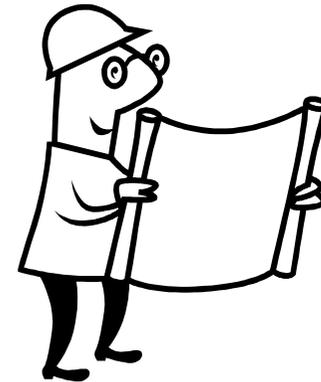


# DSI Service systèmes, réseaux & téléphonie

« Architecture originale de réseau IPV4 & IPV6 sous l'œil d'un ancien RSSI »

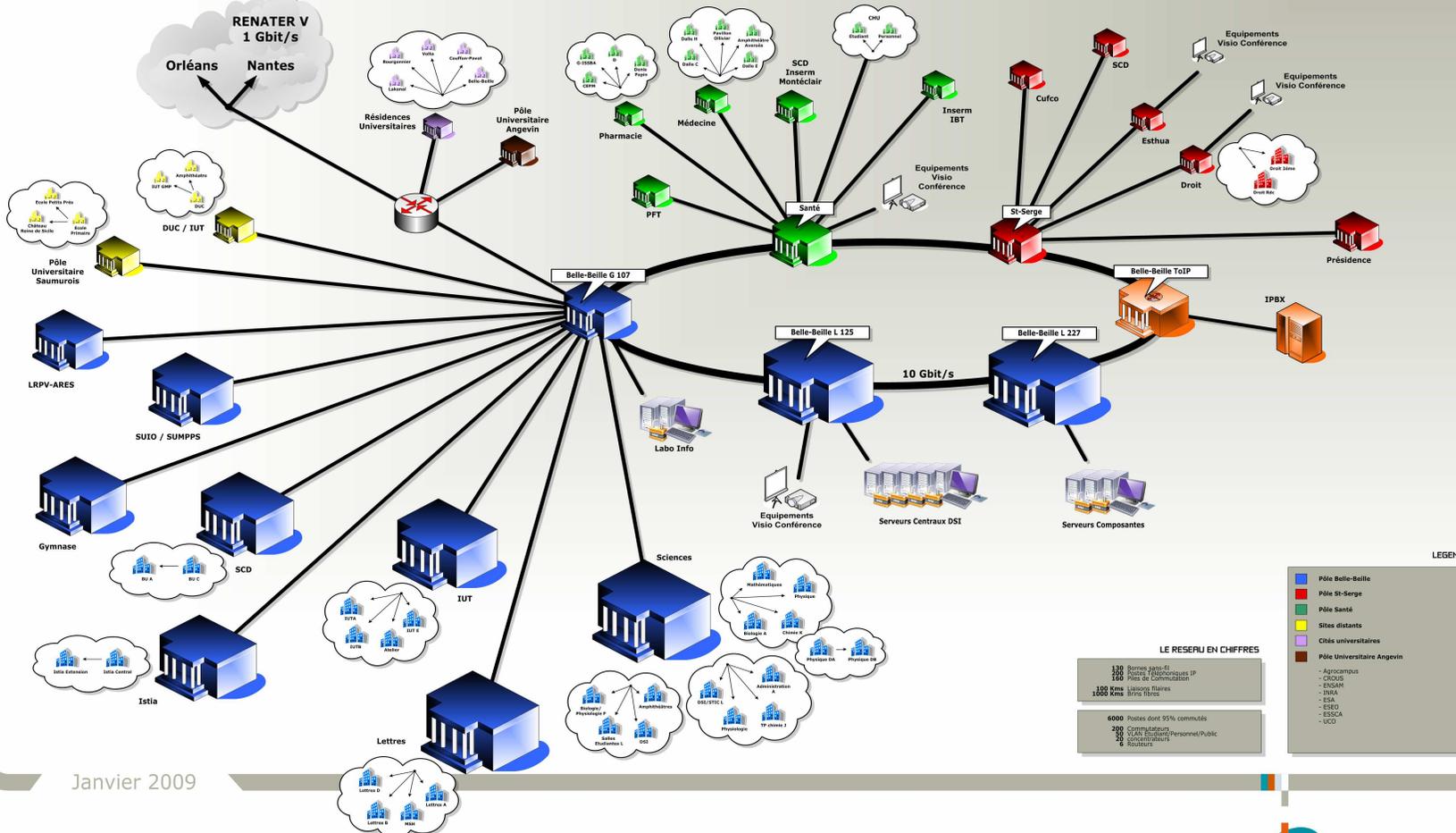
« Valeurs ajoutées d'IPV6 dans une UMR »

- **Introduction plan du réseau**
- **Origine, projet IPV6-adire**
  - **Fourche IPV6**
  - **Plan d'adressage**
- **Schémas logiques de sécurité**
- **Organisation réseau des laboratoires**
- **IPV6 dans une UMR**
- **Configuration d'un poste**
- **Conclusion**



