Le réseau du Département Informatique (et du laboratoire GREYC)

Davy Gigan (davy.gigan@unicaen.fr)
Pierre Blondeau (pierre.blondeau@unicaen.fr)
Alexis Olivier (alexis.olivier@unicaen.fr)

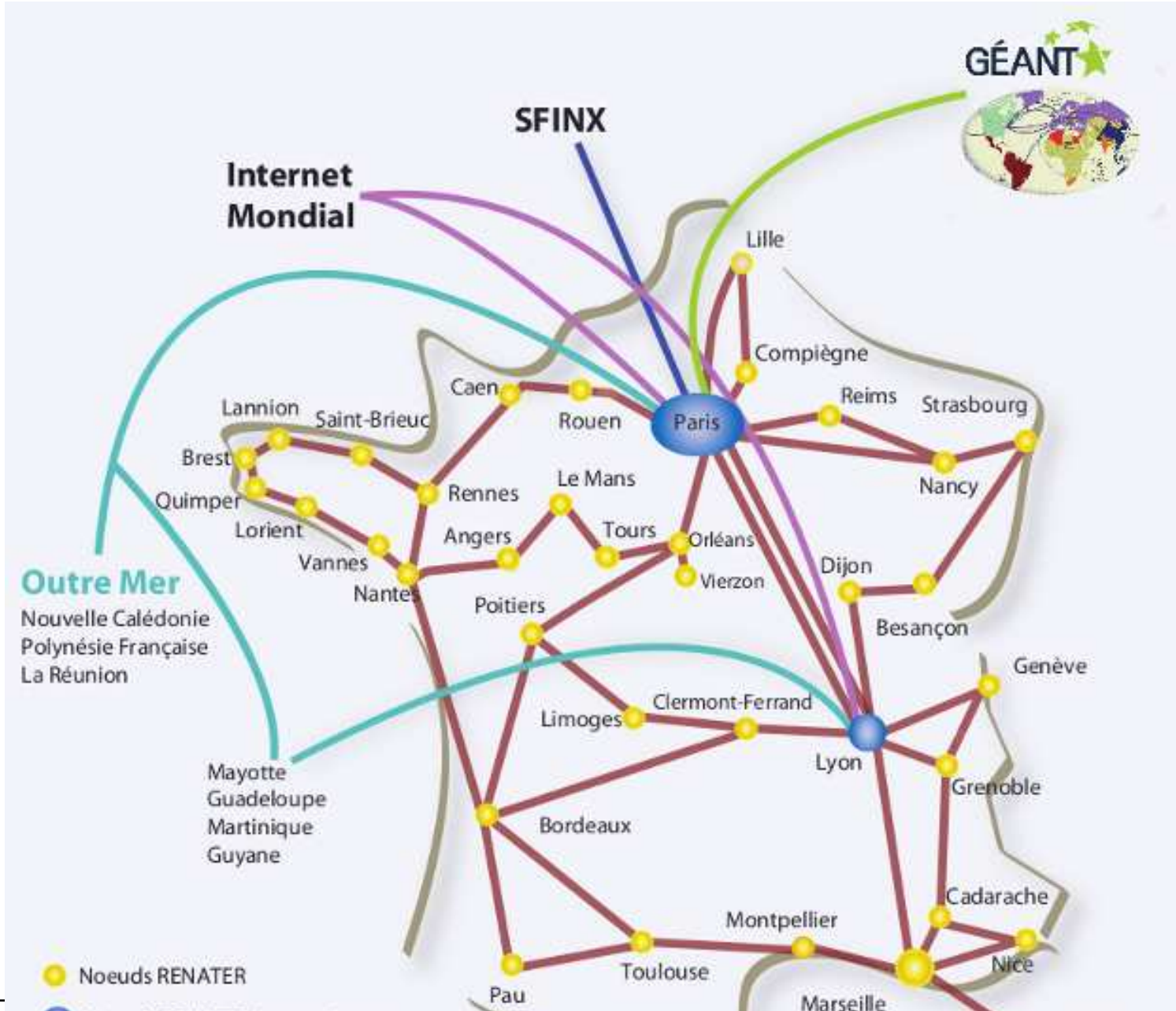
Sommaire

- Situation
- Architecture
- Services
- Sécurité
- Virtualisation

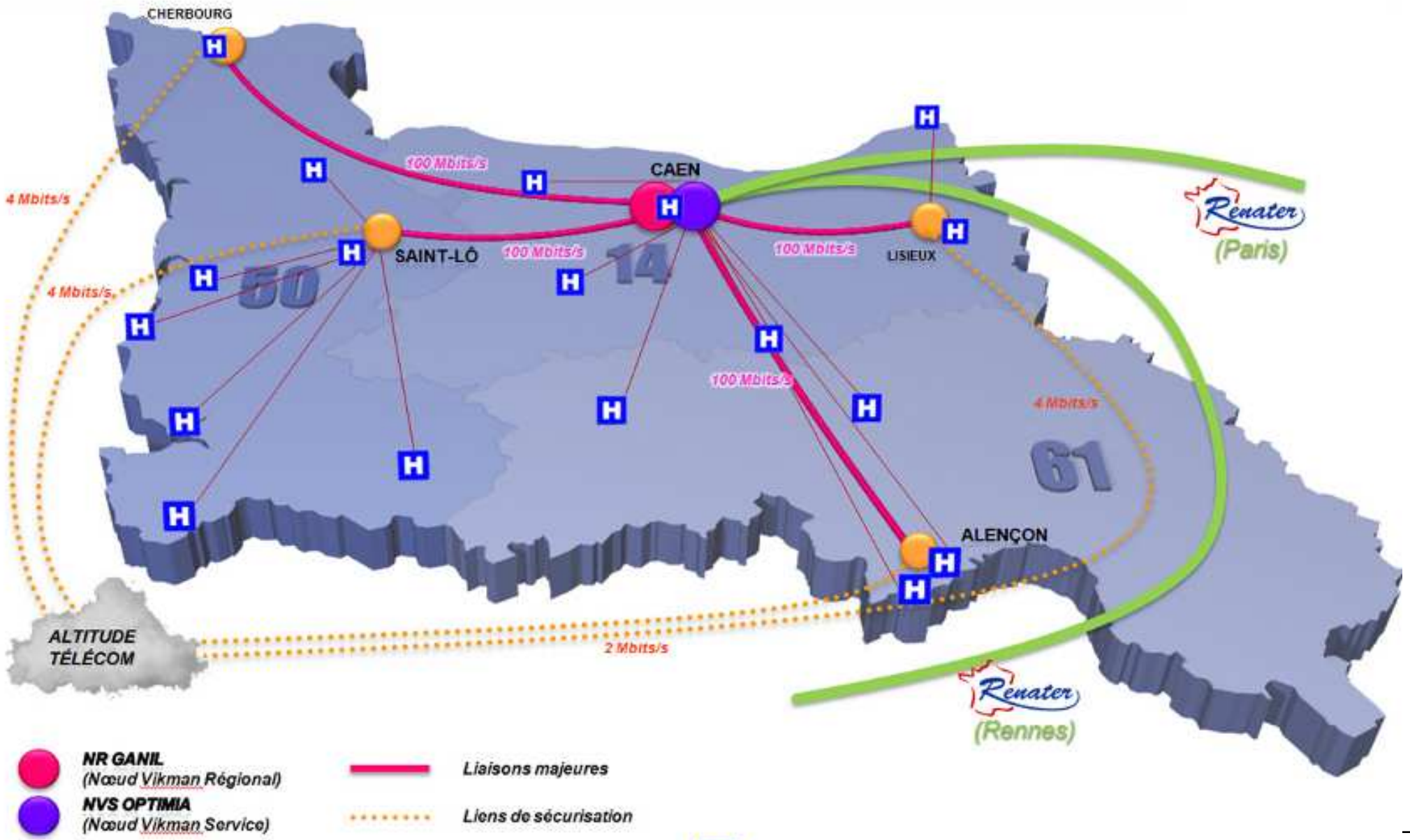
Situation

- Géant / SFINX
  - Réseau Très Haut Débit Européen
  - Noeud d’échange Internet
- Renater
