Master 2 e-secure

Réseaux avancés

Ipv6 – Transition v4-->v6

Bureau S3-354
Mailto:Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M2/rezo

Ipv6 - Transition

Problèmes :

- Accéder à l'Internet v6 lorsqu'on possède seulement une adresse (ou un réseau) Ipv4.
- Faire cohabiter les deux piles sur une même machine, dans un même réseau.
- Communiquer entre applications v4 et v6

Transition – Double pile

Les applications doivent communiquer en v4 et en v6.
Pour un serveur, il n'est pas commode d'utiliser deux ports distincts.
Le mieux est d'utiliser les adresses Ipv4-mappées :

0 (80 bits)	FFFF	Adresse v4

L'application dialogue en v6. Mais les messages sont envoyés et reçus dans des DG v4 ou v6 selon la forme des adresses.

Programmation v6

Les applications devraient en bonne logique être indépendantes du niveau transport.
Ce n'est pas vrai car elle doivent notamment mémoriser les paramètres des connexions ouvertes ou à ouvrir.
En particulier, stocker l'adresse IP du correspondant !
D'où un pb de taille de l'espace réservé.
Il y a aussi le pb de la conversion nom<->adresse(s)

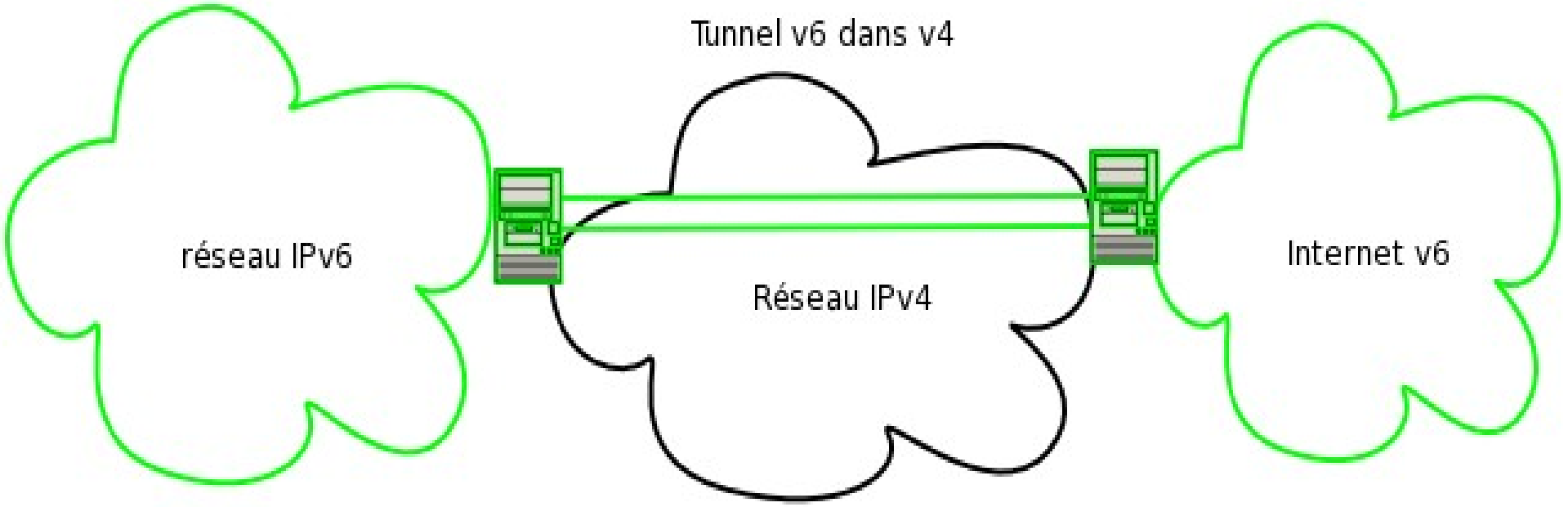
cf. « le livre » : http://livre.g6.asso.fr , chapitre « programmation d'applications »

Transition – Accès à v6

La solution pour qu'une machine ou un réseau ne possédant qu'une adresse v4 accède à v6 consiste en :

- la configuration en double pile des machines
- la mise en place d'un "tunnel" encapsulant les datagrammes v6 dans des datagrammes v4 circulant entre la machine ou une machine du réseau et une machine ayant accès à l'Internet v6, et possédant également une double pile.

