

A un clic de la  
~~catastrophe~~

migration vers  
l'IPv6 ?

Alexis MICHON – Café Aramis – 02/06/2016

---

- Contexte
- Démarche
  - Migration du réseau
  - Qu'en est-il des services ?
- Vous avez dit problèmes ?
- Statistiques

# Plan

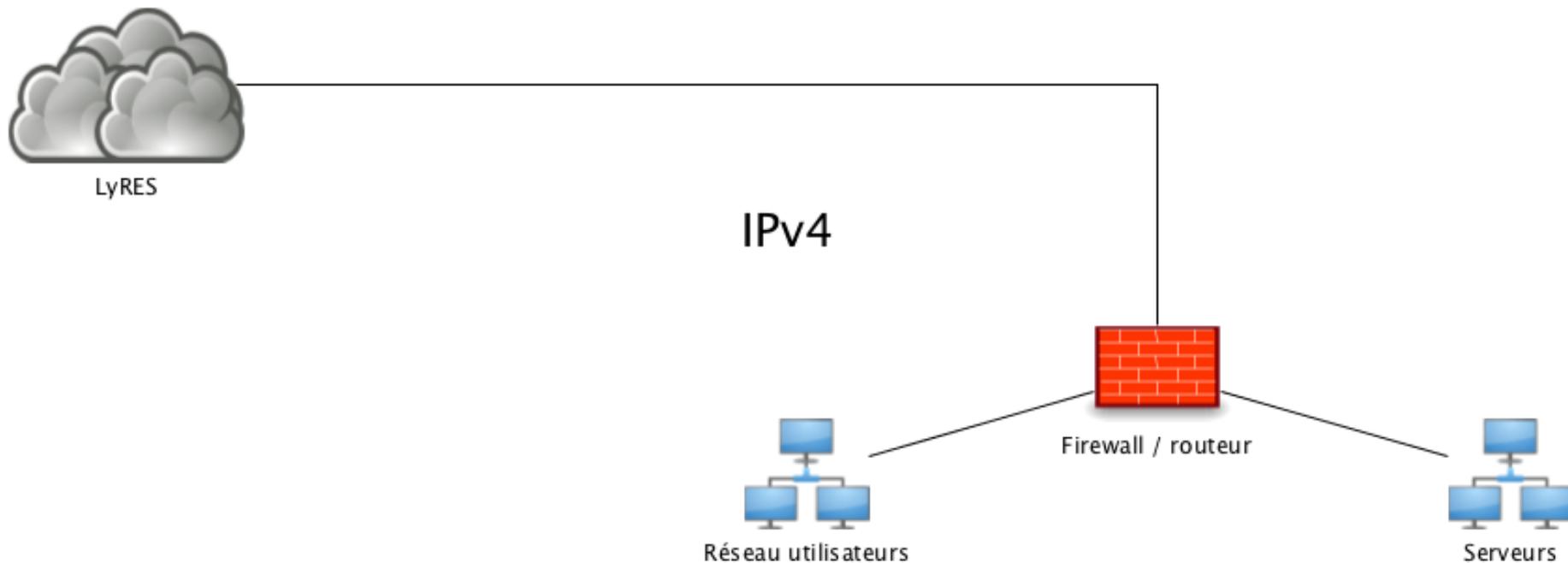
---

## IBCP : Institut CNRS, hors campus

- ~ 230 personnes et autant de postes info
- ~50<sup>ème</sup> d'instruments pilotés
- ~ 70 serveurs
- 3 réseaux wifi (Eduroam, Invites, Interne)
- 2 clusters de calcul
- 1 salle de formation
- Peering direct avec LyRES

