

Présentation et configuration de NAT64

Contenu

[Introduction](#)

[Conditions préalables](#)

[Pourquoi NAT64 est-il nécessaire ?](#)

[Comment rendre possible la communication entre IPv4 et IPv6 ?](#)

[Types de traduction NAT64](#)

[Scénario 1 : Si nous voulons communiquer avec le serveur IPv4 \(situé dans le réseau IPv4\) à partir de l'hôte du réseau IPv6](#)

[Flux de paquets en cas de NAT64 avec état](#)

[Guide de configuration de NAT64](#)

[Configuration sur le routeur NAT 46](#)

[Vérifier les détails de NAT64](#)

[Scénario 2 : Trafic initié des clients IPv4 uniquement vers les serveurs IPv6 uniquement](#)

[Guide de configuration de NAT46](#)

[Configuration sur le routeur NAT 46](#)

[Vérification de NAT46](#)

[Scénarios de traduction et leur application](#)

[Commandes de dépannage importantes en cas de problème lors de l'implémentation NAT64](#)

Introduction

NAT64 est un mécanisme de transition IPv4-vers IPv6 et de coexistence IPv4-IPv6. Avec DNS64, le principal objectif de NAT64 est de permettre à un client IPv6 uniquement d'initier des communications vers un serveur IPv4 uniquement. NAT64 peut également être utilisé pour les clients IPv4 uniquement qui initient des communications avec des serveurs IPv6 uniquement à l'aide de liaisons statiques ou manuelles. J'ai expliqué les deux scénarios dans ce document.

Conditions préalables

Connaissances de base sur IPv6 et NAT

Pourquoi NAT64 est-il nécessaire ?

- Presque tous les périphériques IP modernes sont compatibles IPv6, mais de nombreux périphériques plus anciens sont uniquement compatibles IPv4. Nous avons besoin d'un moyen de connecter ces périphériques à travers un réseau IPv6.
- Certaines applications plus anciennes qui intègrent des adresses IPv4 dans les couches supérieures sont susceptibles d'exister pendant un certain temps et doivent être adaptées à IPv6.
- Lorsque les adresses IPv4 deviennent indisponibles, les adresses IPv6 sont attribuées à de nouveaux périphériques ; cependant, la majorité du contenu accessible sur Internet est

toujours IPv4. Ces nouveaux périphériques doivent atteindre ce contenu.

- Après quelques années, c'est le contraire qui s'appliquera : La majorité du contenu sera IPv6, mais les quelques périphériques IPv4 restants doivent encore l'atteindre.
- Les périphériques IPv4 uniquement doivent parler aux périphériques IPv6 uniquement avec une connaissance minimale ou inexistante de l'utilisateur.

Comment rendre possible la communication entre IPv4 et IPv6 ?

Comme IPv6 n'est pas rétrocompatible avec IPv4, il nous reste à mettre en place des mécanismes de transition, qui relèvent de l'une des trois classes suivantes :

- **Interfaces à deux piles** : La solution la plus simple à la coexistence IPv4 et IPv6 (et non à l'interopérabilité) est de rendre les interfaces " bilingues, " afin qu'elles parlent les périphériques IPv4 à IPv4 et les périphériques IPv6 à IPv6. La version qu'ils utilisent dépend soit de la version des paquets qu'ils reçoivent d'un périphérique, soit du type d'adresse que le DNS leur donne lorsqu'ils demandent une adresse de périphérique. La double pile était le moyen prévu de passer d'IPv4 à IPv6, mais l'hypothèse était que la transition serait terminée avant l'épuisement d'IPv4. Cela ne s'est pas produit, de sorte que la double empilage devient plus complexe : Comment donnez-vous à chaque interface une adresse IPv4 et une adresse IPv6 quand il n'y a pas assez d'adresses IPv4 disponibles ?
- **Tunnels** : Les tunnels sont aussi une question de coexistence, pas d'interopérabilité. Ils permettent aux périphériques ou aux sites d'une version de communiquer sur un segment de réseau, y compris Internet, de l'autre version. Ainsi, deux périphériques ou sites IPv4 peuvent échanger des paquets IPv4 sur un réseau IPv6, ou deux périphériques ou sites IPv6 peuvent échanger des paquets IPv6 sur un réseau IPv4.
- **Traducteurs** : Les traducteurs créent l'interopérabilité entre un périphérique IPv4 et un périphérique IPv6 en remplaçant l'en-tête d'un paquet d'une version par celui de l'autre version.

#Comme d'autres méthodes de transition, la traduction n'est pas une stratégie à long terme et l'objectif final devrait être IPv6 natif. Cependant, la traduction offre deux avantages majeurs par rapport à la transmission tunnel :

- La traduction permet une migration progressive et transparente vers IPv6.
- Les fournisseurs de contenu peuvent fournir des services de manière transparente aux utilisateurs Internet IPv6.

Types de traduction NAT64

NAT64 sans état

Dans NAT64 sans état, l'état n'est pas préservé, ce qui signifie que pour chaque utilisateur IPv6, une adresse IPv4 dédiée est requise. Comme nous sommes en phase d'épuisement IPv4, il est très difficile d'adopter ce mode de NAT64. Le seul avantage de l'utilisation de NAT64 sans état lorsque vous avez peu d'adresses IPv6 (NAT46).

