Grand'Messe

Campus Sciences – Amphi 13

23 octobre 2008

Au programme

14h00 : Présentation de l'équipe et de ses missions
14h20 : Un nouveau contexte pour Lothaire
14h35 : Evolutions de l'infrastructure du réseau Lothaire
15h20 : Evolutions Renater 5
Pause – 15 min
15h35 : Evolutions et nouveaux services réseau
16h40 : Hébergement et salle machine du CIRIL
Pot

reseau@ciril.fr

Équipe Réseau
services et organisation

Pierre MERCIER

Equipe réseau : les services

- En guise d'introduction
  - Dates des « grand-messes » (années olympiques !)
    - 14 décembre 2000
    - 24 juin 2004
    - 23 octobre 2008
  - La convention Lothaire prévoit une réunion annuelle
    - Contrat non respecté ☹
    - A l'année prochaine !
  - D'autres dates :
    - Printemps 2007 : audit du CIRIL
    - Automne 2007 : restructuration du CIRIL

Equipe réseau : les services

- Conséquences de la restructuration
  - Les services que nous n'assurons plus
    - Mail
    - News
    - Hébergement de sites WEB
    - Système (applications de gestion)
  - Ces services ont été
    - abandonnés (ex. : News)
    - ou repris par les CRIs des établissements

Equipe réseau : l'organisation

- Chargé de Mission Lothaire
  - François Schwaab
- Service Administratif et Financier
  - Valérie Petitcolas
  - Martine Schwaab
- Service réseau
  - Annick Faucourt
  - Vincent Delove
  - Stéphane Fetter
  - Olivier Lacroix
  - Pierre Mercier
  - Sébastien Morosi
  - Karol Proch (3)
  - Alexandre Simon
- Service câblage
  - Jean-Claude Branda
  - Jérôme De Deus
  - Olivier Krapp

Equipe réseau : les services

- Les services rendus
  - Pour Lothaire et e-Lorraine (lycées)
    - Supervision des liens
      - 75 liaisons fibres noires
        - CUGN : 65 (Réseau StanNet)
        - DRE : 2 (fibre A31 Nancy-Metz-Thionville)
        - Moselle Télécom : 3 (Ampèrenet)
        - UPVM : 5 (Ampèrenet)
      - 233 liaisons « opérateur »
        - OBS : 215 (e-Lorraine)
        - OBS : 18 (sites d'Epinal + divers)
        - Moselle Télécom : 3 (IUT Moselle Est)
      - 1 lien herzien
        - INRA Champenoux
      - 2 liens Wifi
        - Ferme de La Bouzule,
        - Gymnase SIUAPS Brabois

Equipe réseau : les services

- Les services rendus (suite)
  - Pour Lothaire et e-Lorraine (suite)
    - Gestion des équipements
      - 272 (57+215) routeurs
      - 787 switchs
    - Routage
      - 1208 subnets IPv4 (unicast + multicast)
      - 48 subnets IPv6 (unicast)
    - Accès Internet via Renater
    - Astreintes
    - Permanence
      - reseau@ciril.fr
      - +33 3 83 68 24 24

Equipe réseau : les services

- Les services rendus (suite)
  - Pour les organismes Lothaire
    - Gestion de la sécurité (ACL, Firewall)
    - Gestion du DNS
    - Service de translation d'adresses (NAT)
    - VPN
    - Gestion du GIX lorrain (LOTHIX)
      - Lothaire
      - RMI
      - Renater

Equipe réseau : les services

- Les services rendus :
  - Pour les organismes Lothaire
    - Portail captif (YaCaP)
      - 63 VLANs captifs
    - Gestion des réseaux de Campus
      - INPL
      - UHP
    - Métrologie des flux réseaux
      - externe (netMET)
      - Intra Lothaire (netMAT)
    - Hébergement « sec » de serveurs (salles blanches)
    - Conseils pour le design réseau
    - Prestations de câblage de campus (cuivre et fibre)
    - Etudes de couverture WIFI
    - Mise à disposition d'une salle de formation

Un nouveau contexte pour Lothaire

François SCHWAAB

Situation du réseau Lothaire (2007)

- Analyse du budget de fonctionnement annuel :
  - Les 28 sites délocalisés prélèvent 44% du budget
  - Les 56 sites de StanNet (Nancy) en prélèvent 47%
  - Les 13 sites d'Amperenet (Metz) en prélèvent 10%

- Analyse des coûts de fonctionnement annuel :
  - Un site délocalisé connecté à 2 Mb/s coûte 26 k€ TTC avec une part de 66% pour l'opérateur FT
  - Un site métropolitain à 1 Gb/s coûte 14 k€ TTC

- *Déséquilibre autant sur les services que sur les coûts*

Nouveau contexte financier

- Inscription de Lothaire au CPER 2007-2013
  - financement d'investissements
  - effet levier : accès aux fonds FEDER
- Augmentation des services
  - utilisation des infrastructures des collectivités et de l'État
  - raccordements par des liaisons FON
  - activation Gigabit et plus
- Transfert « fonctionnement » *vers* « investissement »
  - location des liaisons en IRU
  - construction des raccordements

Nouveau contexte juridique

- Nouvelle convention pour l'accès aux services Lothaire
  - adossée au CPER 2007-2013
  - tarif des contributions inchangé
  - annexes actualisées
  - prise d'effet au 1er janvier 2008

Projet transfrontalier

- Projet « Grande Région »
  - Sarre, Lorraine, Luxembourg, Wallonie
  - partenariat Renater, Restena, DFN, Belnet
  - nœud d'interconnexion transfrontalier à Luxembourg
  - mandat à Lothaire pour la maîtrise d'ouvrage
    - dépôt d'un dossier de financement InterReg
  - complément au projet UGR (Université Grande Région)
- Connexion de Longwy au passage

Évolutions de l'infrastructure du réseau Lothaire

Sébastien MOROSI

Les évolutions et projets en cours

- Evolutions de l'infrastructure Lothaire
  - Evolution Nancy-Metz
  - Evolution Metz-Thionville
  - Nouveaux Sites StanNet
  - Evolution AmpereNet
  - Evolution IUT Moselle-Est
  - Autres évolutions
- Projets en cours
  - Projet à Longwy
  - Projet à Epinal
  - Projet pour INRA Champenoux

Liaison Nancy - Metz

- Remplacement de la liaison ‘InterLAN Orange’ à 1Gb
- Convention entre le CIRIL et la DIR-EST (ex. DDE)
  - pour la mise à disposition de 2 brins de fibre optique
  - le long de l’A31, entre Nancy, Metz et Thionville
  - pour l’interconnexion des réseaux de l’Enseignement Supérieur et de la Recherche
- Travaux (longs et laborieux) de génie civil à Metz pour relier la chambre sur la bande d’arrêt d’urgence (BAU) au local réseau situé dans les locaux de l’Université Paul Verlaine

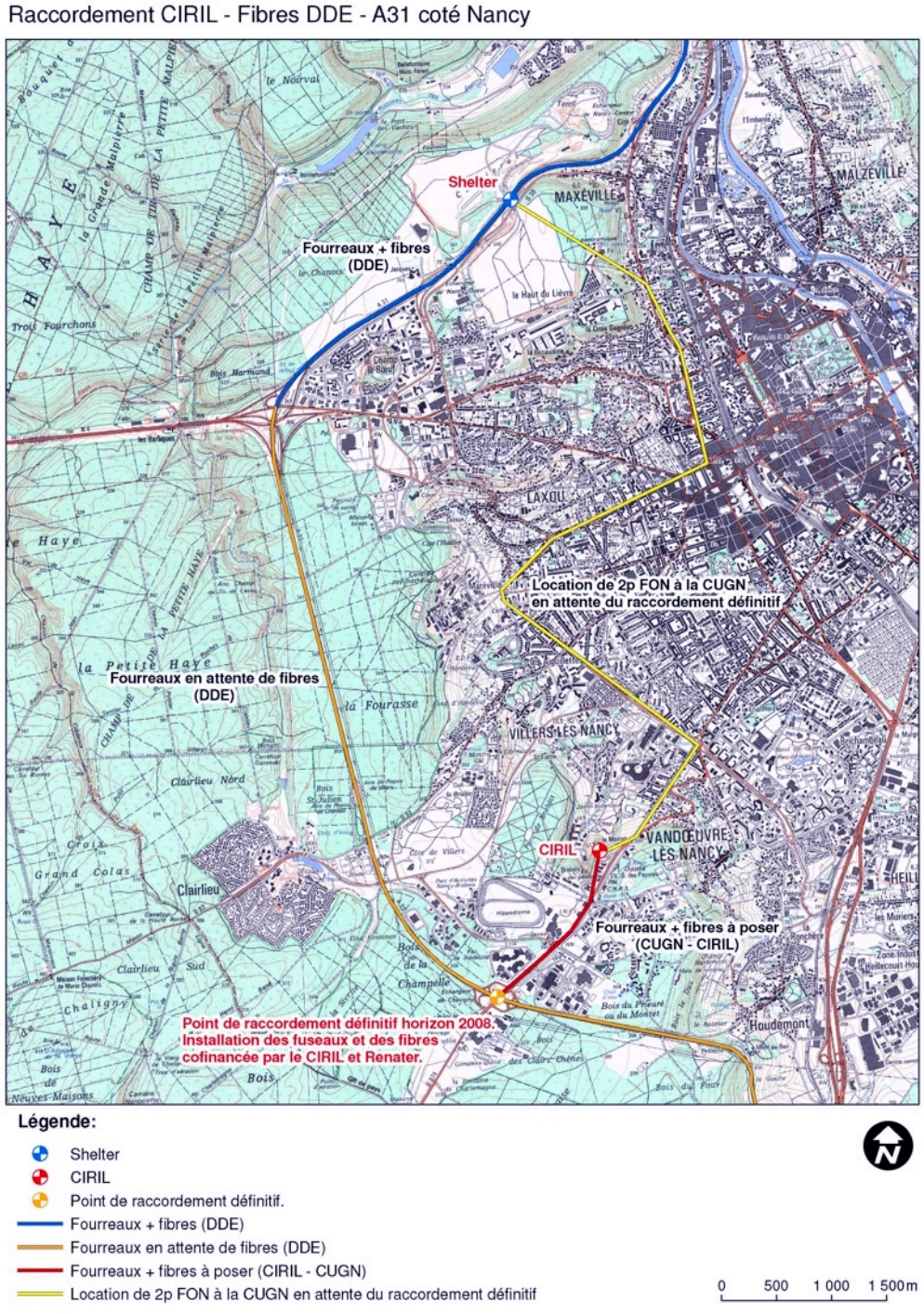
Liaison Nancy - Metz

Liaison Nancy - Metz

- Raccordement du CIRIL à la fibre de l'A31
- Aujourd'hui
  - via le 'Shelter' situé à proximité du Zénith
  - location temporaire d'une fibre à TUTOR (délégataire du RMT de la Communauté d'Aglomération du Grand Nancy)
- A terme
  - via la A33
  - travaux pour raccordement entre le CIRIL et l'échangeur de Brabois

Liaison Nancy - Metz

- En jaune : raccordement temporaire
- En rouge : raccordement définitif



Liaison Nancy - Metz

- Activation de la fibre optique
  - Objectif : prolongation des services Renater à Metz
  - Technologie retenue = Multiplexage de longueur d'onde
    - DWDM
    - Utilisation de multiplexeurs optiques passifs (EWDM)
      - maximum de 8 λ DWDM
      - un λ DWDM = 10Gb/s
    - Utilisation de 2 λ dans un premier temps
- Actif depuis le début du mois d'octobre

Liaison Metz - Thionville

- Remplacement de la liaison Orange à 2Mb/s entre le Saulcy et l'IUT de Yutz-Thionville
- Utilisation de la fibre optique de l'A31 depuis Metz

- Aménagement d'un local informatique à l'IUT de Thionville en vue des autres projets impliquant l'IUT

- Travaux de génie civil pour le raccordement de la chambre située le long de la BAU à l'IUT

Liaison Metz - Thionville

Liaison Metz - Thionville

- Activation de la fibre optique
  - Technologie retenue : Gigabit Ethernet
  - longue distance (35km)
  - utilisation de Gbics plus puissants : ‘ZX’
  - Evolution possible à 10Gb
- Actif depuis le 18 octobre 2008

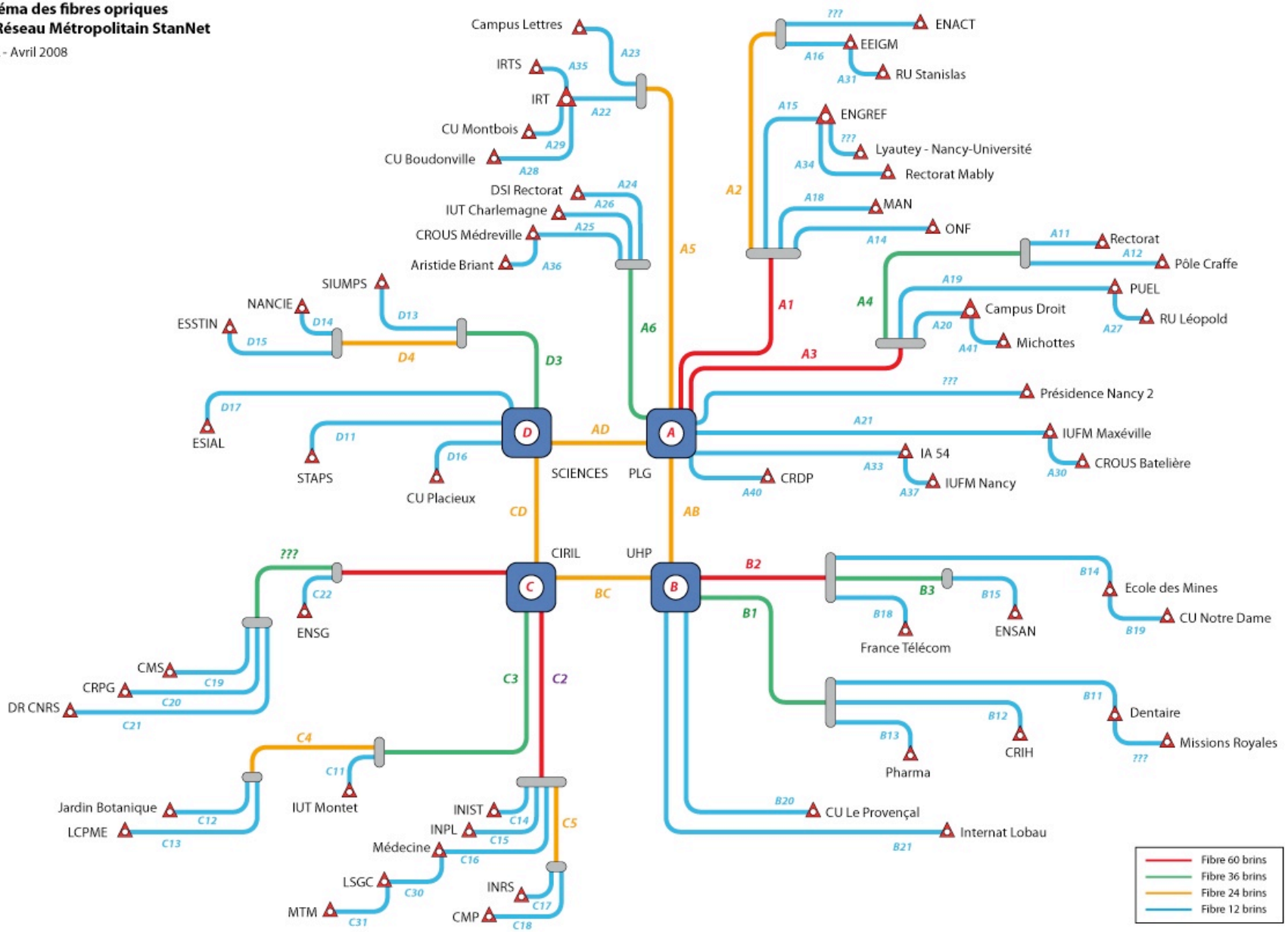
Nouveaux sites StanNet

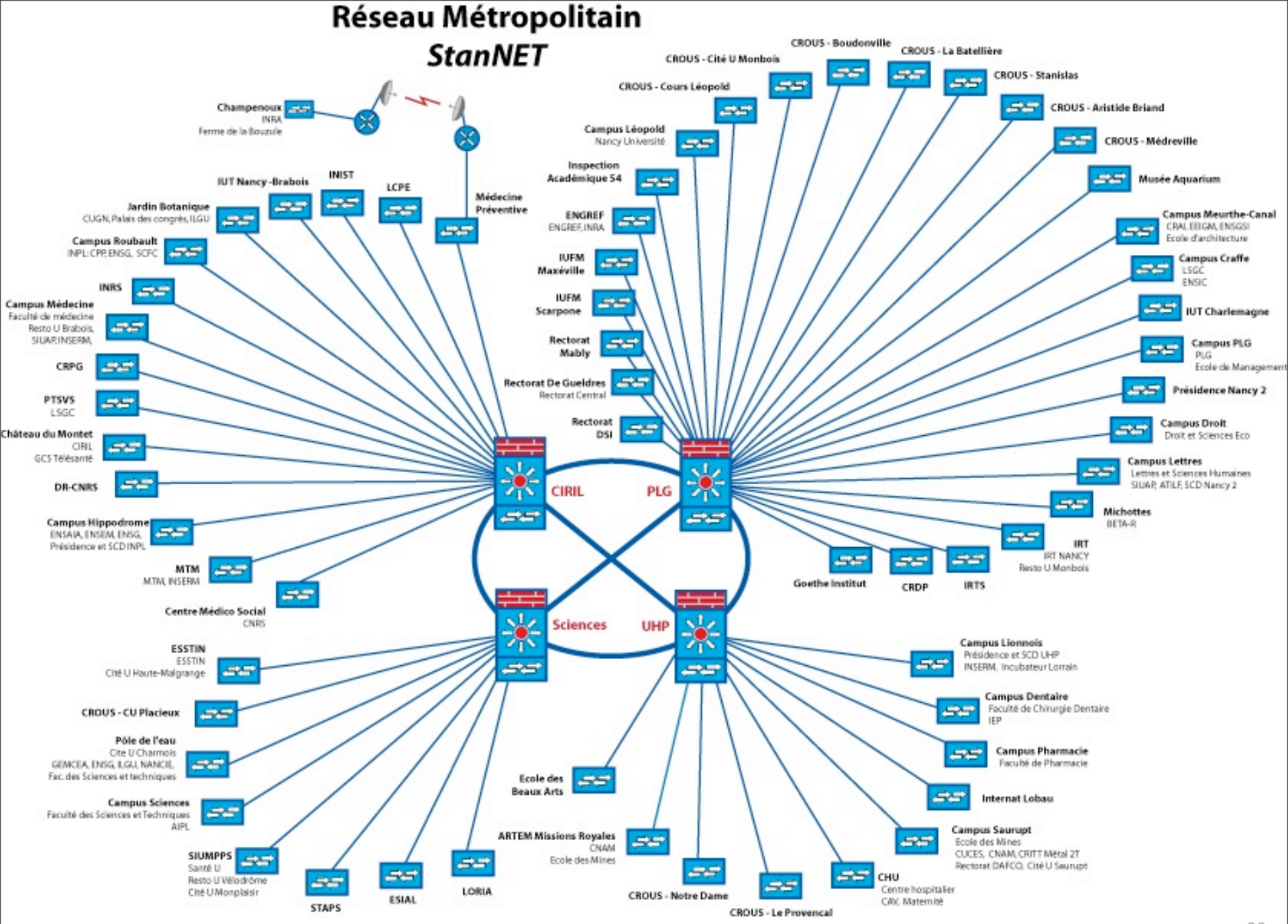
- StanNet : phase 3
  - Extension du réseau optique StanNet
  - Dans le cadre de la convention entre le CIRIL et la Communauté Urbaine du Grand Nancy
- Nouveaux partenaires
  - Le CRDP (Centre Régional de Documentation Pédagogique)
  - Le CNAM (Conservatoire National des Arts et Métiers)
- Evolutions
  - Nouvelles prises
  - Remplacement de liaisons louées par de la fibre

Nouveaux sites StanNet

- Huit nouveaux câbles optiques de 12 brins
  - Liaison IRT – IRTS
  - Liaison CROUS – Résidence A. Briand
  - Liaison PLG - Inspection Académique
  - Liaison Inspection Académique – IUFM
  - Liaison PLG – CRDP
  - Liaison Rectorat - ENGREF
  - Liaison Campus Léopold - Labo BETA
  - Liaison CHU (central) – Internat Lobau

L'infrastructure optique




Réseau Métropolitain
StanNET
Champenoux
INRA
Ferme de la Bouzule
IUT Nancy -Brabois
INIST
LCPE
Médecine Préventive
Jardin Botanique
CUGN, Palais des congrès, ILGU
Campus Roubault
INPL: CPP, ENSG, SCFC
INRS
Campus Médecine
Faculté de médecine
Resto U Brabois,
SIUAP, INSERM,
CRPG
PTSVS
LSGC
Château du Montet
CIRIL
GCS Télésanté
DR-CNRS
Campus Hippodrome
ENSAIA, ENSEM, ENSG,
Présidence et SCD INPL
MTM
MTM, INSERM
Centre Médico Social
CNRS
ESSTIN
ESSTIN
Cité U Haute-Malgrange
CROUS - CU Placieux
Pôle de l'eau
Cite U Charmois
GEMCEA, ENSG, ILGU, NANCIE,
Fac. des Sciences et techniques
Campus Sciences
Faculté des Sciences et Techniques
AIPL
SIUMPPS
Santé U
Resto U Vélodrôme
Cité U Monplaisir
STAPS
ESIAL
LORIA
CIRIL
PLG
Sciences
UHP
CROUS - Boudonville
CROUS - La Batellière
CROUS - Cité U Monbois
CROUS - Stanislas
CROUS - Cours Léopold
CROUS - Aristide Briand
Campus Léopold
Nancy Université
CROUS - Médreville
Inspection Académique S4
Musée Aquarium
ENGREF
ENGREF, INRA
Campus Meurthe-Canal
CRAI, EEIGM, ENSGSI
Ecole d'architecture
IUFM Maxéville
Campus Craffe
LSGC
ENSIC
IUFM Scarpone
IUT Charlemagne
Rectorat Mably
Campus PLG
PLG
Ecole de Management
Rectorat De Gueldres
Rectorat Central
Présidence Nancy 2
Rectorat DSI
Campus Droit
Droit et Sciences Eco
Campus Lettres
Lettres et Sciences Humaines
SIUAP, ATILF, SCD Nancy 2
Michottes
BETA-R
IRT
IRT NANCY
Resto U Monbois
Goethe Institut
CRDP
IRTS
Campus Lionnois
Présidence et SCD UHP
INSERM, Incubateur Lorrain
Campus Dentaire
Faculté de Chirurgie Dentaire
IEP
Campus Pharmacie
Faculté de Pharmacie
Internat Lobau
Campus Saurupt
Ecole des Mines
CUCES, CNAM, CRITT Métal 2T
Rectorat DAFCO, Cité U Saurupt
CHU
Centre hospitalier
CAV, Maternité
CROUS - Le Provencal
CROUS - Notre Dame
ARTEM Missions Royales
CNAM
Ecole des Mines
Ecole des Beaux Arts

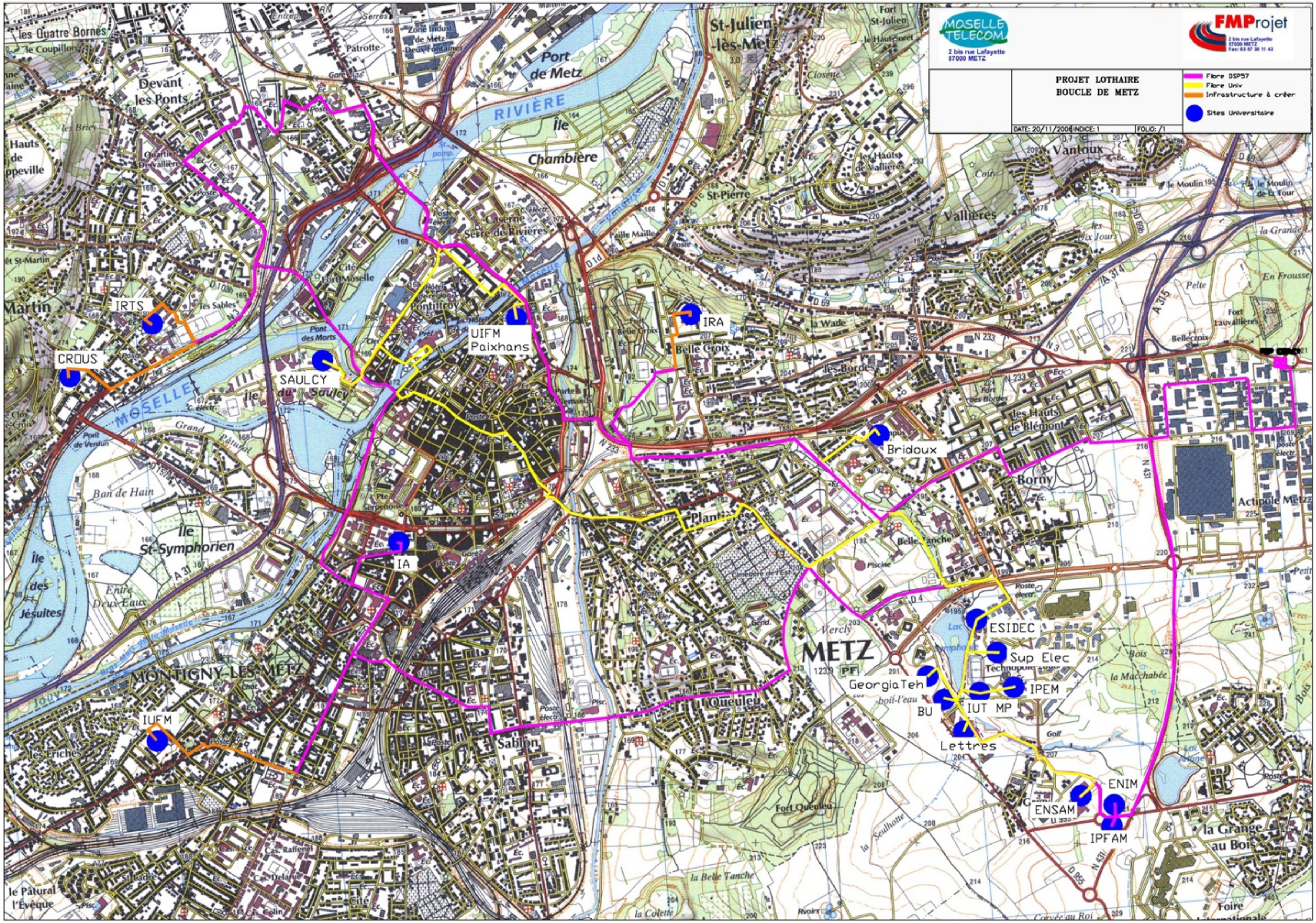
Evolution AmpèreNet

- Prise en charge opérationnelle du backbone AmpèreNet par l'équipe réseau du CIRIL

- Mise en place d'un anneau optique
  - sécurisation de l'accès
  - débit de 2Gb/s
  - utilisation des fibres optiques existantes de l'Université Paul Verlaine
  - location à Moselle Télécom (délégataire pour le conseil régional du RHD 57) pour bouclage
    - ENSAM – IUFM Paixhans
    - IRU – 15 ans

Evolution AmpèreNet

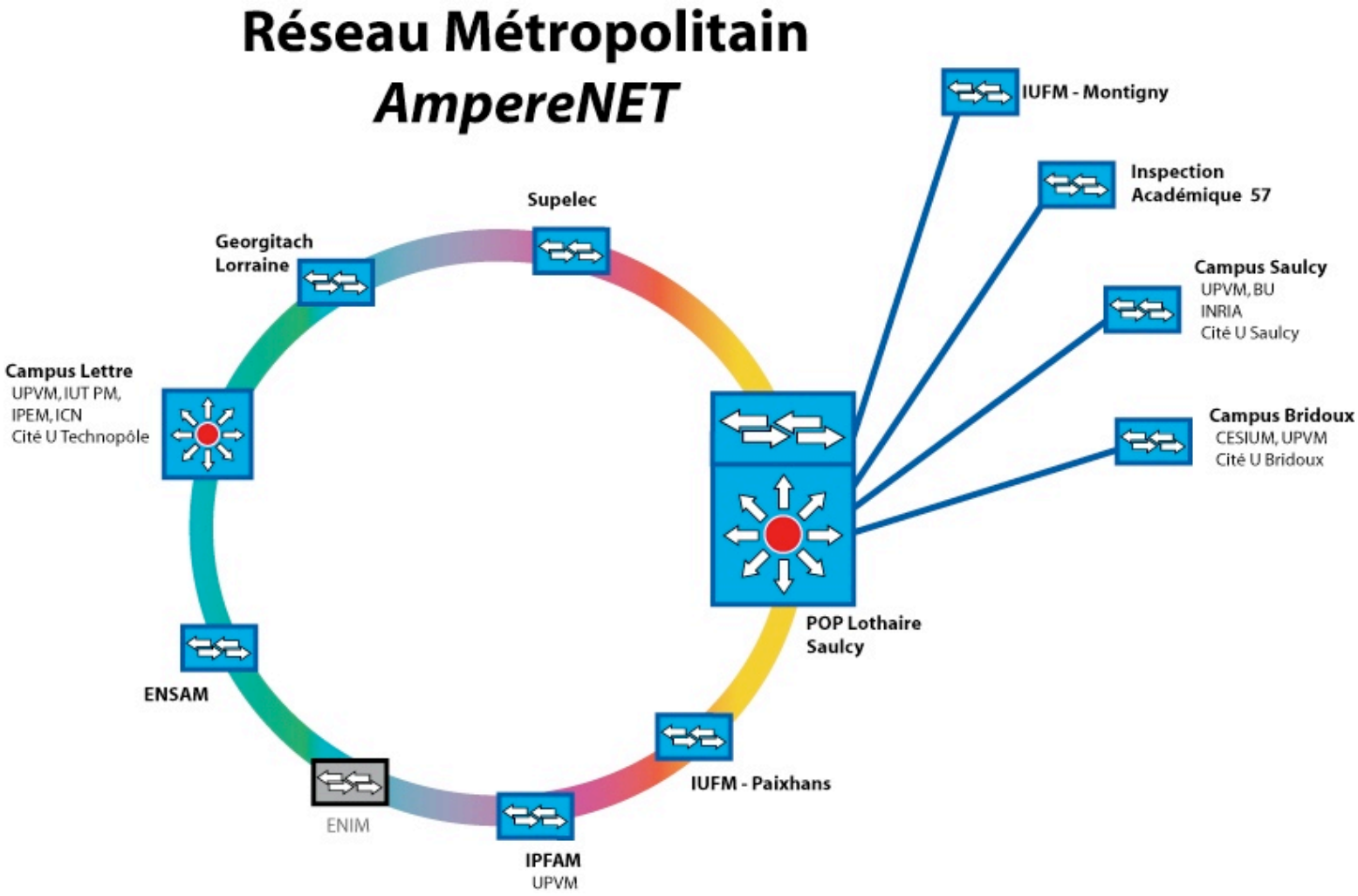
- Pour les sites ne se trouvant pas sur la boucle
  - IA 57
  - IUFM à Montigny-lès-Metz
  - IRTS (à venir)
  - CROUS (à venir)
- Connexion ‘pendulaire’
- Location de fibre optique à Moselle Télécom
  - IRU – 15 ans


MOSELLE TELECOM
2 bis rue Lafayette
57000 METZ
FMProjet
2 bis rue Lafayette
57000 METZ
Fax: 03 87 38 11 43
PROJET LOTHAIRE
BOUCLE DE METZ
DATE: 20/11/2006
INDICE: 1
FOLIO: /1
Fibre DSP57
Fibre Univ
Infrastructure à créer
Sites Universitaire
IRTS
CROUS
SAULCY
UIFM
Paixhans
IRA
Bridoux
IA
IUFM
ESIDEC
Sup Elec
IPEM
GeorgiaTeh
BU
IUT MP
Lettres
ENIM
ENSAM
IPFAM
METZ
MONTIGNY-LES-METZ
MOSELLE
RIVIÈRE
St-Julien-lès-Metz
Vantoux
Vallières
Borny
Actipole Metz
Queuleu
Sablon
Plantières
Belle Croix
Devant les Ponts
Chambière
Port de Metz
Ile St-Symphorien

Evolution AmpèreNet

- Activation de l'anneau
  - Technologie retenue : multiplexage de longueur d'onde
    - CWDM
    - 8 sites maximum en plus du Saulcy
    - chaque site a une double adduction à 1Gb/S
- Topologie physique : anneau
- Topologie logique : étoile
- Activation retardée : le bouclage n'est pas terminé par Moselle Télécom

Evolution AmpèreNet



Evolution IUT Moselle Est

- Sites IUT Moselle Est :
  - IUT de Forbach
  - IUT de Sarreguemines
  - IUT de Saint-Avold
- Remplacement des liaisons 2Mb/s louées à Orange par des Liaisons 10Mb/s louées à Moselle Télécom (évolutives à 100Mb/s)
- Concentration à l'IUT de Thionville
- Spécificité à Sarreguemines
  - liaison optique entre l'IUT et le Pôle Ecoles (IUT, IUFM, IA)
  - mise à disposition par la Communauté d'Agglomération de Sarreguemines Confluences

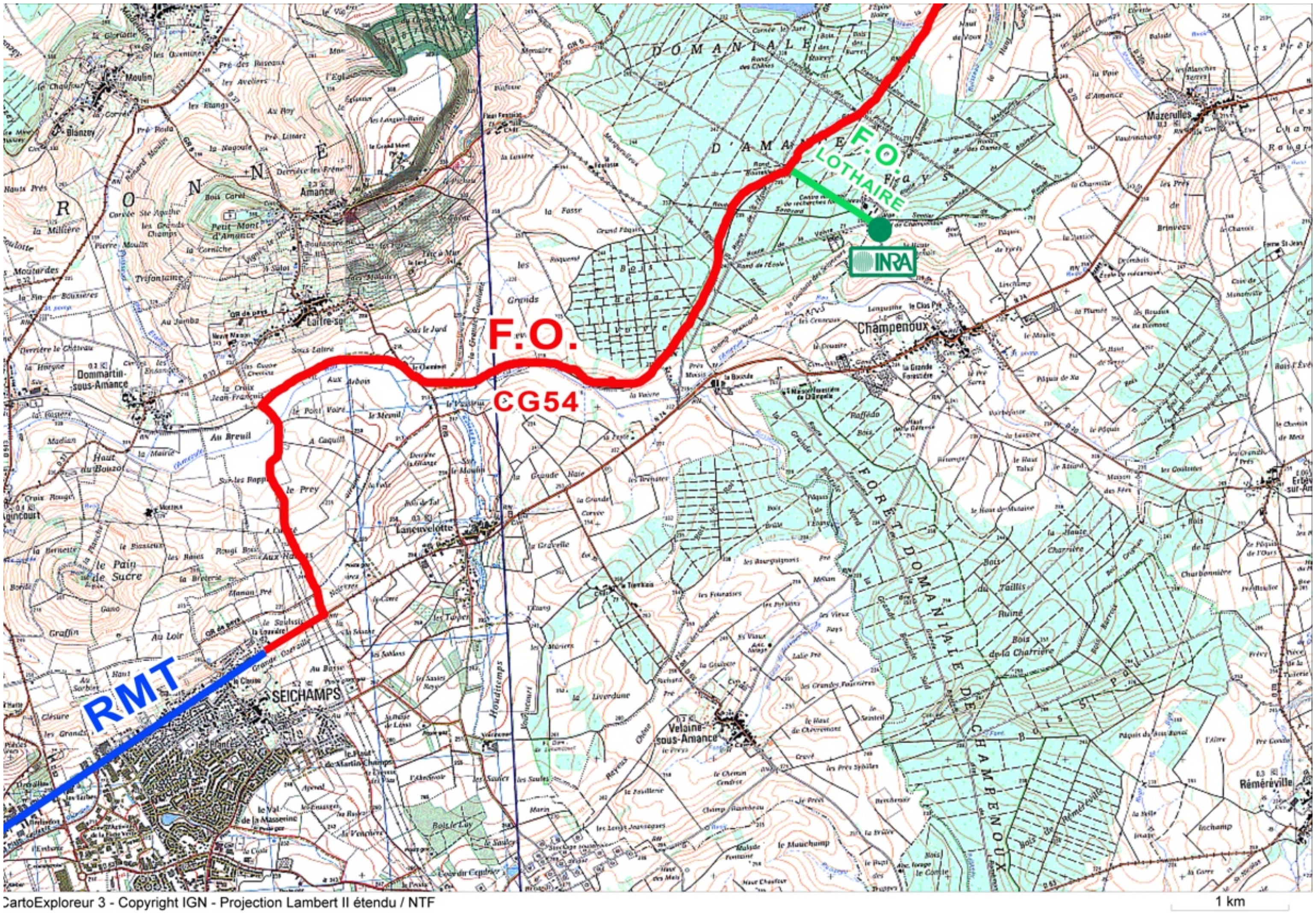
Autres évolutions

- Augmentation de débit pour la liaison entre Nancy et Epinal (2006)
  - liaison Orange à 30Mb/s
- Augmentation de débit pour les IUTs de Saint-Dié et Bar-le-Duc
  - liaison Orange à 30Mb/s
  - connexion directe vers Nancy
- Augmentation de débit pour l'IUT de Lunéville et l'IUT d'Epinal
  - liaison Orange à 8Mb/s

Projet INRA

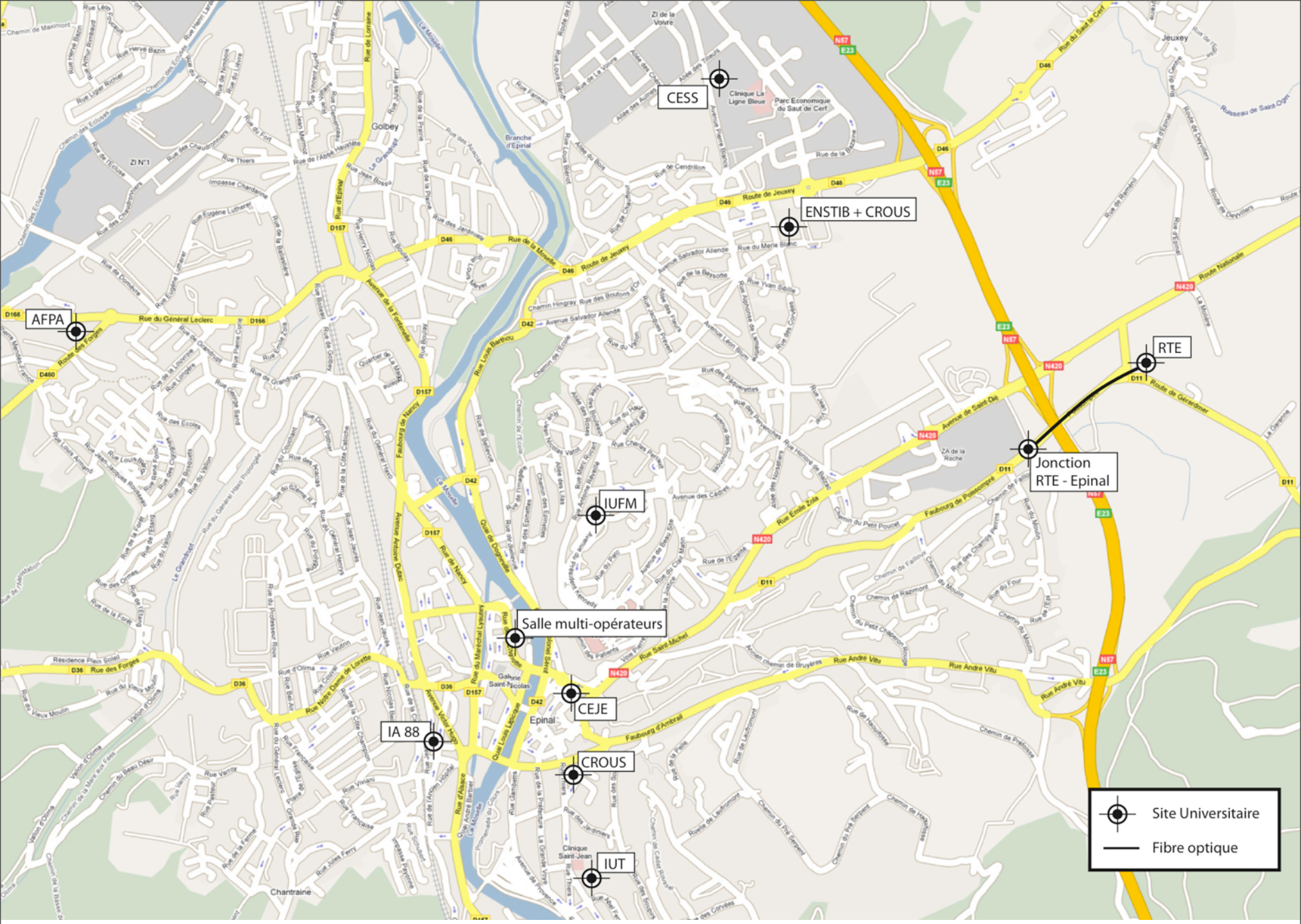
- L'INRA de Champenoux est connecté par un faisceaux hertzien de 2x2Mb/s
- Objectif : remplacer cette connexion par de la fibre optique et intégrer l'INRA aux sites de StanNet
- Projet :
  - Bénéficier du PPP (Partenariat Public Privé) du CG 54 qui est attribué
  - La fin des travaux est programmée dans 23 mois
  - Des contacts sont dès à présent établis afin de disposer au plus vite (septembre 2009) d'une liaison entre la zone Meurthe-Canal et l'INRA.