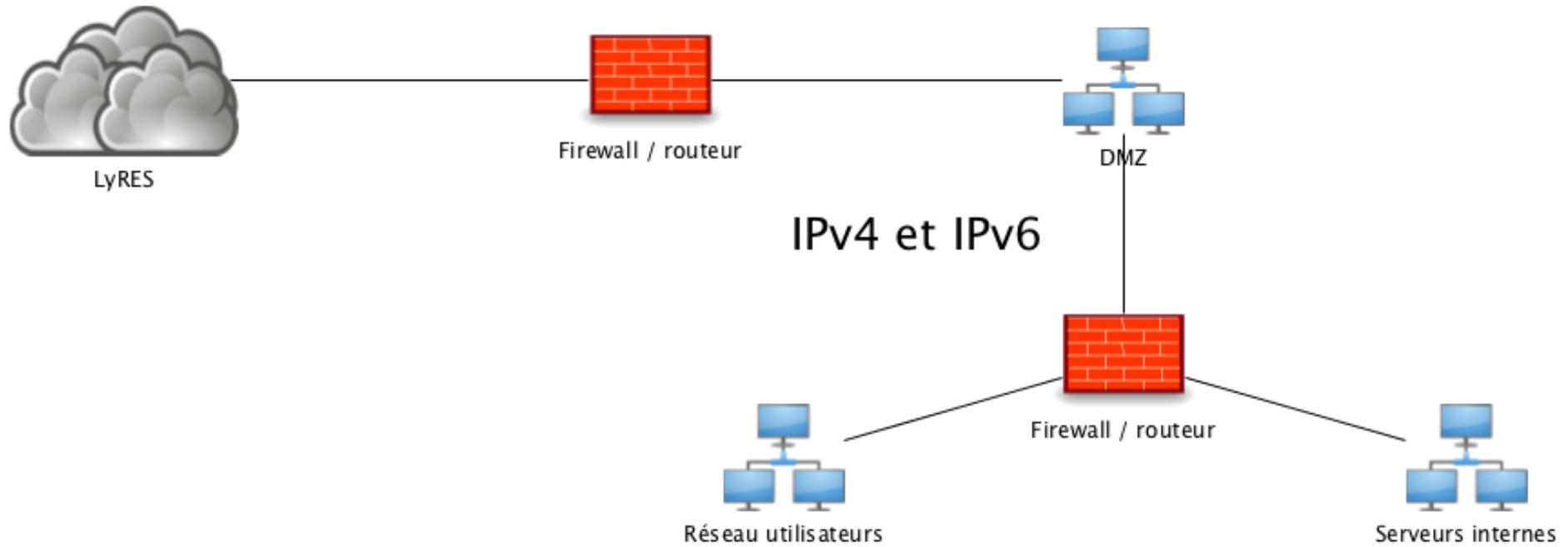
# Contexte





# Contexte (avant)

---



# Contexte (but)

---

- 2013 : 1<sup>ier</sup> tentative de réseau IPv6
  - => pourquoi ?
    - Création d'une DMZ donc pourquoi pas
    - Prometteur en terme de service : Mobilité/sécurité/... : MENSONGE
    - Buzz word sur les CVs, Forums et page FB.  
=> C'était à la mode plus que tout.
  - => Renater fournit un /48
  - => Fail
- Causes
  - Manque de formation
  - Plusieurs erreurs :
    - Découpage réseau (CIDR)
    - Appréhension du raccordement en IPv6 à Internet : Sécurité ?  
=> Partir du service pour remonter aux réseaux.

## 2013 – 2015 : IPv6 first

---

- Formation du GIP renater, d'autres le font ! OUFF
- Pourquoi retenter l'aventure ?
  - C'est un protocole actuel.
  - Persuadé qu'on ne peut s'en passer.
  - Apprendre à l'utiliser en prenant le temps, plutôt qu'en urgence.
- Renater : /48
- Peering avec Lyres, demander à SPIE
  - S'assurer du fonctionnement des équipements (\*)
  - Annoncer /48
  - Fermer l'IPv6 sur le FW
  - => Waouhouhou : on a l'IPv6 (bcp sont dans cette situation)

2015 – 2016 : IPv6 second

---

Toutes les ips sont publiques : Attention !

Comment avons nous procéder ?