# Plan du réseau

## Réseau Informatique IPv4 - IPv6



Janvier 2009

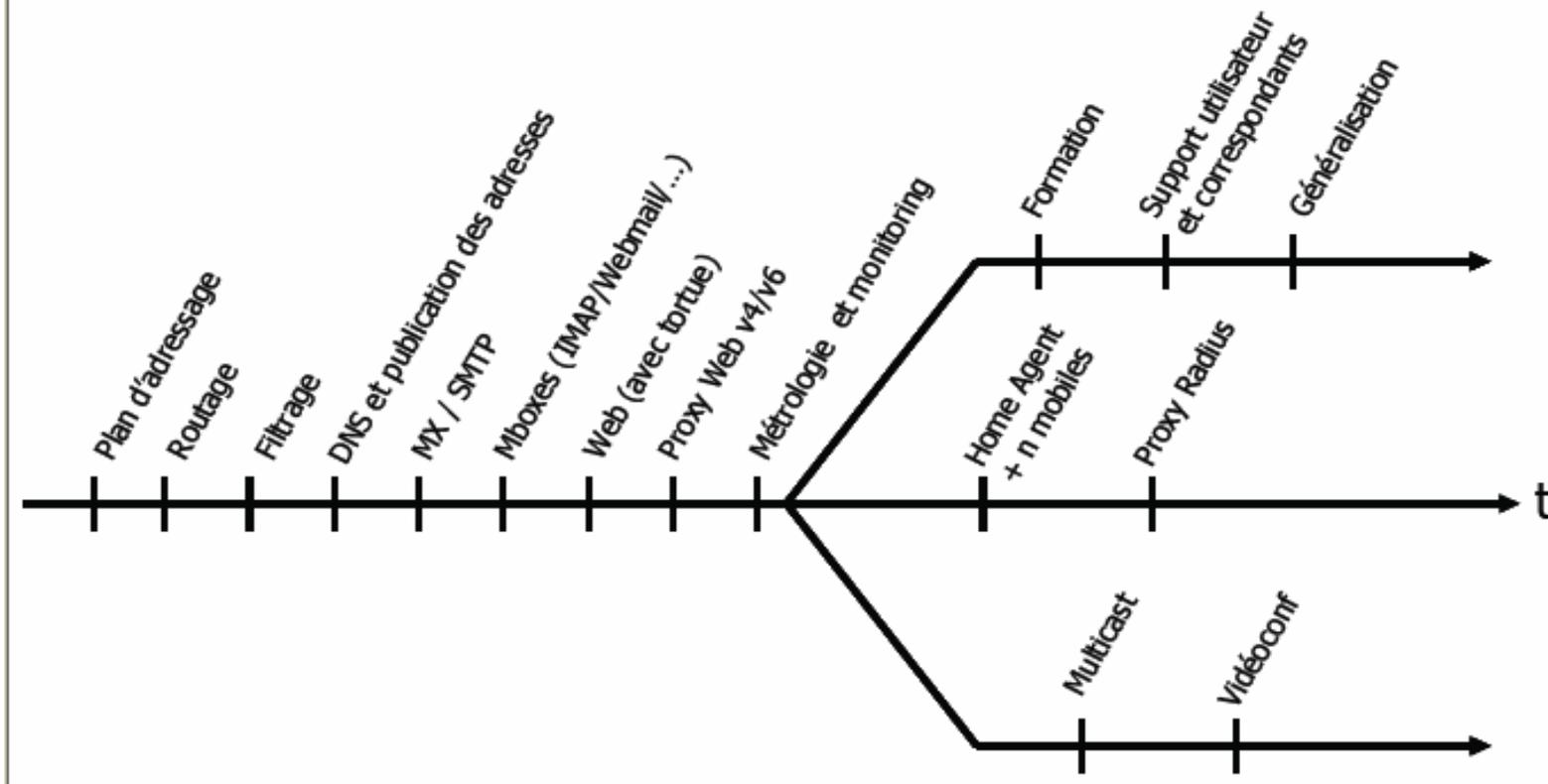