Projet INRA



Projet à Epinal

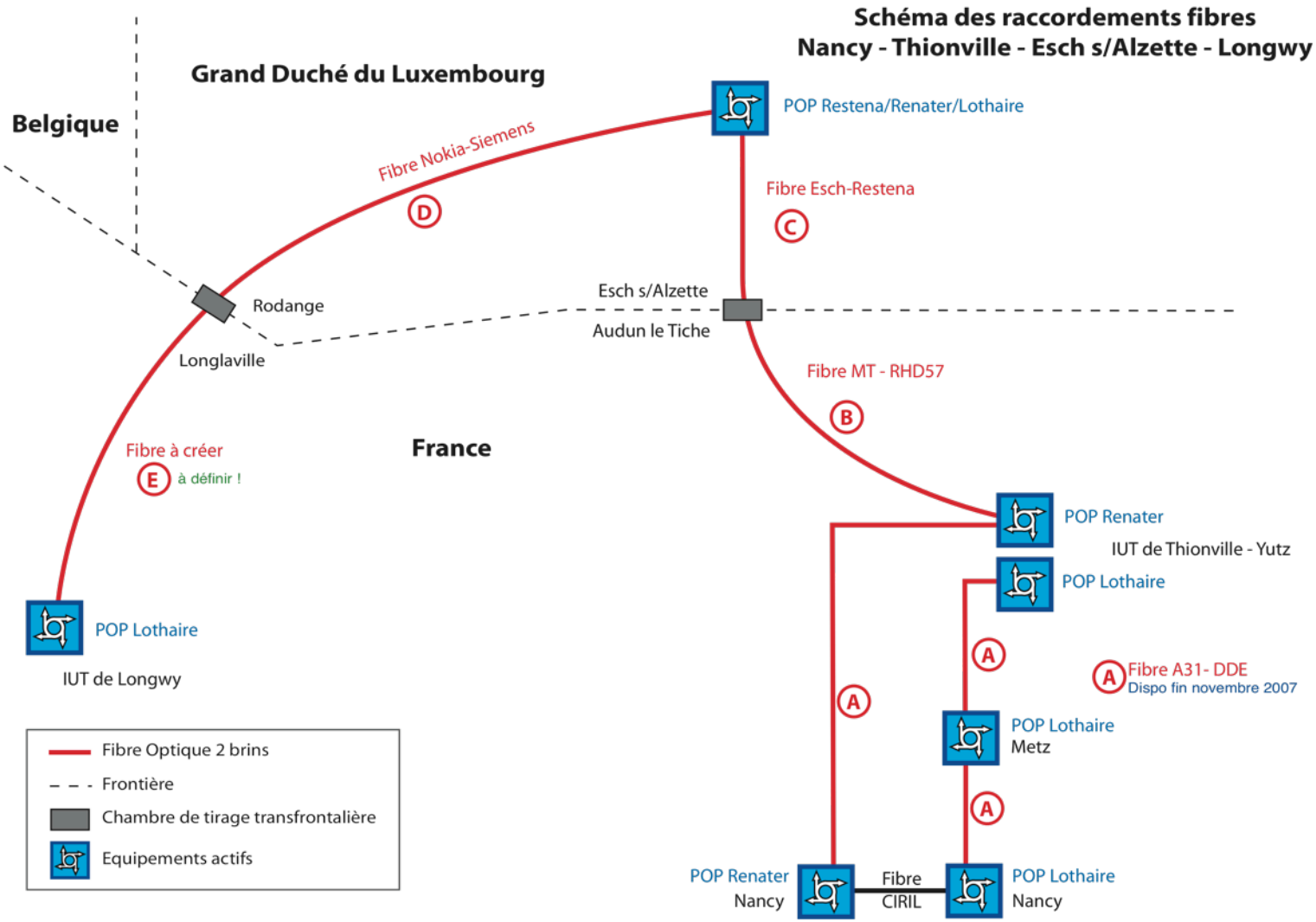
- Projet de convention entre le CIRIL et la Communauté de Communes d'Epinal-Golbey
  - Pour l'utilisation d'une paire de fibres du Sillon Lorrain
  - Réseau d'ARTERIA (pour RTE)
  - IRU de 15 ans
- Raccordements aux extrémités
  - Entre le CIRIL et Laneuveville via liaison TUTOR
  - Entre Jeuxey et Epinal via liaison Numéricâble
- Besoin de mettre en place un réseau métropolitain à Epinal : à l'étude


CESS
ENSTIB + CROUS
AFPA
RTE
Jonction
RTE - Epinal
IUFM
Salle multi-opérateurs
CEJE
IA 88
CROUS
IUT
Site Universitaire
Fibre optique

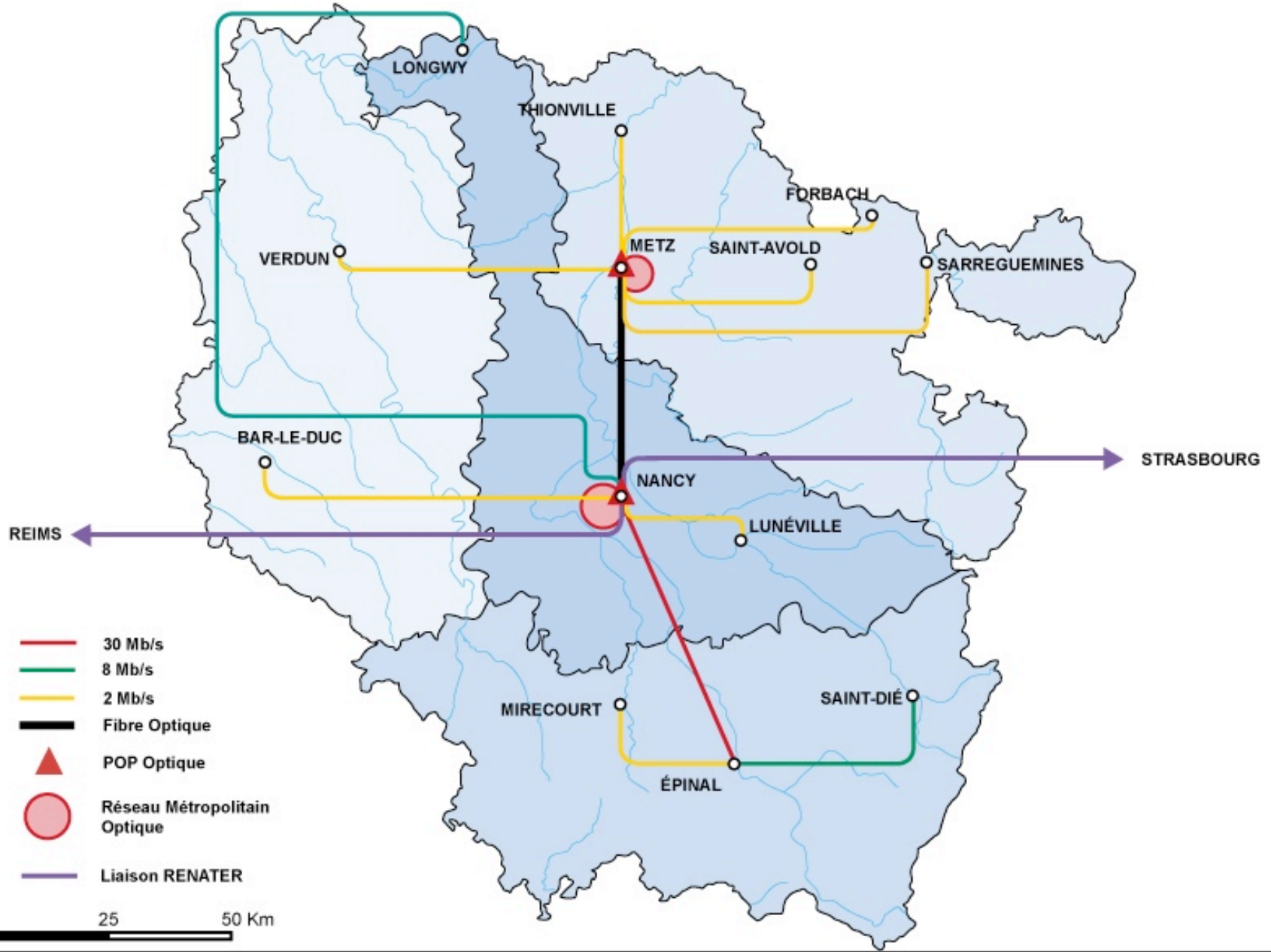
Projet à Longwy

- Remplacement de la liaison Orange à 6Mb/s entre Nancy et Longwy
- Projet transfrontalier
  - Renater sera bientôt connecté au Luxembourg via Nancy
  - Renater pourra bientôt fournir au CIRIL un transport de flux entre le CIRIL et le Luxembourg (POP à Belval)
- Connexion de Longwy
  - Le CIRIL souhaite connecter Longwy à Nancy via son futur point de présence au Luxembourg
  - Le plus gros du chemin est fait, mais les derniers kilomètres sont laborieux
  - Une solution est à l'étude et devrait déboucher sur une mise en service pour fin 2009

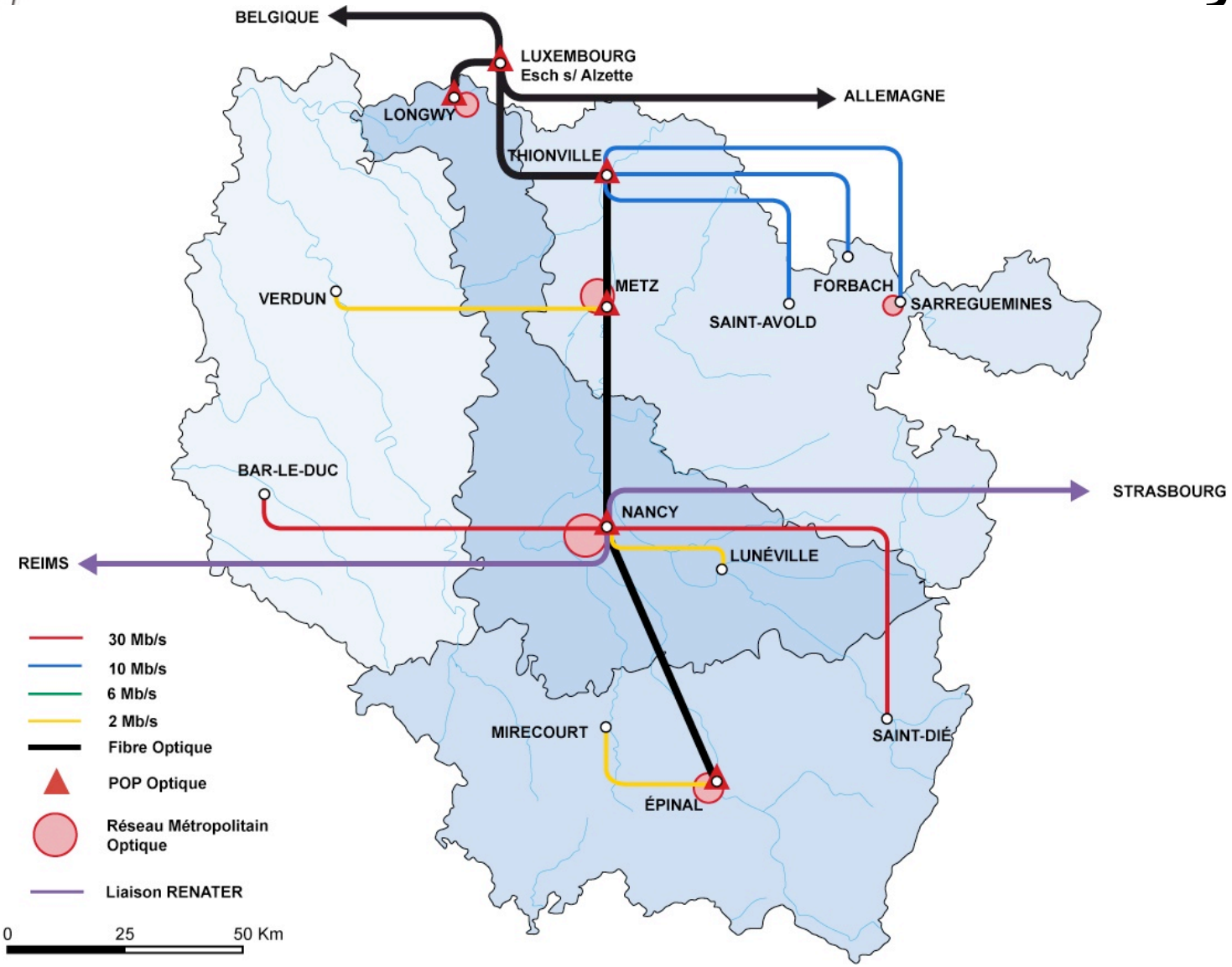
Projet à Longwy



Situation avant les évolutions



Objectif


BELGIQUE
LUXEMBOURG
Esch s/ Alzette
ALLEMAGNE
LONGWY
THIONVILLE
VERDUN
METZ
FORBACH
SARREGUEMINES
SAINT-AVOLD
BAR-LE-DUC
STRASBOURG
NANCY
REIMS
LUNÉVILLE
MIRECOURT
SAINT-DIÉ
ÉPINAL
30 Mb/s
10 Mb/s
6 Mb/s
2 Mb/s
Fibre Optique
POP Optique
Réseau Métropolitain Optique
Liaison RENATER
0
25
50 Km

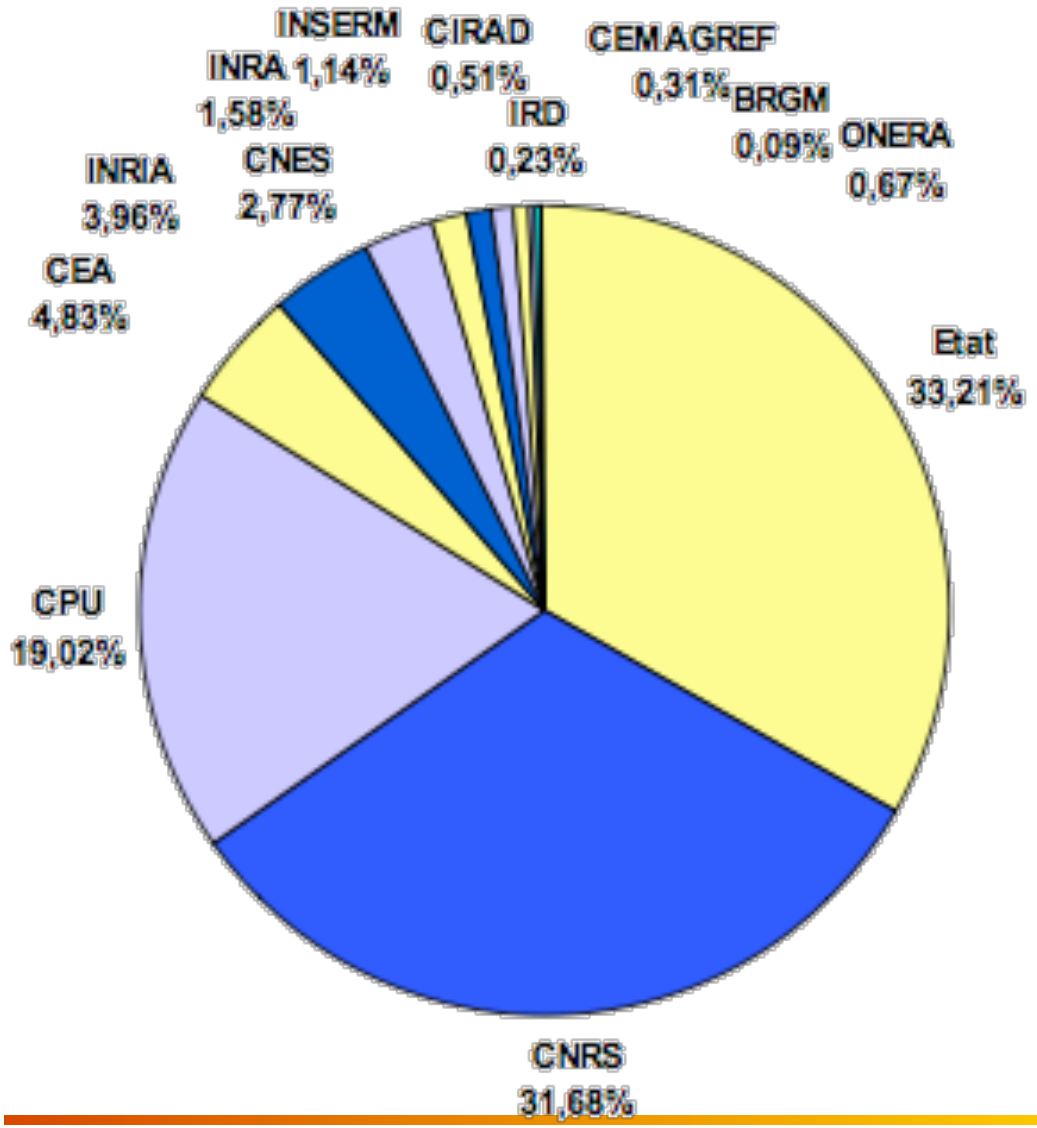
Renater 5

Annick FAUCOURT

RENATER 5

- GIP RENATER
  - Groupement d'Intérêt Public, maître d'ouvrage du réseau Renater
  - Février 2009 : nouveau GIP
  - Durée : 10 ans
    - Lourdeur administrative
    - Location des fibres en IRU
  - Membres : Grands Organismes de Recherche
  - Nouveaux membres
    - la CPU (Conférence des Présidents d'Université)
    - ONERA (Office Nationale d'Etude et de Recherche Aérospatiale)

RENATER 5


INSERM
1,14%
CIRAD
0,51%
CEMAGREF
0,31%
INRA
1,58%
BRGM
0,09%
IRD
0,23%
ONERA
0,67%
INRIA
3,96%
CNES
2,77%
CEA
4,83%
Etat
33,21%
CPU
19,02%
CNRS
31,68%

RENATER 5

- RENATER 4
  - Multi-opérateurs
  - 2 architectures distinctes :
    - Des liaisons louées à 2.5Gbit/s interconnectant les réseaux régionaux .
    - Une architecture WDM sur Fibre Optique Noire pour projets scientifiques nécessitant du Haut débit : GRID5000, LHC

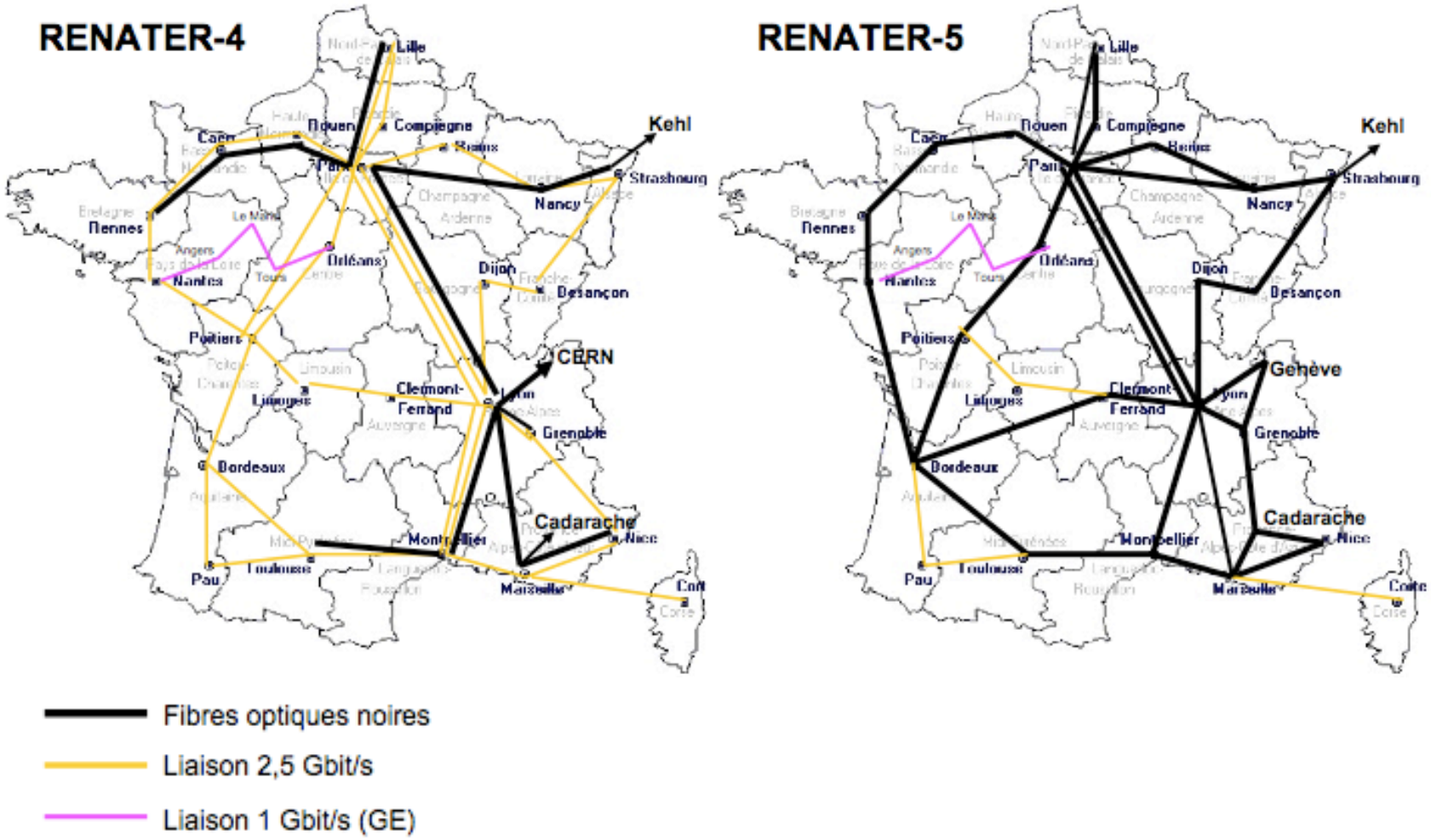
RENATER 5

- RENATER 5
  - Généralisation de la technologie DWDM sur Fibres Optiques Noires (FON)
    - Passage de 2,5 Gbps à 10 Gbps
    - Rattrapage du retard sur les autres réseaux nationaux européens (NREN)
  - RENATER opère lui-même son réseau
    - Fin des solutions opérateurs clef en main
    - Gain économique et maitrise de la technique
  - AO lancé mi-juillet 2007
  - Déploiement : octobre à décembre 2008
  - Exploitation et maintenance du réseau : BTIC
  - Equipements optiques : CIENA, ALCATEL
  - FON : NEUF CEGETEL, SOGEA, LEVEL3, @RTERIA, AXIONE, Orange

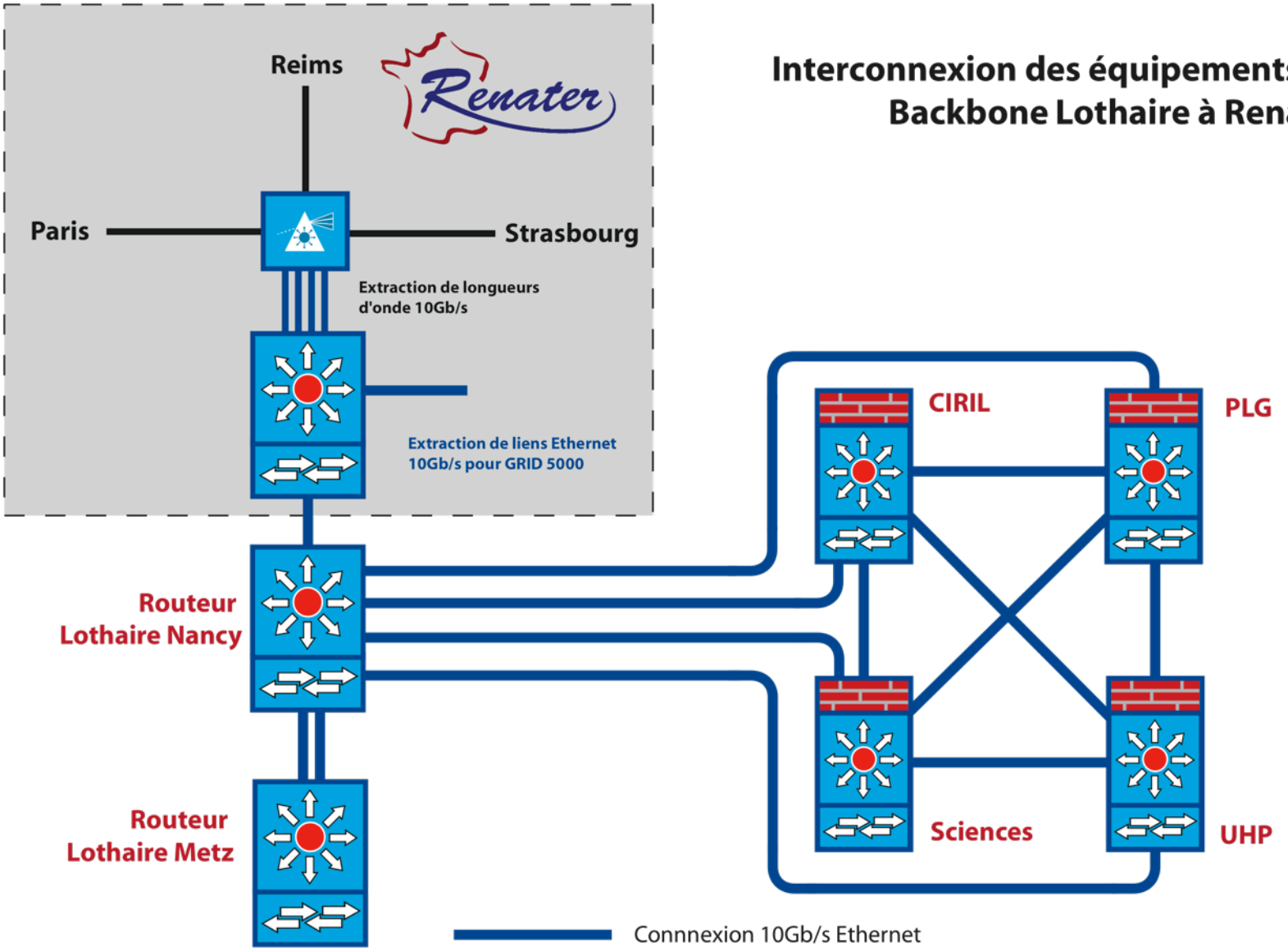
RENATER 5

- Topologie
  - Longueur d'onde point à point (entre 2 NR) pour réseau de production
  - Longueur d'onde de bout en bout pour projets de recherche (GRID 5000, LHC, …)
  - Capacité de 10 Gb/s minimum sur l'ensemble du réseau
  - Evolutivité : Rajout de longueur d'onde sans modifier l'infrastructure
- Sécurisation et qualité de service renforcée
  - Consolidation du maillage par introduction de nouvelles boucles
  - Doublement et bouclage de la FON Lyon-Paris
  - Doublement des équipements dans les NR de Lyon et Paris
    - Téra-routeurs (cisco CRS-1) dans ces 2 NR pour connexions vers l'International

RENATER 5


RENATER-4
Lille
Caen
Rouen
Compiègne
Paris
Reims
Kehl
Strasbourg
Nancy
Rennes
Le Mans
Angers
Orléans
Tours
Nantes
Dijon
Besançon
Poitiers
CERN
Limoges
Clermont-Ferrand
Lyon
Grenoble
Bordeaux
Cadarache
Nice
Montpellier
Toulouse
Pau
Marseille
Corte
RENATER-5
Lille
Caen
Rouen
Compiègne
Reims
Paris
Kehl
Strasbourg
Nancy
Rennes
Le Mans
Angers
Orléans
Tours
Nantes
Dijon
Besançon
Poitiers
Genève
Limoges
Clermont-Ferrand
Lyon
Grenoble
Bordeaux
Cadarache
Nice
Montpellier
Toulouse
Pau
Marseille
Corte
Fibres optiques noires
Liaison 2,5 Gbit/s
Liaison 1 Gbit/s (GE)

RENATER 5


Interconnexion des équipements du
Backbone Lothaire à Renater
Reims
Renater
Paris
Strasbourg
Extraction de longueurs
d'onde 10Gb/s
Extraction de liens Ethernet
10Gb/s pour GRID 5000
Routeur
Lothaire Nancy
Routeur
Lothaire Metz
CIRIL
PLG
Sciences
UHP
Connnexion 10Gb/s Ethernet

RENATER 5

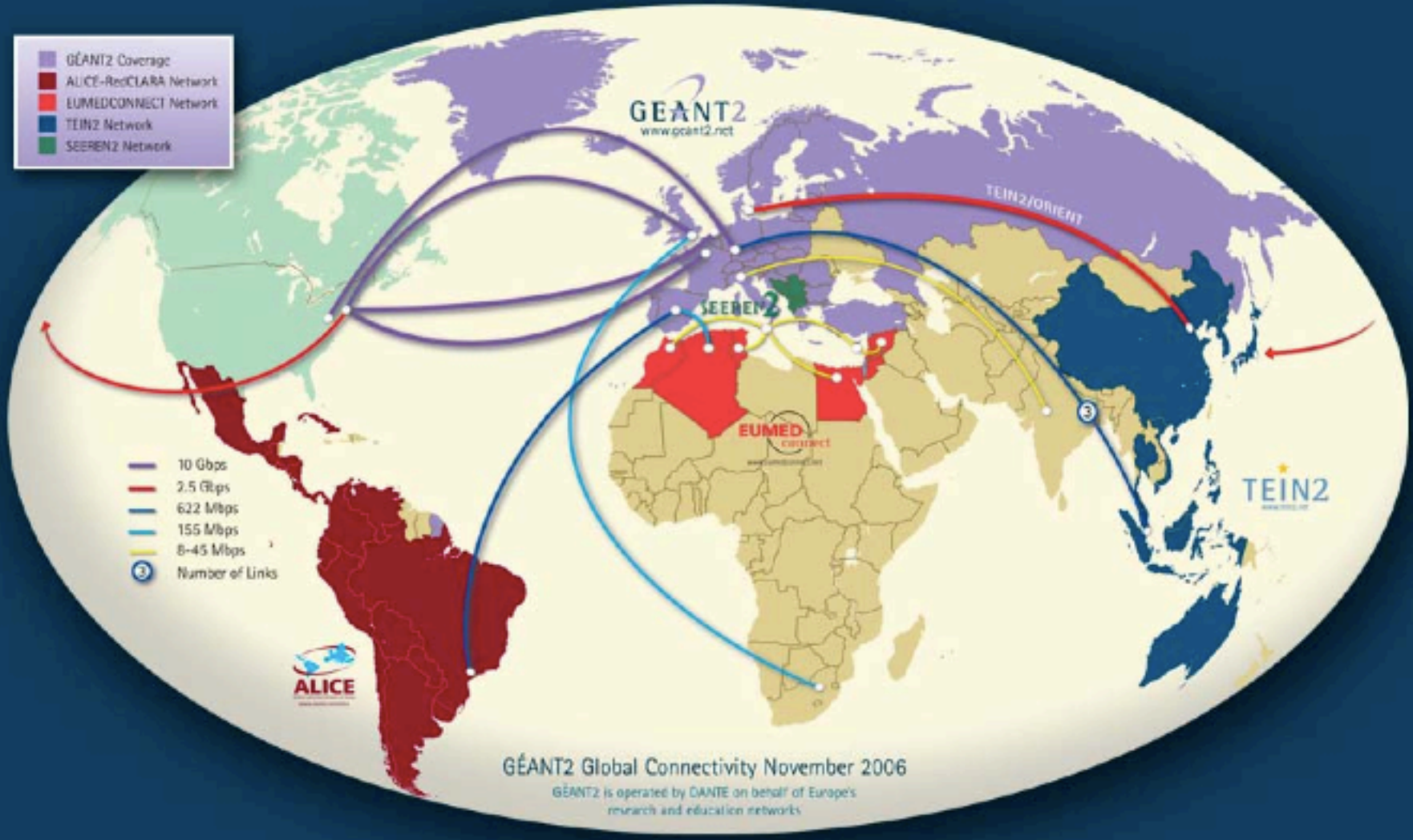
- Services de
  - Connectivité en IPV4 et IPV6 (unicast et multicast)
  - Mobilité : EDUROAM (http://www.eduroam.fr)
  - Visioconférence
  - Réseau privé virtuel
  - D'authentification
    - certificats serveurs
    - fédération d'identités (http://federation.cru.fr)
  - Supervision et métrologie
  - CERT Renater

RENATER 5

- Connexions Nationales et Internationales

  - Réseaux de la Recherche : Lien à 10 Gbps avec GEANT (réseau Européen) qui interconnecte les réseaux de :
    - Pays méditérannéens : EUMEDCONNECT
    - Zone Asie-Pacifique : TEIN2
    - Amérique du Sud : ALICE
    - Amérique Centrale : CLARA
    - Amérique du Nord : ABILENE
  - Internet National : SFINX (noeud d'échange)
    1 lien à 2x10 Gbit/s depuis Paris avec plus de 80 opérateurs
  - Internet Mondial : 2 liens à 10 Gbps depuis Paris et Lyon, via 2 opérateurs de transit : Cable&Wireless et Level3.