NAT64 avec état

Dans NAT64 avec état, les états sont maintenus. Une adresse IP unique est utilisée pour tous les utilisateurs privés avec des numéros de port différents. Dans le schéma ci-dessus, une seule adresse IPv4 est utilisée avec des numéros de port différents pour tous les utilisateurs d'IPv6 qui se trouvent dans ce réseau local pour accéder à un serveur IPv4 public.

Voici plus de détails sur la différence entre la traduction NAT64 avec état et la traduction NAT64 sans état :

NAT64 sans état

Traduction 1:1

Aucune conservation de l'adresse IPv4

Garantit la transparence et l'évolutivité des adresses de bout en bout

Aucun état ni aucune liaison créés sur la traduction

Nécessite l'attribution d'adresses IPv6 traduisibles en IPv4 (obligatoire)

Nécessite l'attribution manuelle ou DHCPv6 d'adresses pour les hôtes IPv6

NAT64 avec état

Traduction 1:N

Conserve l'adresse IPv4

Utilise la surcharge d'adresses, ce qui fait qu'elle manque de transparence d'adresse de bout en

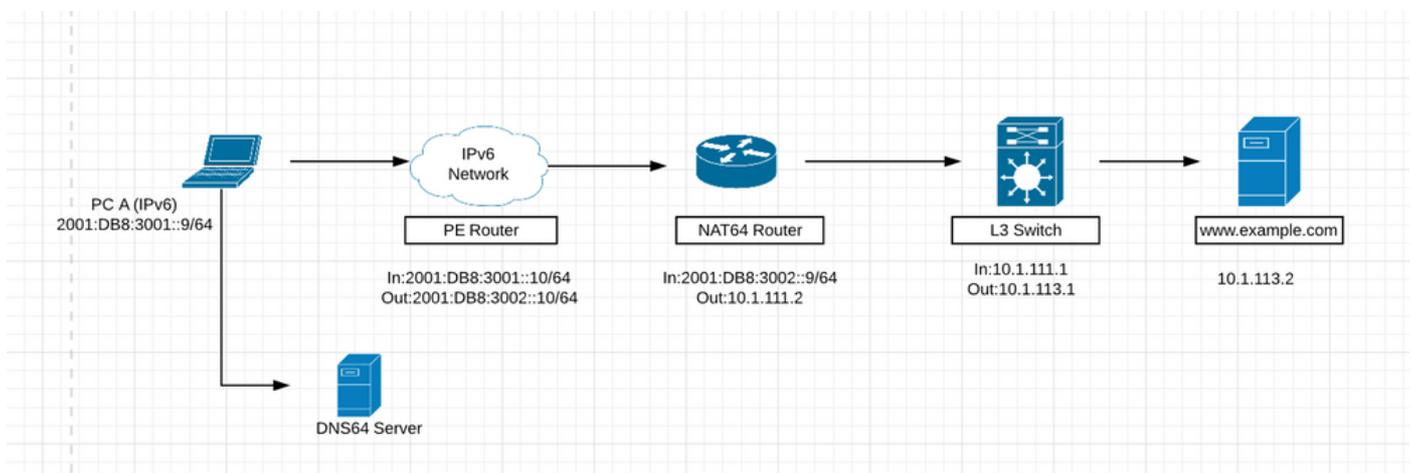
L'état ou les liaisons sont créés sur chaque traduction unique

Aucune exigence sur la nature de l'attribution d'adresses IPv6

Libre de choisir n'importe quel mode d'attribution d'adresse IPv6 (manuel, DHCPv6, SLAAC)

- Dans ce document, j'ai démontré NAT64 avec état avec l'exercice LAB où l'hôte IPv6 veut communiquer avec le serveur IPv4. En outre, j'ai démontré NAT64 sans état où les hôtes IPv6 veulent atteindre le serveur IPv6, ce scénario est également appelé NAT46.

Scénario 1 : Si nous voulons communiquer avec le serveur IPv4 (situé dans le réseau IPv4) à partir de l'hôte du réseau IPv6



