

IPv6

Co- existence et transition IPv4- IPv6

Alain Patrick AINA
aalain@afrinic.net

Co-existence et transition IPv4-IPv6

- Un large éventail de techniques :

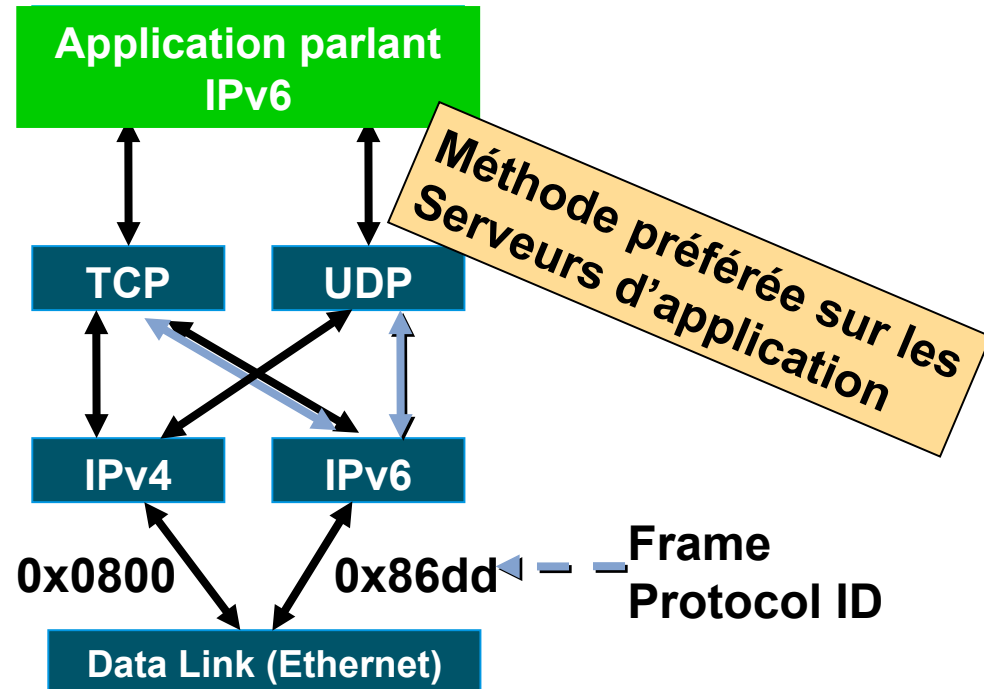
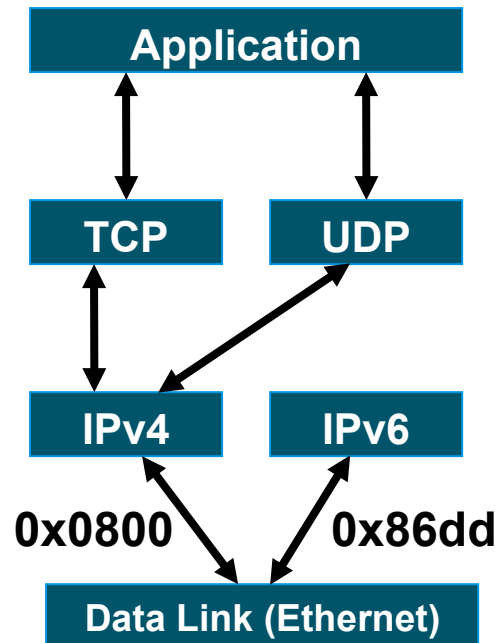
Techniques Dual-stack, IPv4 et IPv6 co-existent sur le même noeud

Techniques de Tunnel, pour éviter les dépendances dans la déploiement

Techniques de Translation, permettre des hôtes pur IPv6 et communiquer à des hôtes pur IPv4

