Plan

Chapitre 4 techniques de migration ipv4-ipv6

Introduction

Un mécanisme de transition est une méthode ou un procédé pour connecter des hôtes/réseaux utilisant les mêmes ou des protocoles IP différents.

La transition de l'IPv4 à l'IPv6 ne peut se faire que d'une manière progressive qui va s'étaler sur une longue période en raison de la complexité de la taille de l'internet et du nombre énorme de dispositifs connectés au temps actuel.

Pour cette raison différents mécanismes de transition peuvent être utilisés pendant la phase de la transition.

Pour faire communiquer des machines IPv4 avec des machines IPv6, il est nécessaire d'implémenter des mécanismes de traduction ou de conversion de paquets.

Comme il ya des différences entre IPv4 et IPv6, ces mécanismes ne peuvent pas marcher dans toutes les circonstances. Il se peut que certains protocoles et certaines options (mobilité, qualité et de service) ne marchent pas (ou de façon dégradé) avec des mécanismes de traduction.

Ce chapitre porte sur l'étude de migration des réseaux IP de la version v4 à la version v6. Cette évolution (à prévoir dans les années à venir) va poser un certain nombre de problèmes.

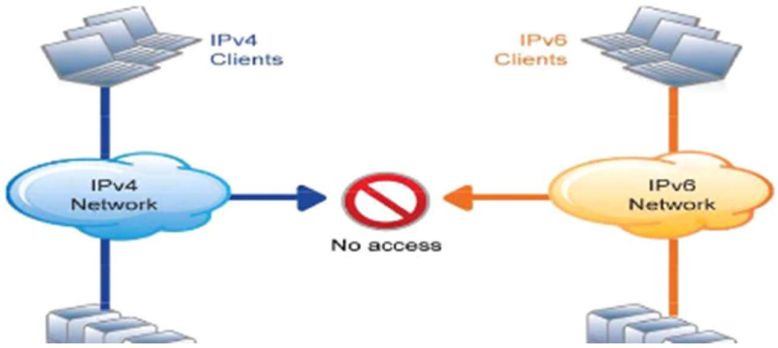


Figure 1: Absence de passerelle ou de compatibilité entre IPv4 et IPv6

I. Techniques de migration réseaux IPv4 vers IPv6

Le passage d'un réseau IPv4 à un réseau IPv6 est prévu pour durer très longtemps. Il est donc nécessaire pendant cette période de transition de permettre aux machines IPv4 et IPv6 de cohabiter et de communiquer entre elles.

Les mécanismes de transitions peuvent être classés en 3 familles : Double pile, Tunneling et Translation.

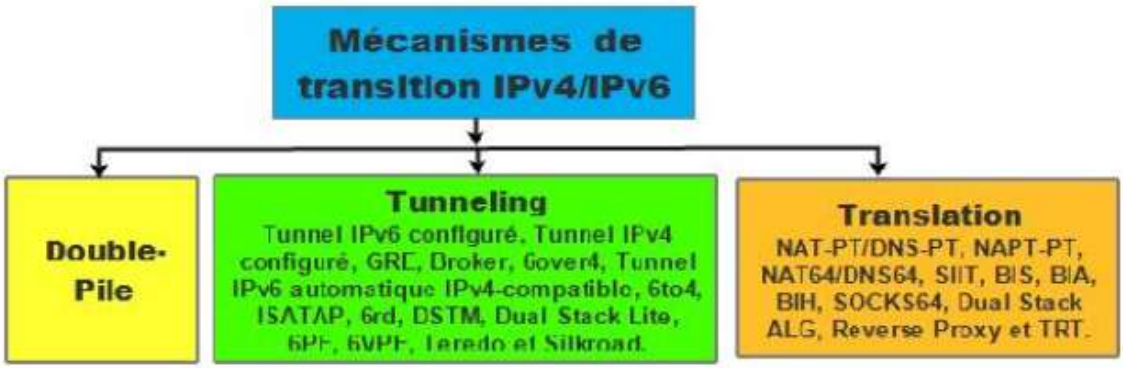


Figure 2: Classification des mécanismes de transition

Pour faciliter cette transition plusieurs solutions sont proposées. Elles reposent sur les principes suivants :

- Technique de double pile (Dual-Stack). IPv4 et IPv6 cohabitent sur le même noeud.

- Techniques de tunnel qui encapsulent le datagramme d'origine dans le protocole de destination

- Techniques de translation qui adaptent le datagramme au protocole du réseau cible (conversion de protocole).

Catégorie	Avantages	Limitations	Cas d'utilisation
Dual stack	-Communication directe entre les nœuds, -Simple à mettre en place, -Evolutive, -Cout faible, -Faible taux de perte des paquets transmis, -Compatible avec tous les systèmes d'exploitation et les équipements.	-Nécessite une adresse ipv4 pour chaque réseau, -Table de routage double, -Double politiques de sécurité, -Processeur de performance forte.	Pratique pour les réseau backbone des FAI,
Tunneling	-Simple à mettre en place, -Administration facile, -Nécessite modification de la configuration des équipements finaux seulement.	-Couteux, -Problème de NAT, -Problème de maintenance, -Lent, -Problème de sécurité.	Connecte des sites ipv6 isolés, Préférable pour les router edge et nœuds des FAI
Traduction	-Connectivité avec des adresses ipv4 seulement ou des adresses ipv6 seulement, -Autorise les FAI de modifier les adresses ipv4 publique par des adresses ipv4 privées.	-Vulnérable aux attaques DDOS, -Faible évolutivité, -N'assure pas les transitions des applications non ipv6, -Plus complexe.	Appliquée seulement pour la phase première de migration

II. Technique de la double pile

1. Principe

Cette solution dite dual-stack (DSTM, Dual Stack Transition Mechanism), la plus simple à priori, consiste à mettre en oeuvre sur chaque noeud du réseau (machines, serveurs, commutateurs, routeurs) les deux piles de protocole. Cela signifie que les deux protocoles (IPv4 et IPv6) fonctionnent côte-à-côte sur la même infrastructure et sur tous les équipements connectés au réseau.

Les applications communiquent avec IPv4 et IPv6. Cela signifie qu'on est sur un réseau IPv4/IPv6 et par conséquent on n'a pas besoin de mécanismes supplémentaires pour accéder à la fois à des machines IPv4 et à des machines IPv6. Dans ce cas, les communications sont transmises par les couches IP correspondantes aux adresses utilisées et il n'y a aucun problème de conversion.

