

Comment monter son propre ISP dans son garage

Nicolas Désir ndesir@saitis.net

François Deppierraz francois.deppierraz@nimag.net

7 mai 2013

Qui sommes-nous ?

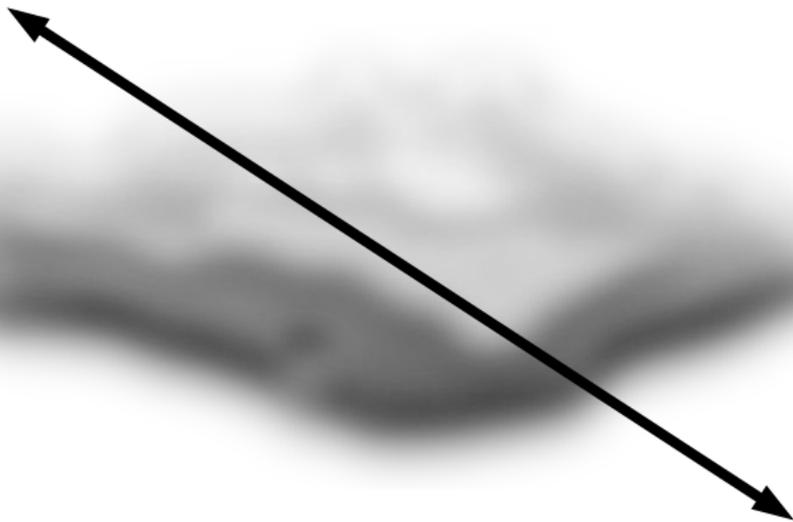


- ▶ PME lausannoise créée en 2000
 - ▶ Services Internet standards
 - ▶ Consulting
 - ▶ Spécialisée dans les infrastructures Linux
 - ▶ Nous opérons notre propre réseau et data center
- ▶ ISP à but non lucratif créé en 2000
 - ▶ Historiquement fournisseur de Nimag
 - ▶ Officiellement le LIR

InterNet ?