Transition – tunnel



La machine double pile encapsule le DG v6, les adresses v4 de l'en-tête ajoutée sont celles des deux extrémités du tunnel (machines v4/v6)

L
a

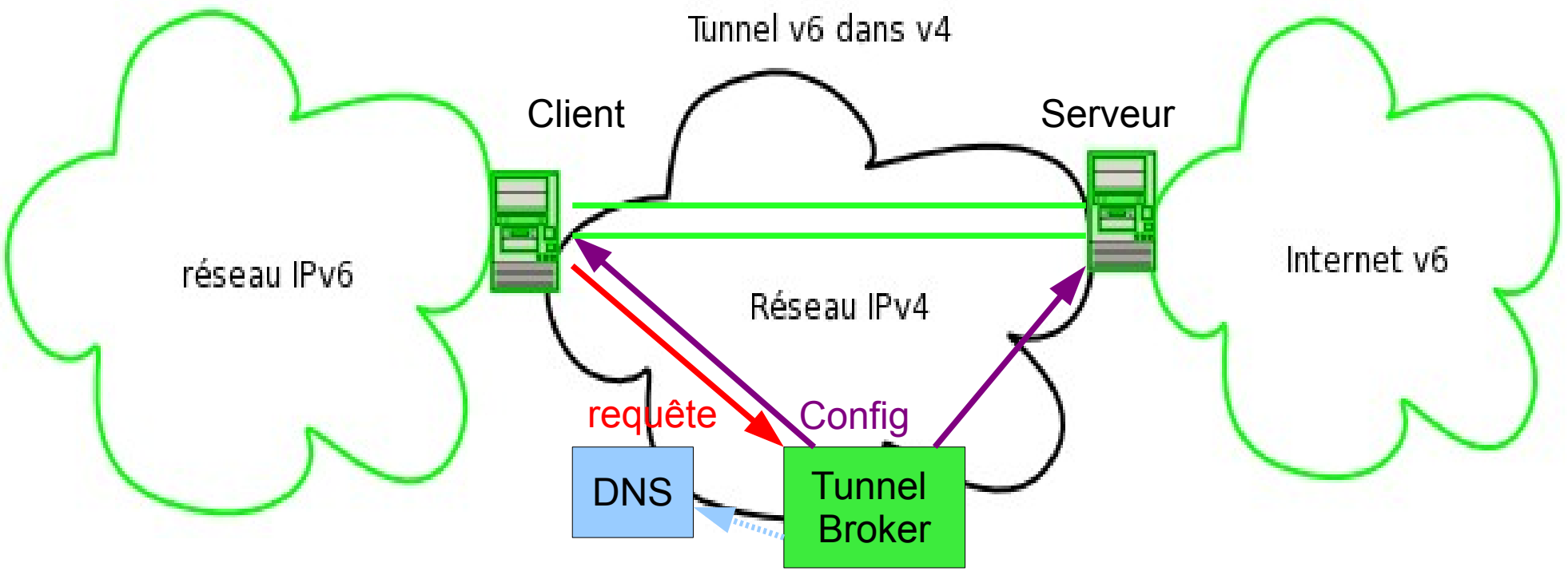
En-tête IPv4	Datagramme IPv6

Transition – tunnel

Le tunnel peut être :

- manuel : les deux extrémités "se connaissent", les administrateurs configurent le tunnel.
- automatique : un "tunnel broker" dispose de "serveurs de tunnel". Les clients lui demandent un accès et il envoie les configurations nécessaires.

Transition – tunnel auto



Mise en place automatique d'un tunnel

Tunnel et adressage

Les adresses "Ipv4-compatibles" peuvent être utilisées par les extrémités du tunnel pour communiquer entre elles en v6 :

Toutefois, leur usage intensif est déconseillé, ceci revient à utiliser un réseau v4 dans v6.

