Grand'Messe
Equipe réseau CiRiL

Campus INPL - ENSAIA – Amphi Cuenot

18 novembre 2010

reseau@ciril.fr

Au programme

- Introduction
- Evolution du réseau Lothaire
- Evolutions des services réseaux
- Salle d'Hébergement
- Quelques petits rappels
- Questions - Réponses

Pot

Introduction

Benoit de la FILOLIE

Benoit.De-La-Filolie@ciril.fr

Présentation du CIRIL

4 activités principales

- Maîtrise d'ouvrage, exploitation et maintenance du réseau Lothaire
- Hébergement
- Diffusion de logiciels
- Exploitation du réseau e-Lorraine

Présentation du CIRIL

Equipe

- Directeur: Benoît de la FILOLIE

Responsable financier	Service réseau	Déploiement logiciel	Développement métrologie
Valérie PETITCOLAS	Responsable: Pierre MERCIER	Patrick SIMON	Karol PROCH
Gestion administrative de Lothaire	Vincent DELOVE Annick FAUCOURT (50%) Stéphane FETTER Olivier KRAPP Olivier LACROIX Sébastien MOROSI Alexandre SIMON M. ou Mme X		
Annick FAUCOURT (50%)			

Gouvernance

- Conseil du CIRIL
- avec une représentation des 4 universités, des pouvoirs publics (CUGN, DRRT, Préfecture de Lorraine, CR de Lorraine), de certains utilisateurs (CNRS, INRIA) et du personnel du CIRIL
- au moins 2 fois par an (budget et compte de résultats)

- Relance de la concertation avec les CRI
- 3 à 4 réunions annuelles (la prochaine 26 novembre 2010)

Financement

- Réseau Lothaire

- Fonctionnement:	les utilisateurs (80%)
	SAIC (15%)
	Collectivités Territoriales (5%)
- Investissement:	CPER (Etat: 5%, CRL: 5%)
(chiffres 2009)	FEDER: 30%
	Etat (FNADT): 10%
	Contrat quadriennal UHP: 4%
	Etablissements: 30%
	Collectivités territoriales: 6%
	Fonds propres: 10%

E-Lorraine

- Marché négocié avec le Conseil Régional de Lorraine
- Marché de 4 ans : février 2010 → janvier 2014
- Supervision des liaisons des 213 lycées et CFA de Lorraine (liaisons fournies par France Télécom)

Au programme

- Introduction
- Evolution du réseau Lothaire
- Evolutions des services réseaux
- Salle d'Hébergement
- Quelques petits rappels
- Questions - Réponses

Pot

Evolutions du réseau Lothaire

Pierre MERCIER

reseau@ciril.fr

Evolutions du réseau Lothaire

- Nouvelles liaisons fibres noires
- Marché Lothaire IV
- Nouveaux sites
- Le Projet IOT@

Nouvelles liaisons fibres noires

- OREFQ
  - Observatoire Régional de l'Emploi, de la Formation et des Qualifications de Lorraine
  - Activée au Gbit/s le 16 juin 2010
  - Remplace une liaison louée (OBS) à 2 Mbit/s
  - Fibre noire de 2 km sur deux tronçons :
    - PLG – 91 Libé : StanNet
    - 91 Libé – OREFQ : StanNet

Nouvelles liaisons fibres noires

- Nancy (CIRIL) – Epinal (ENSTIB)
  - Activée au Gbit/s le 23 juin 2010
  - Remplace une liaison louée (OBS) à 30 Mbit/s
  - Fibre noire de 96 km sur quatre tronçons :
    - CIRIL – Présidence UHP : StanNet
    - Présidence UHP – Laneuveville : RMT (Tutor)
    - Laneuveville – Jeuxey : Sillon Lorrain (Arteria)
    - Jeuxey – ENSTIB : chantier CIRIL

Nouvelles liaisons fibres noires

- La traversée « sauvage » du golf d'Epinal

Nouvelles liaisons fibres noires

- INRA Champenoux
  - Activée au Gbit/s le 12 août 2010
  - Remplace un faisceau hertzien à 2 x 2 Mbit/s
  - Fibre noire de 22 km sur quatre tronçons :
    - PLG – EEIGM : StanNet
    - EEIGM – Seichamps : RMT (Tutor)
    - Laneuvelotte – Carrefour Bouteiller : PPP CG54 (Memonet)
    - Carrefour Bouteiller – INRA : chantier CIRIL

Nouvelles liaisons fibres noires

- ENSTIB – CESS Epinal
  - Sera activée au Gbit/s avant le 31 décembre 2010
  - Remplacera une liaison louée (OBS) à 2 Mbit/s
  - Fibre noire de 1 km : chantier CIRIL

Nouvelles liaisons fibres noires

- Nancy (CIRIL) – Longwy (IUT)
  - Sera activée au Gbit/s avant le 31 décembre 2010
  - Remplacera une liaison louée (OBS) à 6 Mbit/s
  - Liaison composée de deux tronçons :
    - Nancy – Esch-sur-Alzette
      - Activée au Gbit/s en septembre 2010
      - Utilisation d'un lamda fourni par Renater
    - Esch-sur-Alzette – Longwy
      - Fibre noire de 25 km sur deux tronçons :
        - Esch-sur-Alzette – Rodange : Luxconnect
        - Longlaville – Longwy (IUT) : PPP CG54 (Memonet)

Nouvelles liaisons fibres noires

- Nancy (CIRIL) – Lunéville (IUT)
  - Sera activée au Gbit/s avant le 28 février 2011
  - Remplacera une liaison louée (OBS) à 8 Mbit/s
  - Fibre noire de 35 km sur trois tronçons :
    - CIRIL – Présidence UHP : StanNet
    - Présidence UHP – Jarville : RMT (Tutor)
    - Jarville – Lunéville (IUT) : PPP CG54 (Memonet)

Nouvelles liaisons fibres noires

- Metz (Saulcy) – Ban-Saint-Martin (IRTS)
  - Sera activée au Gbit/s avant le 28 février 2011
  - Remplacera une liaison louée (OBS) à 2 Mbit/s
  - Fibre noire de 5 Km : DSP CG57 (Moselle Télécom)
  - Bus CWDM sur 3 tronçons :
    - Saulcy – CROUS Ban-Saint-Martin
    - CROUS Ban-Saint-Martin – Annexe IRTS
    - Annexe IRTS – IRTS

Marché Lothaire IV

- Evolutions des liaisons louées Lothaire
- Marché composé de six lots
- Lancé en juillet 2010
- Attribué en octobre 2010
- Lot 1
  - Liens de secours du backbone Lothaire
    - Nancy – Metz 100 Mbit/s
    - Nancy – Epinal 10 Mbit/s
  - Attribué à ARCAN Networks
  - Mise en service : 1er février 2011

Marché Lothaire IV

- Lot 2
  - Liaisons sur Epinal
    - ENSTIB – IUT : évolution de 8 à 30 Mbit/s
    - ENSTIB – IUFM : 2 Mbit/s
    - ENSTIB – CEJE : évolution de 2 à 8 Mbit/s
    - ENSTIB – IA 88 : 2 Mbit/s
  - Attribué à OBS (France Télécom)
  - Mise en service avant le 30 novembre 2010
- Lot 3
  - Liaison ENSTIB – INRA Mirecourt : évolution de 2 à 8 Mbit/s
  - Attribué à OBS (France Télécom)
  - Mise en service avant le 31 décembre 2010

Marché Lothaire IV

- Lot 4
  - Liaisons en Moselle
    - Thionville (IUT) – Forbach (IUT) : 10 Mbit/s
    - Thionville (IUT) – Saint-Avold (IUT) : 10 Mbit/s
    - Thionville (IUT) – Sarreguemines (IUT + IUFM) : 10 Mbit/s
  - Attribué à Moselle Télécom
  - Mise en service le 31 décembre 2010

Marché Lothaire IV

- Lot 5
  - Liaisons sur Saint-Dié
    - Epinal (ENSTIB) – Saint-Dié (IUT) : 30 Mbit/s
    - Saint-Dié (IUT) - Saint-Dié (INSIC) : 2 Mbit/s
  - Attribué à OBS (France Télécom)
  - Mise en service avant le 31 décembre 2010
- Lot 6
  - Liaisons sur Bar-le-Duc
    - Nancy (CIRIL) – Bar-le-Duc (IUFM+CESS) : 30 Mbit/s
    - Bar-le-Duc (IUFM+CESS) – IA 55 : évolution de 2 à 8 Mbit/s
  - Attribué à OBS (France Télécom)
  - Mise en service avant le 31 décembre 2010

Nouveaux sites

- ENIM
  - Déménagement courant août 2010
  - Avant
    - Bâtiment historique
    - Ile du Saulcy
    - Connexion via UPVM
    - 100 Mbit/s
  - Après
    - Nouveau bâtiment
    - Technopôle de Metz
    - Connexion sur la boucle optique AmpèreNet
    - 2 x 1 Gbit/s

Nouveaux sites

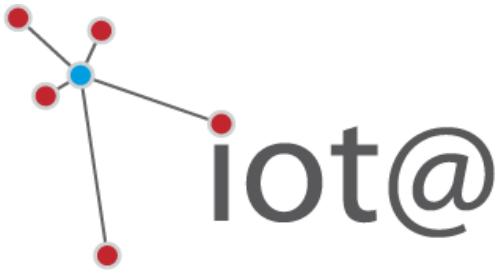
- Cité Universitaire de Bridoux
  - Avant
    - Connexion via UPVM
    - 100 Mbit/s
  - Après
    - Connexion sur AmpèreNet via la prise Supélec
    - 1 Gbit/s
- Restaurant Universitaire de Yutz
  - Connexion sur IUT de Thionville
    - Fibre noire : chantier CIRIL
    - 1 Gbit/s

Nouveaux sites

- ICN – site de Metz
  - Avant
    - Connexion via UPVM
    - 100 Mbit/s
  - Après
    - Connexion sur AmpèreNet via la prise Supélec
    - 1 Gbit/s

Le projet iot@

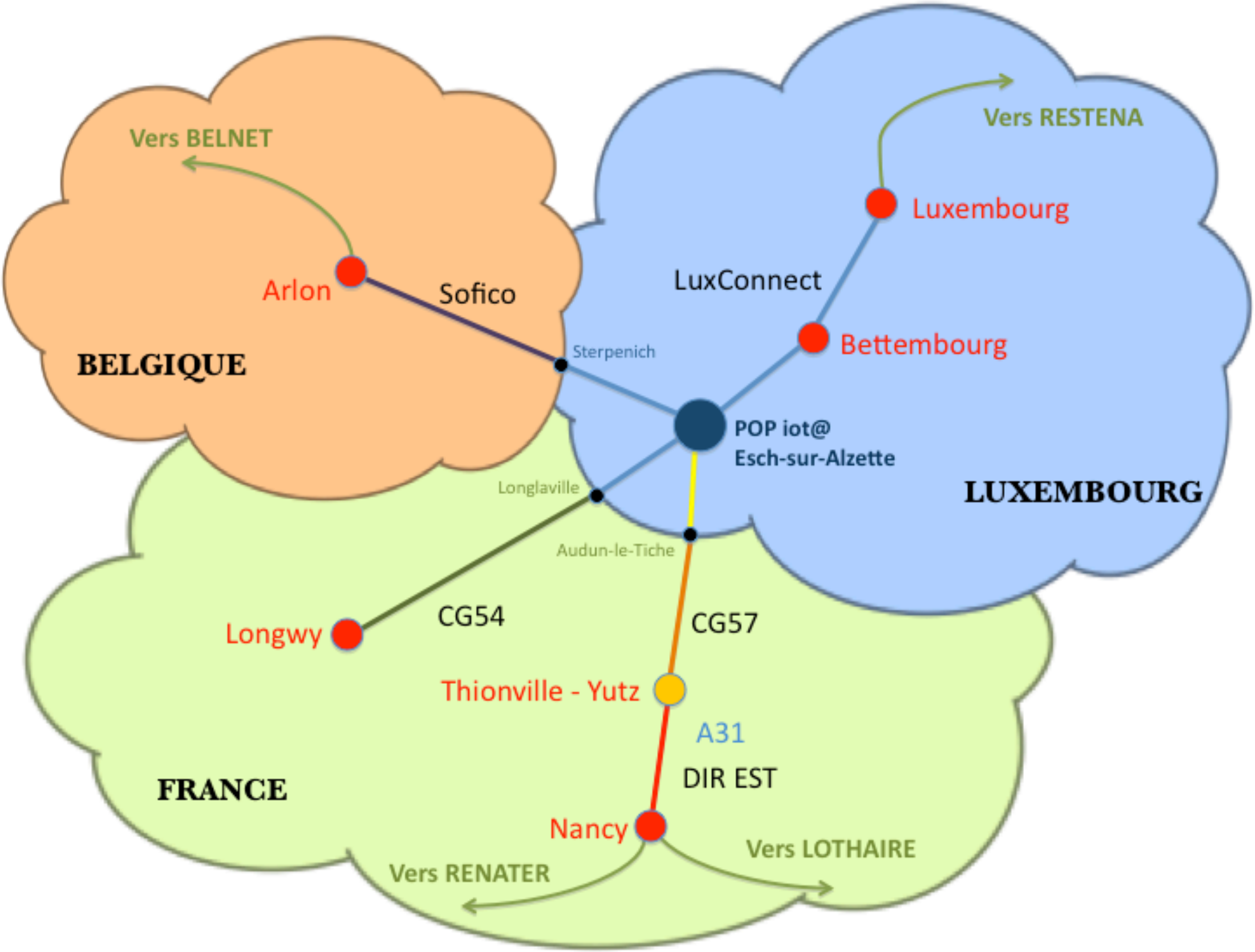
- Création d'un nœud transfrontalier sur la Grande Région
- Déploiement de liens optiques directs interconnectant les quatre NREN's (*National Research and Education Networks)* :
  - BELNET : Belgique
  - DFN : Allemagne
  - RENATER : France
  - RESTENA : Luxembourg



- IOT@ : Infrastructure Optique Transfrontalière

Le projet iot@

- Connexion directe des Universités de la Grande Région
  - Logistique d'appui au projet UGR
  - Besoins spécifiques pour les applicatifs multimédias
- Support de projets de recherche pour les Universités
  - Adhésion de l'Université de Luxembourg au projet GRID'5000 – ALADDIN : INRIA - RENATER
- Desserte de certains sites délocalisés :
  - Connexion des sites de Longwy vers Nancy par LOTHAIRE


Vers BELNET
Arlon
Sofico
BELGIQUE
Sterpenich
LuxConnect
Vers RESTENA
Luxembourg
Bettembourg
POP iot@
Esch-sur-Alzette
LUXEMBOURG
Longlaville
Audun-le-Tiche
Longwy
CG54
CG57
Thionville - Yutz
A31
DIR EST
FRANCE
Nancy
Vers LOTHAIRE
Vers RENATER

Au programme

- Introduction
- Evolution du réseau Lothaire
- Evolutions des services réseaux
- Salle d'Hébergement
- Quelques petits rappels
- Questions - Réponses

Pot

WiFi centralisée

Stéphane FETTER

reseau@ciril.fr

Les concepts

… du moins les principaux !

Ce qui change

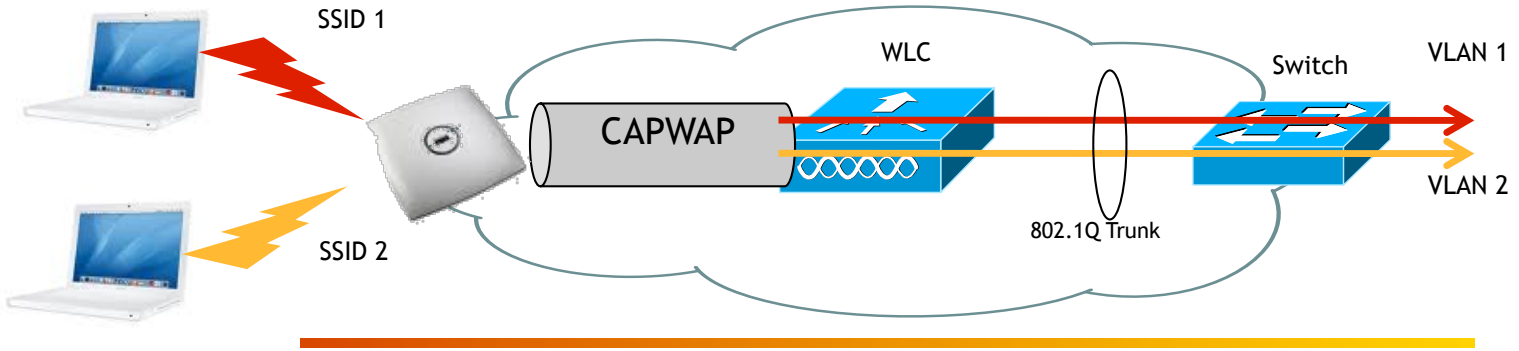
- AVANT
  - Bornes « lourdes »
    - chaque borne était un équipement autonome
    - IOS, configuration, VLANs
  - Transport de VLANs (trunk) jusqu'aux APs
  - Outil central de gestion des bornes (optionnel) : WLSE

- MAINTENANT
  - Bornes « légères »
    - pilotées par des contrôleurs
    - IOS, configuration et ajustements dynamiques (puissance, canaux …)
  - @IP de management
  - Tunnel CAPWAP s'appuie sur les RFC 5415 et 5416
  - Un contrôleur pour N bornes
  - Outils de gestion des contrôleurs (optionnel) : WCS

Le tunnel CAPWAP

- Tunnel CAPWAP (Control and provisioning of wireless access points)
  - Entre contrôleur et bornes
  - Sur IP (routable)
  - Protocole de contrôle et de transport des données

