Administration d'un parc de matériels actifs (routeurs/commutateurs)

Emmanuel Halbwachs

Observatoire de Paris
Division informatique

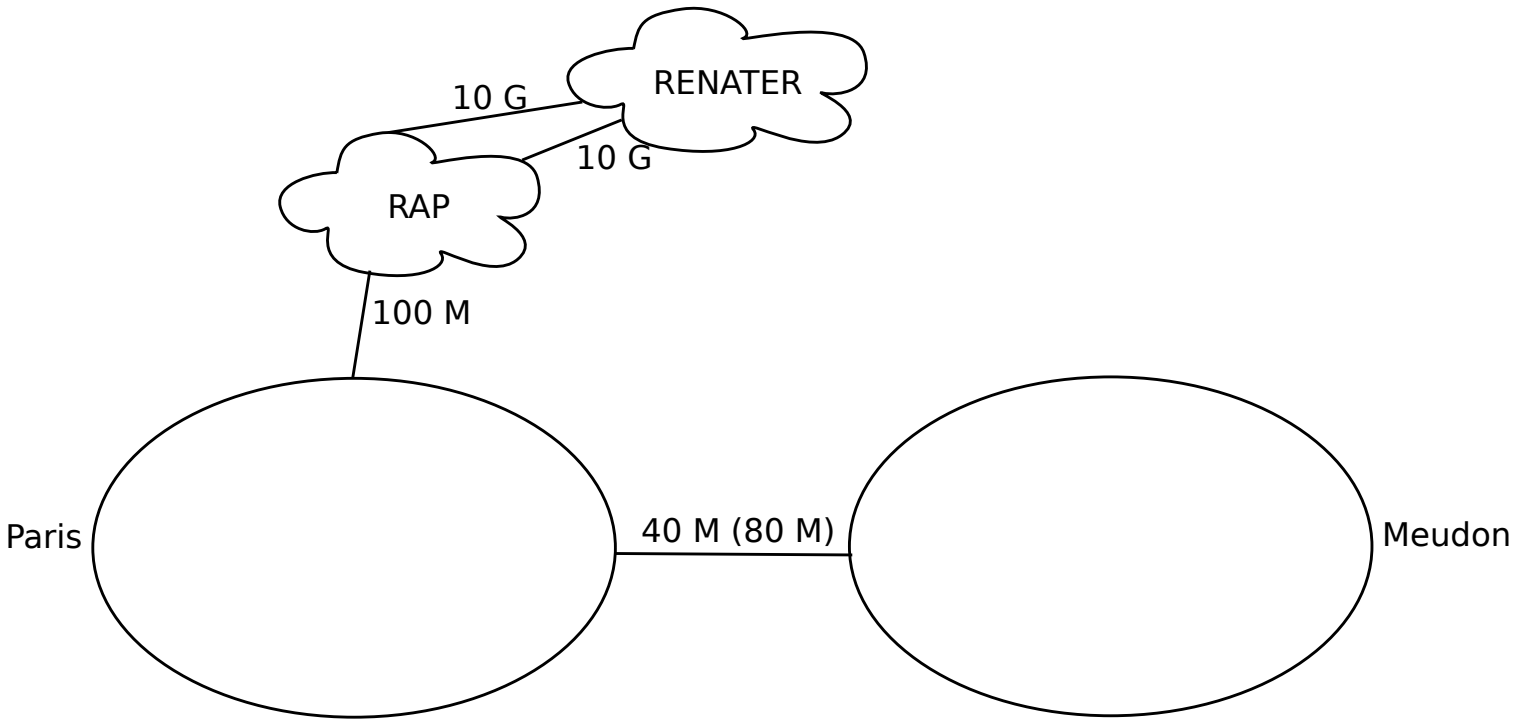
Journées Mathrice
05/10/2010

Outline

En chiffres

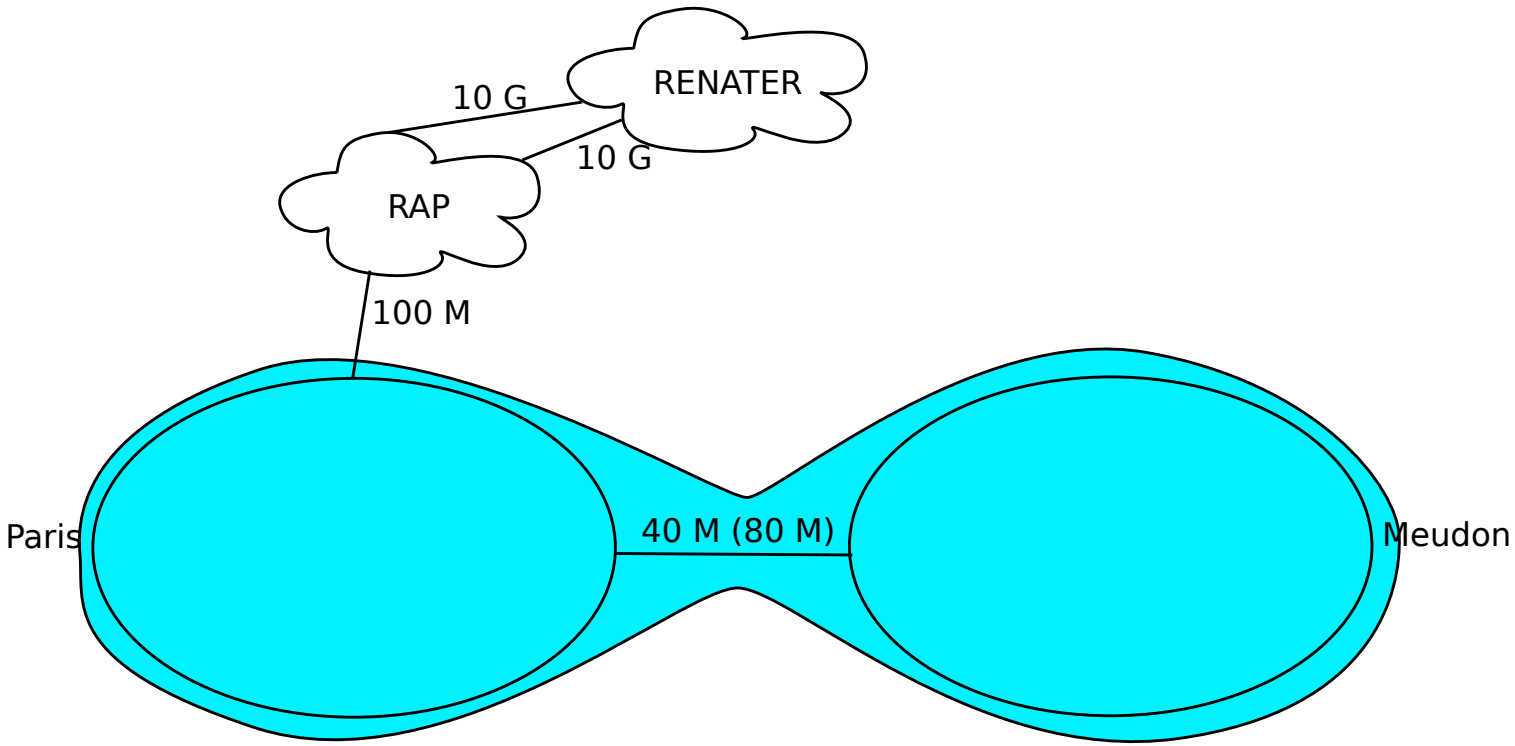
Date	accès MAN	LAN	VLAN	sous-réseaux
2006	1	1	1	1
2007-2008	1	1	1	50
2008	2	2	2	50
2010	2	2	50	50
2011	3	2	50	50