# Origine Projet IPV6-adire

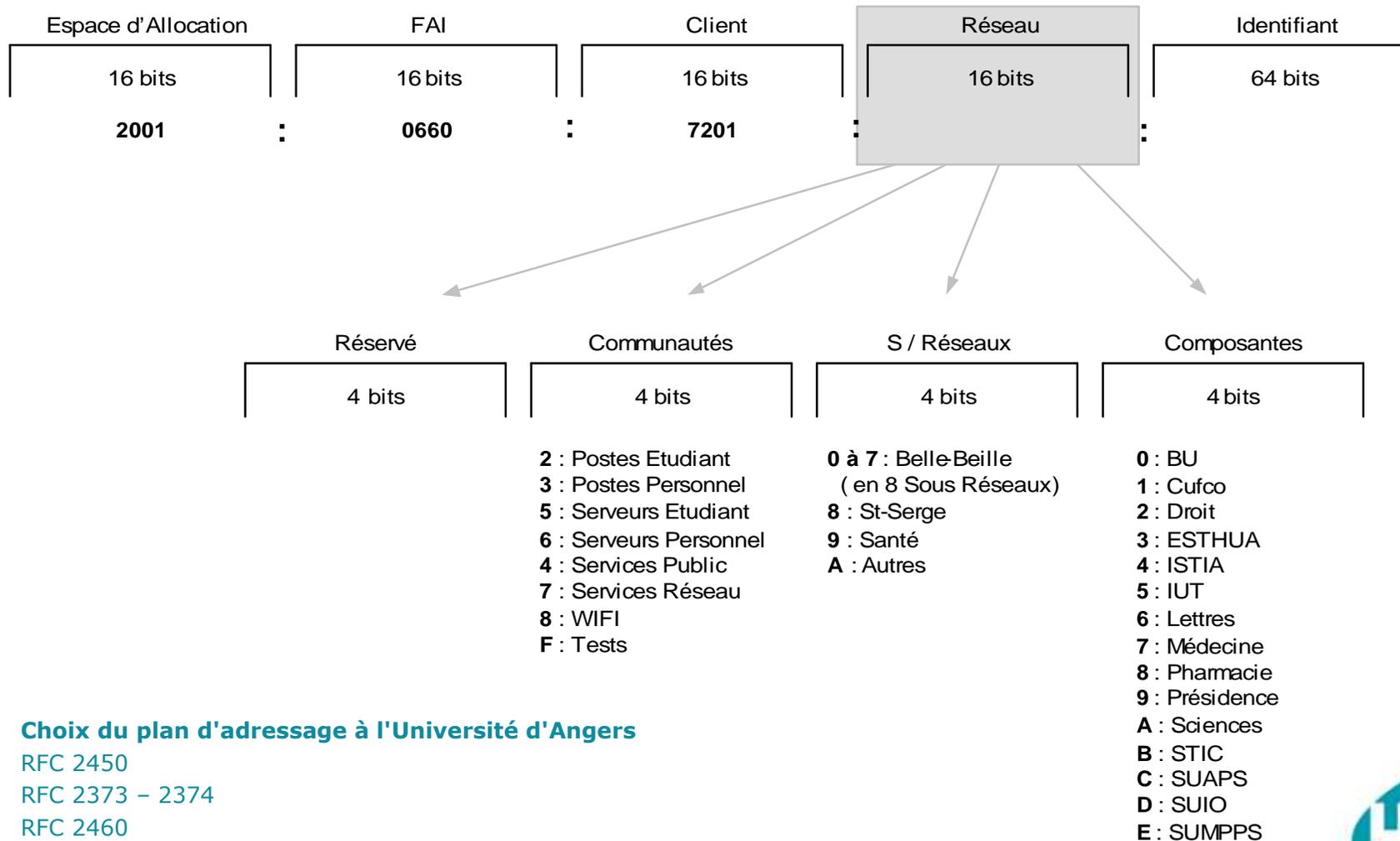
Projet 30 novembre 2004  
Concernait 11 sites

...