Connectivité mondiale



Pause

15 minutes

Au programme

14h00 : Présentation de l'équipe et de ses missions
14h20 : Un nouveau contexte pour Lothaire
14h35 : Evolutions de l'infrastructure du réseau Lothaire
15h20 : Evolutions Renater 5
Pause - 15 min
15h35 : Evolutions et nouveaux services réseau
16h40 : Hébergement et salle machine du CIRIL
Pot

reseau@ciril.fr

Portail des services réseau

Alexandre SIMON

Portail des services réseau

- Principe des outils réseau mis à disposition sur le *web*
  - pas de co-gestion des équipements et des services entre l'équipe réseau Lothaire et les équipes réseau des établissements
  - nécessité de mettre en ligne les outils pour permettre aux correspondants réseau d'administrer les équipements et les services
  - cloisonnement des autorisations : un correspondant ne voit *que* ce à quoi il a droit
- Avant juin 2007
  - de nombreux outils avec de nombreuses URLs
  - pas d'unification de l'authentification (ré-authentification à chaque changement d'outil)
  - pas de communications sécurisées en *HTTPS*
  - pas d'homogénéité des outils proposés

Portail des services réseau

- A partir de juin 2007
  - ouverture du portail http(s)://services.ciril.fr/
  - point d'entrée unique pour l'accès à tous les outils et informations réseau
  - unification de l'authentification (une seule authentification pour accéder à tous ses outils)
  - communication sécurisée par *HTTPS*

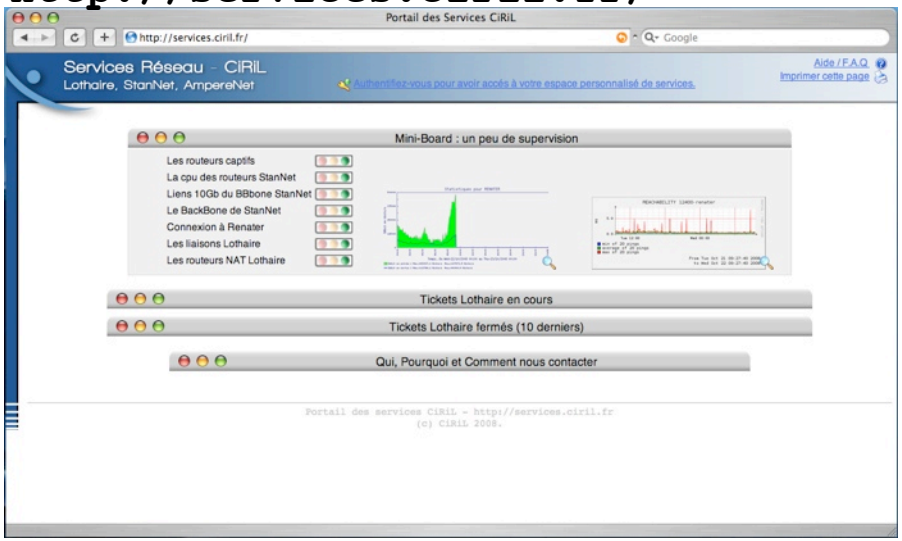
Portail des services réseau

- Portail à deux facettes

Portail des services réseau

- Portail à deux facettes

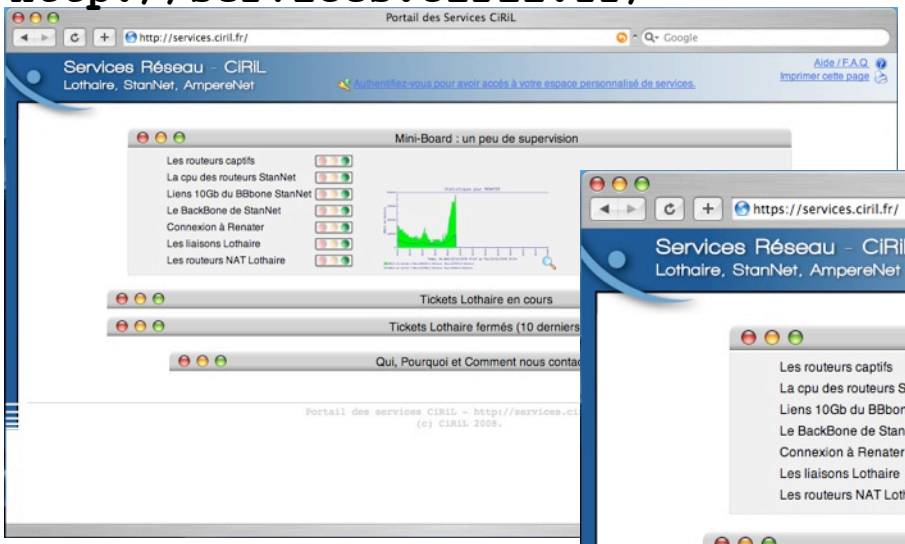
http://services.ciril.fr/



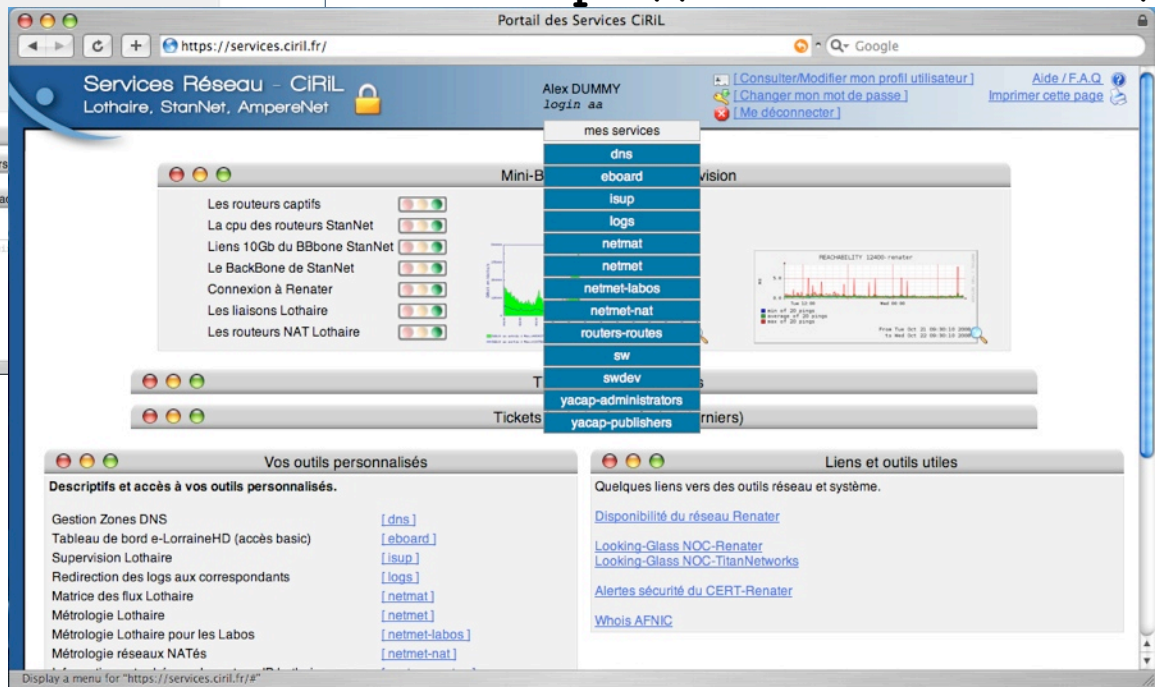
Portail des services réseau

- Portail à deux facettes

http://services.ciril.fr/



https://services.ciril.fr/



Portail des services réseau

- Fonctionnement
  - le portail est fait un *proxy web* qui transpose et cache les serveurs internes qui hébergent véritablement les applications
  - le portail s'appuie sur le système d'information du CiRiL pour les authentifications/autorisations sur les outils
    - SI du CiRiL distinct des SI d'établissements :
      - le CiRiL a comme partenaires les Universités, mais également de nombreux autres établissements (32)
      - nécessité de maîtriser l'unicité des logins pour les droits d'accès
      - simplicité de gestion et robustesse de la solution

Portail des services réseau

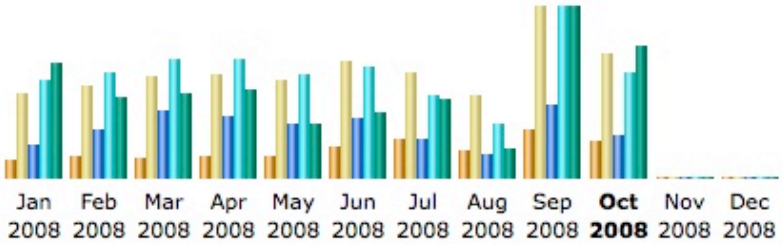
- Le système d'information du CiRiL
  - Base « servuser » (les services et les utilisateurs)
    - service: nom du service, description, URL
    - utilisateur : login/mot de passe, nom, prénom, email…
    - association service/utilisateur
      - attention ! ici on sait juste que *asimon* peut faire du *confin*, mais on ne dit pas à quels vlans il a droit
  - Base « noip » (l'adressage IPv4, IPv6 Lothaire)
    - description de tous les préfixes IPv4 et IPv6
    - description de tous les établissements
    - association préfixes/établissement-entité-site
  - Bases de configuration de chaque outil
    - association utilisateur/droits d'accès sur l'outil
  - Base « lothaire » (base administrative et institutionnelle)
    - description de tous les établissements
    - description des responsables (établissements, RSSI, correspondants réseau)
    - base utilisée pour la génération de la « convention Lothaire »

Portail des services réseau

- Evolution du SI
  - la diversité et la multitude des différentes bases sont historiques
  - il est temps aujourd'hui :
    - de rationaliser toutes ces informations dans une seule et même base
    - de simplifier et d'homogénéiser la gestion de ces informations
    - d'offrir une lisibilité plus fine du contenu de ces bases aux responsables et correspondants d'établissement
    - le projet est en cours…
- Evolution du contenu du portail réseau
  - migrer et remplacer les sites web « lothaire.net » et « stannet.net » par des pages d'informations à jour sur les réseaux lorrains (et surtout maintenables facilement dans le temps)
  - proposer de « vraies » présentations et documentations sur les services réseau rendus
  - le projet est en cours…

Portail des services réseau

- Le portail et le SI en quelques chiffres
  - 35 services *proxiés*
  - 437 utilisateurs connus dans « servusers » et ayant au moins accès à un service



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2008	254	1191	60324	174067	3.74 GB
Feb 2008	307	1291	86419	188023	2.63 GB
Mar 2008	281	1438	119705	212684	2.74 GB
Apr 2008	294	1465	110845	212064	2.82 GB
May 2008	316	1366	98624	185185	1.76 GB
Jun 2008	445	1643	105748	199999	2.13 GB
Jul 2008	550	1476	70684	149475	2.55 GB
Aug 2008	395	1150	43814	98603	975.66 MB
Sep 2008	692	2398	130253	306494	5.52 GB
Oct 2008	518	1743	77508	190628	4.27 GB
Nov 2008	0	0	0	0	0
Dec 2008	0	0	0	0	0
Total	4052	15161	903924	1917222	29.12 GB

Le service DNS

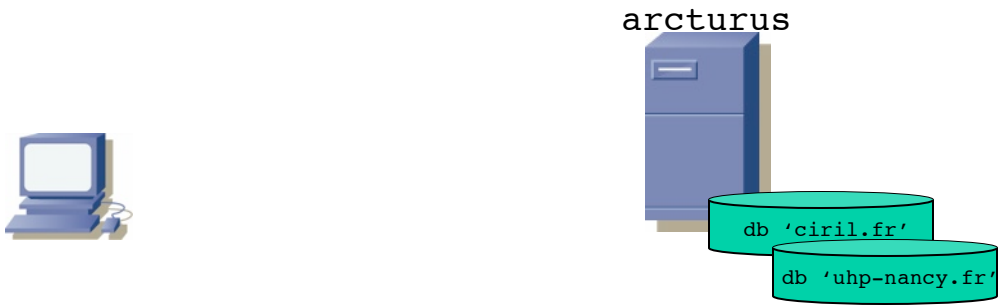
Alexandre SIMON

Service DNS régional

- Synthèse du service :
  - service rendu par l'Equipe Réseau Lothaire depuis avril 2008
  - résolutions de noms à échelle régionale
    - 2 serveurs dédiés (arcturus et orion)
  - résolutions de type « autoritaires » et « récursives » séparées:
    - résolutions « autoritaires » pour tous les clients
    - résolutions « récursives » uniquement pour les clients Lothaire (restriction par réseaux IP)
  - support des adresses IPv4 et IPv6
    - serveurs arcturus et orion en double pile v4/v6
    - support des enregistrements « A » et « AAAA »
  - pas de support des enregistrements « automatiques »
  - hébergement des zones « primaires » et « secondaires »
  - interface de demandes https://services.ciril.fr/DNS

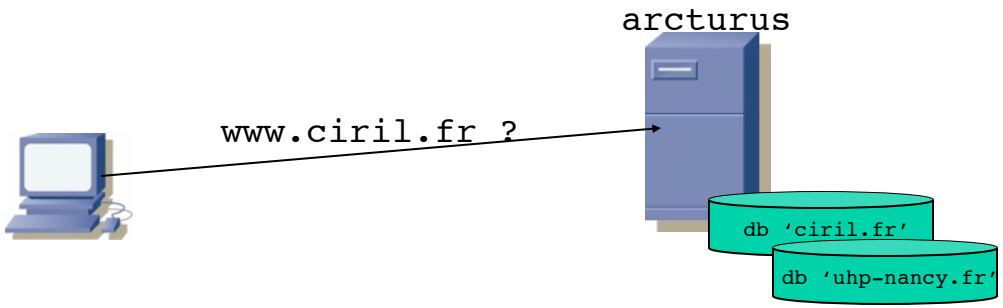
Service DNS régional

- Résolutions « autoritaires » *versus* « récursives »



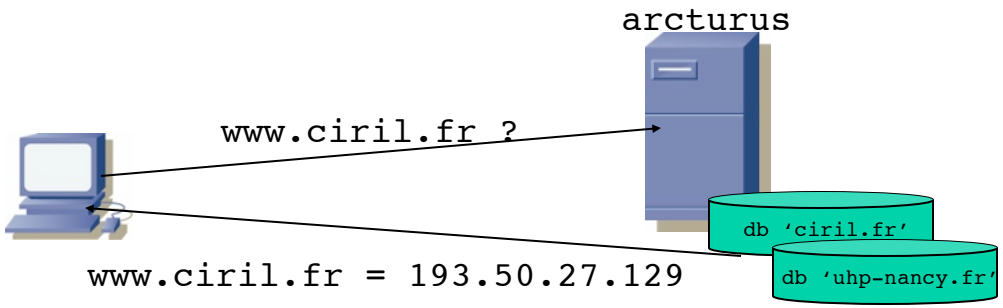
Service DNS régional

- Résolutions « autoritaires » *versus* « récursives »



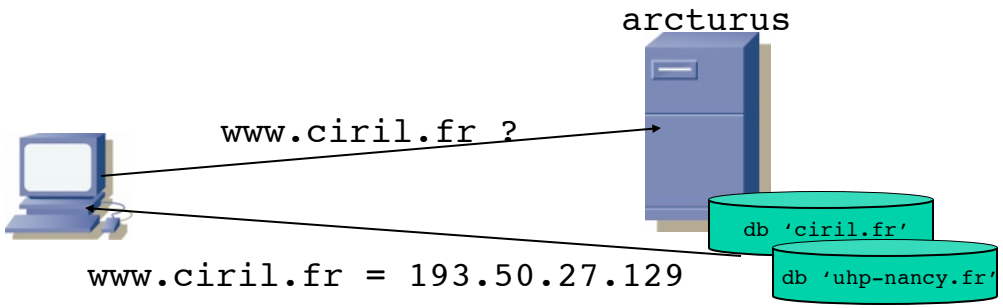
Service DNS régional

- Résolutions « autoritaires » *versus* « récursives »



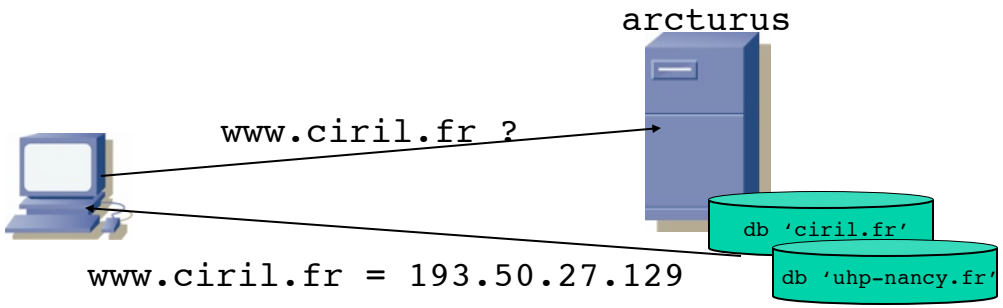
Service DNS régional

- Résolutions « autoritaires » *versus* « récursives »



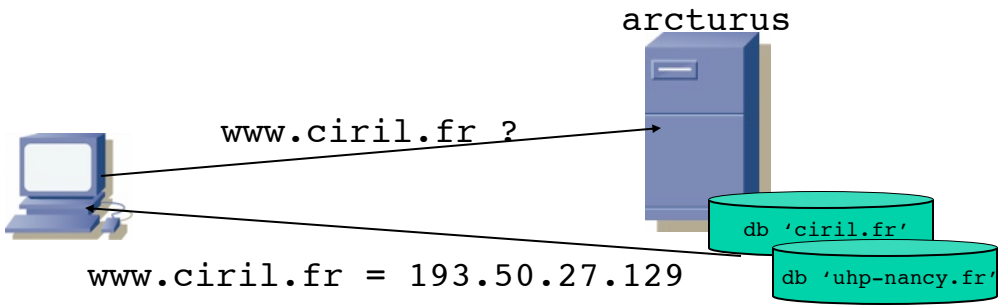
Service DNS régional

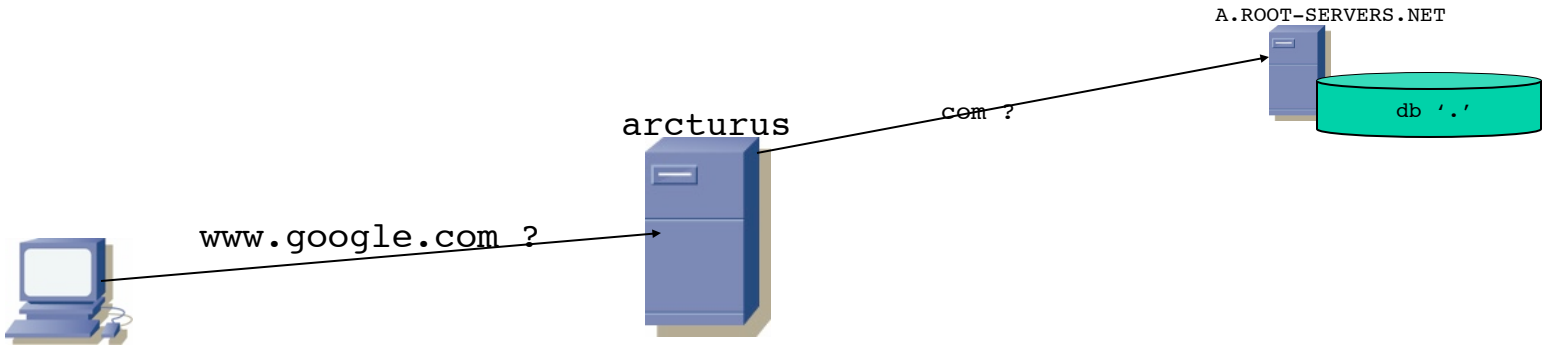
- Résolutions « autoritaires » *versus* « récursives »



Service DNS régional

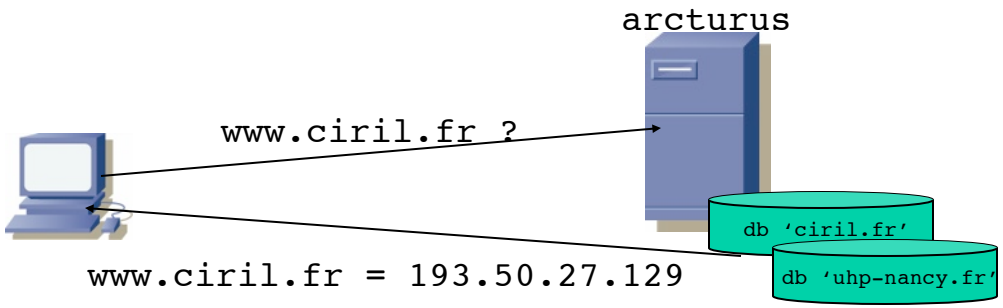
- Résolutions « autoritaires » *versus* « récursives »

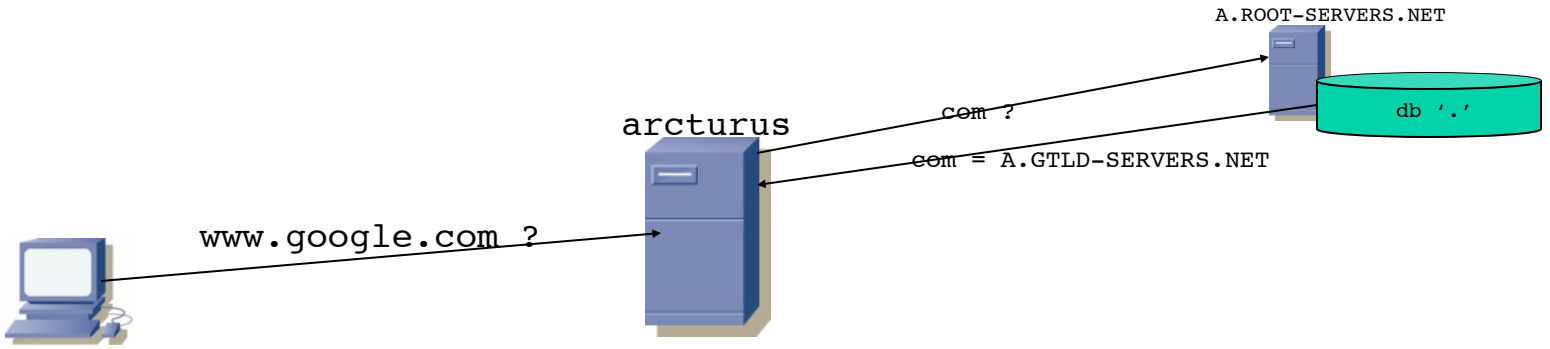




Service DNS régional

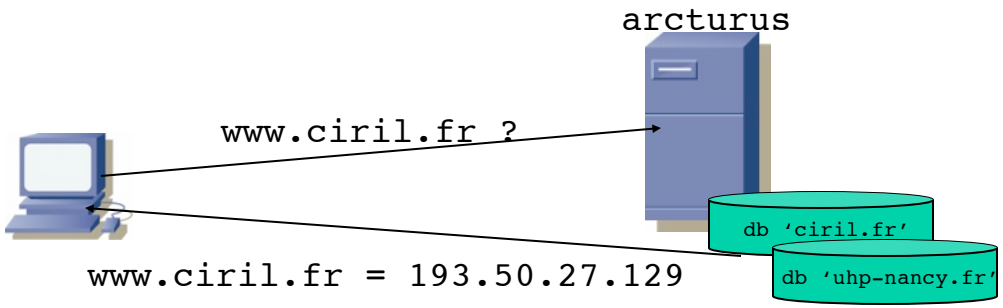
- Résolutions « autoritaires » *versus* « récursives »

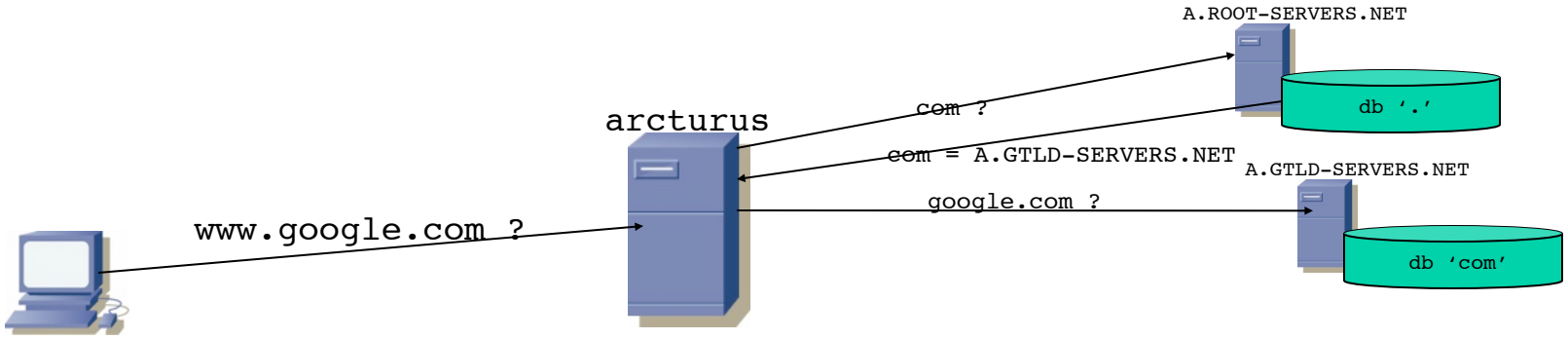




Service DNS régional

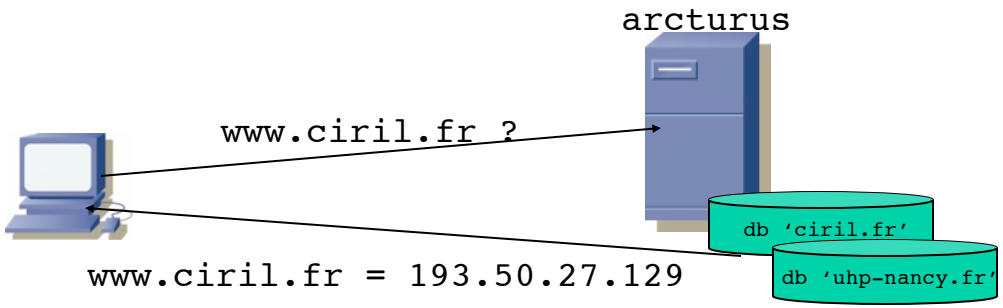
- Résolutions « autoritaires » *versus* « récursives »

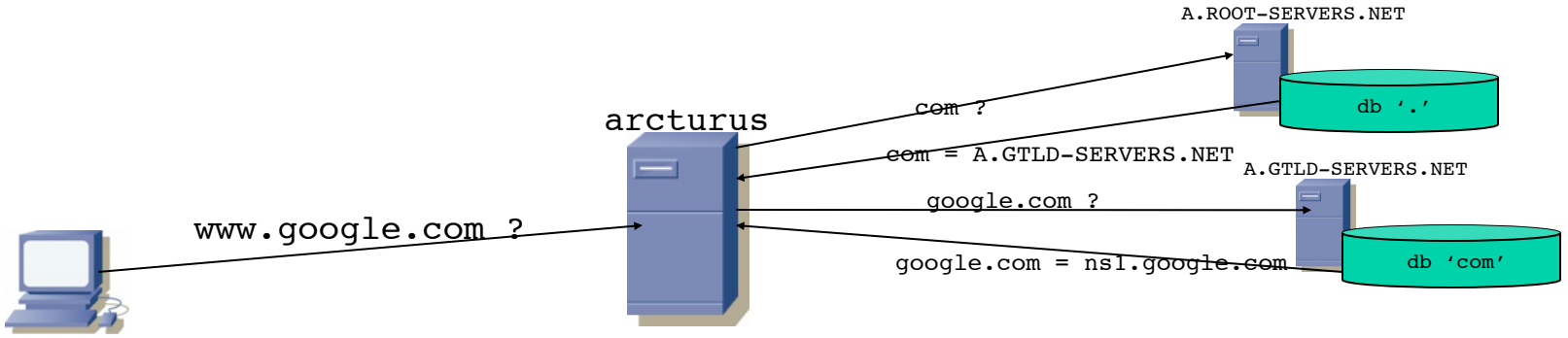




Service DNS régional

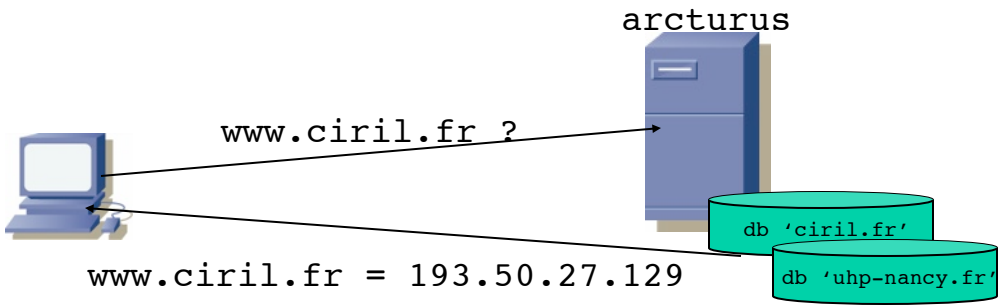
- Résolutions « autoritaires » *versus* « récursives »

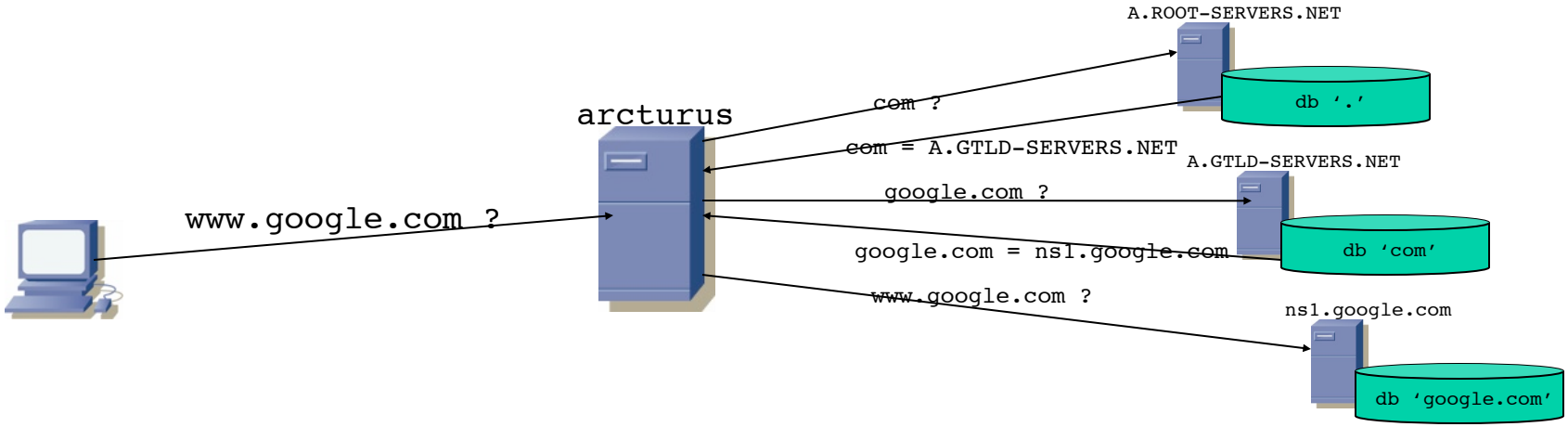




Service DNS régional

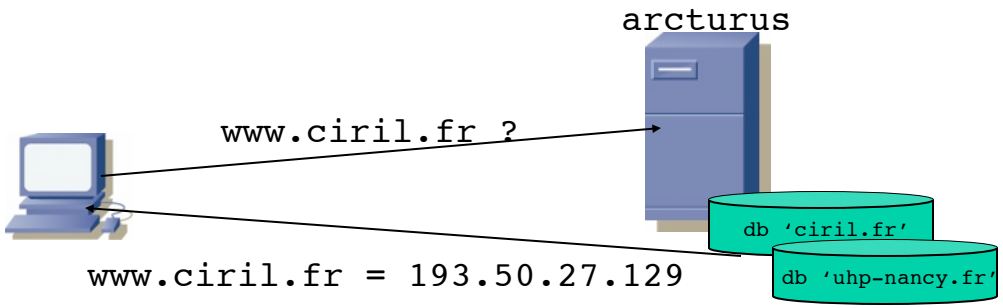
- Résolutions « autoritaires » *versus* « récursives »

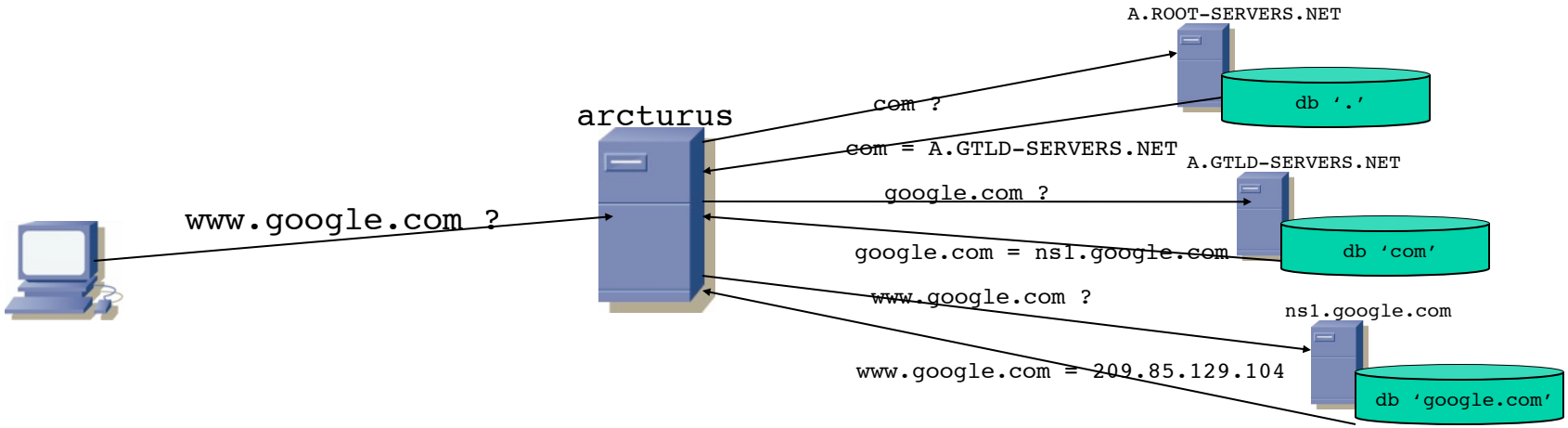




Service DNS régional

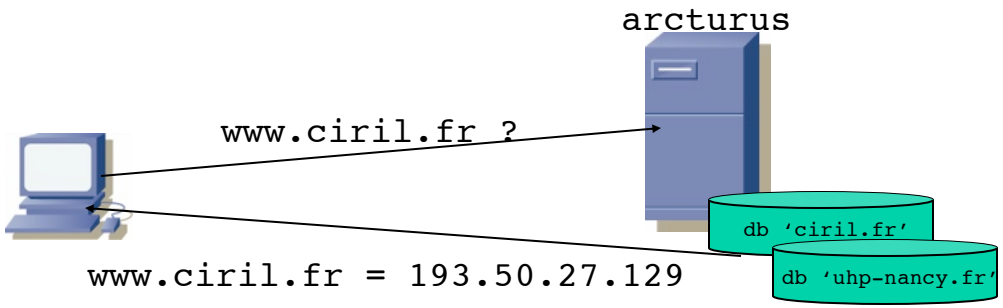
- Résolutions « autoritaires » *versus* « récursives »

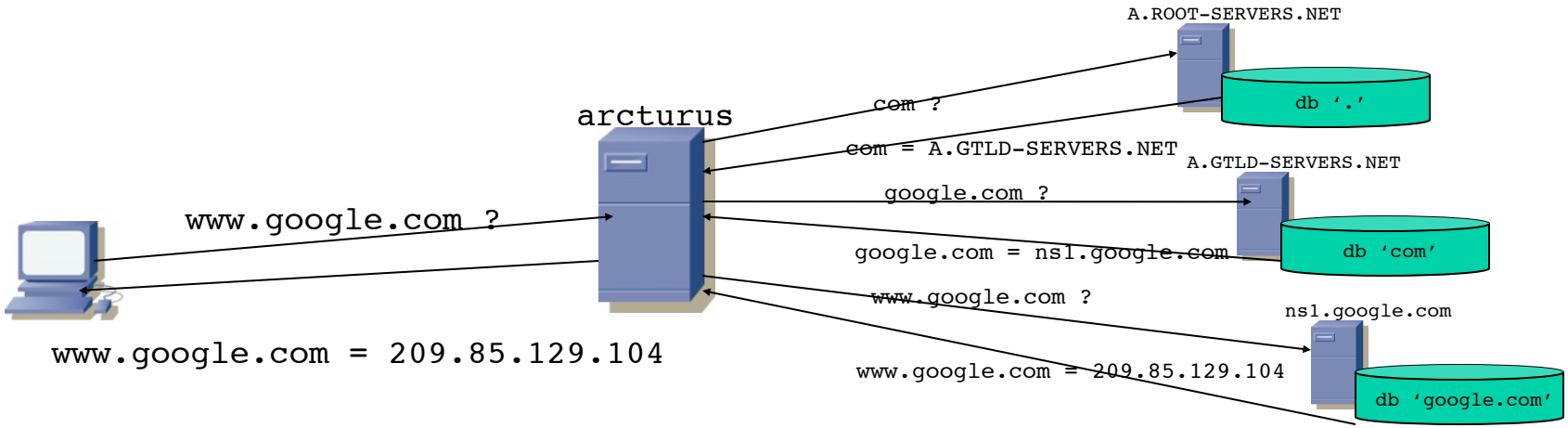




Service DNS régional

- Résolutions « autoritaires » *versus* « récursives »