Transition – 6to4

Le mécanisme "6to4" permet à un site d'obtenir un préfixe Ipv6 spécial, les datagrammes utilisant ces adresses étant automatiquement tunnelés et transmis à un autre point d'accès 6to4 (connu ou en utilisant une adresse "anycast" bien connue).

Transition – 6to4

Format des adresses 6to4 :

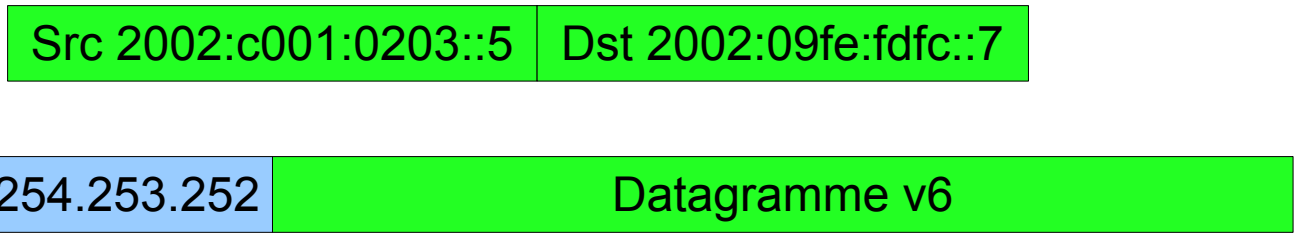
2002	Adresse V4	SLA (16 bits)	Interface (64 bits)

Exemple : adresse v4 192.1.2.3
préfixe 6to4 : 2002:c001:0203::/48
Ce préfixe (ou un /64 dérivé) peut être annoncé sur le réseau se connectant ainsi, pour autoconfiguration des machines de ce réseau.

Transition – 6to4

Deux sites 6to4 peuvent communiquer, les routeurs encapsulant les DG v6 dans un DG v4 dont les adresses sont les ad v4 des deux extrémités.

Exemple :



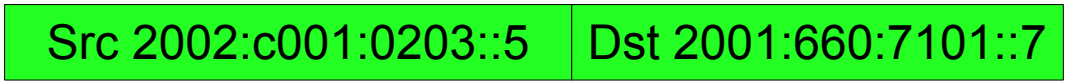
Transition – 6to4

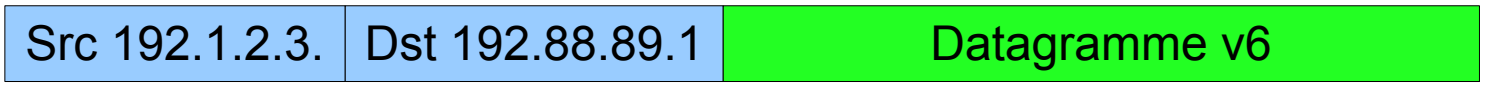
Un réseau 6to4 peut communiquer également avec le monde v6 natif, le mécanisme utilise alors une adresse bien connue : 192.88.99.1 (anycast 6to4). Ce réseau communique alors via un tunnel avec un "relais 6to4" le plus proche, qui lui-même communique avec les autres relais ou réseaux 6to4, et avec l'Internet v6 natif

Transition – 6to4

Les relais 6to4 annoncent (via BGP) l'adresse anycast 6to4de manière à pouvoir être joints en v4.
Le routeur 6to4 du réseau utilisant ce mécanisme encapsule donc les DG v6 dans des DG v4 à destination de cette adresse pour transmission au réseau v6 destinataire
Au retour, le DG est routé vers un relais 6to4 qui encapsule également en v4 vers le routeur 6to4 du demandeur.

Transition – 6to4

Exemple : 

Le routeur 6to4 recherche une route en v4 vers 192.88.99.1. Il encapsule alors le dg v6 dans un dg v4: 

Ici, le dg v6 est transmis par le relais 6to4 via le routage v6 ordinaire. Si la destination était une autre adresse 6to4, il serait transmis de relais en relais 6to4 jusqu'au réseau concerné.