## IPv6 – La fourche



# 1er plan d'adressage



## Choix du plan d'adressage à l'Université d'Angers

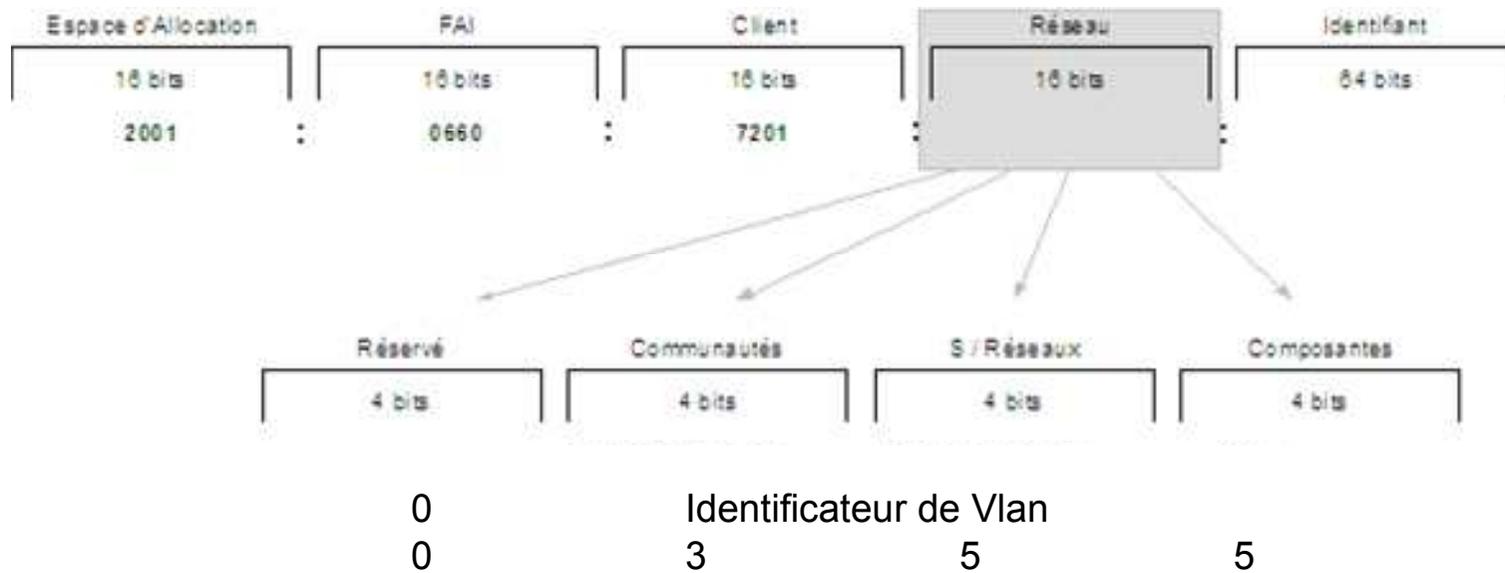
RFC 2450

RFC 2373 – 2374

RFC 2460

...

# 2ème plan d'adressage



## Choix du plan d'adressage à l'Université d'Angers

RFC 2450

RFC 2373 - 2374

RFC 2460

...

7 19/03/2009

DSI - service systèmes & réseaux

# Schéma logique de sécurité

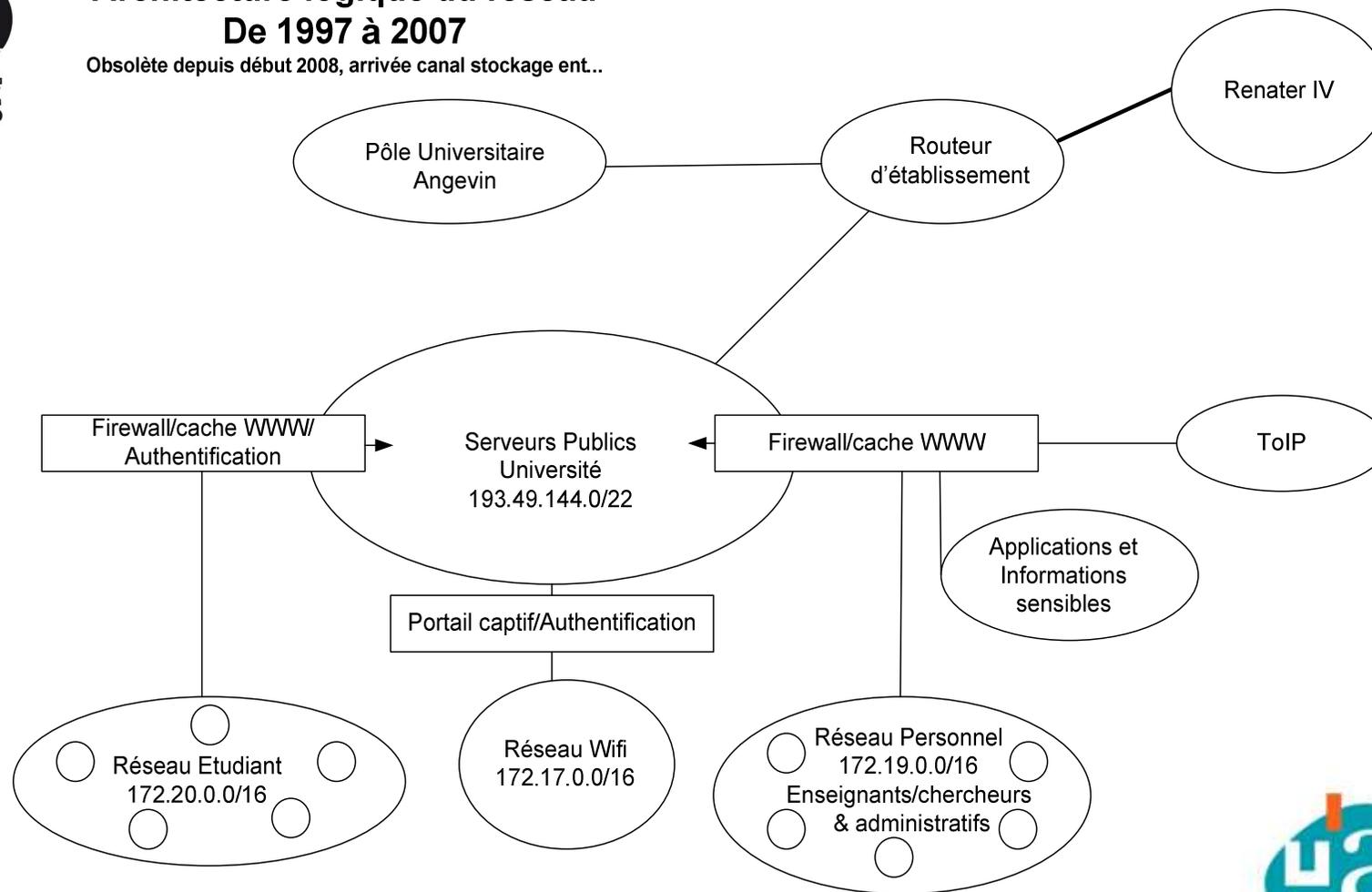
1999 – 2007  
2008-2009  
2010  
...