  - Fournisseur d’Accès Internet pour la recherche et l’éducation
- Vikman
  - Réseau régional Haut Débit
- Université

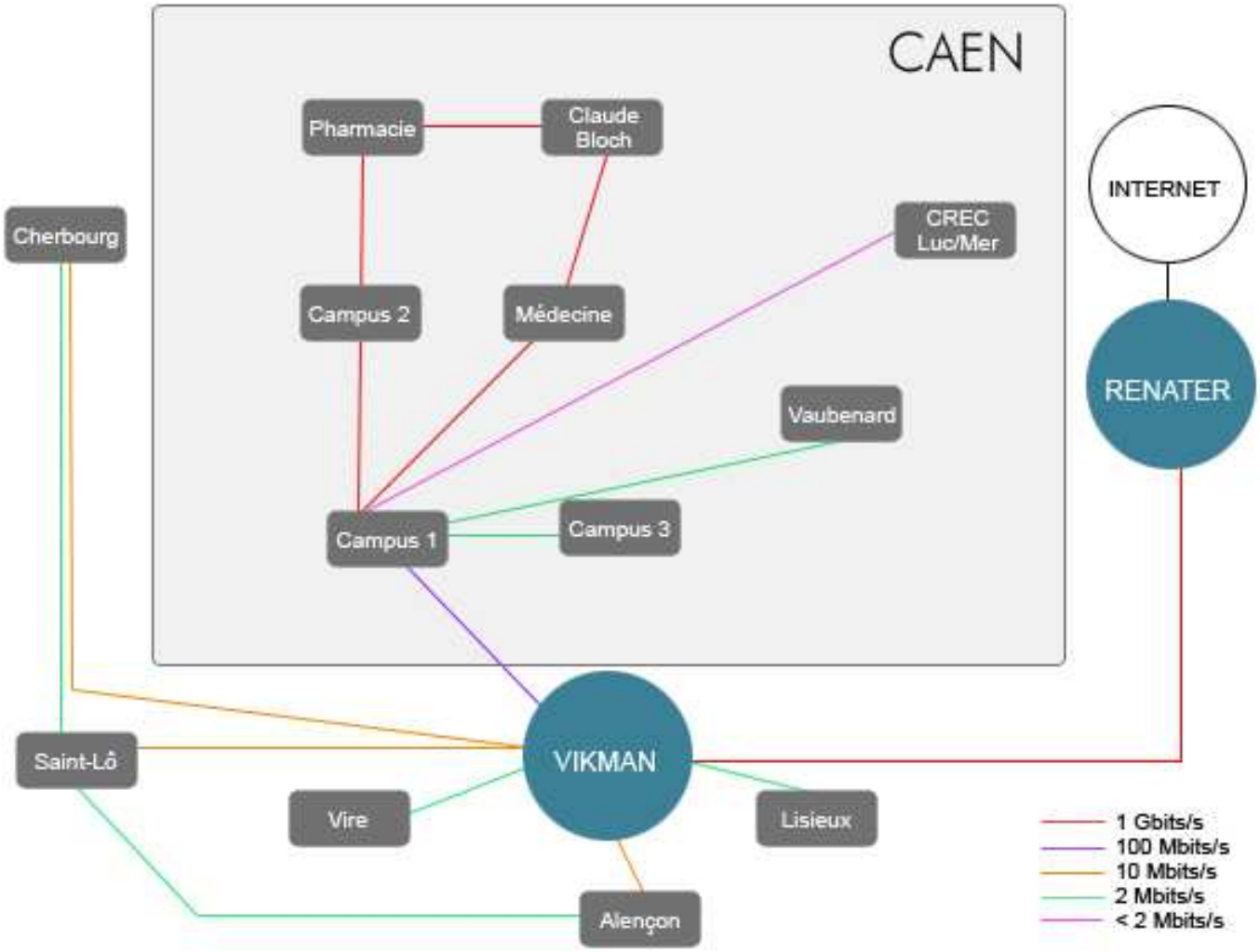
Carte Renater



Vikman 5


CHERBOURG
CAEN
SAINT-LÔ
LISIEUX
ALENÇON
100 Mbits/s
100 Mbits/s
100 Mbits/s
100 Mbits/s
4 Mbits/s
4 Mbits/s
4 Mbits/s
2 Mbits/s
50
14
61
Renater
(Paris)
Renater
(Rennes)
ALTITUDE
TÉLÉCOM
NR GANIL
(Nœud Vikman Régional)
NVS OPTIMIA
(Nœud Vikman Service)
Liaisons majeures
Liens de sécurisation

Université (Basse-Normandie)