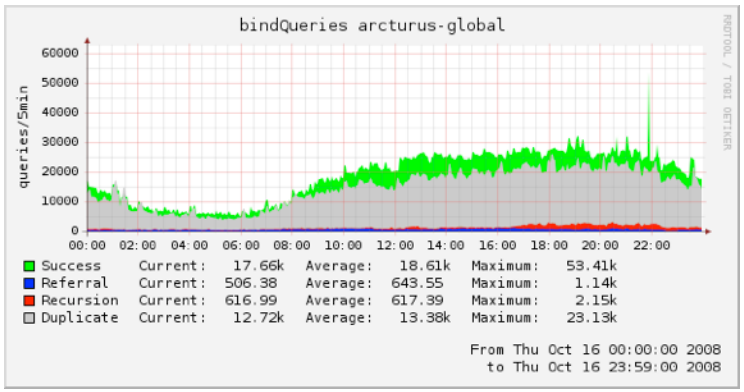


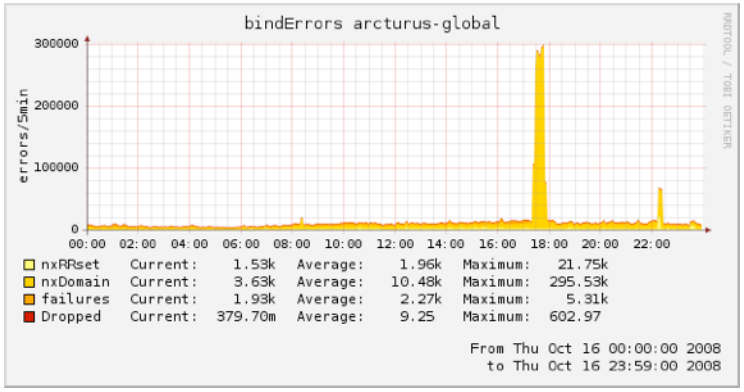
Service DNS régional

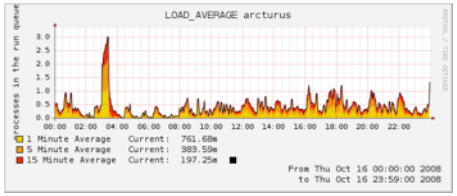
- arcturus et orion
  - serveurs faisant autorités sur des zones publiques, ouverts sur tout l'Internet en 53/udp et 53/tcp
  - serveurs disponibles pour gérer les zones et domaines des établissements lorrains en « primaire » ou en « secondaire » (réplicat du primaire)
  - utilisables en « récursif » uniquement depuis les réseaux Lothaire en IPv4 et IPv6
    - `arcturus.ciril.fr - 193.50.27.66 - 2001:660:4503:201::66/64`
    - `orion.ciril.fr - 193.50.27.67 - 2001:660:4503:201::67/64`
  - serveurs à utiliser en fonction de la politique « configuration poste client » des établissements, exemples :
    - arcturus, orion
    - dns1_établissement, arcturus
    - dns1_établissement, dns2_établissement, orion,
    - …

Service DNS régional

- Le DNS en quelques chiffres
  - arcturus et orion font autorités sur 563 zones
    - 332 zones « primaires » contenant 37 517 enregistrements
    - 321 zones « secondaires » contenant 35 825 enregistrements
  - ils gèrent 12 millions de requêtes par jours avec des pointes à 133 requêtes/s







Service DNS régional

- Interface de demandes
  - https://services.ciril.fr/DNS/
- Interface non modifiée lors de la reprise du service DNS par l'Equipe Réseau Lothaire
  - interface beaucoup critiquée pour son manque d'ergonomie
  - cependant, elle a le « mérite » d'exister : 8004 demandes ont été traitées par l'interface depuis février 2000
- Etude et évolution de cette interface à venir, quelques pistes :
  - modification en directe
  - recherche avancée
  - importation / exportation
  - modification par série
  - …

Portail Captif

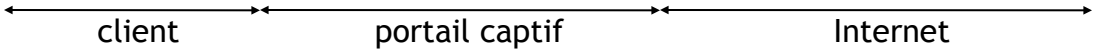
Alexandre SIMON

Portail Captif : YaCaP

- YaCaP : *Yet an other Captive Portal*
  - « un portail captif mutualisé permettant un accès authentifié au réseau pour les Universités et établissements lorrains »
- 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

Portail Captif : YaCaP

- Principe général



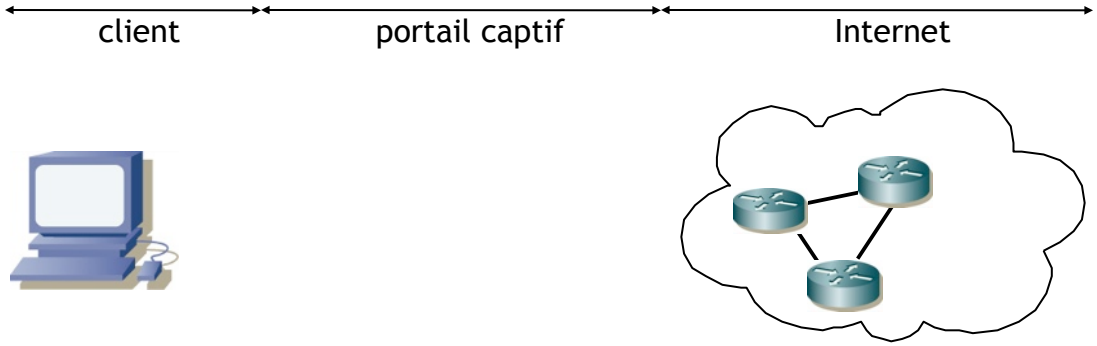
trafic

connexion / authentification
déconnexion

contrôle / autorisation

Portail Captif : YaCaP

- Principe général



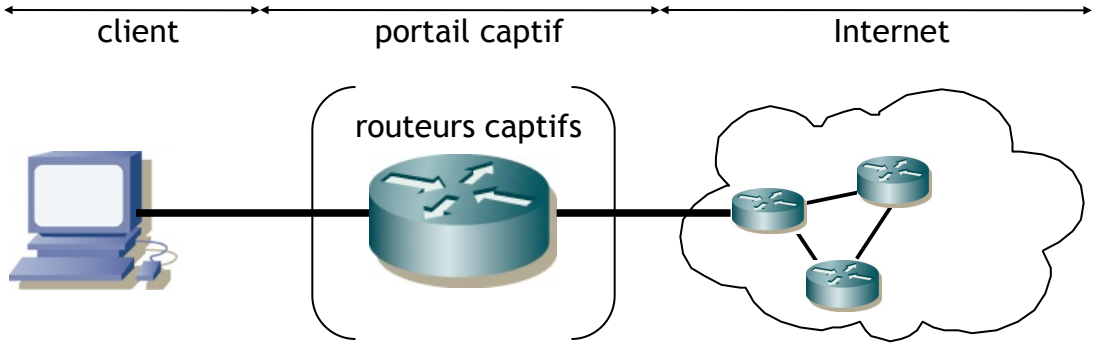
trafic

connexion / authentification
déconnexion

contrôle / autorisation

Portail Captif : YaCaP

- Principe général



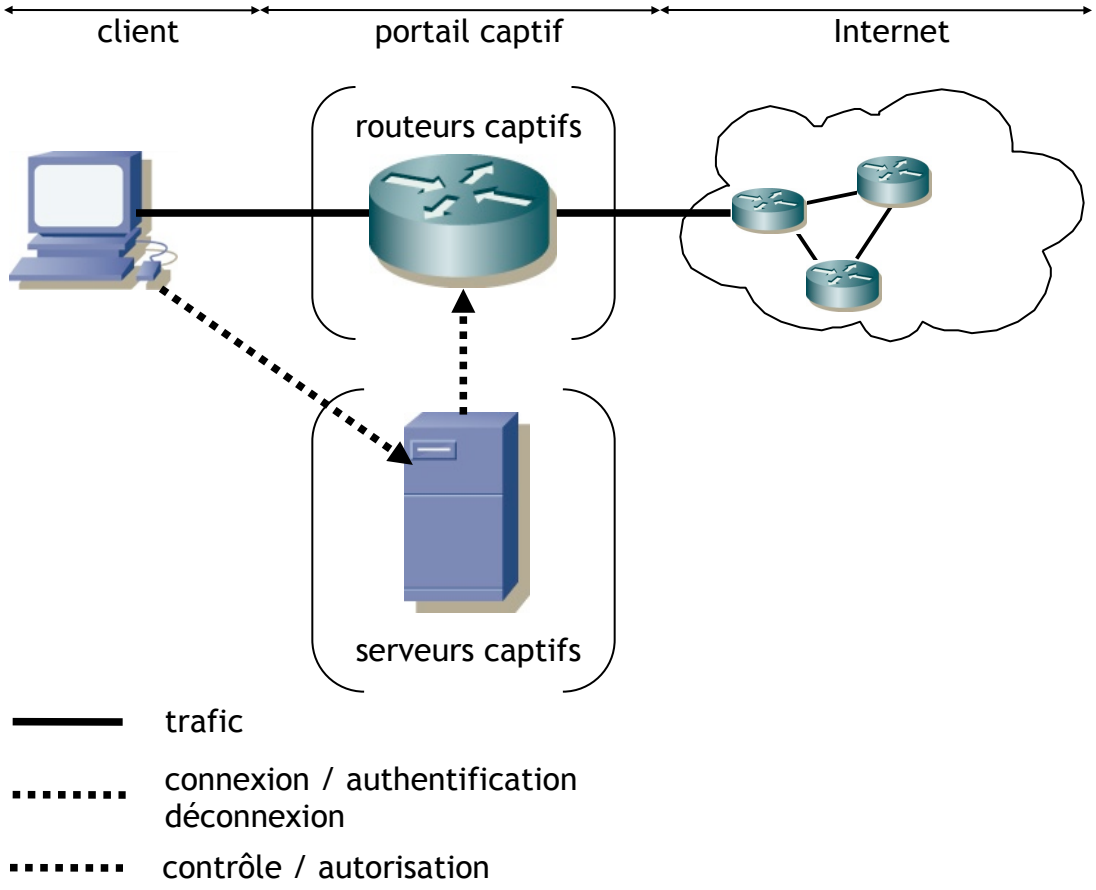
trafic

connexion / authentification
déconnexion

contrôle / autorisation

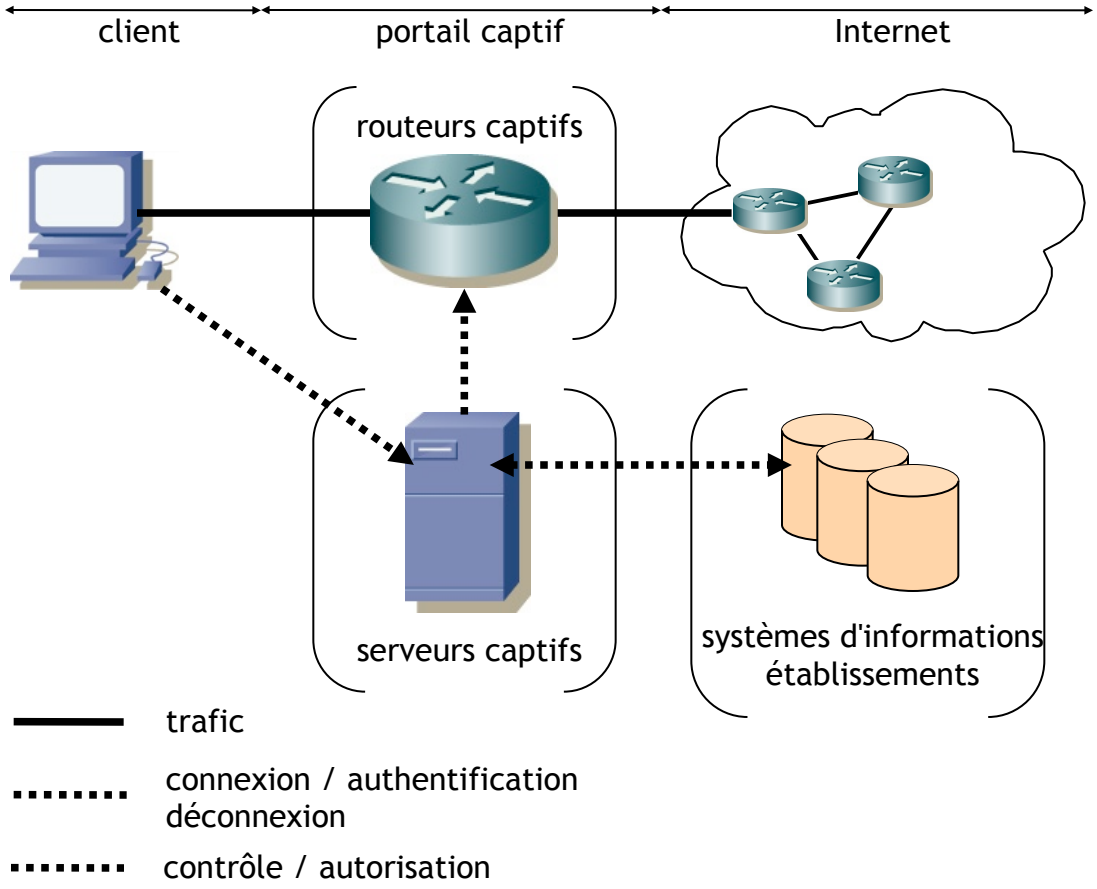
Portail Captif : YaCaP

- Principe général



Portail Captif : YaCaP

- Principe général



Portail Captif : YaCaP

- Fonctionnement
  - branchement poste client sur vlan captif
    - auto-configuration *DHCP*
  - démarrage du navigateur web par le client
    - redirection de la page demandée vers le système de choix d'authentification
  - choix de la provenance du client
    - redirection vers le système d'authentification choisi
  - authentification login/mot de passe
    - vérifications
    - ouverture des accès réseau pour le poste client
  - utilisation du réseau par le client
    - *popup* de session pour maintenir la session YaCaP ouverte
  - le client se déconnecte (ou se fait déconnecter)
    - fermeture des accès réseau pour le poste client

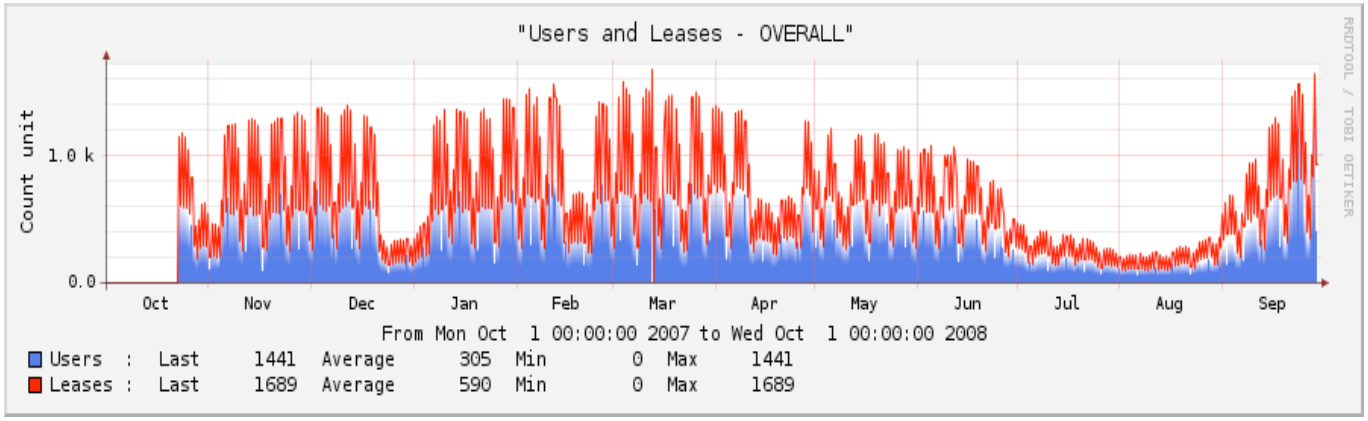
Portail Captif : YaCaP

- Délégations et systèmes d'information
  - YaCaP est conçu pour déléguer les authentifications/ autorisations aux établissements au travers d'interrogations CAS, LDAP/AD de leurs systèmes d'information
    - YaCaP s'appuie totalement sur les SI des établissements pour authentifier/ autoriser les utilisateurs
    - Possibilités de surcharger des paramètres de configuration définis en central par des paramètres positionnés dans les SI

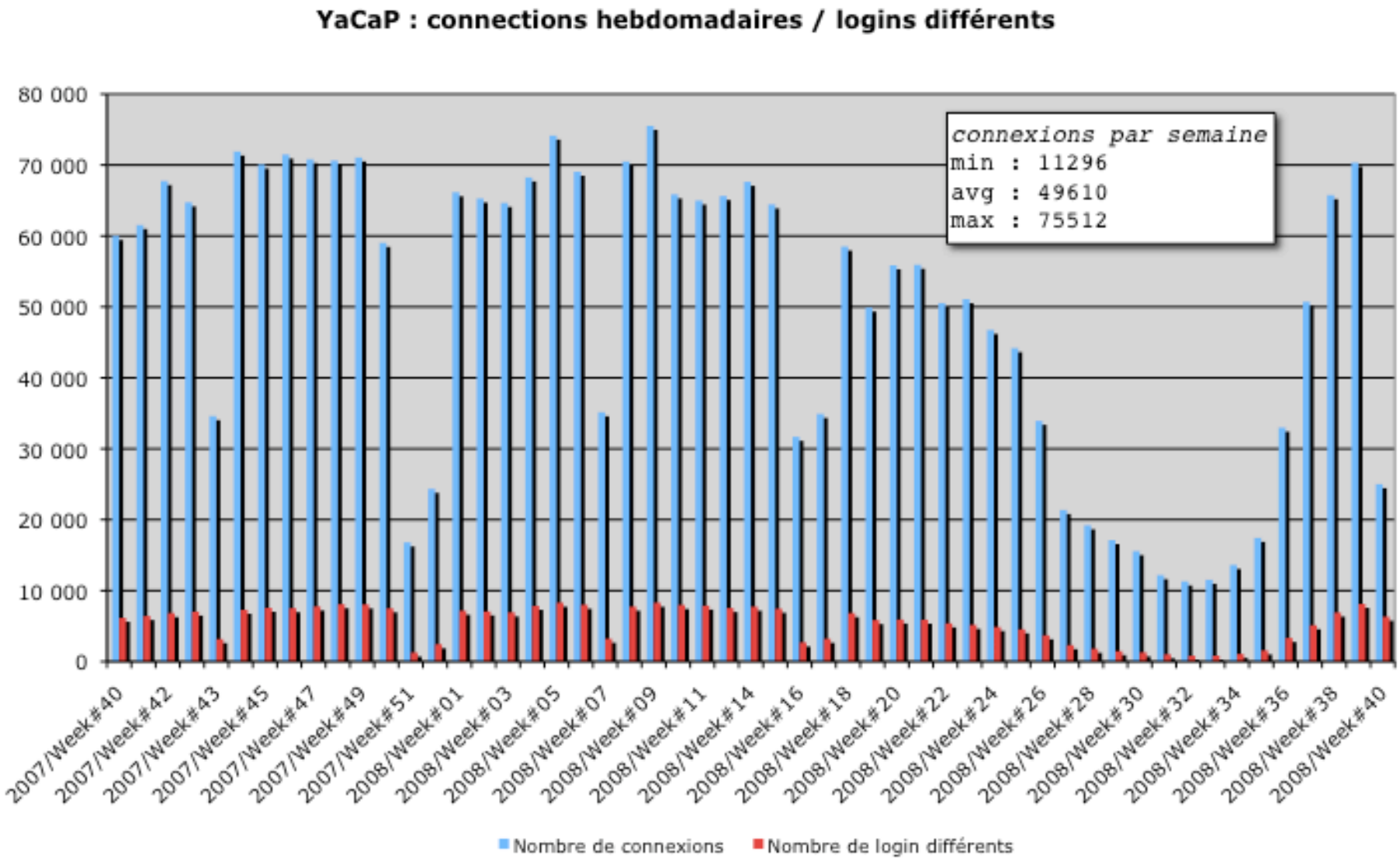
- Scénarii multiples d'authentification/autorisation : mutualisation inter-établissement et authentifications traversales
  - un réseau captif peut proposer plusieurs sources d'authen/authz
    - réseaux wifi « Nancy-Université », proposer l'ensemble des SI des universités
    - réseaux CROUS, proposer l'ensemble des SI des universités + SI du CROUS

Portail Captif : YaCaP

- YaCaP en quelques chiffres
  - Statistiques du 1er octobre 2007 au 1er octobre 2008
    - 63 vlans captifs
    - 6 serveurs + 3 routeurs captifs
    - nombre de connexions : 2 629 321
    - nombre maximum d'utilisateurs simultanés : 1 441
    - nombre de login différents : 31 001
    - nombre d'adresse MAC différentes : 31 030
    - nombre de connexions sans utilisation du DHCP : 8 063

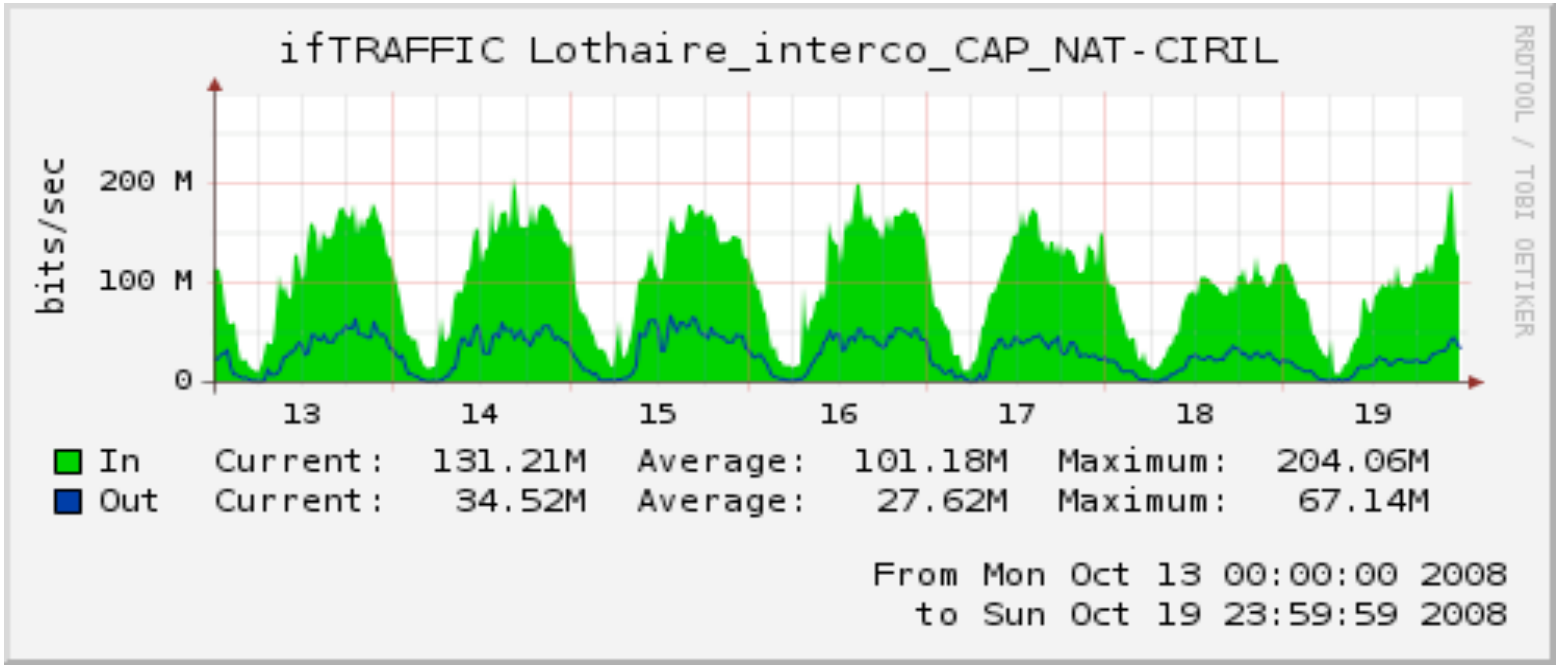


Portail Captif : YaCaP



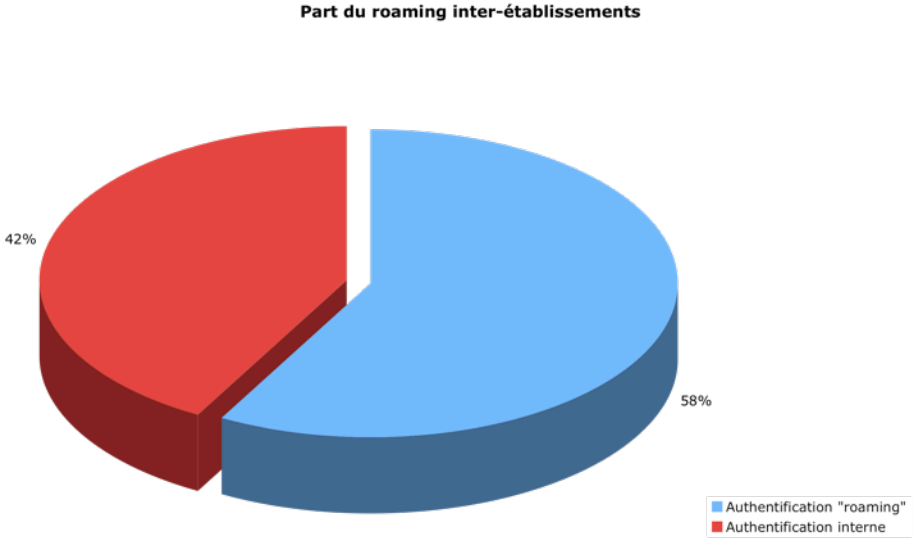
Portail Captif : YaCaP

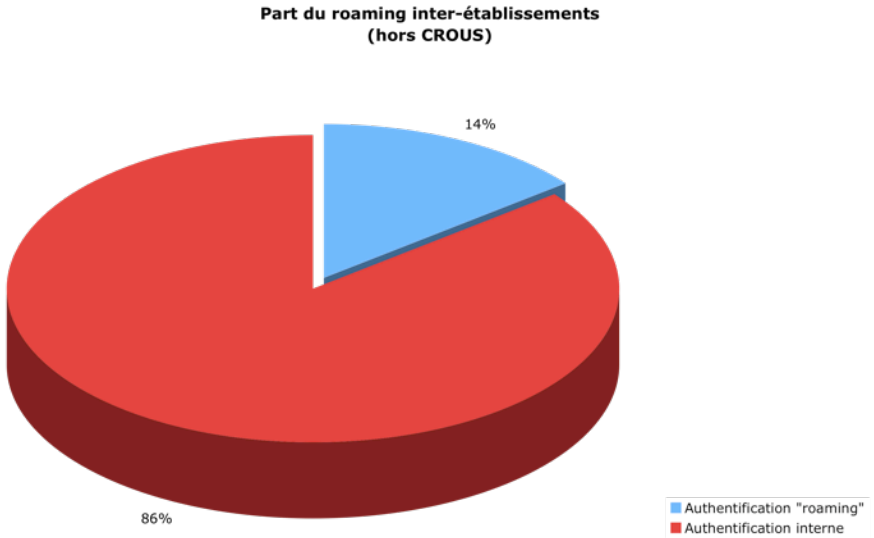
- YaCaP en quelques chiffres
  - Trafic total en entrée/sortie de tous les vlans captifs
  - en moyenne 100 Mb/s avec des max à 200 Mb/s



Portail Captif : YaCaP

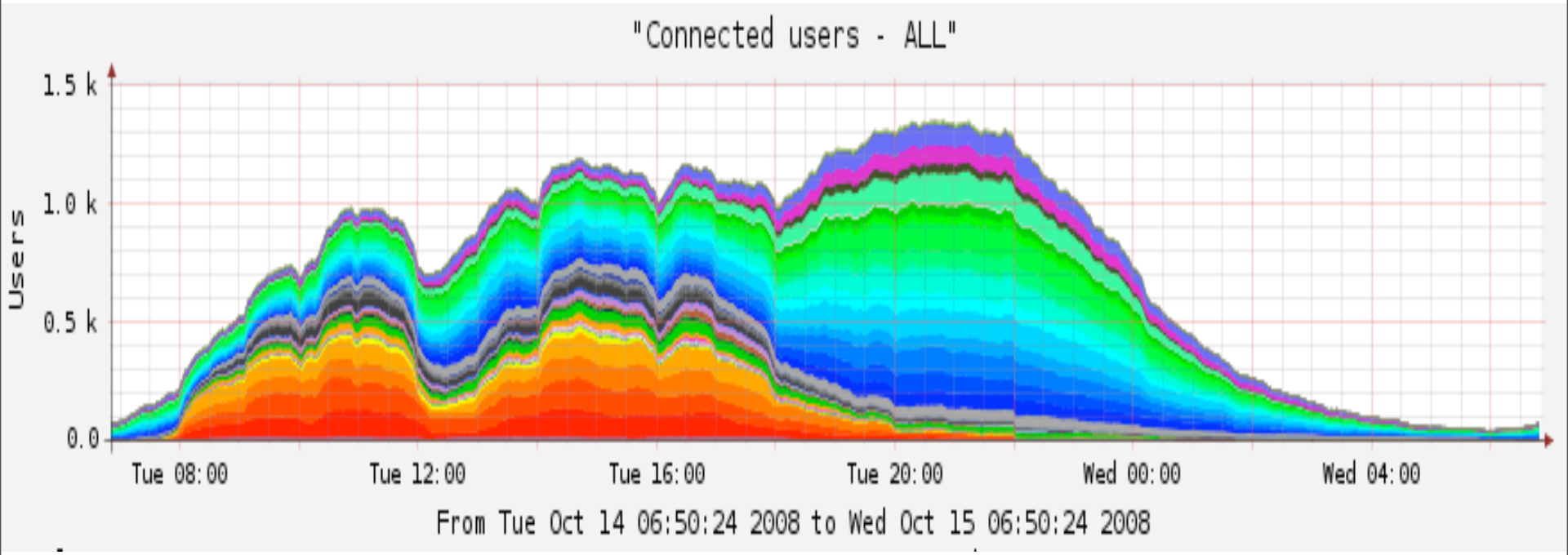
- YaCaP en quelques chiffres
  - « *Roaming* » des utilisateurs entre les établissements





Portail Captif : YaCaP

- YaCaP en quelques chiffres
  - Migration des étudiants vers le CROUS



Firewall

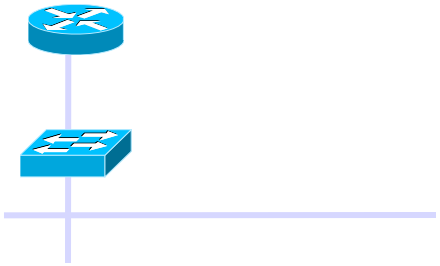
Vincent DELOVE

Service Firewall StanNet

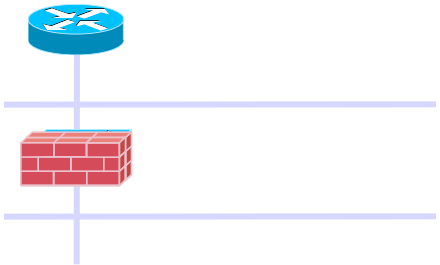
- Pourquoi ?
  - filtrage « stateful » : suivi des connexions
  - ouverture dynamique de ports (FTP,SIP)
- Pour qui ?
  - protection de serveurs
  - VLANs routés sur StanNet
- Comment ?
  - carte mutualisée dans le chassis du gw1.ciril
  - firewall en mode transparent

Firewall transparent

- Insertion d'une nouvelle interface de routage
  - Les clients ne changent ni de VLAN ni d'adresse IP
  - Le routeur utilise une nouvelle Interface VLAN
    - reprend la configuration IP (v4, v6)
    - conserve les access-list (v4, v6) classiques au besoin en entrée/sortie



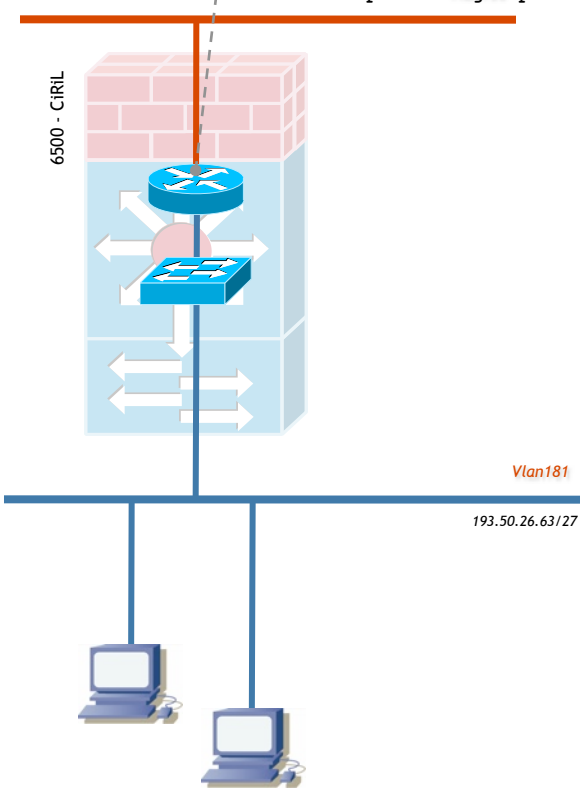
- Le firewall réalise le bridge entre les clients et le routeur
  - application des règles du firewall
  - support de certains protocoles uniquement (attention au multicast à IPv6, ou d'autres protocoles comme CDP)
  - administration du firewall par une adresse du VLAN



Firewall transparent

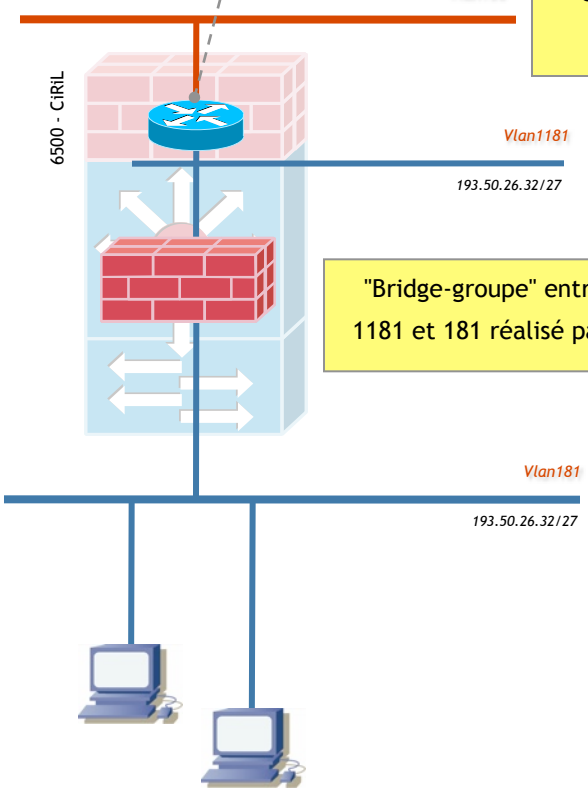
Avant

```
interface Vlan 181
 description ***** Vlan181 - CIRIL CRS *****

 ip address 193.50.26.62 255.255.255.224
 ip broadcast-address 193.50.26.63
 ip access-group vlan168-in in
 ip access-group vlan168-out out
```



Après

```
interface Vlan 1181
 description ***** Vlan181 - CIRIL CRS *****

 ip address 193.50.26.62 255.255.255.224
 ip broadcast-address 193.50.26.63
 ip access-group vlan168-in in
 ip access
```



On (peut) conserve(r) les ACLs classiques sur le routeur

"Bridge-groupe" entre les VLANs 1181 et 181 réalisé par le firewall

Firewall transparent

- Pas de changement du routage
  - Infrastructure des routeurs reste inchangée
  - Protocole de routage indépendant des firewall (EIGRP, ISIS, BGP)
  - Routage classique d'IPv6
  - Métrologie via NetFlow assurée comme pour le reste des réseaux
- 1 firewall transparent
  - = 1 domaine d'administration
  - = 8 bridge-group possibles
- Grande facilité de déploiement sur StanNet
- Contraintes
  - Acheminement des VLANs protégés jusqu'au point de concentration hébergeant le firewall
  - Routage conseillé des VLANs protégés sur le point de concentration hébergeant le firewall