Le choix de la version IP est basé sur le résultat de la requête DNS ou de la préférence de l'application.

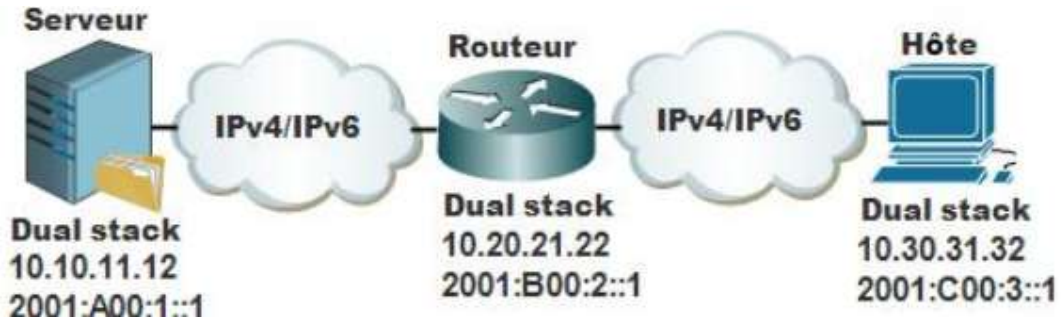


Figure 3: Réseau double pile

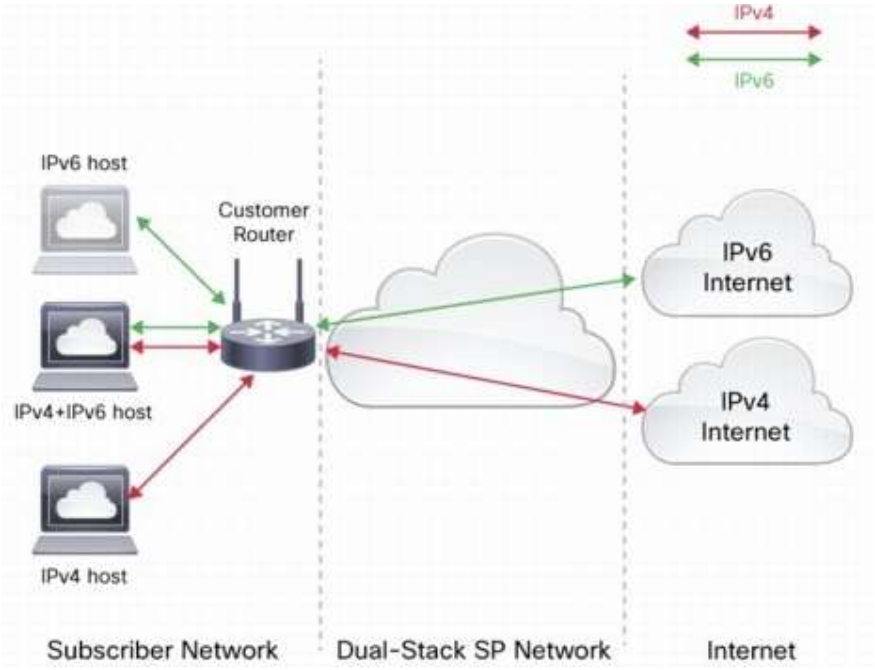


Figure 4: IPv4 and IPv6 Dual stack SP Network

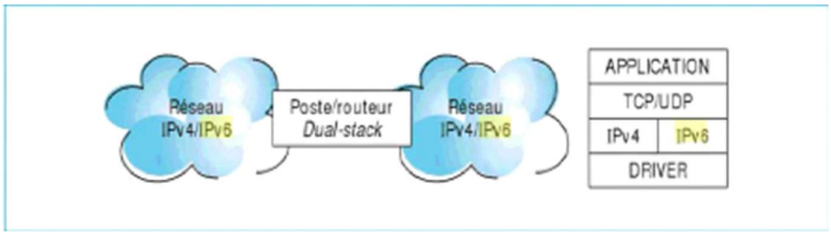
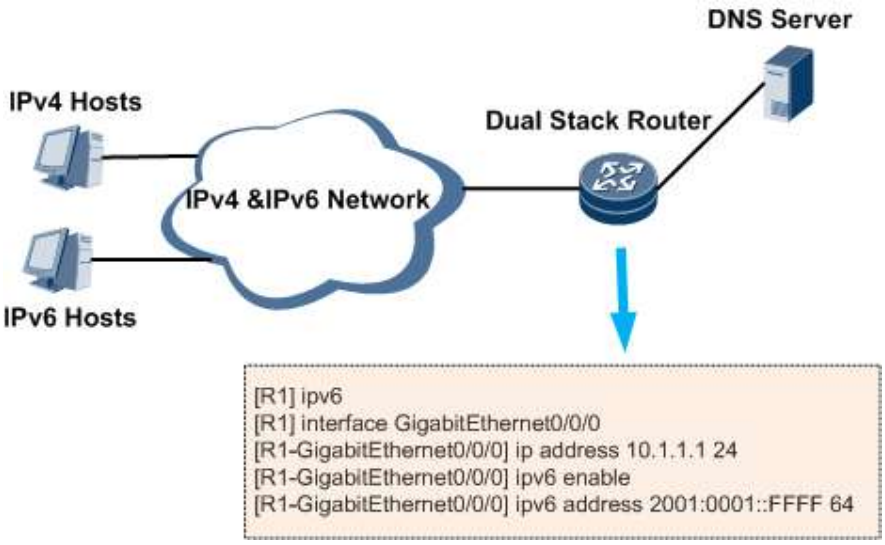


Figure 5: réseau dual-stack



2. Avantages & inconvénients

Avantages	Inconvénients
• Mécanisme de transition le plus simple à mettre en place en termes d'implémentation et configuration • Pas besoin de conversion des paquets • Pas besoin de mécanismes supplémentaires pour accéder à la fois à des machines IPv4 et à des machines IPv6 • Se connecter aux applications IPv4 existantes via IPv4 et accès aux applications IPv6 via IPv6	• Ne résout pas le problème de la pénurie des adresses IP • Augmente les coûts en termes de performance et d'utilisation CPU du fait que les deux protocoles IPv4 et IPv6 fonctionnent simultanément sur tous les équipements connectés au réseau • Augmente la complexité : o Des politiques de sécurité pour IPv4 et IPv6 o Certaines applications fonctionnent différemment dans chacun des deux protocoles

III. Technique du tunnel

1. Principe

Une alternative au déploiement massif d'un système dual-stack consiste à utiliser des tunnels pour le transport IPv6 dans IPv4 (transit de données IPv6 sur un réseau IPv4) ou l'inverse transporter de l'IPv4 sur une infrastructure IPv6.