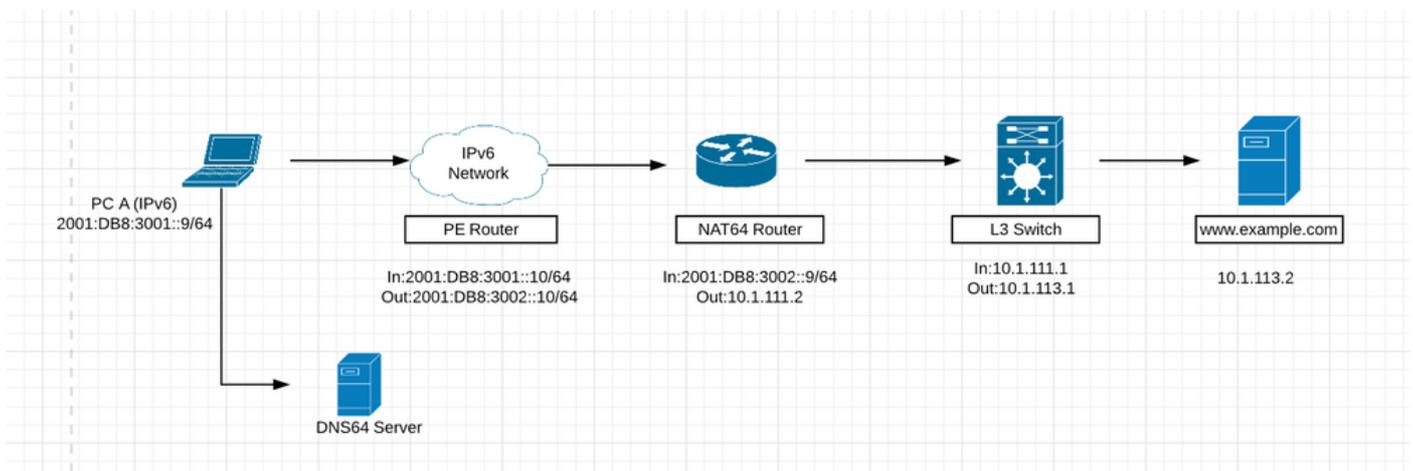
- Dans l'image ci-dessus, l'hôte situé dans le réseau IPv6 veut atteindre le serveur Web (www.example.com) avec l'adresse IP 10.1.113.2 située dans le réseau ipv4.
- Si nous envoyons directement une requête ping à l'adresse ipv4 (10.1.113.2) à partir de l'hôte sur le réseau ipv6, le périphérique ne comprend pas cette adresse ipv4 car il comprend uniquement les adresses ipv6. Ainsi, le paquet sera abandonné sur l'hôte.
- De même, si nous envoyons une requête ping à l'adresse ipv6 à partir du réseau ipv4, le périphérique ne comprendra pas cette adresse ip et lancera une erreur car elle est par défaut configurée pour le réseau ipv4 uniquement.
- En outre, un paquet ipv4 ne peut pas être routé via un réseau ipv6 uniquement et

inversement. Il est donc nécessaire de traduire les paquets sur les périphériques en ipv4 ou ipv6 en fonction des besoins.

NAT64 comporte trois composants principaux

- **Préfixe NAT64** : Tout préfixe /32, /40, /48, /56, /64 ou /96 utilisé avec une adresse IPv4 convertie pour transmettre le paquet sur le réseau IPv6 uniquement. Le préfixe NAT64 peut être un préfixe spécifique au réseau (NSP) ou un préfixe bien connu (WKP). Un NSP est attribué par une organisation et est généralement un sous-réseau du préfixe IPv6 de l'organisation. Le WKP pour NAT64 est 64:ff9b::/96. Si aucun NSP n'est spécifié ou configuré, NAT64 utilise le WKP pour préempter l'adresse IPv4 convertie. Le préfixe NAT64 est également appelé Pref64::/n.
- **Serveur DNS64** : Le serveur DNS64 fonctionne comme un serveur DNS normal pour les enregistrements AAAA IPv6, mais tente également de localiser un enregistrement IPv4 A lorsqu'un enregistrement AAAA n'est pas disponible. Si un enregistrement A est localisé, DNS64 convertit l'enregistrement IPv4 A en enregistrement AAAA IPv6 à l'aide du préfixe NAT64. Cela donne l'impression à l'hôte IPv6 uniquement qu'il peut communiquer avec un serveur à l'aide d'IPv6.
- **Routeur NAT64** : Le routeur NAT64 annonce le préfixe NAT64 dans le réseau IPv6 uniquement et effectue la traduction entre les réseaux IPv6 uniquement et IPv4 uniquement.

Flux de paquets en cas de NAT64 avec état



1. Supposons que dans l'image ci-dessus, l'hôte présent dans le réseau IPv6 souhaite communiquer avec le serveur Web www.example.com (10.1.113.2) qui est un serveur IPv4 uniquement.
2. Pour rendre cette communication possible, nous devons installer un serveur DNS64 sur notre réseau IPv6 qui puisse comprendre et résoudre les requêtes DNS pour ipv4.
3. Le serveur DNS64 fonctionne comme un serveur DNS normal pour les enregistrements AAAA IPv6, mais tente également de localiser un enregistrement IPv4 A lorsqu'un enregistrement AAAA n'est pas disponible. Si un enregistrement A est localisé, DNS64 convertit l'enregistrement IPv4 A en enregistrement AAAA IPv6 à l'aide du préfixe NAT64. Cela donne l'impression à l'hôte IPv6 uniquement qu'il peut communiquer avec un serveur à l'aide d'IPv6.
4. Maintenant, la demande de résolution DNS pour www.example.com est envoyée au serveur

DNS64. Il recherche d'abord dans sa table d'enregistrements AAAA IPv6, mais il ne trouve aucun enregistrement AAAA IPv6 car ce serveur de site Web appartient à l'adresse IPv4. Après cela, il recherche dans sa base de données IPv4 et trouve l'adresse IPv4 correspondant à ce site Web. Maintenant, le serveur DNS64 convertira cette adresse IPv4 en adresse IPv6 en convertissant cette adresse IPv4 en adresse hexadécimale et en préservant le préfixe NAT64. Ce faisant, cela donnera l'impression à l'hôte IPv6 uniquement qu'il peut communiquer avec le serveur Web à l'aide d'IPv6.

5. Les paquets sont acheminés dans le réseau IPv6 uniquement vers le périphérique faisant NAT64 à l'aide du préfixe NAT64 qui était préfixé à la valeur hexadécimale de l'adresse IPv4.