- Ajout de l'IPv6 statique sur des serveurs en DMZ
- Reconfiguration des firewalls serveurs pour l'IPv6 :
  - => Ouverture du ping uniquement
  - => En interne : machine joignable en IPv6

2015 – 2016 : IPv6 second en vrai

---



Cela permet de communiquer



Aucun Service

---

- Pré-requis pour qu'un service réponde en IPv6 ?
  - Enregistrement AAAA
  - Service en écoute sur l'IPv6
  - Suivant logiciel, de la configuration
  
- DNS
- Serveur web
- Serveur mail

2015 – 2016 : IPv6 second (3)

---

- DNS : pas obligatoire, très fortement conseillé.
- Très simple
  - Ajout du service en écoute sur l'IPv6
  - Ajout du AAAA
- Test à l'aide d'un autre serveur en DMZ
- Renater : Mise à jour des zones
- Ouverture du FW de site
  - => Premier traffic IPv6

2015 – 2016 : IPv6 second (4)

---

- Serveur web
  - AAAA et socket v6 en écoute
    - Apache : serveur et vhost
  - Attention au code maison
    - Méfiance : Serveur tomcat executant du JAVA
- Serveur mail & serveur ssh
  - Fail2ban : incompatible

2015 – 2016 : IPv6 second (4)

---

- Serveurs Ldap : simple
  - => acl : problème de permission
- Service non migré IPv6
  - Serveur base de données : Très simple, manque de temps.
  - Serveur VPN : Nécessite 3 ou 4 jours de travail.
  - Serveur voixip (asterisk + xivo), géré par Avencall.
  - Pont de visioconférence : Frileux, peu/pas de client.

2015 – 2016 : IPv6 second (5)

---

- Deux POCs :
  - Salle de TP : 17 postes double pile
    - DHCP static.
  - Wifi eduroam
    - Double pile
    - DHCP libre
- Postes de l'institut
  - 2 postes configurés en statique

Et les clients dans tout ca ?

---

Aujourd'hui les postes des utilisateurs ont des droits d'accès aux réseaux différents (VPN/SSH) et par simplicité nous sommes partie sur le postulat :

une IPv4 = une adresse mac = un ordinateur = un utilisateur

Questions :

Comment fait-on avec l'IPv6 ?

Comment attribuer une ip automatiquement ?

Et les clients dans tout ca ?

---

# Deux possibilités

## Autoconfiguration

- Comment connaître le couple IP  $\Leftrightarrow$  Ordinateur

## DHCP static

- Nécessité du DUID

une IPv6 = un DUID = un ordinateur = un utilisateur

Choix de la deuxième option (en cours)

# Adressage dynamique v6

---

- Pas de killer app.
- Deux réseaux qui cohabitent, 2 fois plus de problèmes
- Appareil(s) peu ou pas mature(s)
- Stock d'IPv4 gigantesque
- Problème de sécurité : pareil qu'en IPv4

=> Apprendre à se servir d'un protocole actuel.

## L'intérêt de l'IPv6 aujourd'hui

---

Réveil douloureux le jour ou :

- IPv4 ok de partout
- IPv6 fonctionne mais sur des portions réduites

⇒ Lenteur sur le réseau

⇒ Pas de monitoring IPv6 : Diagnostic long

- Résultat : un switch Dell semble dropper les paquets IPv6

Mais c'est quoi ce bordel ?!  
Ca marche pu ... enfin à moitié

---

- Un switch Dell semble dropper les paquets IPv6.
- Surprise !
- Confirmé par le reboot du switch.
  
- Même problème un mois plus tard  
=> Mise à jour du firmware

**Problème résolu depuis.**

Mais c'est quoi ce bordel ?!

Ca marche pu ... enfin à moitié (2)

---

Déploiement de l'IPv6 avec du monitoring v4.

**Fail**

Mais c'est quoi ce bordel ?!  
Ca marche pu ... enfin à moitié (3)