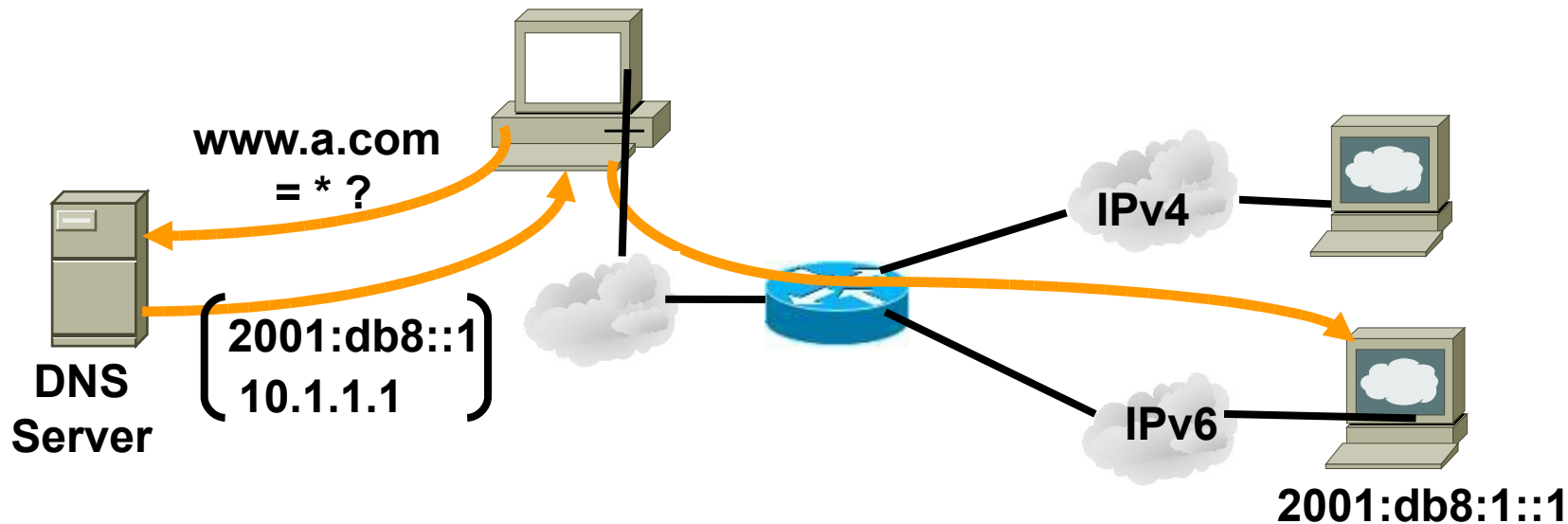
- On utilise les trois en combinaison

Approche Dual-Stack



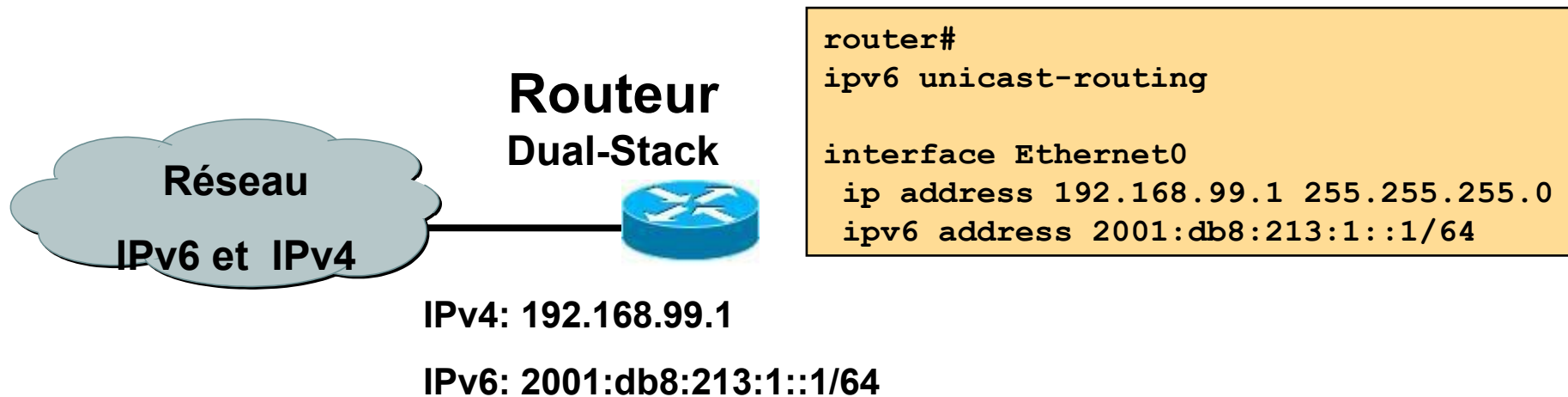
- Dual stack implique:
 - Piles IPv4 et IPv6 activées
 - Les applications communiquent avec IPv4 et IPv6
 - Le choix de la version IP est basé sur le résultat de la requête DNS ou de la préférence de l'application.