6. Le routeur NAT64 annonce le préfixe NAT64 dans le réseau IPv6 uniquement et effectue la traduction entre les réseaux IPv6 uniquement et IPv4 uniquement.

7. Une fois que le paquet atteint le périphérique effectuant la traduction NAT64, les paquets sont mis en correspondance avec la liste de contrôle d'accès que nous avons configurée pour Nat64. Si les paquets correspondent à cette liste de contrôle d'accès, le paquet sera traduit à l'aide de la NAT64, si le paquet ne correspond pas à la liste de contrôle d'accès configurée, il sera routé à l'aide du routage IPv6 normal vers sa destination.

8. La NAT64 avec état utilise des listes de contrôle d'accès configurées et des listes de préfixes pour filtrer les flux de trafic initiés par IPv6 qui sont autorisés à créer l'état NAT64. Le filtrage des paquets IPv6 s'effectue dans la direction IPv6-IPv4, car l'allocation dynamique du mappage entre un hôte IPv6 et une adresse IPv4 ne peut être effectuée que dans cette direction. NAT64 avec état prend en charge le filtrage dépendant des points d'extrémité pour le flux de paquets IPv4 vers IPv6 avec configuration PAT.

9. Dans une configuration PAT NAT64 avec état, le flux de paquets doit provenir du domaine IPv6 et avoir créé les informations d'état dans les tables d'état NAT64. Les paquets du côté IPv4 qui n'ont pas d'état précédemment créé sont supprimés. Le filtrage indépendant des points de terminaison est pris en charge par les configurations NAT (Network Address Translation) et non PAT statiques.

Le premier paquet IPv6 est acheminé vers l'interface virtuelle NAT (NVI) en fonction de la configuration de routage automatique configurée pour le préfixe avec état. La fonction NAT64 avec état effectue une série de recherches pour déterminer si le paquet IPv6 correspond à l'un des mappages configurés en fonction d'une liste de contrôle d'accès (ACL). En fonction du mappage, une adresse IPv4 (et un port) est associée à l'adresse de destination IPv6.

Le paquet IPv6 est traduit et le paquet IPv4 est formé en utilisant les méthodes suivantes :

1. Extraction de l'adresse IPv4 de destination en supprimant le préfixe de l'adresse IPv6. L'adresse source est remplacée par l'adresse IPv4 allouée (et le port).
2. Les autres champs sont traduits d'IPv6 à IPv4 pour former un paquet IPv4 valide.

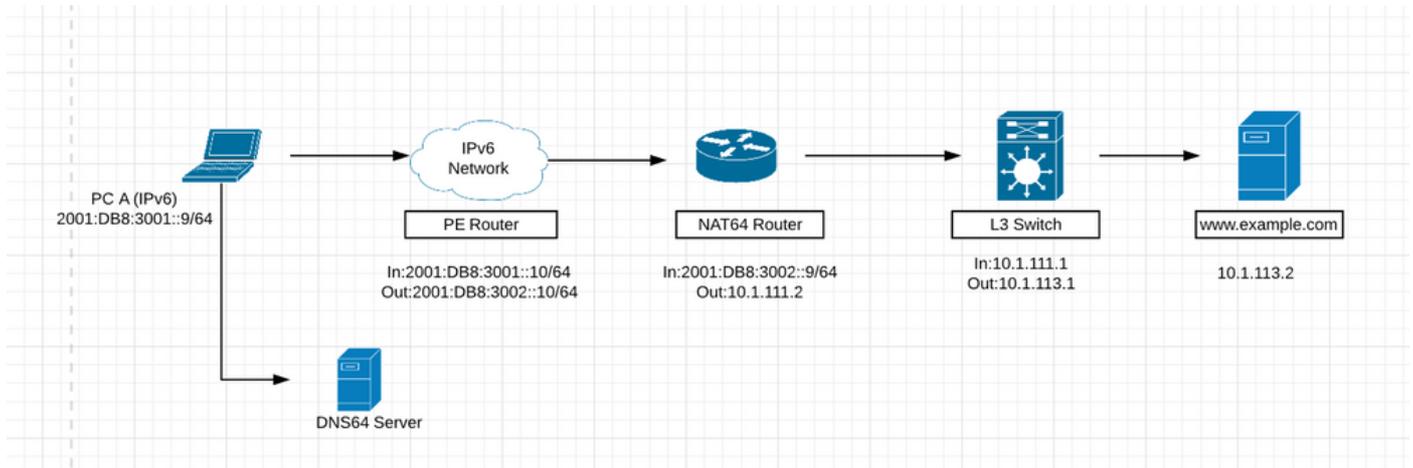
10. Une nouvelle traduction NAT64 est créée dans la base de données de session et dans la base de données de liaison. Les bases de données de pool et de ports sont mises à jour en fonction de la configuration.

11. Le trafic de retour et le trafic ultérieur du flux de paquets IPv6 utiliseront cette entrée de base de données de session pour la traduction.

- Pour que NAT64 fonctionne, il doit y avoir une accessibilité à l'adresse ipv6 de l'interface qui

se trouve dans le réseau ipv6 à partir de l'ipv6 et l'accessibilité doit également être du routeur NAT64 à l'adresse ipv4 du serveur.