Transition – 6to4

Le mécanisme 6to4 utilise des tunnels, mais la configuration est simple:
Il suffit en effet de l'activer, le préfixe /48 se déduit de l'adresse Ipv4 possédée, la connexion au relais 6to4 le plus proche est automatique grâce à l'adresse anycast v4.
Le réseau de l'utilisateur peut être configuré à partir de ce préfixe avec les mécanismes habituels v6 (sous-adressage, auto-configuration)

Variante – 6to4rd

Le FAI Free fournit en France un préfixe v6 à ses clients (zones totalement dégroupées).
En fait, il fournit classiquement une adresse v4 et encapsule les DGs v6 dans des v4 en fournissant à ses clients le préfixe :
2a01:5d8:<adresse v4> ::/64
2a01:5d8 ::/32 est le préfixe de Free. Il lui faudrait un préfixe plus court pour offrir des sous-réseaux à ses clients.

Transition – traduction

Pour communiquer entre v4 et v6 :
Nécessité d'une TRADUCTION du DG
De plus, il faut "faire croire" à la machine v6 qu'elle dialogue avec une autre machine v6, et de même en v4.
Utile pour qu'une machine v6-only puisse dialoguer avec une machine v4-only.

Transition – NAT-PT

Combine traduction d'adresses (v6 / v4) et du datagramme.
Le Nat-PT dispose d'un pool d'adresses v4, tout comme le NAT v4 dispose d'adresses publiques.
La machine v6 doit "voir" son partenaire v4 comme s'il possédait une adresse v6
==> nécessité d'un relais au niveau du DNS.

Transition – NAT-PT

Combine traduction d'adresses (v6 / v4) et du datagramme.
Le Nat-PT dispose d'un pool d'adresses v4, tout comme le NAT v4 dispose d'adresses publiques.
La machine v6 doit "voir" son partenaire v4 comme s'il possédait une adresse v6
==> nécessité d'un relais au niveau du DNS.

NAT-PT et DNS-ALG

Principe :
La machine v6 lance une requête DNS (de type AAAA) pour obtenir l'@IP du correspondant.
Le DNS-ALG intercepte cette requête et envoie les deux requêtes de type A et de type AAAA.
S'il y a une réponse de type AAAA, on utilisera v6, sinon le DNS-ALG modifie la réponse de type A en indiquant à la machine v6 :<prefix>::<@v4>, où <prefix> a été configuré pour NAT-PT