Approche Dual-Stack & DNS



- Dans le cas dual stack, une application :
 - Qui communique en IPv4 et IPv6
 - Demande tous types d'adresses au DNS
 - Choisit une adresse, et par exemple, se connecte à l'adresse IPv6

Configuration Dual-Stack



■ Routeur IPv6

Si IPv4 et IPv6 sont présents sur la même interface
Telnet, Ping, Traceroute, SSH, DNS client, TFTP,...

Tunnels Pour le déploiement Dual-Stack

- Plusieurs techniques possibles:

Configurer manuellement

- Tunnel manuel (RFC 2893)
- GRE (RFC 2473)

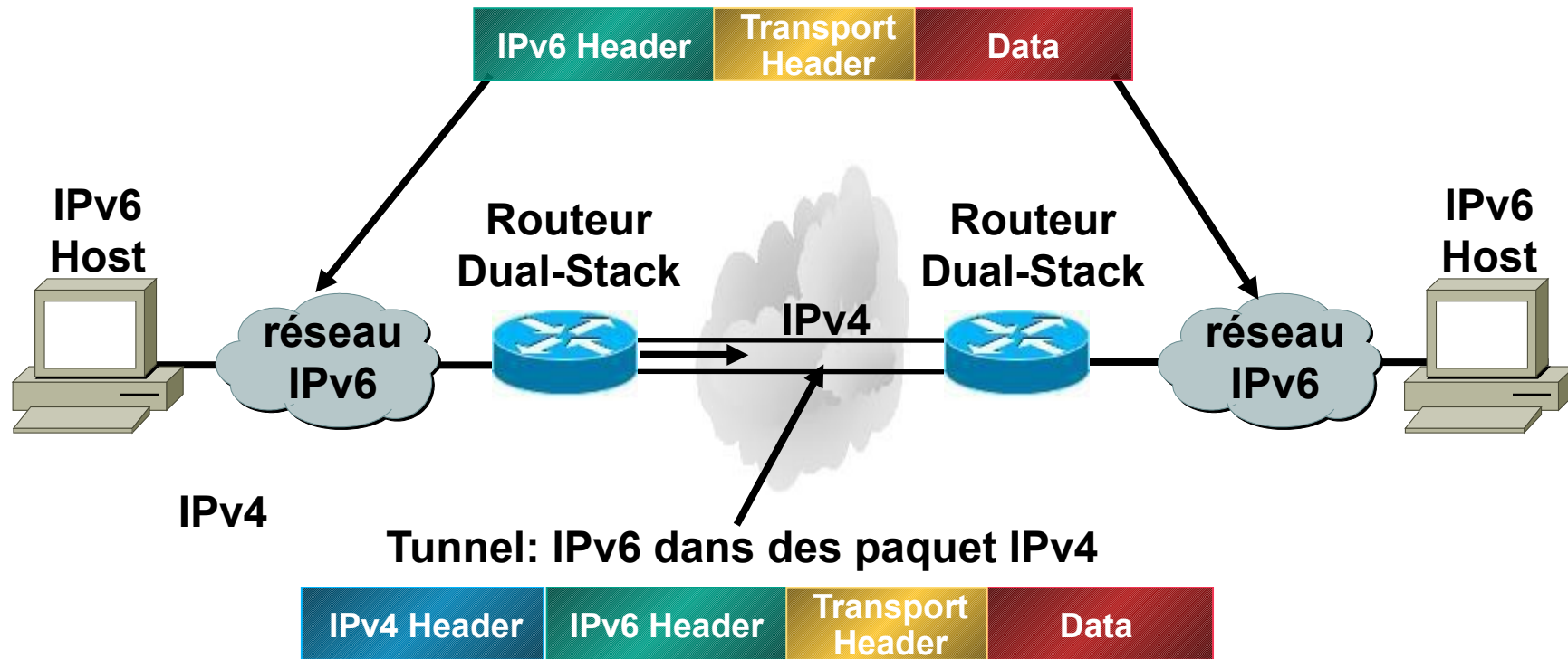
➤ Semi-automatiques

Tunnel broker

➤ Automatiques

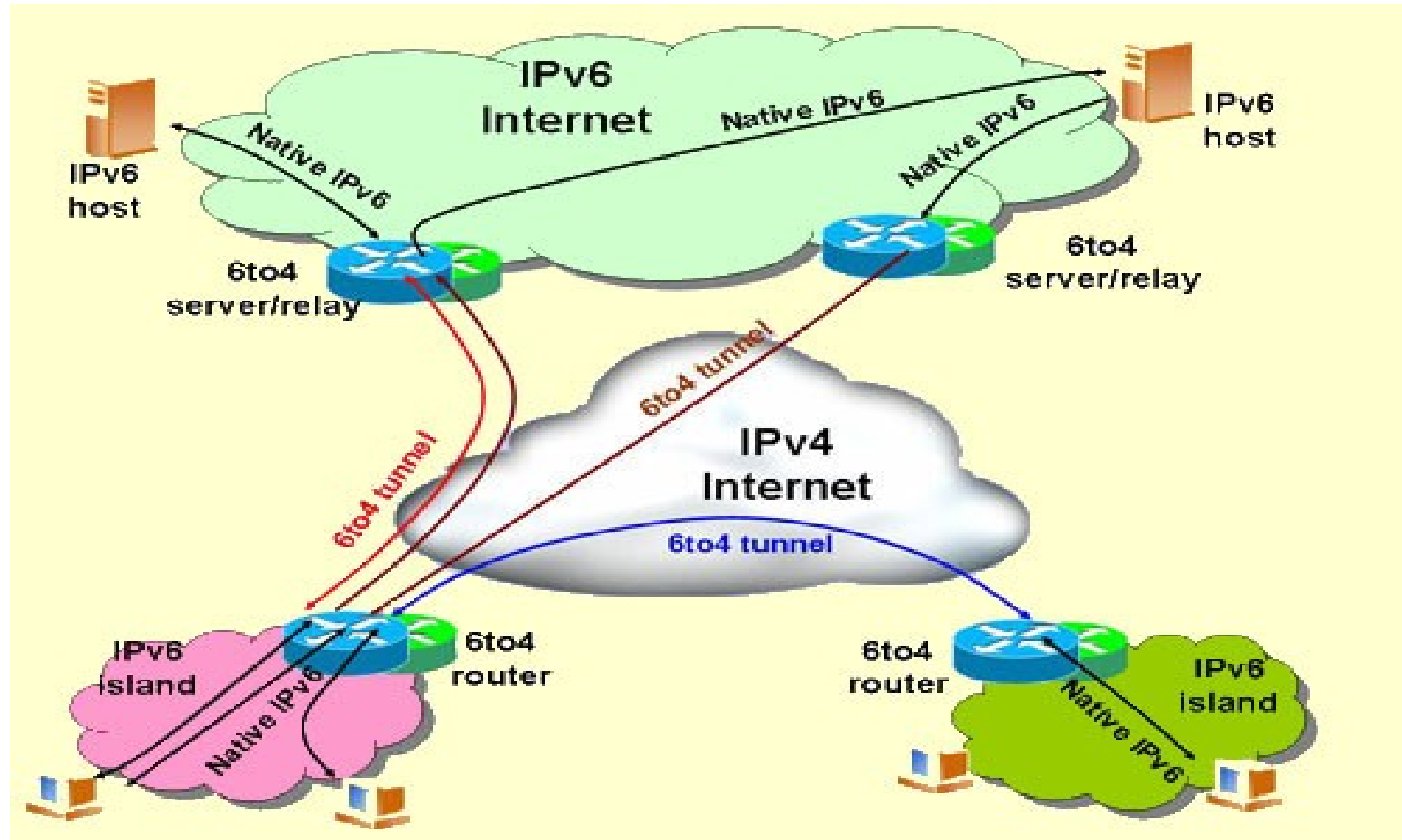
- 6to4 (RFC 3056)
- ISATAP
- 6rd

Tunnels IPv6 sur IPv4



- Encapsulation des paquets IPv6 dans IPv4
- On peut utiliser cette technique pour des hôtes ou des routeurs.

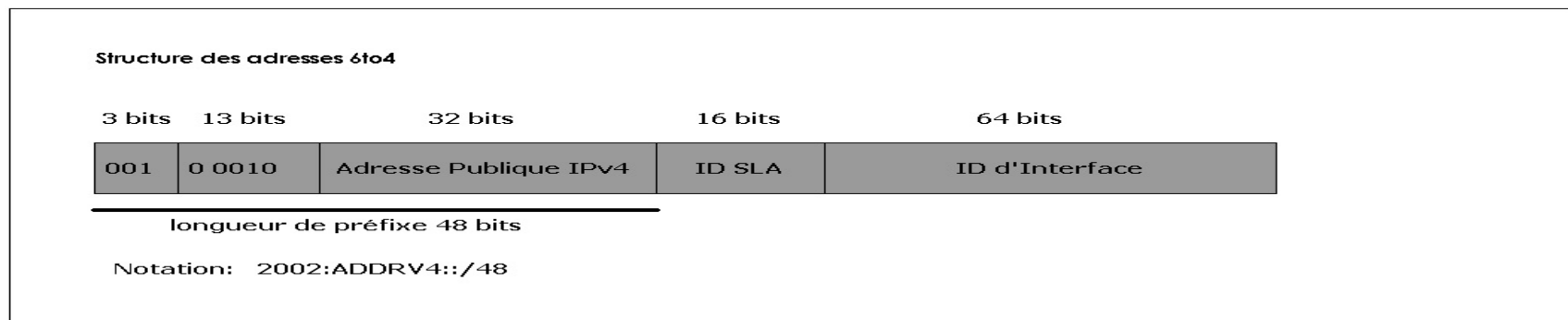
6to4(1)



6 to 4 (2)

■ Mécanisme standard de communication entre sites IPv6 sans configuration explicite de tunneling.

- L'approche 6to4 a été conçue pour permettre à des sites IPv6 isolés de se connecter ensemble sans attendre que leurs FAI fournissent du transport v6
- Mieux adapté pour les extranets et les VPN.
- En utilisant des relais 6to4, les sites 6to4 peuvent aussi joindre des sites sur l'Internet IPv6
- Communication à travers des passerelles (routeurs) spécifiques 6to4
 - **Il existe plusieurs routeurs 'public' sur Internet**
- Encapsulation IPv6 dans IPv4. Au moins une adresse unicast public est requise
- 2002::/16
- Un préfixe anycast IPv4 a été assigné aux routeurs relais 6to4: **192.88.99.0/24**