(1/12) Situation initiale : 2 sites



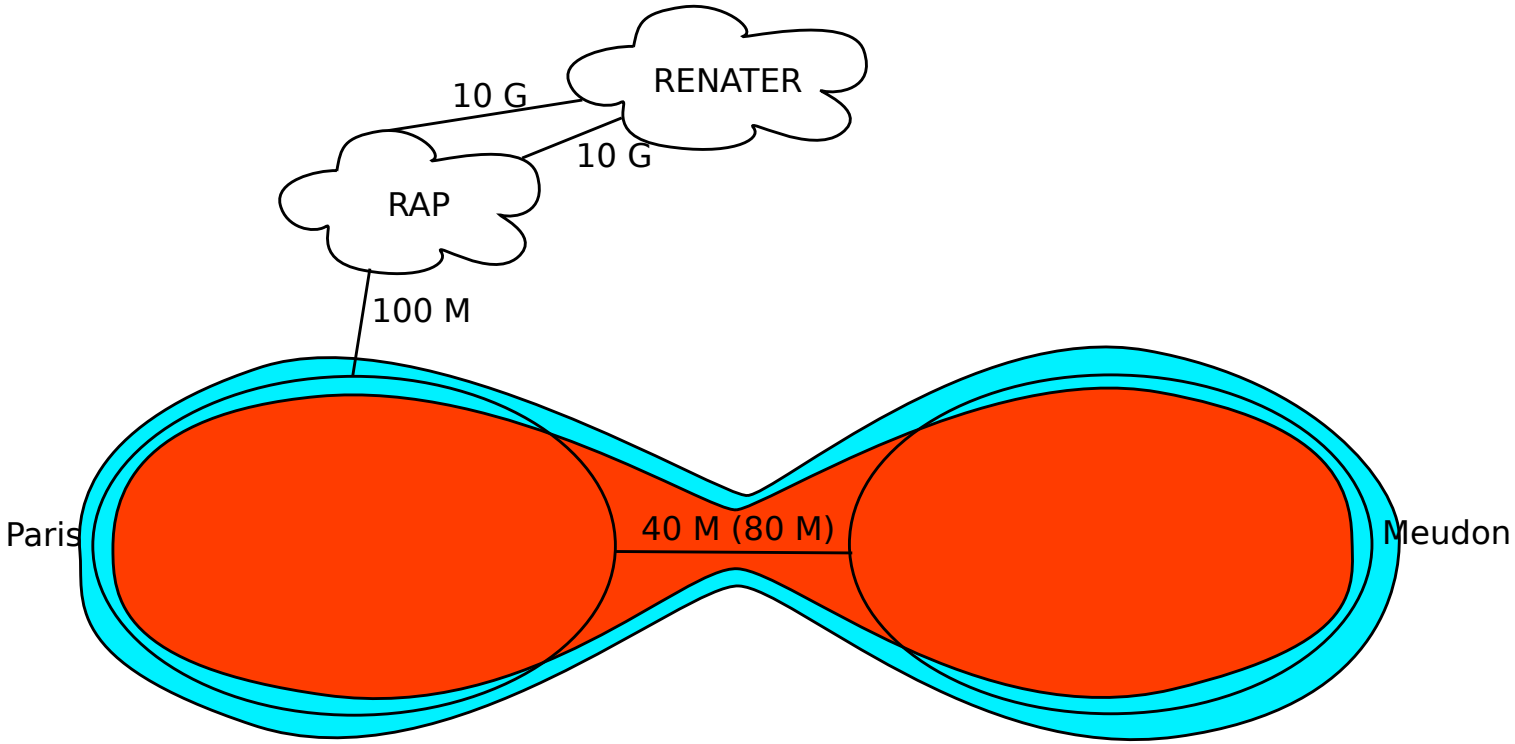
01/2006 :