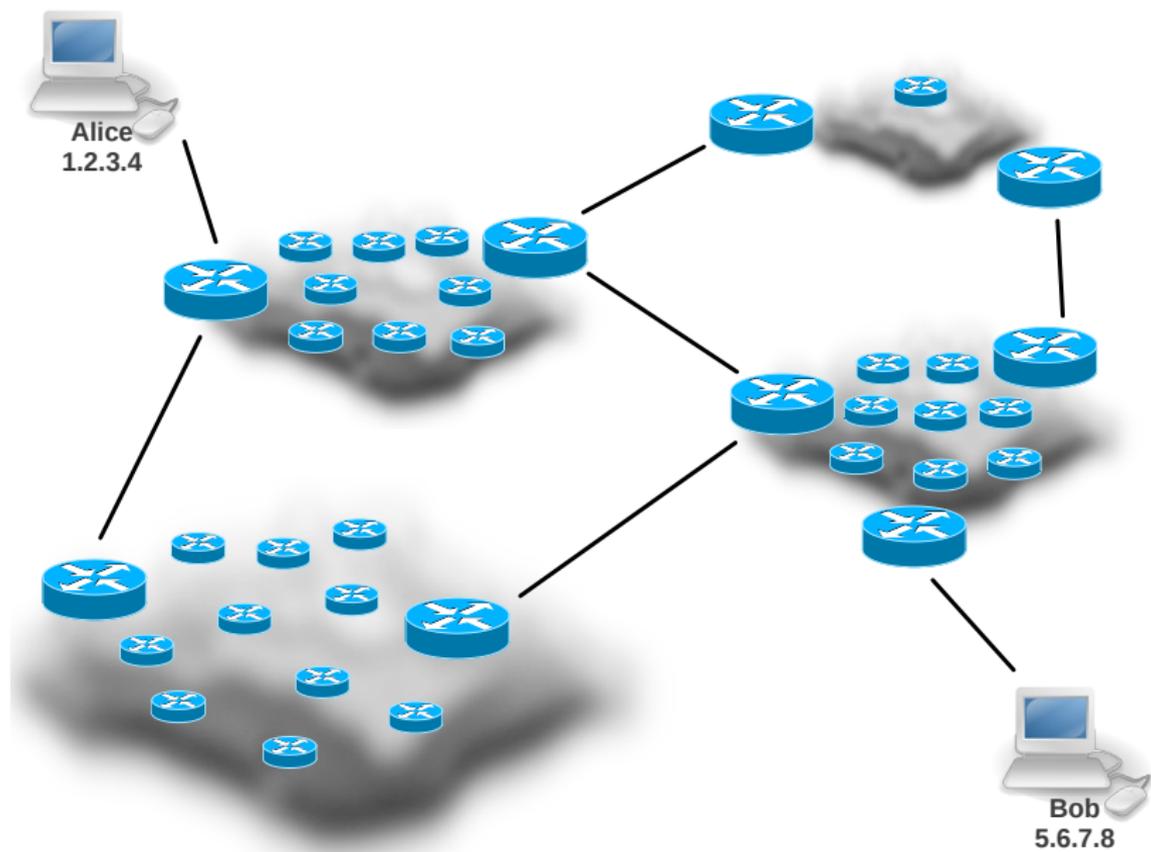


Alice
1.2.3.4

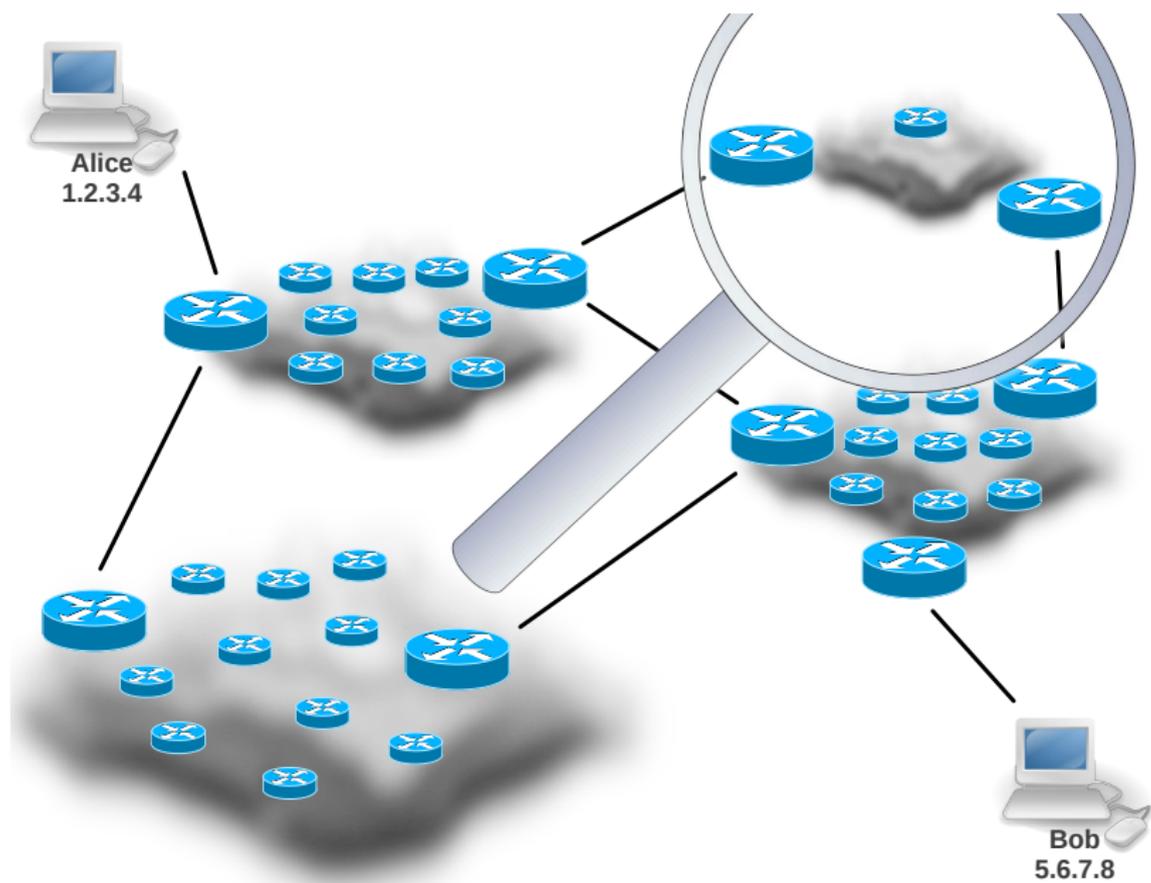


Bob
5.6.7.8

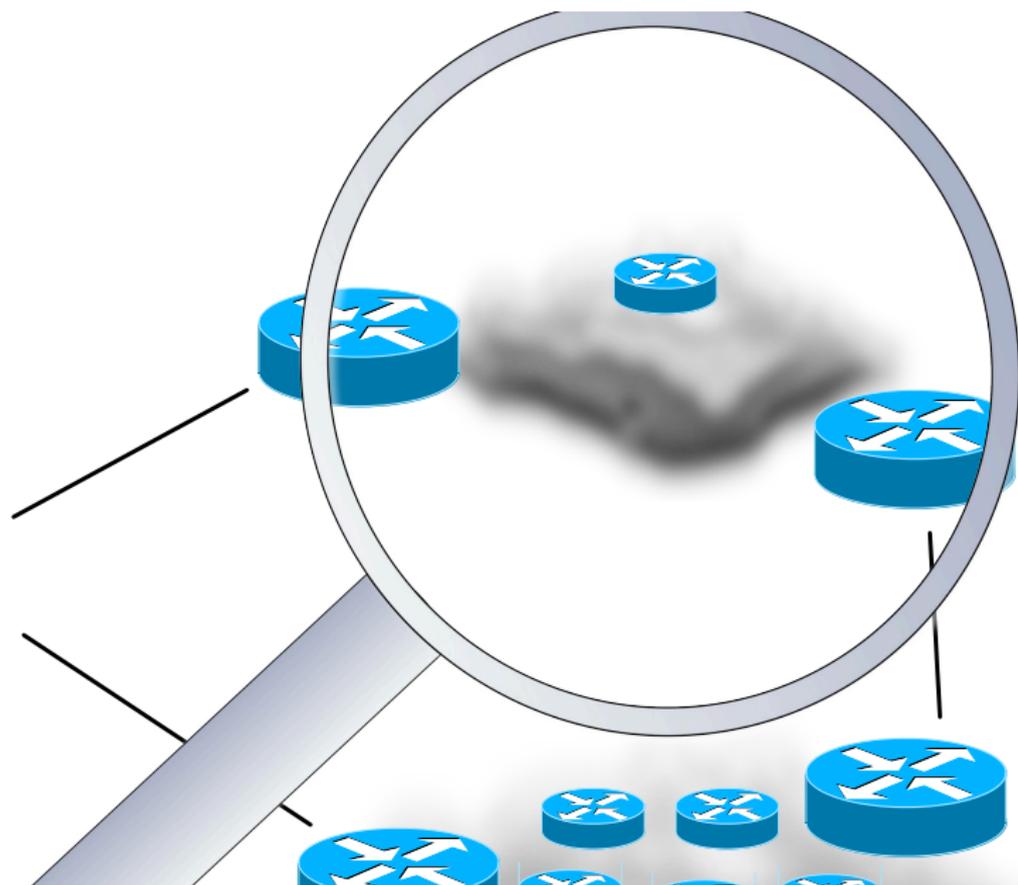
InterNet ?



InterNet ?



InterNet ?



Pourquoi monter son propre ISP ?

- ▶ Pas besoin de renuméroter pour changer de fournisseur
- ▶ Net neutrality
- ▶ Pour le fun... et le troubleshooting au milieu de la nuit !
- ▶ Propre choix de routage
- ▶ Gérer sa propre sécurité
 - ▶ (D)DoS
 - ▶ Spam
 - ▶ Fishing
- ▶ Gérez vos propres exceptions dans les règles antispoofing :-)

Pourquoi monter son propre ISP ?

- ▶ Pas besoin de renuméroter pour changer de fournisseur
- ▶ Net neutrality
- ▶ Pour le fun... et le troubleshooting au milieu de la nuit !
- ▶ Propre choix de routage
- ▶ Gérer sa propre sécurité
 - ▶ (D)DoS
 - ▶ Spam
 - ▶ Fishing
- ▶ Gérez vos propres exceptions dans les règles antispoofing :-)
- ▶ Fournir de l'accès à Internet dans des cas "sensibles"
 - ▶ Concours de sécurité informatique ?
 - ▶ Participer au réseau Tor

Quelles sont les étapes pour monter son propre ISP ?

Data Center

Equipements réseau

Ressources RIPE (AS + IP)

Routage BGP

Electricité

Refroidissement

Dernier kilomètre

Administratif

Data Center

Data Center

- ▶ Électricité
 - ▶ Le nerf de la guerre
 - ▶ Les datacenters se classent par puissance
 - ▶ Fourchette à la louche de 10KW à plus 10MW
- ▶ Emplacement
 - ▶ Un garage?
 - ▶ Local de dépôt
 - ▶ Bâtiment industriel
 - ▶ Accès en voiture/camion, quai de chargement, monte charge (transports publiques?)
- ▶ Connectivité, fibres optiques
 - ▶ Opérateurs, pouvoirs publics, services industriels
 - ▶ Habituellement le long des autoroutes, voies de train, lignes électrique ou conduites de gaz
- ▶ Redondance
 - ▶ Plusieurs fournisseurs
 - ▶ Plusieurs chemins

Data Center (2)



Equipements réseau

Routeurs

Hardware

- ▶ Gros constructeurs (Cisco, Juniper, etc.)
 - ▶ 10^3 à 10^6 CHF
- ▶ Plus petits constructeurs (Mikrotik, Ubiquiti, etc.)
 - ▶ 10^1 à 10^3 CHF
- ▶ On trouve beaucoup de choses sur EBay

Software

- ▶ Daemons de routage dynamique
 - ▶ Quagga
 - ▶ OpenBGPD et OpenOSPF
 - ▶ BIRD

Capacités

- ▶ Attention aux capacités des équipements !
 - ▶ Nombre de routes supportées ($\sim 450'000$ routes BGP par transit)
 - ▶ Trafic routé (Gbps)
 - ▶ Nombre de paquets par seconde (Mpps)

Ressources RIPE (AS + IP)

Ressources RIPE (AS + IP)

Adresses IP réparties par l'IANA
(Internet Assigned Numbers Authority)
entre les RIR :

RIR = Regional Internet Registry

Au nombre de 5 :

- ▶ RIPE Network Coordination Centre (RIPE NCC)
- ▶ American Registry for Internet Numbers (ARIN)
- ▶ Asia-Pacific Network Information Centre (APNIC)
- ▶ Latin American and Caribbean Internet Address Registry (LACNIC)
- ▶ African Network Information Centre (AfrinIC)



RIPE

Caractéristiques :

- ▶ fonctionnement associatif/buts non lucratifs
- ▶ complètement transparent dans les coûts
- ▶ gestion de la base de données de leurs ip/contacts etc (certains gros isp ont la leur)
- ▶ très beaux rapports d'activité
- ▶ engagement dans des projets intéressants

LIR chez RIPE

LIR = Local Internet Registry

- ▶ ISP
- ▶ Entreprise

Devenir membre :

- ▶ Montrer un minimum de compétences
- ▶ Payer sa coti
 - ▶ €2000 d'inscription
 - ▶ €1800 de cotisation annuelle
- ▶ Accepter de retourner à un régime presque scolaire
- ▶ Recevoir ses adresses IP

Un AS et des IPv4 et/ou IPv6

AS - Système Autonome

- ▶ Analogie avec un Pays
- ▶ Numéro unique attribué par le RIR responsable
- ▶ Collection de réseaux et de routeurs
- ▶ Sous le contrôle d'une entité
- ▶ Politique de routage unique
- ▶ Au choix principalement :
 - ▶ transit(\$\$\$)
 - ▶ peering(\$)

Service whois

- ▶ Les données publiques collectées par RIPE sont accessible via le protocole whois.
- ▶ L'utilitaire `whois` permet d'y accéder en CLI

```
$ whois 2001:788:1337:3::/64
% Information related to '2001:788:1337::/48'

inet6num:       2001:788:1337::/48
netname:        V6-INSOMNI-HACK-2012
descr:          Insomni'hack 2012
remarks:        .
remarks:        .          uuuuuuuu
remarks:        .          uu$$$$$$$$$$$$$$$$$uu
remarks:        .          uu$$$$$$$$$$$$$$$$$$$$$uu
remarks:        .          u$$$$$$$$$$$$$$$$$$$$$$$$$u
remarks:        .          u$$$$$$$$$$$$$$$$$$$$$$$$$$$$$u
remarks:        .          u$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$u
remarks:        .          u$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$u
remarks:        .          u$$$$$$$ " $$$" "$$$$$$u
remarks:        .          "$$$$" u$u " $$$"
remarks:        .          $$$u u$u u$$$
remarks:        .          $$$u u$$$$$ u$$$
remarks:        .          "$$$uu$$$ $$$uu$$$"
remarks:        .          "$$$$$$" "$$$$$$"
remarks:        .          u$$$$$$u$$$$$$$$$u
remarks:        .          u$" "$ "$ "$ "$ $u
remarks:        .          uuu          $$$ $ $ $ $ $u$          uuu
remarks:        .          u$$$$          $$$u$u$u$$$          u$$$$
remarks:        .          $$$u$uu          "$$$$$$$$"          uu$$$$$$$
remarks:        .          u$$$$$$$$$$$$$uu          "" ""          uuuu$$$$$$$$$$$$$
remarks:        .          $$$ "$" "$$$$$$$$$$uu          uu$$$$$$$$$$$ "$" "$"
remarks:        .          "" "" "$$$$$$$$$$uu          "$" "$"
remarks:        .          uuuu          "$$$$$$$$$$uuu
remarks:        .          u$$$$uuu$$$$$$$$$$$$$uu          "$$$$$$$$$$$$$$uuu$$$
remarks:        .          $$$$$$$$$$$$ "" ""          "$$$$$$$$$$$$$$"
remarks:        .          "$$$$$"          "" "$$$$$"
remarks:        .          $$$          $$$"
country:        CH
admin-c:        FD4391-RIPE
tech-c:         FD4391-RIPE
status:         ALLOCATED-BY-LIR
mnt-by:         SAITIS-MNT
mnt-lower:      SAITIS-MNT
mnt-routes:     SAITIS-MNT
source:         RIPE # Filtered
```

IPv4 Exhaustion

[News](#) [Press Centre](#) [Internet Governance](#) [IPv6](#) [IPv4 Exhaustion](#) [IPv6 Act Now](#)

[News Feeds from the RIPE NCC](#) · [NRO News](#)

You are here: [Home](#) > [Internet Coordination](#) > [News](#) > [Announcements](#) > [RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8](#)

RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8

14 Sep 2012

On Friday 14 September, 2012, the RIPE NCC, the Regional Internet Registry (RIR) for Europe, the Middle East and parts of Central Asia, distributed the last blocks of IPv4 address space from the available pool.