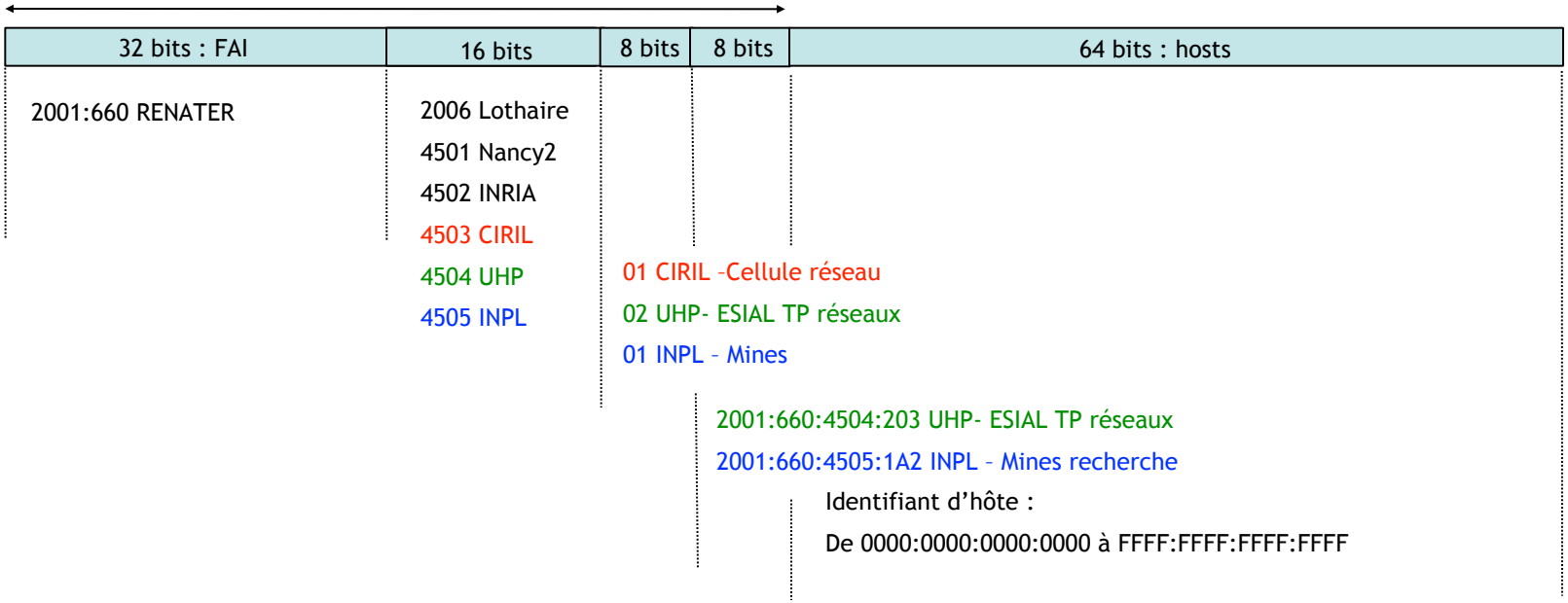
IPv6

Vincent DELOVE

IPv6

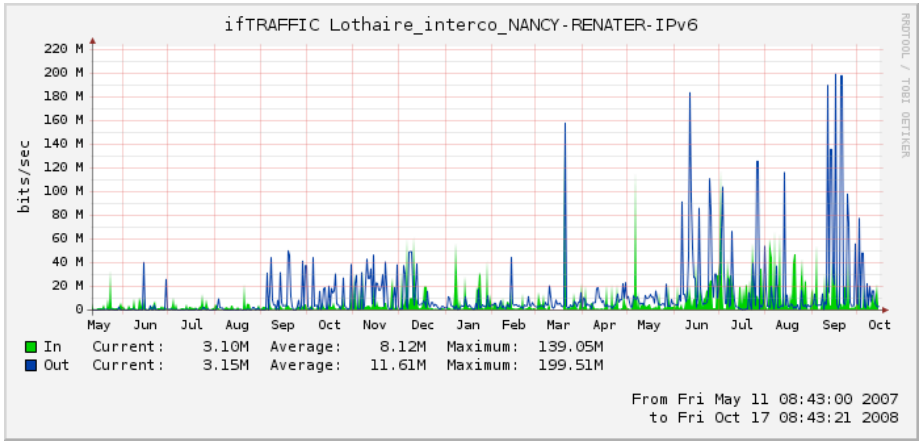
- Connectivité IPv6 existante depuis novembre 2000
  - architecture spécifique
  - utilisation limitée à des réseaux de tests et de recherche
  - pas de services IPv6 (DNS)
- Participation au projet IPv6-ADIRE courant 2005
  - étude des possibilités
  - mise en production
  - création d'une base de documentation (http://ipv6.u-strasbg.fr)
  - déploiement de services IPv6 avancés tels que la mobilité ou le multicast
- Fusion des réseaux IPv4 et IPv6 début 2008
- Transport d'IPv6 sur Lothaire partout où cela est possible

- Adresses de 128 bits en notation hexadécimale
  - XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
  - exemple : 2001:0660:4503:0101:0000:0000:d5e3:9586
  - S'écrit aussi : 2001:660:4503:101::d5e3:9586
- Utilisation de 64 bits pour le préfixe réseau



IPv6

- Services IPv6
  - DNS : transport et enregistrement de ressources (2001:660:4503:201::66, 2001:660:4503:201::67)
  - ConfIn : mise en place d'ACLs IPv6
  - iSup : disponibilité des équipements IPv6
  - FTP, HTTP, NTP, …
- A v6fier
  - netMET/netMAT : en cours
- Migration v4/v6 ?
  - serveurs ≠ utilisateurs
  - cohabitation
    - Pas de NAT-PT
    - configuration de postes en double pile



Outil ‘SW’

Vincent DELOVE

- Nouvelle interface d'administration des switchs
  - Support étendu
  - Visualisation de l'état des ports
    - Voisin CDP
  - Possibilité de modifications des paramètres
    - description
    - speed : auto/10/100/1000 Mbps
    - duplex : auto/full/half
    - shut / no shut
    - affectation à un vlan
    - « vlans allowed »
    - portfast :
      - Le port ne participe plus au *Spanning Tree* (STP), passe immédiatement dans l' état *forwarding* : plus de délai d'attente lié au passage du port par différents états
    - serveurs VMPS
  - Visualisation des paramètres supplémentaires d'une interface
    - voice-vlan, channel-group, …

- Gestion des droits d'accès :
  - Un correspondant ne peut visualiser/modifier que les switchs de son site
  - Granularité du droit attaché au port
    - Exemple d'un switch mutualisé entre plusieurs entités
    - Droit rw : droit de modification
      - Modification d'un trunk soumise à validation (modification différée)
      - Sauvegarde systématique de la configuration
      - Envoi d'un message au correspondant
    - Droit ro : droit de lecture
    - Droit rs : droit d'activation / désactivation
  - Visualisation de tous les droits pour un switch donné
  - Visualisation de l'ensemble des droits de l'utilisateur

- Outil de recherche d'un poste :
  - Retrouve le port de connexion à partir
    - d'une adresse IPv4
    - d'une adresse MAC et d'un switch
  - Localisation
    - d'adresses dupliquées
    - d'intrusion (couplé à arpwatch)
  - Couplé à la gestion des droits
    - présentation du résultat si l'utilisateur dispose du droit de lecture

Supervision

Vincent DELOVE

- Mise en œuvre d'une plateforme de supervision
  - unification des outils
  - automatisation
  - multiplicité des usages
    - administrateurs/opérateurs des services
    - décideurs administratifs et financiers
    - correspondants locaux et proches des usagers
  - gestion des autorisations

- Réutilisation de briques logicielles
  - configurer / collecter / analyser / présenter
  - développements spécifiques
  - intégration de l'ensemble

iSup

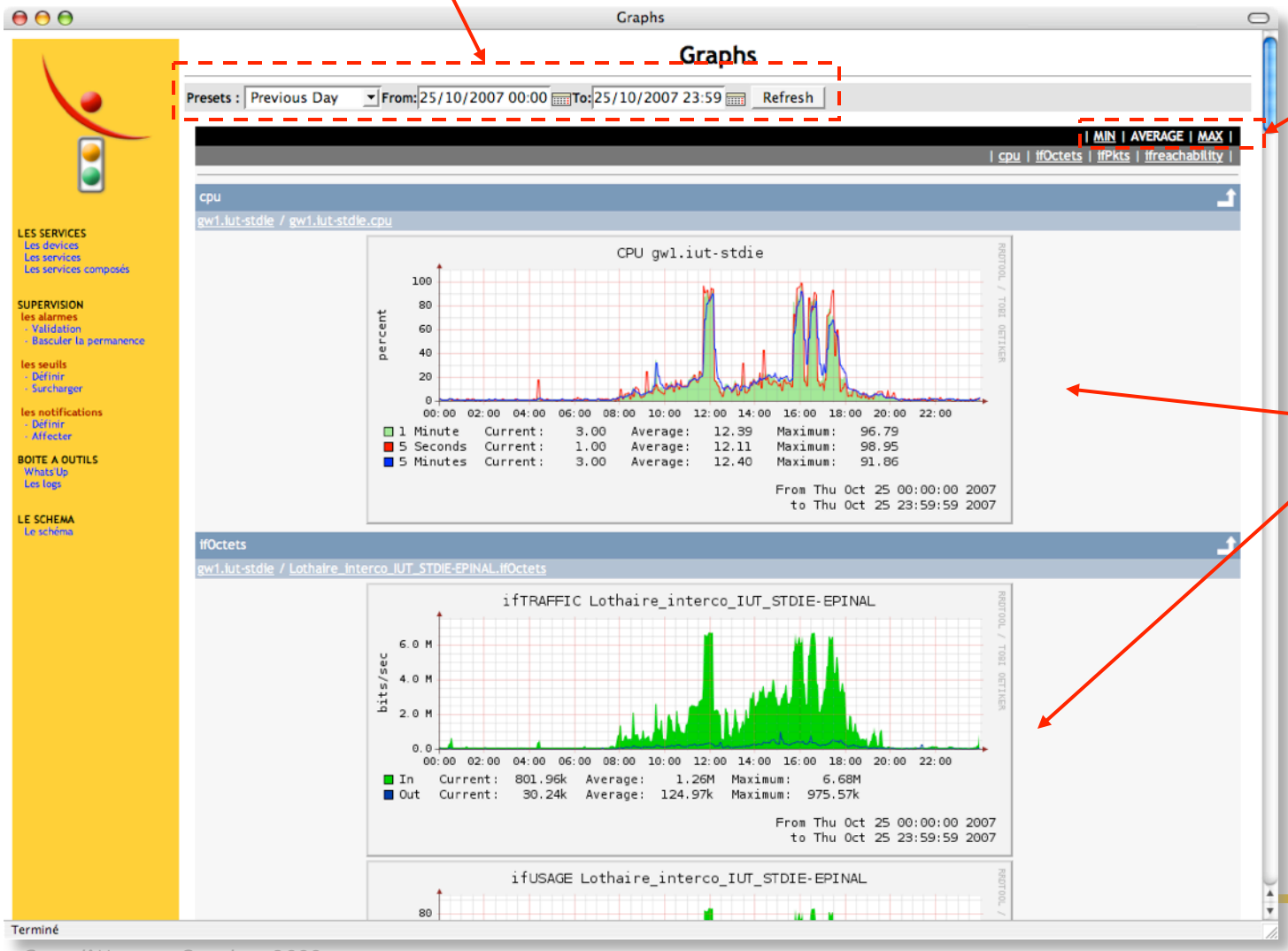
- Ouverture d'une vue sur le réseau
  - disponibilité des équipements
  - statistiques, mesure d'utilisation
  - disponibilité de services agrégés
- Pas de délégation de la configuration
  - supervision des équipements gérés par l'équipe réseau
  - possibilité d'ajouts sur demande des correspondants
  - potentiellement tout est supervisable
  - sélection de l'information la plus pertinente

- L'analyse des données génère pour chaque service un état
  - ROUGE : le service est indisponible
  - ORANGE : le service fonctionne
    - soit de façon dégradée
    - soit un risque de disfonctionnement a été détecté
  - VERT : le service fonctionne correctement
  - GRIS : l'état du service n'a pu être déterminé

- Un changement d'état peut donner lieu à des alertes ou à l'exécution de commandes
  - prendre en compte
    - la criticité du service ou de l'équipement
    - les plages horaires de supervision
    - les personnes à alerter
    - l'agrégation des alertes
  - activation/désactivation de la réception des alertes

iSup

Choisir la période d'affichage

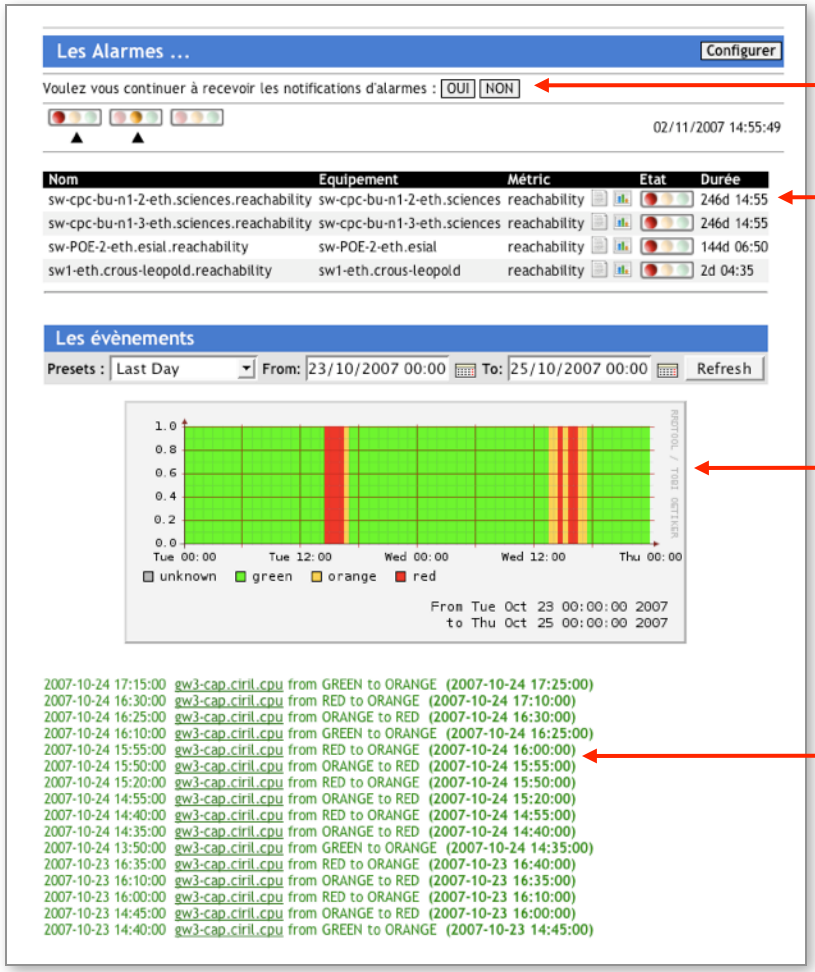


Choisir la valeur représentée :

- Minimum
- Moyenne
- Maximum

Disposer sur une même page des données différentes afin de permettre les corrélations

Tableau de bord



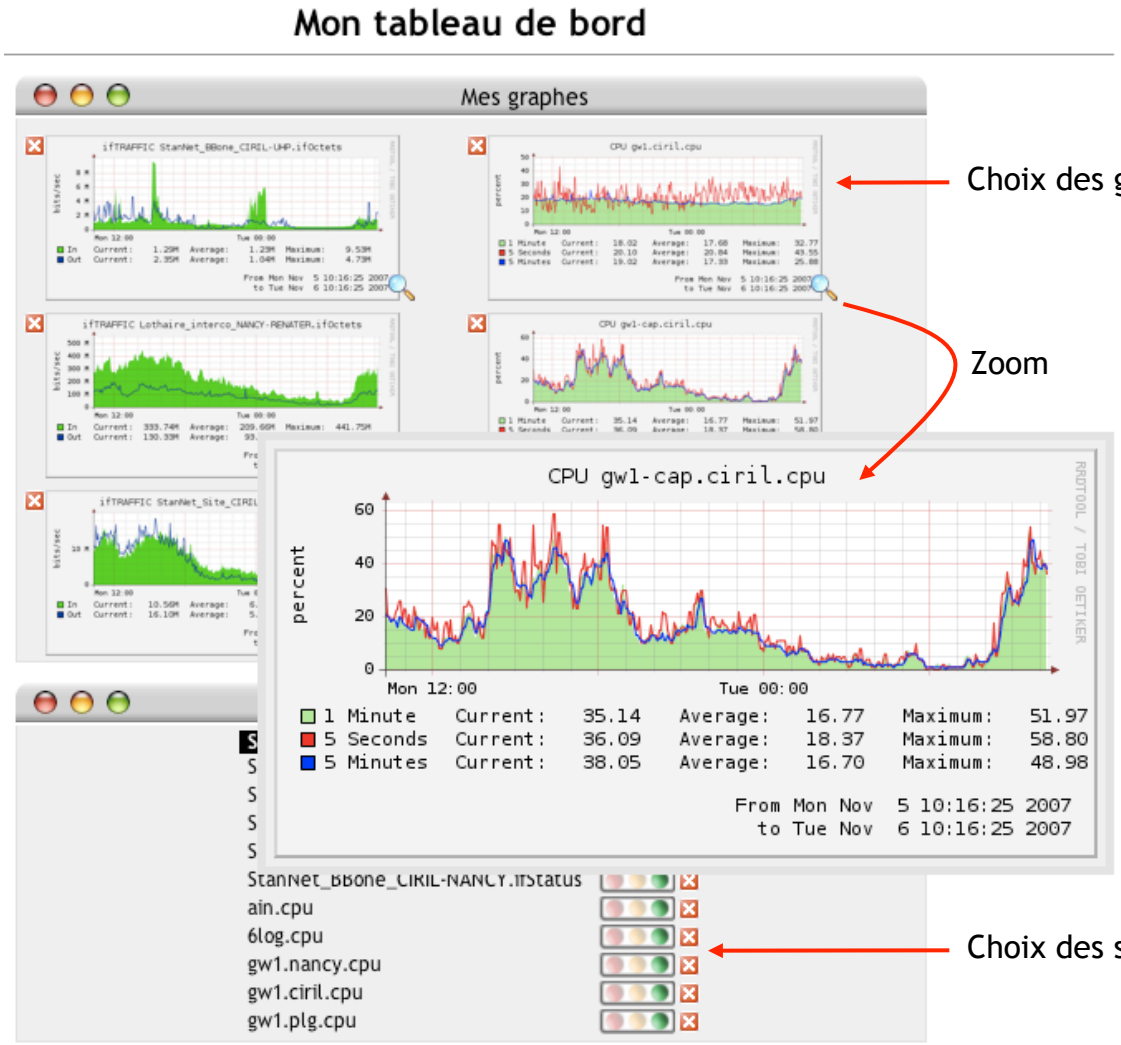
Configuration de la notification des alarmes

Alarmes en cours

Graphique de disponibilité du service

Journal des évènements

Tableau de bord



Choix des graphes favoris

Zoom

Choix des services favoris

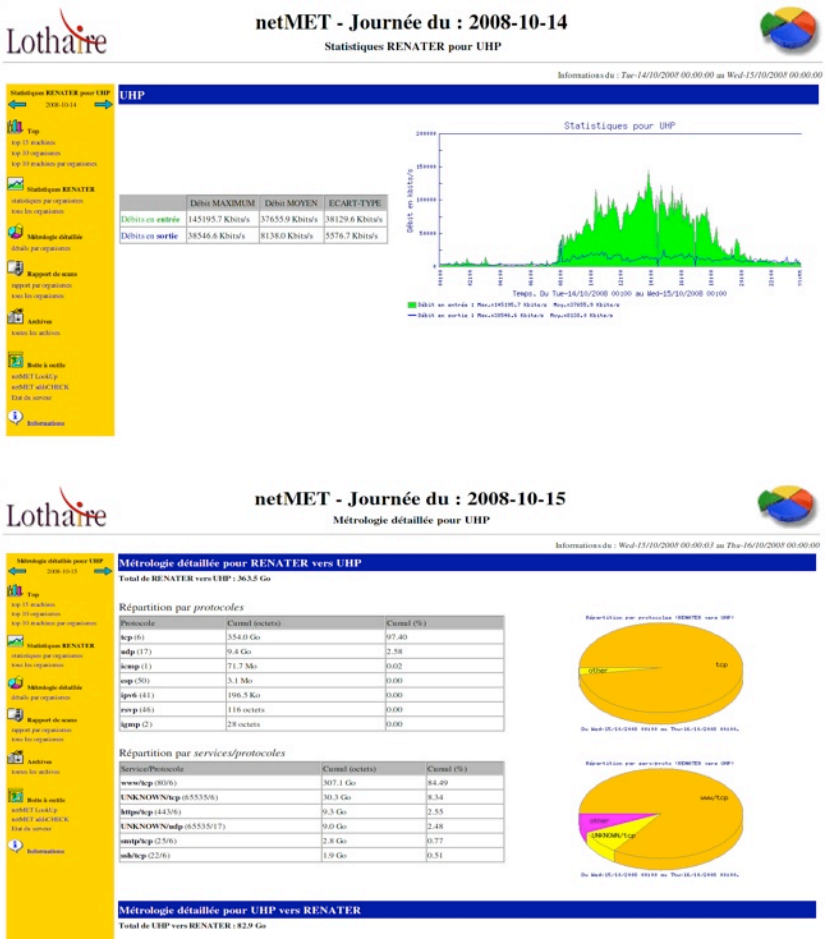
- En quelques chiffres
  - Plus de 1000 équipements supervisés
    - 265 routeurs
    - 765 commutateurs
    - 40 serveurs
    - 11 bornes WiFi
    - 8 onduleurs
    - 5 sondes de températures
    - 2 firewalls
  - 26 métriques : cpu, trafic, SAA, température, …
  - environ 3000 services, plus de 4000 graphes
  - 15 alertes par jour en moyenne

Métrologie

Karol PROCH

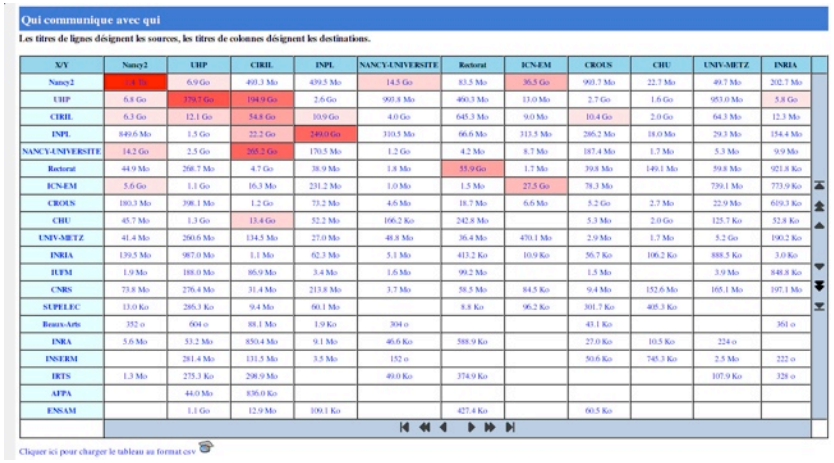
netMET

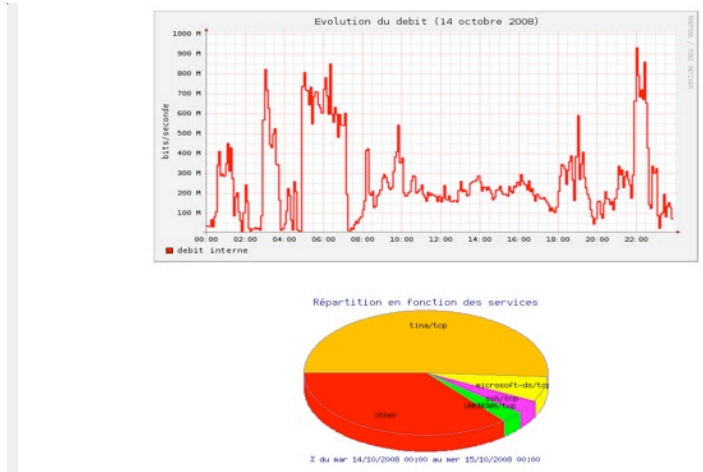
- Utilisé depuis 2000 pour mesurer le trafic entre Lothaire et Renater
  - débits en entrée, en sortie
  - volumes par organisme, par service/protocole, en entrée, en sortie
  - « tops » des organismes, des machines d'un organisme, ...



netMAT

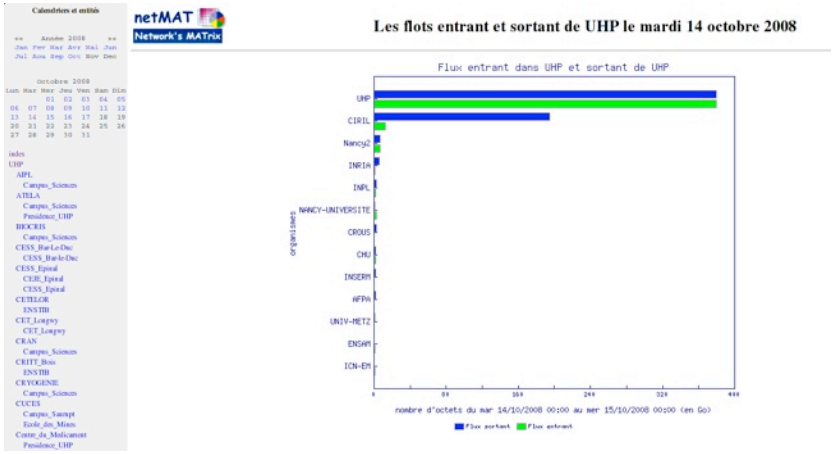
- Utilisé pour mesurer le trafic (routé) « interne » à Lothaire (collecte des informations de flux envoyées par les routeurs)
  - visualisation de la matrice des flux
  - évolution du débit
  - répartition en services / protocoles

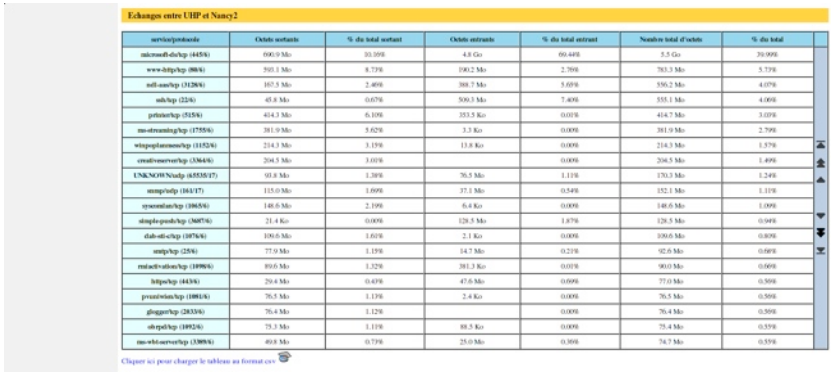




netMAT

- Ces informations sont disponibles pour chaque organisme et structurées selon les composantes et les sites de ces composantes.
- Des tableaux montrent la répartition en services/protocoles du trafic entre chaque couple d'organismes (ils peuvent être téléchargés au format CSV).



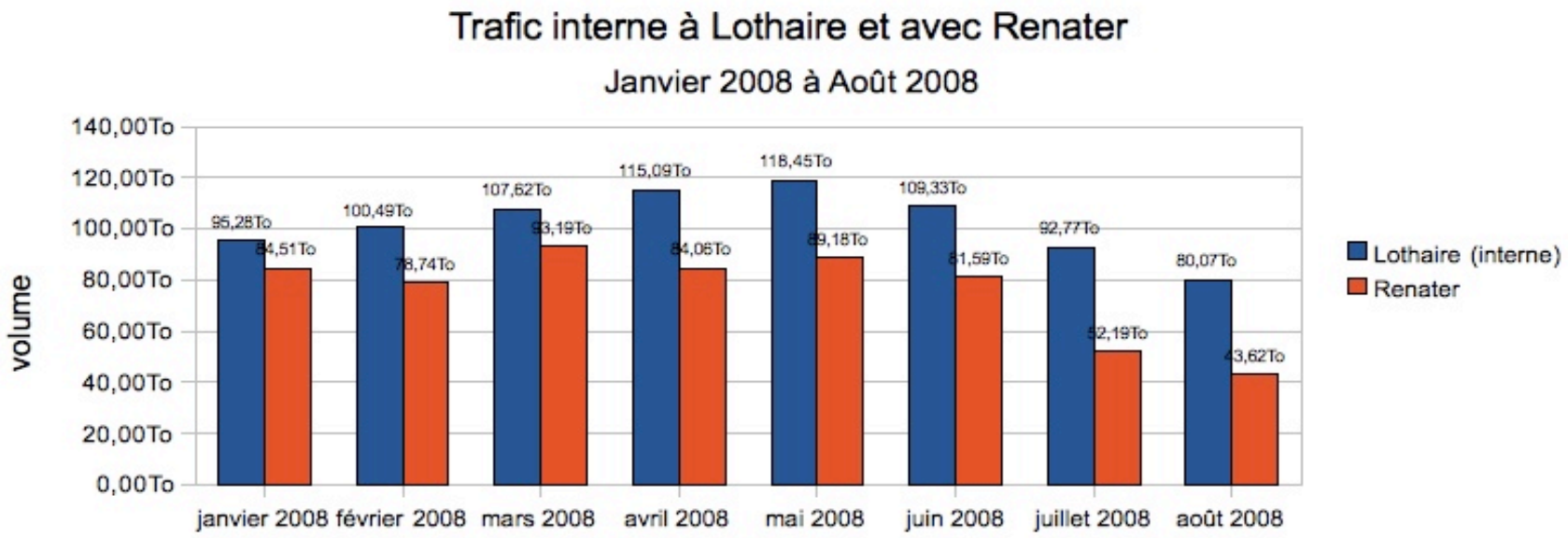


netMAT

- Les pages produites par netMAT sont accessibles via le portail des services dans les mêmes conditions que les pages générées par netMET.
- Une première distribution netMAT est (presque) prête, nous sommes en attente du « feu vert » du service Transfert et Valorisation de la Recherche pour distribuer netMAT sous licence CeCILL (licence française de logiciel libre créée par le CEA, le CNRS et l'INRIA).
- La suite :
  - « organiser » la diffusion du produit (site web)
  - prendre en compte IPv6 (réécriture du collecteur)

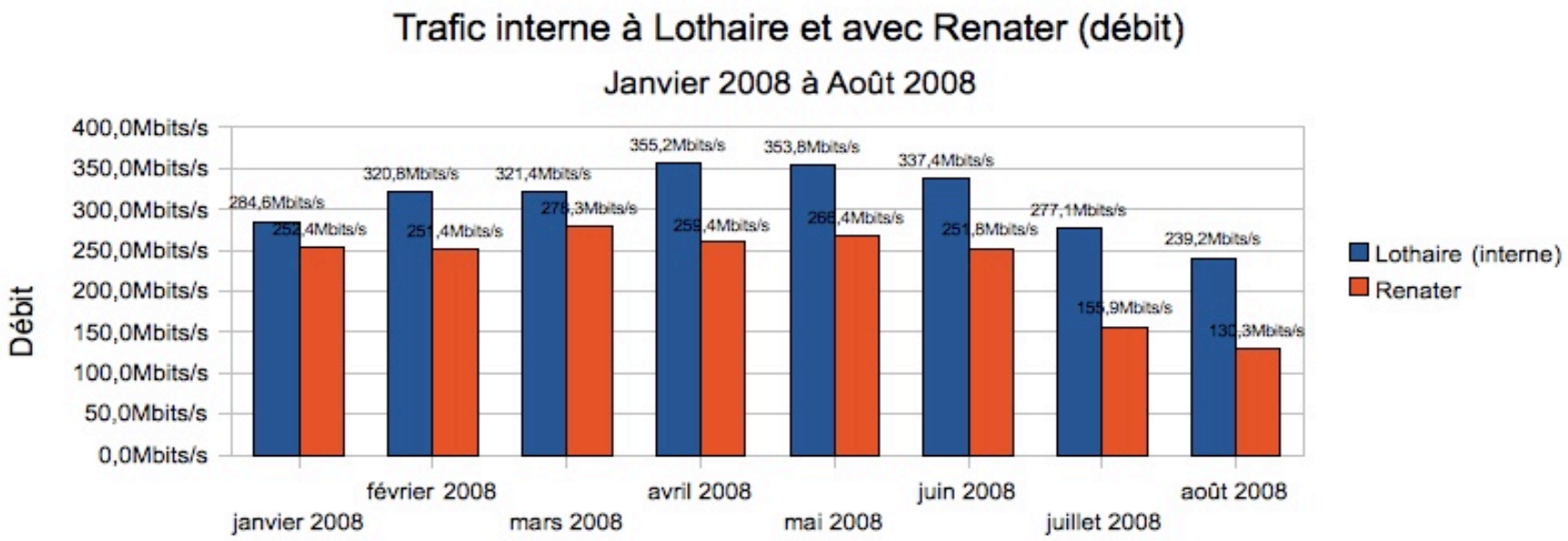
Quelques résultats

- La rédaction des dossiers relatifs au Contrat de Projet Etat-Région et au Fond Européen de Développement Régional a conduit à synthétiser les informations issues de netMET/netMAT sur l'utilisation des réseaux Lothaire et Renater :



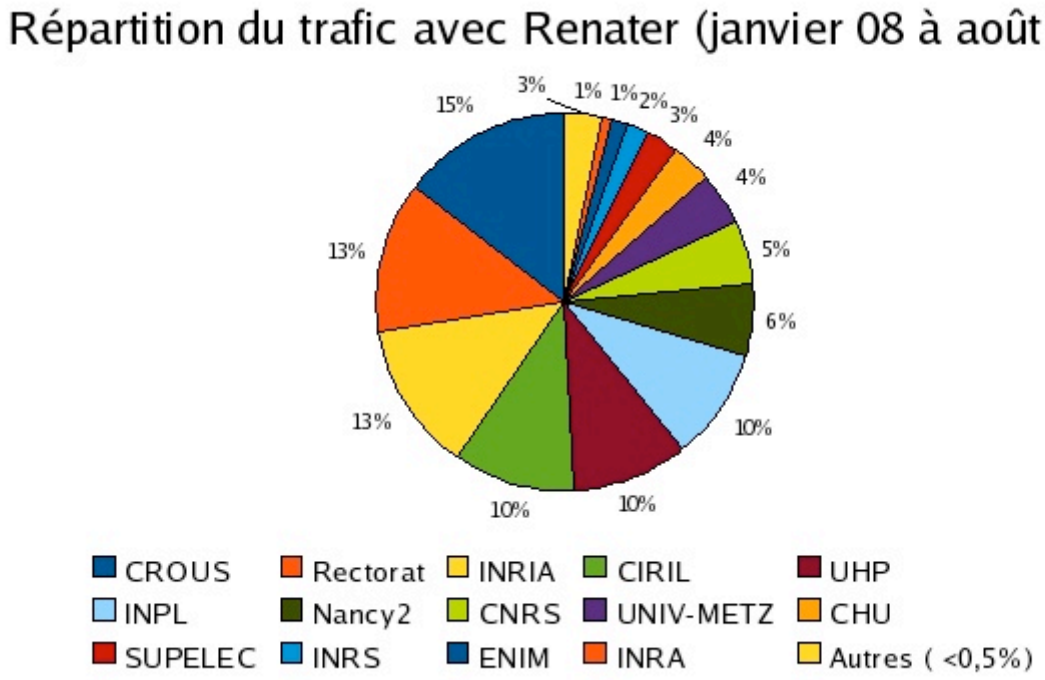
Quelques résultats

- ... soit en terme de débit :



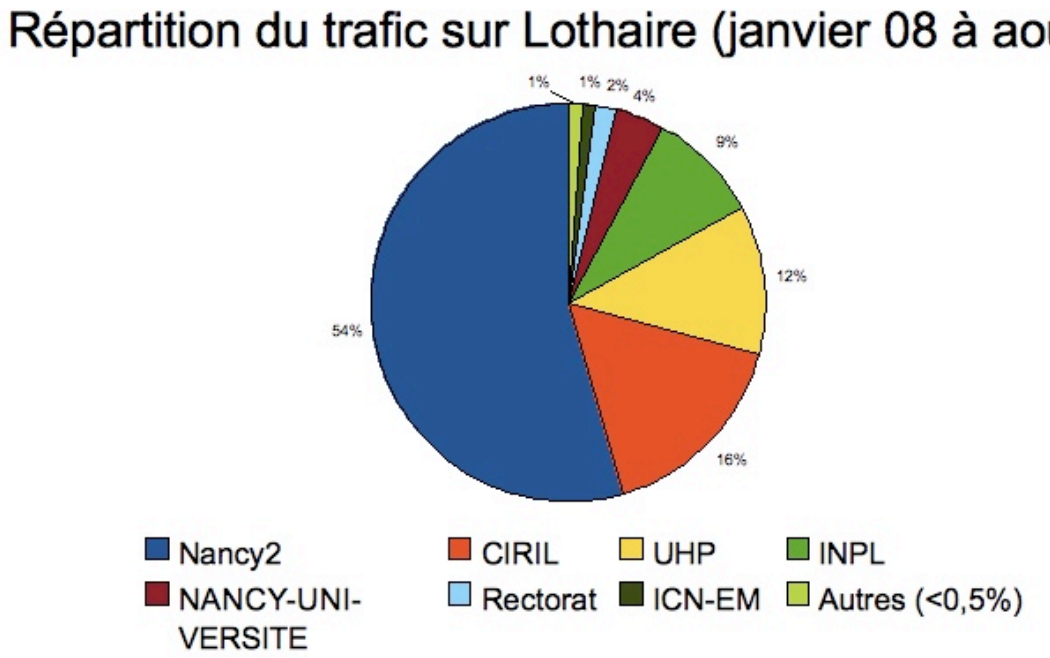
Quelques résultats

- Répartition du trafic avec Renater entre les organismes partenaires
  - CROUS : accès Internet dans les cités U
  - Rectorat : accès Internet dans les lycées