(2/12) 2 sites mais 1 LAN, 1 VLAN



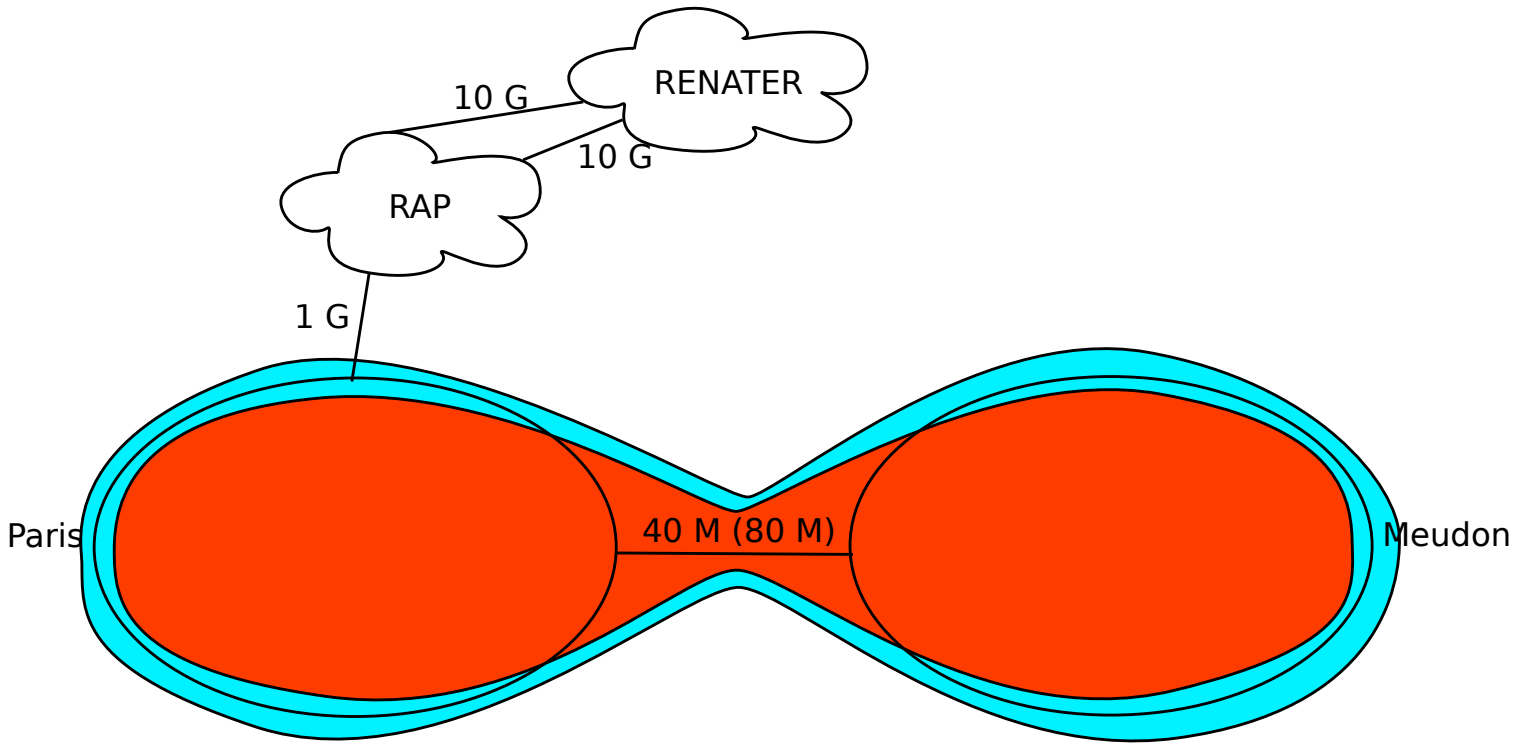
01/2006 : 1 VLAN,

(3/12) Et 1 sous-réseau /16 à plat...