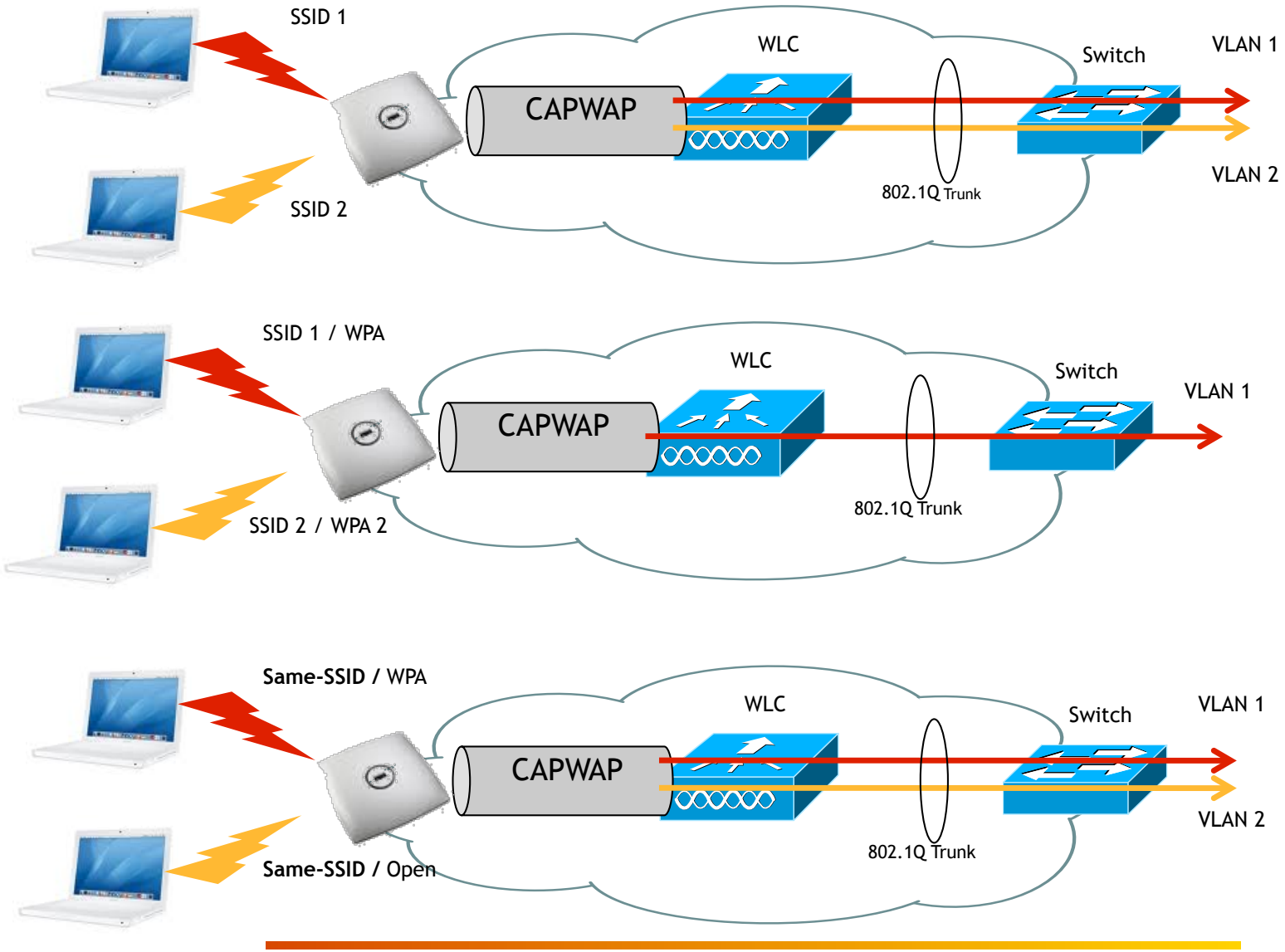
- Transport des VLANs jusqu'au(x) contrôleur(s)
- Tunnelisation des VLANs jusqu'aux APs



Mise en œuvre

- Concept
  - Associer un VLAN (celui qu'on connaît !) avec un WLAN
  - Définir les WLANs sur les contrôleurs
    - SSID
    - Authentification
    - Cryptage
    - QoS …
  - Définir pour un ensemble de bornes (ie. Un 'AP group'), quels sont les WLANs à diffuser et quel VLAN associer à chaque WLAN
- Possibilités multiples de mise en œuvre

Exemples de mise en œuvre

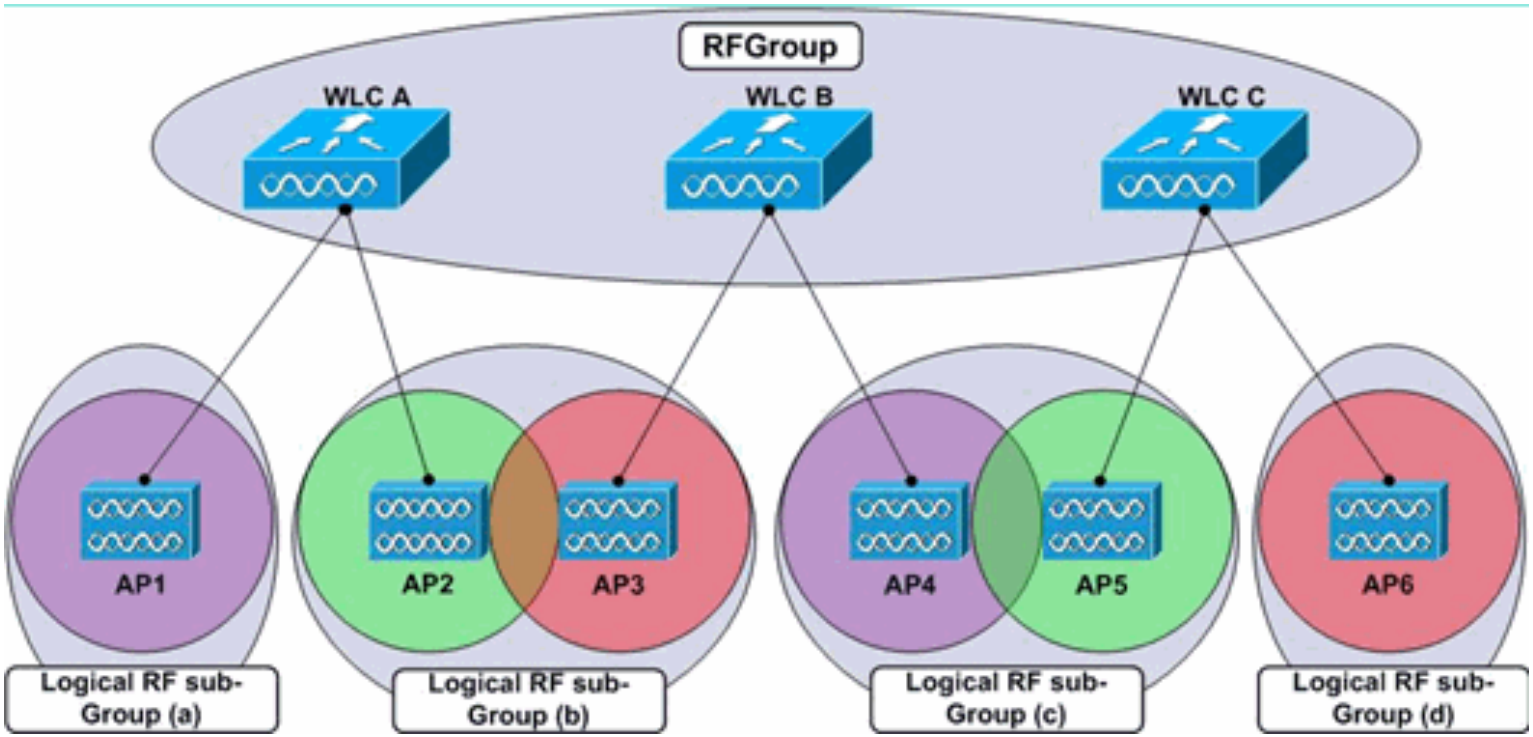


WLC : Wireless Lan Controler

- Plusieurs types de contrôleurs
  - Autonomes
  - Modules de 6500
- Taille du contrôleur fonction du nb de bornes à gérer
- Wireless Service Module (WiSM)
  - 1 module de 6500
  - 2 contrôleurs indépendants
  - Chaque contrôleur pouvant gérer 150 bornes
- Le contrôleur embarque et upgrade l'IOS des bornes
- Interface de configuration
  - HTTP
  - CLI

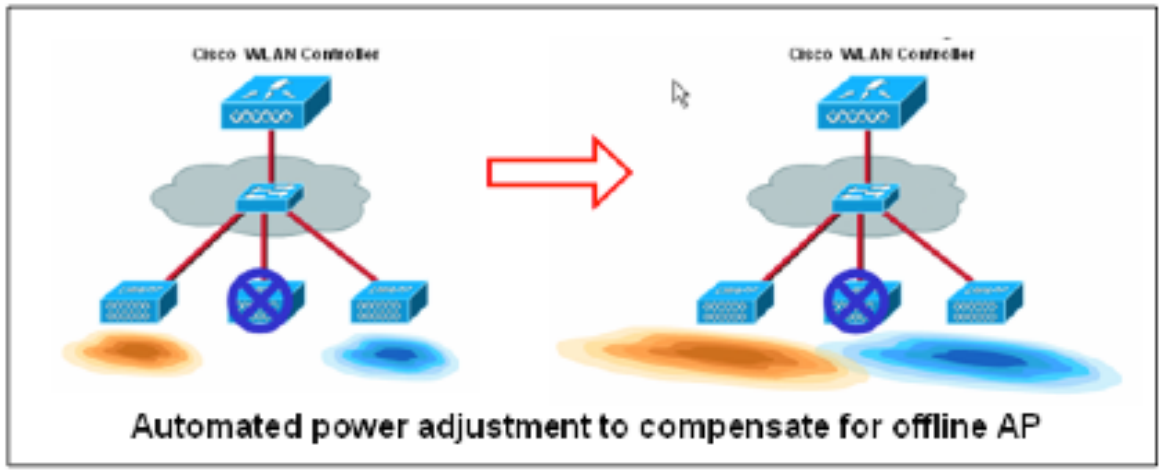
WLC : Wireless Lan Controler

- Gestion dynamique des fréquences : RF Group



WLC : Wireless Lan Controler

- Gestion dynamique de la puissance



- Gestion du *roaming*
  - Intra/Inter-contrôleur
- Authentification RADIUS
  - dialogue des contrôleurs avec le RADIUS et non les APs

La découverte des contrôleurs

- Au 1er boot, l'AP ne connaît pas son contrôleur
- L'AP dispose de quatre modes de découverte
  - Découverte sur réseau filaire
  - Requête DNS
  - Option de bail DHCP
  - Découverte sans fils
- L'AP mémorise le ou les contrôleurs auxquels s'associer ultérieurement

Logiciel Wireless Control System (WCS)

- Gestion centralisée des contrôleurs
- Modification des configurations
  - uniformisation
  - configuration par « templates »
- Mise à jour de l'OS des contrôleurs
  - Procédure simplifiée
  - MàJ contrôleur = MàJ des bornes
- Gestion des administrateurs
  - Authentification
  - Autorisations
  - Notions de vues
- Supervision des contrôleurs et des bornes
- Cartographie

Architecture CROUS

Infrastructure et Design

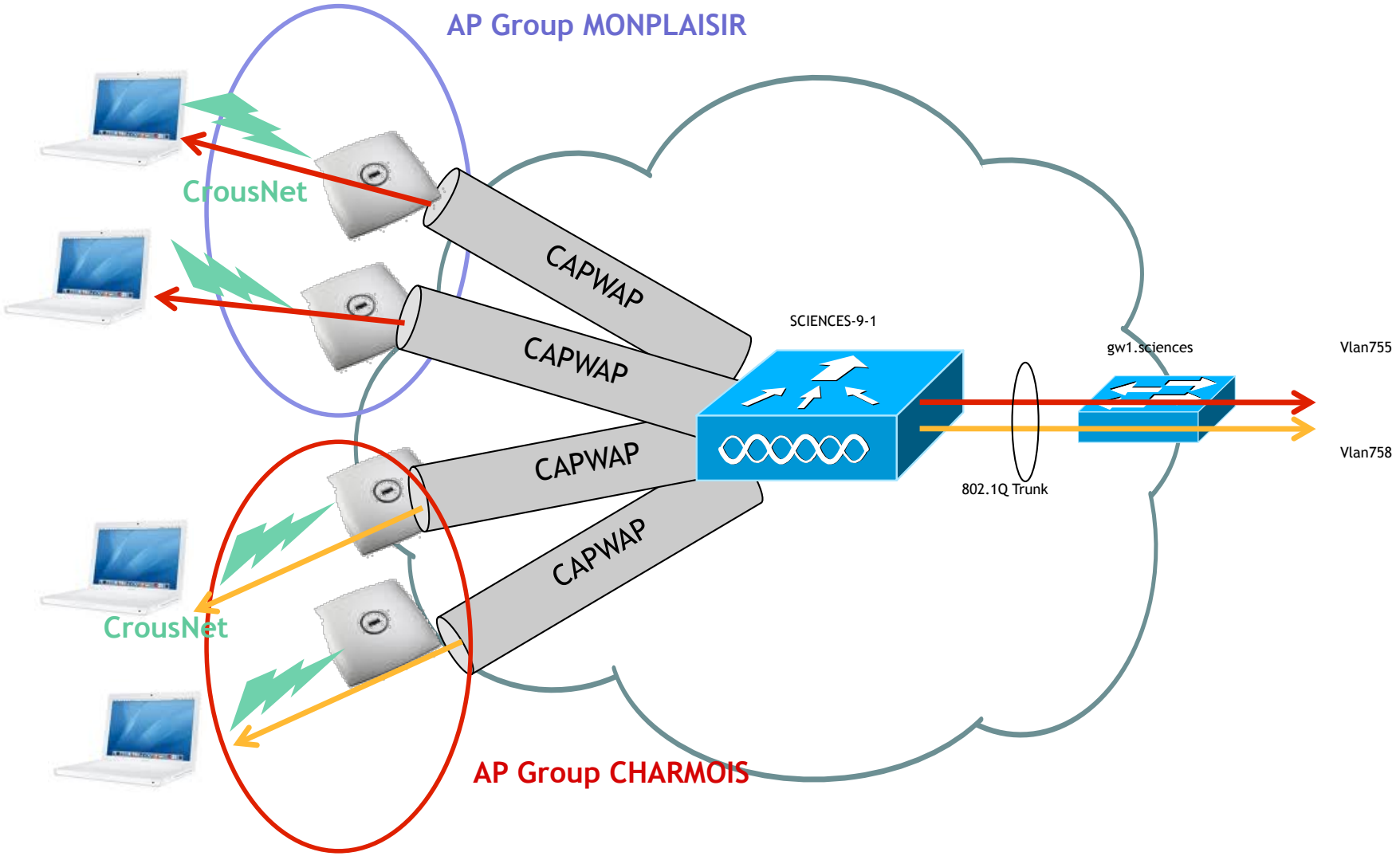
Equipements

- 4 modules WiSM
  - 8 contrôleurs
  - Metz, PLG, Sciences, CIRIL
  - 4x300 = 1200 bornes max
- Les Access Points (AP)
  - 850 bornes déployées et près de 1000 à terme
  - AP 1131 : a/b/g
  - Réparties sur les 4 contrôleurs
- WCS
  - Pour gestion centralisée des 8 contrôleurs
  - Licence pour 1000 bornes
  - Sur serveur Windows 2003
- Un serveur DHCP

WLAN, VLANs et AP Groups

- Un seul WLAN
  - SSID : CrousNet équivalent SSID : Nancy-Universite
  - Pas d'authentification auprès de la borne
  - Pas de chiffrement
- VLANs
  - Les VLANs YaCaP
  - Règle
    - 1 Cité U = 1 vlan YaCaP
    - VLAN captif filaire = VLAN captif WiFi

Mise en œuvre CROUS



DHCP

- APs adressées dans les VLANs de management des switchs
- APs configurées pour obtenir une @IP via DHCP
- Serveur DHCP
  - Configuration dynamique puis statique des baux

- Découverte initiale du contrôleur par AP
  - Utilisation de l'option 43
  - DHCP envoie à l'AP l'@IP du contrôleur auquel se rattacher lors de la première installation de l'AP

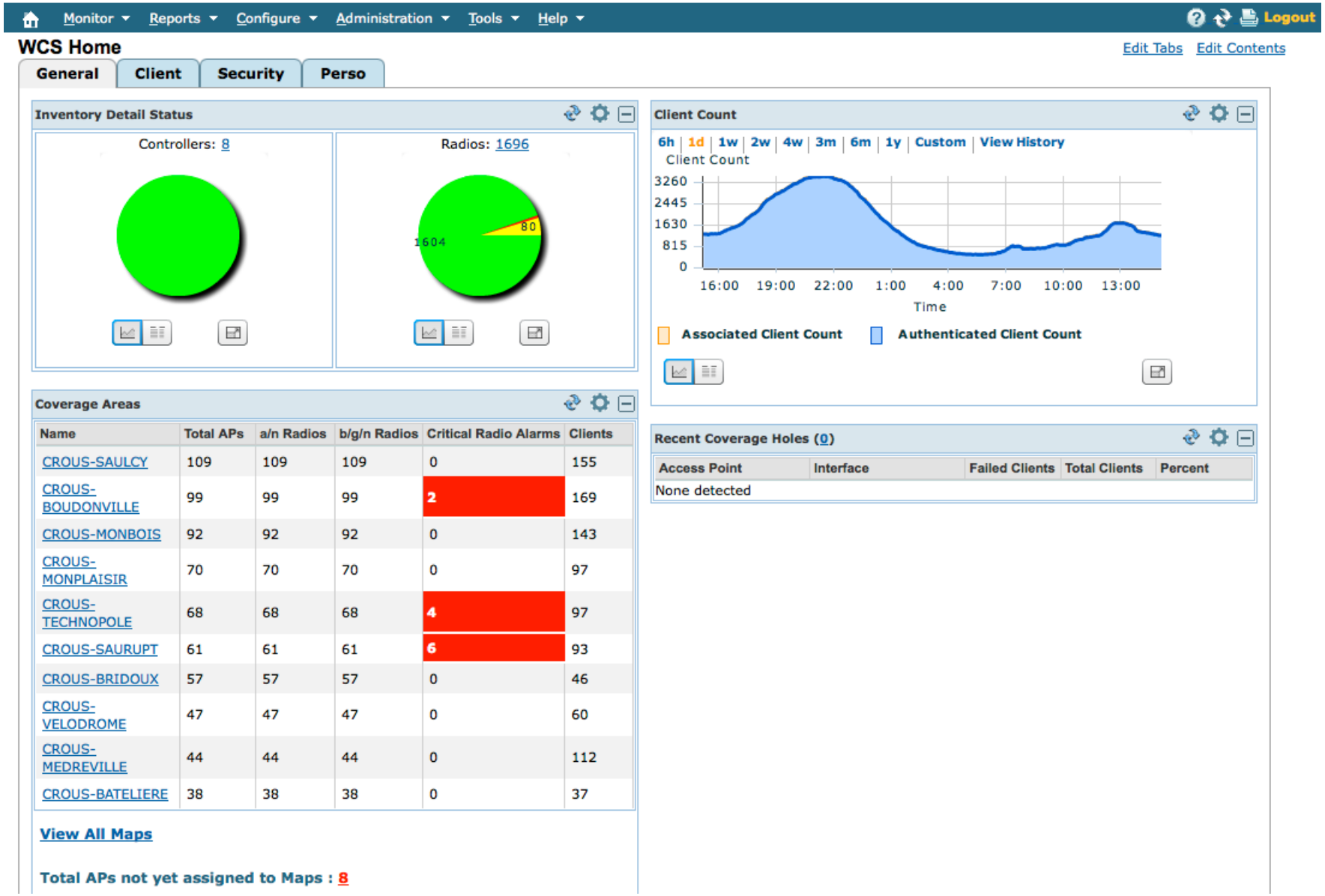
Migration

- Migration autonome -> light via WCS
  - Importation des bornes autonomes dans WCS
  - Test de la capacité à migrer en IOS light
  - Lancement du processus de migration vers light par Cité U
- Intégration des bornes dans les bons AP Groups
- Création des MAPS dans WCS