This means that we are now distributing IPv4 address space to Local Internet Registries (LIRs) from the last /8 according to section 5.6 of "IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region".

This section states that an LIR may receive one /22 allocation (1,024 IPv4 addresses), even if they can justify a larger allocation. This /22 allocation will only be made to LIRs if they have already received an IPv6 allocation from an upstream LIR or the RIPE NCC. No new IPv4 Provider Independent (PI) space will be assigned.

It is now imperative that all stakeholders deploy IPv6 on their networks to ensure the continuity of their online operations and the future growth of the Internet.

[More information on IPv6 and its deployment, advice from experts and where to get training](#)

[More information on reaching the last /8](#)

Service Announcements

All of our services are operating normally.

[CHECK NETWORK HEALTH →](#)

IPv4 Exhaustion

We are now allocating IPv4 address space from the last /8.

[FIND OUT MORE →](#)

- ▶ Un nouveau LIR reçoit maximum un /22 (1024 IPv4)



- ▶ Migration nécessaire mais pénible...
- ▶ Deux réseaux en parallèle
- ▶ Problème de l'oeuf et de la poule
 - ▶ Fournisseurs de contenu
 - ▶ Fournisseurs d'accès
- ▶ Nouveaux protocoles, nouveaux bugs !

BGP

BGP

Session BGP

- ▶ Configuration d'une session entre deux routeurs nécessite des deux côtés
- ▶ Utilise une connexion TCP sur le port 179

Une fois la session établie, elle permet :

- ▶ D'envoyer les routes connues (des autres et les siennes)
- ▶ On y rajoute son num. d'AS dans le chemin (AS-PATH)
- ▶ Ceci évite les boucles car BGP ne ré-annonce pas une route qui contient son num. d'as
- ▶ Ensuite si une route change chez nous, nous y enverrons un update
- ▶ Si elle disparaît, on enverra un message de suppression

Selection

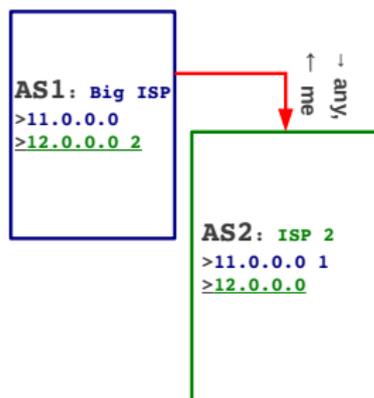
Quelle route choisir :

- ▶ quelque soit l'origine de la route, le préfixe le plus spécifique :
 - ▶ 12.13.14.0/24 gagne sur 12.13.14.0/23
- ▶ entre deux préfixes qui ont BGP comme origine :
 - ▶ principalement, on choisit celui qui à l'as-path le plus court
 - ▶ et s'ils ont le même : d'autres paramètres interviennent, dans l'algorithme complet

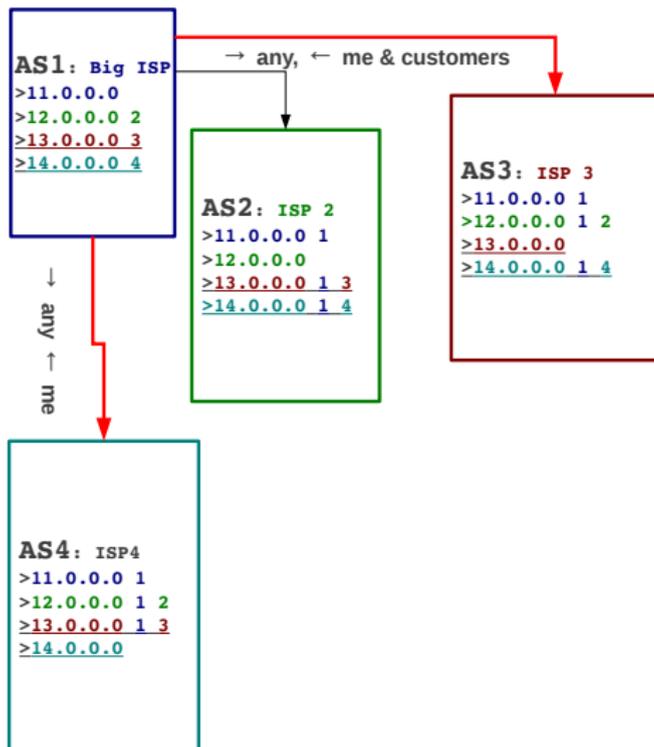
Exemple

```
AS1: Big ISP  
>11.0.0.0
```