---

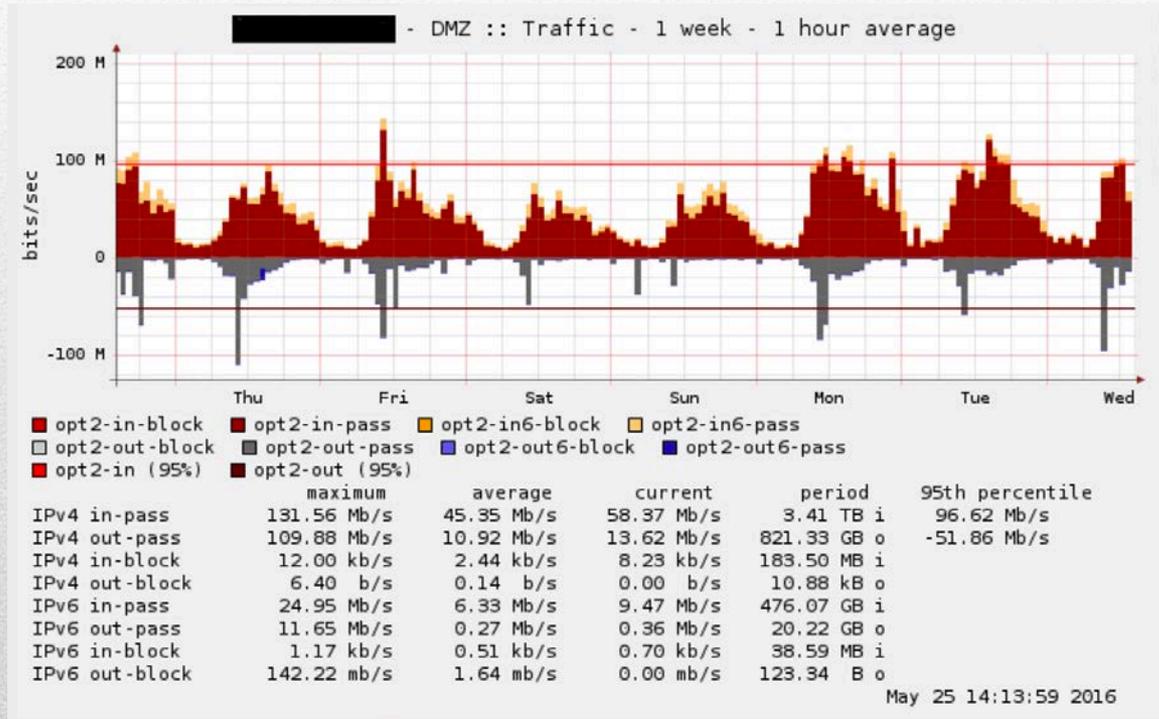
- Rencontre de Alain Bidaud (CRIANN)
- Groupe de travail IETF : démonter IPv4 sur les réseaux ou IPv6 only.
- SYRHANO :
  - IPv6 only sauf sur les interfaces avec d'autres réseaux