Teredo

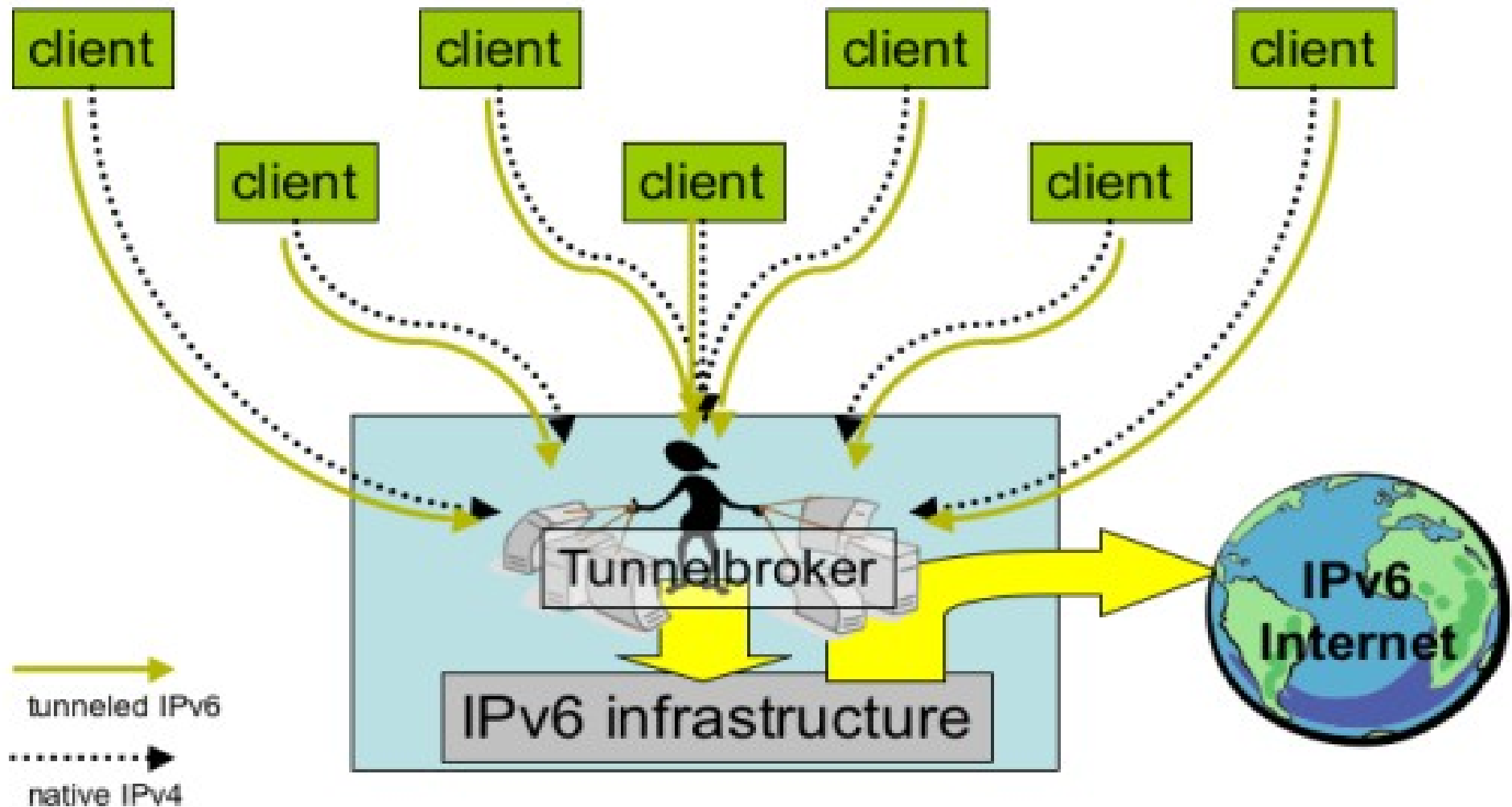
■ Teredo(RFC 4380)