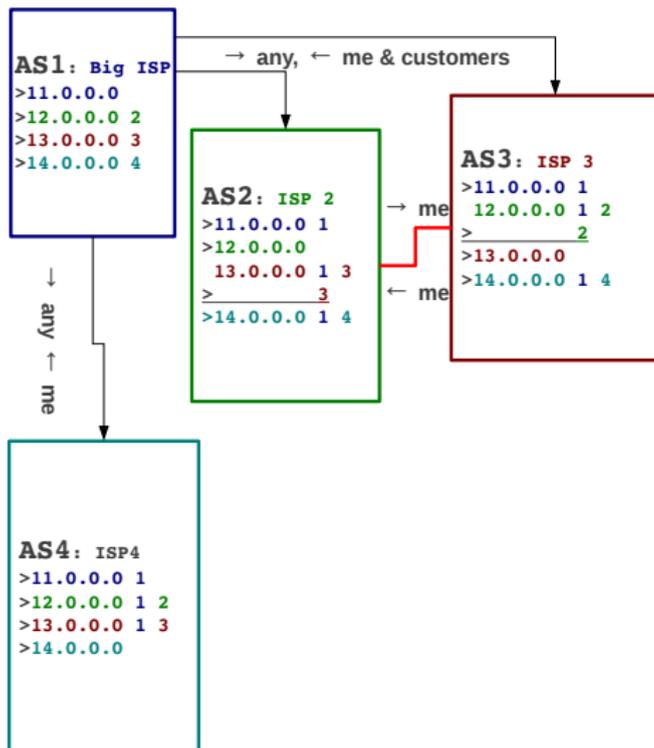
Example



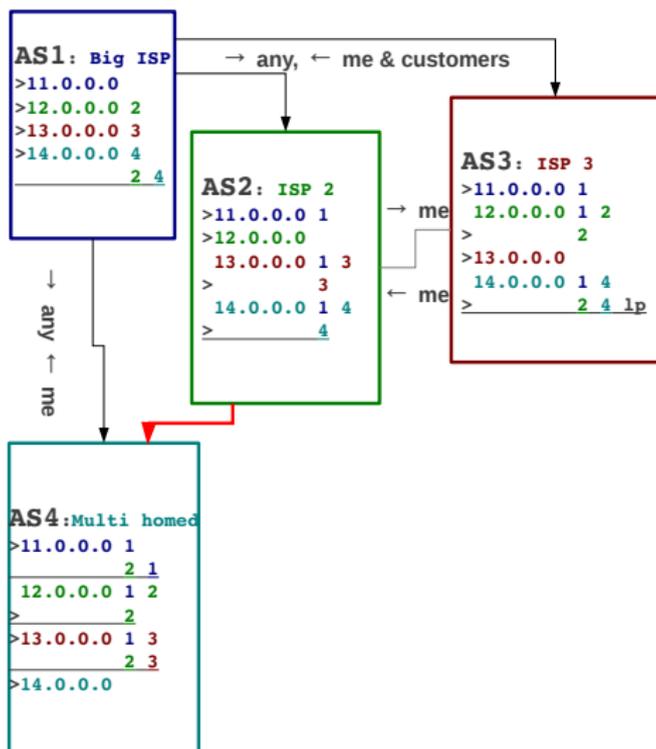
Example



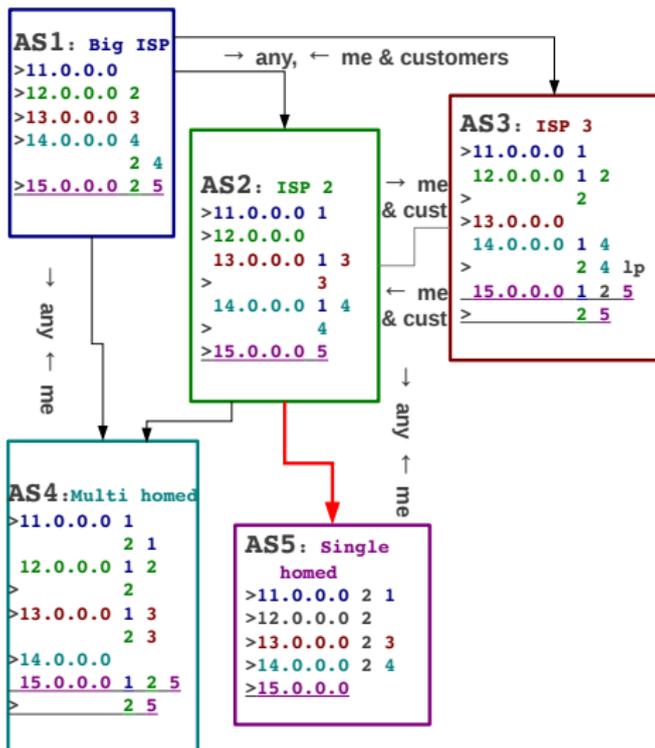
Exemple



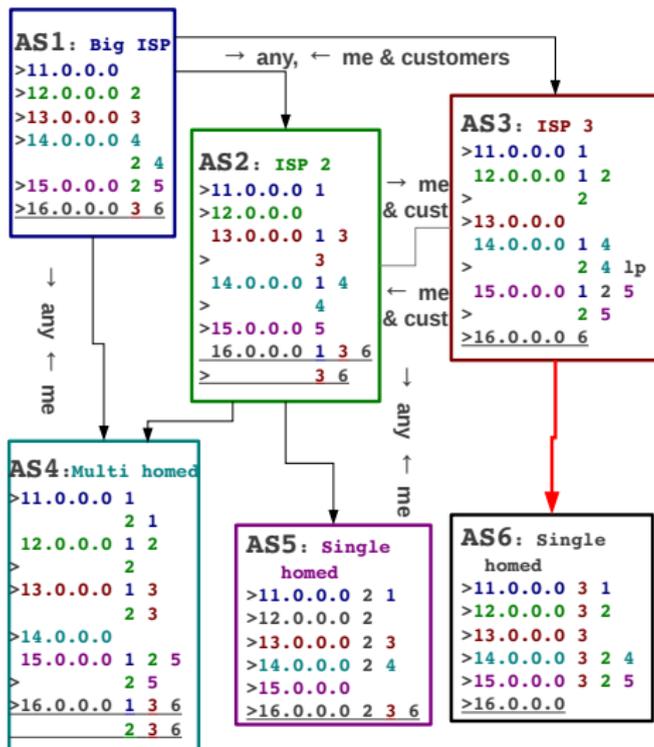
Exemple



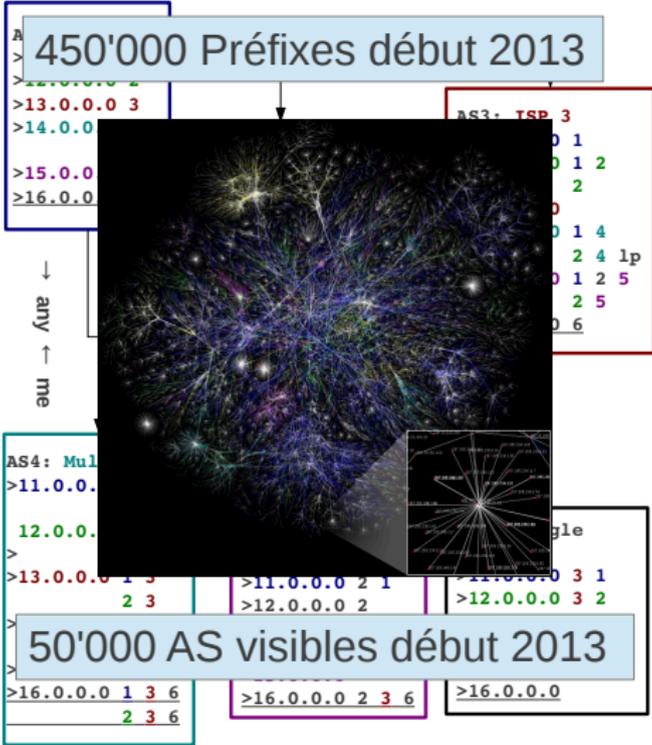
Exemple



Exemple



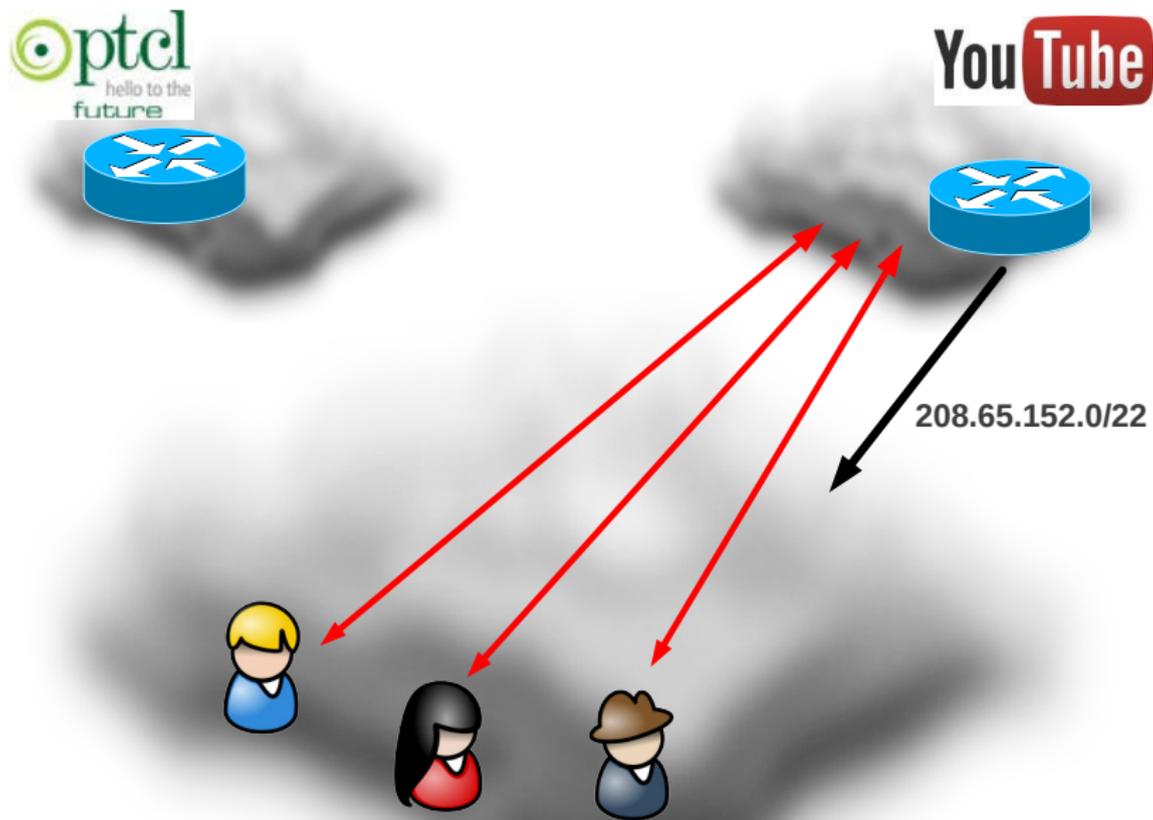
Exemple



YouTube Hijacking

- ▶ En février 2008, hijacking involontaire d'une route de `http://youtube.com` par Pakistan Telecom
- ▶ Résultat : 2h de downtime

YouTube Hijacking (2)



YouTube Hijacking (2)