=> Réseau de supervision v6 only

# IPv6 only ?

---

- DMZ : 40 à 50 % (à verifier) en v6
- 2 et 7 % de trafic avec l'extérieur en v6

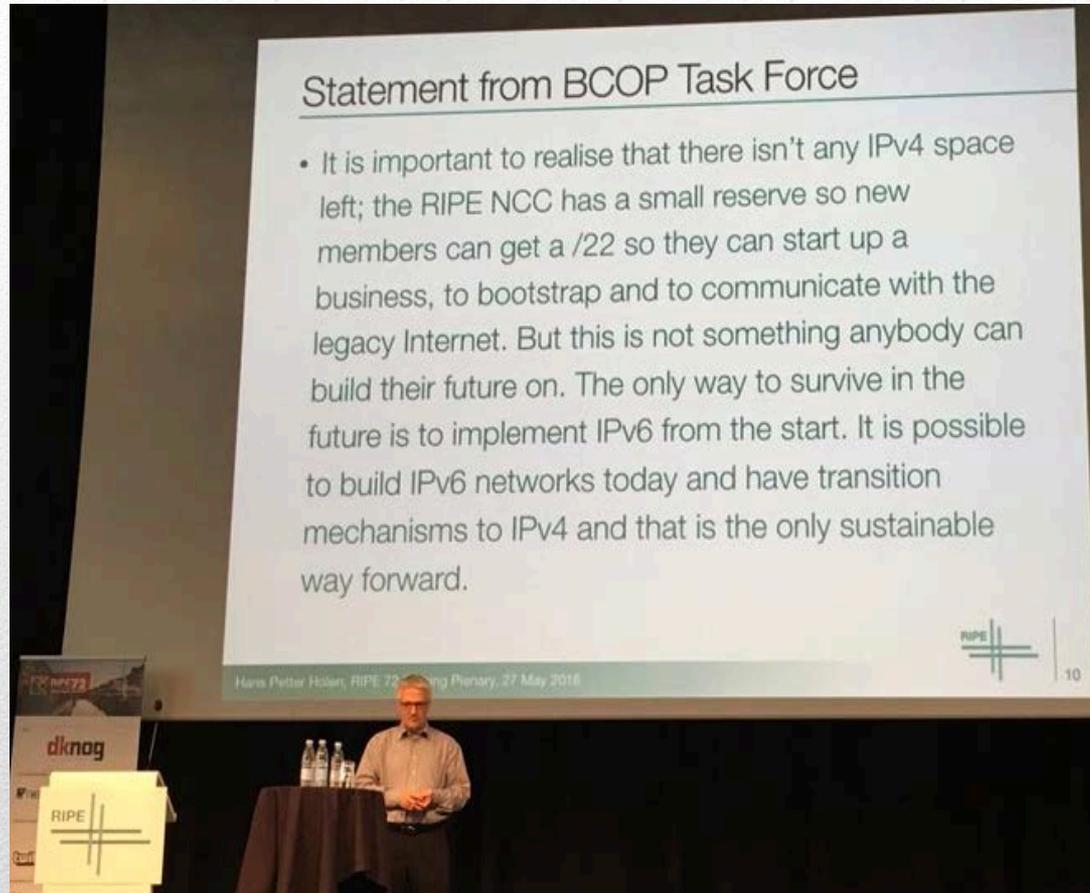


# Statistiques

- Jamais demandé par les utilisateurs
- Simple, si anticipé.
- Maquette si possible
- Monitoring
- Attention aux applications (maison) incompatibles

# Résumé

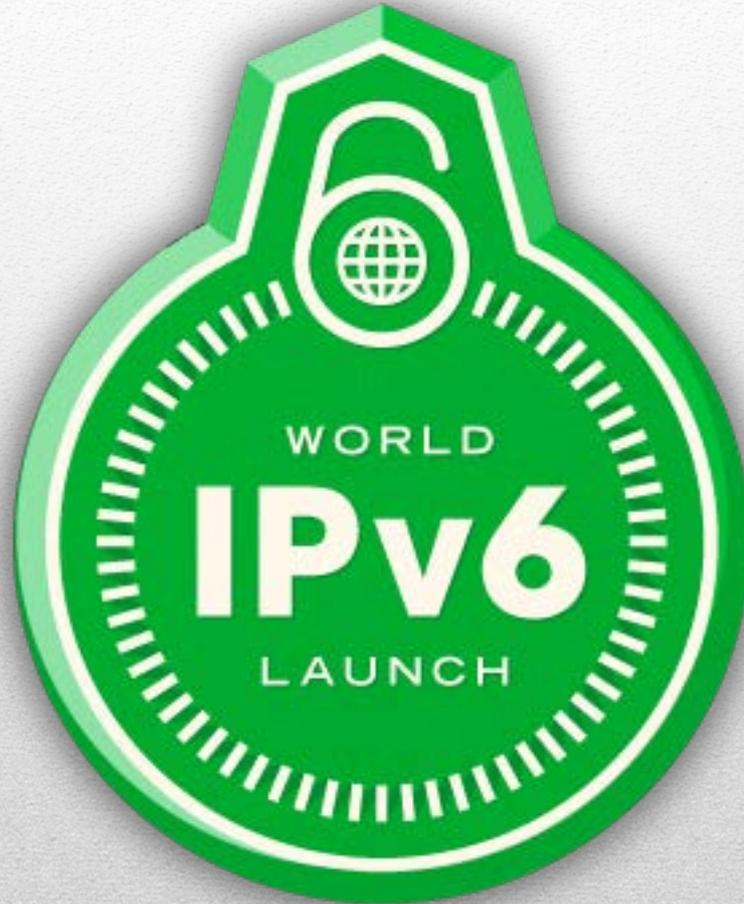
---



# Ripe 72

---

# Questions



193.55.43.0/24, 193.51.160.0/24 et 194.254.245.0/25

- Prefix v6 : 2001:660:500b::/48
- 194.254.245.0/25  $\Leftrightarrow$  2001:660:500b:245::/64
- 193.55.43.0/24  $\Leftrightarrow$  2001:660:500b:43::/64
- 193.51.160.0/24  $\Leftrightarrow$  2001:660:500b:160::/64

# Plan d'adressage

---