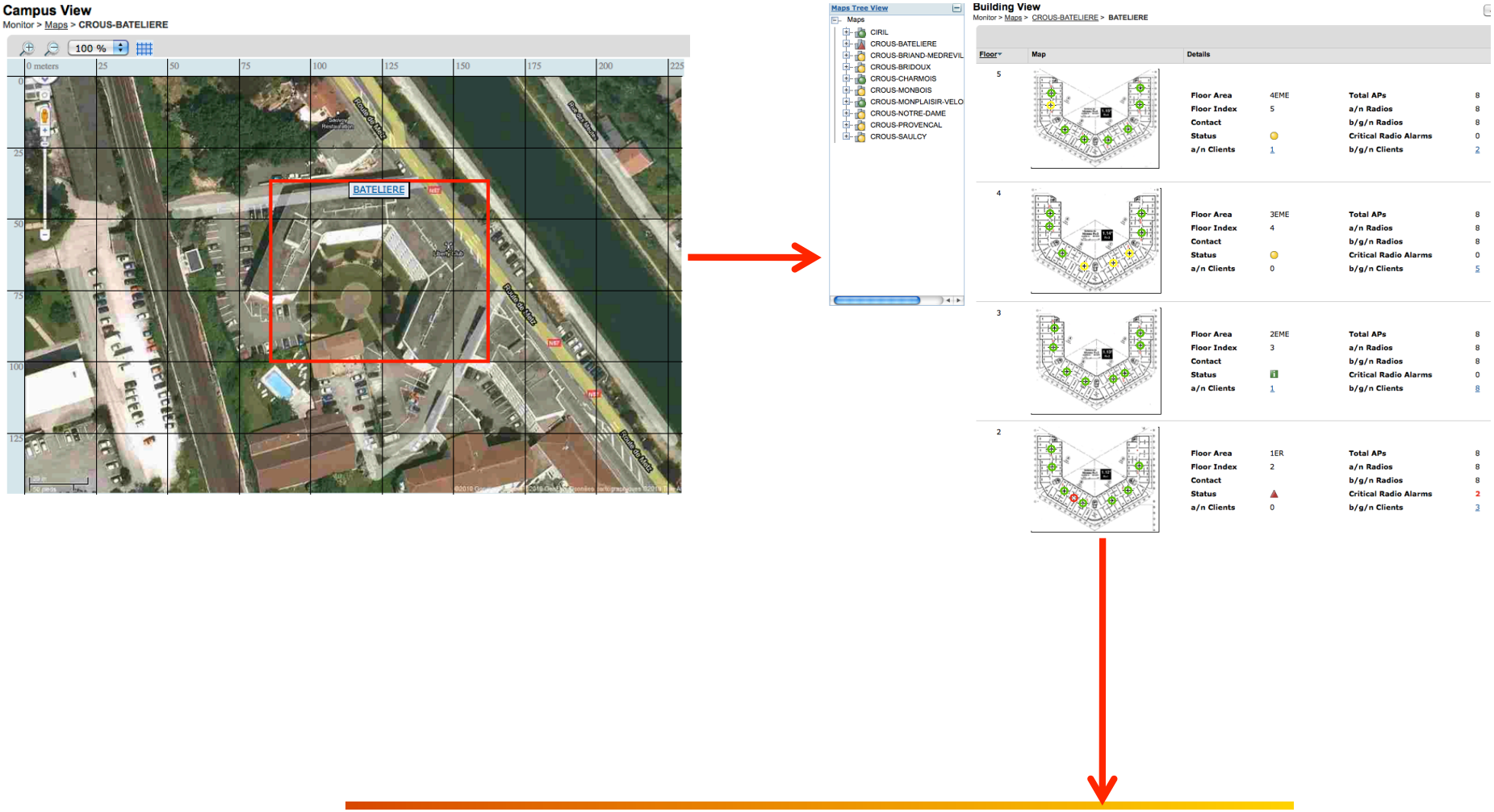
Interface WCS

- Authentification
  - Utilise un serveur RADIUS ou TACACS
  - Environnement personnalisable (onglet, graphe …)
  - Portée de la visibilité par utilisateur configurable
- Accueil avec les indicateurs
  - Suivi de l'état
    - des contrôleurs
    - des bornes
    - des clients connectés

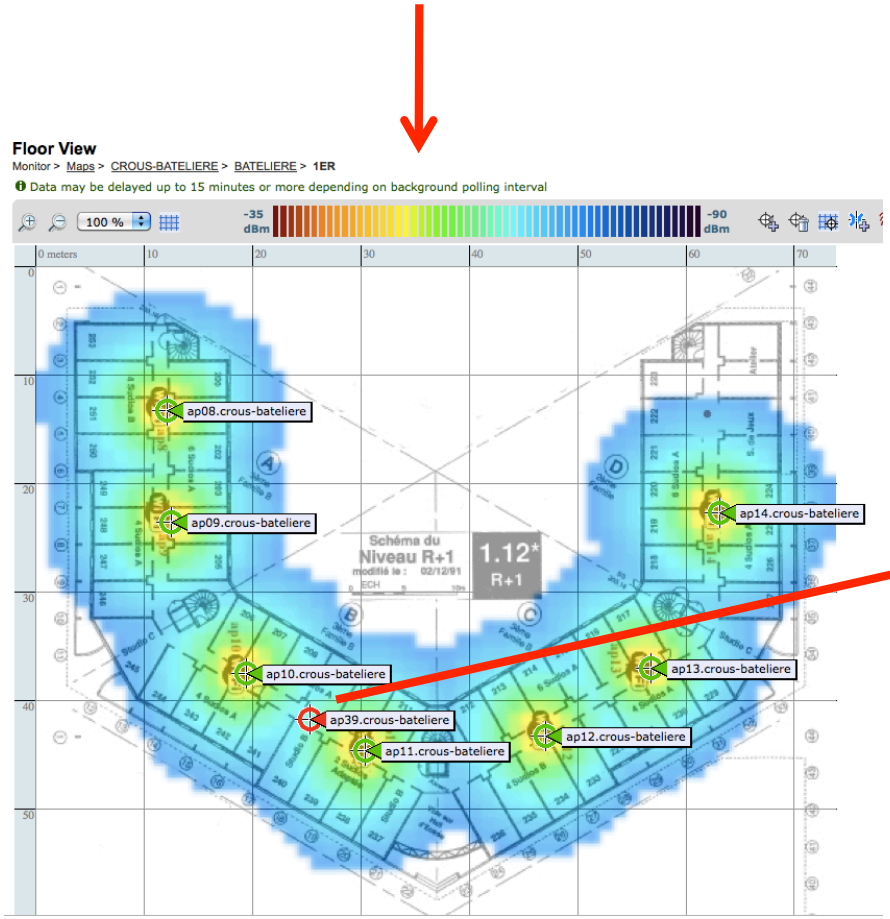
WCS : ACCUEIL

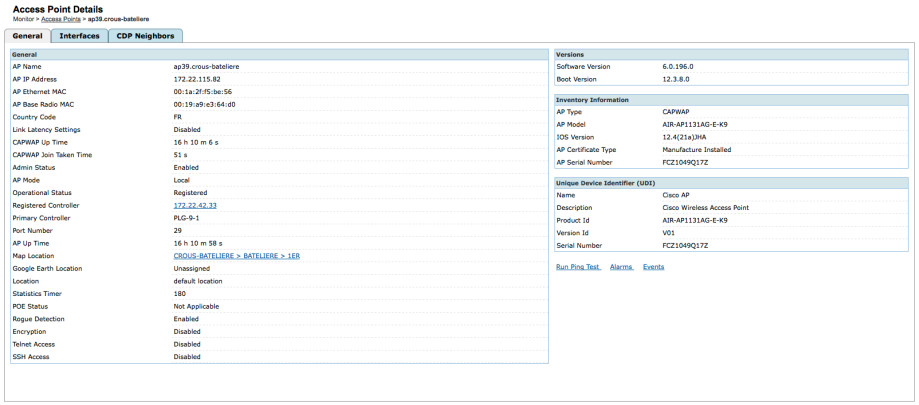

Monitor
Reports
Configure
Administration
Tools
Help
Logout
WCS Home
Edit Tabs
Edit Contents
General
Client
Security
Perso
Inventory Detail Status
Controllers: 8
Radios: 1696
1604
80
Client Count
6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom | View History
Client Count
3260
2445
1630
815
0
16:00
19:00
22:00
1:00
4:00
7:00
10:00
13:00
Time
Associated Client Count
Authenticated Client Count
Coverage Areas
Name
Total APs
a/n Radios
b/g/n Radios
Critical Radio Alarms
Clients
CROUS-SAULCY 109 109 109 0 155
CROUS-BOUDONVILLE 99 99 99 2 169
CROUS-MONBOIS 92 92 92 0 143
CROUS-MONPLAISIR 70 70 70 0 97
CROUS-TECHNOPOLE 68 68 68 4 97
CROUS-SAURUPT 61 61 61 6 93
CROUS-BRIDOUX 57 57 57 0 46
CROUS-VELODROME 47 47 47 0 60
CROUS-MEDREVILLE 44 44 44 0 112
CROUS-BATELIERE 38 38 38 0 37
View All Maps
Total APs not yet assigned to Maps : 8
Recent Coverage Holes (0)
Access Point
Interface
Failed Clients
Total Clients
Percent
None detected

Cartographie et Couverture



Cartographie et Couverture





Mutualisation du service

Certains de nos utilisateurs ont émis un intérêt pour cette technologie :

- Acquisition d'une carte contrôleur partagée
  - Bénéficier des avantages de la centralisation même pour un nombre restreint de bornes
  - Proposer le service pour un coût d'entrée moindre
  - Solution clé en main rapidement opérationnelle
- Le service est ouvert à tous dès maintenant. Contactez nous pour en connaitre les modalités
- Questions ?

Service DNS et DNSSEC

Alexandre SIMON

reseau@ciril.fr

Service DNS et DNSSEC

- DNSSEC, *quèsaco* ?
  - Un ensemble d'extensions au protocole DNS
    - anciens systèmes toujours compatibles !
  - Utilisation de signature asymétrique (clés publiques/privées)
  - Ajouts de nouveaux enregistrements dans les zones (DNSKEY, RRSIG, NSEC, NSEC3, DS)

Service DNS et DNSSEC

- Ce que fait DNSSEC :
  - vérification de l'authenticité des données
  - vérification de l'intégrité des données
  - vérification de l'intégrité de la "non existence" d'une donnée
  - la protection contre certaines attaques, notamment le *cache poisonning*

- Ce que ne fait pas DNSSEC :
  - la confidentialité des échanges (cf. TSIG et IPsec)
  - la protection contre des attaques de type DoS et DDoS
  - la protection contre le phishing, virus et vers …

Service DNS et DNSSEC

- Fonctionnement de DNSSEC

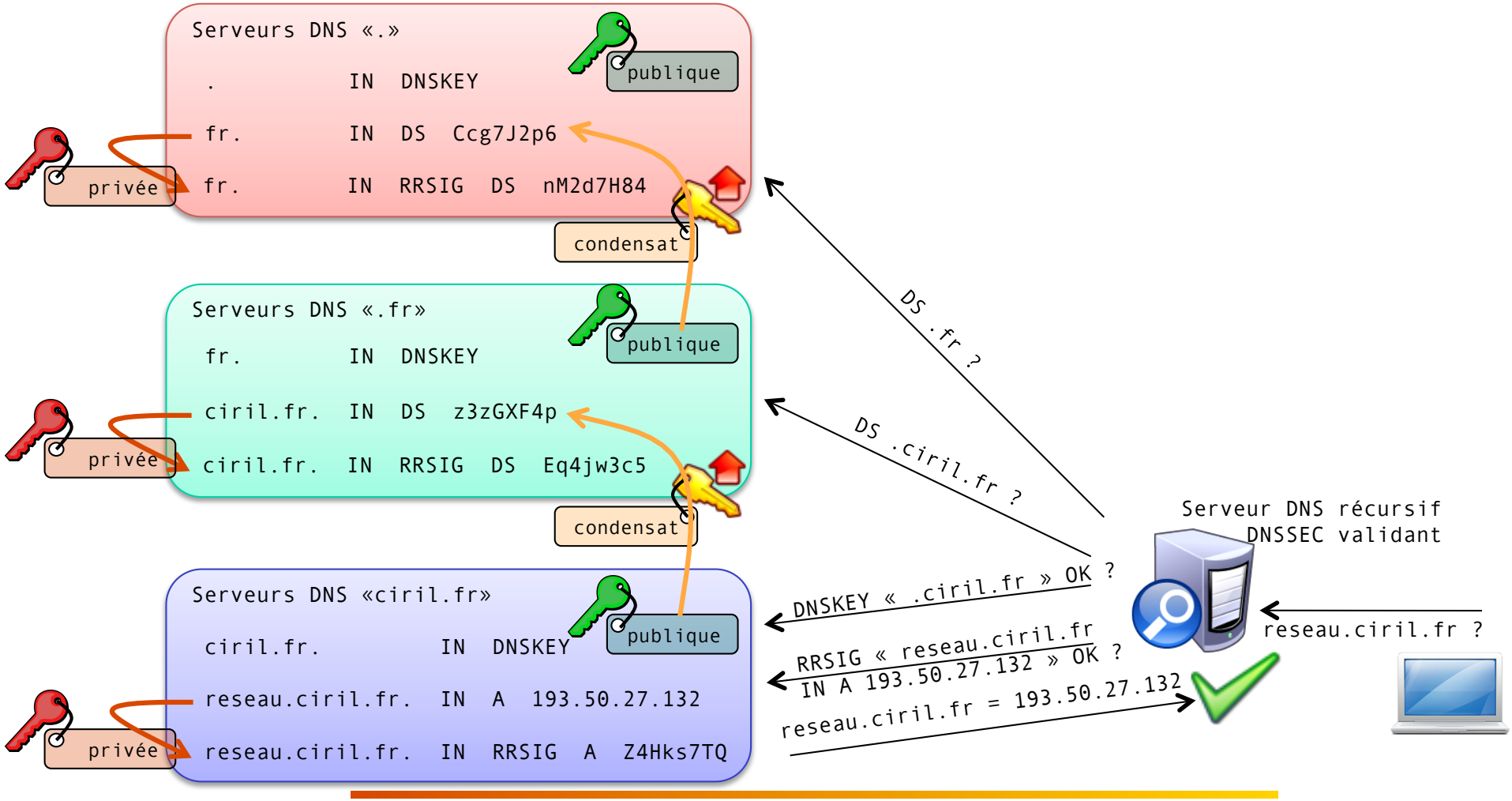
ATTENTION

L'animation qui suit n'est pas totalement correcte.

Au delà des détails techniques, c'est le principe qu'il faut appréhender et comprendre.

Service DNS et DNSSEC

- Fonctionnement de DNSSEC



Service DNS et DNSSEC

- Fonctionnement de DNSSEC : les points à retenir
  - tous les enregistrements classiques (A, PTR, CNAME, MX, TXT…) sont signés → champs RRSIG
  - les zones signées sont plus « grosses »
  - existence d'une chaine de certification et de confiance entre les zones parentes et les sous zones → champs DS

```
$ dig +dnssec fr. NS @arcturus.ciril.fr

; <<>> DiG 9.6.0-APPLE-P2 <<>> +dnssec fr. NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3021
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 15


$ dig +dnssec . NS @arcturus.ciril.fr

; <<>> DiG 9.6.0-APPLE-P2 <<>> +dnssec . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53936
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 15
```

Flag AD = Authentic Data

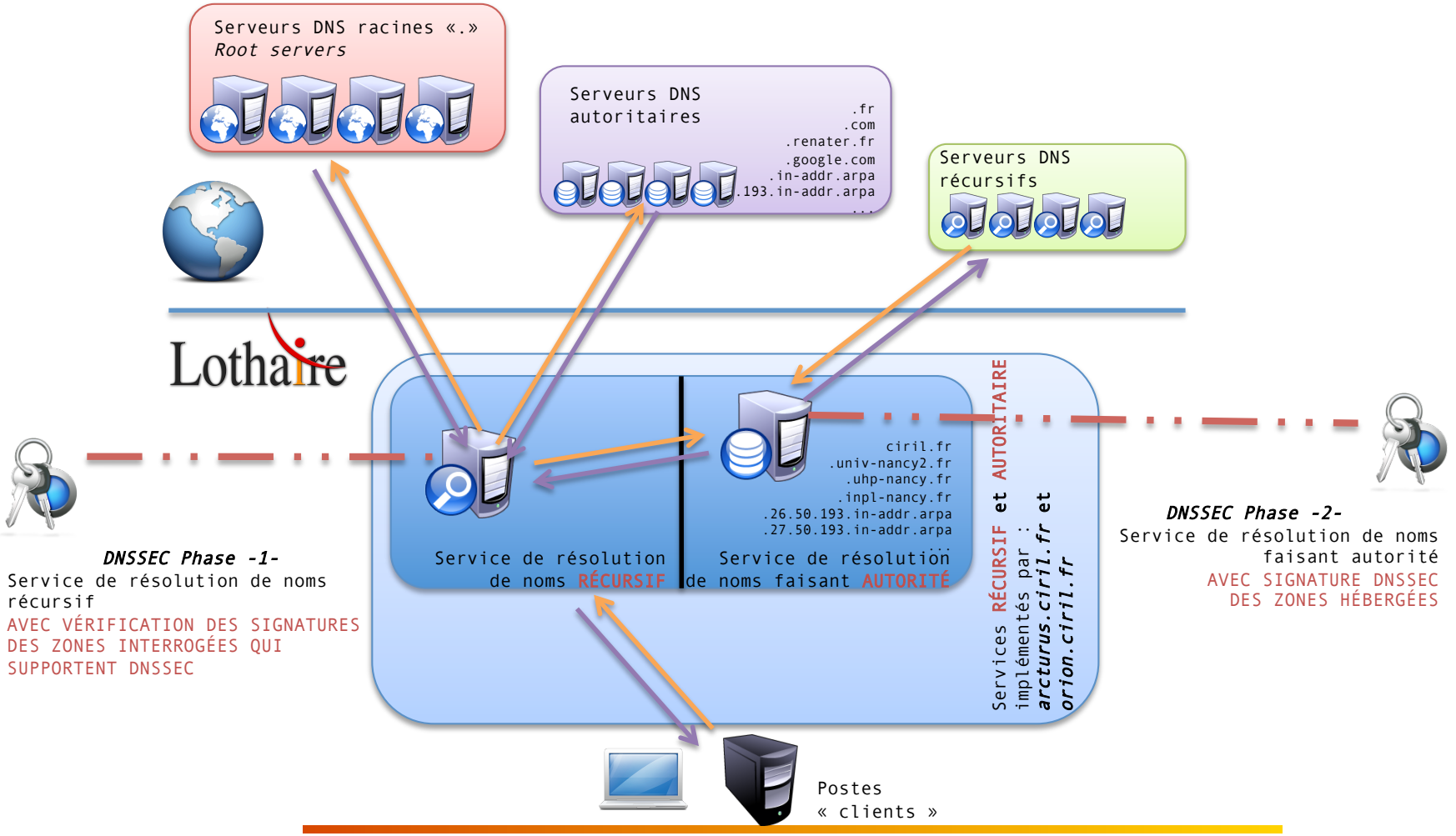
Service DNS et DNSSEC

- Pourquoi DNSSEC est si important ?
  - le DNS est LE service de base de l'Internet
  - les attaques par « empoissonnement de cache » jusqu'ici théoriques… sont maintenant possibles ! → cf. la puissance croissante des ordinateurs
  - DNSSEC révolutionne le fond, pas la forme :
    - utilisateur final ne sait pas qu'il fait du DNSSEC
    - le correspondant de zone ne se soucie pas des signatures dans le fichier de zone