# Schéma logique 1999



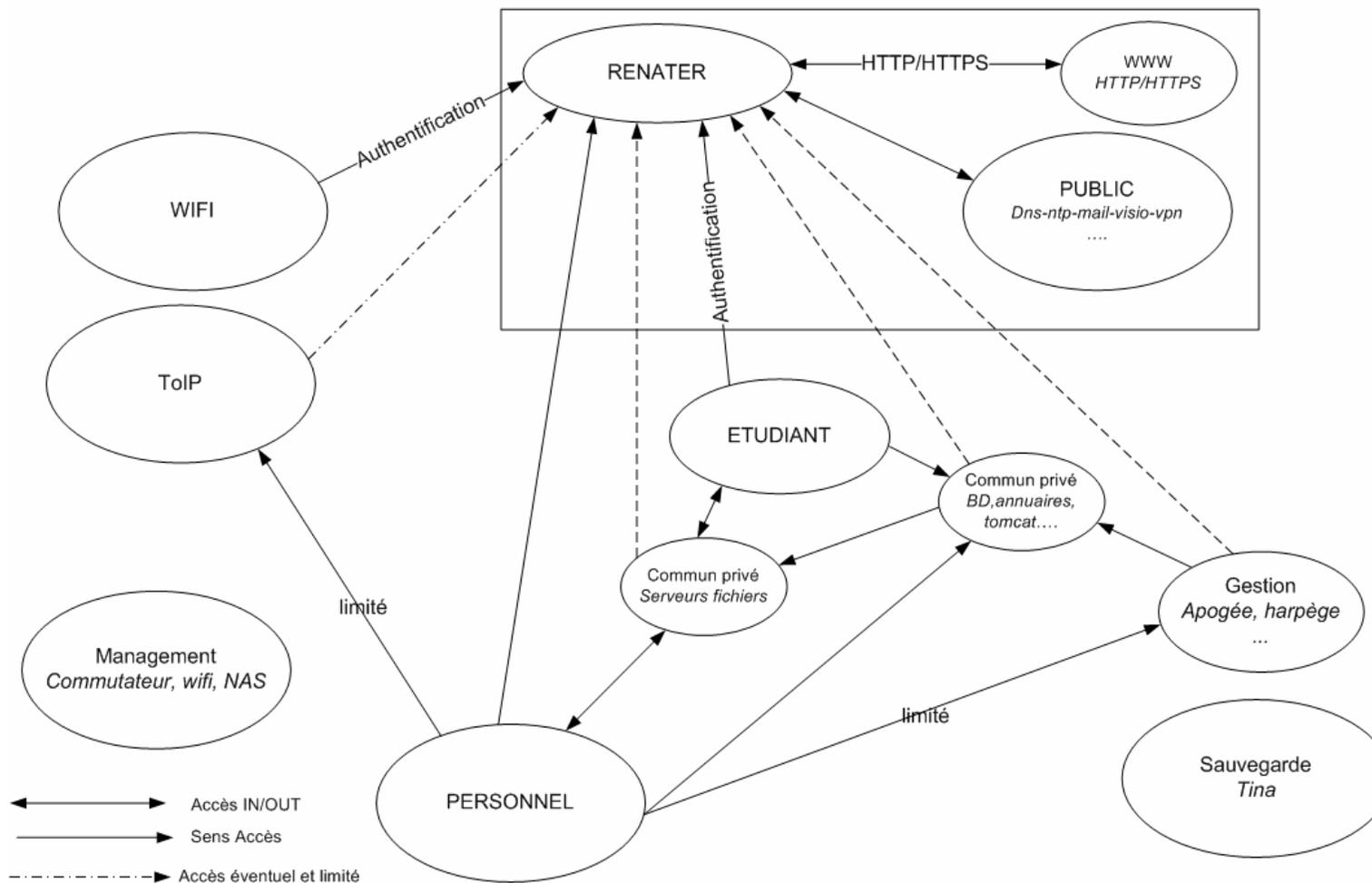
## Architecture logique du réseau De 1997 à 2007

Obsolète depuis début 2008, arrivée canal stockage ent..