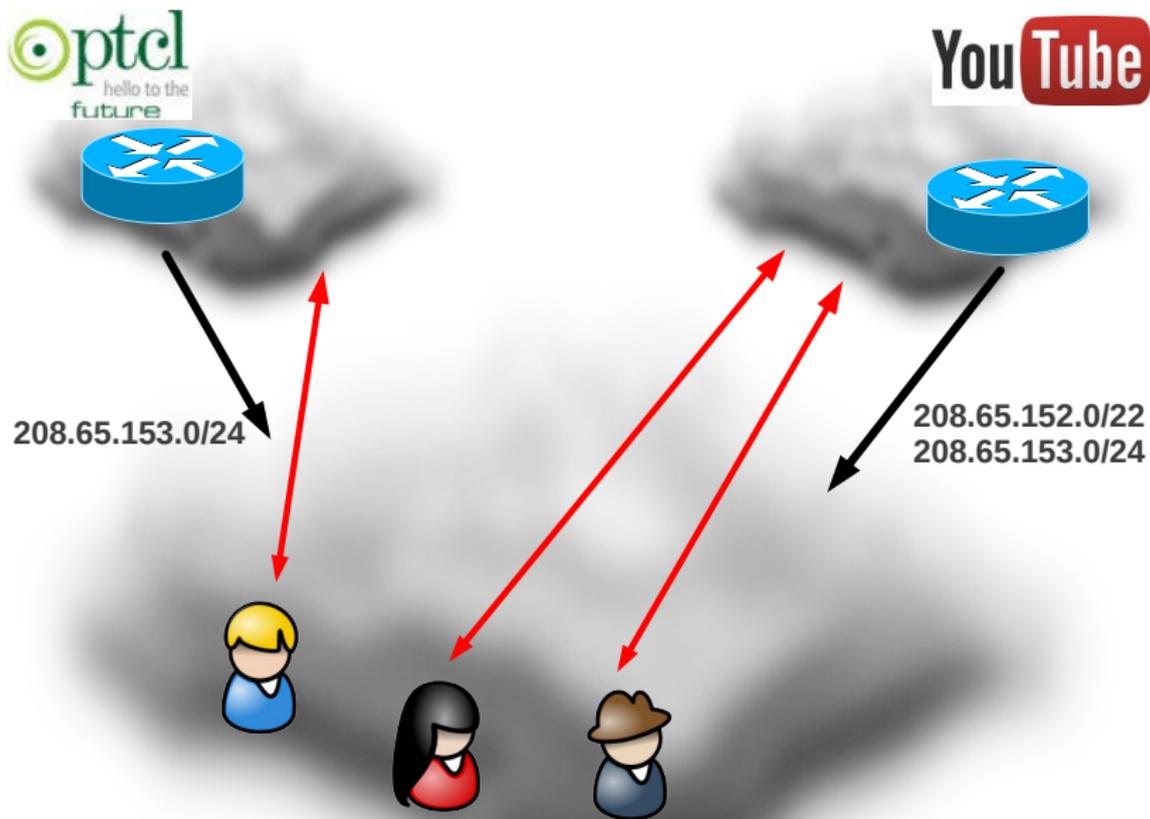


208.65.153.0/24

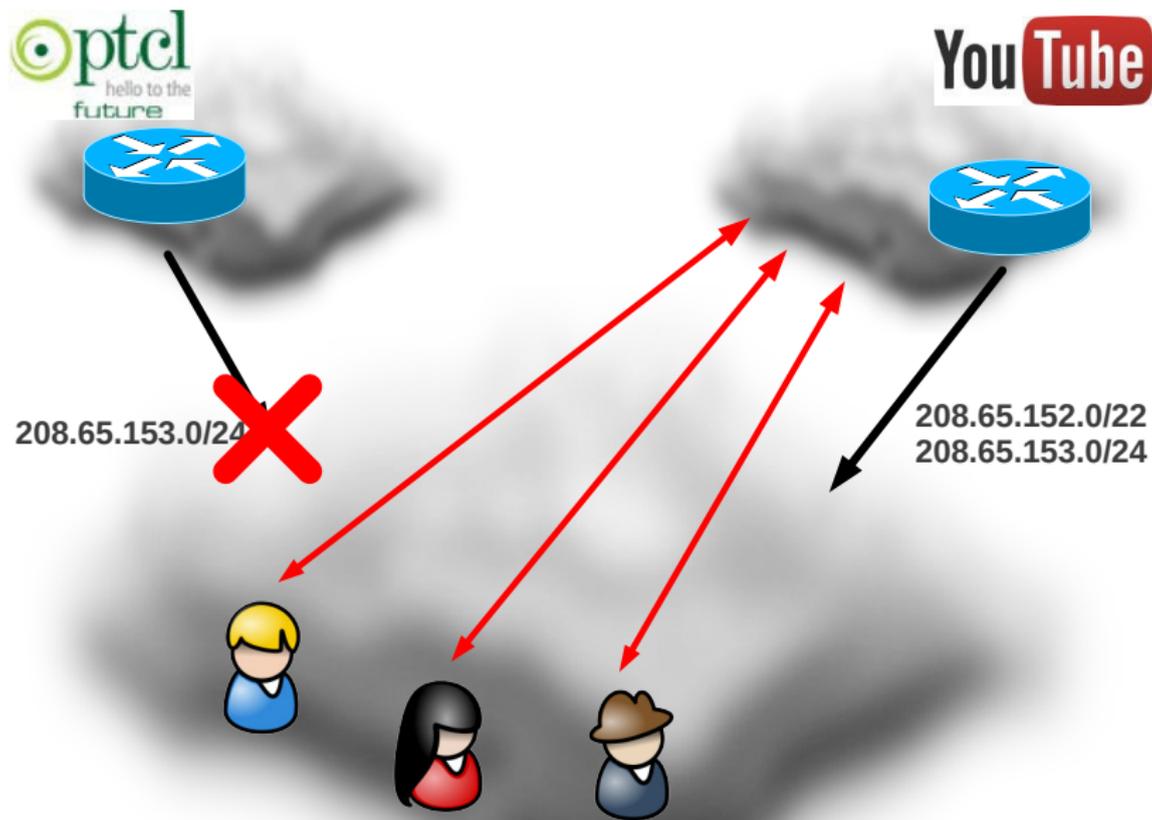


208.65.152.0/22

YouTube Hijacking (2)



YouTube Hijacking (2)



Filtrage des routes BGP

▶ Problèmes

- ▶ Il n'existe pas vraiment d'entité en dessus des RIR
- ▶ Système très distribué
- ▶ Le filtrage réduit la résilience d'Internet

▶ Solutions

- ▶ Ne pas filtrer...
- ▶ Limiter le nombre de routes reçues par un peer `max-prefix`
- ▶ RPSL – Routing Policy Specific Language
- ▶ RPKI – Resource Public Key Infrastructure

RPSL

- ▶ Bases de données gérées par les RIR
- ▶ Les AS source de chaque préfixe est enregistré dans la base RPSL de RIPE
- ▶ Des filtres sont créés automatiquement d'après ces données

```
$ whois -h whois.ripe.net AS1111
remark: Transit
import: from AS2222 accept ANY
export: to AS2222 announce AS1111
remark: Peerings
import: from AS3333 accept AS3333
export: to AS3333 announce AS1111
remark: Customers
import: from AS3333 accept AS3333
export: to AS3333 announce ANY
```

RPSL

- ▶ Bases de données gérées par les RIR
- ▶ Les AS source de chaque préfixe est enregistré dans la base RPSL de RIPE
- ▶ Des filtres sont créés automatiquement d'après ces données

```
$ whois -h whois.ripe.net AS1111
remark: Transit
import: from AS2222 accept ANY
export: to AS2222 announce AS1111
remark: Peerings
import: from AS3333 accept AS3333
export: to AS3333 announce AS1111
remark: Customers
import: from AS3333 accept AS3333
export: to AS3333 announce ANY
```

RPSL

- ▶ Bases de données gérées par les RIR
- ▶ Les AS source de chaque préfixe est enregistré dans la base RPSL de RIPE
- ▶ Des filtres sont créés automatiquement d'après ces données

```
$ whois -h whois.ripe.net AS1111
remark: Transit
import: from AS2222 accept ANY
export: to AS2222 announce AS1111
remark: Peerings
import: from AS3333 accept AS3333
export: to AS3333 announce AS1111
remark: Customers
import: from AS3333 accept AS3333
export: to AS3333 announce ANY
```

RPSL

- ▶ Bases de données gérées par les RIR
- ▶ Les AS source de chaque préfixe est enregistré dans la base RPSL de RIPE
- ▶ Des filtres sont créés automatiquement d'après ces données

```
$ whois -h whois.ripe.net AS1111
remark: Transit
import: from AS2222 accept ANY
export: to AS2222 announce AS1111
remark: Peerings
import: from AS3333 accept AS3333
export: to AS3333 announce AS1111
remark: Customers
import: from AS3333 accept AS3333
export: to AS3333 announce ANY
```

et dans la pratique...

From: noc@worldcompanyswitzerland.corp
To: swinog@swinog.ch
Subject: [swinog] New PI prefix from AS1234

Hello...

World Company Switzerland (AS1234) is announcing a new prefix:

123.456.789.0/24

I know...route object is missing...but that is not in my hands (o;

Please update your filters if you have to.

thanx in advance

et dans la pratique...

From: noc@worldcompanyswitzerland.corp
To: swinog@swinog.ch
Subject: [swinog] New PI prefix from AS1234

Hello...

World Company Switzerland (AS1234) is announcing a new prefix:

123.456.789.0/24

I know...**route object is missing**...but that is not in my hands (o;

Please update your filters if you have to.

thanx in advance

et dans la pratique...

From: noc@worldcompanyswitzerland.corp
To: swinog@swinog.ch
Subject: [swinog] New PI prefix from AS1234

Hello...

World Company Switzerland (AS1234) is announcing a new prefix:

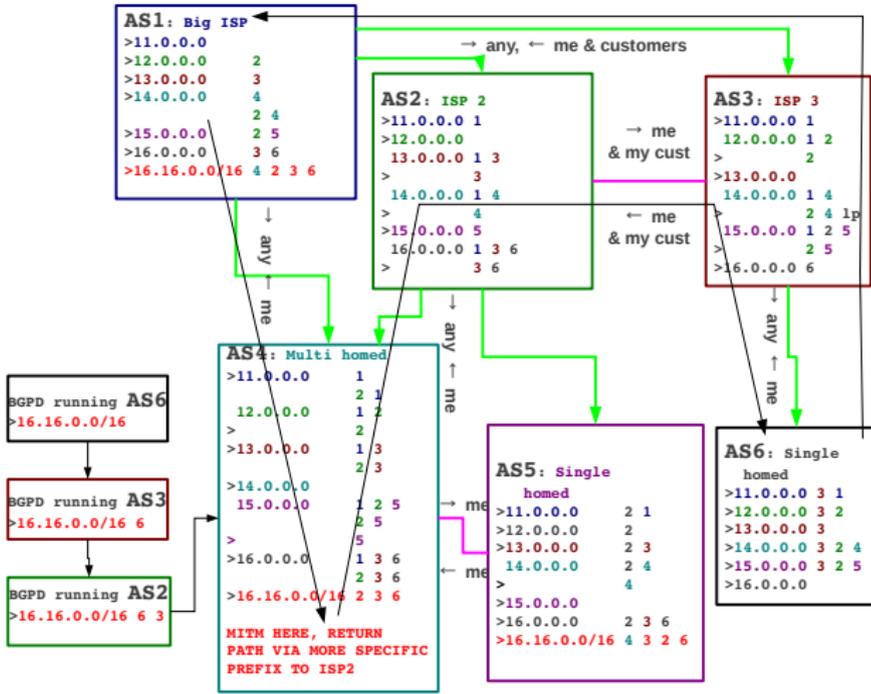
123.456.789.0/24

I know...route object is missing...but that is not in my hands (o;

Please update your filters **if you have to**.

thanx in advance

Man in the middle with BGP



Quelqu'un bricole dans l'AS4 pour s'approprier le trafic vers 16.16.0.0/16

Electricité

Electricité

Poste très important :

- ▶ 20 KW à 25ct le KWh : 3600 chf/mois
- ▶ 10 MW à 8ct le KWh : 600 KCHF/mois

Dans notre cas :

- ▶ Electricité fournie par les SIL à 25ct
- ▶ Télé-relève
- ▶ Verte, on essaie de faire sa pub
- ▶ Concurrence rude
- ▶ Refacturation au plus juste

Quand y'en a plus ? !

- ▶ et que l'ups a 90min d'autonomie



Refroidissement

Climatisation



DIY?