  → seul l'administrateur du DNS doit « faire ce qu'il faut » pour être « DNSSEC aware »

Service DNS et DNSSEC

- Déploiement du service DNSSEC sur Lothaire



Service DNS et DNSSEC

- Déploiement du service DNSSEC sur Lothaire
  - ***Phase -1-*** : déploiement de serveurs DNS récursif DNSSEC validants

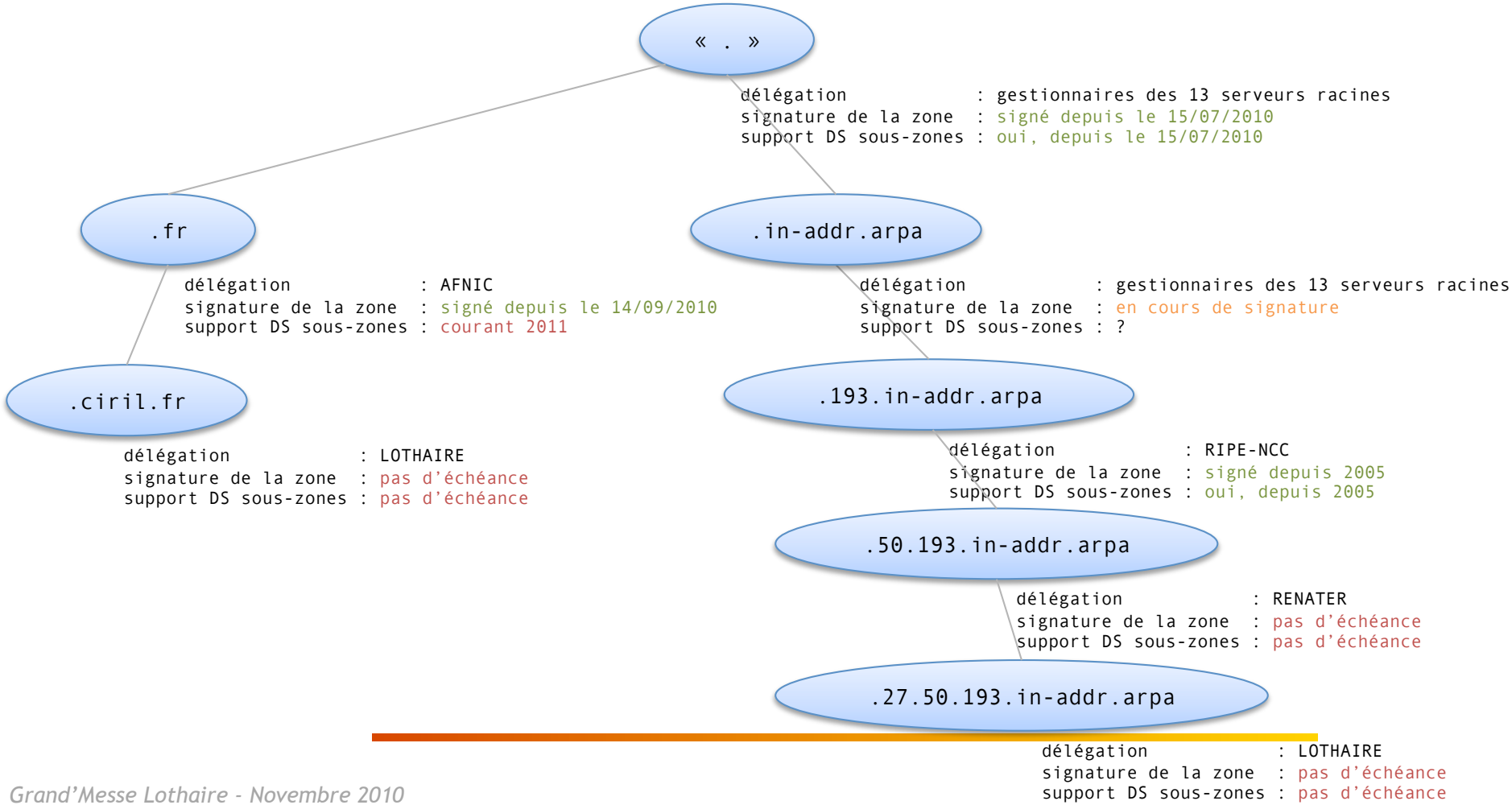
    → FAIT, sur arcturus et orion depuis le 19/07/2010
    http://reseau.ciril.fr/doc/News/News-20100720-0
    http://reseau.ciril.fr/doc/Services/DNS#tocLink5

  - ***Phase -2-*** : signature des zones hébergées « ciril.fr, uhp-nancy.fr, 27.50.193.in-addr.arpa, … »

    → A FAIRE
    - à intégrer dans l'interface de gestion du DNS
    - zones signées réellement utilisables quand toute le chaine du DNS le sera

Service DNS et DNSSEC

- Déploiement du service DNSSEC sur Lothaire
  - ***Phase -2-*** : état des signatures des zones parentes



Service DNS et DNSSEC

- Nouvelle interface de gestion du DNS
  - fin 2008 - 2010 : restructuration du S.I. CIRIL
    → nécessaire pour le développement de la nouvelle interface
    (cf. partie Vincent « SI : le point »)
  - début 2011 : début du développement en concertation avec les CRI et les correspondants

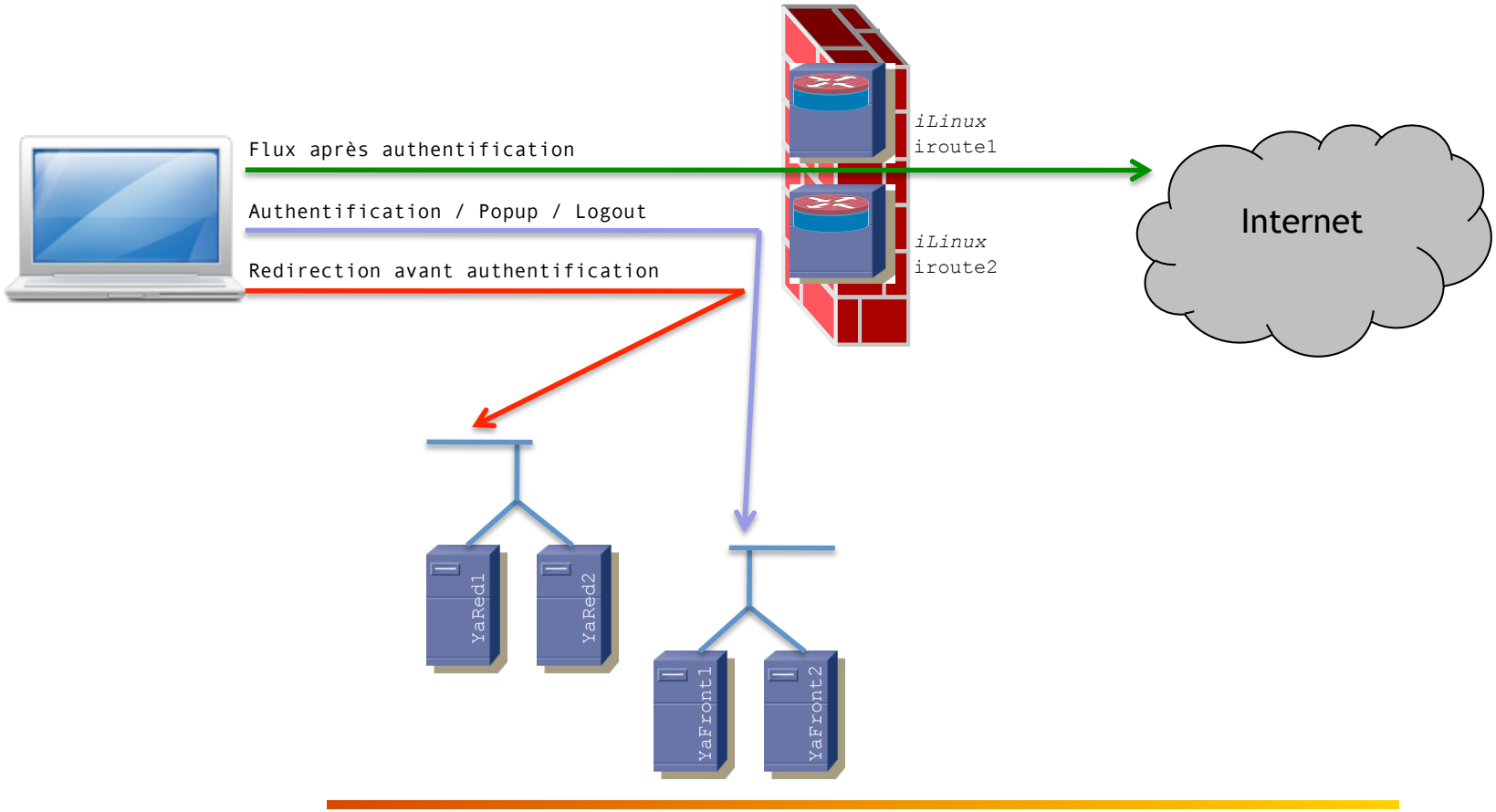
YaCaP : portail captif
Limiteurs *HTTP* et chronos SI

Alexandre SIMON

reseau@ciril.fr

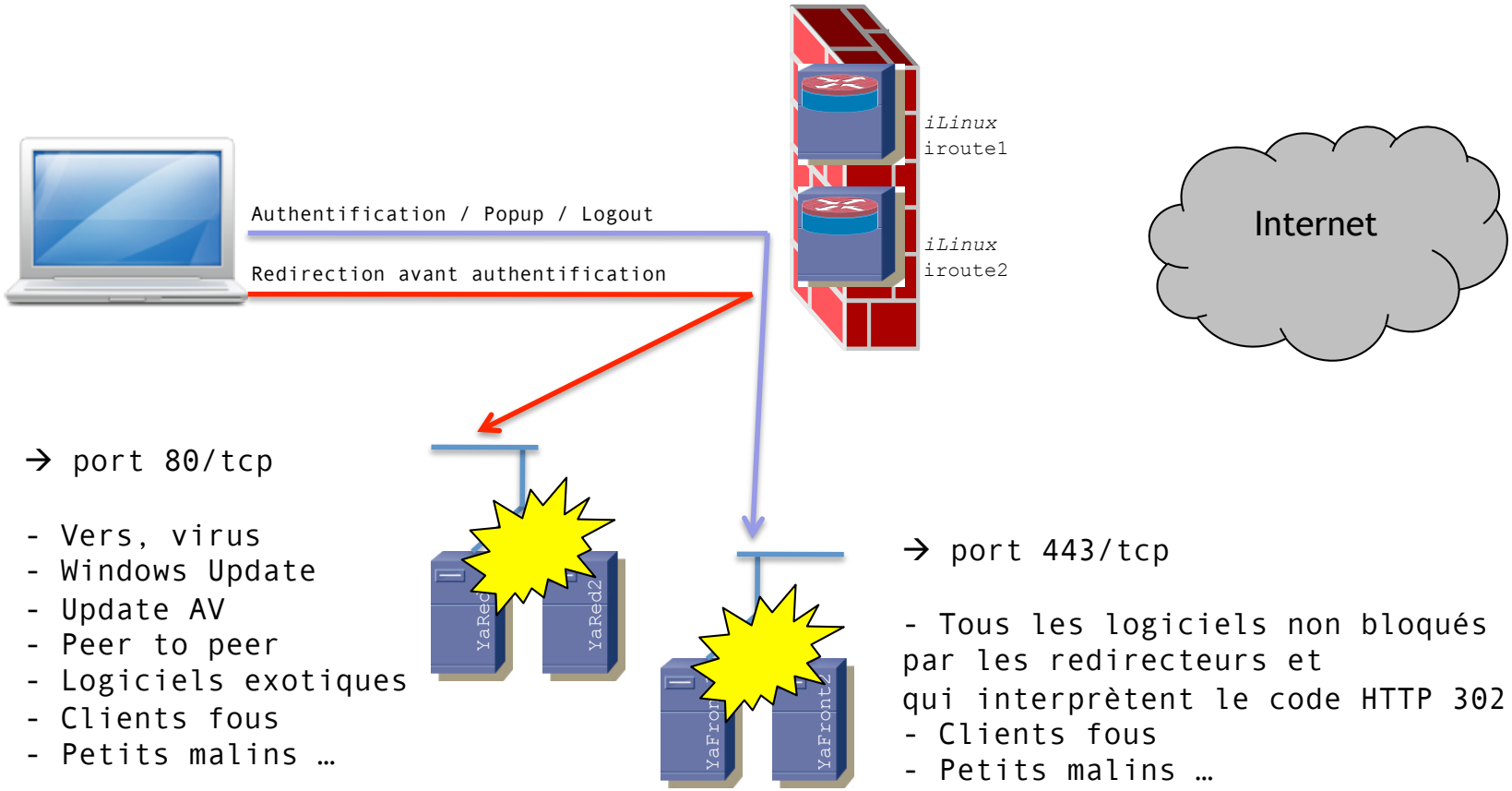
YaCaP : limiteurs HTTP et chronos

- Les flux « normaux » HTTP(S) entre les clients et YaCaP



YaCaP : limiteurs HTTP et chronos

- Les flux « bizarres » HTTP(S) entre les clients et YaCaP



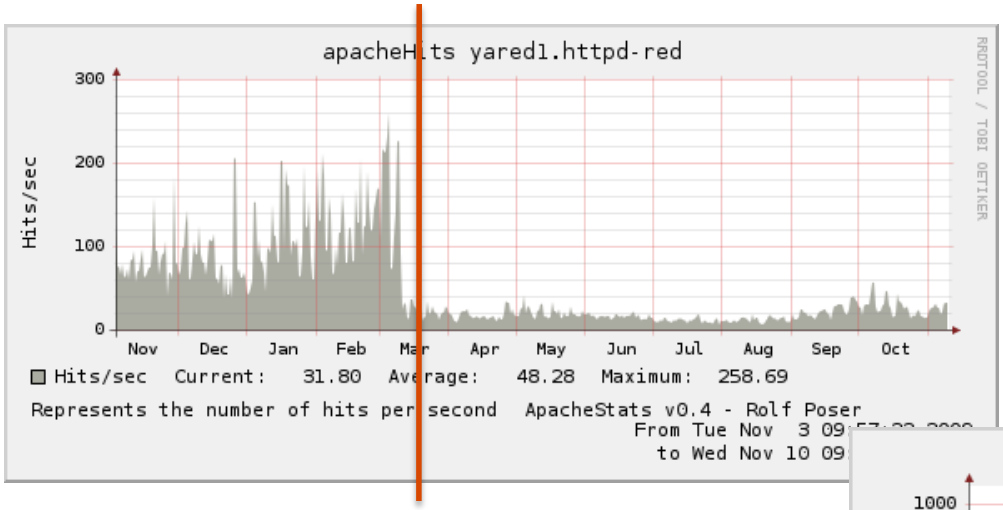
YaCaP : limiteurs HTTP et chronos

- Ressources limitées sur les serveurs yared* et yafront*
  - nombre de *socket* ouvertes
  - nombre de processus *Apache forkés* (+processus → +mémoire +cpu +charge)

- *Netfilter/Iptables rate-limiter HTTP/HTTPS*
  - assurer que les ressources critiques sont protégées
  - utilisation des modules *Netfilter connlimit* et *hashlimit*
    - *connlimit* : limitation du nombre de socket / client
    - *hashlimit* : limitation du nombre de nouvelle socket / seconde / client (paquet SYN)