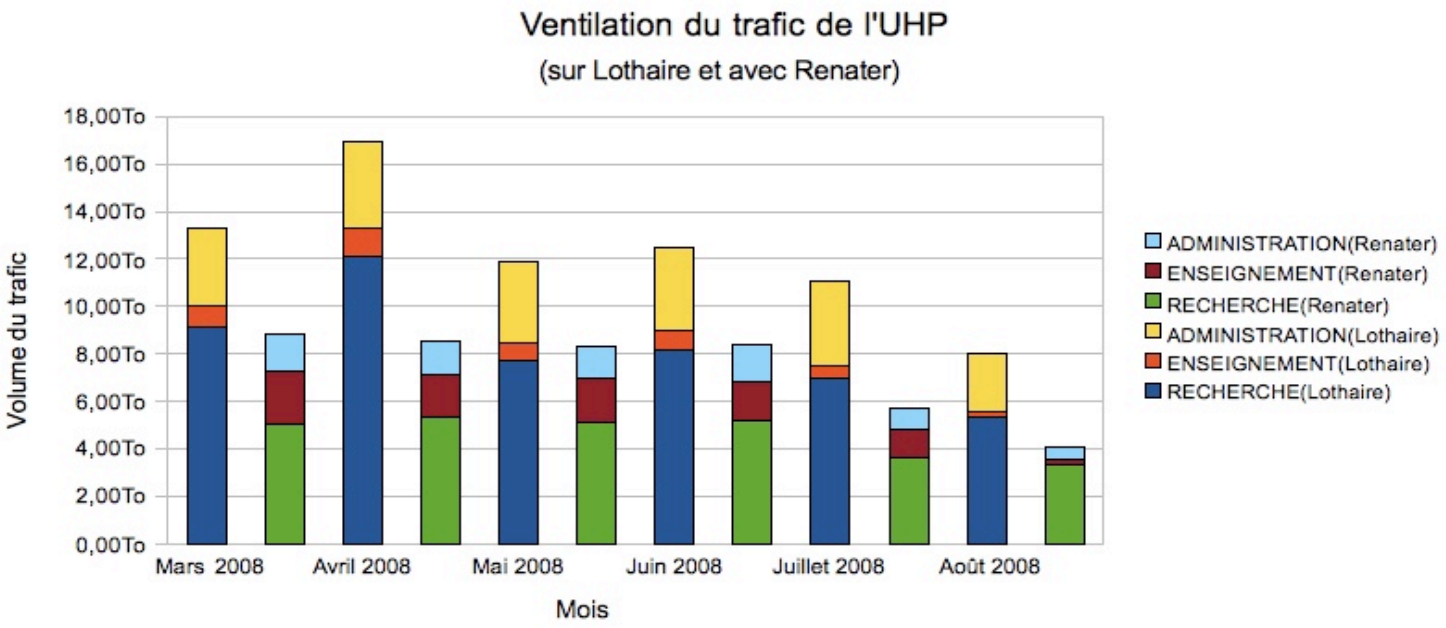
Quelques résultats

- Répartition du trafic interne
  - La part importante de Nancy 2 dans le trafic est due essentiellement (75%) aux sauvegardes (la nuit et le week-end)
  - Idem pour le CIRIL



Quelques résultats

- Évaluation de la part du trafic de l'UHP due à chaque type d'activité (Enseignement, Recherche, Administration)
  - part importante de la recherche ~ 2/3
  - part relativement faible de l'enseignement à comparer avec la part du CROUS dans le trafic Renater



ConfIn

Olivier LACROIX

ConfIn

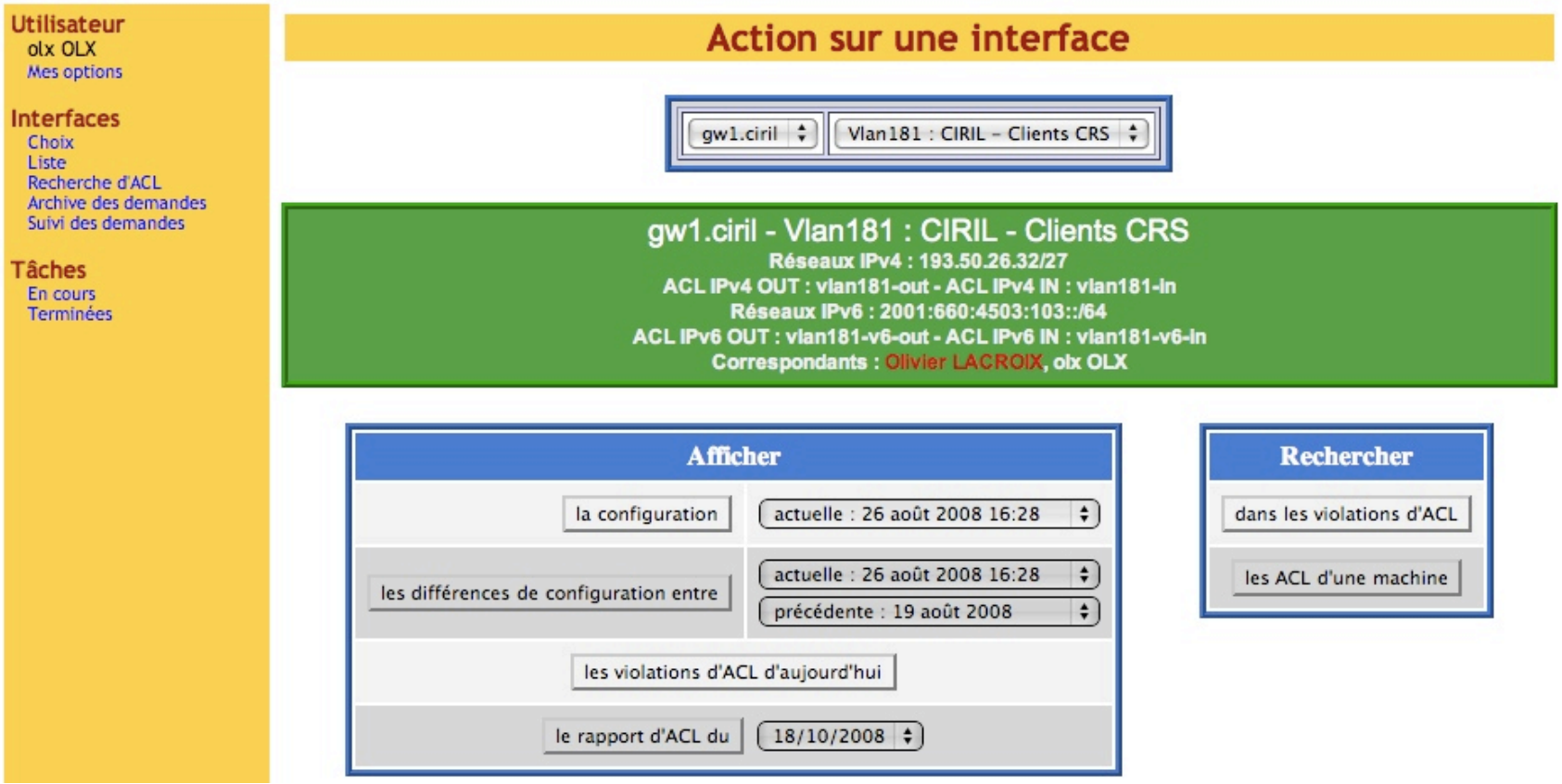
- ConfIn pour CONFigurations des INterfaces

- Permet aux correspondants autorisés de gérer le filtrage de leurs réseaux :
  - Visualisation de toutes les informations concernant un réseau
  - Eventuellement demande de modification du filtrage en place (ces demandes sont soumises à validation de la part de l'équipe réseau pour des réseaux de sécurité)
  - Accès aux violations d'ACL (Access Control List = filtrage de niveau 3) des 60 derniers jours et à leurs synthèses, recherche dans celles-ci
  - Recherche de filtres mis en place sur Lothaire
  - …

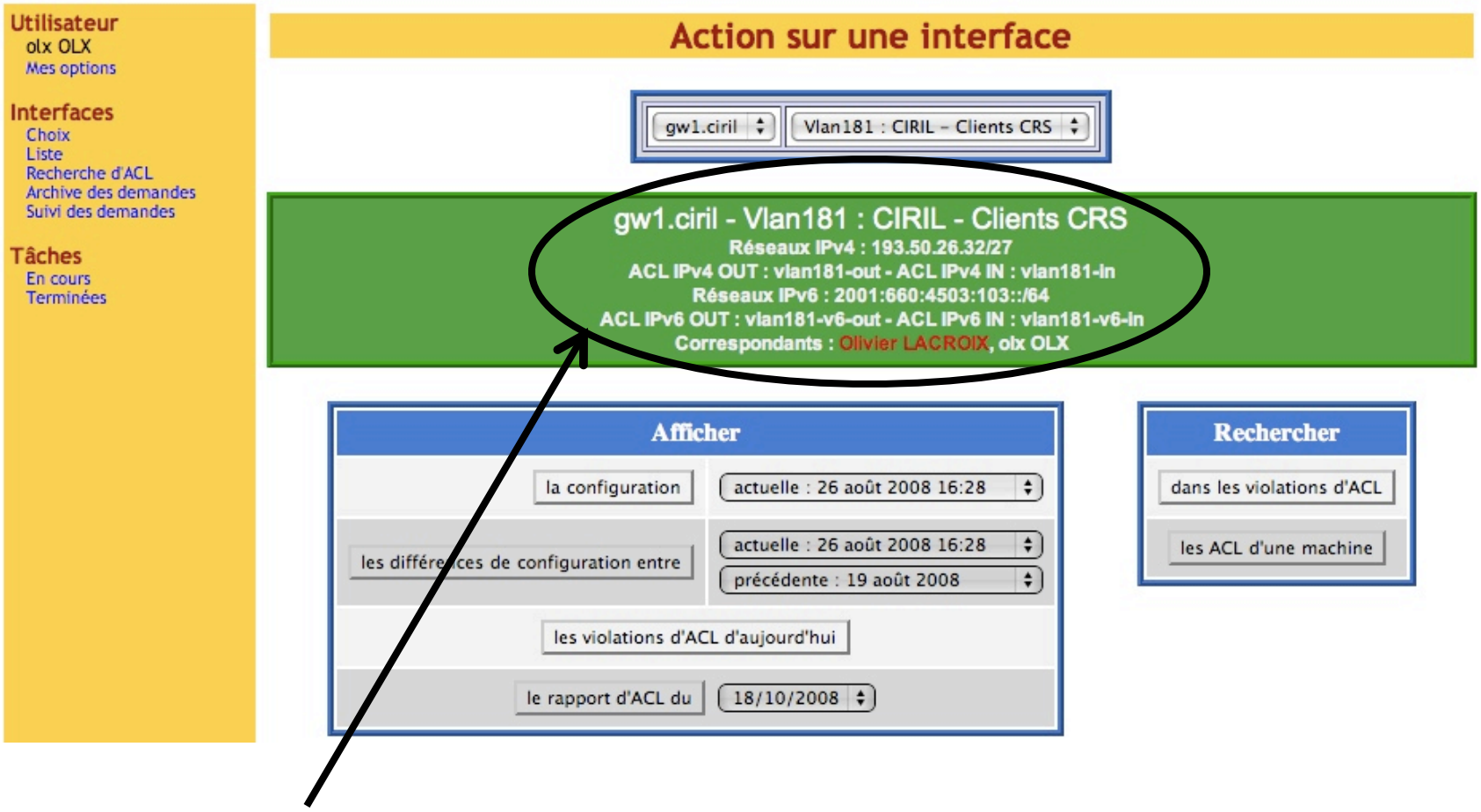
ConfIn : le mécanisme

- ConfIn est un ensemble de modules
  - Une interface Web permettant les interactions avec les utilisateurs
  - Un gestionnaire de tâches traitant les recherches, les mises en place des filtres et les sauvegardes des équipements
  - Un programme de génération des rapports (violations d'ACL, messages aux correspondants) lancé une fois par jour

ConfIn : l'interface



ConfIn : l'interface



Les informations sur l'interface en cours

ConfIn : une interface

ConfIn : une interface

La ou les adresses

IPv4 et les noms d'ACL

ConfIn : une interface

La ou les adresses IPv4 et les noms d'ACL

La ou les adresses IPv6 et les noms d'ACL

ConfIn : une interface

La ou les adresses

IPv4 et les noms d'ACL

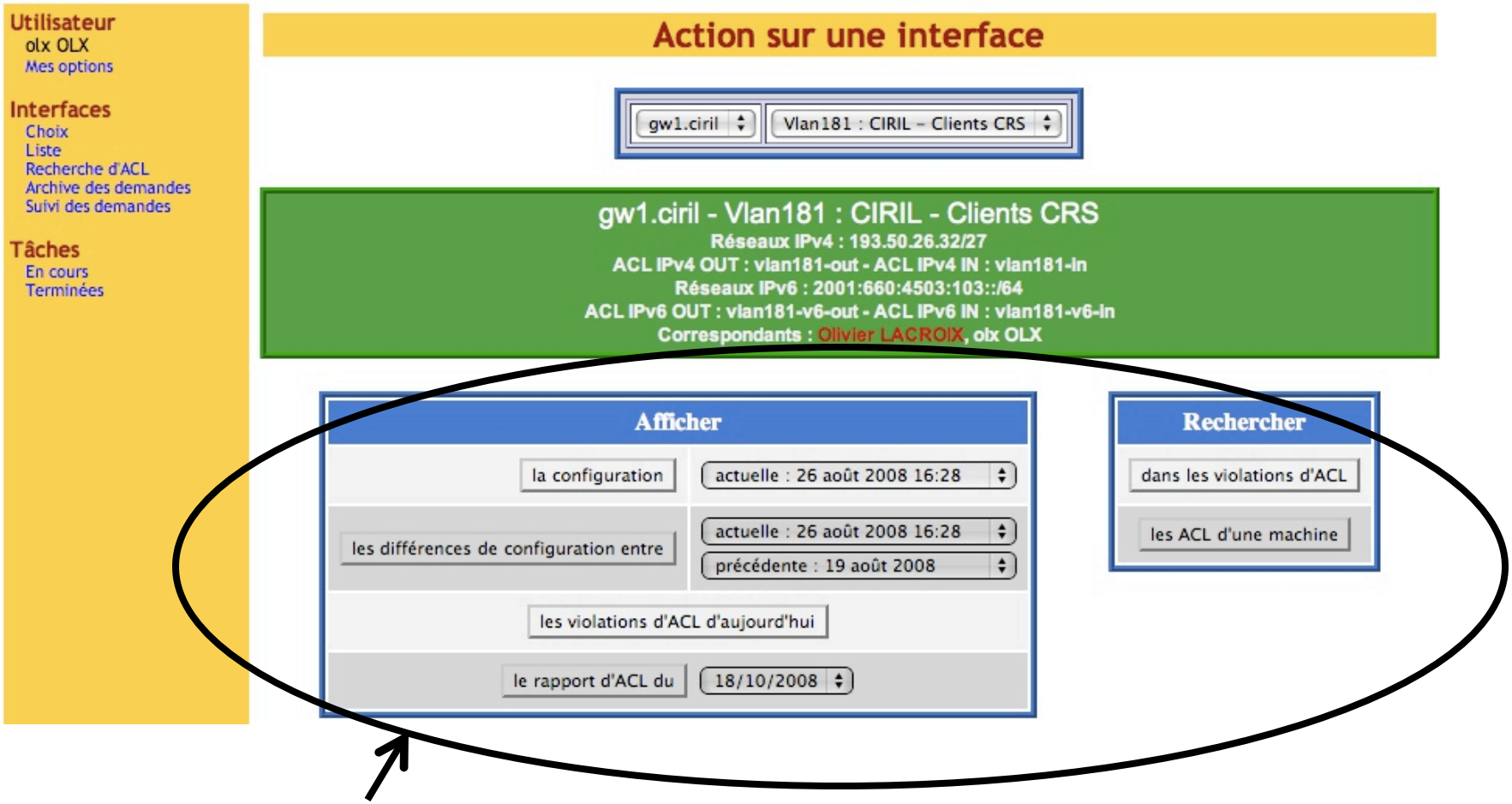
La ou les adresses

IPv6 et les noms d'ACL

Les correspondants de l'interface

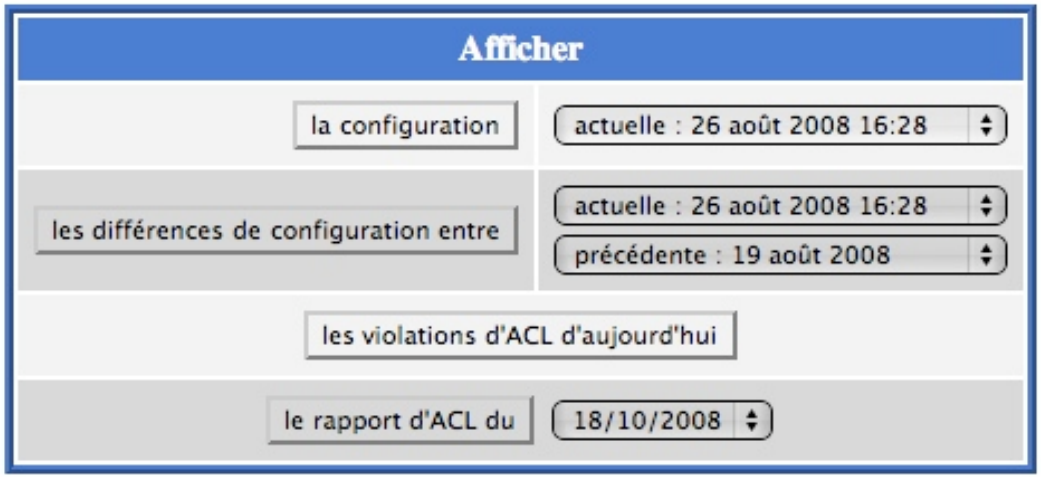
En rouge, ceux qui peuvent faire de modifications

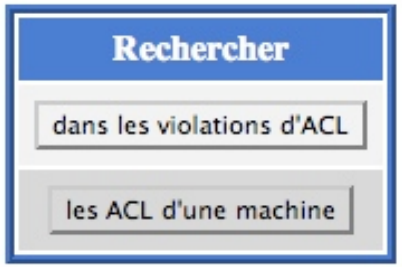
ConfIn : les actions



Les actions réalisables

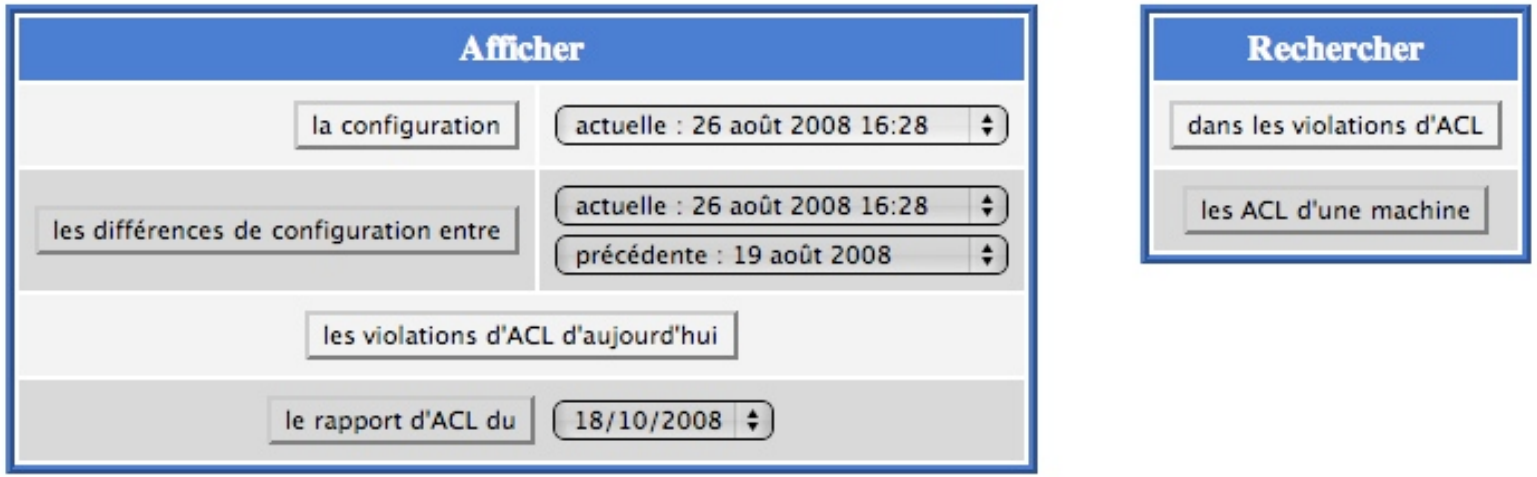
ConfIn : les actions





ConfIn : les actions

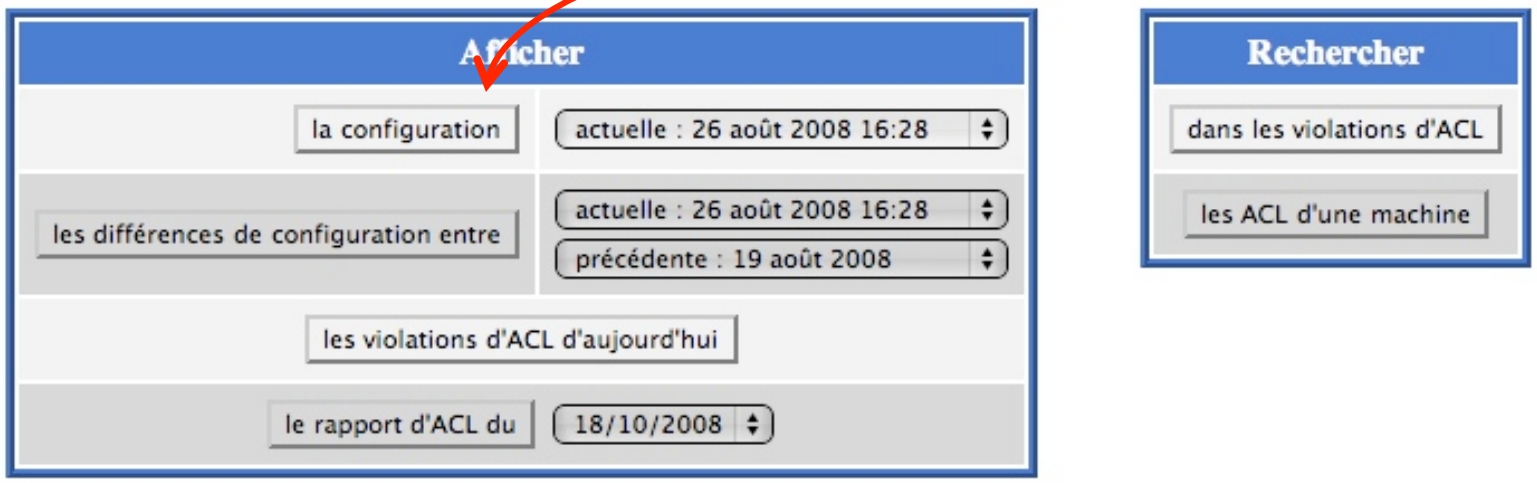
Visualisation



ConfIn : les actions

Visualisation

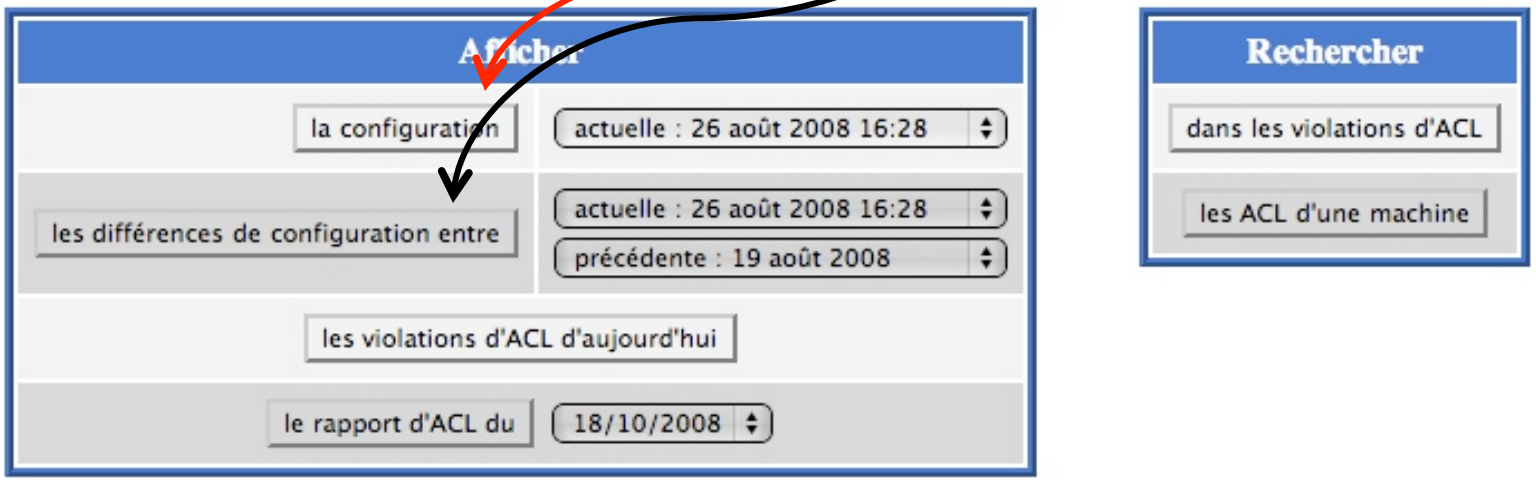
Des configuration actuelles et passées



ConfIn : les actions

Visualisation

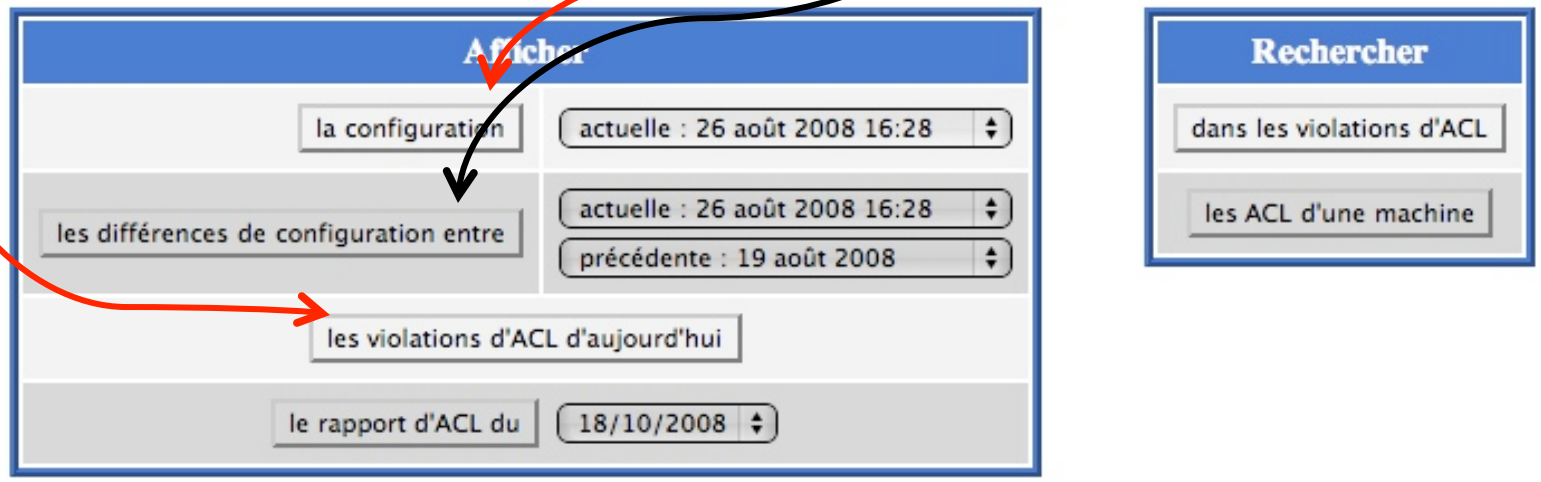
Des configuration actuelles et passées
Des différences entre 2 configurations



ConfIn : les actions

Visualisation

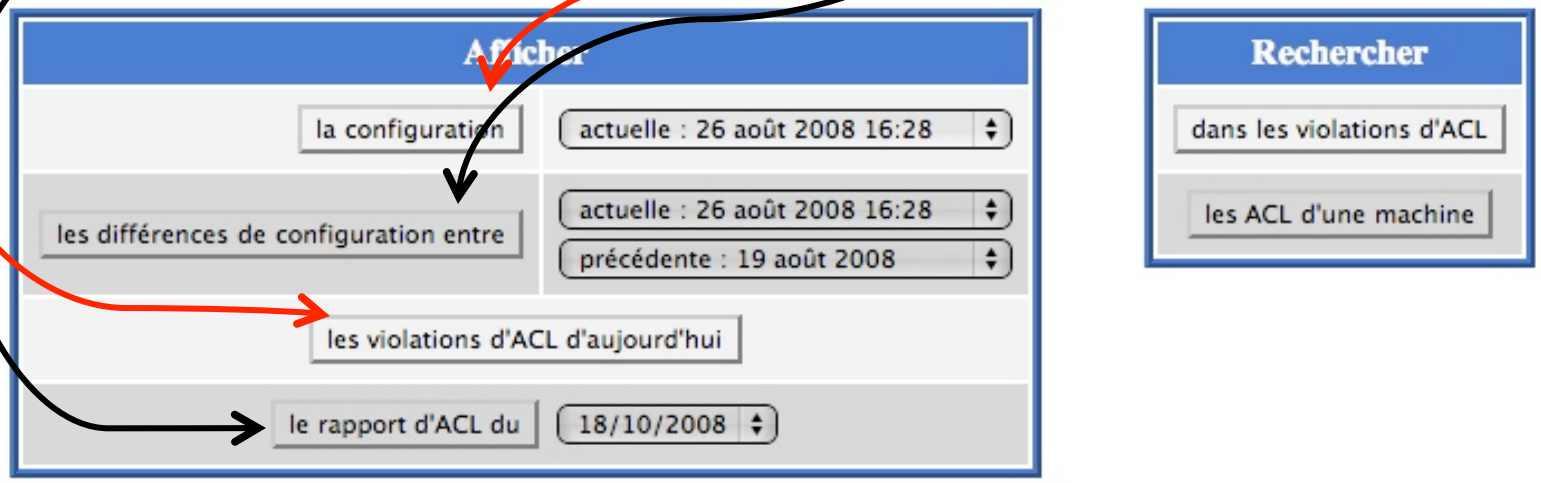
Des configuration actuelles et passées
Des différences entre 2 configurations
Des violations d'ACL en direct



ConfIn : les actions

Visualisation

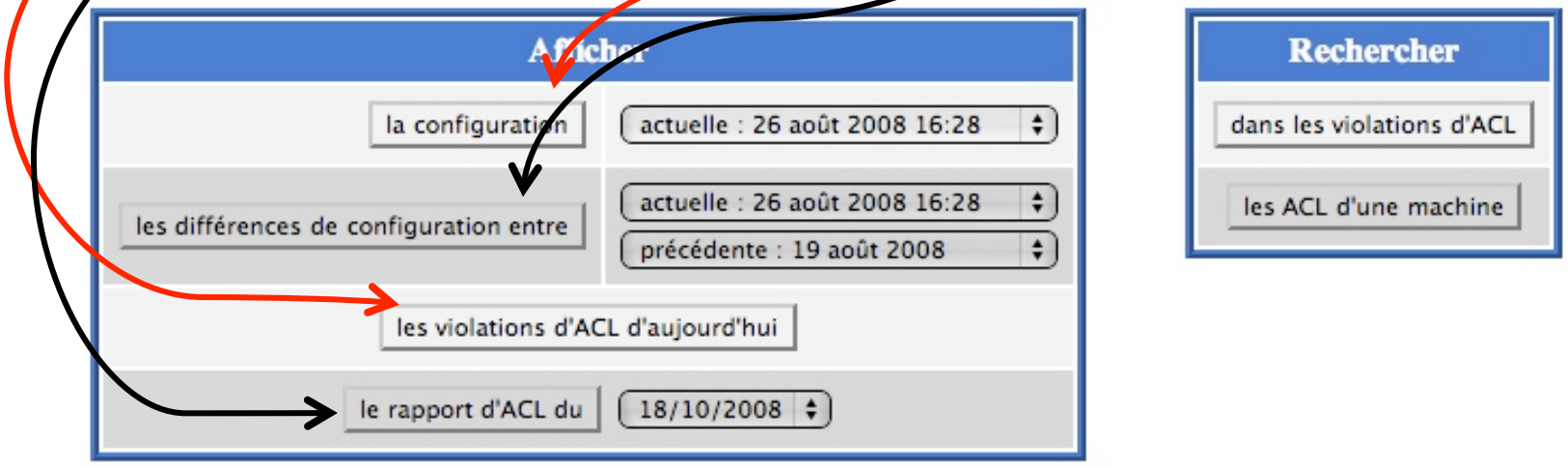
Des configuration actuelles et passées
Des différences entre 2 configurations
Des violations d'ACL en direct
Des rapports journaliers de violations d'ACL



ConfIn : les actions

Visualisation

Des configuration actuelles et passées
Des différences entre 2 configurations
Des violations d'ACL en direct
Des rapports journaliers de violations d'ACL

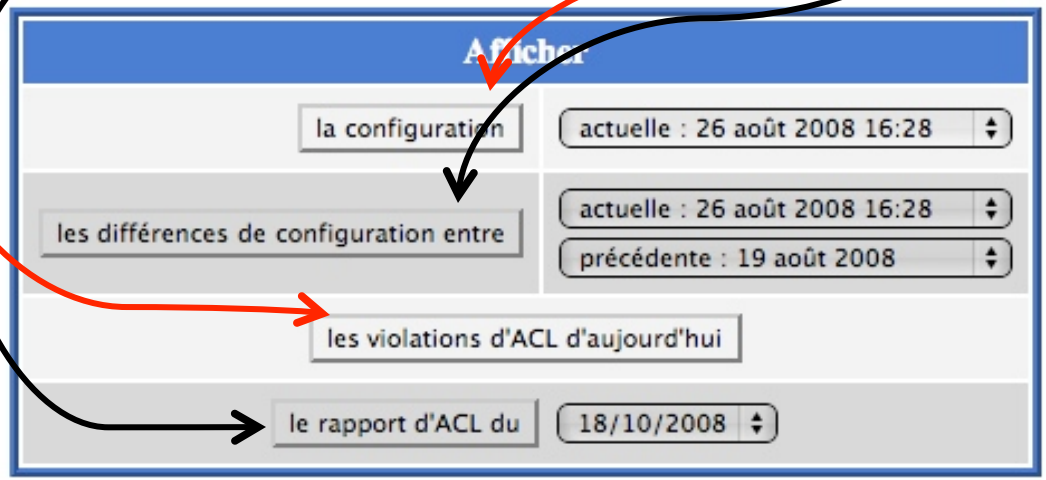


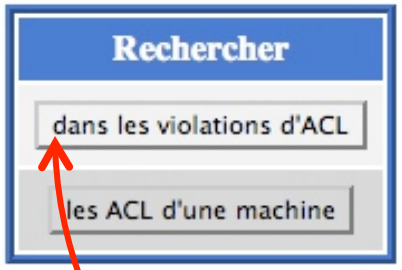
Recherche en différé

ConfIn : les actions

Visualisation

Des configuration actuelles et passées
Des différences entre 2 configurations
Des violations d'ACL en direct
Des rapports journaliers de violations d'ACL





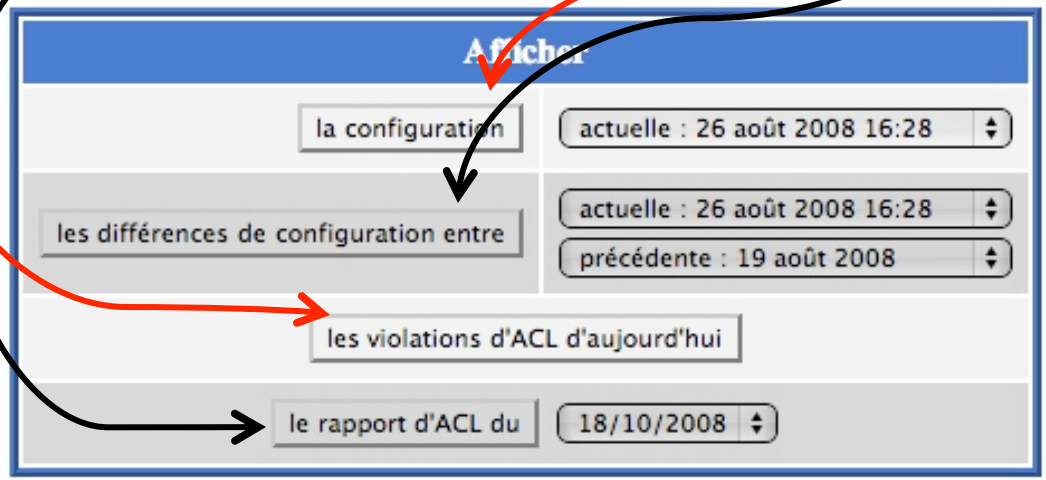
Recherche en différé

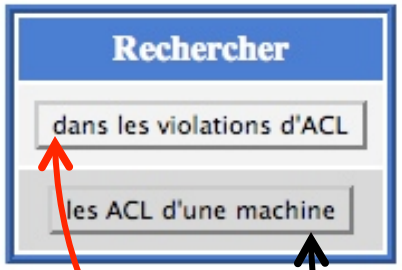
Par critère dans les violations d'un 60 derniers jours

ConfIn : les actions

Visualisation

Des configuration actuelles et passées
Des différences entre 2 configurations
Des violations d'ACL en direct
Des rapports journaliers de violations d'ACL