Architecture : VLANs

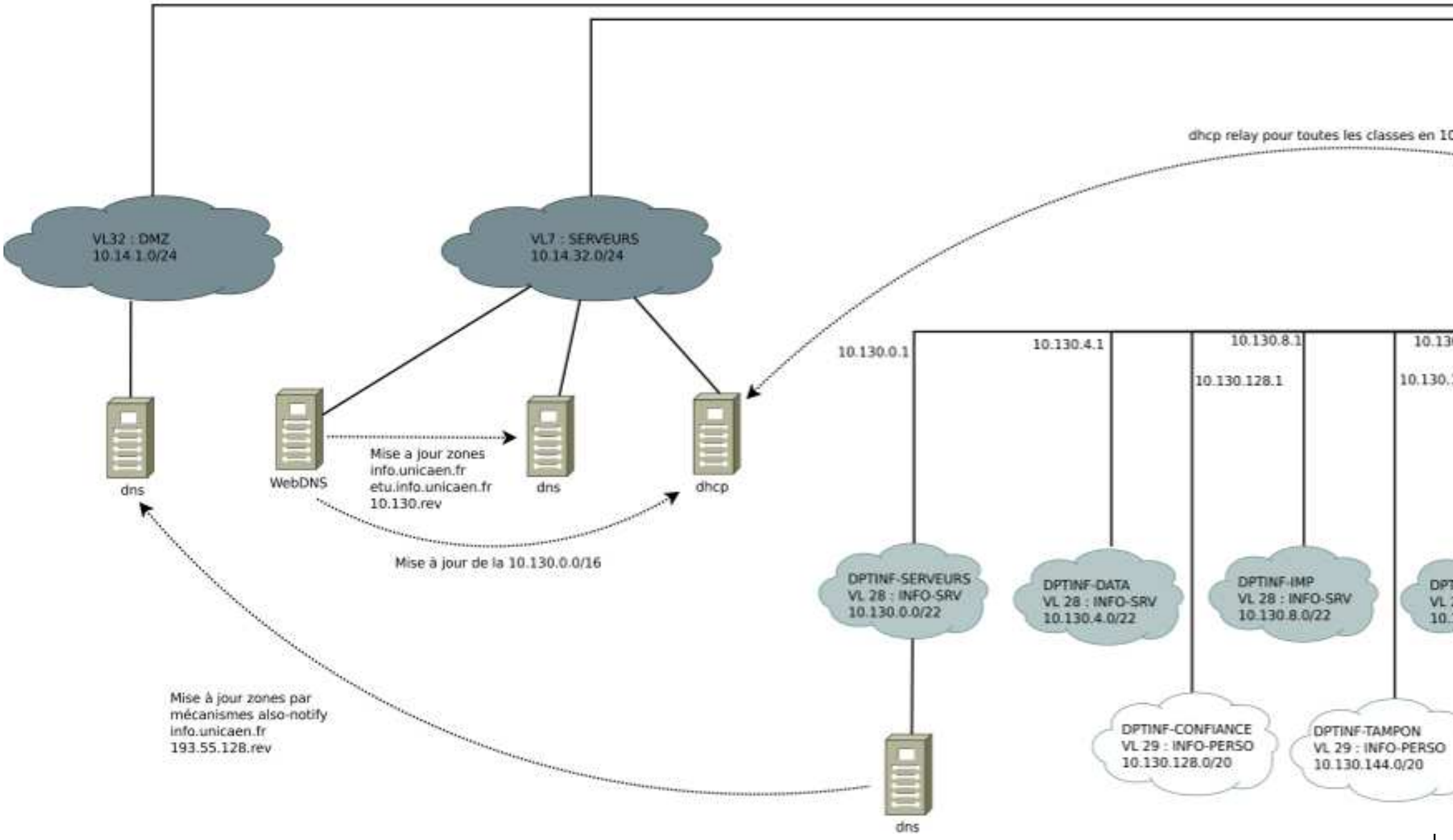
- 26 (INFO-DMZ) : DMZ
- 27 (INFO-ETU) : Enseignement
- 28 (INFO-SRV) : Serveurs et matériels
- 29 (INFO-LABO) : Recherche
- 30 (INFO-WAN) : Interconnexion

- 66 IPv6 vers IUT
- 67 IPv6 vers CERTIC
- 68 IPv6 vers CRISI

Architecture : le réseau

- Réseau filaire
  - Routage / Filtrage redondant
  - IPv4 et IPv6
- Switches sécurisés sur adresse MAC
  - contournement possible mais difficile
- Utilisation de dot1x
  - un mot de passe est nécessaire pour la connexion physique au réseau
- Wifi : eduroam, unicaen