Guide de configuration de NAT64



Étape 1. L'hôte A est un hôte IPv6 uniquement qui souhaite communiquer avec le serveur www.example.com. Cela déclenche une requête DNS (AAAA : www.example.com) vers le serveur DNS64. Le DNS64 est un composant clé de ce processus. Un serveur DNS64 est à la fois un serveur DNS pour IPv6 et IPv4. Cela crée l'illusion pour le client que les serveurs IPv4 peuvent être atteints à l'aide d'une adresse IPv6.

L'hôte A envoie une requête DNS (AAAA : www.example.com) vers le serveur DNS64. En ce qui concerne l'hôte A, il s'agit d'une requête AAAA DNS normale pour un serveur IPv6.

Étape 2. Le serveur DNS64 reçoit la requête DNS AAAA de l'hôte A. Dans une tentative de résolution du nom de domaine, le serveur DNS64 envoie une requête au serveur DNS AAAA faisant autorité pour www.example.com.

Étape 3. Le serveur faisant autorité AAAA DNS IPv6 retourne une réponse indiquant qu'il n'a pas d'enregistrement de ressource AAAA pour www.example.com.

Étape 4. À la réception d'une réponse vide (erreur de nom) à la requête AAAA, cela déclenche le serveur DNS64 à envoyer une requête A (A : www.example.com) vers le serveur DNS A IPv4 faisant autorité.

Étape 5. Le serveur DNS IPv4 A faisant autorité possède un enregistrement de ressource A pour www.example.com et renvoie une réponse avec l'adresse IPv4 du serveur (A : www.example.com (10.1.113.2)).

Étape 6. Le serveur DNS64 reçoit l'adresse IPv4 du serveur DNS A faisant autorité et synthétise un enregistrement AAAA en préfixant l'adresse avec son préfixe NAT64, 2800:1503:2000:1:1::/96, et convertit l'adresse IPv4 en hexadécimal 0a 01:7102. Cette adresse sera utilisée par l'hôte A comme adresse IPv6 de destination pour atteindre le serveur www.example.com.

Étape 8. L'enregistrement AAAA synthétisé est totalement transparent pour l'hôte A. Pour l'hôte A, il semble que www.example.com soit accessible via le réseau IPv6 et Internet. L'hôte A dispose désormais des informations d'adressage nécessaires pour transmettre des paquets IPv6 à www.example.com avec les éléments suivants :

- Adresse de destination IPv6 : 2800:1503:2000:1:1::0a01:7102
- Adresse source IPv6 : 2001:DB8:3001::9

Étape 9. Le routeur NAT64 reçoit le paquet IPv6 envoyé par l'hôte A sur son interface NAT64 activée. Il fait correspondre les paquets entrants à la liste de contrôle d'accès configurée. Si aucune correspondance n'est trouvée, le paquet est transféré sans traduction à l'aide du routage IPv6 normal. Si une correspondance est trouvée, le paquet subit la traduction suivante :

- L'en-tête IPv6 est traduit en en-tête IPv4.
- L'adresse de destination IPv6 est traduite en adresse IPv4 en supprimant le préfixe NAT64 avec état IPv6 2800:1503:2000:1:1::/96 . Les 32 bits inférieurs de l'adresse IPv6, 0a01:7102, sont représentés comme l'adresse IPv4 décimale à point 10.1.113.2.
- L'adresse source IPv6 est traduite en adresse IPv4 à l'aide du pool d'adresses IPv4 configuré. Selon la configuration NAT64, il peut s'agir d'une traduction d'adresses 1:1 ou d'une surcharge d'adresses IPv4. Ceci est similaire à NAT pour IPv4. Dans ce scénario, l'adresse IPv6 source de l'hôte A est traduite en adresse IPv4 50.50.50.50.
- Les états de traduction d'adresses IP NAT64 avec état sont créés pour les adresses source et de destination. Ces états sont créés la première fois que la traduction est effectuée sur le paquet. Cet état est maintenu pour les paquets suivants dans le flux. L'état se termine lorsque le trafic et le minuteur de maintenance d'état expirent.

```
HUB-BR-1#sh nat64 translations
Proto  Original IPv4      Translated IPv4
      Translated IPv6  Original IPv6
-----
icmp   10.1.113.2:2654   [2800:1503:2000:1:1:0:a01:7102]:2654
      50.50.50.50:2654 [2001:db8:3001::9]:2654
Total number of translations: 1
```

Étape 10. Après la traduction NAT64, le paquet IPv4 traduit est transféré à l'aide du processus normal de recherche de route IPv4. Dans ce scénario, l'adresse de destination IPv4 10.1.113.2 est utilisée pour transférer le paquet.

Étape 11. Le serveur www.example.com sur 10.1.113.2 répond, qui est finalement reçu par le routeur NAT64.

Étape 12. Le routeur NAT64 reçoit le paquet IPv4 du serveur www.example.com sur l'une de ses interfaces NAT64. Le routeur examine le paquet IPv4 pour déterminer s'il existe un état de traduction NAT64 pour l'adresse de destination IPv4. Si aucun état de traduction n'existe, le paquet est rejeté. Si un état de traduction existe pour l'adresse de destination IPv4, le routeur NAT64 effectue les tâches suivantes :

- L'en-tête IPv4 est traduit en un en-tête IPv6.
- L'adresse source IPv4 est traduite en adresse source IPv6 à l'aide de l'état de traduction NAT64 existant. Dans ce scénario, l'adresse source est traduite d'une adresse IPv4 10.1.113.2 à l'adresse IPv6 2800:1503:2000:1:1::0a01:7102. L'adresse de destination est traduite d'une adresse IPv4 50.50.50 à 2001:DB8:3001::9.