# Schéma logique 2009

Idées de schéma de sécurité 2009



# Organisation «réseau» des laboratoires

# Les familles

## Extrait d'organisation des laboratoires, UMR, Inserm, CNRS.....

|                     |  |  |  |  |  |  |  |  |                |                |  |  |
|---------------------|--|--|--|--|--|--|--|--|----------------|----------------|--|--|
| Istia               |  |  |  |  |  |  |  |  | 250 eistia     | 350 pistia     |  |  |
| Lettres             |  |  |  |  |  |  |  |  | 251 elettres   | 351 plettres   |  |  |
| IUT                 |  |  |  |  |  |  |  |  | 252 eiut       | 352 piut       |  |  |
| IUT Cholet          |  |  |  |  |  |  |  |  | 253 eiutcholet | 353 piutcholet |  |  |
| Géographie          |  |  |  |  |  |  |  |  | 254 esci       | 354 psci       |  |  |
| Sci Chimie          |  |  |  |  |  |  |  |  | 254 esci       | 354 psci       |  |  |
| Sci Physique        |  |  |  |  |  |  |  |  | 254 esci       | 354 psci       |  |  |
| Sci Math            |  |  |  |  |  |  |  |  |                | 355 pmath      |  |  |
| Sci Info            |  |  |  |  |  |  |  |  | 256 einfo      |                |  |  |
| LRPV                |  |  |  |  |  |  |  |  |                | 354 psci       |  |  |
| Sci Biologie A et F |  |  |  |  |  |  |  |  |                | 354 psci       |  |  |

# Adressage IPv4

- **Pour chaque laboratoire**

- **172.19.x.y**

- *X est différent pour chaque laboratoire*

- **Avantages : « large »**

- **Inconvénients : « classe B »**

- \* ACL.....

|            |                    |
|------------|--------------------|
| 7          | Application        |
| 6          | Présentation       |
| 5          | Session            |
| 4          | Transport          |
| 3          | Réseau             |
| 2          | Liaison de données |
| 1          | Physique           |
| Modèle OSI |                    |

|          |              |
|----------|--------------|
| 7        | HTTP, SMTP   |
| 6        | SSL, TLS     |
| 5        | NetBios      |
| 4        | TCP-UDP      |
| 3        | IPv4-IPv6    |
| 2        | Ethernet     |
| 1        | 10/100 baseT |
| EXEMPLES |              |

# Filtrages commutateur

- **Principes**

- **ACL niveau 3 évalué au niveau 2 de la couche OSI**

- **Où**

- *Tous les commutateurs de cœur de réseau*

+

- *Commutateur mathématique*

|            |                    |
|------------|--------------------|
| 7          | Application        |
| 6          | Présentation       |
| 5          | Session            |
| 4          | Transport          |
| 3          | Réseau             |
| 2          | Liaison de données |
| 1          | Physique           |
| Modèle OSI |                    |

|          |              |
|----------|--------------|
| 7        | HTTP, SMTP   |
| 6        | SSL, TLS     |
| 5        | NetBios      |
| 4        | TCP-UDP      |
| 3        | IPv4-IPv6    |
| 2        | Ethernet     |
| 1        | 10/100 baseT |
| EXEMPLES |              |

# Exemple IPV4

- **Policy sur les commutateurs**

```
entry math{
  if {
    source-address 172.19.45.0/24;
    destination-address 172.19.45.0/24;
  }
  then
  {
    permit;
  }
}

entry nomath1{
  if {
    source-address 172.19.0.0/16;
    destination-address 172.19.45.0/24;
  }
  then
  {
    deny;
  }
}

entry nomath2{
  if {
    source-address 172.19.45.0/24;
    destination-address 172.19.0.0/16;
  }
  then
  {
    deny;
  }
}
```

# Exemple IPV6

- **IPV6**

```
#
# ACL IPV6
#      0200 etudiant
#      0300 personnel
#      0400 public146
#      0500 public145
#      0600 public147
#      0700 public144
#      0800 toip
#      0900 wifi

entry etu-pers {
if {
source-address 2001:660:7201:0200::/56 ;
destination-address 2001:660:7201:0300::/56 ;
}
then {
deny;
}
}

entry etu-toip {
if {
source-address 2001:660:7201:0200::/56 ;
destination-address 2001:660:7201:0800::/56 ;
}
then {
deny;
}
}
```