Les mécanismes de tunneling sont des techniques dans lesquelles un protocole est encapsulé dans un autre protocole, selon le réseau où le paquet doit être acheminé.

Plusieurs mécanismes de tunneling peuvent être utilisés pour cette raison : tunnel IPv4/IPv6 configuré, 6to4, Broker, ISATAP, Silkroad, Teredo

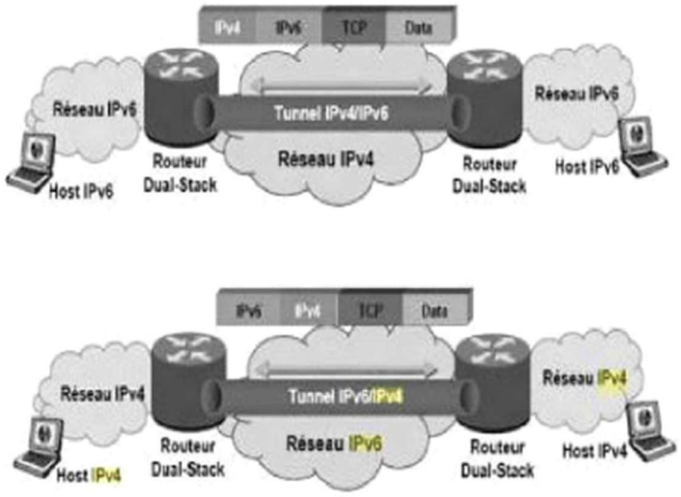


Figure 6: Principe des tunnels IPv6/IPv4 et IPv4/IPv6.

La tunnellisation est utilisée pour interconnecter des réseaux IPv6 isolés sur un réseau IPv4 ou des îlots IPv4 isolés sur un réseau IPv6.La technique de tunnellisation ne nécessite que des nœuds frontières pour implémenter une double pile et permet aux données d'une famille d'adresses de traverser le réseau d'une autre famille d'adresses via un tunnel.

Au tout début du développement d'IPv6, la technique de tunnellisation fonctionnait bien pour connecter des réseaux IPv6 isolés et déployer progressivement IPv6 sans mise à niveau à l'échelle du réseau, ce qui a progressivement élargi le champ d'application d'IPv6. Par conséquent, le tunneling est une technologie des plus intéressantes pour la transition vers IPv6 à un stade précoce. Au fur et à mesure que la transition IPv6 se développe, même les réseaux IPv4 isolés peuvent être connectés via des tunnels.

Cependant, les inconvénients de la technique de tunnellisation sont que les doubles en-têtes IP augmentent les coûts du réseau, les points de terminaison du tunnel nécessitent un travail supplémentaire sur l'évolutivité et la fiabilité, et certains problèmes de MTU peuvent survenir.

Le tableau 2-1 répertorie les techniques de tunnellisation couramment utilisées et leurs scénarios d'utilisation.

Tableau 2-1 Comparaison des techniques de tunnelisation courantes

Type de tunnel	Caractéristique technique	Usage Scenario
Tunnelier manuel	IP-in-IP ou GRE est utilisé pour l'encapsulation des paquets.	Les tunnels de ce type sont configurés manuellement. Ils sont faciles à mettre en œuvre et largement pris en charge par les périphériques réseau. Cependant, ils ne sont pas adaptés à un déploiement à grande échelle.

Type de tunnel	Caractéristique technique	Usage Scenario
Tunnelisation automatique	Le mode IPv6-in-IP est utilisé. L'encapsulation de tunnel automatique sans état est mise en œuvre via des adresses IPv6 avec des adresses IPv4 intégrées. Les adresses 6to4 utilisent le préfixe bien connu, 2002:IPv4-globe-Addr:Suffix. La caractéristique d'une adresse ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) est Prefix:0:5EFE:IPv4-Addr.	Les tunnels automatiques sont utilisés uniquement comme tunnels IPv6 dans IPv4. Ils sont implémentés via des adresses IPv4 intégrées. S'appuyant sur la topologie IPv4, les tunnels automatiques sont applicables au stade précoce de la transition IPv6. Pris en charge par les systèmes d'exploitation courants, ils conviennent aux hôtes. 6to4 a besoin d'adresses IPv4 publiques pour l'interconnexion entre les îlots IPv6. Les routeurs relais 6to4 sont utilisés pour la communication avec les hôtes IPv6 natifs. L'ISATAP n'a aucune restriction sur les adresses IPv4. Il s'applique davantage aux réseaux d'entreprise.
Tunnel MPLS	6PE / 6VPE, IPv6 en MPLS	Les tunnels MPLS ont de bonnes performances de transfert. Ils sont applicables aux cœurs de réseau. Des infrastructures MPLS sont nécessaires.

De plus, 6rd continue d'utiliser le mode de tunnellisation sans état 6to4. 6rd utilise des préfixes de fournisseur au lieu du préfixe bien connu 2002/16 utilisé dans 6to4. Ainsi, les préfixes IPv6 peuvent être libérés sur le réseau IPv6 natif, ce qui résout à son tour le problème de routage par lequel le réseau IP natif accède aux îlots 6to4.

1. Les différents types de tunnels

Les tunnels peuvent être statiques (configurés par l'administrateur) ou dynamiques.

Cette méthode voit tout son intérêt lors d'une migration d'un réseau IPv4 vers IPv6.
La passerelle d'accès au réseau examine le datagramme, si le datagramme d'arrivée correspond au protocole du réseau de transit, le datagramme est acheminé nativement ; si ce n'est pas le cas, il sera encapsulé dans un datagramme du protocole du réseau de transit.

a. Tunnel statique

Les tunnels statiques sont utilisés pour relier un réseau ou une machine IPv6 à un réseau IPv6 par l'intermédiaire d'un réseau IPv4.