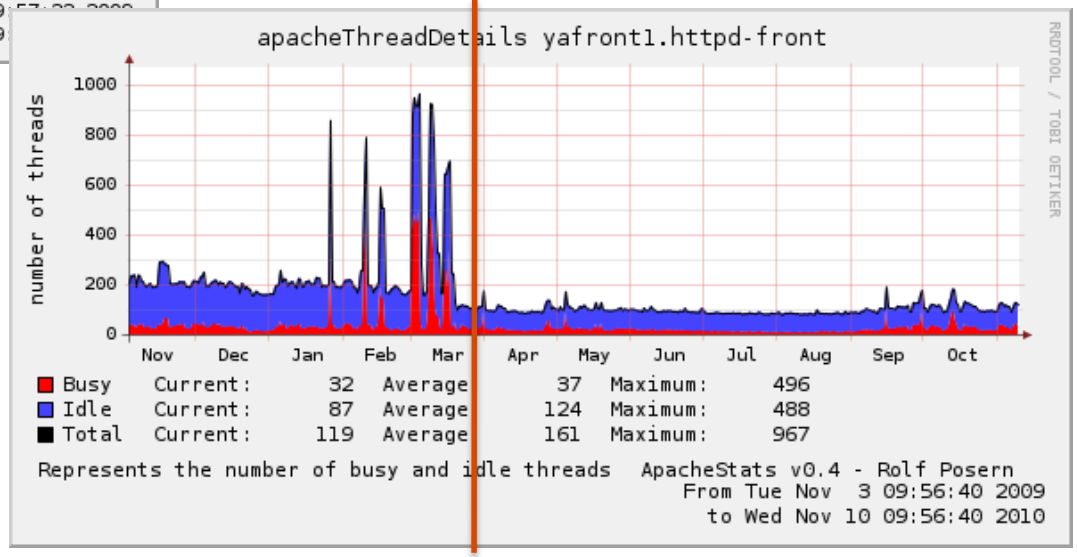
YaCaP : limiteurs HTTP et chronos

- Pertinences des limitations : mise en service 03/2010



Fonction de redirection
→ machines yared*

Fonction frontale : WAYF,login, popup, logout
→ machines yafront*



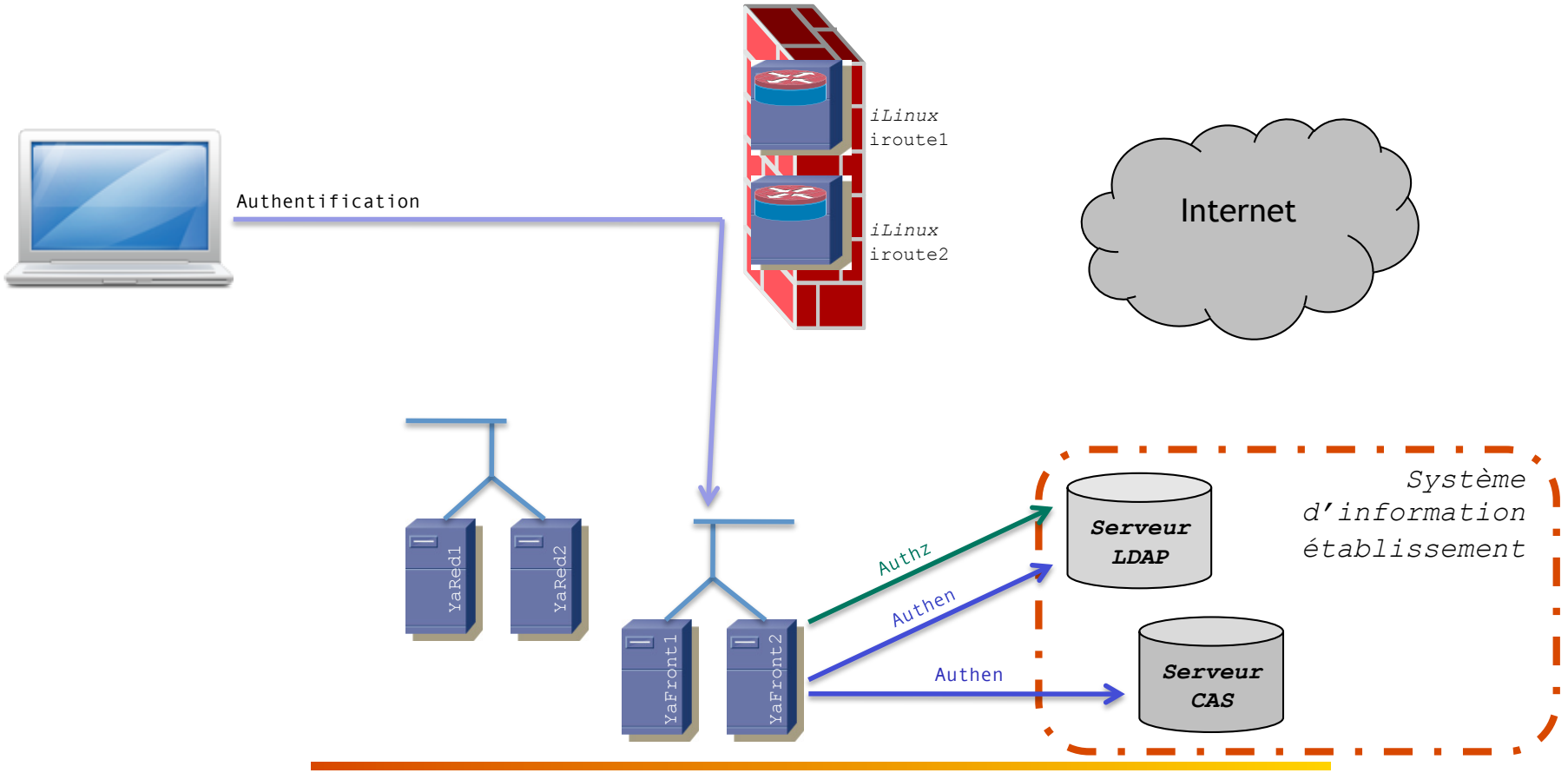
YaCaP : limiteurs HTTP et chronos

- Pertinences des limitations : mise en service 03/2010
  - depuis mars 2010 : plus aucune dégradation notable des fonctions *red* et *front* malgré l'omniprésence des clients bizarres et de l'augmentation des usages

- Autres limitations et améliorations (cf la news) :
  - *http://reseau.ciril.fr/doc/News/News-20100325-0*

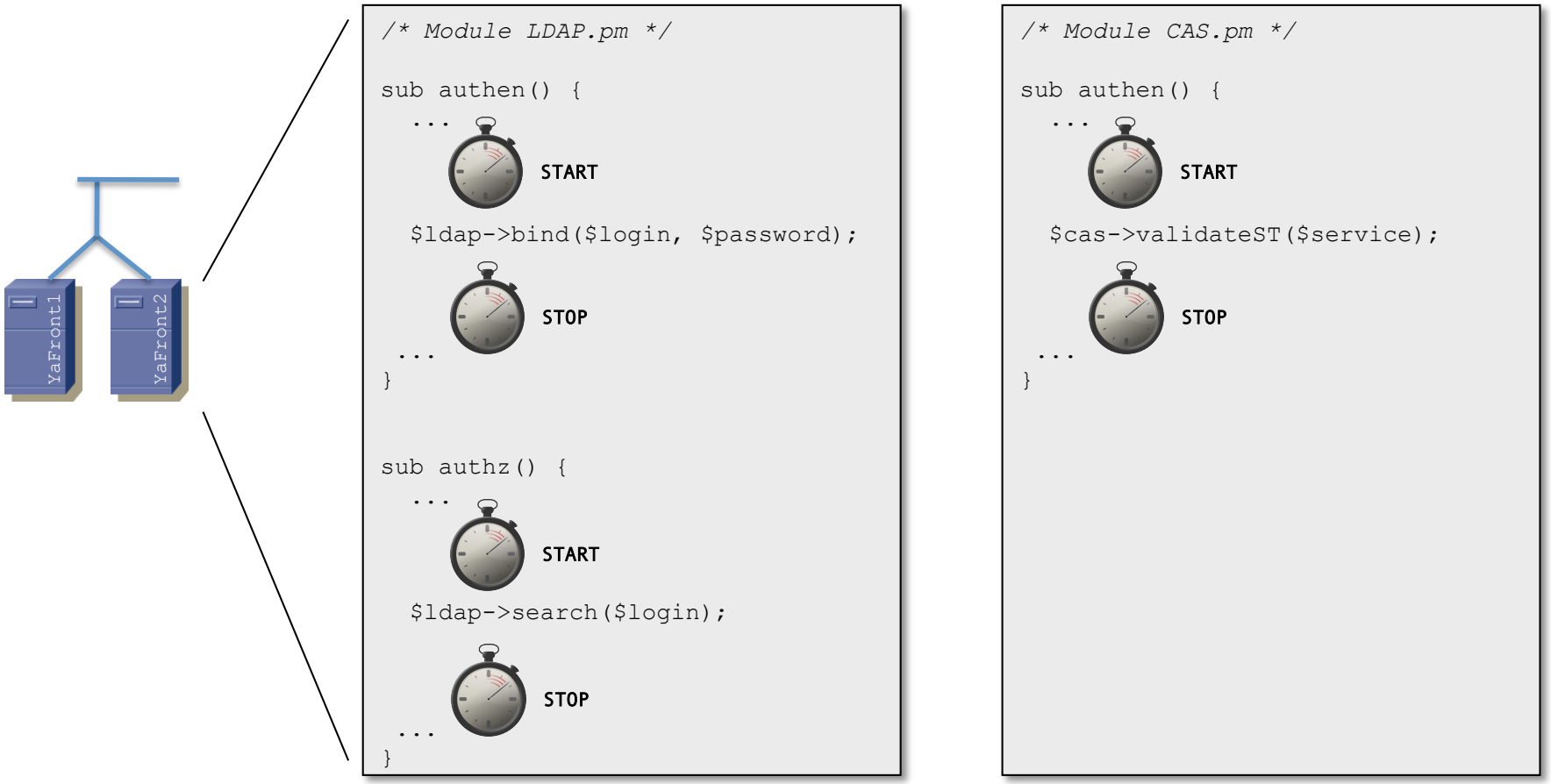
YaCaP : limiteurs HTTP et chronos

- Chronos YaCaP : mesures des performances des SI des établissements



YaCaP : limiteurs HTTP et chronos

- Chronos YaCaP : mesures des performances des SI des établissements

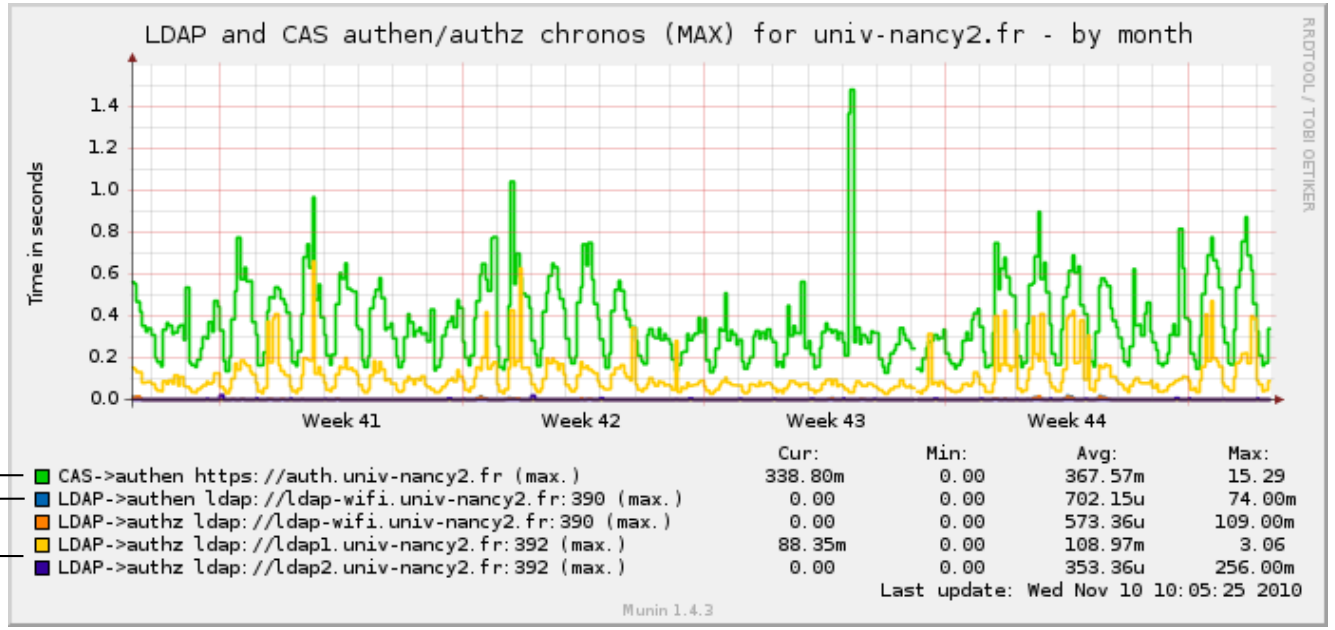


YaCaP : limiteurs HTTP et chronos

- Chronos YaCaP : mesures des performances des SI des établissements
  - temps mesurés par les chronos = temps ressenti par les utilisateurs
  - temps mesurés par les chronos ≠ supervision classique
    - nombre d'échantillons plus important
      - supervision / 5mn = 288 échantillons par jour
      - chronos LDAP Nancy2 = plus de 16000 échantillons par jour
      - chronos CAS Nancy2 = plus de 16000 échantillons par jour
    - métrique testée toujours différente
      - supervision = test sur dn: cn=test, dc=univ-nancy2, dc=fr
      - chronos = test sur toutes les fiches des clients YaCaP

YaCaP : limiteurs HTTP et chronos

- Chronos YaCaP : mesures des performances des SI des établissements



Temps autorisation LDAP

Temps authentification LDAP

Temps authentification CAS

YaCaP : limiteurs HTTP et chronos

- Chronos YaCaP : mesures des performances des SI des établissements
  - informations disponibles en ligne sur l'interface *yacap-administrators* : *https://reseau.ciril.fr/SERVICES/YACAP-ADMINISTRATORS/chronos/*

Lothaire

CRIL

Mise en place d'un service de filtrage d'URLs

Sébastien MOROSI

reseau@ciril.fr

Etat des lieux

- Usages abusifs ou illicites de l'accès à Internet
  - Non respect de la charte informatique des établissements
  - Non respect de la charte déontologique Renater
  - Non respect de la législation
- Traitement des alertes du CERT concernant ces usages
  - Contraignant et consommateur de temps pour les RSSI
  - Risque élevé de voir le nombre de plaintes devenir très important avec l'application d'HADOPI
- Réseaux généralement concernés par les usages abusifs
  - Souvent des postes « non maitrisés » pour les établissements universitaires (portail captif, EDUROAM, réseaux Recherche …)
  - Cités Universitaires pour les CROUS

Doit-on filtrer ?

- Mise en place d'un groupe de travail (rentrée 2009)
  - Universités de Lorraine
  - CROUS de Lorraine
  - CIRIL
- Caractérisation du traffic
  - P2P « has-been » : remplacé par « megaupload & co » : flux HTTP
- Réflexion
  - sur la législation
    - la responsabilité de chacun
    - les droits et devoirs de l'employeur
    - le principe de précaution
  - sur les moyens : les logs et le filtrage des flux HTTP

Doit-on filtrer ?

- Mise en œuvre d'une plate-forme de test au CROUS
  - sur plusieurs Cités-U du CROUS
  - avec produit commercial Olfeo
  - assez peu de plaintes des utilisateurs
  - assez peu intrusif : tous les 'clics' ne sont pas équivalents !
  - réactivité intéressante face à de nouveaux comportements WEB
  - respect de la législation
  - un aspect inattendu : protection des utilisateurs (phishing, propagation de virus , risques de sécurité, publicité …)
- Décision très politique soumise aux quatre présidents
  - Juin 2010 : OUI

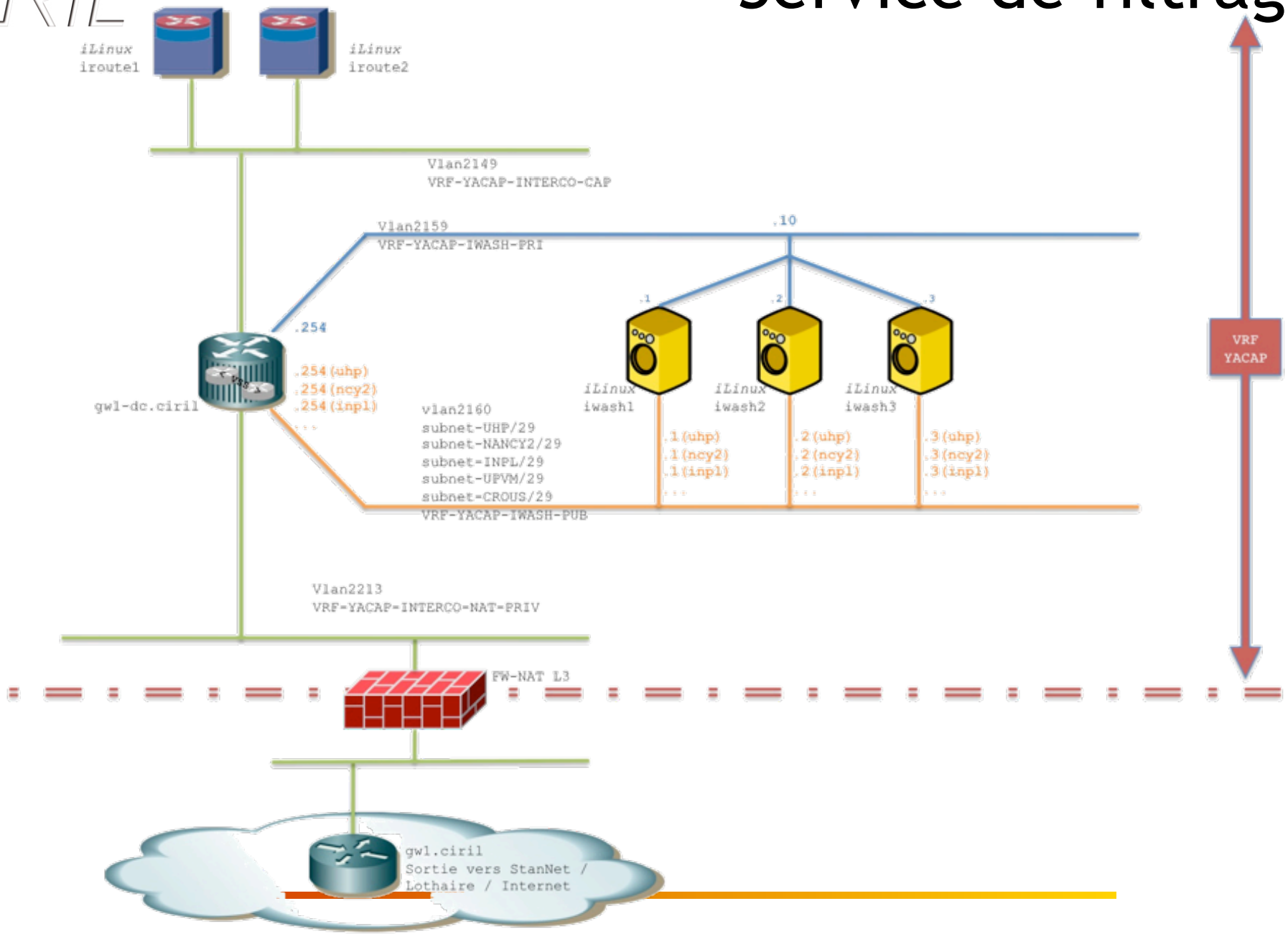
Service de filtrage

- Décision des présidents et du CROUS
  - mise en place d'un service de filtrage des URLs,
  - pour les quatre Universités de Lorraine,
  - pour le CROUS,
  - sur les réseaux « ouverts »
    - portails captifs
    - cités Universitaires
  - extension possible à d'autres réseaux par la suite

Service de filtrage

- Mise en place du service sur les réseaux YaCaP
- Redirection des flux
  - HTTP (port 80)
  - en mode transparent
  - au niveau de l'infrastructure YaCaP
- Plateforme de filtrage
  - mise en œuvre de Proxy : SQUID
  - interrogation d'une base de catégorisation : Olfeo