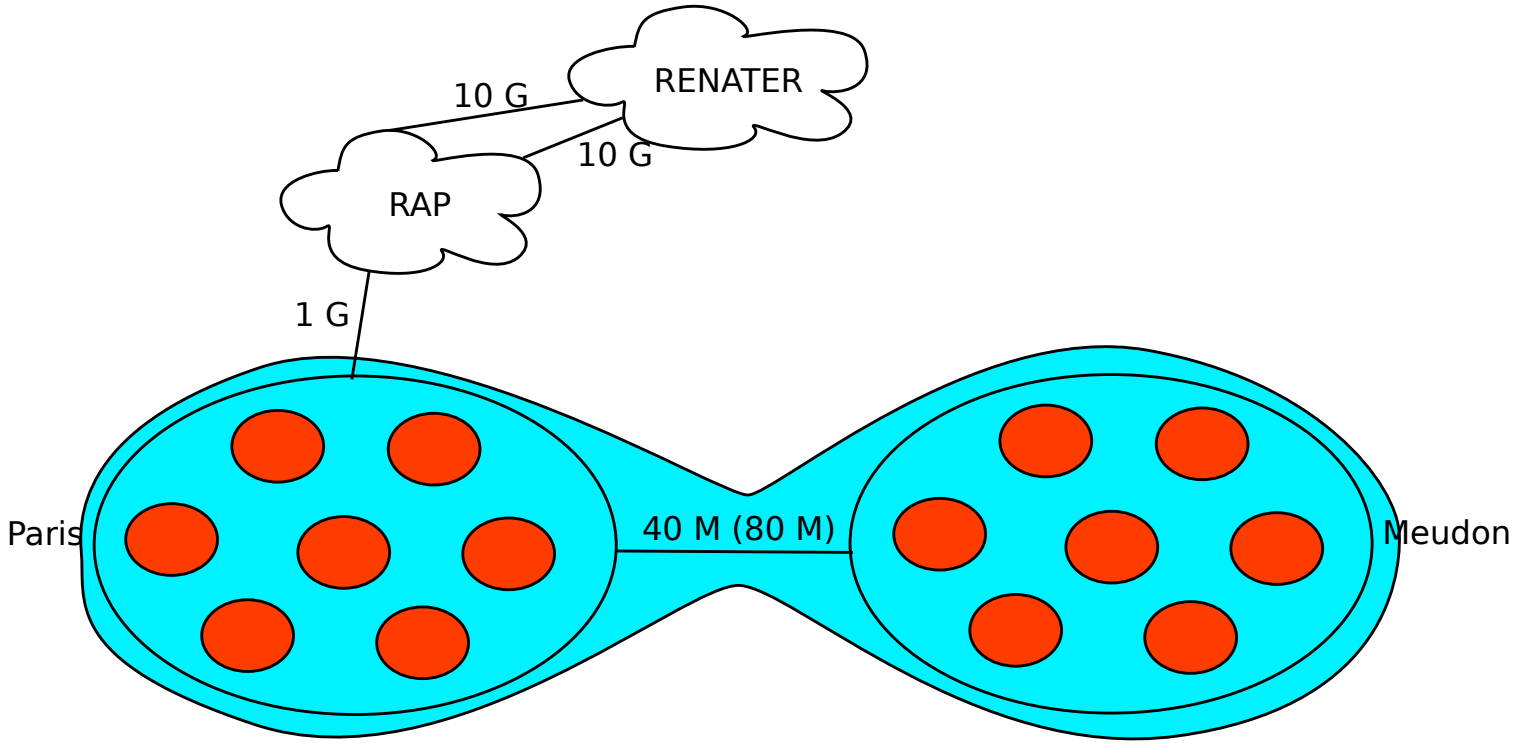
01/2006 : 1 VLAN, 1 sous-réseau

(4/12) Changement de routeur, sortie 100 M → 1 G



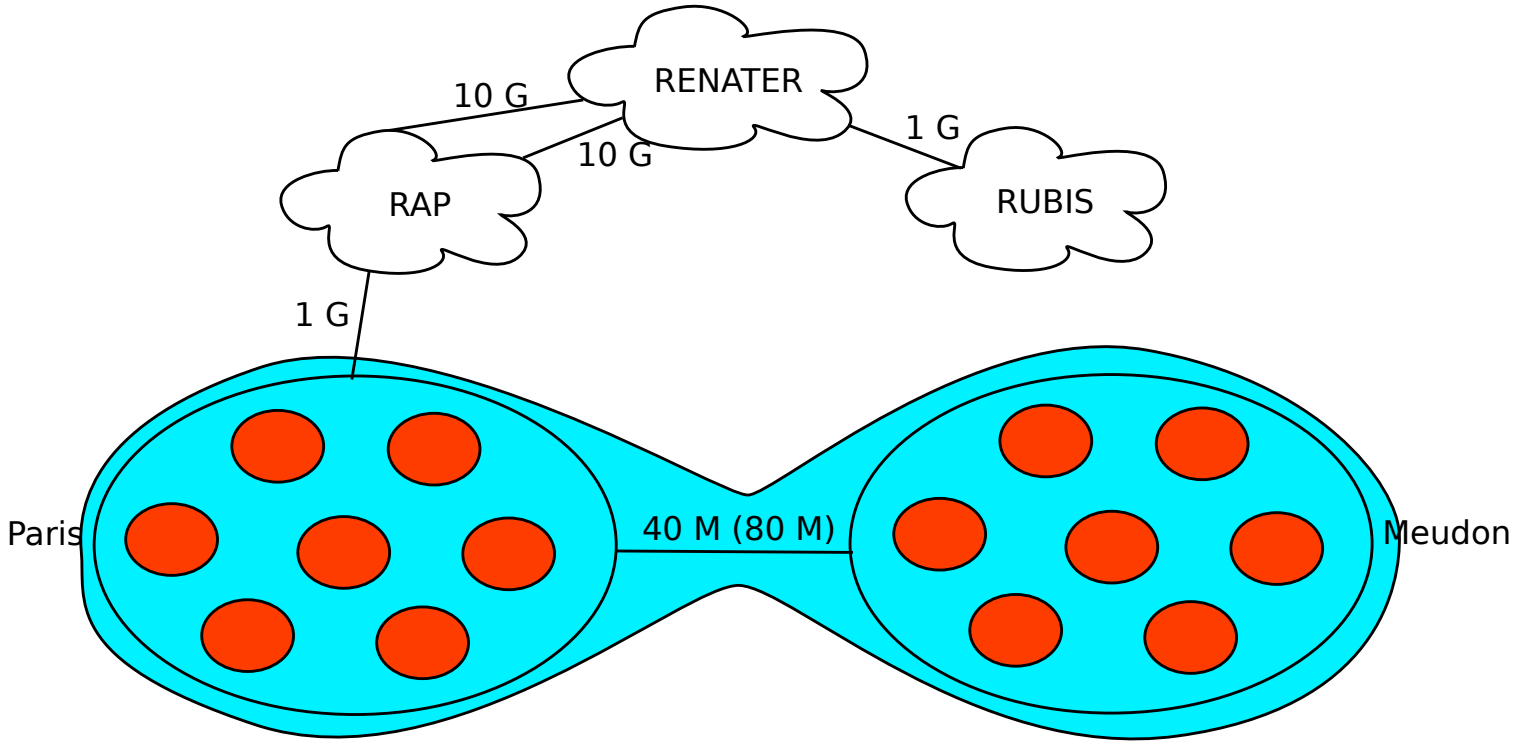
01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G