Ils sont configurés à la main et sont mis en place avec une durée de vie importante.

Les machines qui sont aux extrémités du tunnel doivent avoir une double pile IPv4/IPv6 et disposer chacune d'une adresse IPv4 globale.

Les autres machines du réseau IPv6 n'ont donc pas besoin de cette double pile pour communiquer avec les machines IPv6 situées de l'autre coté du tunnel, mais elle peut être utile pour communiquer avec des machines IPv4 (sans passer par le tunnel).

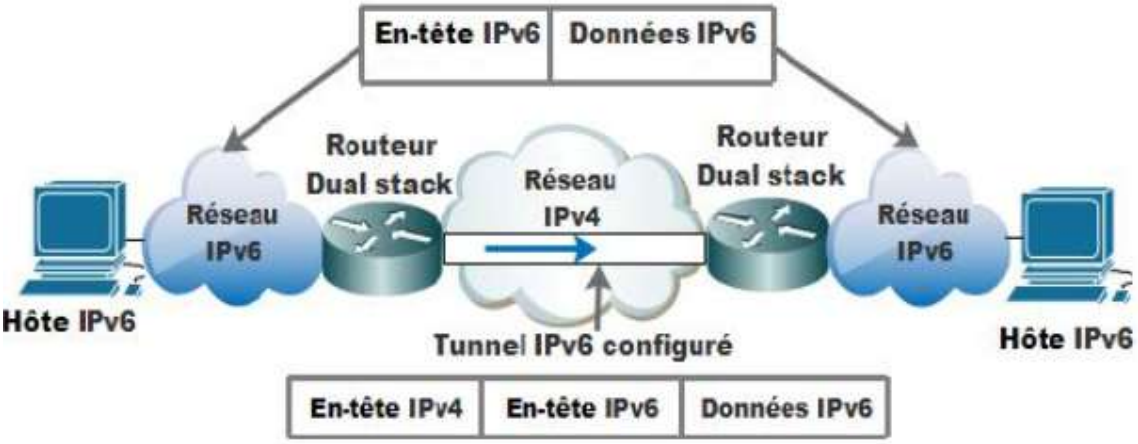


Figure 7: Tunnel configuré

Avantages	Inconvénients
• Permettre à des machines IPv6 isolées sur l'internet IPv4 d'échanger des contenus entre elles • Simple à mettre en place en terme de configuration • Idéal pour les petits réseaux	• Ne résout pas le problème de la pénurie des adresses IP • Nécessite une configuration manuelle aux deux extrémités du tunnel • Ne supporte pas les grands réseaux

b. Tunnels automatiques

Les tunnels automatiques servent à communiquer en IPv6 avec une machine connectée sur un réseau IPv4.

Cette méthode est souvent utilisée pour joindre une machine IPv6 isolée. Les deux machines établissant le tunnel doivent disposer d'une double pile IPv4/IPv6.

La machine de destination du tunnel doit être la machine destinataire du paquet, alors que la machine source du tunnel peut être la machine source du paquet ou un routeur qui a reçu le paquet sur son réseau IPv6.

Dans ce cas il faudra que la machine source possède une adresse IPv4 compatible.

Les adresses IPv4 compatible sont des adresses IPv6 particulières qui sont formées en ajoutant 32 bits d'une adresse IPv4 au préfixe ::/96.

Par exemple ::192.168.1.1 est l'adresse IPv4-compatible de 192.168.1.1.

Tunnel IPv6 GRE

Le tunnel IPv6 GRE (Generic Routing Encapsulation) est utilisé traditionnellement pour encapsuler les données IPv4 contenant une adresse privée de destination.

L'adresse de destination encapsulée n'était donc pas routable. Dans l'utilisation nous intéressant, les données IPv6 sont encapsulées à l'intérieur d'un tunnel fournissant une connexion point-à-point entre deux routeurs.

Ce tunnel a un en-tête d'encapsulation supplémentaire pour l'en-tête GRE, par conséquent, le tunnel aura un paquet IPv6 encapsulé dans l'en-tête GRE, puis dans l'en-tête IPv4.

Ce tunnel est également utilisé pour les connexions stables et n'existe qu'entre une paire de routeurs. Cette solution n'est donc pas évolutive (scalable), si le nombre de sites augmente.

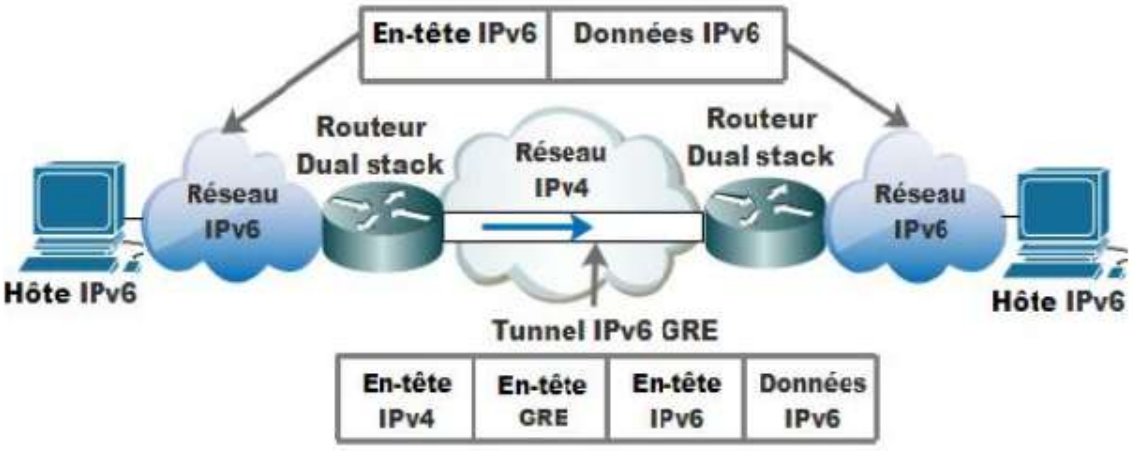


Figure 8: Tunnel IPv6 GRE

Avantages	Inconvénients
• Permettre à des nœuds IPv6 distants et isolés sur l'internet IPv4 de se connecter entre eux • Simple à mettre en place en terme de configuration • Peut réaliser plus de choses que le tunnel IP dans IP (permet d'encapsuler n'importe quel paquet de la couche 3 dans n'importe quel paquet de la couche 3)	• Ne résout pas le problème de la pénurie des adresses IP • Nécessite une configuration manuelle aux deux extrémités du tunnel • N'existe qu'entre une paire de routeurs ==>solution n'est pas évolutive (scalable)