- - Un service qui permet aux machines situées derrière un ou plusieurs NAT d'obtenir une connectivité IPv6 en créant un tunnel des paquets sur UDP
- - Utilise des serveurs et relais Teredo
- - Adresse Teredo sous le préfixe 2001:0000:/32
- - Section 3.2.1. Quand utiliser Teredo
- “Teredo is designed to robustly enable IPv6 traffic through NATs, and the price of robustness is a reasonable amount of overhead, due to UDP encapsulation and transmission of bubbles. Nodes that want to connect to the IPv6 Internet SHOULD only use the Teredo service as a "last resort" option: they SHOULD prefer using direct Ipv6 connectivity if it is locally available, if it is provided by a 6to4 router co-located with the local NAT, or if it is provided by a configured tunnel service; and they SHOULD prefer using the less onerous 6to4 encapsulation if they can use a global¹⁰ IPv4 address”

Tunnel Broker(1)

- Tunnel Broker(RFC 3053)
 - Tunnel Broker utilise une autre approche basée sur des serveurs dédiés appelés “Tunnel Brokers” qui gèrent automatiquement les demandes de tunnel des utilisateurs
 - Tunnel Broker est bien adapté pour les petits sites IPv6 isolés, et spécialement les machines IPv6 isolées sur l'Internet IPv4, qui veulent se connecter à un réseau IPv6 existant
 - Tunnel Broker permet à des FAI IPv6 de facilement gérer les contrôles d'accès des utilisateurs, renforçant ainsi leur politique sur l'utilisation des ressources réseau

Tunnel Broker(2)



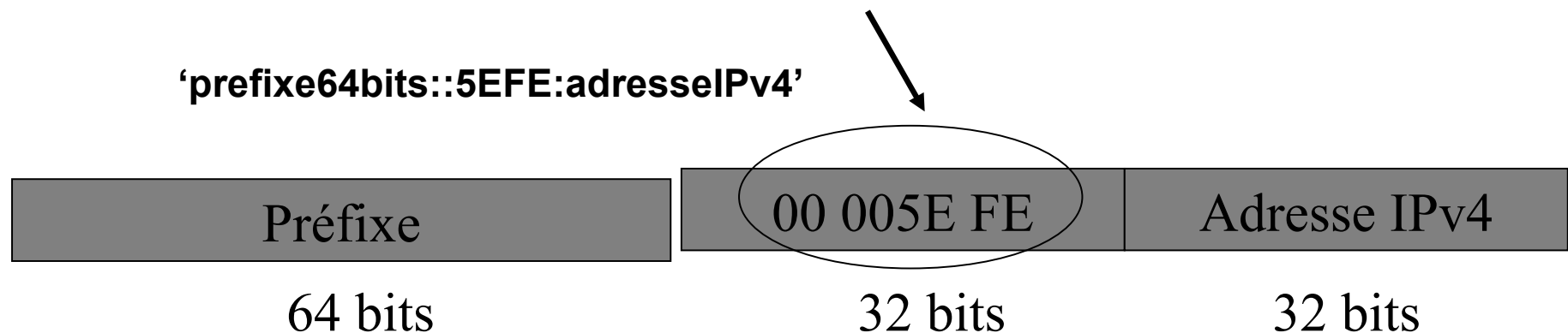
Tunnel Broker (3)

- La configuration automatique est généralement assurée par du Tunnel Setup Protocol (TSP), ou du TIC (Tunnel Information Control protocol).
- Un client capable de ceci est le AICCU (Automatic IPv6 Connectivity Client Utility)
- Pour régler les problèmes de tunnels à travers le NAT
 - Utiliser la DMZ du NAT comme terminaison de tunnel
 - AYIYA (Anything in Anything)
 - V6-UDP-V4 tunneling protocol de Hexago
- Le groupe de travail de l'IETF softwire essaye d'harmoniser les techniques de configuration automatique

ISATAP(expérimental)

■ Intra-Site Automatic Tunnel Addressing Protocole

- Tunneling pour intranet n'ayant pas de routeur IPv6
- Intégration de l'adresse IPv4 dans l'ID Interface (64 derniers bits)
- Présentation