(5/12) Très gros travail de renumérotation/segmentation IP



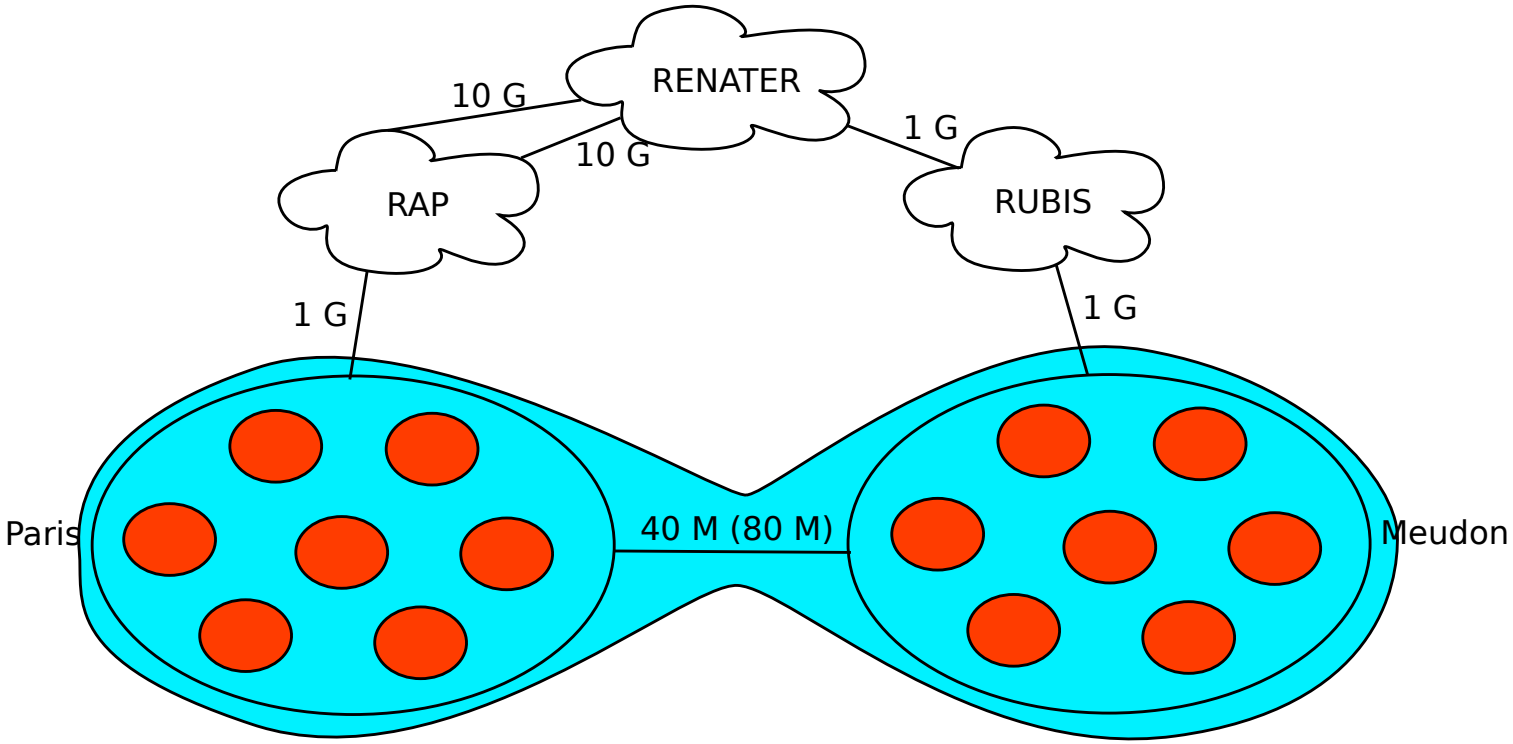
01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