• Idéal pour les petits réseaux et pour les connexions stables	

Tunnel Broker

Le Tunnel Broker est une société tierce fournissant un service de tunnel après une simple demande aux serveurs dédiés appelés « Tunnels Brokers » qui gèrent les demandes de tunnel des utilisateurs. Pour ce faire, il faut généralement s'inscrire chez le tunnel broker, puis demander l'ouverture du tunnel. Alors, le tunnel broker va configurer un de ses routeurs afin de mettre en place le tunnel. Enfin, il enverra un script à exécuter sur la machine souhaitant utiliser le tunnel, pour configurer correctement les paramètres réseaux. La machine est alors connectée à l'IPv6 via le service du tunnel broker.

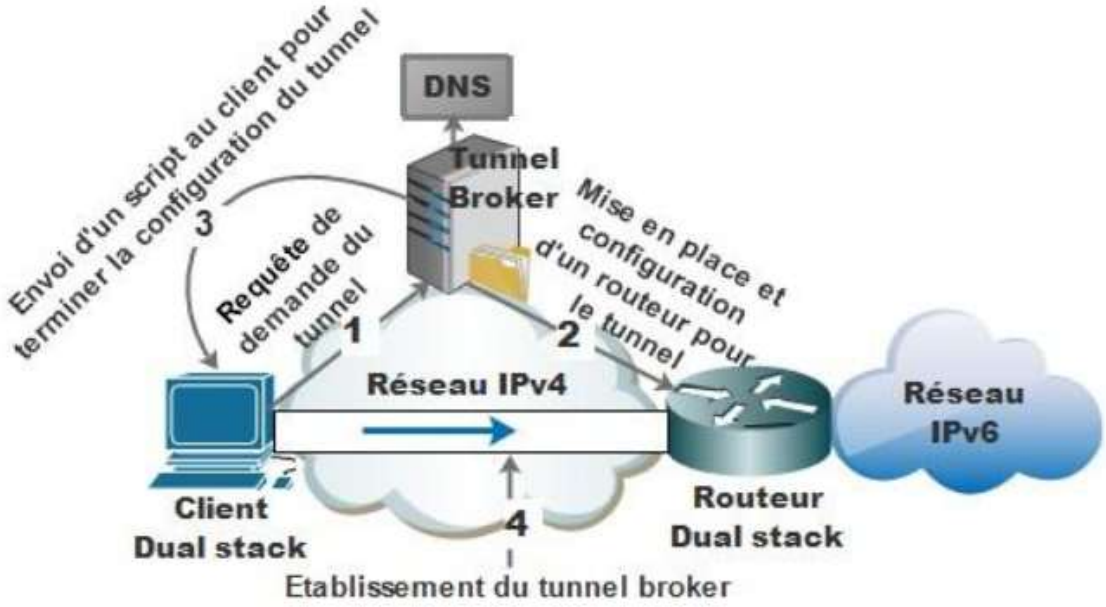


Figure 9: Tunnel Broker

Avantages	Inconvénients
• Bien adapté pour les petits sites IPv6 isolés et les machines IPv6 isolées sur l'internet IPv4, qui veulent se connecter à un réseau IPv6 existant • Mise en place semi-automatique du tunnel après une inscription et demande du tunnel depuis le client • Permet à des FAI (Fournisseurs d'Accès à Internet) IPv6 de gérer facilement les contrôles d'accès des utilisateurs, renforçant ainsi leur politique d'utilisation des ressources réseau.	• Ne résout pas le problème de la pénurie des adresses IP • Les performances dépendent de l'emplacement géographique du routeur du tunnel broker • La sécurité car le routeur du tunnel broker doit accepter des modifications de configuration depuis un serveur distant

NAT-PT

NAT-PT (Network Address Translation-Protocol Translation) fournit des possibilités de traduction bidirectionnelle pour les communications entre des postes IPv4 seul et des postes IPv6 seul.

La traduction est initialisée par la requête DNS initiale ; elle nécessite l'ajout d'une traduction DNS spéciale (DNS ALG)

L'ALG (Application Layer Gateway) est utilisée pour supporter la traduction d'applications contenant des adresses IP au niveau de la couche applicative. NAT-PT intercepte les paquets à la frontière entre les réseaux IPv4 et IPv6, traduit l'en-tête au format du réseau de destination. Il dispose d'un pool d'adresses IPv4 pour en allouer le cas échéant à un poste IPv6.

Le fonctionnement est transparent pour l'utilisateur et aucun paramètre n'est nécessaire au niveau du poste.

NAT-PT peut être étendu à NAPT-PT (Network Address Port Translation - Protocol Translation). En combinant un numéro de port à l'adresse IPv4, il est possible d'utiliser la même adresse IPv4 pour identifier plusieurs postes IPv6.

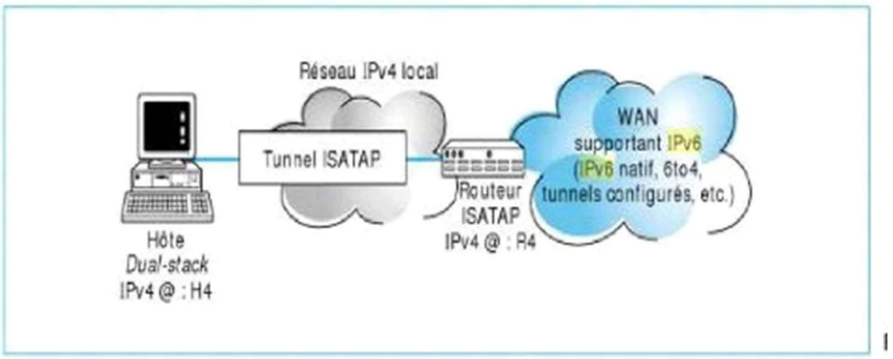
ISATAP

ISATAP (Intra-site Automatic Tunnel Addressing Protocol) a été définie pour fournir une connectivité IPv6 à des équipements terminaux ou des routeurs au sein de réseaux IPv4 et pour ainsi permettre un premier déploiement d'applications IPv6, l'infrastructure IPv4 étant vue comme une technologie de niveau liaison.