# Exemple IPV6

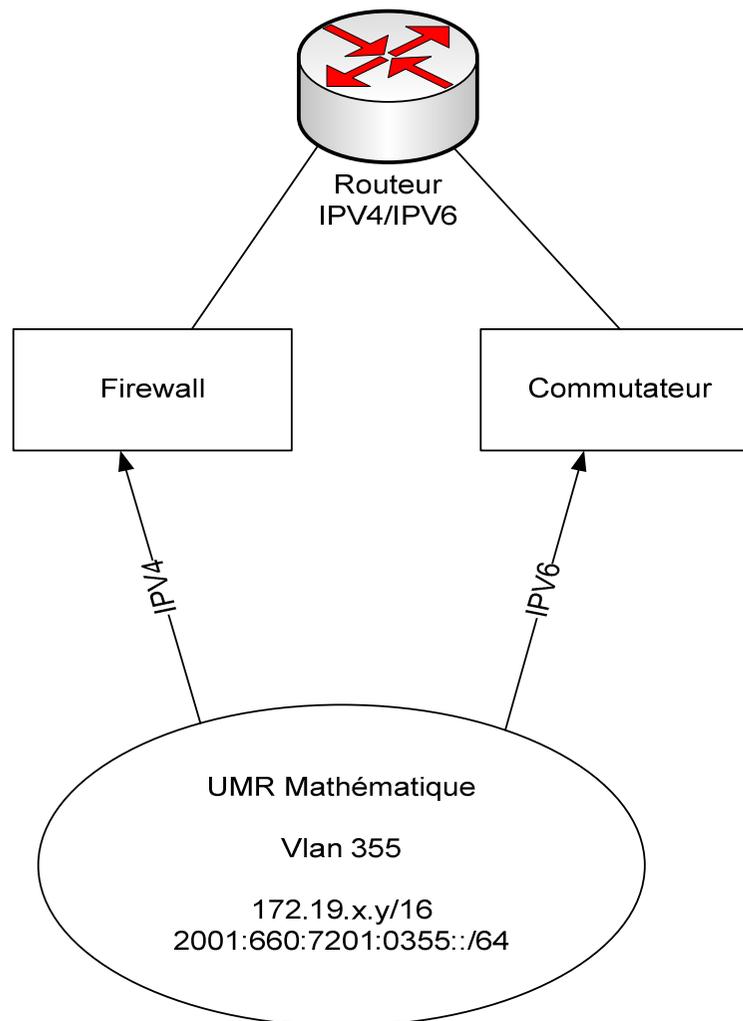
- **ICMP, attention au filtrage**
  - **Nouvelles fonctionnalités, exemples**
  - ....
  - ICMPv6 type 137 : utilisé par les routeurs pour informer les stations de travail quand un autre routeur est plus approprié pour atteindre la destination demandée.
  - ICMPv6 type 138 : redéfinir les préfixes réseaux au niveau routeur
  - .....

# IPV6 dans une UMR

...

# Filtrages PIX/commutateur

- Principe dans une UMR



# Configuration commutateur

- **Adressage du vlan pmath**
  - **configure pmath ipaddress 2001:660:7201:355::254/64**

```
BD12804-G107.2 # show vlan pmath
VLAN Interface with name pmath created by user
  Admin State:      Enabled          Tagging:           802.1Q Tag 355
  Virtual router:  VR-Default
  IPv6:             fe80::204:96ff:fe1e:f360/64
                   2001:660:7201:355::254/64
  STPD:             None
  Protocol:         Match all unfiltered protocols
  Loopback:         Disabled
  NetLogin:         Disabled
  QosProfile:       QP2
  Egress Rate Limit Designated Port: None configured
  Flood Rate Limit QosProfile:         None configured
  Ports:           5. (Number of active ports=4)
  Tag:             *1:1, *1:2, *5:7, *5:15, 5:18
  Flags:           (*) Active, (!) Disabled, (g) Load Sharing port
                   (b) Port blocked on the vlan, (m) Mac-Based port
                   (a) Egress traffic allowed for NetLogin
                   (u) Egress traffic unallowed for NetLogin
                   (t) Translate VLAN tag for Private-VLAN
                   (s) Private-VLAN System Port, (L) Loopback port
                   (e) Private-VLAN End Point Port

BD12804-G107.3 #
```

# Configuration commutateur

- **BD12K, Extreme Networks, adressage du vlan pmath**
  - **configure pmath ipaddress 2001:660:7201:355::254/64**
  - **configure vlan pmath router-discovery ipv6 add prefix 2001:660:7201:355::/64**
  - **configure vlan pmath router-discovery ipv6 set prefix 2001:660:7201:355::/64 autonomous-flag on**
  - **configure vlan pmath router-discovery ipv6 set prefix 2001:660:7201:355::/64 onlink-flag on**
  - **configure vlan pmath router-discovery ipv6 set prefix 2001:660:7201:355::/64 preferred-lifetime 604800**
  - **configure vlan pmath router-discovery ipv6 set prefix 2001:660:7201:355::/64 valid-lifetime 2592000**
  - **configure vlan pmath router-discovery ipv6 reachable-time 30000**
  - **configure vlan pmath router-discovery ipv6 retransmit-time 1000**
  - **enable router-discovery ipv6 vlan pmath**

# Routage

- **eBGP sur Renater**
- **OSPF v3 ....licence...**
- **Ripng**
  - **enable ripng**
  - **enable ripng export Direct cost ...**
  - **enable ripng export Static cost ...**
  - **configure ripng add pmath**