- ▶ Pas de trop de \$
- ▶ On saura aussi dépanner les installations
- ▶ Offres correctes d'occace (Ebay et autres)
- ▶ Se former, s'outiller

Climatisation 2, outillage et permis

▶ Manos



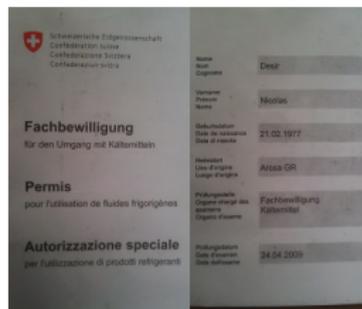
▶ Pompe à vide



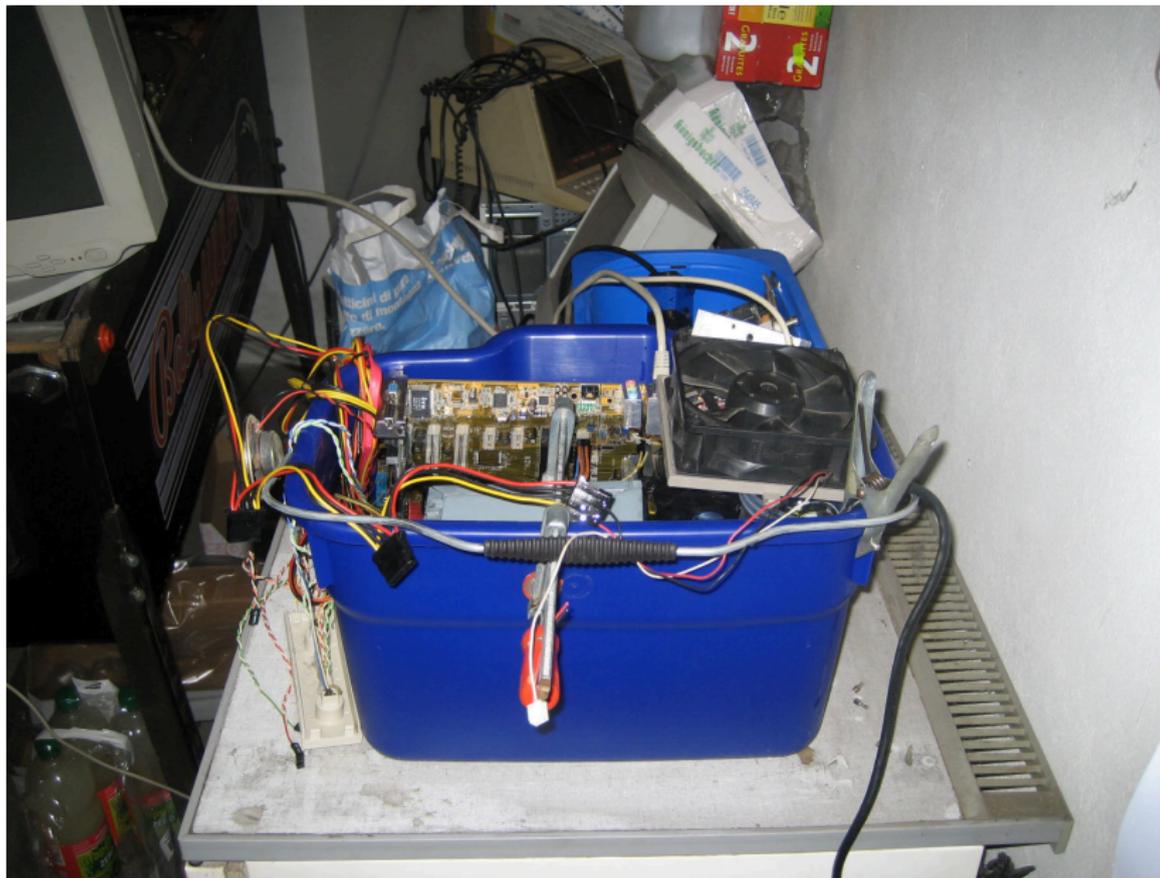
▶ Chalumeau Oxy-Acétylène



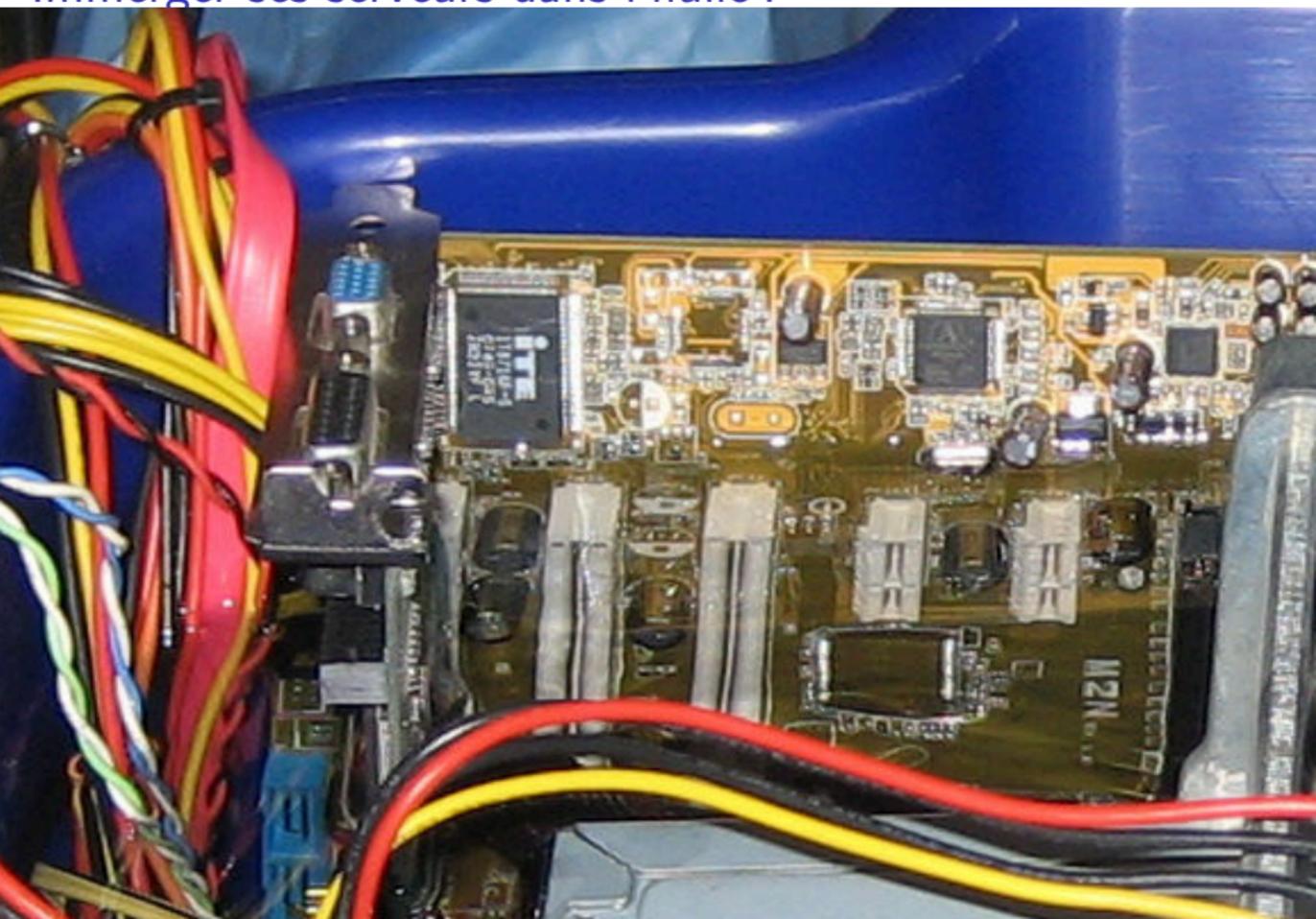
▶ Permis de manipuler



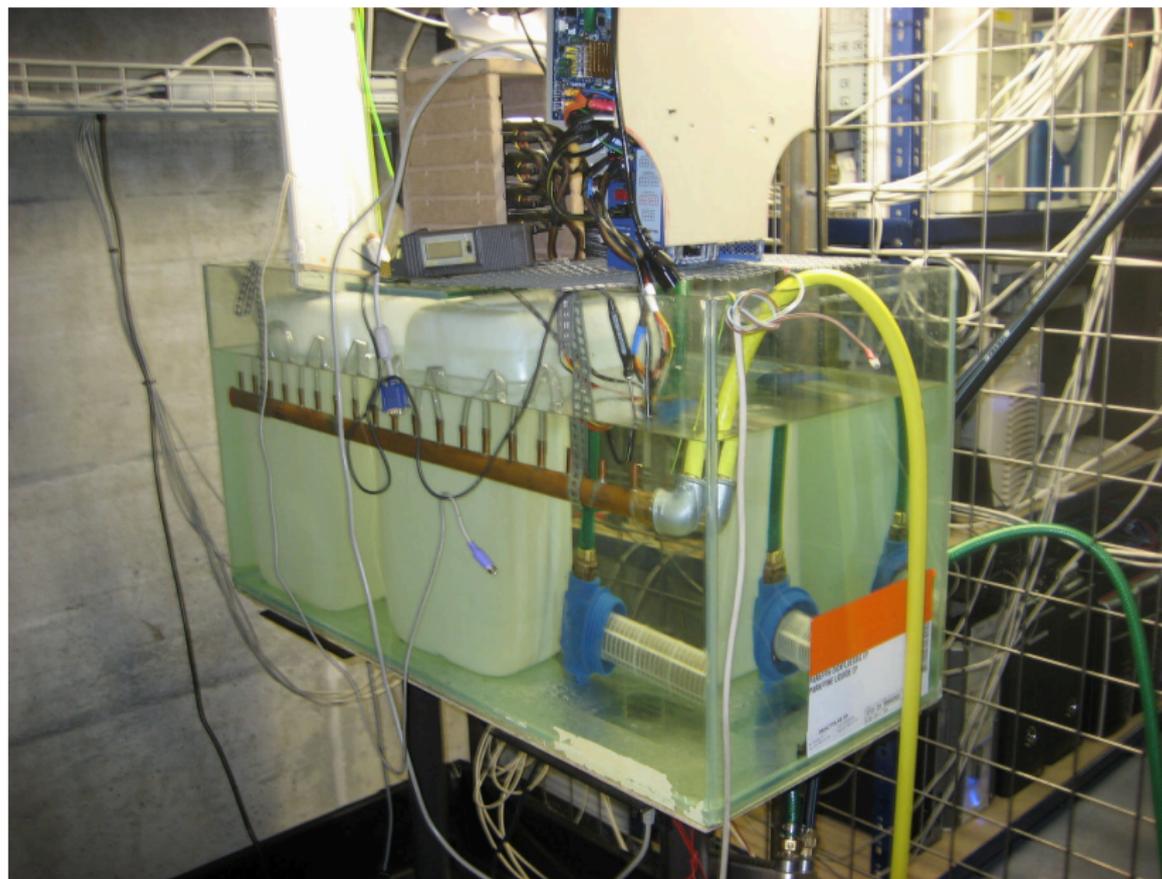
Immerger ses serveurs dans l'huile ?