La méthode ISATAP utilise un format d'identificateur de machine qui inclut l'adresse IPv4.

64	16	16	32 bits
Standard IPv6 Prefixe	0	5EFE	IPv4 @

/ 64



6to4

C'est une autre façon automatique pour connecter des hôtes/sites IPv6 entre eux en encapsulant les paquets IPv6 dans des entêtes IPv4 et traversant une infrastructureIPv4,

L'encapsulation de ces paquets se fait par un routeur 6to4 dont l'adresse IPv6 est 2002:@IPv4(Hexa)::/48.

L'adresse IPv4 du point final du tunnel peut être intégrée dans l'adresse 6to4 de destination. Parfois il y'a l'utilisation d'un routeur relais, au cas où un hôte 6to4 envoie un paquet IPv6 à un nœud IPv6 natif résidant sur un réseau IPv6 natif, les paquets IPv6 sont encapsulés dans IPv4 par le routeur 6to4 et acheminés vers le routeur relais qui est accessible par l'adresse IPv4 anycast 192.88.99.1. Ces paquets une fois arrivés, le routeur relais à son tour, en supprime l'entête IPv4, puis transmet le paquet IPv6 à l'hôte IPv6 approprié.

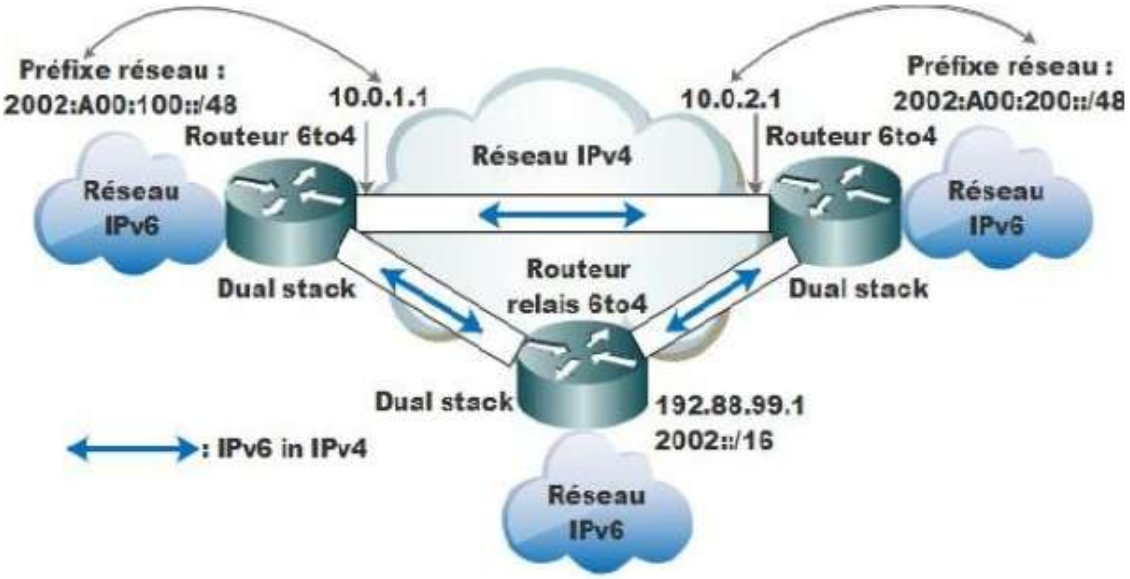


Figure 10: Architecture 6to4

Avantages	Inconvénients
• Tunnel automatique pour relier un site ou LAN IPv6 à l'internet IPv6 par une connexion à internet par IPv4 • Toute machine qui dispose d'une adresse IPv4 globale (routable) peut utiliser le 6to4 • Le format des paquets est le même que pour le tunnel statique, mais les paquets sont échangés entre de très nombreuses machines supportant le 6to4 (tunnel point à multipoints)	• Ne résout pas le problème de la pénurie des adresses IP • la sécurité, car l'administrateur du routeur relais, constituant la frontière entre le site 6to4 et le site IPv6 natif, n'as pas le moyen de contrôler qui utilise le service (le trafic est accepté de partout). • 6to4 peut induire un routage asymétrique et les délais peuvent être très élevés à cause des tunnels. • N'est pas une solution globale Connecte uniquement des ilots IPv6 ! pas de communication possible entre des machines IPv4-only & IPv6-only ▪ Pas de traversée de NAT

6rd

6rd (IPv6 Rapid Deployment) est un mécanisme de transition utilisé par certains fournisseurs de services pour déployer rapidement IPv6 à leurs clients qui veulent utiliser IPv6 sur une infrastructure IPv4 existante.

6rd a repris les principes de fonctionnement du protocole 6to4, tout en corrigeant ses défauts. Au lieu d'utiliser un seul et unique préfixe (2002::/16 pour 6to4), 6rd utilise un préfixe différent pour chaque FAI, de même les routeurs 6to4 sont remplacéspar des routeurs 6rd et le routeur relais par un routeur BR(Border Relay) qui est accessible par l'adresse IPv4 anycast 10.1.1.1.