Service de filtrage



Service de filtrage

- Mise en place d'une politique de filtrage des URLs
  - Politique personnalisée par établissement
  - A déterminer avec chaque établissement
  - Politique commune souhaitable
    - Catégories illicites
    - Risques de sécurité
    - Publicités
    - …
- Ouverture du service prévue fin 2010 / début 2011 sur les réseaux YaCaP
- Extension(s) envisagée(s) par la suite


iWash

StanNet vers un Backbone L3

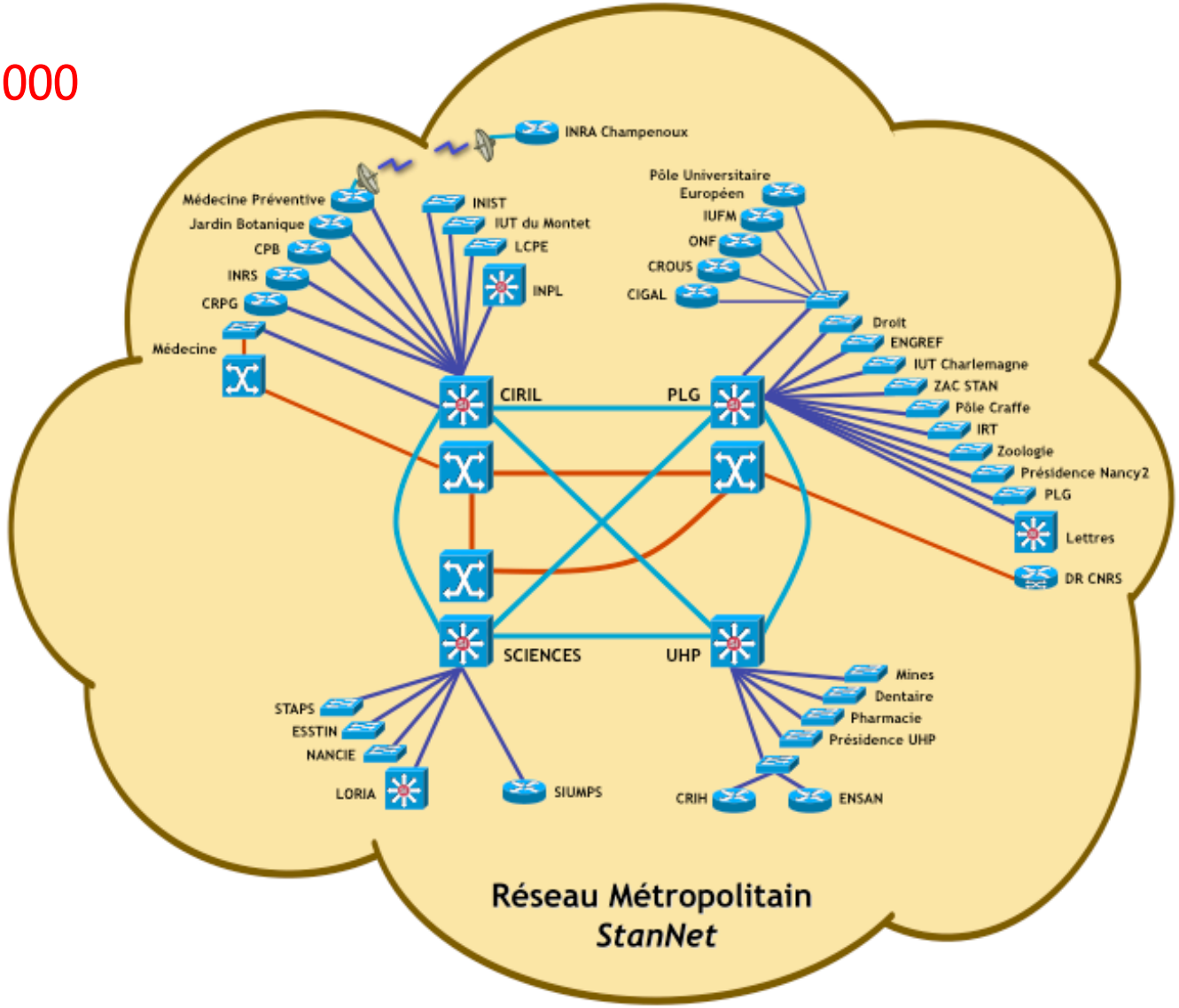
Annonce d'une évolution incontournable

Sébastien MOROSI

reseau@ciril.fr

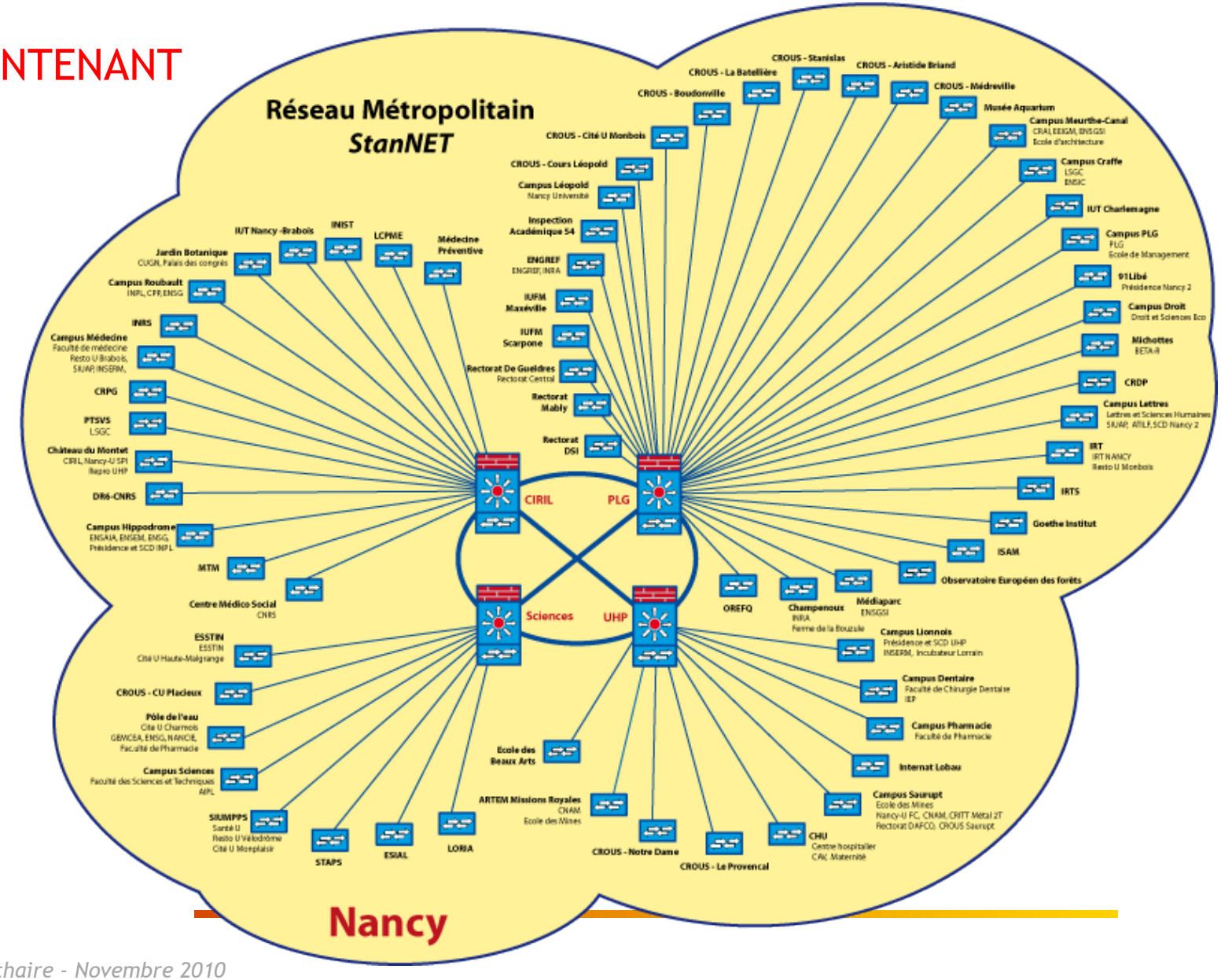
L'histoire …

EN 2000



L'histoire …

MAINTENANT



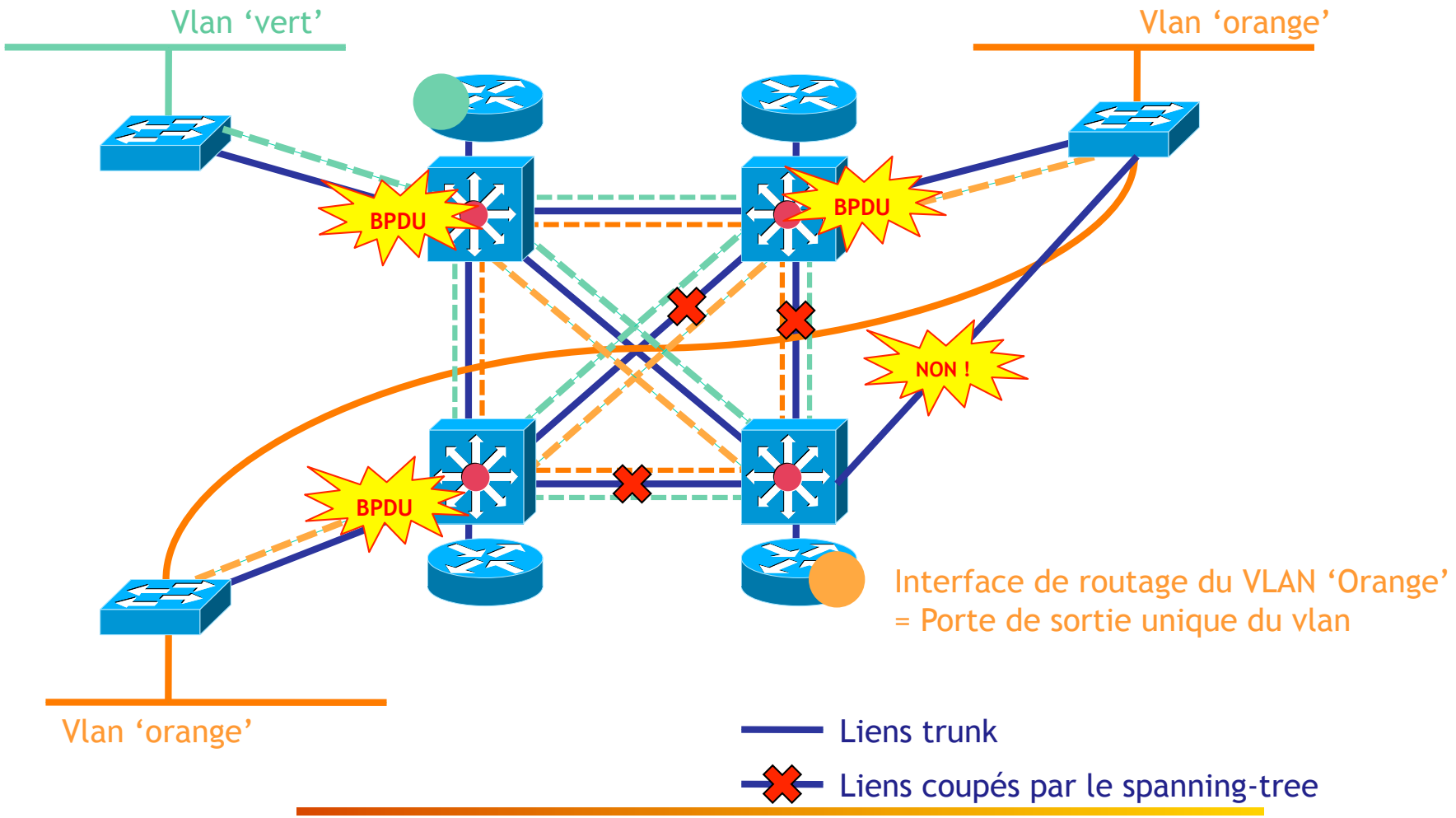
Etat des lieux

- Le changement d'échelle a été progressif
  - Aujourd'hui ~1000 switchs sont gérés par l'équipe réseau
  - Le nombre total de switchs sur StanNet n'est pas connu
- L'architecture n'a pas évoluée
  - StanNet est un réseau commuté/"switché"/de niveau L2
  - Avec un routage réparti sur 4 cœurs de concentration
- La configuration a été adaptée
  - Contraintes liées à la stabilité L2
  - Les limites du spanning-tree sont dépassées depuis longtemps
- L'architecture actuelle est bloquante pour les besoins et évolutions à venir

Backbone L2

- Backbone de niveau 2
  - Liens redondants en mode actif/passif
  - Convergence en cas de panne liée au Spanning Tree
- Domaines de Spanning-Tree isolés par site
  - Filtrage BPDU en entrée du backbone
  - Pour garantir la stabilité du backbone
  - Impossibilité de sécuriser le raccordement d'un site au backbone
- Domaine VTP unique sur le Backbone
  - Numéros de VLANs ont une portée sur tout StanNet
  - Limitation à 1024 (vtp < v3) il y a pénurie
- Transport de VLANs possible

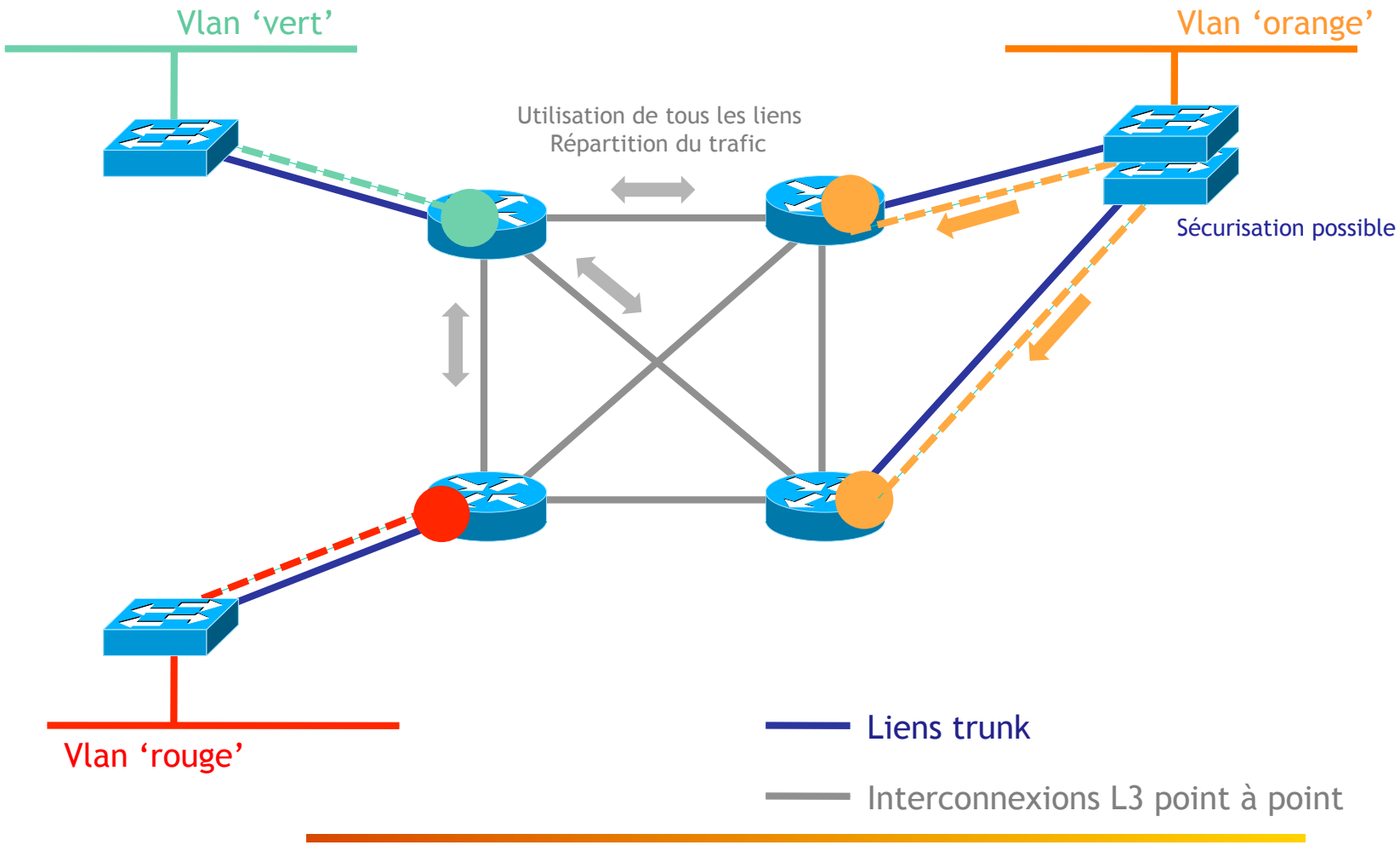
Backbone L2


Vlan ‘vert’
Vlan ‘orange’
BPDU
BPDU
NON !
BPDU
Vlan ‘orange’
Interface de routage du VLAN ‘Orange’
= Porte de sortie unique du vlan
Liens trunk
Liens coupés par le spanning-tree

Migration vers L3

- Migration vers un backbone de niveau 3
  - pour permettre la sécurisation
  - pour limiter les domaines de broadcast
  - pour améliorer la stabilité du backbone
  - pour améliorer la convergence en cas de panne
  - pour disposer de liaisons redondantes en mode actif/actif
- Sécurisation d'une site possible à plusieurs niveaux
  - L1 : double adduction fibre
  - L2 : connexion sur des points différents du backbone et sécurisation des switchs d'entrée de site
  - L3 : redondance de routage

Migration


Vlan ‘vert’
Vlan ‘orange’
Utilisation de tous les liens
Répartition du trafic
Sécurisation possible
Vlan ‘rouge’
Liens trunk
Interconnexions L3 point à point

La migration en étapes

- Eliminer les VLANs transversaux
  - les problématiques ont évoluées
  - des alternatives sont disponibles
- Passer au Backbone L3
- Initier les projets de sécurisation

VRFs

Vincent DELOVE

reseau@ciril.fr

VRFs

- StanNet → infrastructure routée
  - évolutivité, disponibilité, sécurité
  - une seule infrastructure mutualisée pour tous les réseaux

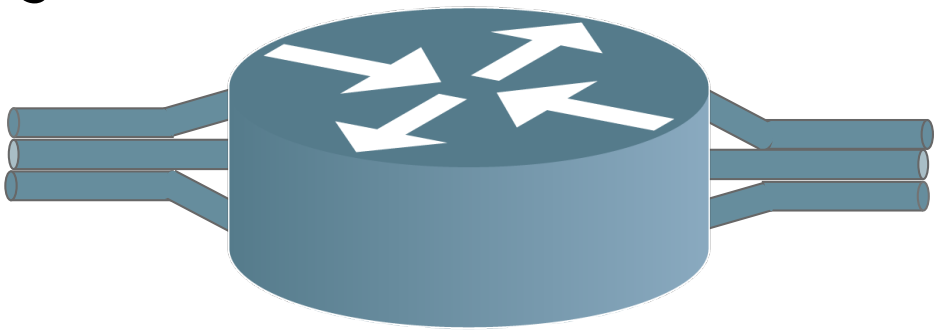
  → besoin de segmentation / virtualisation

- Virtualisation réseau
  - VLAN : Virtual Local Area Network (niveau 2)
  - VPN : Virtual Private Network
  - Firewall : contextualisation