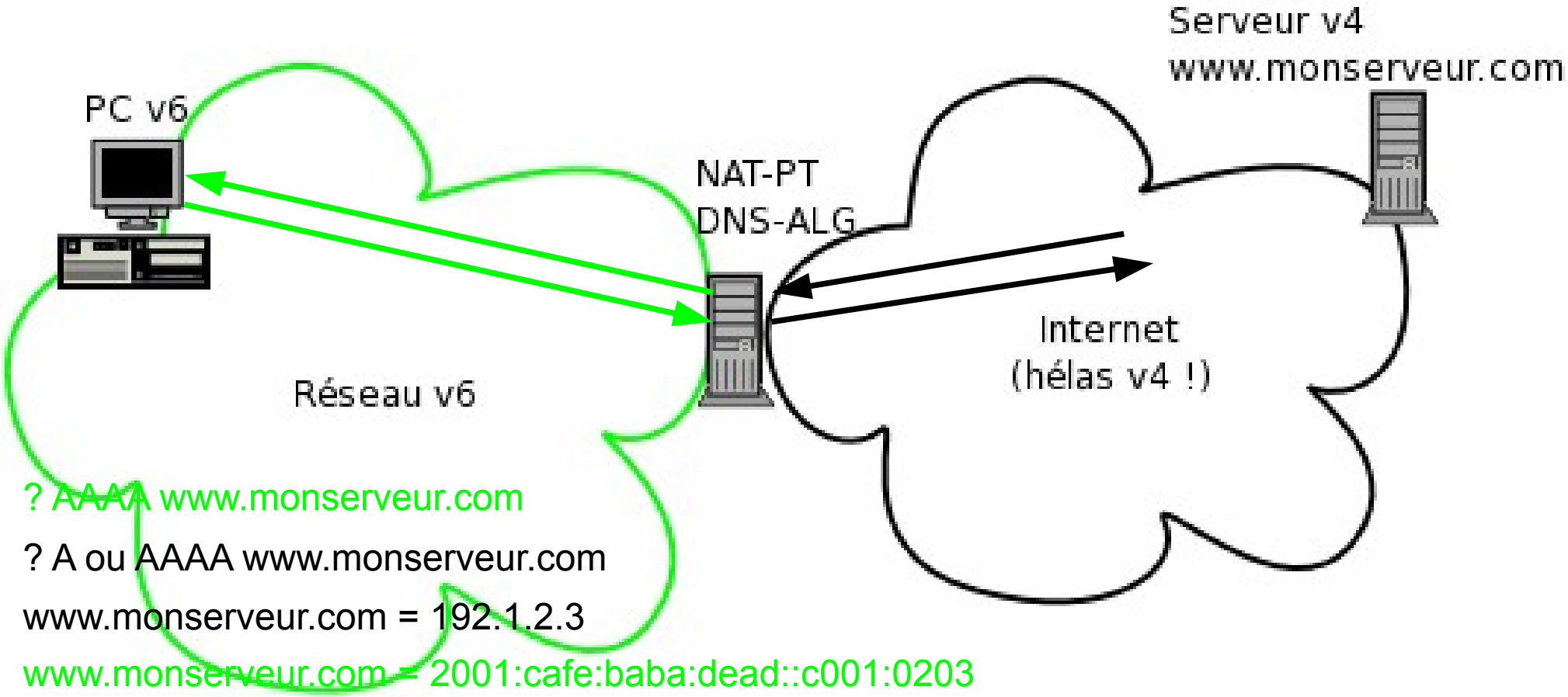
NAT-PT et DNS-ALG

Exemple : prefix = 2001:cafe:baba:dead::/96
(en fait n'importe quoi, il suffit de laisser 32 bits)
réponse à la requête :192.1.2.3
Adresse v6 annoncée à la machine demandeuse:
2001:cafe:baba:dead:0:0:c001:0203
La machine va donc dialoguer avec cette adresse imaginaire.

NAT-PT et DNS-ALG

Bien entendu, tout datagramme commençant par le prefixe sera transformé par le NAT-PT :
Traduction en un datagramme v4, utilisant une adresse v4 disponible en source, et 192.1.2.3 en destination.
Le NAT-PT doit mémoriser ceci pour pouvoir traduire la réponse (fonctionnement semblable à un NAT ou NAPT v4 privé / public)
==> mêmes inconvénients qu'un NAT