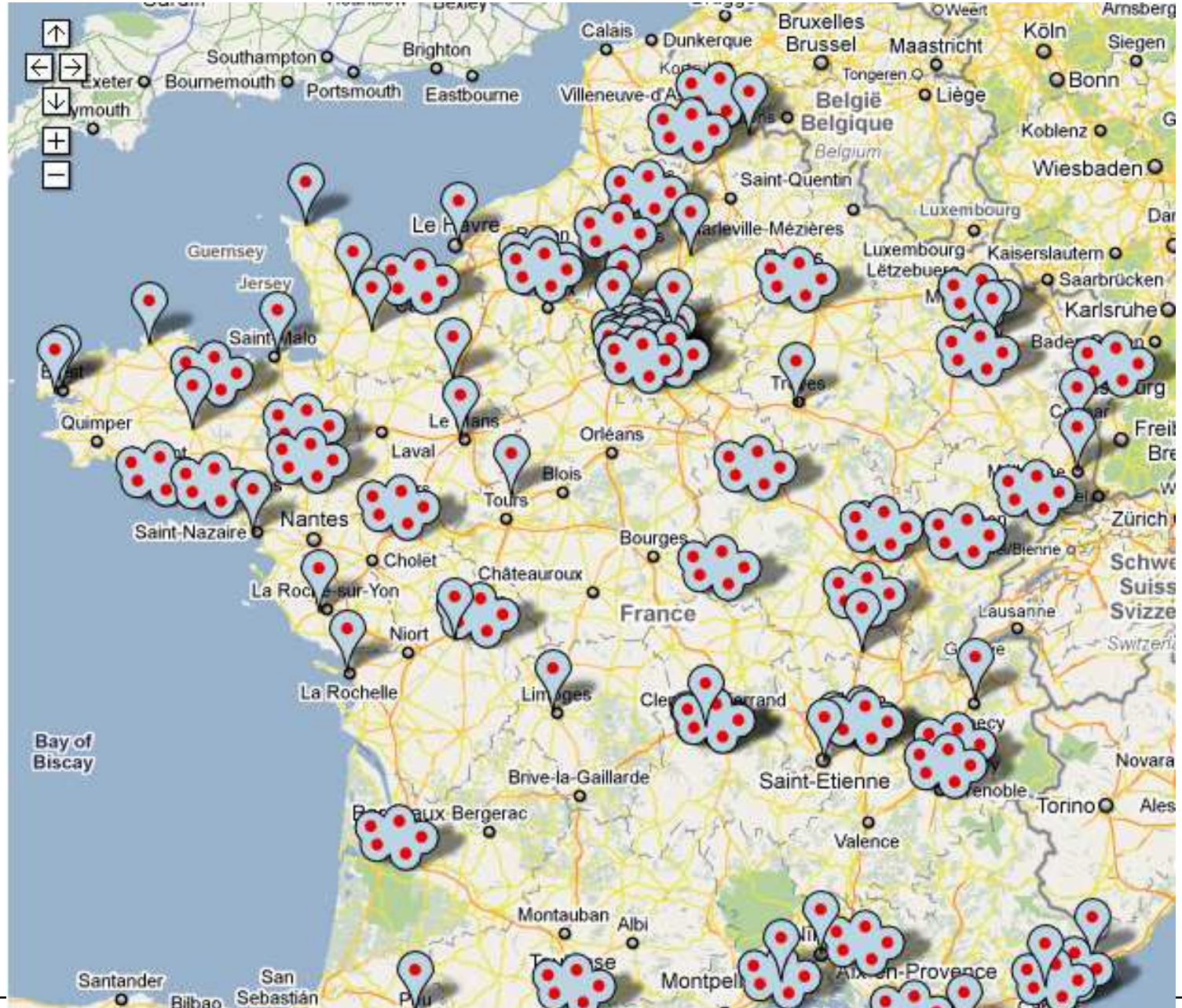
Architecture : le réseau



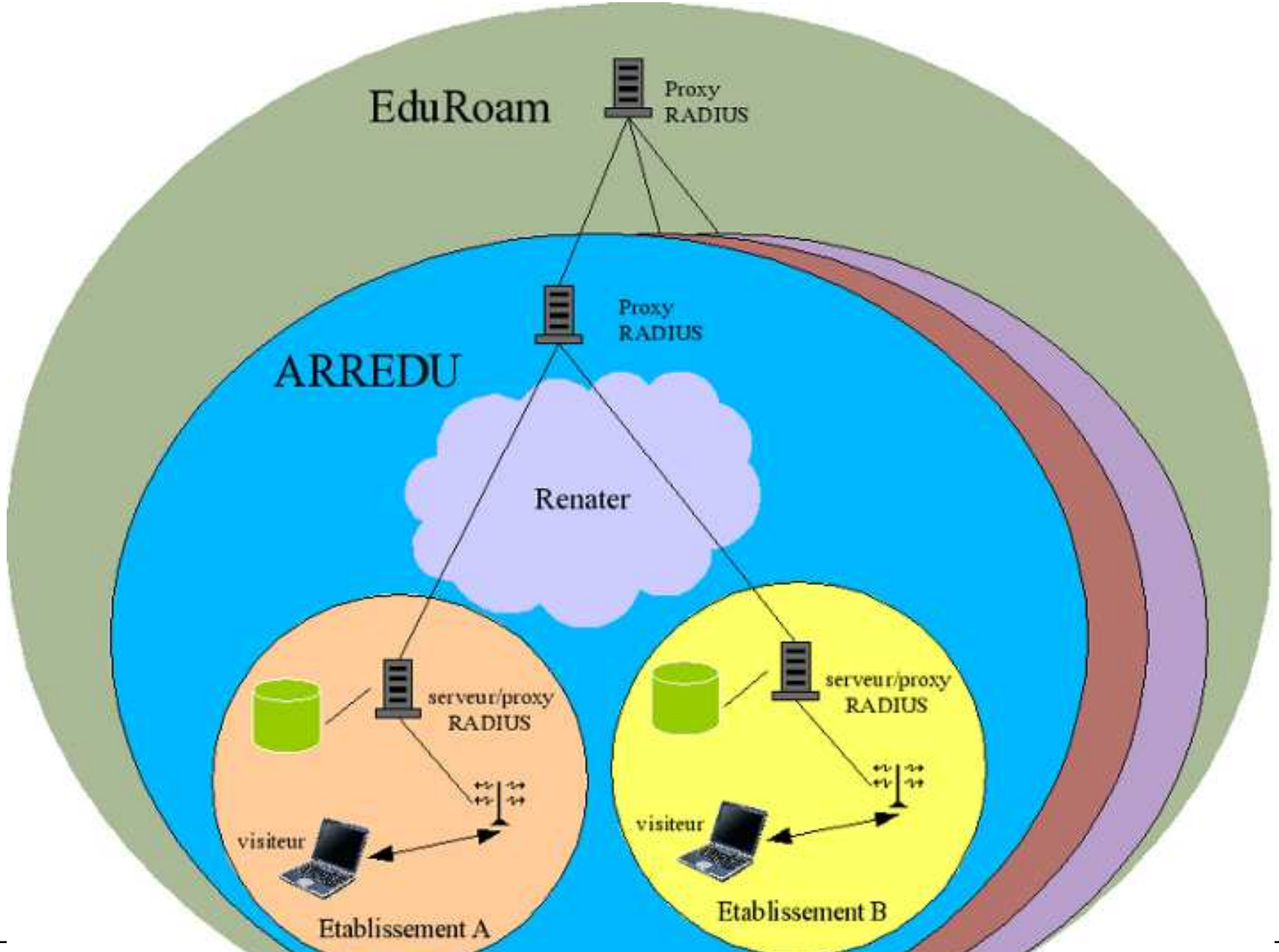
Architecture

- Mixte IPv4 / IPv6
- Adressage privé IPv4 sur plusieurs sous-réseaux
  - DHCP
- Adressage public d’une partie des serveurs
  - IPv4 via NAT 1:1
  - IPv6 statique
- Adressage IPv6 public pour toutes les machines
  - rtadvd, dhcp6s

WiFi Eduroam



WiFi Eduroam



Filtrage Eduroam

- HTTP et HTTPS
- DNS
- ICMP
- IPSec (ESP, AH, IKE)
- OpenVPN
- SSH
- POPs
- IMAPs
- SMTPS
- NTP

Wifi Unicaen et ex Dept-info

- Unicaen : non sécurisé, service limité au http(s) via proxy
  - un bon pirate saura passer au travers
- Mutualisation des bornes WiFi courant 2008 avec le CRISI.
- Dept-info n’existe plus depuis 2010 sauf :
  - besoin pour les robots (équipe MAD)

