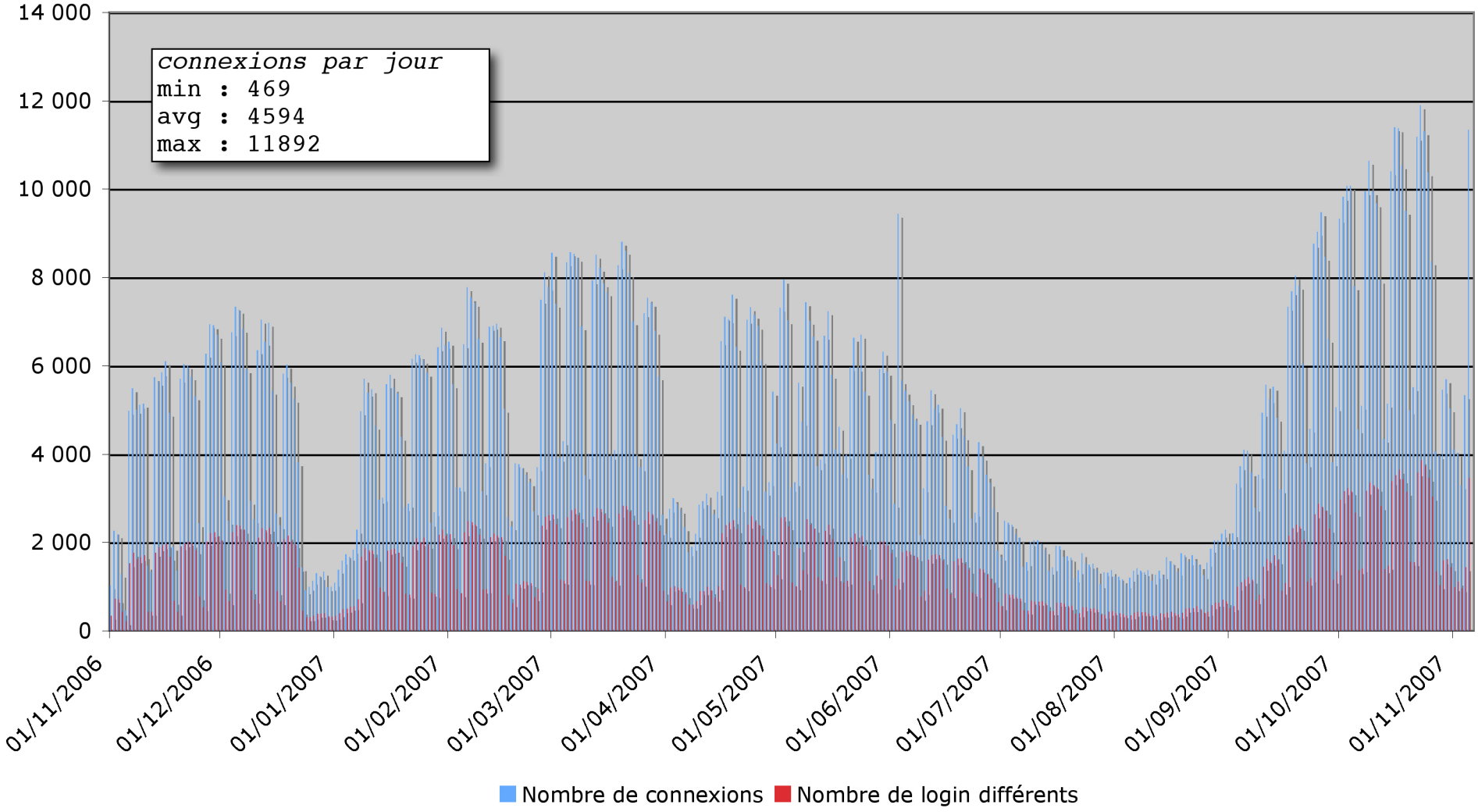
- Utilisation YaCaP en quelques chiffres et graphiques
  - nombre maximum d'utilisateurs simultanés : 917
  - statistiques entre octobre 2006 et octobre 2007
    - nombre de connexions : 1 805 564
    - nombre de *login* différents : 25 524
    - nombre d'@ *MAC* différentes : 22 404
    - nombre de connexion sans *DHCP* : 10 087