NAT-PT et DNS-ALG



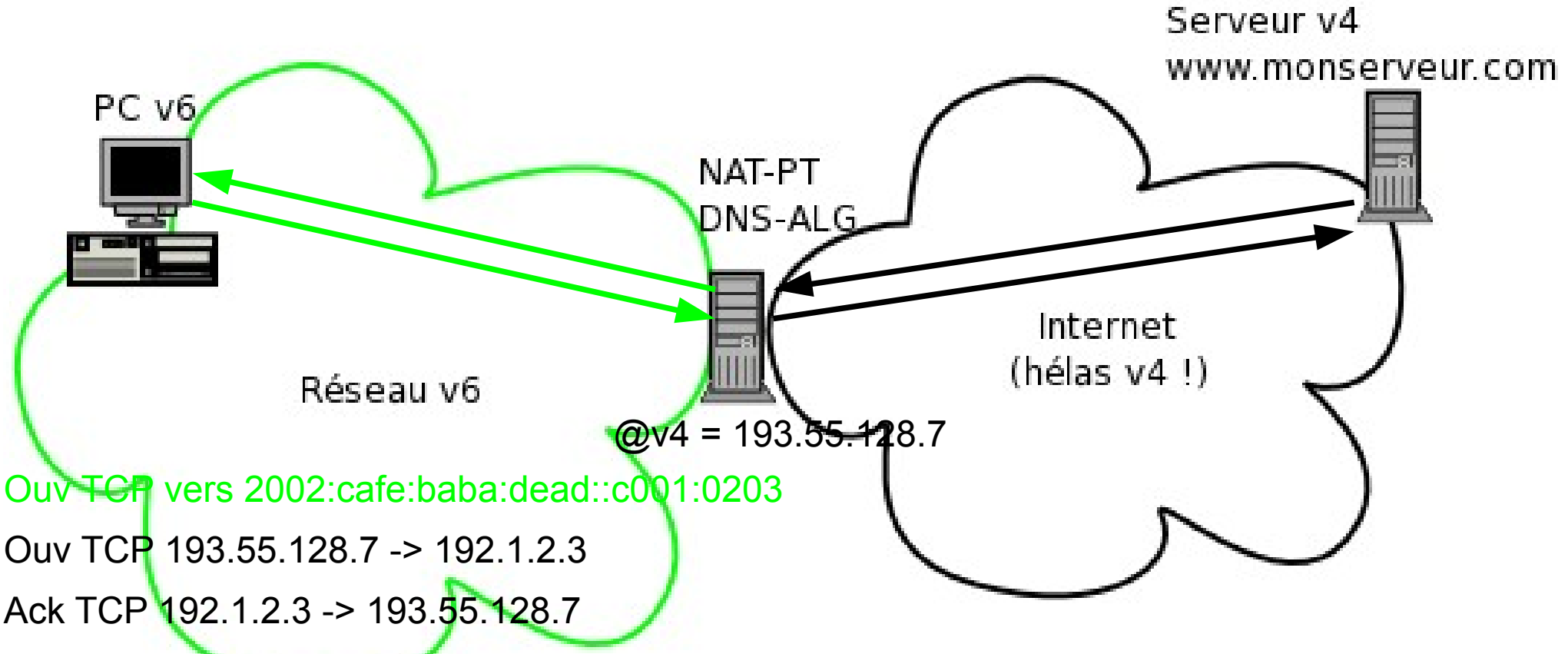
? AAAA www.monserveur.com

? A ou AAAA www.monserveur.com

www.monserveur.com = 192.1.2.3

www.monserveur.com = 2001:cafe:baba:dead::c001:0203

NAT-PT et DNS-ALG



Ouv TCP vers 2002:cafe:baba:dead::c001:0203

Ouv TCP 193.55.128.7 -> 192.1.2.3

Ack TCP 192.1.2.3 -> 193.55.128.7

Ack TCP de 2002:cafe:baba:dead::c001:0203

NAT-PT et DNS-ALG

Le préfixe NAT-PT n'a d'existence que dans le réseau v6 du site utilisant ce mécanisme.

Il faut le choisir différent de tout préfixe réel, car cela interdirait la communication avec les machines v6 ayant réellement ce préfixe.
On peut éventuellement prendre un préfixe "site-local" (en réservant un sous-réseau à cet usage)

NAT-PT « deprecated »

Le pb de NAT-PT est la charge de la passerelle qui doit :
- opérer une translation d'adresse
- être proxy-dns avec transformation des questions et réponses
- faire une traduction de datagrammes v4/v6