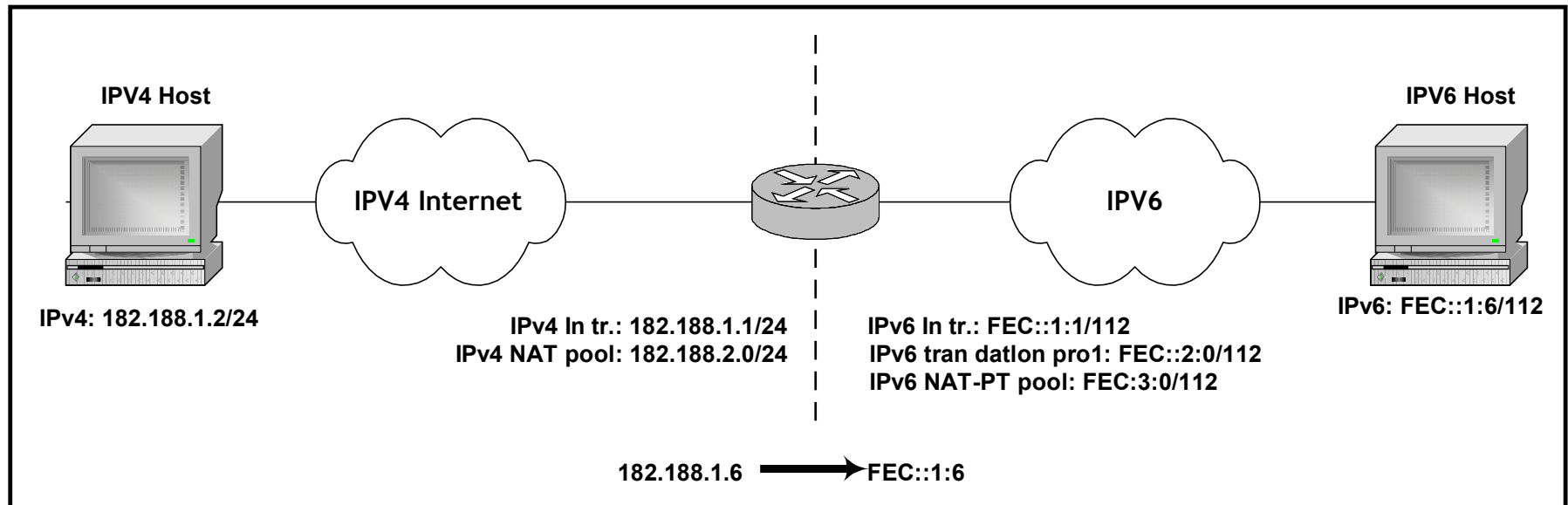
DSTM: Dual Stack Transition Mechanism

- La technique DSTM fournit une unique solution au problème de transition IPv4-IPv6. Ce mécanisme est conçu pour réduire rapidement la dépendance vis à vis du routage IPv4 et est destiné aux réseaux uniquement IPv6 où les machines ont toujours besoin occasionnellement d'échanger d'information directement avec d'autres machines ou applications IPv4.
- L'administration du réseau est simplifiée et le besoin d'adresses globales IPv4 est réduit. DSTM peut être intégré à un Tunnel Broker IPv6 pour une intégration de sécurité plus serrée.
- <http://www.ipv6.rennes.enst-bretagne.fr/dstm/>

Interopérabilité & transition Translation(1)

- **Les “translateurs” sont des équipements capable d'assurer la translation de trafic IPv4 vers IPv6 et vice versa.**
 - **Supposés éliminer le besoin de double pile**
 - **Solution de dernier recours, car la translation interfère avec le end to end**
 - **Besoin de DNS ALG**
 - **NAT-PT**
- **L'utilisation des “translateurs” de protocoles crée des problèmes avec le NAT et réduit considérablement l'utilisation de l'adressage IP.**

Interopérabilité & transition Translation(2)



IPv6

Questions?

Ready to go now ?