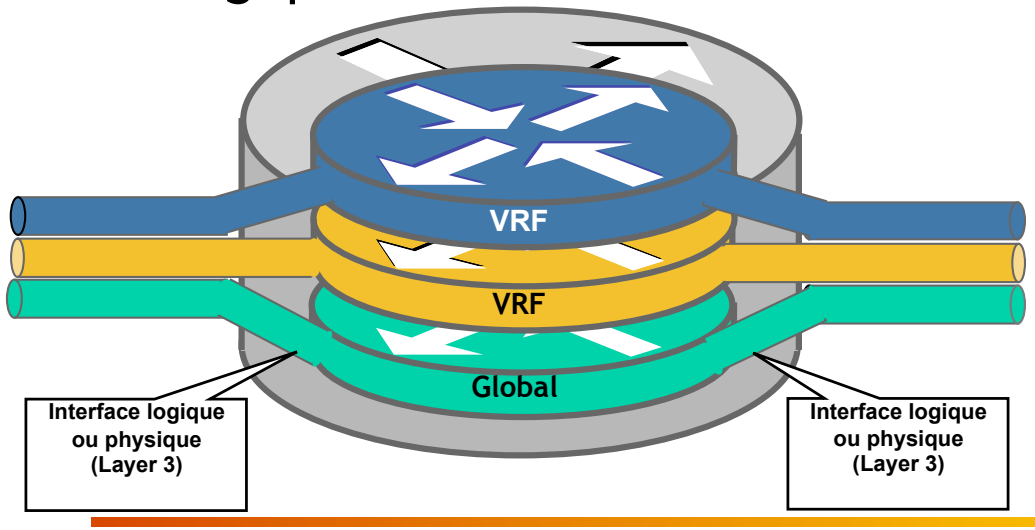
- VRF : Virtual Routing and Forwarding
  - service de virtualisation d'un routeur (niveau 3)

VRFs

- Sans VRF :
  - routage direct entre les réseaux

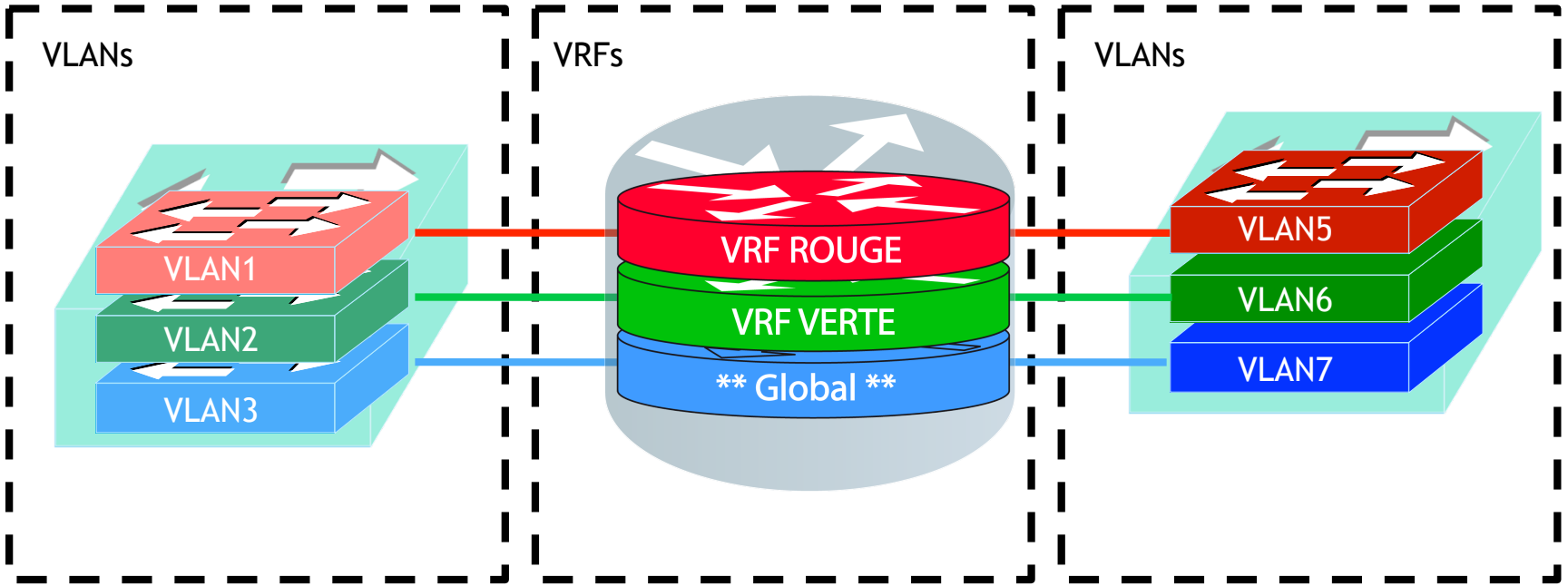


- VRF :
  - séparation logique des réseaux sur un même routeur.



VRFs

- VRFs et VLANs
  - association des VLANs dans les VRFs
  - virtualisation de l'infrastructure (niveau 2 et 3)



VRFs

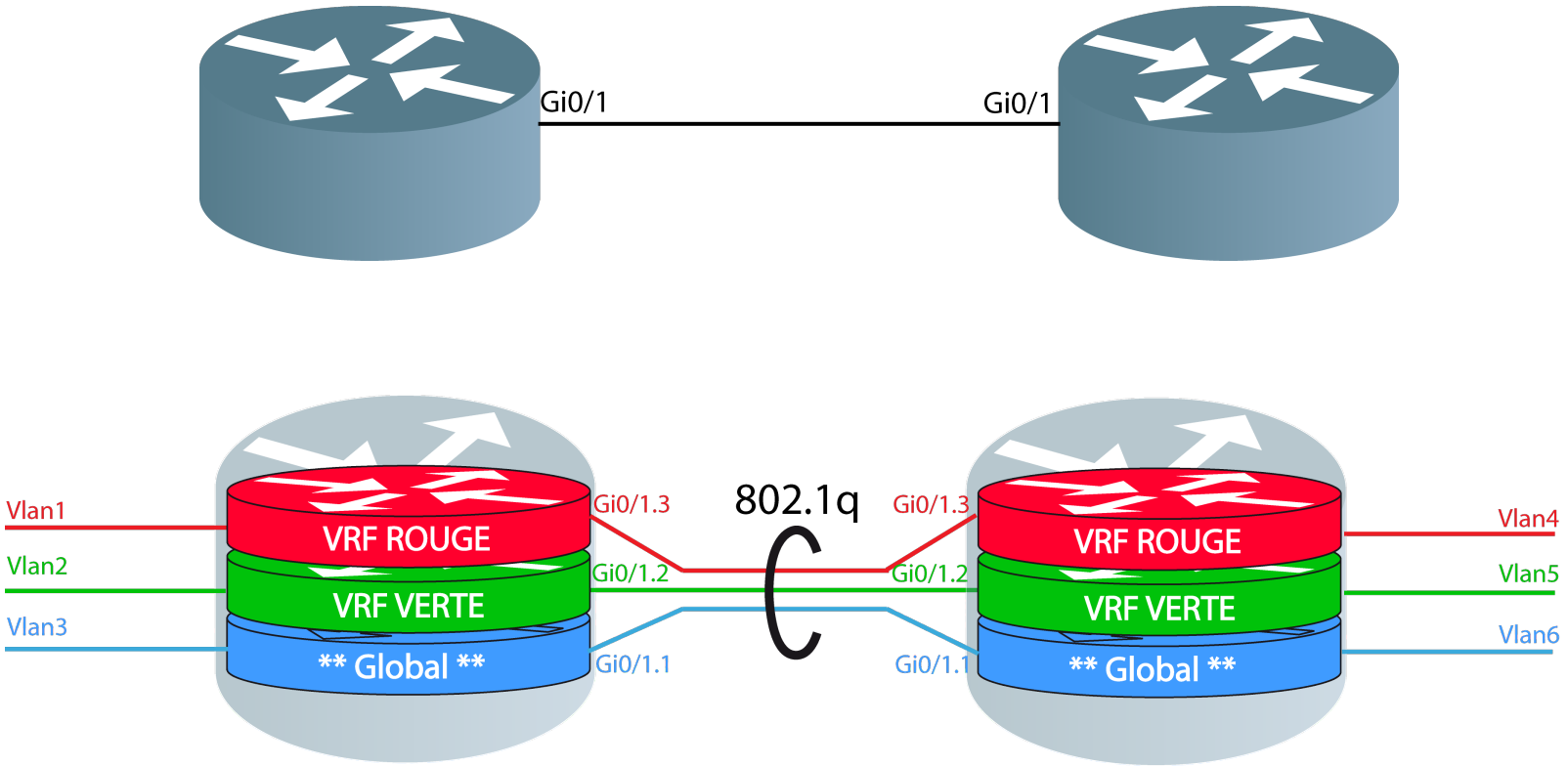
- Ce qui ne change pas avec les VRFs
  - L'administration des équipements
    - Pas de changement de fond
      - VRF-Lite : VRF sans MPLS
    - modifications locales au routeur
      - pas d'échanges concernant les VRFs
      - nécessité d'une cohérence dans le transport des VRFs
    - administration d'un seul équipement virtualisé
  - La gestion des réseaux
    - gestion des vlans (SW)
    - gestion des ACLs (CONFIN)
    - gestion des firewalls

VRFs

- Ce qui change avec les VRFs
  - isolation totale entre les réseaux de différentes VRFs
    - plus de communication directe
  - une interface de routage est associée à une seule VRF
  - une table de routage par VRF
    - possibilité de recouvrement des adressages
    - un processus de routage par VRF
    - multiplication des domaines de routage

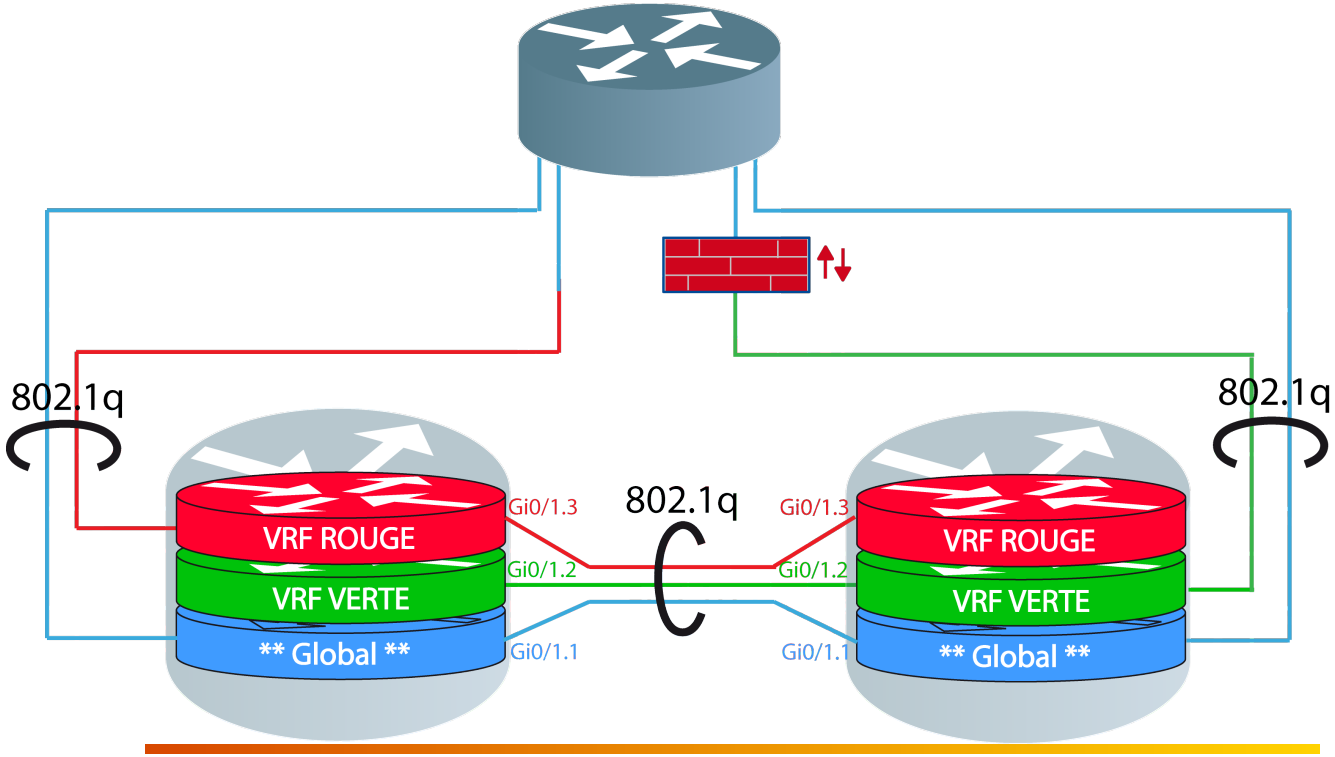
VRFs

- Ce qui change avec les VRFs
  - interconnexion des routeurs



VRFs

- Communication inter-VRF
  - passage à un autre domaine de routage
  - utilisation d'un firewall pour contrôler le trafic
  - possibilité de différencier les topologies



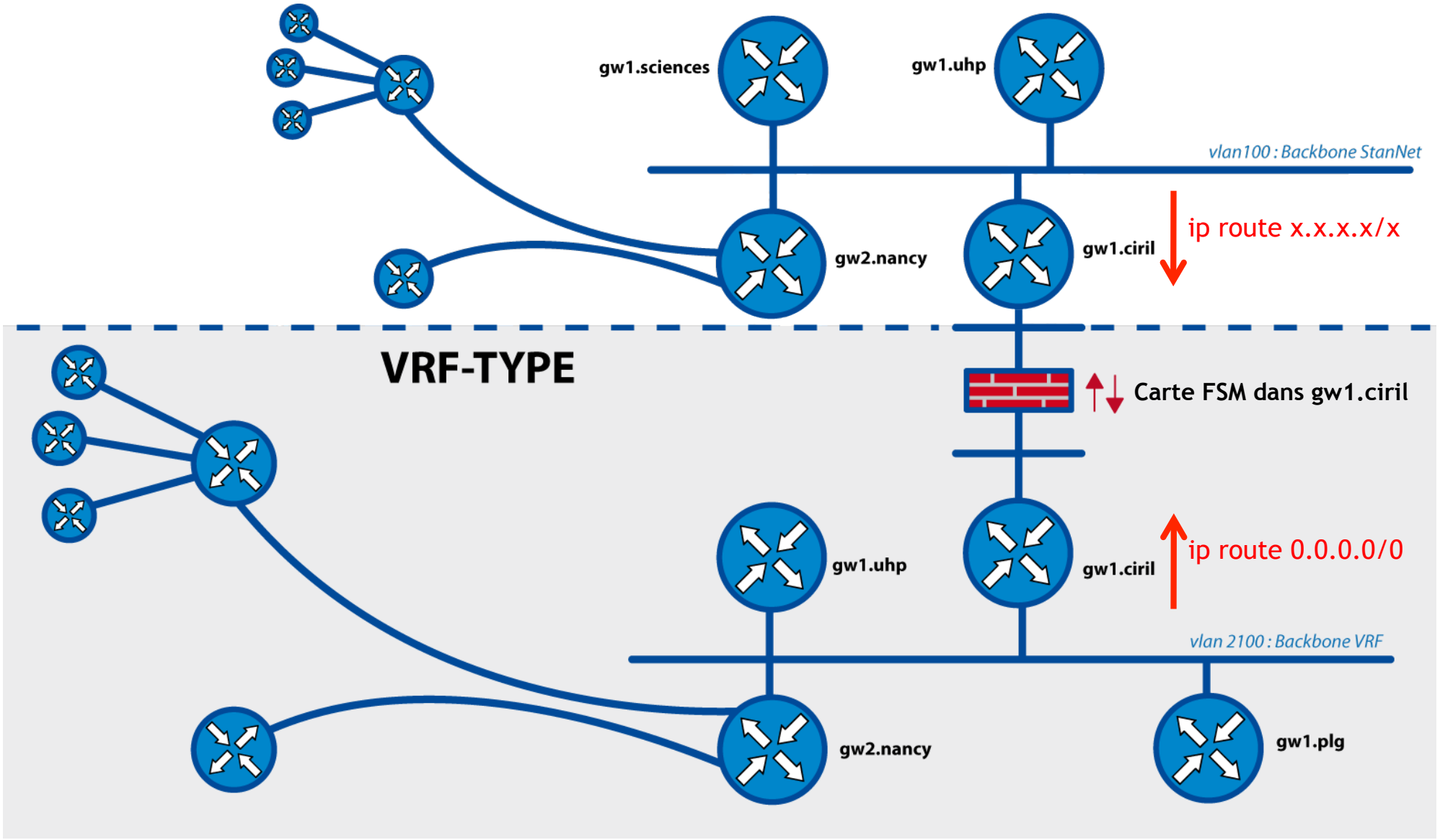
VRFs

- Pourquoi virtualiser le L3 sur Lothaire ?
  - Eviter le transport de niveau 2
  - Simplifier des architectures complexes
    - NAT
    - YaCaP
  - Eliminer des points de congestion et de faiblesse
    - CPU des routeurs NAT
    - tirer profit des mécanismes avancés du L3
  - Proposer des nouveaux services
    - Sécurisation
    - Transports de réseaux privés sur Lothaire