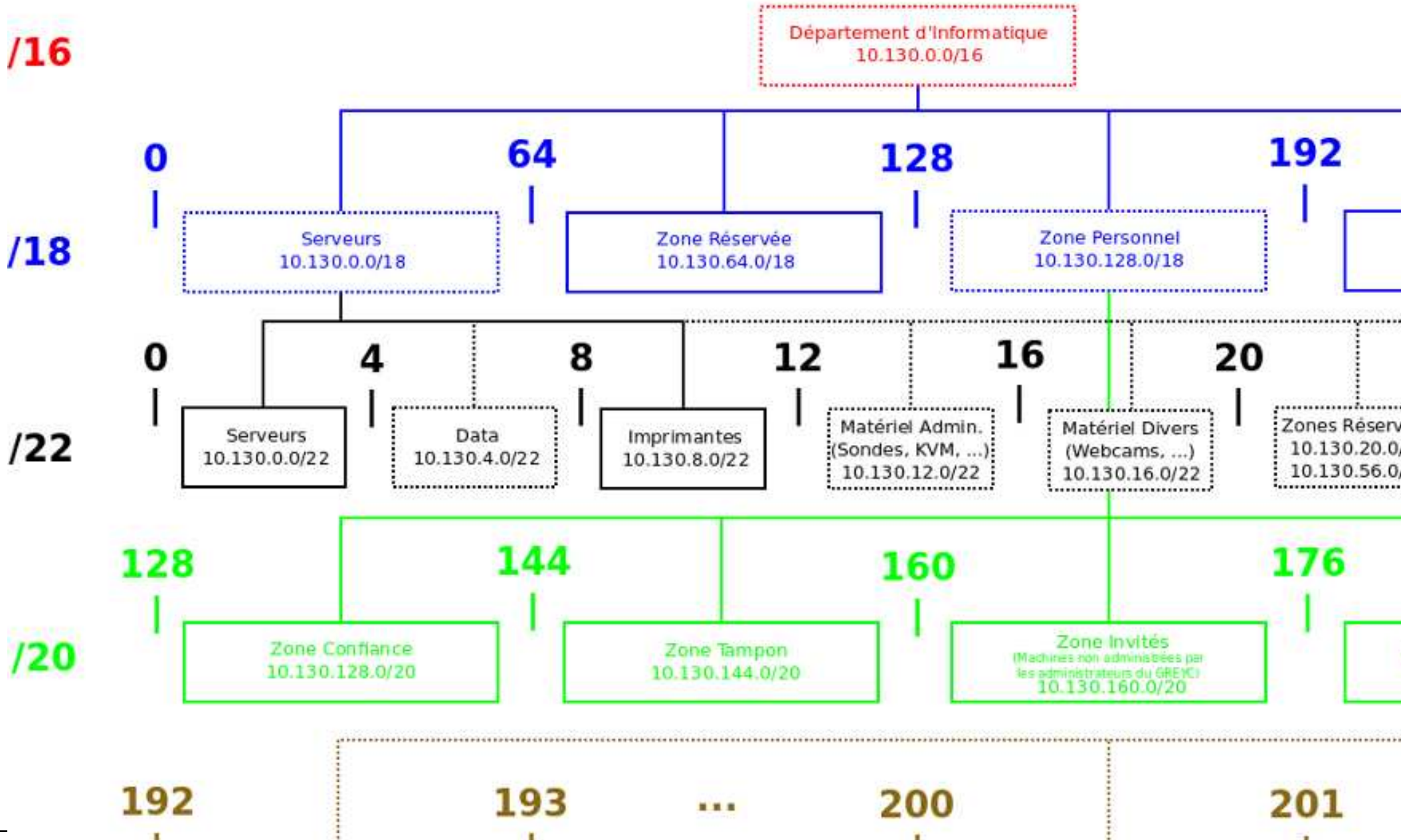
Adressage IPv4

- Différents réseaux pour différentes utilisations
  - architecture hiérarchique : découpage en sous-réseaux (subnetting)

- 5 zones principales :
  - 10.130.0.0/18 : les serveurs
  - 10.130.64.0/18 : réservé pour usage futur
  - 10.130.128.0/18 : partie recherche
  - 10.130.192.0/18 : zone enseignement
  - 193.55.128.0/24 : adressage public et DMZ

- Redécoupage des zones selon utilisation
  - Taille des sous-réseaux variables

Adressage IPv4



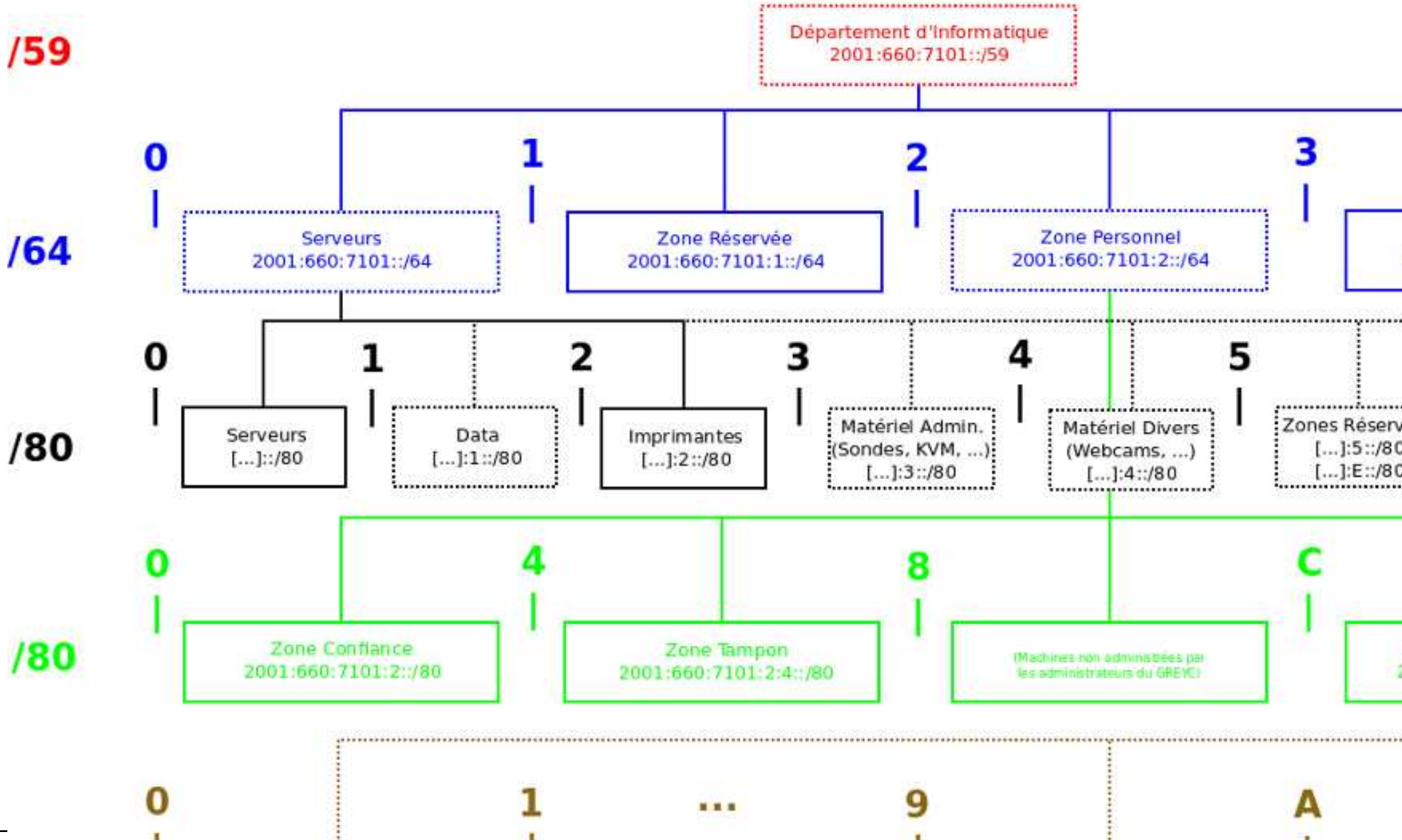
Adressage IPv4 public et DMZ

- Une classe C publique pour le département, découpée en 2 :
  - partie inférieure (<128) : adressage public
  - partie supérieure (>127) : DMZ
- Une adresse par service ou type de service
- Le minimum de services
- Le minimum d’adresses possible
- Filtrage ad-hoc entrée ET sortie

Adressage IPv6

- 2001:660:7101::/48 pour l'université
- 2001:660:7101::/59 pour le département informatique
  - soient les réseaux 2001:660:7101::/64 à 2001:660:7101:1f::/64
- Architecture réseau calquée sur l'IPv4
  - découpage en zones principales
  - adressage beaucoup plus large !