(6/12) Arrivée du MAN Rubis à 1 km de Meudon



01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

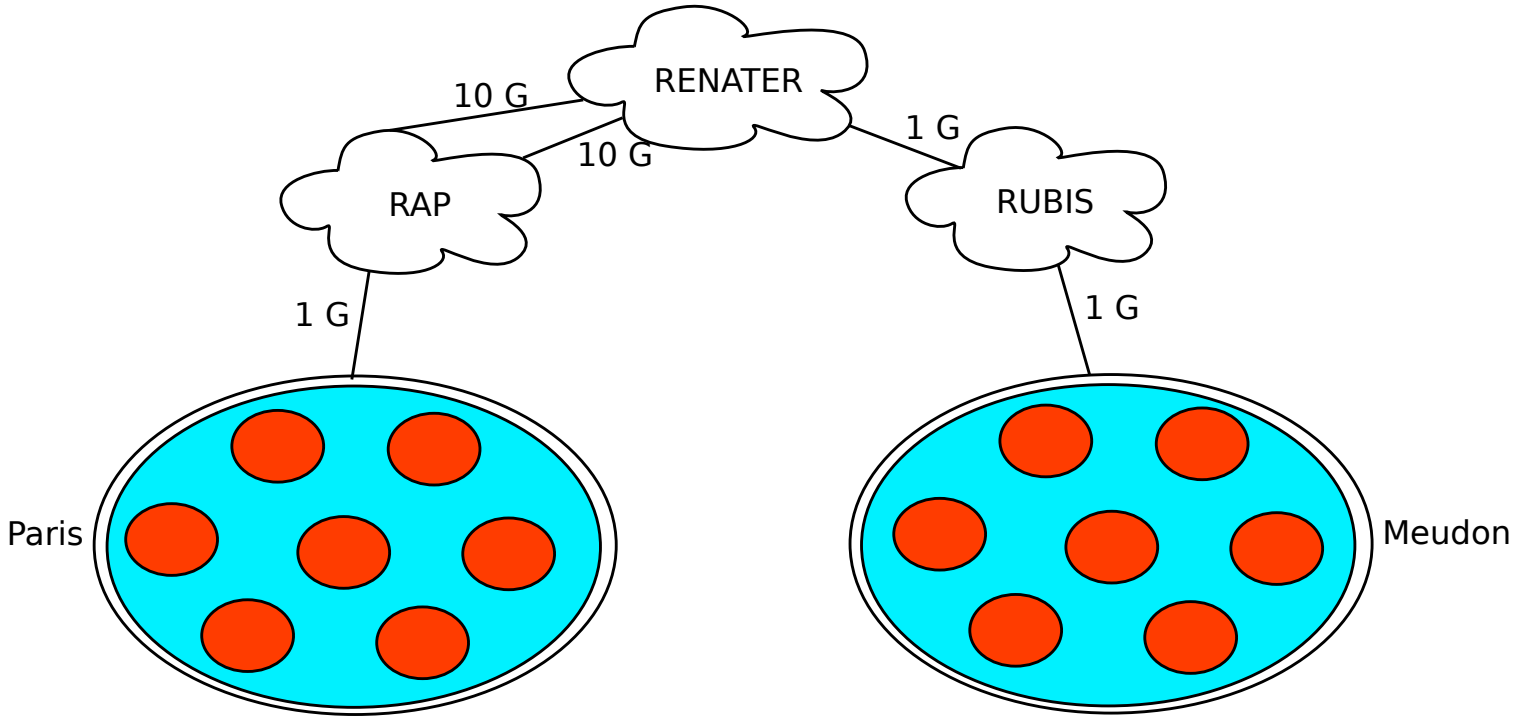
(7/12) Connexion à Rubis à 1 G



01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

04/2008 : RUBIS 1 G,