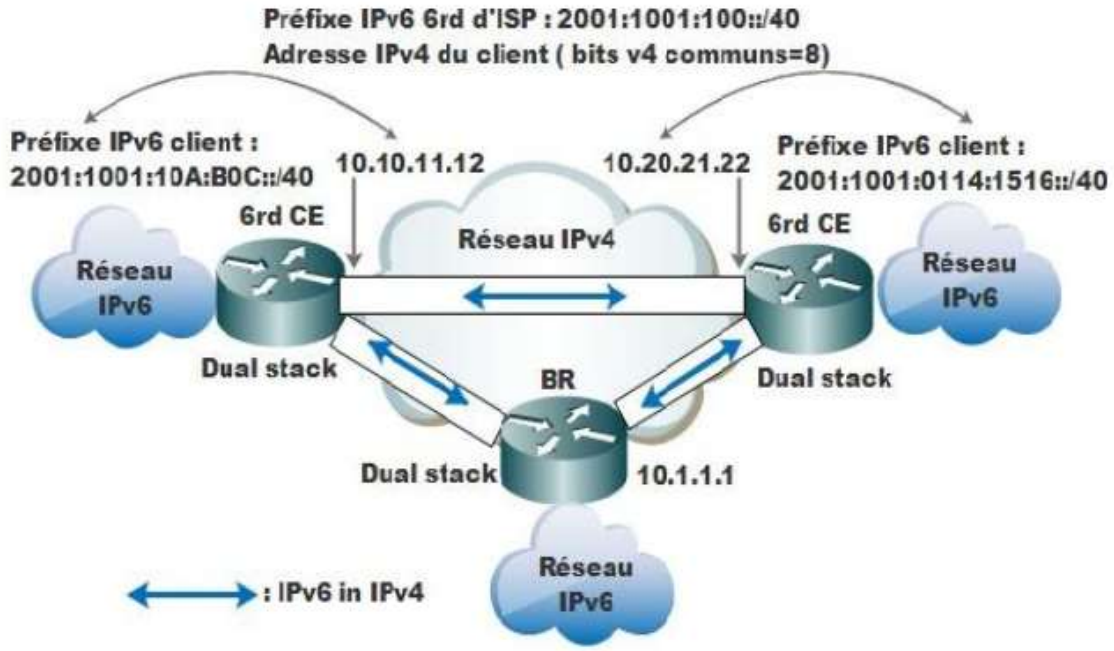


Figure 11: 6rd

Avantages	Inconvénients
Permettre à des nœuds IPv6 isolés sur l'internet IPv4 de se connecter entre eux • Rapide à déployer - tous les CPEs ont la même configuration • Utilise un préfixe différent pour chaque FAI au lieu d'un seul et unique préfixe (2002::/16) en 6to4 • Efficace en raison de son mode de fonctionnement apatride qui est léger et naturellement évolutif	• Ne résout pas le problème de la pénurie des adresses IP • Nécessite un équipement compatible 6rd, par exemple un routeur compatible 6rd localisé au niveau de l'utilisateur final • 6rd peut induire un routage asymétrique (les délais peuvent être très élevés) • Ne traverse pas les NATs

Teredo

Ce mécanisme permet aux nœuds situés derrière un ou plusieurs NATs IPv4 d'obtenir une connectivité IPv6 en encapsulant les paquets IPv6 dans des paquets UDP puis dans IPv4.

L'hôte Teredo obtient d'abord un préfixe IPv6 à partir du Teredo Server, puis l'adresse IPv6 est formée comme suit : PrefixTeredoServer:Server IPv4:Flags:Port:client IPv4. La communication entre les clients Teredo peut être faite directement avec le tunnel IPv6 in UDP in IPv4. La connectivité vers le réseau IPv6 sera atteinte par le Teredo Relay Gateway. Les tunnels automatiques entre les hôtes Teredo distribuent le trafic entre eux et partagent le Teredo Relay Gateway.

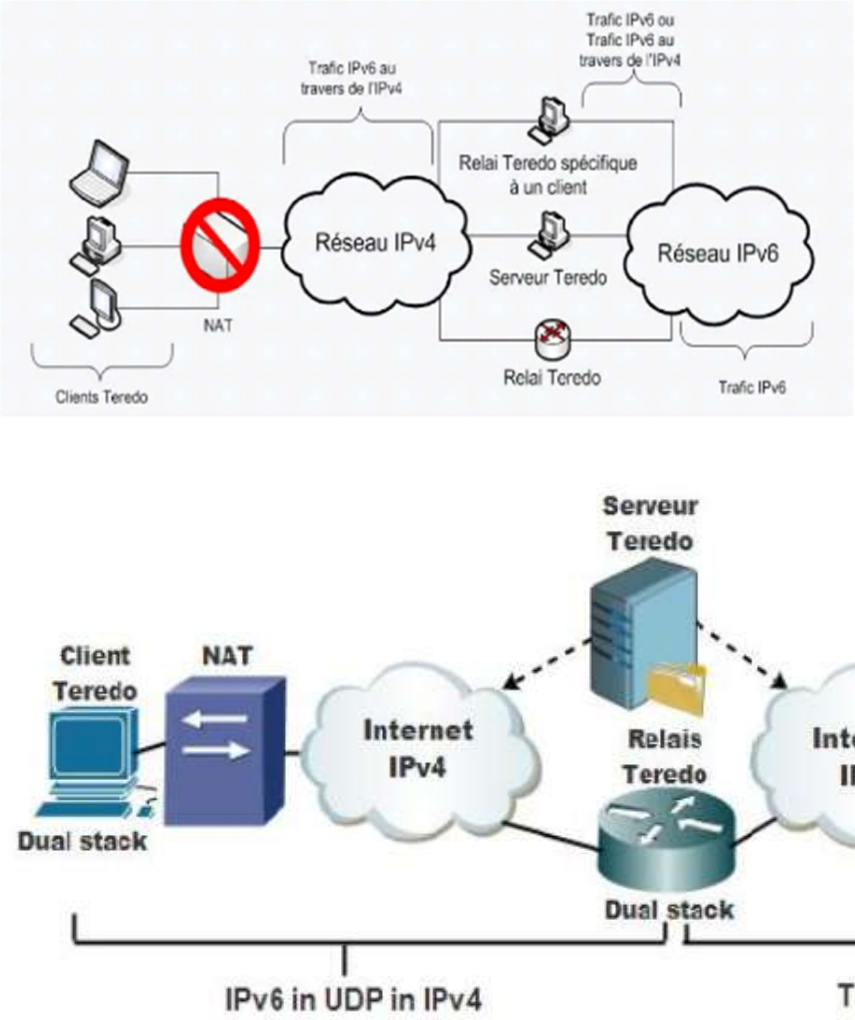


Figure 12: Teredo

Avantages	Inconvénients
• Permettre à des clients IPv4 (d'adresses IPv4 privées) résidant derrière un ou plusieurs NATs IPv4 d'obtenir une connectivité IPv6 • La capacité de traverser la plupart des NATs sur un ou plusieurs niveaux, en encapsulant les	• Ne résout pas le problème de la pénurie des adresses IP • Le client Teredo ne peut faire le travail du serveur Teredo, ils doivent être séparés (l'inverse de l'ISATAP) • Ne traverse pas les NATs symétriques

paquets IPv6 dans des paquets UDP puis dans IPv4	

IV. Technique de traduction

La traduction est utilisée pour l'interfonctionnement entre les réseaux IPv6 uniquement et les réseaux IPv4 uniquement. Les dispositifs de traduction sont situés à la frontière de deux réseaux. Ils doivent échanger de force les champs correspondants de l'en-tête IP et traduire l'adresse IP contenue dans le corps du paquet.