Étape 13. Après la traduction, le paquet IPv6 est transféré à l'aide du processus normal de recherche de route IPv6.

Configuration sur le routeur NAT 46

1.Interface orientée IPv6 :

```
HUB-BR-1#sh run int gig0/0/1
Building configuration...

Current configuration : 131 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 nat64 enable
 cdp enable
 ipv6 address 2001:DB8:3002::9/64
end
```

2.Interface orientée IPv4 :

```
HUB-BR-1#sh run int gig0/0/0
Building configuration...

Current configuration : 119 bytes
!
interface GigabitEthernet0/0/0
 ip address 10.1.111.2 255.255.255.0
 negotiation auto
 nat64 enable
 cdp enable
end
```

3.Créer une liste de contrôle d'accès correspondant au trafic ipv6

```
HUB-BR-1#sh ipv6 access-list nat64acl
IPv6 access list nat64acl
 permit ipv6 2001:DB8:3001::/64 any sequence 10
HUB-BR-1#
```

4.activez le mappage d'adresses IPv6-à-IPv4 NAT64 :

#nat64 prefix stateful 2800:1503:2000:1:1::/96 —> L'adresse IP du serveur sera mappée à cette adresse IP ipv6. Vous pouvez configurer n'importe quelle adresse réseau ipv6 ici, mais cette adresse réseau ipv6 doit être accessible à partir de votre réseau ipv6. En outre, le serveur DNS64

doit avoir mappé cette adresse réseau ipv6 à l'adresse ipv4 du serveur.

5. #nat64 v4 pool1 50.50.50 50.50.50.50.50 —> L'adresse source ipv6 d'origine sera traduite en ips de ce pool alors que le paquet entrera dans le réseau ipv4.

6. #nat64 v6v4 list nat64acl pool1 overload —>Ceci va traduire les adresses ipv6 correspondant à nat64acl en adresse ipv4 à partir du pool

7. La valeur hexadécimale 10.1.113.2 est 0a01:7102. Une fois cette configuration effectuée, envoyez une requête ping à l'adresse 2800:1503:2000:1:1::0a01:7102 à partir du PC A.

```
#ping 2800:1503:2000:1:1::0a01:7102
```

Vérifier les détails de NAT64

```
#show nat64 translation
```

```
HUB-BR-1#sh nat64 translations
Proto  Original IPv4      Translated IPv4
       Translated IPv6  Original IPv6
-----
icmp   10.1.113.2:7749   [2800:1503:2000:1:1:0:a01:7102]:7749
       50.50.50.50:7749 [2001:db8:3001::9]:7749
Total number of translations: 1
```

```
#show nat64 statistics
```

```

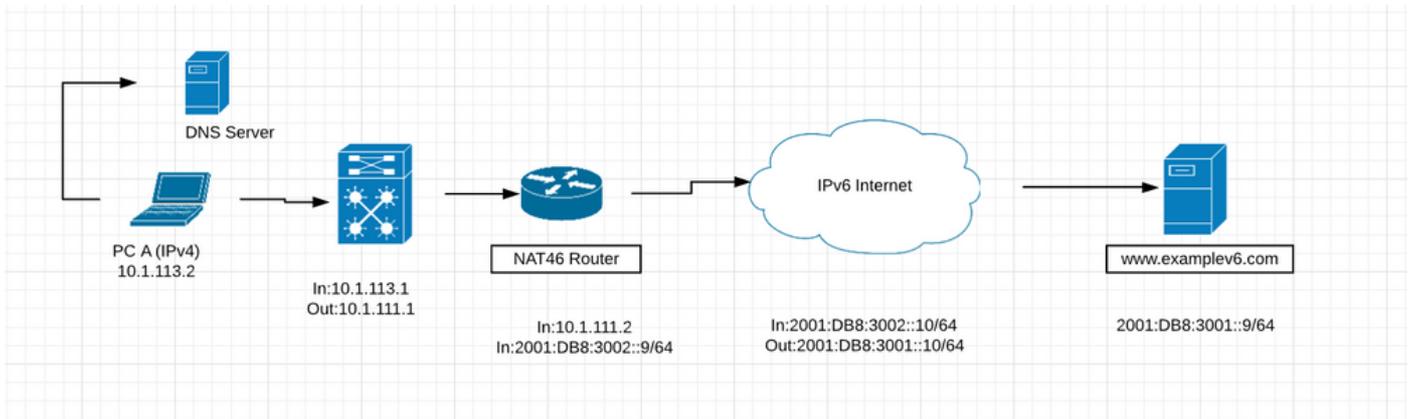
HUB-BR-1#sh nat64 statistics
NAT64 Statistics

Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Sessions found: 33
Sessions created: 4
Expired translations: 4
Global Stats:
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 18
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 20
    MAP-T: 0

Interface Statistics
GigabitEthernet0/0/0 (IPv4 configured, IPv6 not configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 15
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 0
    MAP-T: 0
  Packets dropped: 5
GigabitEthernet0/0/1 (IPv4 not configured, IPv6 configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 0
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 20
    MAP-T: 0
  Packets dropped: 0
Dynamic Mapping Statistics
v6v4
  access-list nat64acl pool pool1 refcount 1
  pool pool1:
    start 50.50.50.50 end 50.50.50.50
    total addresses 1, allocated 1 (100%)
    address exhaustion packet count 0
Limit Statistics