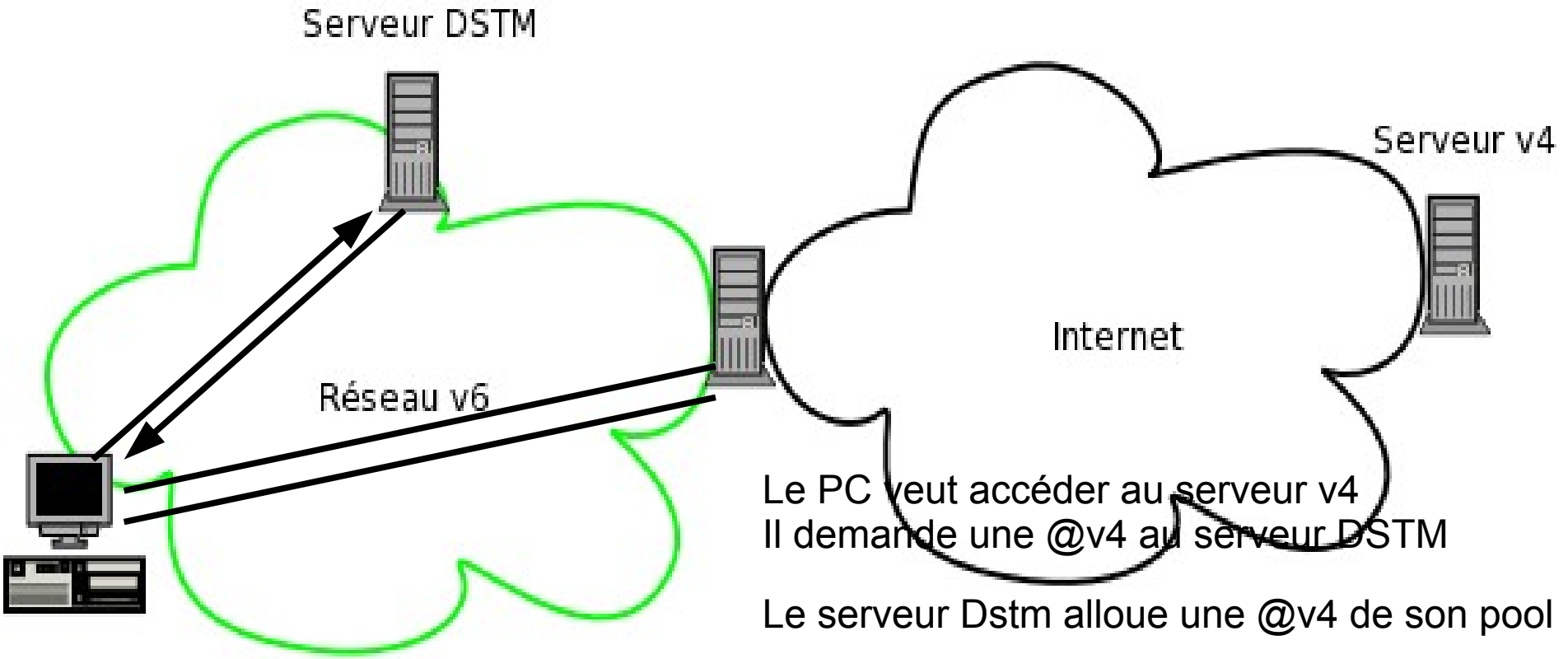
→ Utilisable pour de petits réseaux
→ Remplacé par NAT64 (sépare la fonction DNS-ALG devenue DNS64, permet le NAT inverse par translation fixe).

Transition – traduction

Autre possibilité :

Affecter temporairement une adresse v4 à la machine v6 (ou à un traducteur servant la machine v6)
Exemple : DSTM : dans un réseau v6, un serveur alloue temporairement des adresses v4 aux clients qui en ont besoin.
Les dg v4 sont encapsulés dans des dg v6 à l'intérieur du réseau v6.

Transition – DSTM



Le PC veut accéder au serveur v4
Il demande une @v4 au serveur DSTM

Le serveur Dstm alloue une @v4 de son pool

Le PC initialise sa pile v4 avec cette @
et configure un tunnel avec la passerelle DSTM

Autres mécanismes

La plupart des mécanismes ci-dessus nécessitent une adresse v4 au moins, donc ne règlent pas le problème du manque de ces adresses.
La difficulté est de passer les NATs (pour v6 comme pour v4).
Selon les types de Nats, il existe des solutions, pouvant être exploitées pour du v6.
Exemple : Teredo
Voir cours spécifique complémentaire NATs

Relais applicatifs

Une manière de traduire les dg v4 en v6 ou inversement est de remonter au niveau application. Exemples :

- serveur de courrier
- relais DNS (DNS-ALG)
- proxy http

Ceci peut être utilisé conjointement avec d'autres mécanismes.

Réseau "v6-only" ?

Il faut vérifier la compatibilité v6 de toutes les applications utilisées, par exemple :

- partage de fichiers en réseau
- systèmes d'authentifications en réseau
- agendas partagés
- ... et bien sûr systèmes d'exploitation !

L'accès à v4 est alors du même niveau qu'avec un NAT ordinaire privé/public. Les applications v6 offrent des possibilités supplémentaires.