Adressage IPv6



Routage

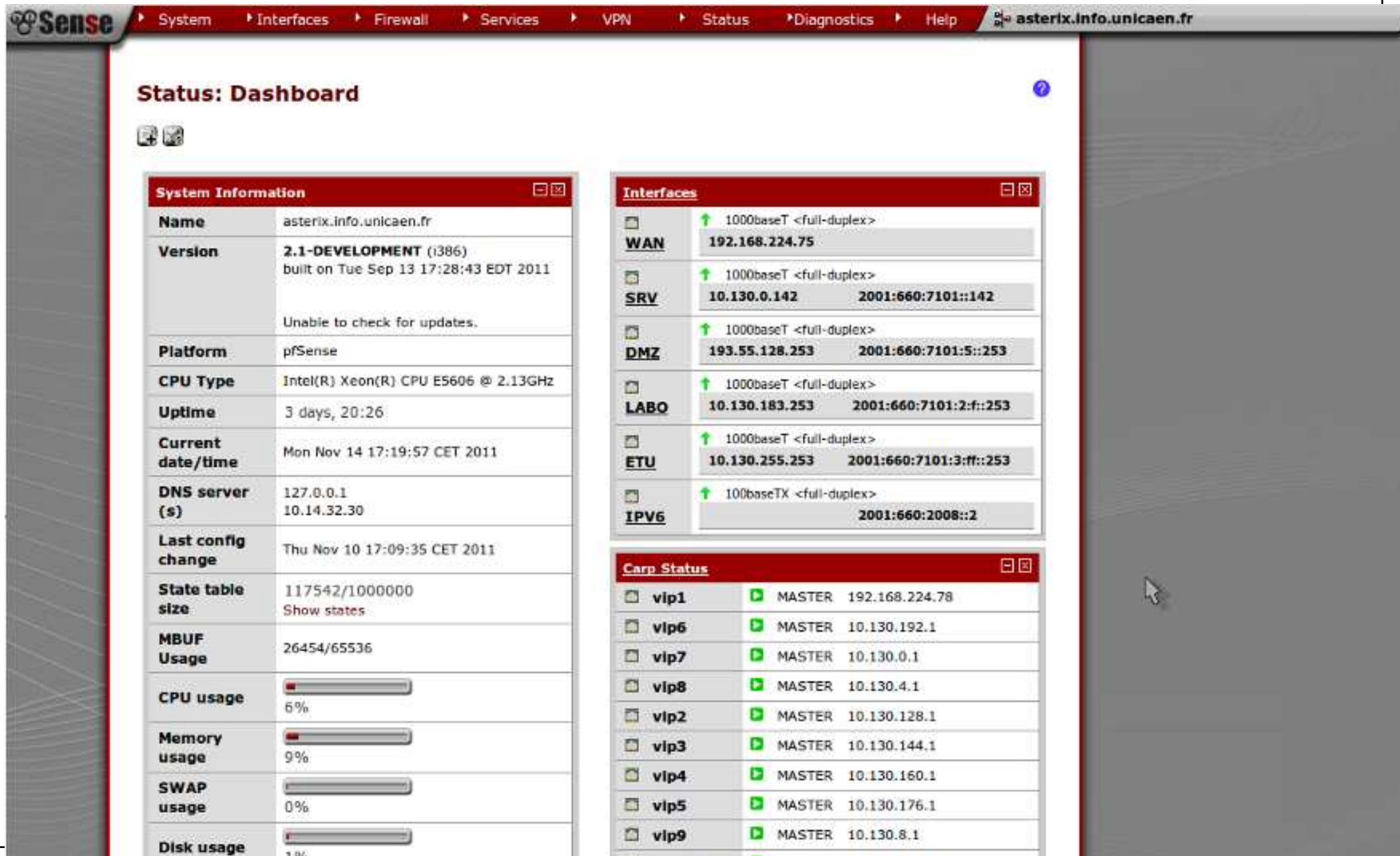
- Routage géré par 2 routeurs / firewalls redondants
  - routeurs sous pfSense (distribution FreeBSD)
  - redondance via CARP
  - synchronisation des états à l’aide de pfSync

- Le routage est complètement statique pour IPv4 et IPv6
  - exception faite des réseaux de TP en IPv6, gérés dynamiquement avec ripng

pfSense

- Distribution libre FreeBSD pour routeurs / firewalls
- Interface Web en PHP
- Configuration de l'ensemble du système :
  - interfaces / adresses IPs
  - redondance des firewalls
  - règles de pare-feu
  - traduction d'adresse
  - services annexes :
    - serveur ou relai DHCP(v6)
    - forwarder DNS
    - systèmes de VPN (OpenVPN, PPTP, IPSec)
    - Wake On LAN, SNMP, RIP, NTPd, ...

pfSense


pfSense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
asterix.info.unicaen.fr
Status: Dashboard
System Information
Name
asterix.info.unicaen.fr
Version
2.1-DEVELOPMENT (i386)
built on Tue Sep 13 17:28:43 EDT 2011
Unable to check for updates.
Platform
pfSense
CPU Type
Intel(R) Xeon(R) CPU E5606 @ 2.13GHz
Uptime
3 days, 20:26
Current date/time
Mon Nov 14 17:19:57 CET 2011
DNS server (s)
127.0.0.1
10.14.32.30
Last config change
Thu Nov 10 17:09:35 CET 2011
State table size
117542/1000000
Show states
MBUF Usage
26454/65536
CPU usage
6%
Memory usage
9%
SWAP usage
0%
Disk usage
Interfaces
WAN
1000baseT <full-duplex>
192.168.224.75
SRV
1000baseT <full-duplex>
10.130.0.142
2001:660:7101::142
DMZ
1000baseT <full-duplex>
193.55.128.253
2001:660:7101:5::253
LABO
1000baseT <full-duplex>
10.130.183.253
2001:660:7101:2:f::253
ETU
1000baseT <full-duplex>
10.130.255.253
2001:660:7101:3:ff::253
IPV6
100baseTX <full-duplex>
2001:660:2008::2
Carp Status
vip1 MASTER 192.168.224.78
vip6 MASTER 10.130.192.1
vip7 MASTER 10.130.0.1
vip8 MASTER 10.130.4.1
vip2 MASTER 10.130.128.1
vip3 MASTER 10.130.144.1
vip4 MASTER 10.130.160.1
vip5 MASTER 10.130.176.1
vip9 MASTER 10.130.8.1

Filtrage IPv4

- Politique par défaut : rien ne passe !
- Basé sur l’appartenance à un des sous-réseaux
  - droits par zone
  - hiérarchique
- Journalisation de toutes les connexions refusées (entrantes ET sortantes)
  - centralisé sur un serveur de logs
- Quelques règles temporaires (exceptions par machine)
  - nettoyage de temps en temps

Filtrage IPv6

- Politique par défaut : rien ne passe non plus !
- Droits calqués sur les règles IPv4 :
  - mêmes groupes / zones
  - mêmes autorisations
- Blocage de l’accès direct aux machines

Protection des services

- Utilisation de fail2ban sur les services ssh
  - diminution des risques liés aux attaques par dictionnaire
- Limitation du nombre de connexions entrantes sur tous les services
- Les machines avec services ont moins d’accès vers l’extérieur que les autres
  - la plupart des attaques ayant besoin d’un accès externe sont ainsi mises en échec

WebDNS

- Application WEB gérant les données IP des machines
  - gestion du DNS privé
  - configuration DHCP

- Hébergé par le CRISI
  - serveurs redondants
  - haute disponibilité

WebDNS

WebDNS

APPLICATION WEBDNS

WEBDNS V1.5

- ACTIONS
  - Accueil
  - Consulter
  - Ajouter
  - Supprimer
  - Modifier
  - Plages DHCP
  - Rechercher un correspondant
  - Où suis-je ?
- VOIR AUSSI
  - CRISI

Liste des adresses declarees

Liste au 15/11/2011 10h51.