YaCaP et Lothaire

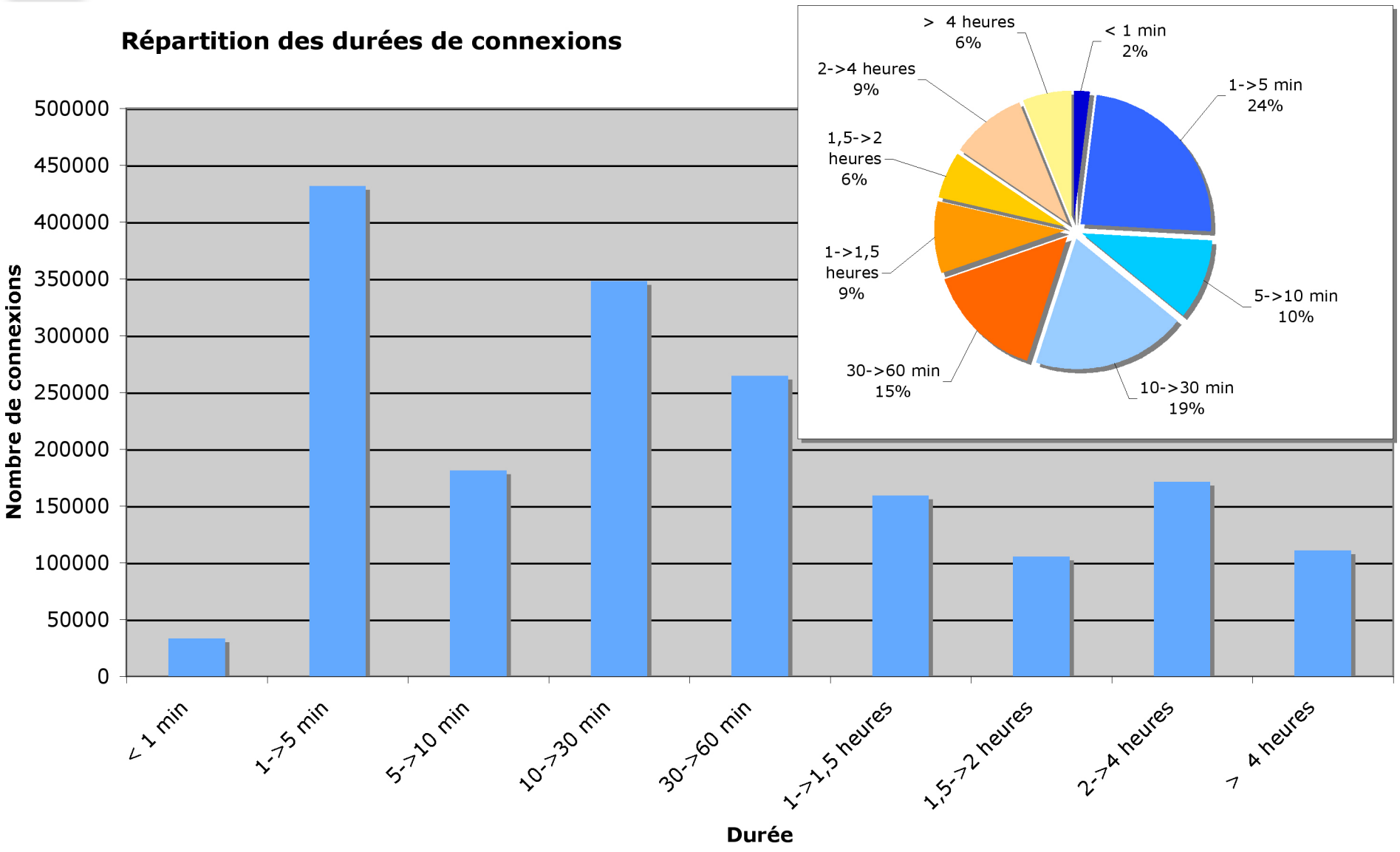


YaCaP et Lothaire