```

Scénario 2 : Trafic initié des clients IPv4 uniquement vers les serveurs IPv6 uniquement



- La figure ci-dessus montre un scénario où les clients d'un réseau IPv4 uniquement communiquent avec un serveur IPv6 uniquement à l'aide de NAT64. L'objectif est de fournir un accès transparent aux services IPv6 aux clients IPv4. Dans ce scénario, le serveur DNS64 n'est pas requis. Le mappage statique entre les adresses IPv6 et IPv4 est configuré sur le routeur NAT64.
- Veuillez noter que ce scénario est peu probable dans un avenir prévisible. La plupart des serveurs qui sont activés pour IPv6 seront également compatibles avec IPv4. Il est plus probable que les serveurs IPv6 exécutent une double pile pendant un certain temps. Les serveurs uniquement IPv6 deviendront plus courants, mais pas de sitôt.

Guide de configuration de NAT46

Étape 1. La première étape consiste à configurer le mappage statique IPv6 vers IPv4 sur le routeur NAT46 pour fournir l'accès au serveur IPv6 2001:DB8:3001::9/64 à partir de l'adresse IPv4 10.1.113.2. En outre, l'adresse IPv4 50.50.50.50 doit être enregistrée en tant qu'enregistrement de ressource DNS pour www.examplev6.com sur le serveur DNS. Le mappage NAT64 statique est créé à l'aide de cette commande :

```
NAT64-Router(config)# nat64 v6v4 static 2001:DB8:3001::9 50.50.50.50
```

Étape 2. PC A est un hôte IPv4 uniquement qui souhaite communiquer avec le serveur www.examplev6.com. Cela déclenche une requête DNS (A : www.examplev6.com) à son serveur DNS faisant autorité IPv4.

Étape 3. Le serveur DNS répond avec un enregistrement de ressource A pour www.examplev6.com, 50.50.50.50.

Étape 4. L'hôte A dispose désormais des informations d'adressage nécessaires pour transmettre des paquets IPv4 à www.examplev6.com avec

- Adresse de destination IPv4 : 50.50.50.50
- Adresse source IPv4 : 10.1.113.2

Étape 5. Le routeur NAT64 reçoit le paquet IPv4 sur son interface NAT64 activée et effectue les tâches suivantes :

- L'en-tête IPv4 est traduit en un en-tête IPv6.
- L'adresse de destination IPv4 est traduite en adresse IPv6 à l'aide de l'état de traduction NAT64 existant créé par la configuration statique à l'étape 1. L'adresse IPv4 de destination

50.50.50.50 est traduite en adresse de destination IPv6 2001:DB8:3001::9.

- L'adresse source IPv4 est traduite en adresse IPv6 en ajoutant le préfixe NAT64 avec état 2800:1503:2000:1:1::/96 à l'adresse IPv4. Cela donne une adresse source IPv6 de 2800:1503:2000:1:1::0a01:7102. (0a01:7102 est l'équivalent hexadécimal de 10.1.113.2.)

Étape 6. Après la traduction, le paquet IPv6 est routé à l'aide du processus de routage IPv6 normal. Le paquet est finalement acheminé vers le serveur www.examplev6.com à l'adresse 2001:DB8:3001::9 .

Étape 7. Le serveur www.examplev6.com répond avec un paquet destiné à l'hôte A.

Étape 8. Le routeur NAT64 reçoit le paquet IPv6 envoyé par le serveur IPv6 sur son interface NAT64 activée et effectue les tâches suivantes :

- L'en-tête IPv6 est traduit en en-tête IPv4.
- L'adresse source IPv6 est traduite en 50.50.50.50 à l'aide de la table de traduction dynamique.
- L'adresse de destination IPv6 est traduite en adresse IPv4 en supprimant le préfixe NAT64 avec état IPv6 2800:1503:2000:1:1::/96. Les 32 bits inférieurs de l'adresse IPv6, 0a01:7102, sont représentés comme l'adresse IPv4 décimale à point 10.1.113.2.

Étape 9. Après la traduction, le routeur NAT64 transfère le paquet à 10.1.113.2 en utilisant le processus de routage IPv4 normal.

- Comme dans le scénario précédent, une communication transparente est établie entre le client IPv4 uniquement et le serveur IPv6 uniquement à l'aide de la NAT64 avec état. Les configurations sont similaires, à l'exception de la commande de mappage statique décrite à l'étape 1.