Adresses declarees (IPv4 + IPv6) : 1430

Adresse IP	Noms et alias	Adresse MAC	Profil DHCP	Systeme	Structure	Commentaire
10.130.128.10	aglae.info.unicaen.fr	00:19:99:27:7c:80	Dptinf-perso-confiance	Ordinateur de bureau sous Linux	--->Groupe de Recherche en Informatique,Image,Automatique et Instrumentation de Caen (GREYC/U) [UMR 6072]	Johann Brault-Baron:S3-388:u64:syst
10.130.128.11	aladin.info.unicaen.fr	00:25:4b:c5:66:32	Dptinf-perso-confiance	Ordinateur portable Mac	--->Groupe de Recherche en Informatique,Image,Automatique et Instrumentation de Caen (GREYC/U) [UMR 6072]	Patrice Enjalbert:S3-385
10.130.128.12	albinoni.info.unicaen.fr	64:b9:e8:bd:9b:46	Dptinf-perso-confiance	Ordinateur de bureau Mac	--->Groupe de Recherche en Informatique,Image,Automatique et Instrumentation de Caen (GREYC/U) [UMR 6072]	Frederic Jurie:S3-203:M
10.130.128.13	amacc.info.unicaen.fr	00:24:81:02:5b:53	Dptinf-perso-confiance	Ordinateur portable sous Linux	--->Groupe de Recherche en Informatique,Image,Automatique et Instrumentation de Caen (GREYC/U) [UMR 6072]	portable laboratoire equi amacc:S3-356:Ubuntu:
10.130.128.14	ambre.info.unicaen.fr	00:19:99:28:04:57	Dptinf-perso-confiance	Ordinateur de bureau sous Linux	--->Groupe de Recherche en Informatique,Image,Automatique et Instrumentation de Caen (GREYC/U) [UMR 6072]	Alain Bretto:S3-386:u64
10.130.128.15	ambroise.info.unicaen.fr	00:19:99:28:0e:8e	Dptinf-perso-confiance	Ordinateur de bureau sous Linux	--->Groupe de Recherche en Informatique,Image,Automatique et Instrumentation de Caen (GREYC/U) [UMR 6072]	Samir Loudni:S3-385:u

DNS public

- 2 serveurs (master / slave)
  - slaves externes supplémentaires
- Servent la zone publique
  - adresses IP des services publics et machines DMZ
  - champs A et AAAA (IPv4 et IPv6)
- Quelques zones "hébergées" gracieusement (en tant que secondaire et/ou primaire)

Services web

- www : le site du département
  - hébergement de sites tiers (jfpc, biblio-fr, afrif, gdr-im ...)
- users.greyc.fr : les pages personnelles des utilisateurs du laboratoire
  - https://login.users.greyc.fr/
  - version ITK d'apache (UID de l'utilisateur)
  - utilisé par les enseignants / chercheurs
- users.info.unicaen.fr : les pages personnelles des utilisateurs du d épartement
  - http://login.users.info.unicaen.fr/
  - version ITK d'apache (UID de l'utilisateur)
  - très sollicité par les formations webmestre et ingénierie de l'internet

Services web

- proxy cache + filtrage
  - serveur proxy de l'université
- Serveurs variés sur machines virtuelles à la demande
  - zope+plone, tomcat, eXist...
- Projets spécifiques :
  - projet-si pour les m2-radis
  - projets de recherche
  - ...

Service mail

- Service d’archivage mail pour les enseignants-chercheurs
- Dovecot + authentification LDAP
  - mot de passe unifié PersoP@ss
  - pas de quota
- Listes de diffusion SYMPA pour le laboratoire
- Domaines supplémentaires hébergés :
  - gdr-im.fr
  - guibray.org
  - ...

Services BDD

- Bases de données
  - MySQL (jusqu’à 10 bases par utilisateur)
  - PostgreSQL

- Bases locales sur les serveurs en ayant besoin
  - MySQL sur machine www (http)
  - PostgreSQL pour les services de log et de supervision

Machines de calcul

- Machines à 4 processeurs
  - cody, appo : 4x16core, 256G RAM (calculs)
  - rex, fox : 4x12core, 256G RAM (calculs)
  - sully : 4x4core, 64G RAM (calculs)
- Machines à 2 processeurs
  - roadrunner : Dual Core AMD Opteron (passerelle)
- Ces machines disposent de 4Go à 256Go de mémoire vive