# Utilisation IPV6

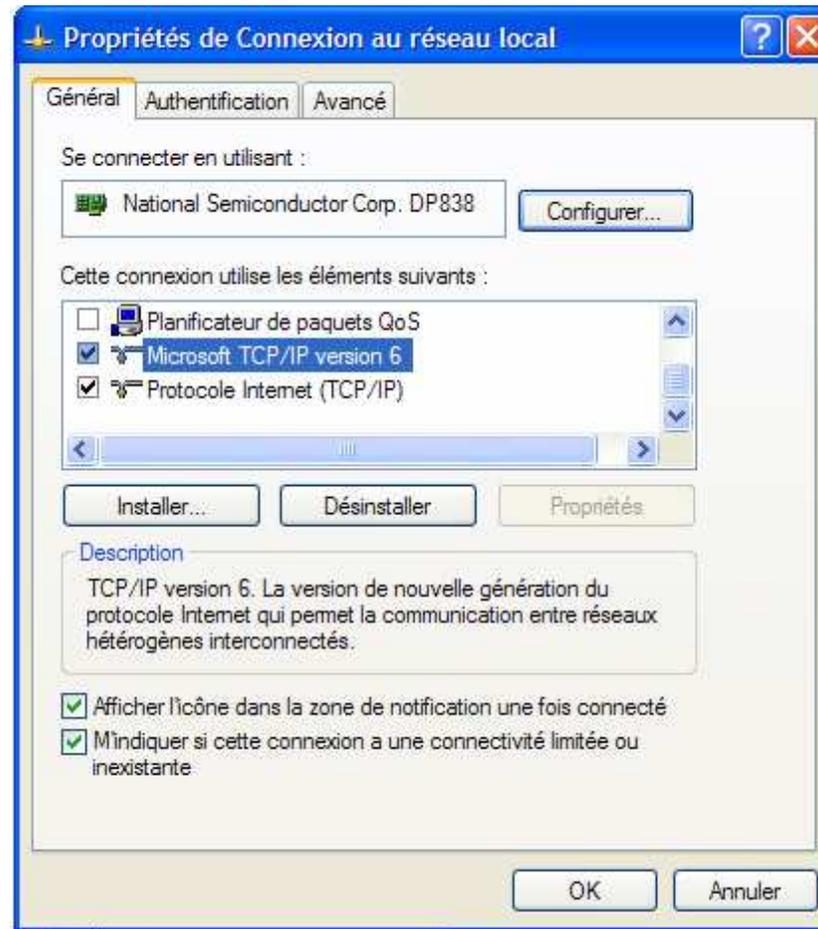
- **Multicast en lien local**
  - All nodes FF02::1 joindre les stations du lien (neighbor discovery protocol )
  - All routers FF02::2 joindre les routeurs du lien
  - ...
- **Multicast en site local**
  - All routers FF05::2
  - ...
- **Plus de broadcast !!!!!!!!!!!!!**
- **Postes clients multiples adresses**
- **Mobilité, home agent**
- **Absence fragmentation de paquets...**

# Configuration d'un poste

...

# Sous XP

- **Juste à cocher**



- **Dual Stack IP v4-v6**

```
C:\ Fenetre Dos
-----
Carte Ethernet Connexion au réseau local:

    Suffixe DNS propre à la connexion : uang
    Adresse IP. . . . . : 172.19.2.15
    Masque de sous-réseau . . . . . : 255.255.0.0
    Adresse IP. . . . . : 2001:660:7201:309:c503:150:c274:3f27

    Adresse IP. . . . . : 2001:660:7201:309:20d:9dff:fec8:2f
    Adresse IP. . . . . : fe80::20d:9dff:fec8:2f%4
    Passerelle par défaut . . . . . : 172.19.0.254
                                       fe80::9:c0ff:fe5c:96f4%4

Carte Tunnel Teredo Tunneling Pseudo-Interface :

    Suffixe DNS propre à la connexion :
    Adresse IP. . . . . : fe80::5445:5245:444f%5
    Passerelle par défaut . . . . . :

Carte Tunnel Automatic Tunneling Pseudo-Interface :

    Suffixe DNS propre à la connexion : uang
    Adresse IP. . . . . : fe80::5efe:172.19.2.15%2
    Passerelle par défaut . . . . . :

C:\Travail>
```

# Sous FreeBSD

- **Fichier /etc/rc.conf pour un serveur**
  - **ipv6\_enable="YES"**
  - **ipv6\_ifconfig\_dc0="2001:660:7201:709::10 prefixlen 64"**
  - **ipv6\_defaultrouter="2001:660:7201:709::254"**

# Conclusion

Règles de filtrages doivent être doublées  
ACL, Ip6tables...

Chemins différents IP v4-v6

Adressage simplifiée...

...

- **Iptable & ip6tables**

- ip6tables -A INPUT -j DROP
- ip6tables -A OUTPUT -j DROP
- ip6tables -A FORWARD -j DROP

**Ecrire les règles similaires iptable et ip6tables**

# Questions