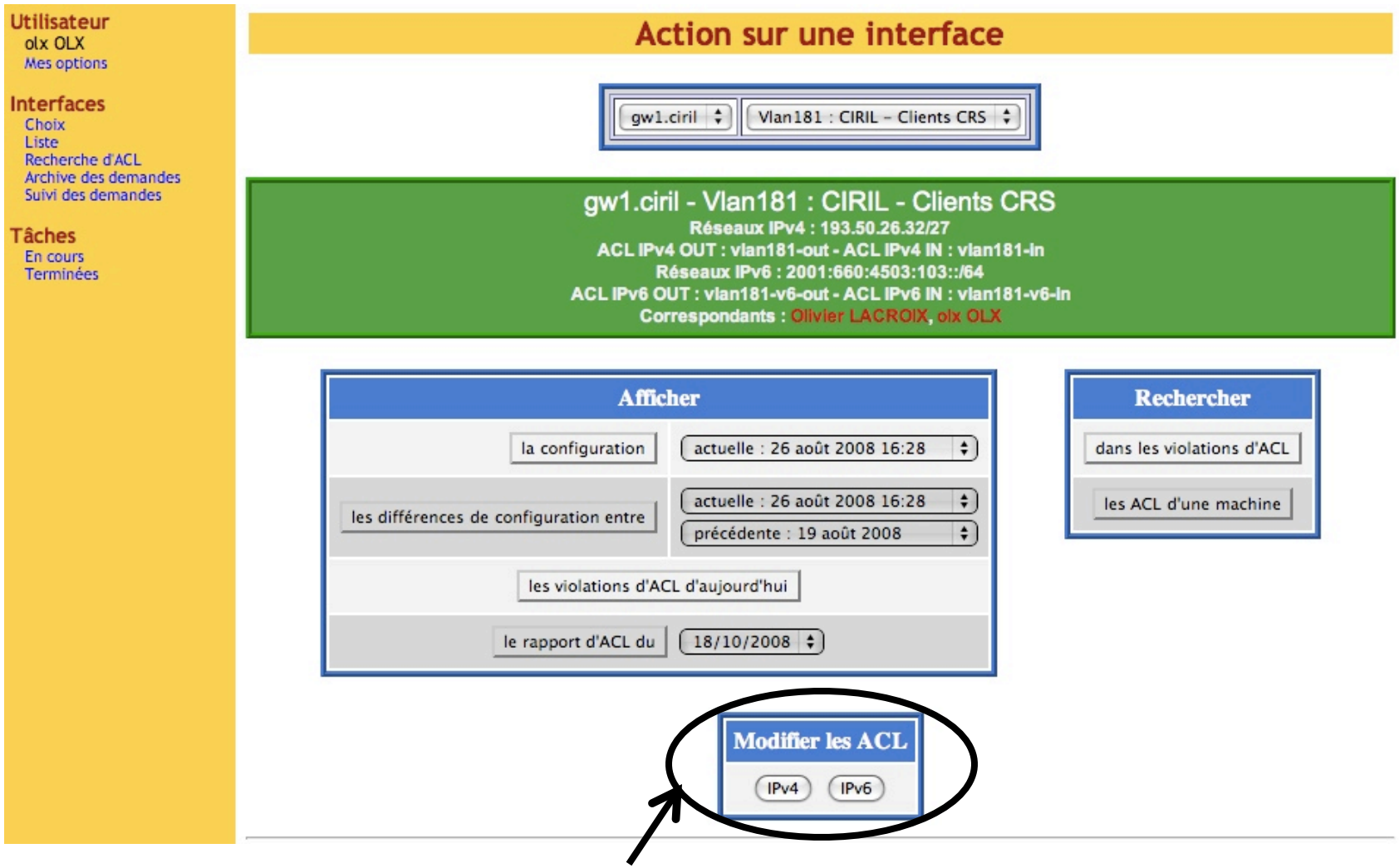


Recherche en différé

Par critère dans les violations d'un 60 derniers jours

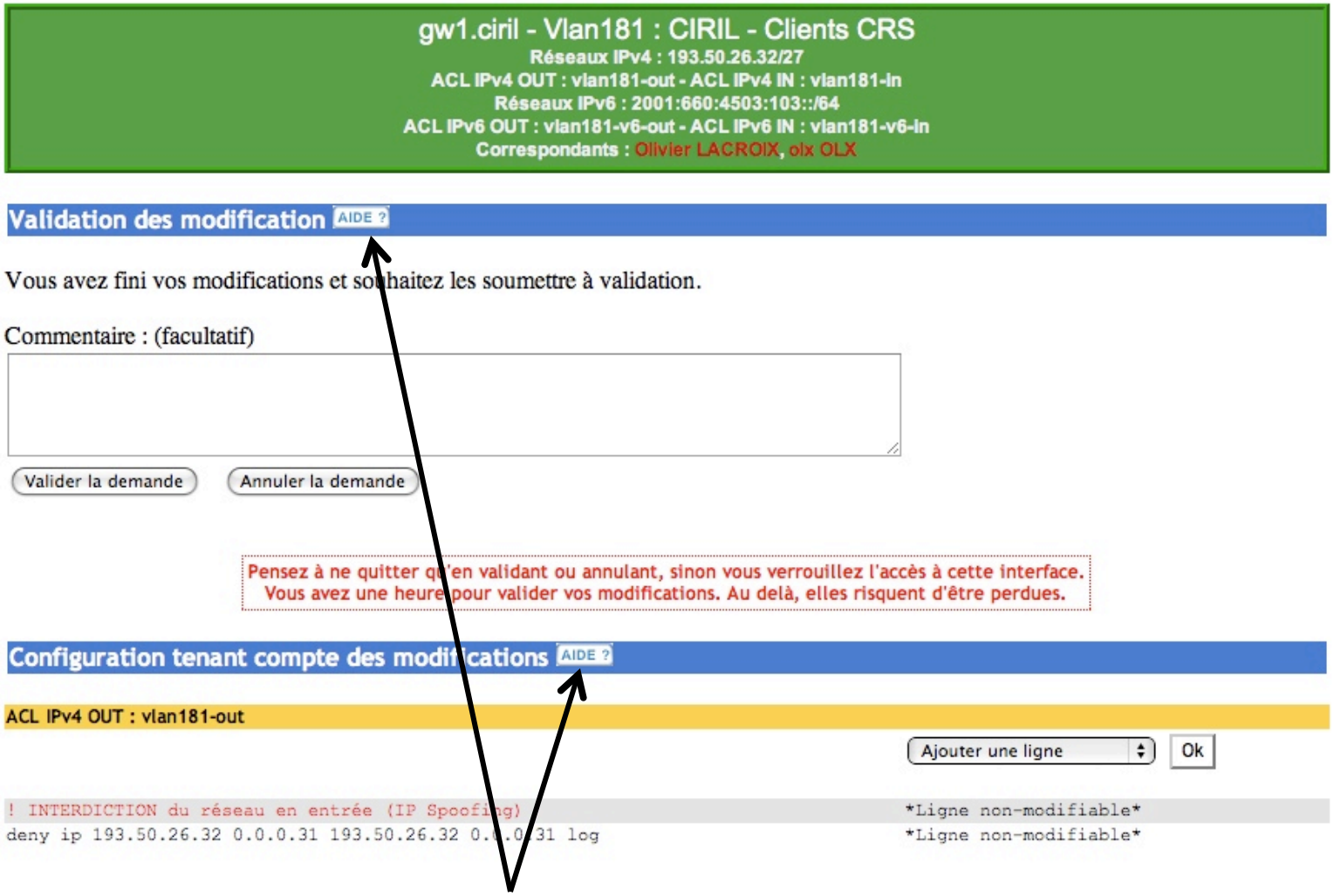
Du filtrage existant pour une machine ou un réseau dans tous les filtres sur Lothaire

ConfIn : modifications d'ACL



Si l'utilisateur est autorisé, possibilité de modifier les filtres

ConfIn : modification d'ACL

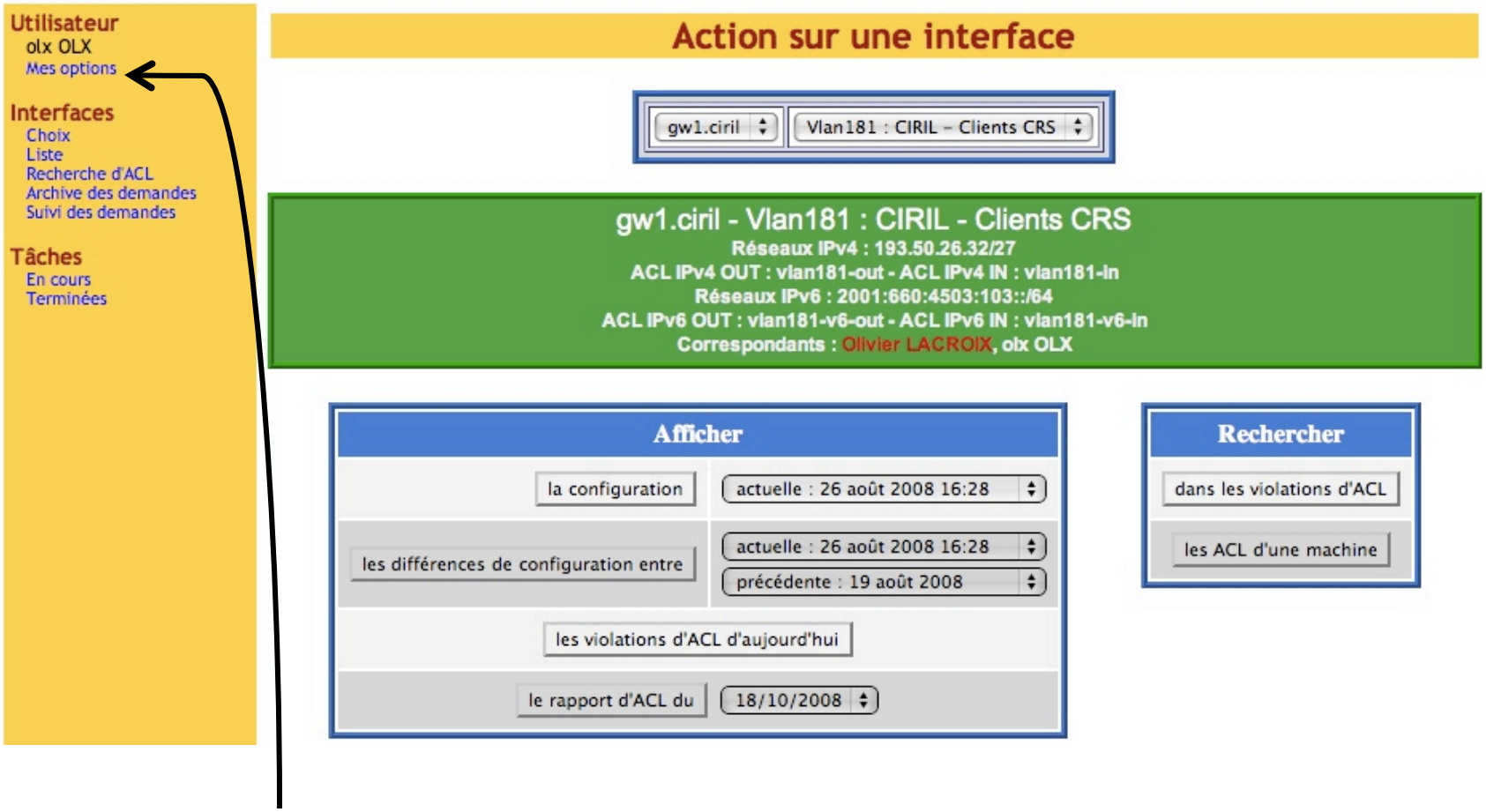


Modification des ACL : il existe une aide en ligne

ConfIn : les ACL

- Les modifications peuvent utiliser des modèles
- Il est possible de définir des ACL temporaires activables à la demande par les correspondants (bouton visible sur l'interface). Celles-ci sont automatiquement retirées tous les jours à minuit
- Les 2 options ci-dessus sont définies par l'équipe réseau (nous écrire pour les obtenir)

ConfIn : les options



Pensez aussi à vos options

ConfIn : les options

Mes options

Vos renseignements	olx OLX <lacroix@ciril.fr>
Notification des changements	par jour
Envoi des changements par Email	configuration
Envoi des violations d'ACL	oui
Valider les changements	

Choix des interfaces et des types de notification

Interface	Notifie modif	Notifie ACL
gw1.ciril - Vlan181 (CIRIL - Clients CRS)	☑	☑
gw1.ciril - Vlan199 (CIRIL - Serveurs PUBLICS)	☑	☑
	Coche / Décoche	Coche / Décoche
Valider les notifications		

ConfIn : quelques chiffres

- ConfIn, c'est aujourd'hui :
  - Un service inauguré en août 2000
  - 10794 demandes traitées au 22 octobre 2008 depuis la mise en place de la possibilité de modification le 22 août 2006 (43417 lignes de configurations modifiées)
  - 575 interfaces réseaux gérées sur 33 routeurs par 151 correspondants différents (certains gèrent plusieurs interfaces)
  - 57 000 ACLs réparties sur les routeurs de Lothaire

Serveur FTP

Olivier LACROIX

Serveur FTP

L'origine

- Ce service a été créé il y a plus de 10 ans lorsque la bande passante était faible
- Son but était de fournir rapidement des logiciels utilisés par notre communauté
- Le choix des logiciels était fait en fonction des besoins ressentis et des demandes

Aujourd'hui

- La bande passante est suffisante, mais le besoin de proximité existe toujours
  - Les logiciels très demandés ont besoin de miroir
  - Plus de bande passante, mais des logiciels plus « gros »
  - Pour pouvoir facilement fournir leurs logiciels, les concepteurs de « freeware » ont besoin d'aide

Serveur FTP

Physiquement

- Biprocesseur Pentium 4 2,8 GHz
- 1 Go RAM
- 2,6 To d'espace disque en RAID 5
- Connexion en gigabit ethernet
- Adresses IPv4 et IPv6

Que stocke-t-il ?

- Il y a 2 fonctions
  - Miroir de sites mettant à disposition des logiciels libres : Fedora, Ubuntu, Mozilla, Xemacs, Postfix, Sendmail, GNU, cygwin, openldap, mysql, bind, signatures antivirus, etc. (liste complète sur le site web du serveur)
  - Miroir des logiciels antivirus du ministère

Serveur FTP

Comment y accéder ?

- Pour la partie publique (ftp anonyme), 3 méthodes :
  - ftp « classique » : ftp://ftp.ciril.fr/
  - Web : http://wwwftp.ciril.fr/
  - Rsync : rsync://ftp.ciril.fr/
- Pour la partie logiciel antivirus :
  - Contactez le correspondant logiciel de votre établissement qui vous indiquera les modalités d'accès si vous êtes autorisés

Comment évolue-t-il ?

- Son contenu change de temps à autre en fonction de la place disponible :
  - Suppression de miroirs devenu obsolète ou plus utilisé
  - Ajout de nouveaux miroirs
    - Choisis par l'équipe réseau en fonction des besoins ressentis
    - Demandés par les utilisateurs (écrire à ftpmaster@ciril.fr)
      => n'hésitez pas à nous contacter

Service VPN

Olivier LACROIX

Service VPN

Qu'est que le VPN ?

- VPN = Virtual Private Network
- Permet d'établir un tunnel crypté entre votre ordinateur et un concentrateur VPN
- Dans le cadre de l'accès depuis son fournisseur ADSL vers un serveur sur Lothaire, si le concentrateur VPN est sur Lothaire, il permet un dialogue crypté entre chez soi et le concentrateur

Service VPN

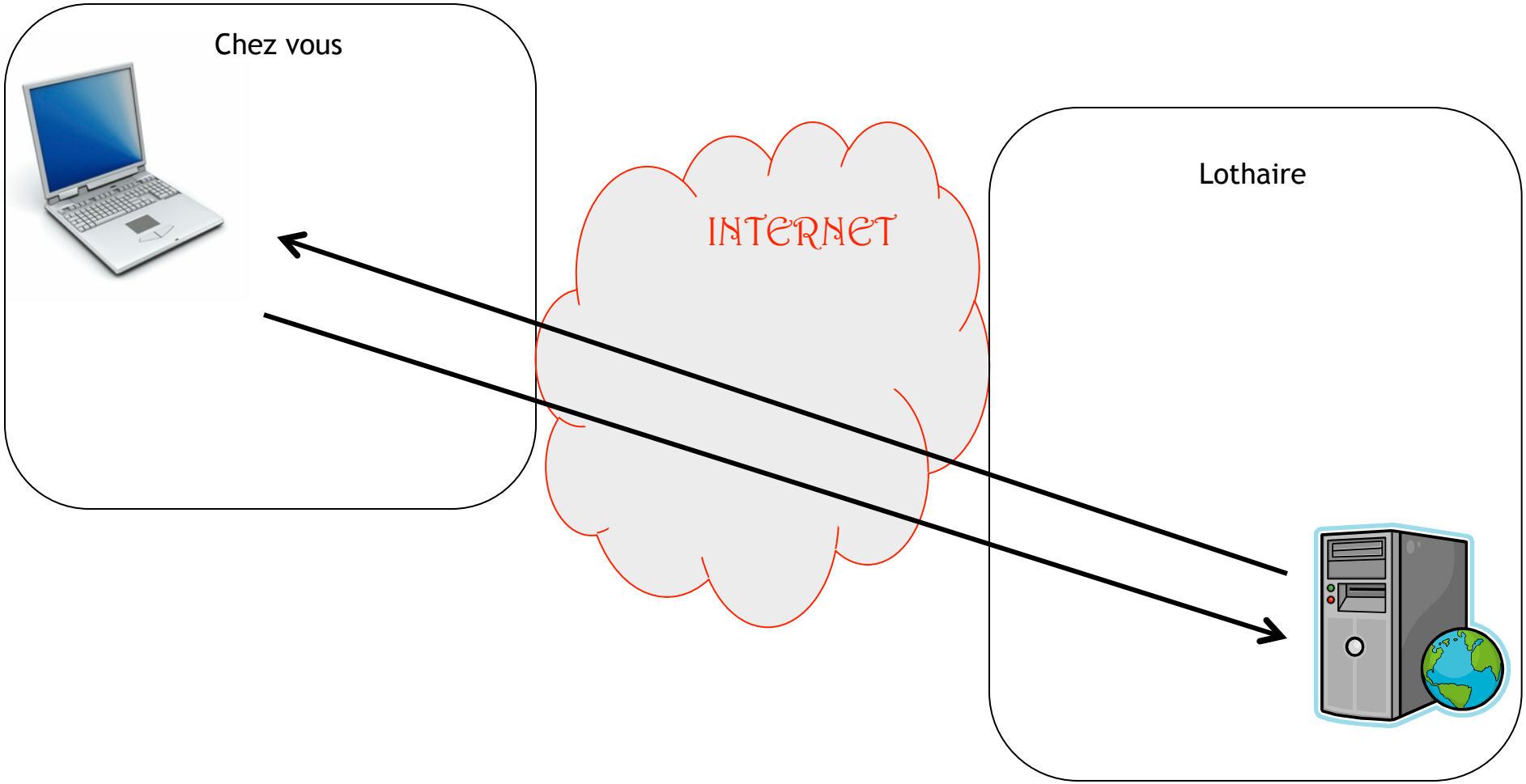
- A notre connaissance, il existe 4 concentrateurs VPN Cisco sur le réseau StanNet :
  - UHP
  - Nancy 2
  - INPL
  - CIRIL
- Le CIRIL héberge les concentrateurs de l'UHP, de l'INPL et du CIRIL

Service VPN : qui pour qui ?

- Chaque établissement universitaire propose un service VPN à ses personnels
- Le CIRIL propose un service VPN pour les établissements/EPST ne disposant pas d'un tel service