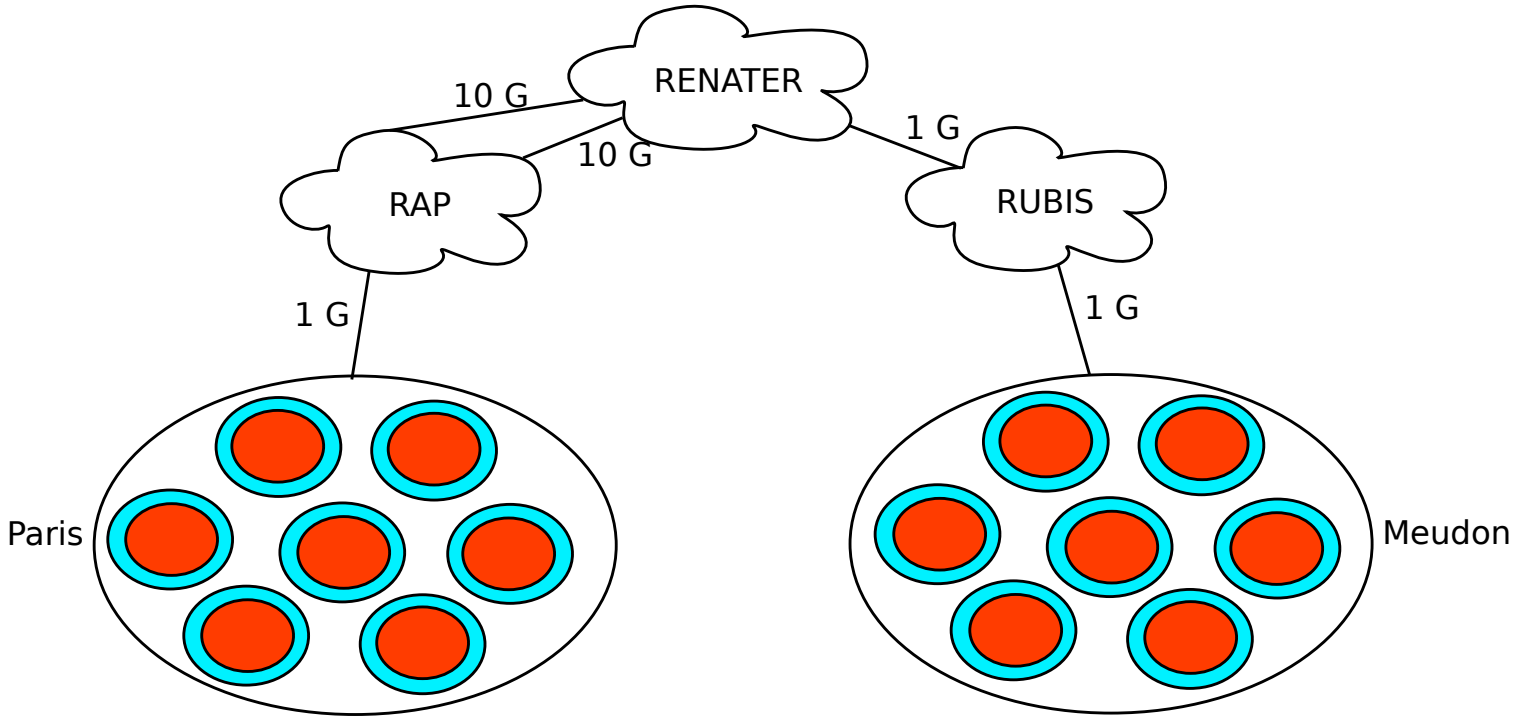
(8/12) Résiliation InterLAN → 2 LAN distincts



01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

04/2008 : RUBIS 1 G, 2 VLAN

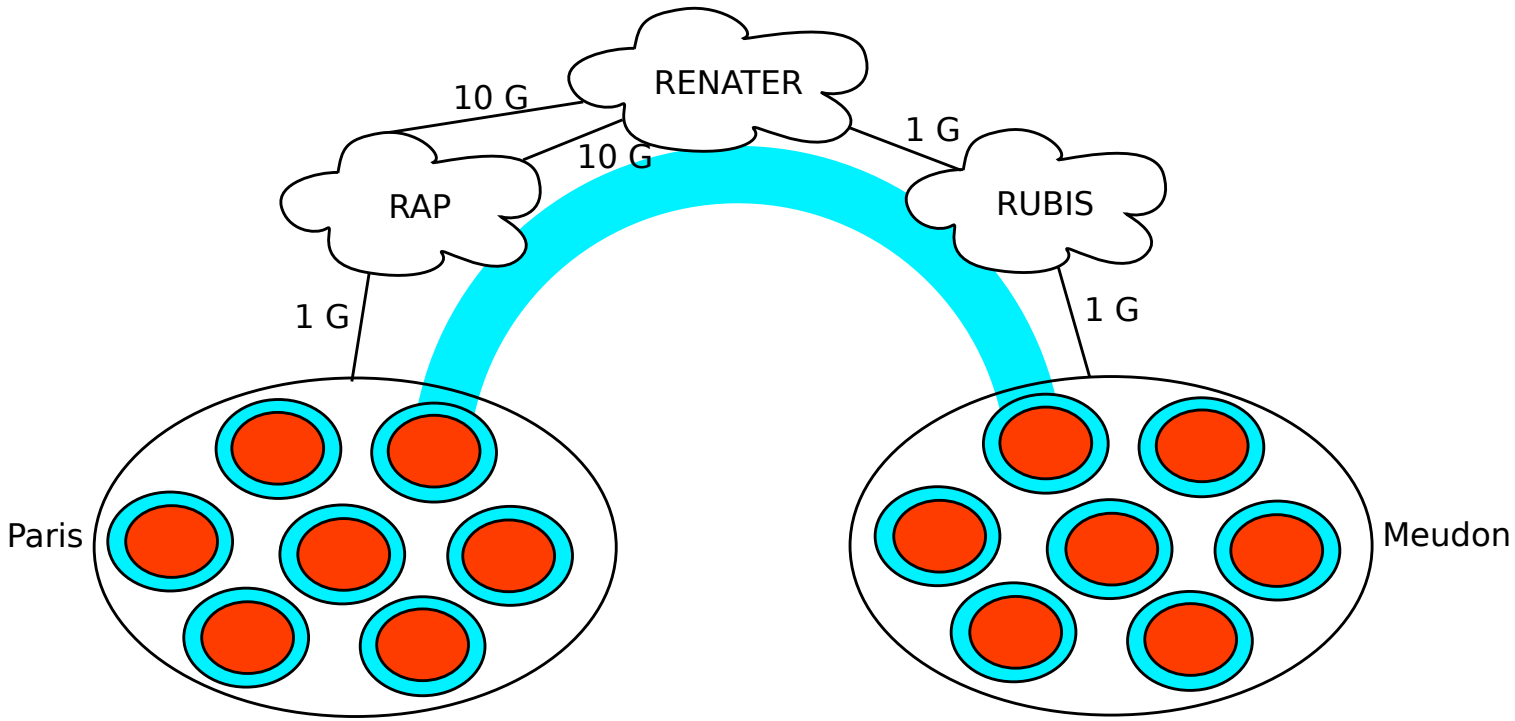
(9/12) Gros travail de segmentation en VLAN