Configuration sur le routeur NAT 46

1. Interface orientée IPv4 :

```
HUB-BR-1#sh run int gig0/0/0
Building configuration...

Current configuration : 137 bytes
!
interface GigabitEthernet0/0/0
 ip address 10.1.111.2 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 nat64 enable
 cdp enable
end
```

2. Interface orientée IPv6 :

```

HUB-BR-1#sh run int gig0/0/1
Building configuration...

Current configuration : 131 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 nat64 enable
 cdp enable
 ipv6 address 2001:DB8:3002::9/64
end

```

3. D'autres configurations sont nécessaires sur le routeur pour traduire correctement le trafic IPv4 vers IPv6 :

```

nat64 prefix stateful 2800:1503:2000:1:1::/96
nat64 v6v4 static 2001:DB8:3001::9 50.50.50.50

```

Une fois la configuration terminée, envoyez une requête ping à 50.50.50.50 à partir de l'hôte IPv4.

```
#ping 50.50.50.50
```

Vérification de NAT46

```
#show nat64 translations
```

```

HUB-BR-1#sh nat64 translations

Proto  Original IPv4      Translated IPv4
       Translated IPv6  Original IPv6
-----
illegal ---
       50.50.50.50    2001:db8:3001::9
icmp   10.1.113.2:11     [2800:1503:2000:1:1:0:a01:7102]:11
       50.50.50.50:11  [2001:db8:3001::9]:11

Total number of translations: 2

```

```
#show nat46 statistics
```

```

HUB-BR-1#sh nat64 statistics
NAT64 Statistics

Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Sessions found: 9967
Sessions created: 14
Expired translations: 14
Global Stats:
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 4990
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 4992
    MAP-T: 0

Interface Statistics
  GigabitEthernet0/0/0 (IPv4 configured, IPv6 not configured):
    Packets translated (IPv4 -> IPv6)
      Stateless: 0
      Stateful: 1947
      MAP-T: 0
    Packets translated (IPv6 -> IPv4)
      Stateless: 0
      Stateful: 0
      MAP-T: 0
    Packets dropped: 58
  GigabitEthernet0/0/1 (IPv4 not configured, IPv6 configured):
    Packets translated (IPv4 -> IPv6)
      Stateless: 0
      Stateful: 0
      MAP-T: 0
    Packets translated (IPv6 -> IPv4)
      Stateless: 0
      Stateful: 1947
      MAP-T: 0
    Packets dropped: 0
Dynamic Mapping Statistics
  v6v4
Limit Statistics

```

Scénarios de traduction et leur application

| Scénarios de traduction | Applicabilité | Exemple |
|---|--|---|
| IPv6/IPv4 | | |
| Scénario 1 : Un réseau IPv6 vers Internet IPv4 | ·réseau IPv6 uniquement souhaitant accéder de manière transparente au contenu IPv6 et IPv4 existant ·initié à partir d'hôtes IPv6 et du réseau | ·FAI déploie de nouveaux services et réseaux pour les smartphones IPv6 uniquement (combinaison de 3G [3G], LTE [Long-Term Evolution], etc.) ·entreprises déployant un réseau IPv6 uniquement |
| Scénario 2 : Internet IPv4 vers un réseau IPv6 | ·serveurs d'un réseau IPv6 uniquement souhaitant desservir de manière transparente les utilisateurs IPv4 et IPv6 ·initié à partir d'hôtes IPv4 et du réseau | Fournisseurs de contenu existants ou à venir déployant des services dans un environnement IPv6 uniquement |
| Scénario 3 : Internet IPv6 vers un réseau IPv4 | · Serveurs uniquement existant souhaitant servir les utilisateurs Internet IPv6 ·initié à partir d'hôtes IPv6 et du réseau | Fournisseurs de contenu existants qui migrent vers IPv6 et qui souhaitent donc offrir des services aux utilisateurs Internet IPv6 dans le cadre de la stratégie de coexistence |
| Scénario 4 : Un réseau | · n'est pas viable dans un avenir proche ; ce scénario ne se produira probablement | Aucune |

| | | |
|------------------------------------|--|--|
| IPv4 vers Internet IPv6 | qu'un certain temps après le début de la transition IPv6/IPv4 | |
| Scénario 5 : | | |
| Un réseau IPv6 vers un réseau IPv4 | Un réseau IPv4 et un réseau IPv6 font partie de la même organisation | Semblable au scénario 1, qui traite de l'intranet plutôt que de l'Internet |
| Scénario 6 : | | |
| Un réseau IPv4 vers un réseau IPv6 | Même chose que ci-dessus | Semblable au scénario 2, la prise en charge de l'intranet plutôt que de l'Internet |
| Scénario 7 : | | |
| Internet IPv6 vers Internet IPv4 | pâтираient d'un débit médiocre | Aucune |
| Scénario 8 : | | |
| Internet IPv4 vers Internet IPv6 | Aucune technique de traduction viable pour gérer la traduction d'adresses IPv6 illimitée | Aucune |

Commandes de dépannage importantes en cas de problème lors de l'implémentation NAT64

```
#show platform hardware qfp active statistics drop ( pour voir s'il y a des pertes nat64)
```

```
#show running-config | include nat64 ( pour voir si tout est configuré sur IOS)
```

```
#show platform hardware qfp active feature nat64 datapath statistics (pour vérifier la raison du compteur de pertes)
```

```
#show platform hardware qfp active feature nat64 datapath pool (pour vérifier que le pool est configuré correctement)
```

```
#show platform hardware qfp active feature nat64 datapath map (vérifier et voir la configuration du pool à mapper est fait correctement)
```

```
#show platform software object-manager F0 en attente-ack-update (pour vérifier s'il y a des objets en attente)
```