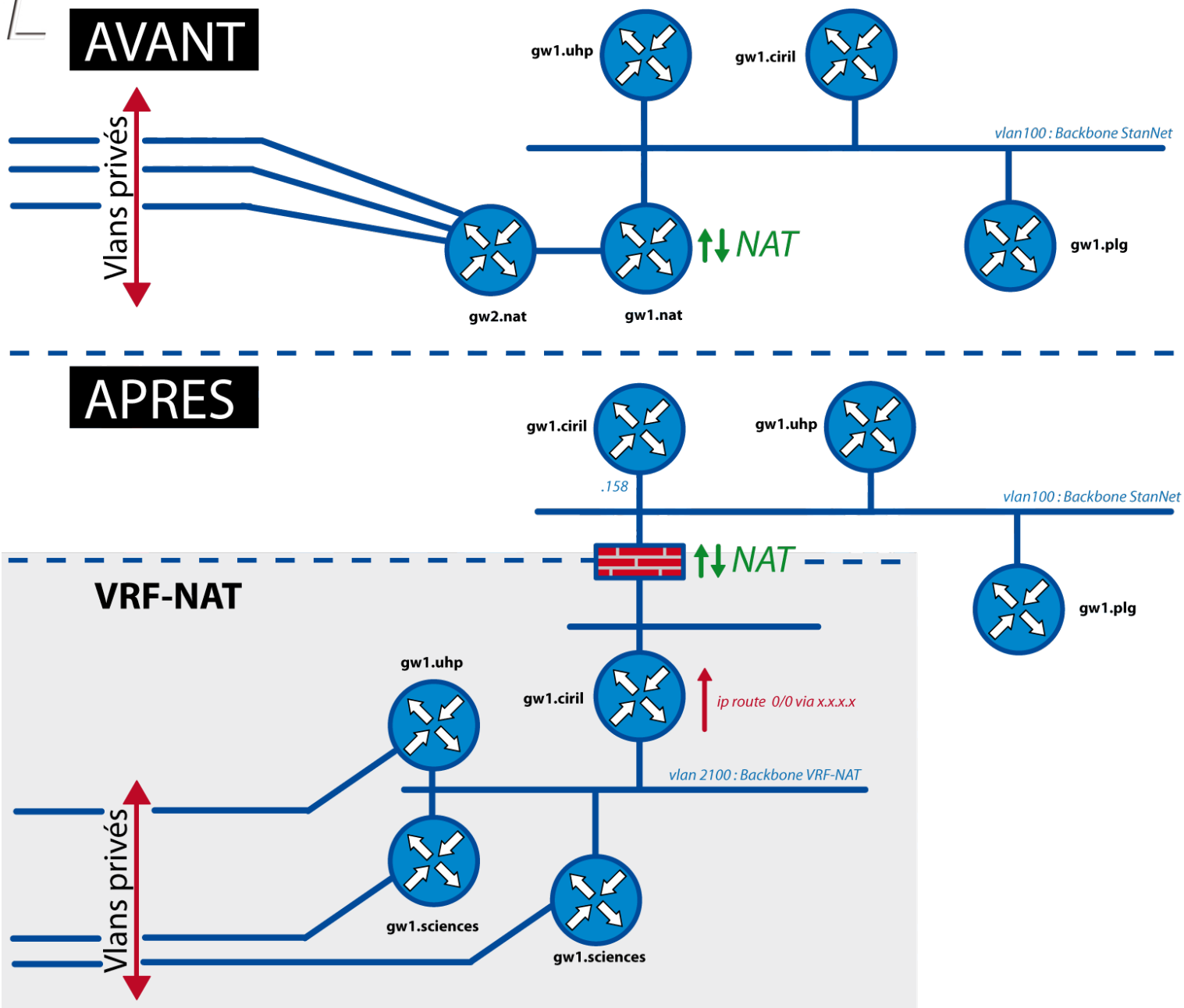
VRFs

- Les VRFs sur Lothaire
  - Avant :
    - Transport de VLANs
    - Tunnel GRE
    - Policy Based Routing
  - première VRF en septembre 2008
    - difficulté de transports sur certains sites
  - possibilité de transport sur l'ensemble des routeurs
    - adaptation des liaisons
  - aujourd'hui en quelques chiffres :
    - 10 VRFs
    - 24 routeurs / 34 au total
    - 317 interfaces de routage

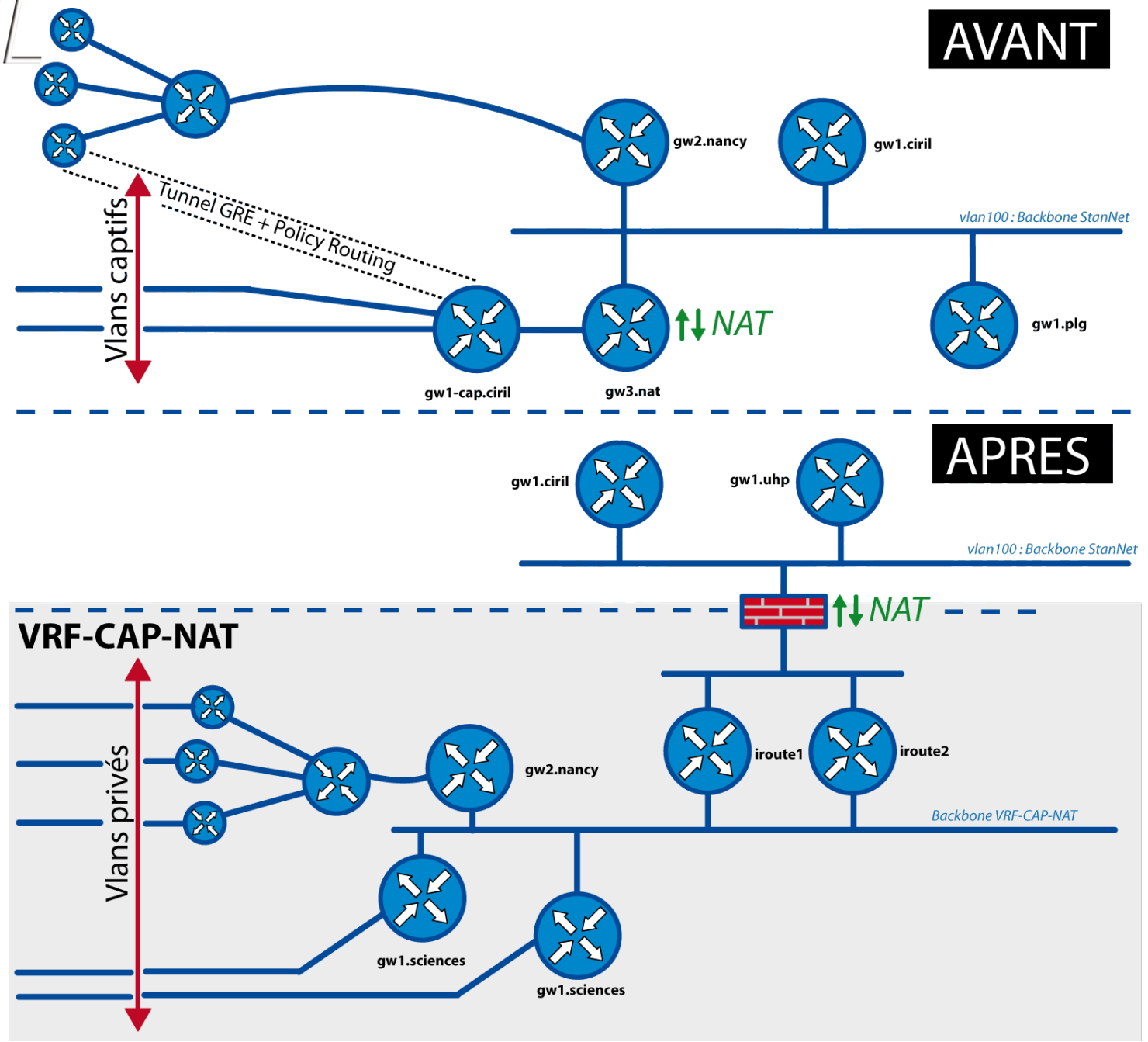
VRFs


gw1.sciences
gw1.uhp
vlan100 : Backbone StanNet
gw2.nancy
gw1.ciril
ip route x.x.x.x/x
VRF-TYPE
Carte FSM dans gw1.ciril
gw1.uhp
gw1.ciril
ip route 0.0.0.0/0
vlan 2100 : Backbone VRF
gw2.nancy
gw1.plg

VRFs


AVANT
Vlans privés
gw1.uhp
gw1.ciril
vlan100 : Backbone StanNet
gw1.plg
NAT
gw2.nat
gw1.nat
APRES
gw1.ciril
gw1.uhp
.158
vlan100 : Backbone StanNet
NAT
gw1.plg
VRF-NAT
gw1.uhp
gw1.ciril
ip route 0/0 via x.x.x.x
vlan 2100 : Backbone VRF-NAT
Vlans privés
gw1.sciences
gw1.sciences

VRFs


AVANT
gw2.nancy
gw1.ciril
vlan100 : Backbone StanNet
Tunnel GRE + Policy Routing
Vlans captifs
NAT
gw1.plg
gw1-cap.ciril
gw3.nat
APRES
gw1.ciril
gw1.uhp
vlan100 : Backbone StanNet
NAT
VRF-CAP-NAT
Vlans privés
gw2.nancy
iroute1
iroute2
Backbone VRF-CAP-NAT
gw1.sciences
gw1.sciences

Système d'information : le point

Vincent DELOVE

reseau@ciril.fr

SI : le point

- 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
  - Base « noip » (l'adressage Lothaire)
    - description de tous les préfixes
    - 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 »

SI : le point

- Pourquoi faire évoluer le système d'information ?
  - pour plus de souplesse
    - gestion de groupes
    - délégation des droits
  - pour centraliser l'information
    - ajout d'information manquante
  - pour plus de cohérence
    - fusionner les bases → pas d'information dupliquée
  - pour suivre les évolutions du réseau
    - VRFs, réseaux non-routés, IPv6, …
    - Principe : « la vérité est sur le réseau »
  - pour permettre le développement de nouveaux services

SI : le point

- Evolution du SI
  - l'année dernière nous disions : « le projet est toujours en cours… »
  - … et le projet est (~~*toujours en cours*~~) se termine !
  - la première phase de développement est terminée :
    - évolution de la base « servuser » (30/04/2010)

      http://reseau.ciril.fr/doc/News/News-20100430-0
      - système de gestion des autorisations plus performants
  - la nouvelle base institutionnelle est prête
  - la nouvelle base des noip est en cours de développement
    - nécessité de la relier à la base institutionnelle

  - Dernière étape : mise à disposition d'une vue sur le SI

Au programme

- Introduction
- Evolution du réseau Lothaire
- Evolutions des services réseaux
- Salle d'Hébergement
- Quelques petits rappels
- Questions - Réponses

Pot

Les salles d'hébergement du CIRIL

Olivier LACROIX

reseau@ciril.fr

Les travaux réalisés

- En 2009 :
  - Création d'une nouvelle salle
  - Nouveau TGBT
  - Remplacement des alimentations électriques en faux-plancher par des canalis
  - Groupe électrogène plus puissant (passage de 165 à 550 KVA)
  - Onduleur modulaire plus puissant (passage de 3x30 KVA à 4x50 KVA, évolutif à 5x50 KVA)
  - Nouvelle climatisation redondante
  - Nouveaux panneaux de brassage plus souples
  - Chemin aérien pour les fibres

Les travaux réalisés

Le nouveau panneau de brassage

Les travaux réalisés

Les canalis

Les travaux réalisés

Le groupe électrogène de 550 KVA et sa cuve de 4000 l

Les travaux réalisés

- En 2010 :
  - Pour la nouvelle salle, création d'une entrée spécifique avec un sas

Les conditions d'hébergement

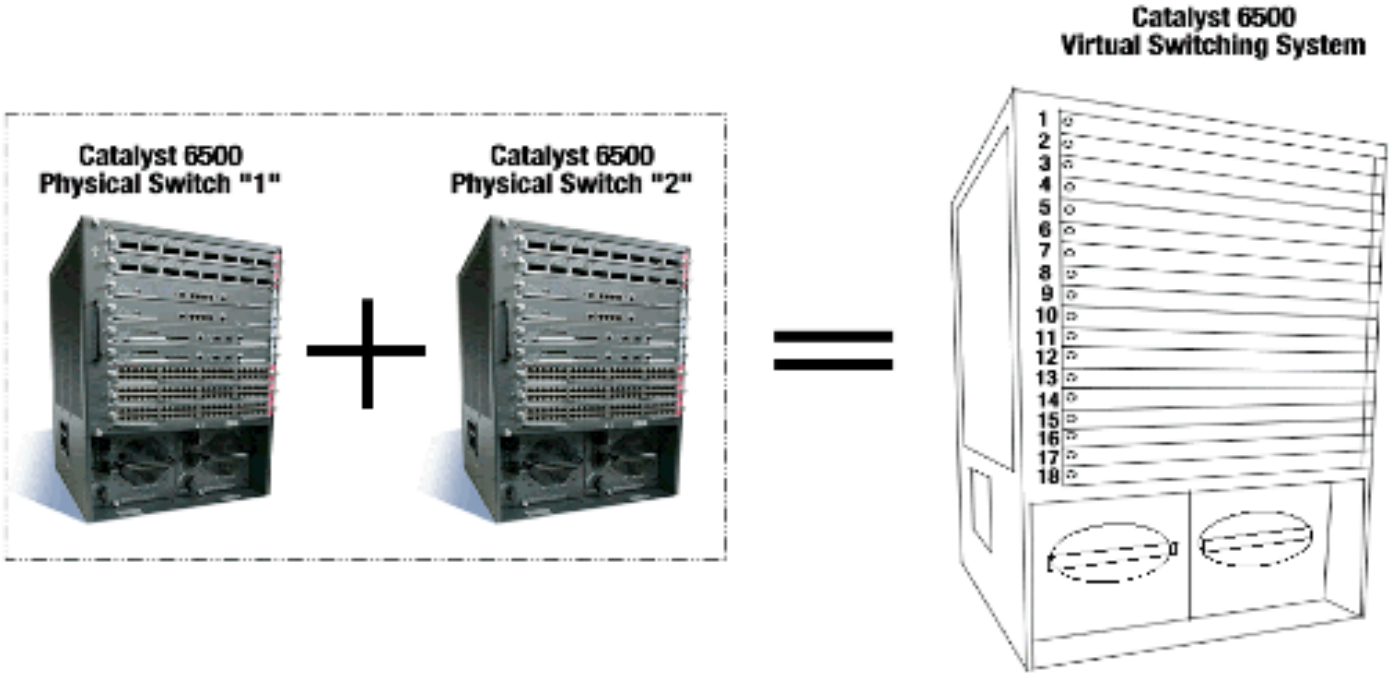
- 2 salles d'hébergement :
  - Pour chaque armoire :
    - Double alimentation électrique, ondulée et EDF, 16 ou 32 A
    - Par défaut, 48 ports cuivre RJ45 catégorie 6 ou 6A
  - Climatisation redondante
  - Alimentation ondulée et climatisation soutenues par un groupe électrogène de 550 KVA
  - Système de détection d'incendie et d'extinction automatique par gaz inerte (argonite ou argo55)
  - Contrôle d'accès par badge nominatif
  - Chemin pour fibre passant au dessus de toutes les armoires et entre les 2 salles

Les conditions d'hébergement

- Particularités des armoires de la nouvelle salle
  - Armoires 800x1000 au lieu des armoires 600x1000 de l'ancienne salle
- Moins d'armoires, mais :
  - 45 U au lieu de 42
  - Passage de 10 cm de chaque coté des rails pour les alimentations et les câbles
    - Gain de place et de souplesse

Les conditions d'hébergement

- Dans chaque salle, 2 commutateurs-routeurs combinés en VSS (Virtual Switching System) :
  - 1 seul gros commutateur-routeur virtuel



Les conditions d'hébergement

- Les avantages de VSS
  - Les cartes de supervision sont redondantes entre elles (une active et une en standby)
  - Une seule table d'adresses MAC et de routage pour les deux châssis
  - En cas de « perte » d'un châssis, bascule sur l'autre en 200 ms
- Les châssis d'une salle sont reliés entre eux par 2 liens 10 GBPS
- Les châssis entre les salles sont reliés par 2 liens 10 GBPS

Recommandations sur les matériels

- Seuls des matériels « rackables » sont acceptés

- Pour bénéficier de la sécurisation, tout équipement hébergé au CIRIL doit :
  - Avoir une double alimentation (une branchée sur le courant ondulée, l'autre sur EDF)
  - Avoir 2 cartes réseaux configurées en « bounding » (chaque carte sera branchée sur un commutateur-routeur différent)

➔ Seule cette double sécurisation garantie un maximum de disponibilité

Qui peut être hébergé ?

- En théorie, toute machine d'un établissement du réseau Lothaire

- En pratique, tout demandeur doit obtenir au préalable l'accord des instances dirigeantes de son établissement et la validation par le CIRIL

Les conditions financières

- Le service d'hébergement ne peut plus être gratuit
  - Le coût de fonctionnement des salles est important (électricité, maintenances, etc.)
  - Le CIRIL a vu ses subventions de fonctionnement se réduire fortement depuis 2008

Les conditions financières

- Afin d'équilibrer le budget de fonctionnement du CIRIL, le Conseil du CIRIL a validé le 7 avril 2010 les tarifs d'hébergement suivants :

	Montant HT
Frais d'installation	
Frais d'installation pour une armoire complète	**270,00 €**
Frais d'installation d'une alimentation électrique supplémentaire	**1 000,00 €**
Frais d'installation d'une rocade cuivre 12 ports	**540,00 €**
Frais d'installation d'une rocade cuivre 24 ports	**770,00 €**
Redevances d'hébergement	
Montant annuel pour une armoire complète de type "classique"	**5 700,00 €**
Montant annuel pour une armoire complète de type "data center"	**11 400,00 €**
Montant annuel pour un "U" dans une armoire de type "classique"	**220,00 €**
Montant annuel pour un "U" dans une armoire de type "data center"	**440,00 €**
Services à la demande	
Frais d'intervention pour une installation d'équipements par demi-journée	**270,00 €**

Les conditions financières

- Les nouveaux établissements hébergés sont facturés dès leur installation dans une salle

- A partir du 1er janvier 2011, tous les hébergements actuels seront facturés
  - Conventions d'hébergement en cours de rédaction
  - Un ticket « modérateur » sera appliqué à chacune des 4 universités de Lorraine

Au programme

- Introduction
- Evolution du réseau Lothaire
- Evolutions des services réseaux
- Salle d'Hébergement
- Quelques petits rappels
- Questions - Réponses

Pot

Quelques petits rappels

Olivier LACROIX

reseau@ciril.fr

Rappels

- Le portail *http(s)://reseau.ciril.fr*
  - missions et activités du service
  - documentation des infrastructures et des services proposés
  - statistiques
  - accès rapide aux outils

Merci de maintenir et renseigner vos profils utilisateurs

Email, n° de téléphone, GSM, …

https://reseau.ciril.fr/my-profile

Rappels

- Système de « News » et flux RSS
  - « News » directement via le portail
    - depuis la dernière grand'messe : 39 news publiées

    http(s)://reseau.ciril.fr/doc/News/News
  - un flux RSS pour le suivi des News

    http://reseau.ciril.fr/feeds/news/rss
  - un flux RSS pour le suivi des changement sur le site

    http://reseau.ciril.fr/feeds/portail/rss

- Liste de diffusion : *tickets@ciril.fr*
  - Connaissance des incidents ou des interventions sur le réseau Lothaire
  - Procédure d'abonnement décrit dans « Supervision -> Incidents »

    http://reseau.ciril.fr/doc/Services/Tickets
  - Depuis la dernière grand'messe : 171 tickets émis

Rappels

- Comment nous contacter et quand
  - par mail uniquement à l'adresse : *reseau@ciril.fr*
  - par téléphone : 03.83.68.24.24
  - permanence du lundi au vendredi : de 8h00 à 18h00

- IPv6
  - Routage généralisé sur toute la plaque Lothaire
  - Actuellement 71 réseaux routés (dont 85% d'interconnexion)
  - Possibilité de double adressage IPv4, IPv6

Au programme

- Introduction
- Evolution du réseau Lothaire
- Evolutions des services réseaux
- Salle d'Hébergement
- Quelques petits rappels
- Questions - Réponses

Pot

Conclusion
Questions - Réponses

Benoit de la FILOLIE

reseau@ciril.fr

Conclusion – Questions - Réponses

- Demi-journée dense : tous les sujets prévus n'ont pu être traités
  - Service H323 / Gatekeeper H323
    http://reseau.ciril.fr/doc/Services/H323
  - Salle de formation
    http://reseau.ciril.fr/doc/Services/SalleDeFormation

- A venir (demain) le « traditionnel » questionnaire de satisfaction sur cette demi-journée

- Questions – Réponses …


Lothaire