Immerger ses serveurs dans l'huile ?

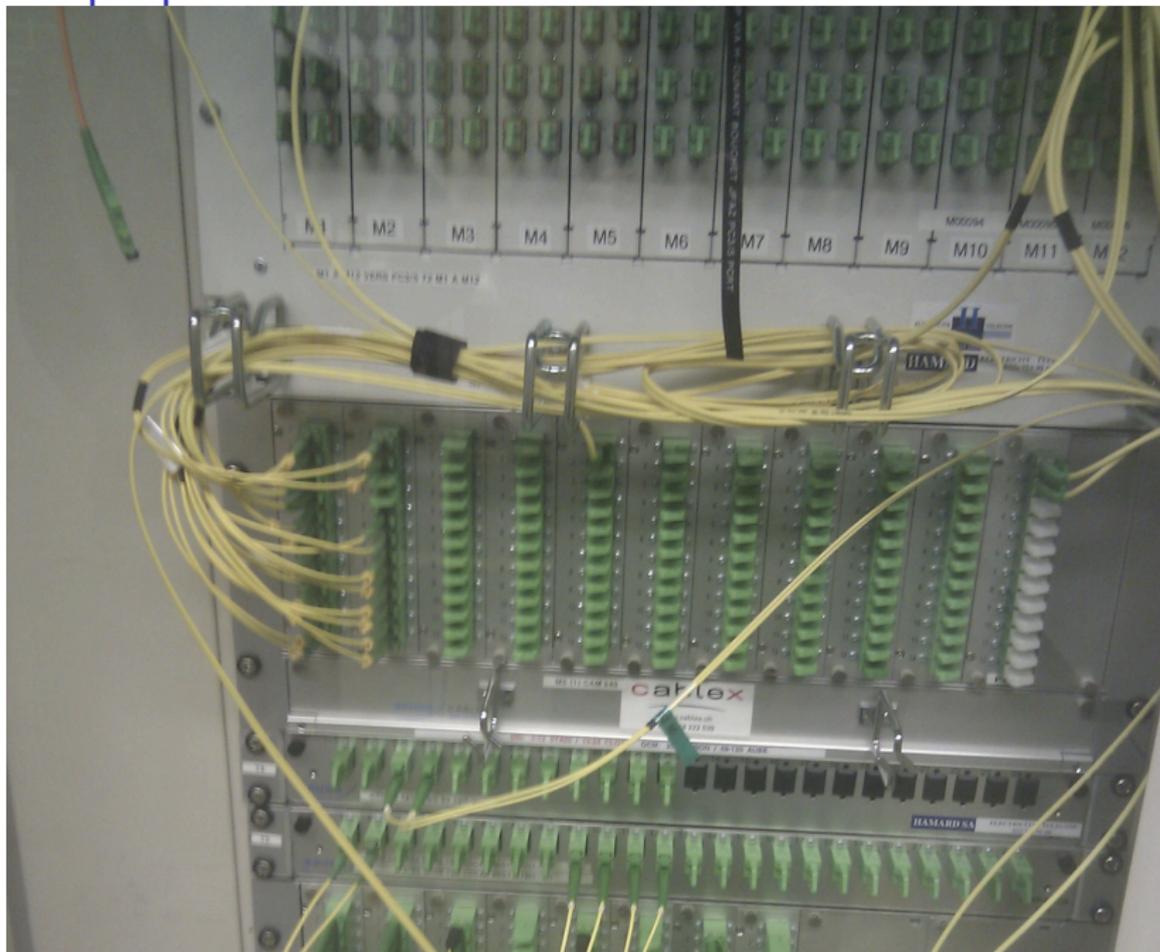


Immerger ses serveurs dans l'huile? (2)

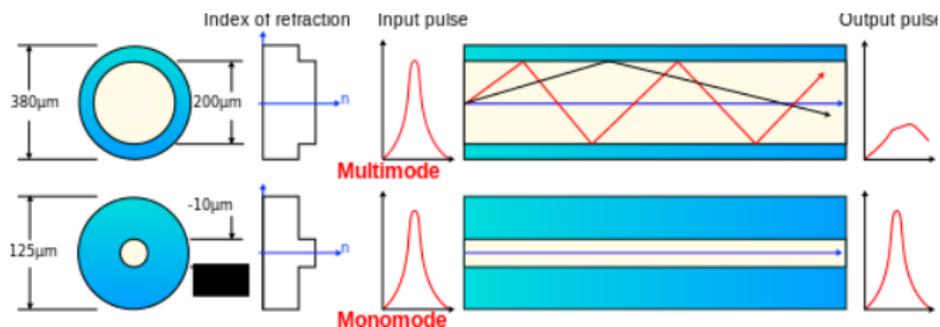


Dernier kilomètre

Fibre optique

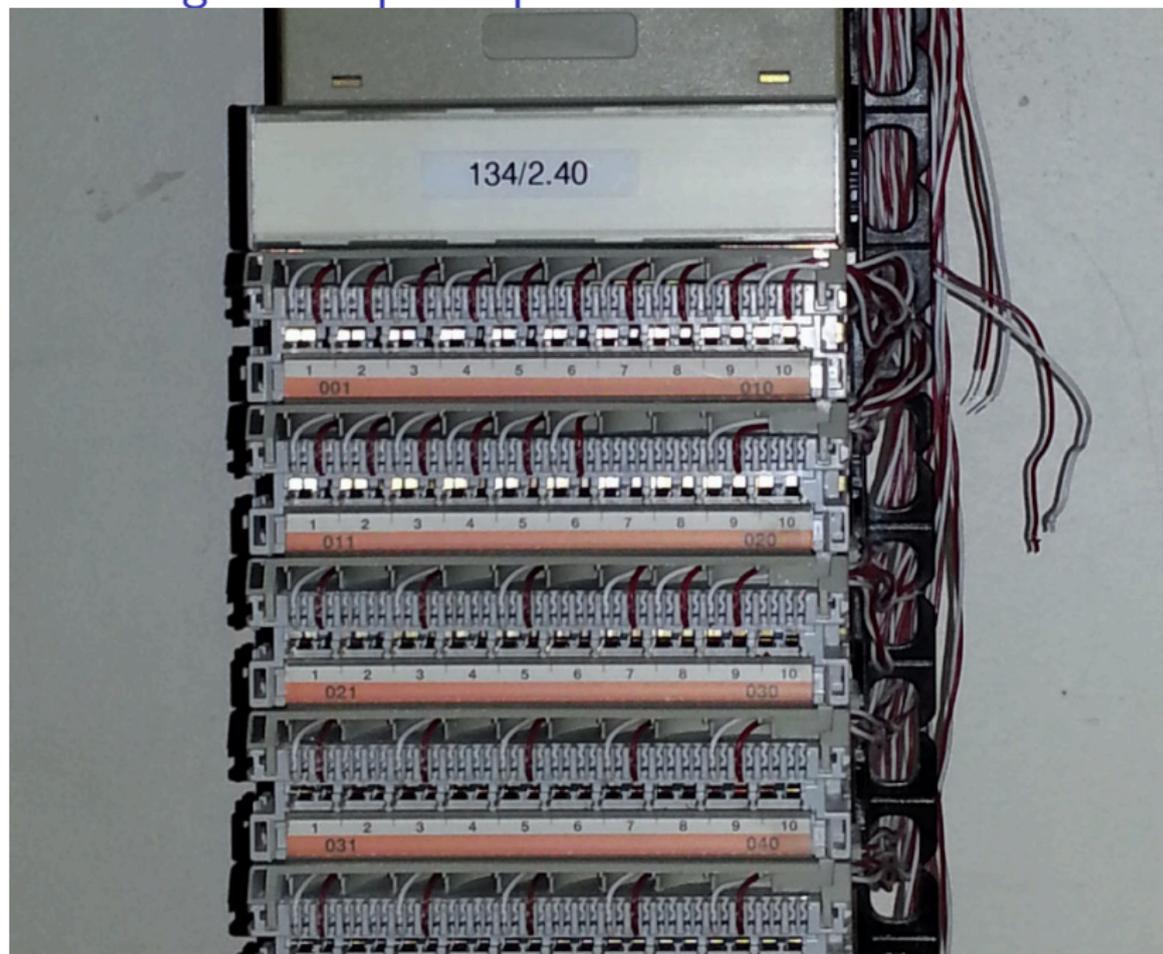


Fibre optique



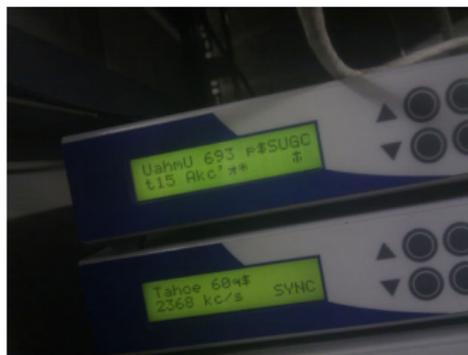
- ▶ Multimode
 - ▶ Plus de réflexions donc étalement spectral
 - ▶ Courtes distances
- ▶ Monomode
 - ▶ Longues distances
- ▶ Connecteurs
 - ▶ C'est la jungle !
 - ▶ Wikipedia en dénombre pas moins de **37** types
- ▶ Habituellement connectées via un module SFP