01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

04/2008 : RUBIS 1 G, 2 VLAN
06/2010 : 50 VLAN

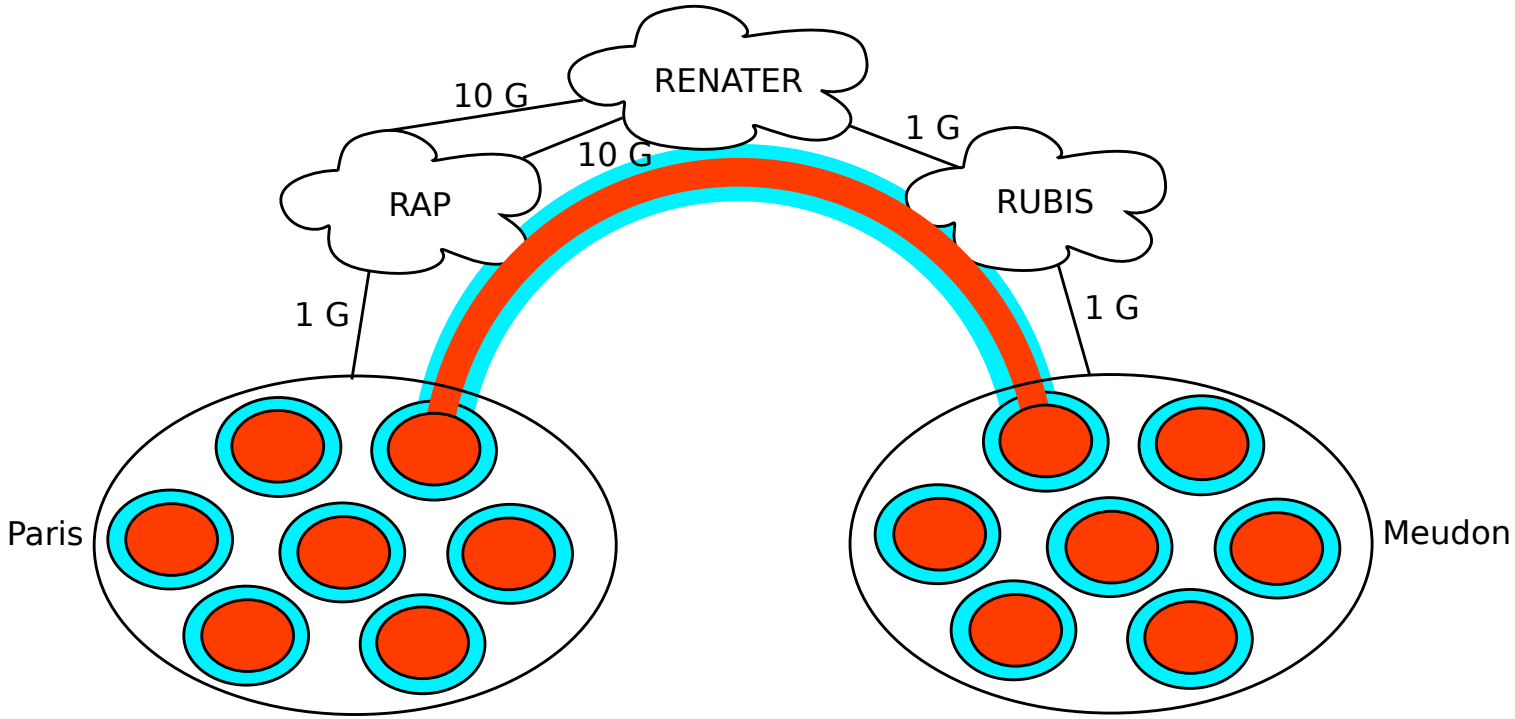
(10/12) L2 VPN



01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

04/2008 : RUBIS 1 G, 2 VLAN
06/2010 : 50 VLAN
Bonus : L2 VPN

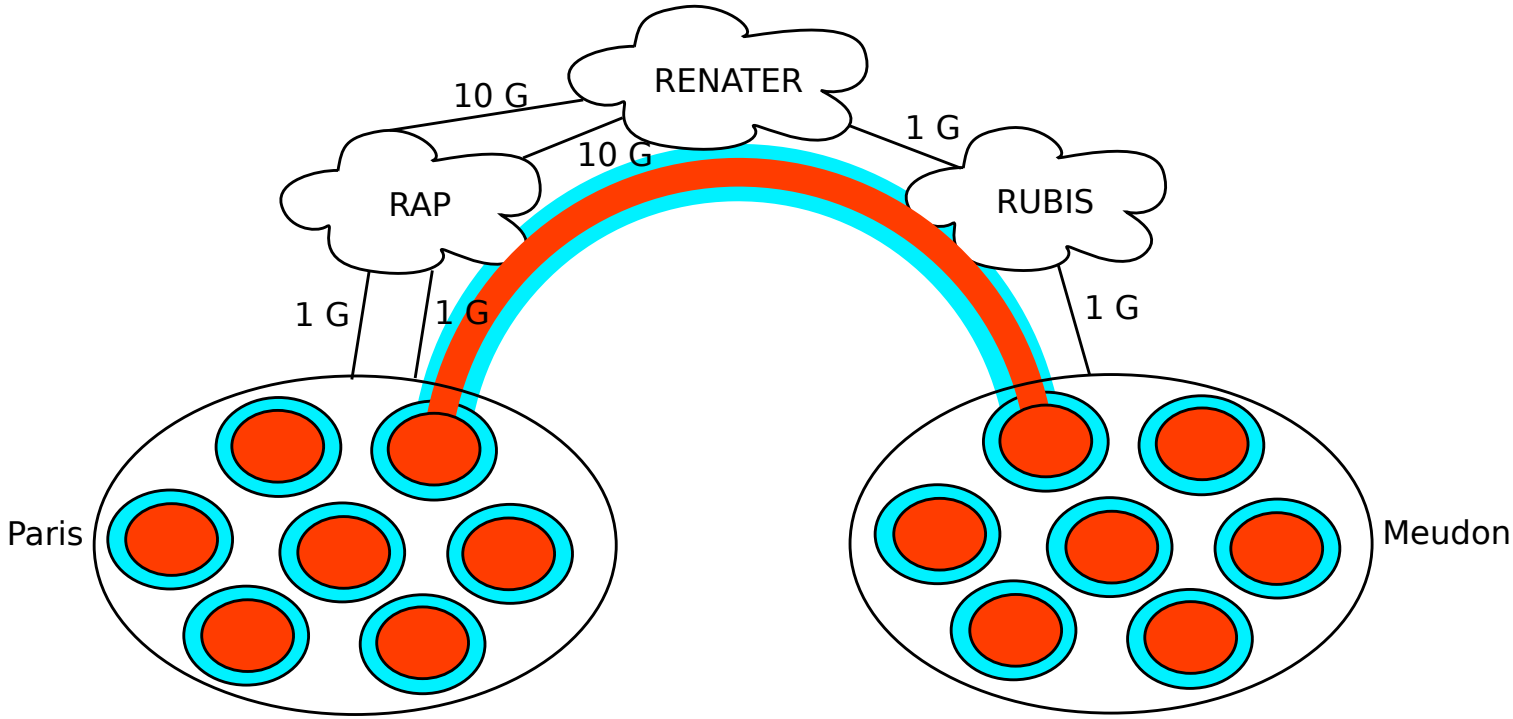
(11/12) Un sous-réseau IP à cheval sur les 2 sites



01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

04/2008 : RUBIS 1 G, 2 VLAN
06/2010 : 50 VLAN
Bonus : L2 VPN

(12/12) Bientôt : raccordement à RAP doublé (actif/passif)



01/2006 : 1 VLAN, 1 sous-réseau
12/2006 : RAP 100 M -> 1 G
02/2008 : 50 sous-réseaux

04/2008 : RUBIS 1 G, 2 VLAN
06/2010 : 50 VLAN
Bonus : L2 VPN
12/2010 : RAP fiabilisé

Emploi précédent (LPN, 150 pers)

- 1 routeur + 13 commutateurs
- très homogène
  - 1 marque (Foundry), 1 OS
  - 2 modèles, 2 versions d'OS
- architecture stable (locaux neufs)
  - 3 bâtiments
  - 5 locaux techniques (max 1' du bureau)
- artisanal
  - fonction « broadcast » de Konsole
- Nagios, Cricket, Ntop

Observatoire (1000 pers)

- architecture en perpétuel mouvement (travaux)
- un ordre de grandeur en plus
  - 2 campus distants
  - $\approx$ 50 locaux techniques
  - 2006 : $\approx$ 90 commutateurs, 1 routeur
- inflation
  - 2010 : $\approx$ 150 commutateurs, 7 routeurs
- hétérogénéité
  - 3 marques (HP, Cisco, Juniper), 3 OS
  - 12 modèles, 12 versions d'OS (33 mineures)
- on industrialise...

Locaux techniques

- publicité : JRES 2009 : article et présentation no 67
  https ://2009.jres.org/planning_files/summary/html/67.htm

Inventaire

- visite exhaustive des locaux
  - obtention des clés/codes (fastidieux)
  - photos → site web
  - tableau
- mots de passe : de plus de 10 (!) à 2
- fichier CSV
  - référentiel unique
  - édition avec votre tableur favori
  - texte : awk, sed, grep, python, etc.
- CLI obligatoire (telnet, SSH)

Boîte à outils (logiciels libres)

- Nagios
- MRTG
- essai de Cacti puis abandon (pas de conf texte, perte des data lors màj)
- Extra (suspendu, attente de son successeur NeTS)
- Netdisco
- Rancid

Outils maison

- « traceroute L2 » vers une machine : wheremac (B. de Batz)
- génération automatique config Nagios
- représentation réseau graphique (graphviz/graphdot) : inutilisable
- représentation réseau texte : nwtree
- sauvegarde des config des matériels actifs

Méthodes

- déploiement d'un commutateur
  - config en atelier
  - montage puis retour au bureau
  - relevé ports interco : local et parent (LLDP, CDP)
  - édition du CSV
  - « make »
  - sauvegarde des configs
- firmware : on ne met plus à jour sauf si besoin, là où on en a besoin

Démo

- fichier d'inventaire en CSV
- représentation graphique : illisible
- Nwtree
- Netdisco
- MRTG
- Rancid

Plus et moins

- passe à l'échelle en nombre
- mais pas en topologie : arbre → maillage
- Netdisco : granularité des droits trop grossière pour une délégation partielle aux labos

Perspectives

- VLAN dynamique par Radius/MAC : on en parle depuis 4 ans...
- NeTS (extra2)
- Netdisco 1.0 : changement de VLAN via l'interface web
- réécriture du « traceroute L2 » avec prise en compte des VLAN (stage ?)
- carte météo des principaux liens d'interco