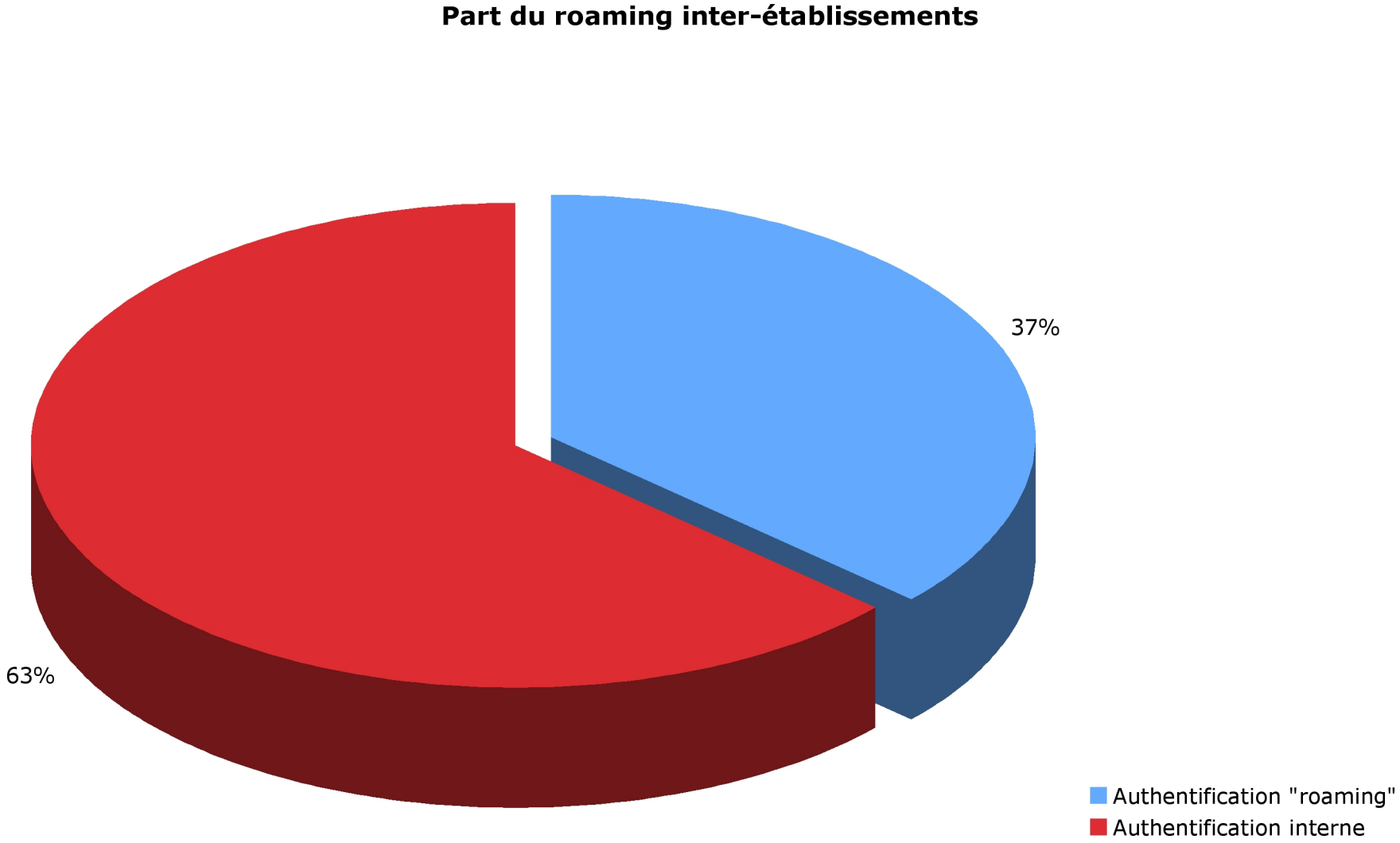
YaCaP : connections quotidiennes / logins différents