xDSL sur lignes téléphoniques

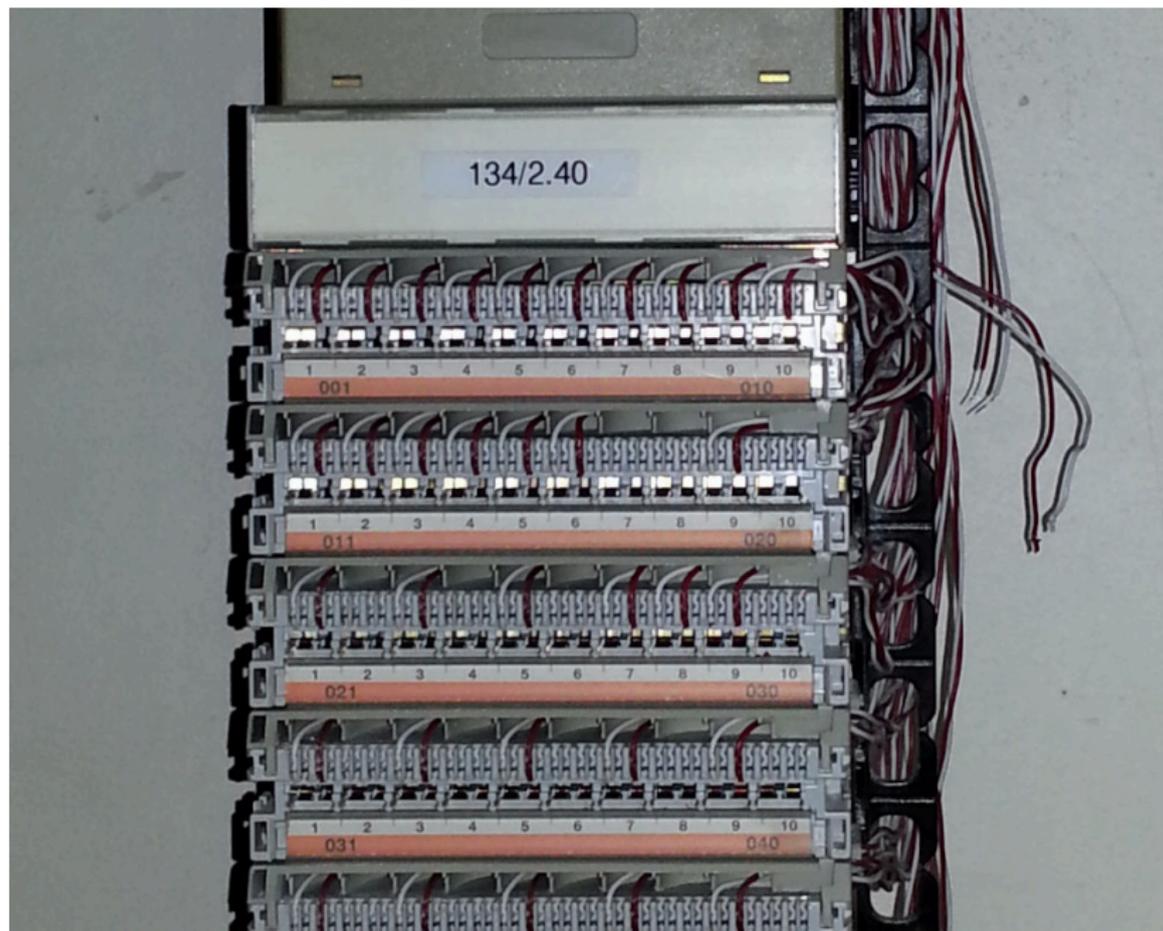


xDSL sur lignes téléphoniques

- ▶ Digital Subscriber Line (DSL)
- ▶ Utilisation des lignes téléphoniques
- ▶ Beaucoup de variantes de DSL existent
- ▶ Débits dépendant de la ligne
 - ▶ Longueur
 - ▶ Qualité de câble
 - ▶ Interférences



xDSL (2)



WiFi

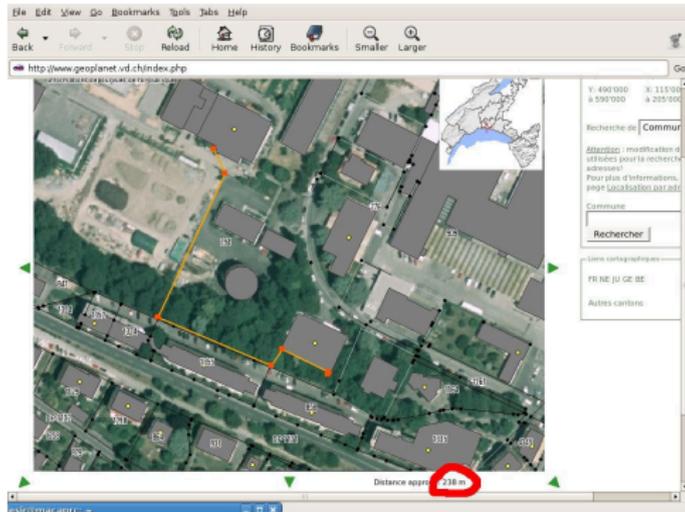
- ▶ 802.11n
- ▶ Bandes ISM :
 - ▶ 2.4 GHz (indoor et outdoor)
 - ▶ 5.15 à 5.35 GHz (indoor)
 - ▶ 5.47 à 5.75 GHz (outdoor)
 - ▶ Attention bandes de fréquences partagées
- ▶ Liaisons point à point ou point à multipoints
- ▶ Débit pratique de 150 Mbps (total des deux directions)



DSL sur câble de l'armée suisse



DSL sur F2E câble de l'armée suisse



- ▶ Expérience mais concluante
- ▶ Trajet court et peu perturbé
- ▶ Pas bien adapté à la Suisse
- ▶ Pratique dans le cas d'événements temporaires
 - ▶ En forêt sans vue directe par exemple

Ronja



Ronja



Ronja

- ▶ Reasonable Optical Near Joint Access
- ▶ Projet Open Hardware
- ▶ Triple Play en 2004
- ▶ Avantages : mitm/snif très compliqué, densité des liaisons
- ▶ Désavantage : sujet aux intempéries

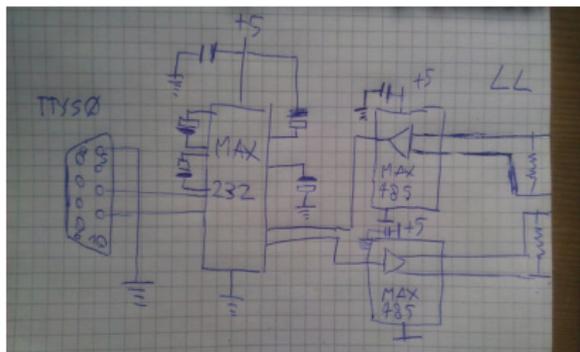
Ethernet 10BASE5

- ▶ Bon vieux temps
- ▶ Maximum 5 segments de 500m, dont 3 vampirisables (ext,milieu,ext) et 2 de liaison uniquement
- ▶ Pas besoin de prévoir exactement le futur utilisateur
- ▶ Eu un exemple de MAN



RS422

- ▶ 1998 : une paire de modem Nokia BB512 coûtait 5000 chf
- ▶ on a tenté et réussi à faire 115200bit/s en slip sur une paire de cuivre de 1.3km
- ▶ la liaison a fonctionné en permanence pendant presque une année
- ▶ 2 MAX 232 et 4 MAX 485, quelques condos et des terminateurs (j50chf)



Administratif

Copyright Infringement...

From: paramount@copyright-compliance.com
Subject: 11-42531394 Notice of Unauthorized Use of
Paramount Pictures Corporation Property

Evidentiary Information:

Notice ID: 11-42531394
Initial Infringement Timestamp: 29 Jan 2013 11:33:22 GMT
Recent Infringement Timestamp: 29 Jan 2013 11:33:22 GMT
Infringers IP Address: 62.220.X.Y
Protocol: BitTorrent
Infringed Work: Hugo
Infringing File Name: Hugo.3D.2011.1080p.MKV.AC3.DTS.NL.Su
Infringing File Size: 11064794960
Bay ID: 0859efac62e552e3c1be70ddb19c86638a94fc36|1106479496
Port ID: 49120
Infringer's User Name:

Conclusion

1. Trouver un garage
2. Inscription en tant que LIR chez RIPE
3. Trouver un/deux fournisseur(s) de transit
4. Vérifier l'alimentation électrique
5. Installer une climatisation
6. Configurer son/ses routeur(s) en BGP
7. Connecter des clients



Merci pour votre attention !