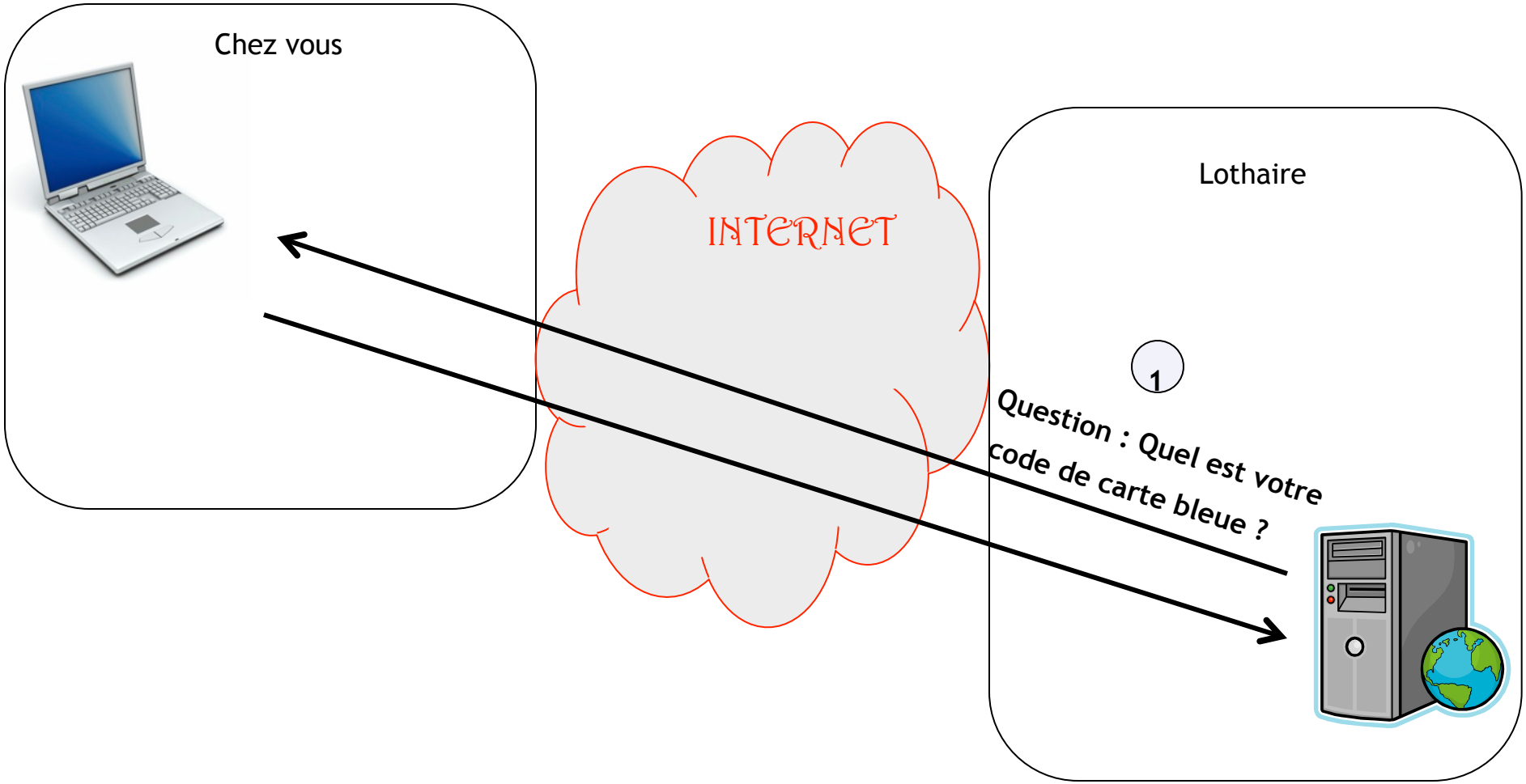
Service VPN : explication

Sans VPN



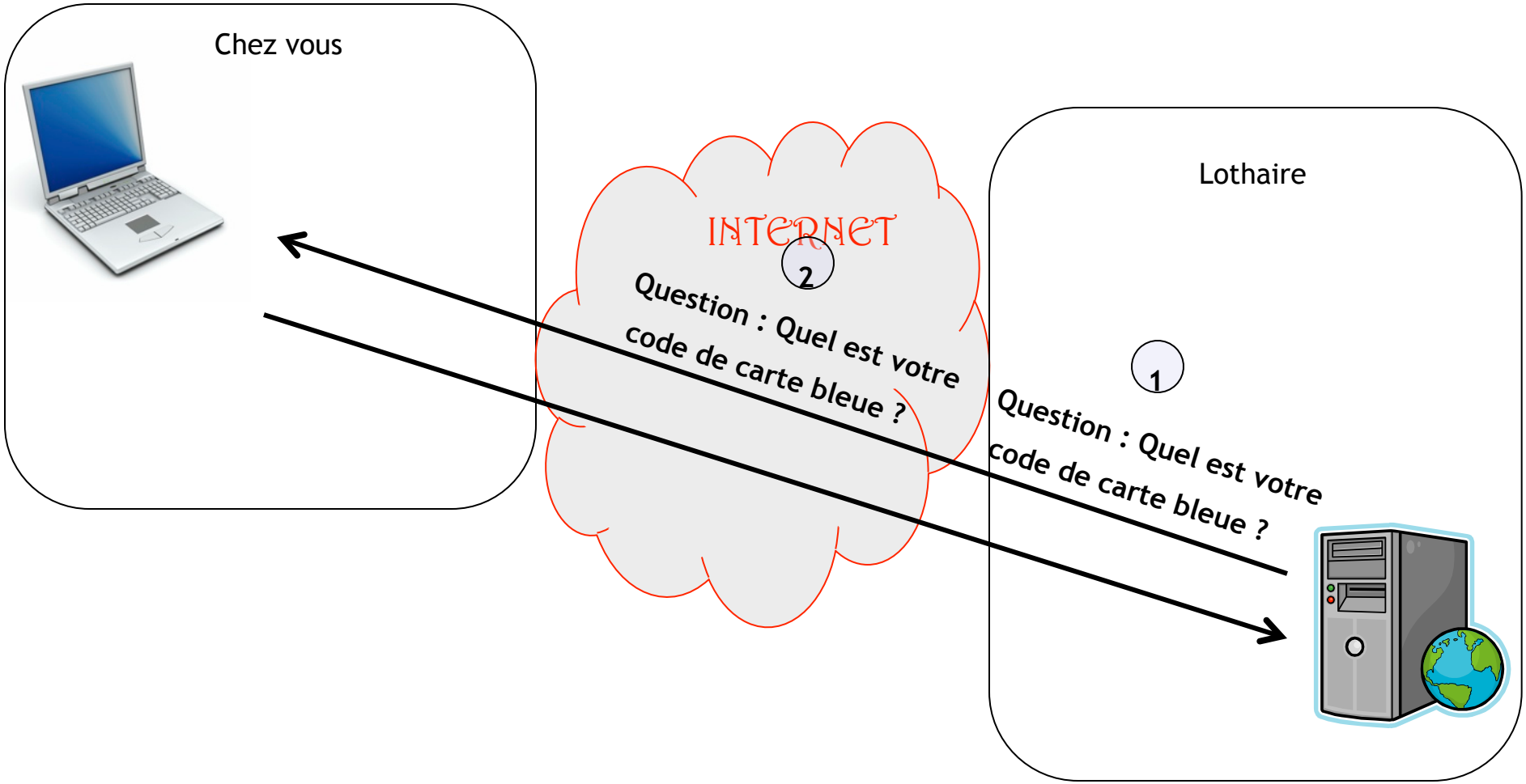
Service VPN : explication

Sans VPN



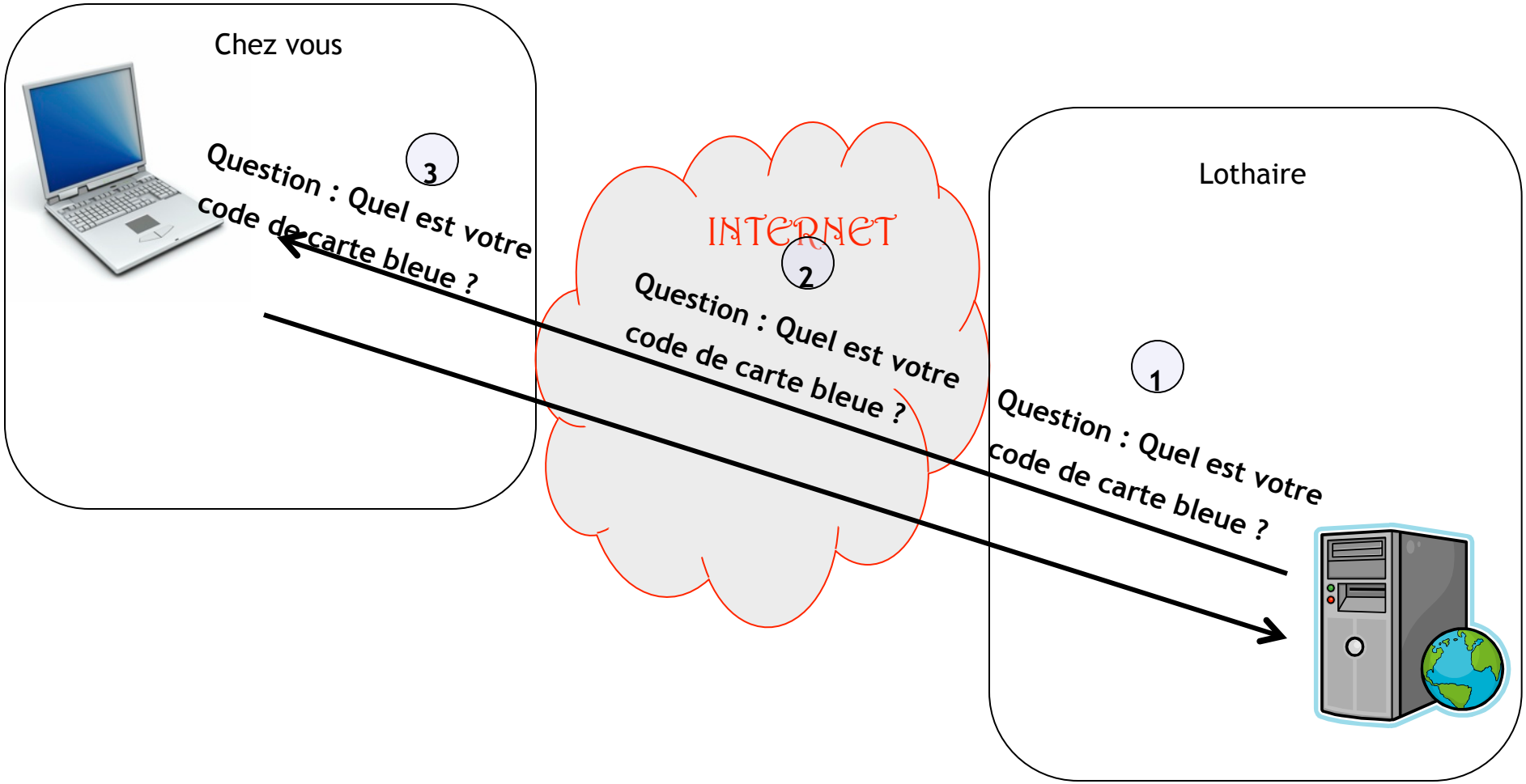
Service VPN : explication

Sans VPN



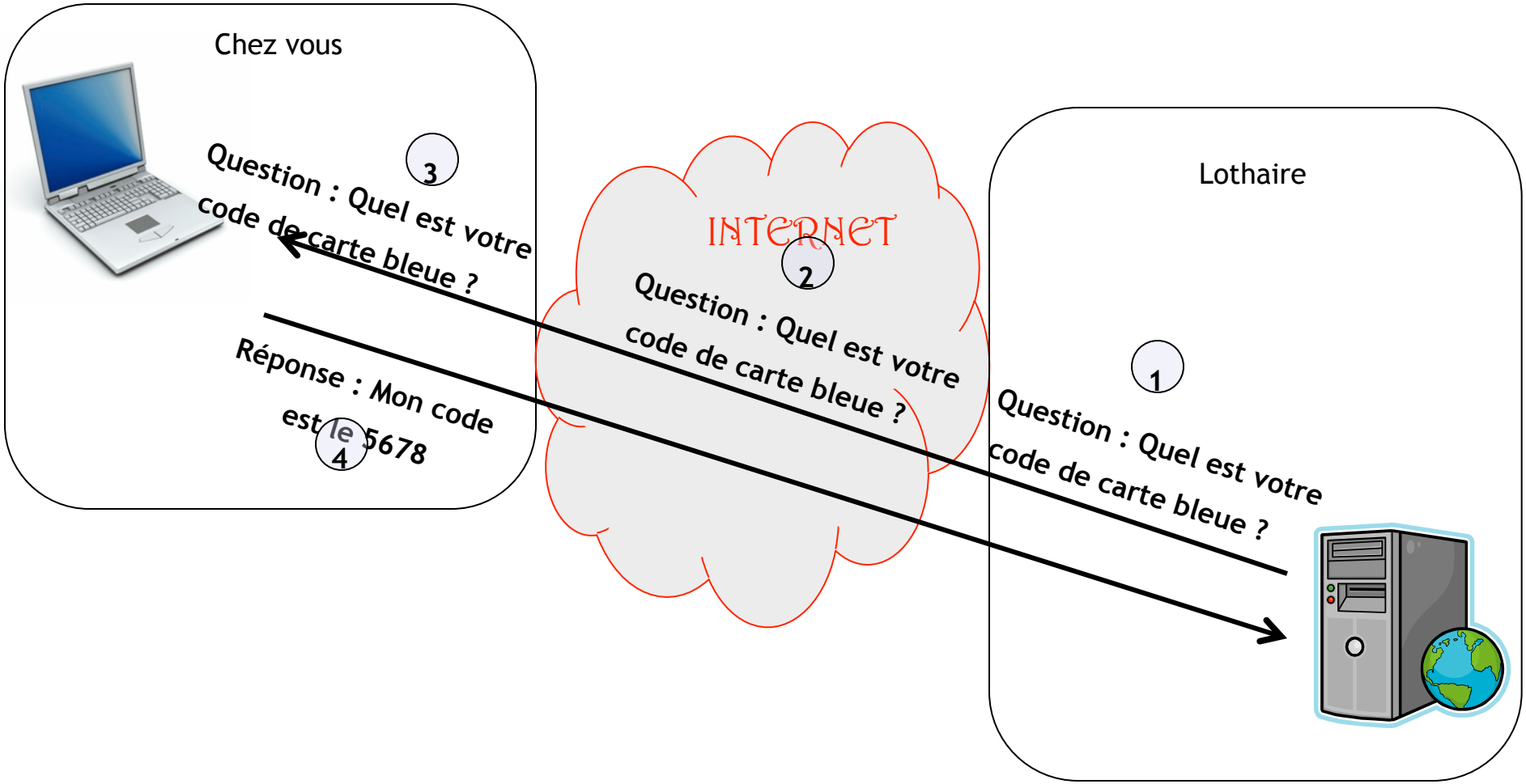
Service VPN : explication

Sans VPN



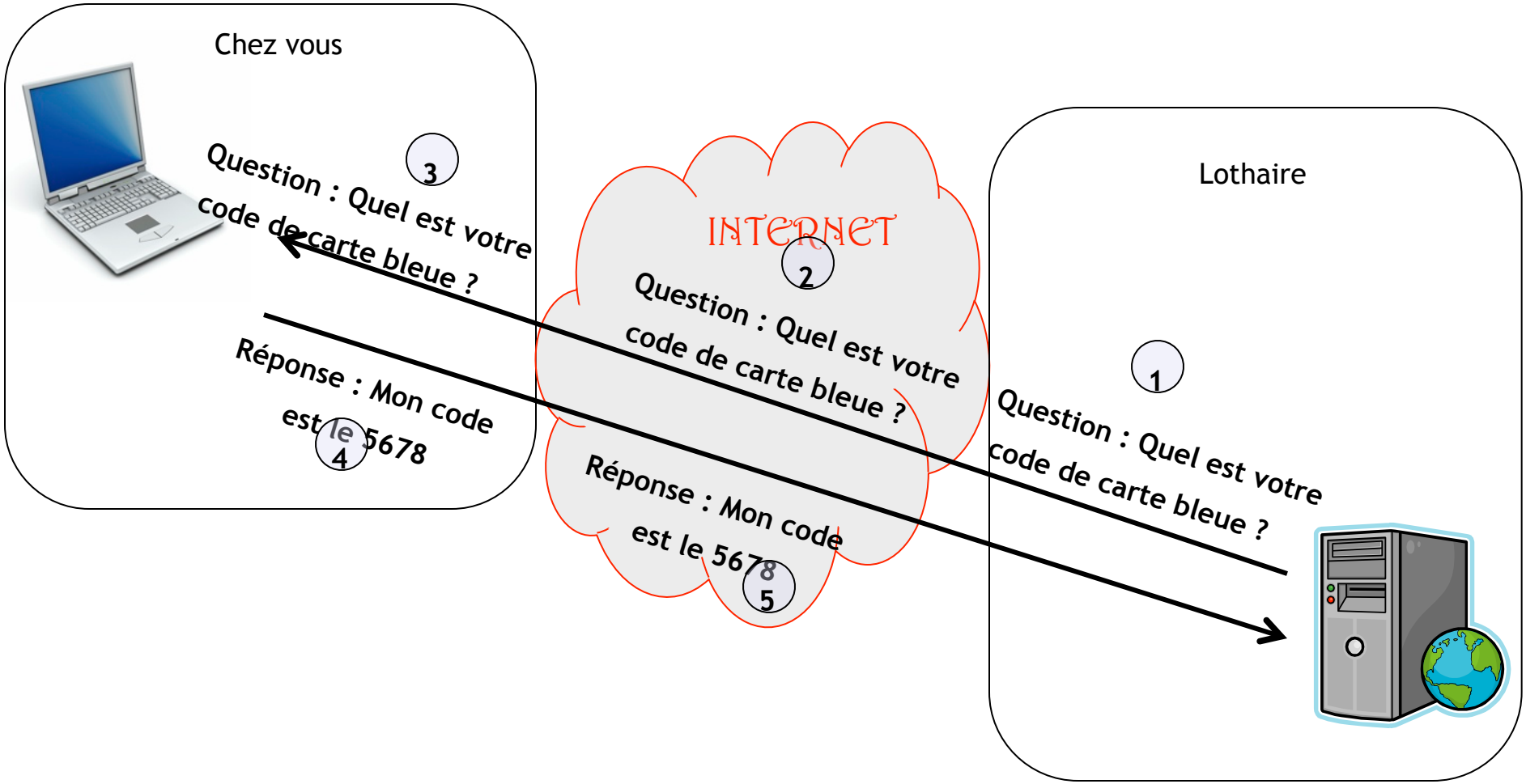
Service VPN : explication

Sans VPN



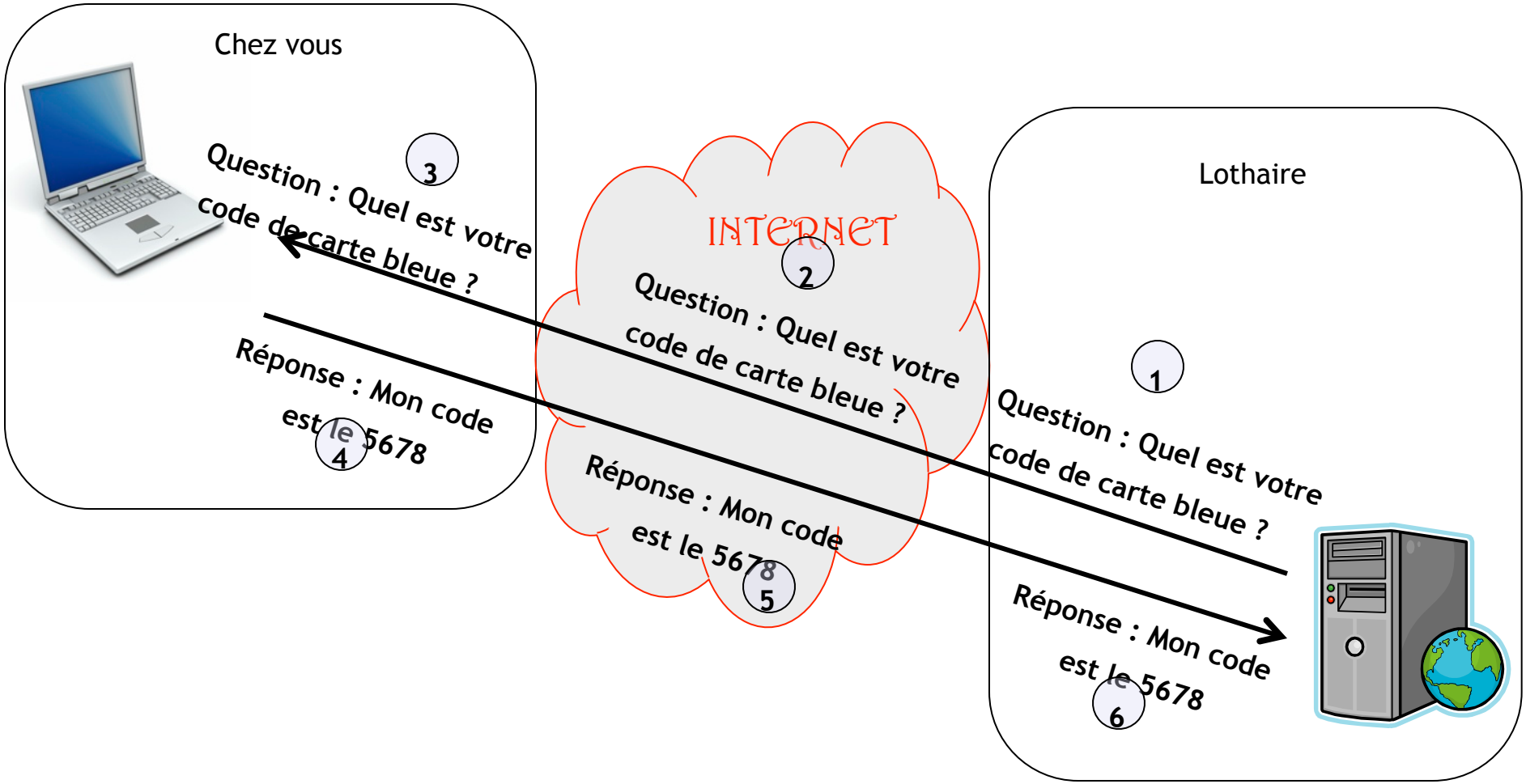
Service VPN : explication

Sans VPN

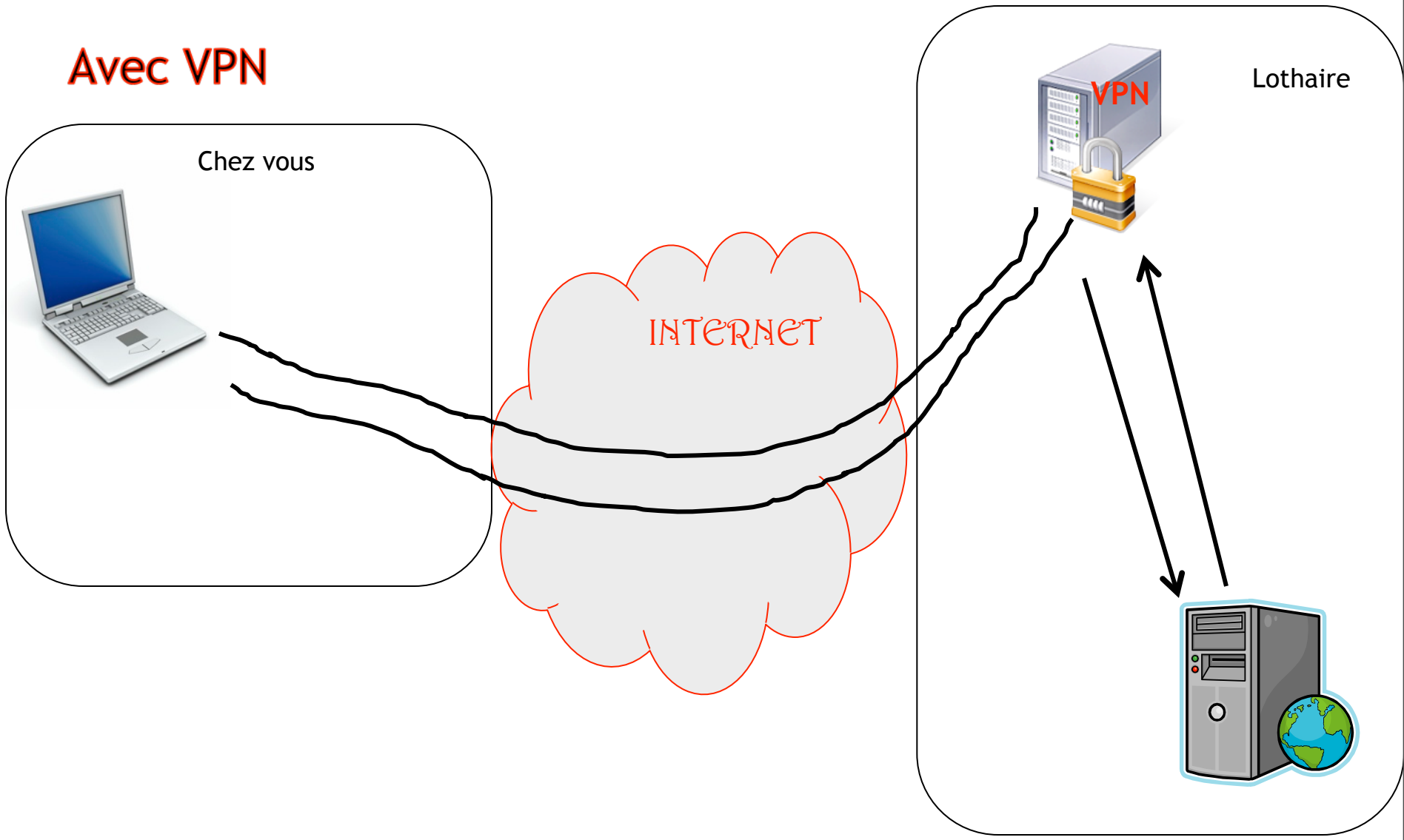


Service VPN : explication

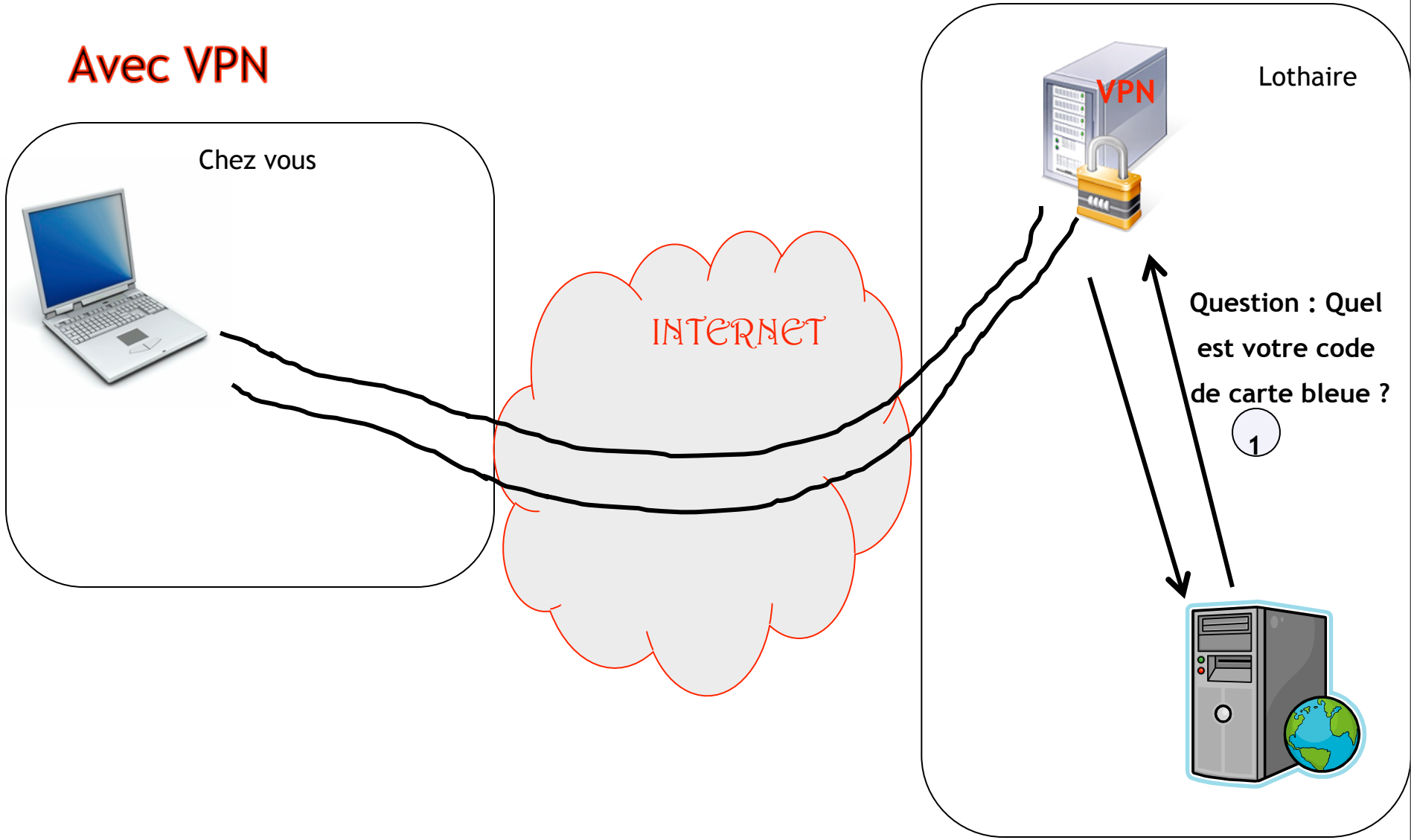
Sans VPN



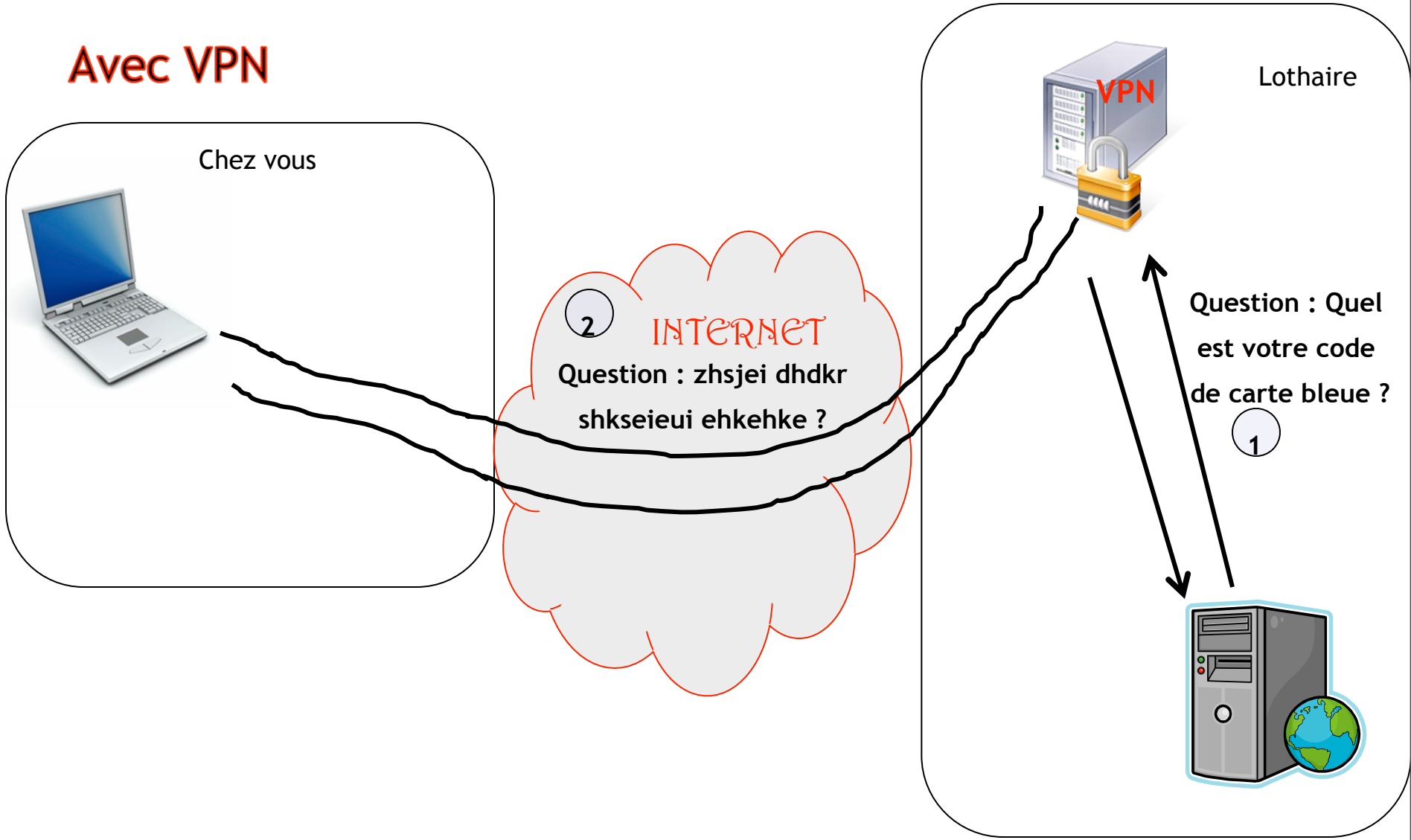
Service VPN : explication



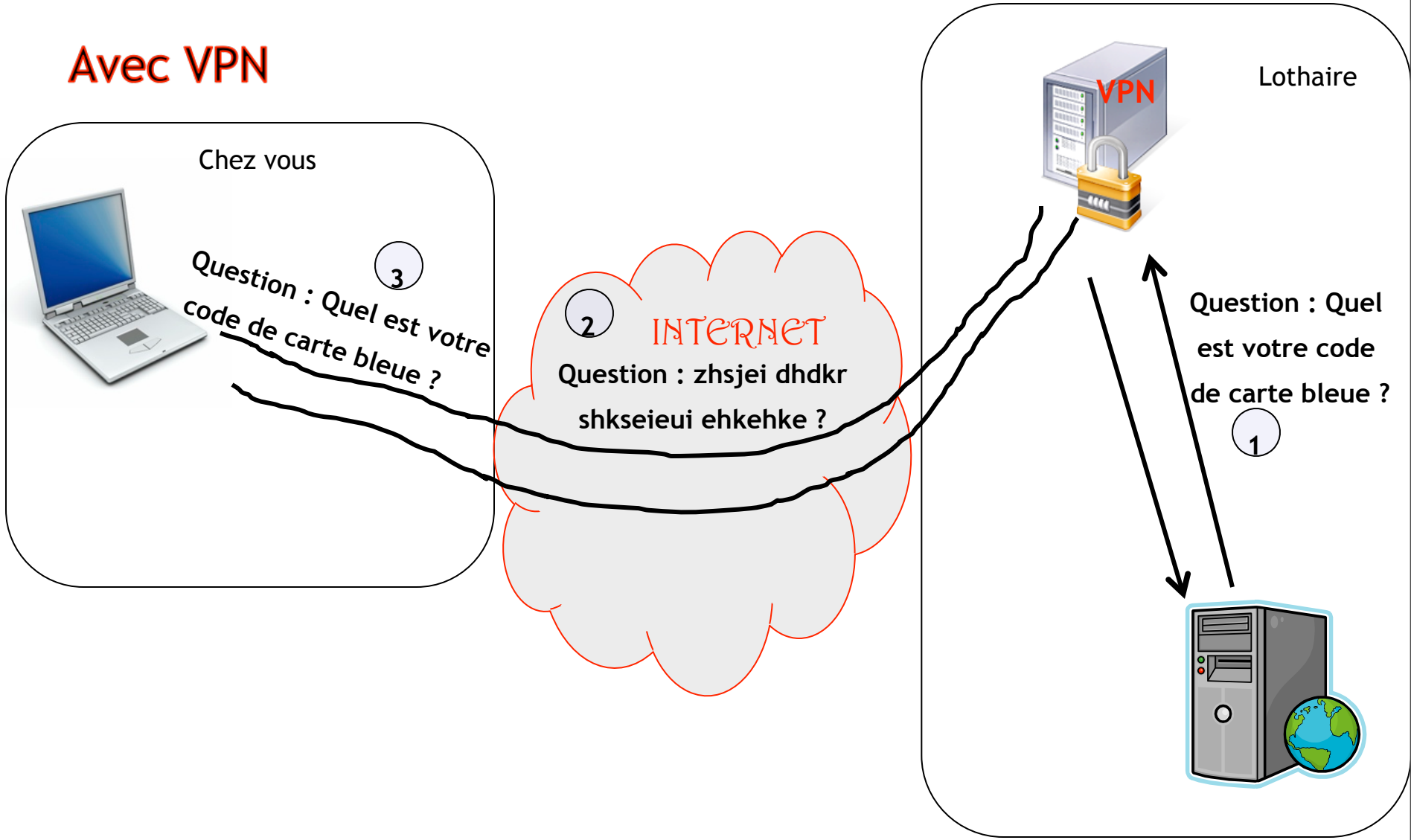
Service VPN : explication



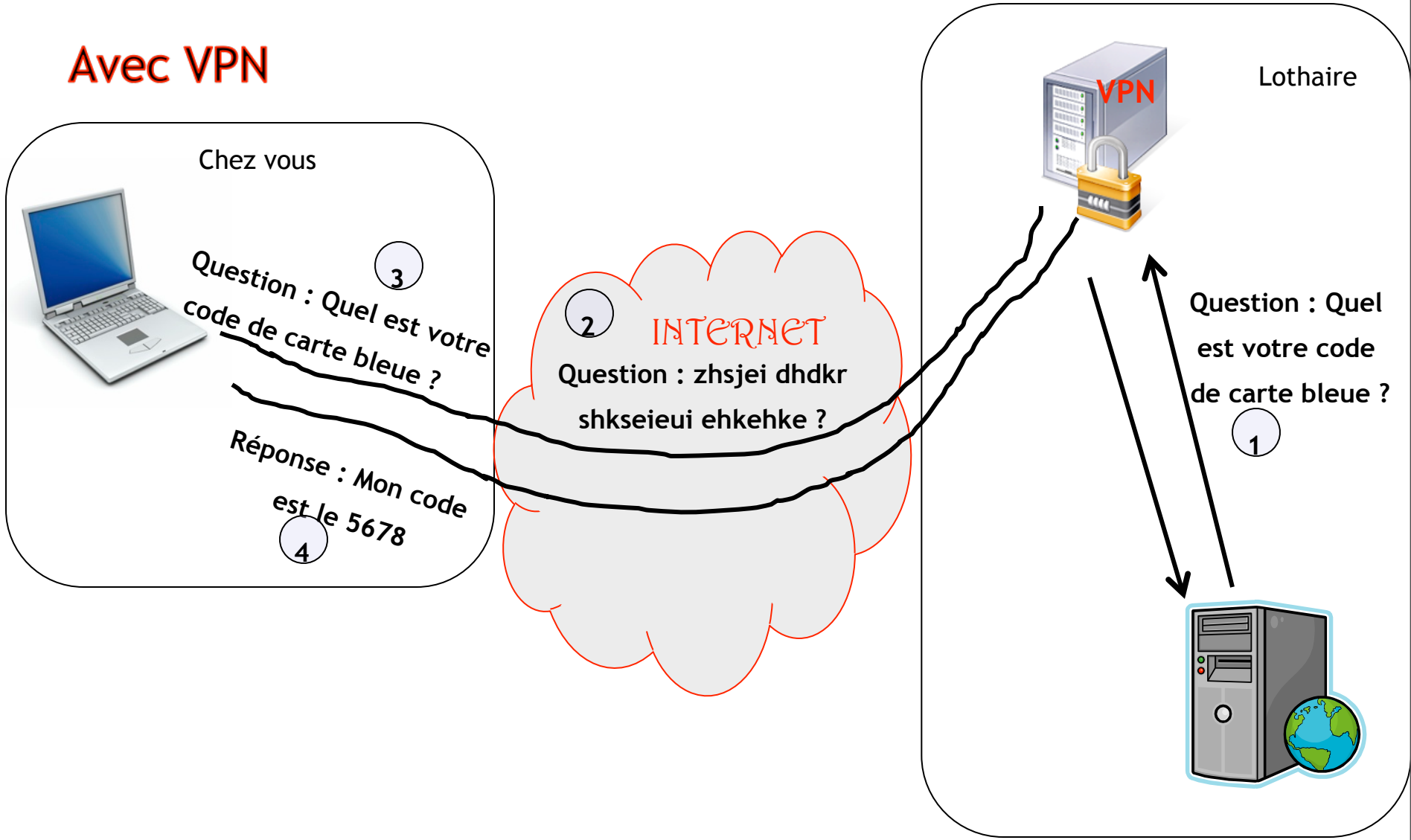
Service VPN : explication



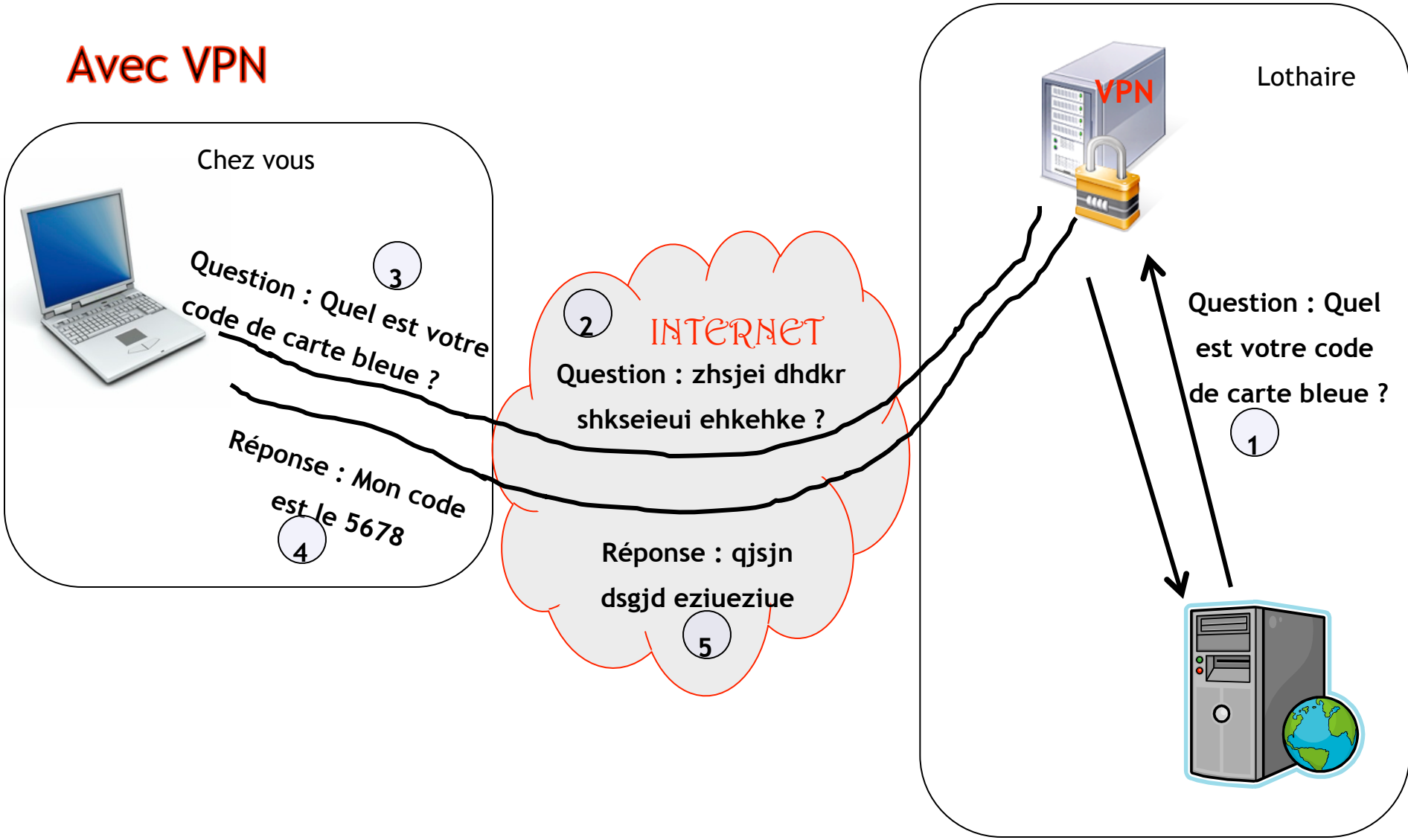
Service VPN : explication



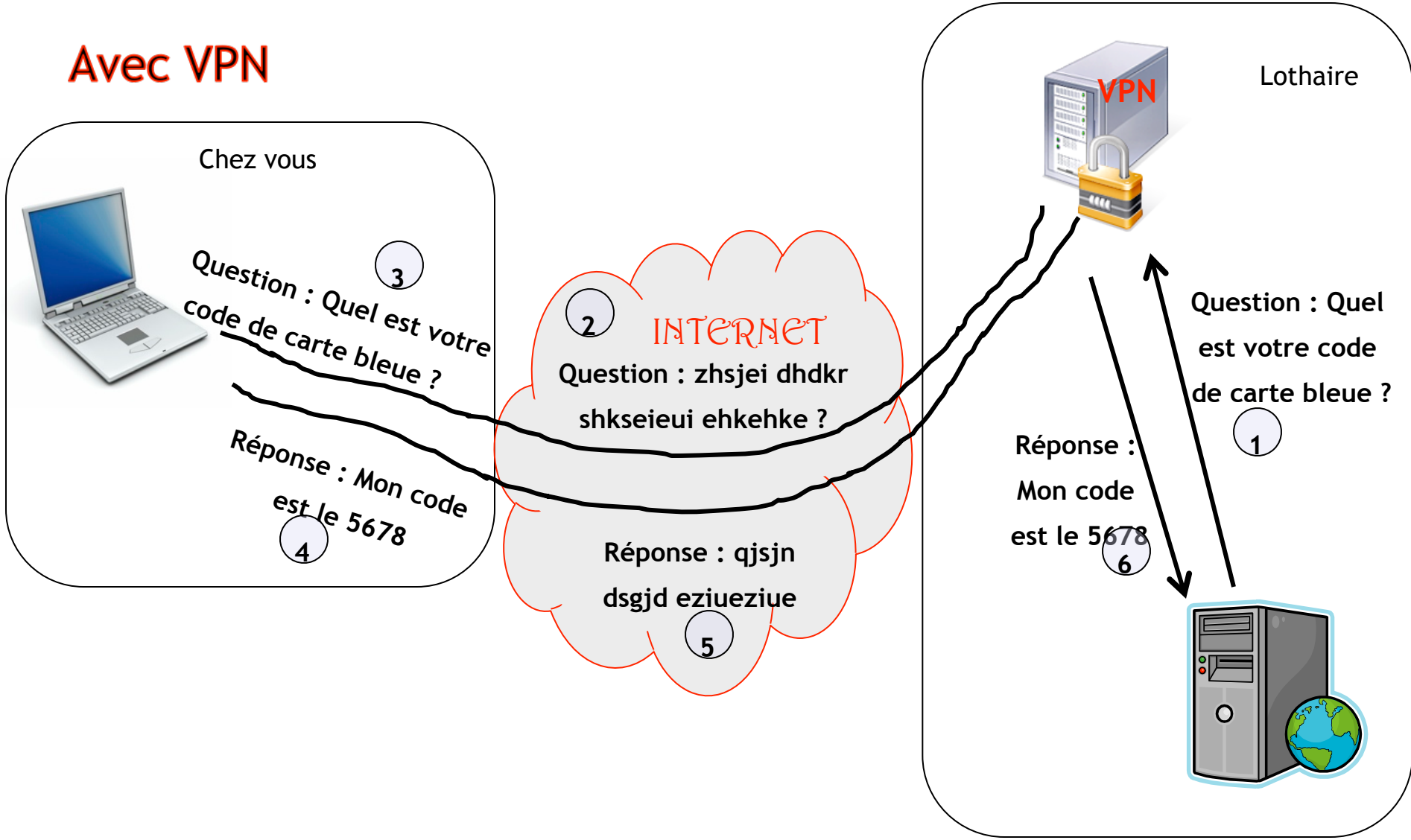
Service VPN : explication



Service VPN : explication



Service VPN : explication



Service VPN : comment ?

- Sur son concentrateur, le CIRIL propose un service VPN pour les établissements ne disposant pas d'un tel équipement
  - Demande devant émaner du responsable de l'établissement
  - « Groupe VPN » avec des adresses IP fournies par l'établissement
  - Authentification utilisant les comptes du portail des services

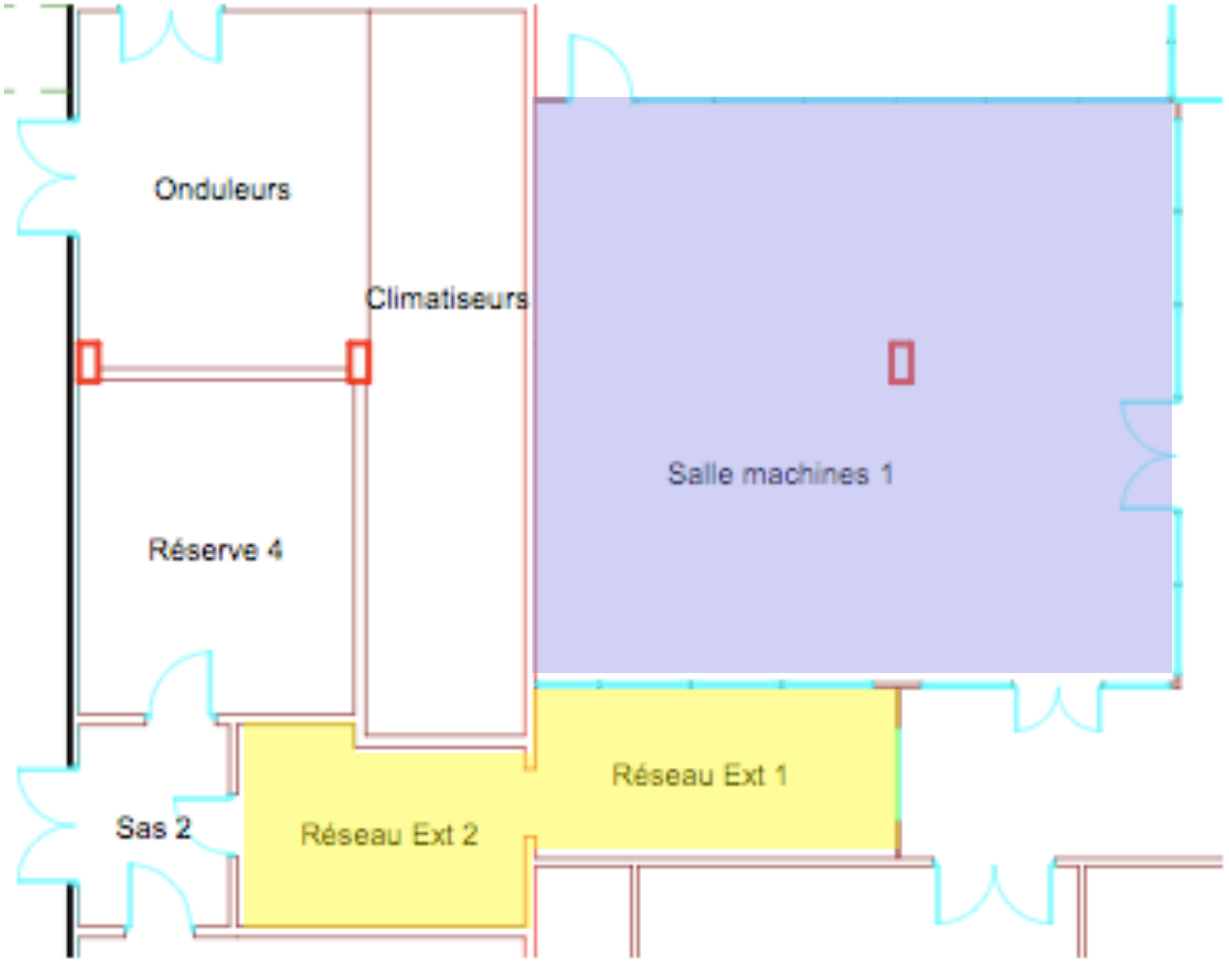
Hébergement et salle machine

Olivier LACROIX

Service d'hébergement

- Le CIRIL dispose actuellement de 2 salles d'hébergement :
  - Une petite salle multi-opérateurs accueillant entre autre :
    - Renater
    - Lothix
    - Orange Business Service (téléphonie, liaisons SDSL Lothaire et eLorraine)
    - Alcatel (fibres Renater)
  - Une salle machine dédiée à Lothaire contenant :
    - Les équipements réseaux Lothaire
    - Des serveurs propres au CIRIL (DNS, YaCaP, …)
    - Les équipements eLorraine
    - Des serveurs des universités et des EPST

Service d'hébergement



Service d'hébergement

- Chaque salle dispose :
  - De courant ondulé et secouru par un groupe électrogène,
  - D'une climatisation
  - D'un système de contrôle d'accès par badge
  - D'un système automatique de détection et d'extinction d'incendie
- Le site est surveillé en permanence par :
  - un gardien logé sur place
  - une société de gardiennage, qui reçoit toutes les alarmes

Service d'hébergement

Quel type d'hébergement ?

- Uniquement un hébergement « sec » :
  - De l'espace au sol
  - L'alimentation électrique et les prises réseau
  - Un petit espace de stockage pour quelques docs ou des pièces de rechange
- L'hébergé gère lui-même :
  - La surveillance de ses machines
  - Les sauvegardes
  - Les dépannages
  - …

Service d'hébergement

Qui peut y prétendre ?

- Le service d'hébergement est proposé à tous les clients du réseau Lothaire
- Les demandes doivent émanées des responsables des établissements
- Il est conditionné par les capacités d'accueil de la salle et des armoires

Service d'hébergement

Les conditions techniques

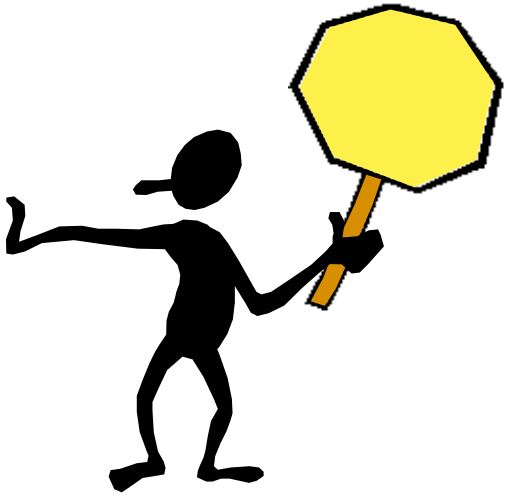
- La salle machine n'héberge que des armoires
- Les machines doivent être « rackées »
- Une armoire fournit par un hébergé lui est dédiée (à condition qu'elle soit suffisamment remplie)

Service d'hébergement

Les conditions financières

- Pour l'instant gratuit pour les 4 universités lorraines et forfaitaire pour les autres.
- Le forfait est calculé :
  - En fonction de la surface au sol et du nombre de U occupés
  - à partir des frais du CIRIL pour la salle : électricité, climatisation, …

Mais ne vous précipitez pas



Service d'hébergement

- La salle actuelle est saturée :
  - Plus d'espace au sol pour de nouvelles armoires
  - Climatisation au maximum de sa capacité
  - Onduleurs très chargés
  - Plus de prises réseau disponibles

- Pourquoi ?
  - Les demandes d'hébergement ont « explosé » durant les trois dernières années
  - Il y a actuellement environ 200 serveurs, sans compter les équipements Lothaire (routeurs, switchs, VPN, etc.)

Service d'hébergement

Les évolutions prévues

- Création d'une nouvelle salle machine en plus de l'existante
  - Nouvelle salle dédiée à l'hébergement des partenaires Lothaire
- Nouvelle climatisation plus évolutive
  - Climatisation à eau glacée permettant de distribuer les échangeurs
- Augmentation des capacités de l'onduleur

Service d'hébergement

Les évolutions prévues (suite)

- Groupe électrogène plus puissant
  - Il pourra alimenter la climatisation principale
- Changement du type d'alimentation électrique
  - Alimentation par le plafond via des canalis
    - Plus de câbles électriques dans le faux-plancher mélangés aux câbles réseaux
    - Branchement et déplacement simplifiés

Service d'hébergement

Les évolutions prévues : quand ?

- Appel d'offre d'ici la fin de l'année
- Fin des travaux au plus tard fin juin 2009
- Puis déménagement des hébergés dans la nouvelle salle et réaménagement de l'ancienne


Lothaire