Tableau 2-2 Comparaison des techniques de traduction courantes

Couche	Technique	Faits saillants techniques	Scénarios d'utilisation
Couche réseau	SIIT (Traduction IP/ICMP sans état)	SIIT définit la traduction d'adresse mise en œuvre via les formats d'adresse spécifiques suivants : adresse de mappage IPv4 0 :: ffff : abcd et adresse de traduction IPv4 0 : : ffff : 0 : abcd	SIIT est une traduction sans état. Il fait face au problème de la pénurie d'adresses IPv4 et n'est donc applicable qu'à la communication d'un réseau IPv6 vers l'Internet IPv4.
	NAT-PT (traducteur de protocole de traduction d'adresses réseau)	NAT-PT est un type de NAT qui établit une correspondance entre les adresses/ports IPv4 et les adresses IPv6.	NAT-PT est une traduction avec état. Il est intégré dans un routeur ou un pare-feu. Il a une efficacité plus élevée que les techniques utilisées au niveau de la couche application.
	BIS (bosse dans la pile)	BIS est une sorte de NAT-PT implémenté dans les hôtes.	BIS est applicable aux hôtes à pile unique.
Couche transport	TRT (traducteur de relais de transport)	TRT fait référence à la traduction au niveau de la couche de transport.	TRT est applicable aux routeurs.
Couche d'application	CHAUSSETTES64	Le protocole SOCKS permet à un serveur proxy SOCKS d'implémenter la traduction d'adresse.	Le logiciel hôte doit être mis à niveau et un serveur SOCKS spécial doit être déployé. SOCKS est applicable à des scénarios d'application spécifiques.
	BIA (adresse MAC gravée)	BIA est un type de SOCKS64 implémenté dans les hôtes.	BIA est une technique de traduction d'hôte, applicable aux

Couche	Technique	Faits saillants techniques	Scénarios d'utilisation
			programmes d'application traditionnels des hôtes à double pile.
	ALG (passerelle de niveau application)	ALG indique la traduction d'adresse au niveau de la couche application.	ALG est utilisé avec NAT pour traduire les messages.

En raison des problèmes existant dans ces techniques de traduction, seul NAT-PT est actuellement déployé sur les produits. Les techniques de traduction au-dessus de la couche réseau sont peu performantes du fait de plusieurs couches à traiter. La traduction de la couche réseau est confrontée au problème de l'ALG. Les corps de paquet de certains protocoles contiennent des adresses IP. Pour mettre en œuvre l'ALG, les dispositifs de traduction doivent identifier le protocole de couche d'application spécifique.
L'IETF a remarqué les problèmes liés aux techniques de traduction et décrit les problèmes dans les normes pertinentes, y compris les problèmes de passerelle de couche d'application pour le serveur de noms de domaine (DNS-ALG), les problèmes de NAT, les problèmes d'ALG et les problèmes d'évolutivité. Sur cette base, le groupe de travail Behavior Engineering for Hindrance Avoidance (BEHAVE) de l'IETF a repensé les techniques de traduction et apporté les améliorations suivantes :

- La traduction avec état utilise NAT64+DNS64 pour simplifier et supplanter NAT-PT. NAT64 permet uniquement au côté IPv6 d'initier des connexions. De plus, les fonctions NAT-ALG sont implémentées par un DNS64 séparé.
- La traduction sans état intègre les notions de SIIT et IVI et utilise des préfixes de fournisseur. Les adresses IPv6 sont intégrées aux adresses IPv4 et peuvent être auto-mappées et sont donc faciles à gérer.
- Le mappage entre la traduction d'en-tête IPv4 et IPv6 et les formats de traduction d'adresse sont redéfinis.
- Le mode de comportement NAT qui est utile pour l'interfonctionnement des services pendant la traduction IPv4/IPv6 est spécifié.

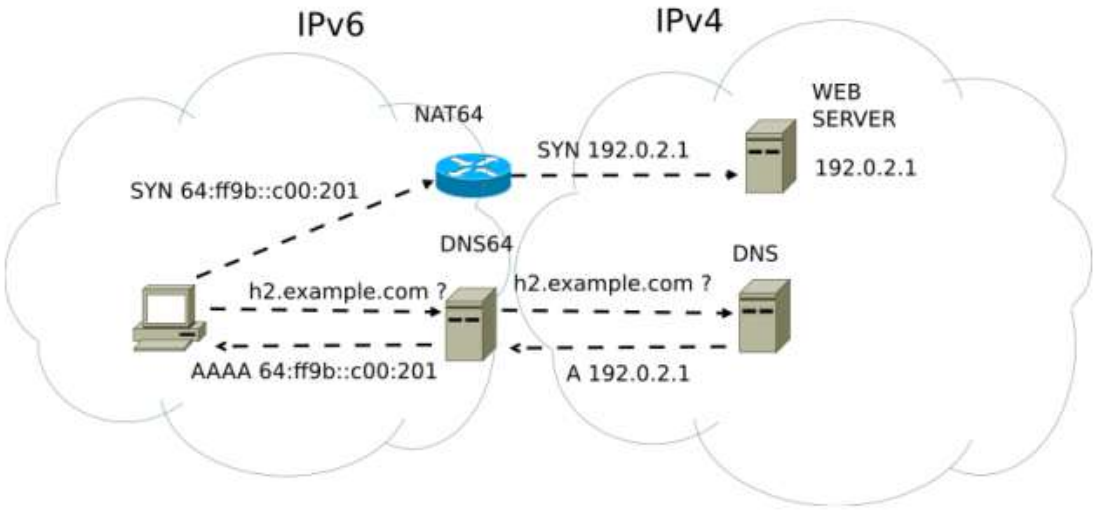


Figure 13: DNS64 and NAT64

Conclusion