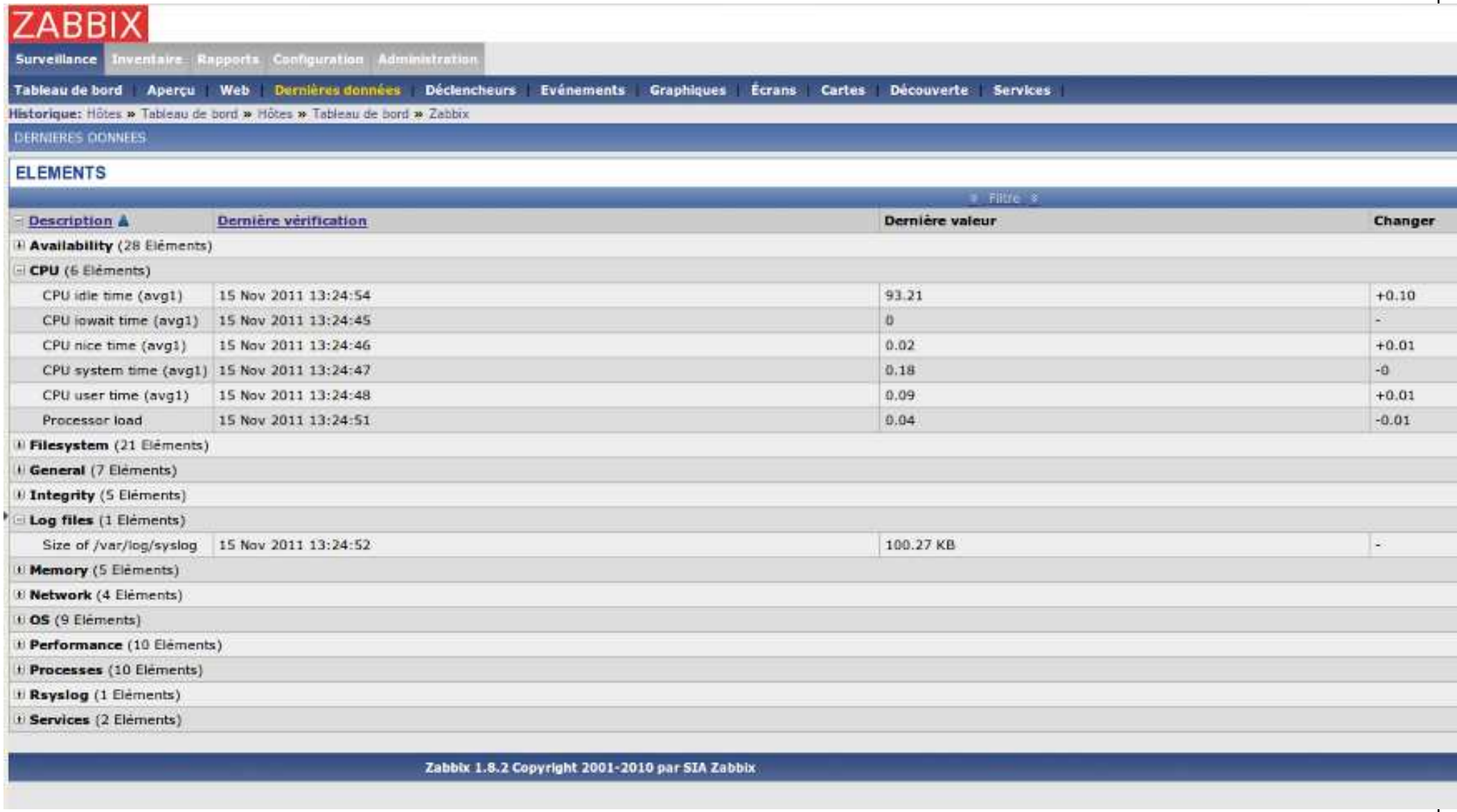
Supervision

- Zabbix
  - machines / serveurs
  - espace disque disponible
  - interfaces réseau
  - charge cpu / mémoire
  - utilisateurs / processus
  - accès aux services

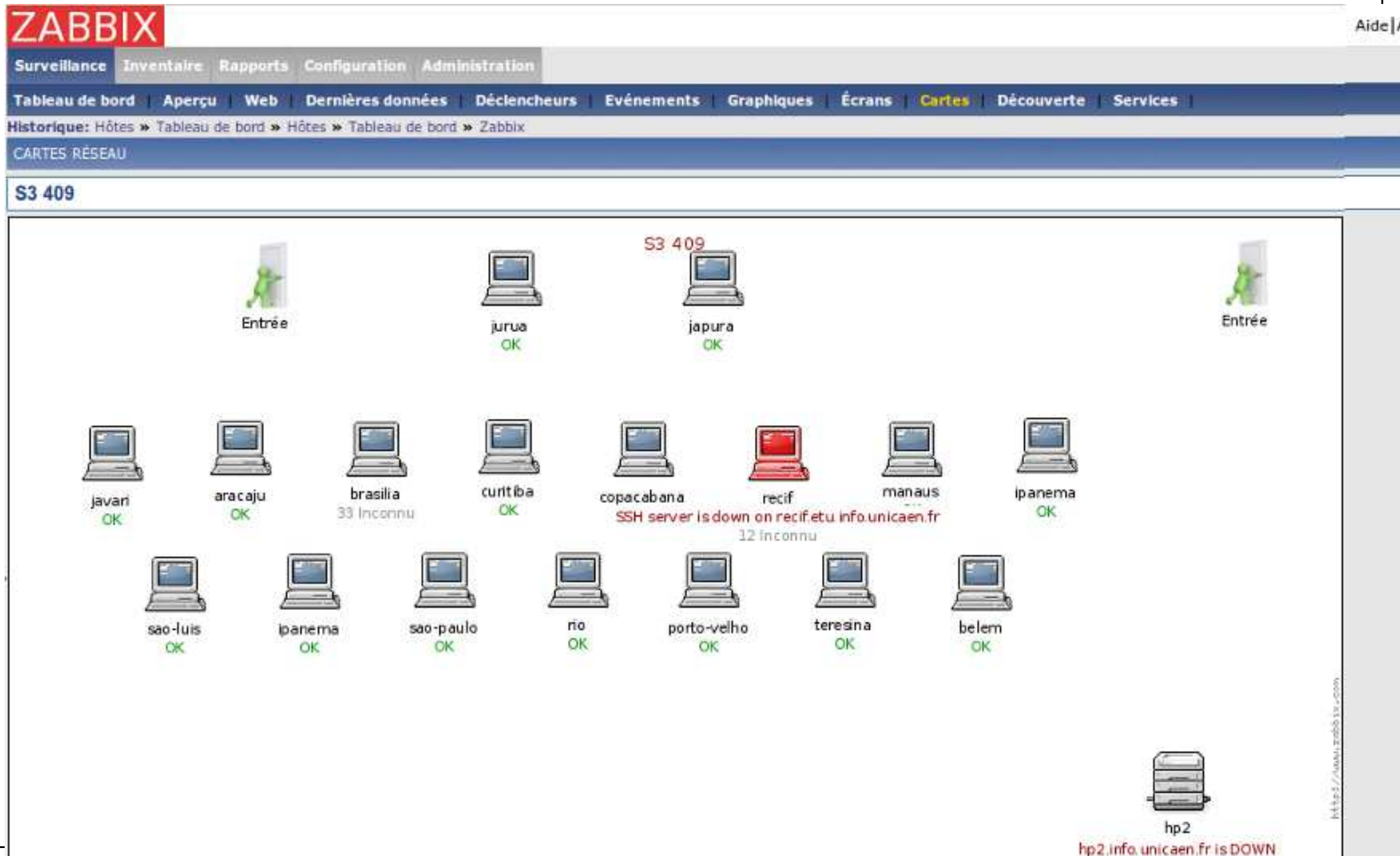
- Agent sur les machines clonées

Zabbix: exemples

Zabbix: données



Zabbix: carte



Politique de sécurité

- Personne n’est administrateur de sa machine de bureau
  - exception faite des portables
- Mises à jour fréquentes
  - mises à jour de sécurité automatiques (unattended-upgrades)
  - clonage fréquent des machines
  - une grande partie des machines a en permanence moins de 6 mois

Installations et mises à jour

- Proxy cache pour les paquets debian
- Système de "clonage" des Linux
  - systemimager
  - couplé à bittorent
  - activé au boot réseau
- Simulation d’update de sécurité tous les jours
  - sur tous les serveurs
  - sur l’image principale systemimager
  - avertissement par mail
- Clonage des Mac OS X par logiciel ad-hoc + netboot

Sécurité sur les postes de travail

- BIOS
- Bootloader
- Chiffrements
- Console d’administration
- Clonage

Sauvegarde / Archivage

Les serveurs

- Raid logiciel niveau 1 sur tous les serveurs
  - 2 hdd identiques nécessaires
- Sauvegarde incrémentale sur baie de disques raid
  - via rsync+ssh
  - problème du owner
- Versionning de la configuration
  - Etckeeper + Bazaar
  - suivi des modifications

Sauvegarde / Archivage

Les données utilisateur

- 1 baie raid

- Sauvegarde incrémentale
  - quotidien sur 15 jours
  - hebdomadaire sur 4 semaines
  - mensuelle sur 1 an

Services Réseau Avancés

- Fournisseur d’accès IPv6 pour l’IUT c3 et le CERTIC
- Multicast IPv6 lors de conférences
- TP Réseau
  - Infrastructure pour les TPs
- OpenVPN
  - Quelques clients pour le moment (~ 10)
  - Zone réseau dédiée

OpenVPN

- Sous-réseau dédié 10.130.152.0/21
  - partie du sous réseau "Tampon" (10.130.144.0/20)
- Destiné aux machines personnelles des enseignants/chercheurs
- Utilisation de certificats signés par notre autorité
  - notre autorité est auto certifiée

Autres services divers

- Forge
- Serveur de temps
- Serveurs SAN redondants
- Serveur d’impression
- ...

Questions

Des questions ?