YaCaP et Lothaire

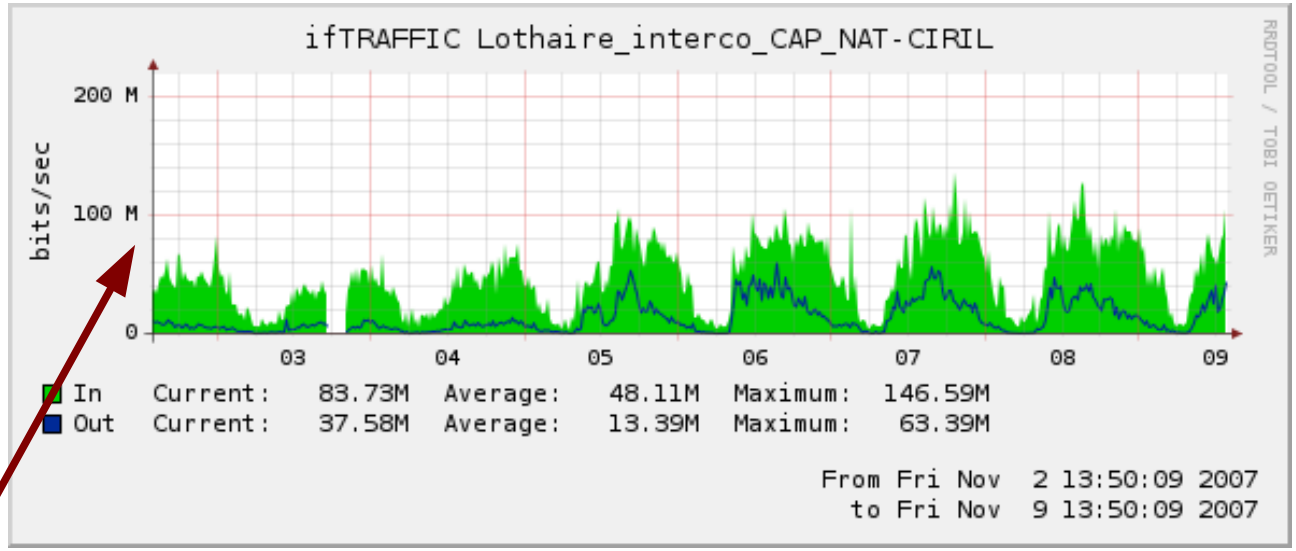


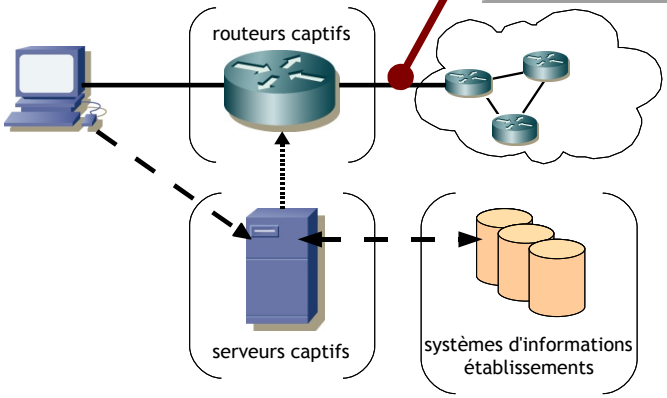
YaCaP et Lothaire



YaCaP et Lothaire

- Plus de 100 Mb/s entre YaCaP et l'Internet





Au programme

- Introduction
- Historique, besoins et choix
- Architecture / Infrastructure
- Fonctionnement
- Systèmes d'information
- Architecture logicielle
- YaCaP et Lothaire
- Conclusion

Conclusion

- YaCaP : ça fonctionne (1 800 000 connexions en 1 an)
- YaCaP : c'est utile (roaming des *logins*)
- YaCaP : c'est l'autonomie et la maîtrise des accès réseaux par les établissements
- YaCaP : c'est une des premières applications transversale aux *SI* des établissements lorrains


Ya
CaP