Centre
Interuniversitaire de
Ressources
Informatiques de
Lorraine

IPv6-ADIRE

Expérimentation de la mise en œuvre de NAT-PT (Cisco)

- Octobre 2005 -

Table des matières

Introduction **3**

1 – Principe **3**
1.1 - Translation statique 3
1.2 - Translation dynamique 4
2 – Mise en oeuvre de l'implémentation CISCO **5**
2.1 – Disponibilité dans l'IOS 5
2.2 – Configuration 5
3 – Résultats **6**

Conclusion **7**

Références **8**

Annexe A : Capture ping6 ..... **9**
Annexe B : Capture HTTP **12**

Introduction

NAT-PT signifie **N**etwork **A**ddress **T**ranslation and **P**rotocol **T**ranslation. Ce mécanisme réalise donc à la fois une translation d'adresse et de protocole pour permettre à un équipement uniquement IPv6 de communiquer avec des équipements IPv4 (et inversement). Il existe également d'autres solutions comme les relais traducteurs de transport ou encore les proxy applicatifs qui permettent de réaliser une translation d'IPv6 vers IPv4. Ce document qui s'inscrit dans le cadre du projet **IPv6-ADIRE**[1] va donc présenter le principe de fonctionnement de NAT-PT puis les résultats obtenus lors des différents tests réalisés avec l'implémentation CISCO.

1 – Principe

NAT-PT repose sur le maintient d'une table de correspondance au niveau du routeur entre adresses IPv6 et adresses IPv4. Il existe deux techniques de translations d'adresses différentes pour construire cette table :

1. la translation statique
2. la translation dynamique

1.1 - Translation statique

La translation statique consiste à ce que l'administrateur réalise en personne l'ajout des entrés dans la table de correspondance. L'exemple suivant illustre une utilisation de ce type de translation :

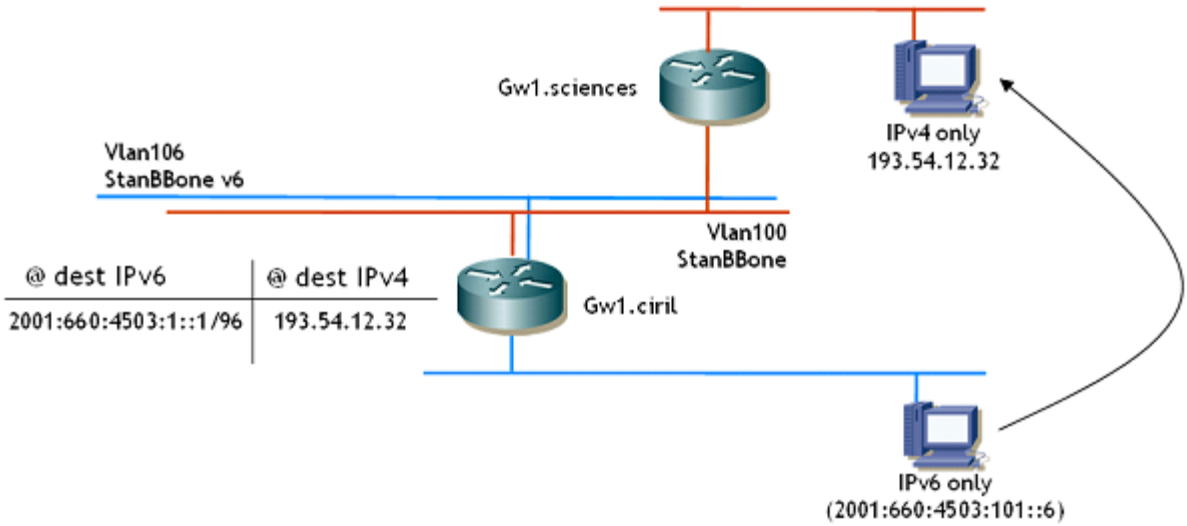


Figure 1 : Schéma de présentation de NAT-PT

Dans ce cas précis, imaginons que le poste IPv6 connecté à Gw1.ciril veuillent communiquer avec le poste IPv4 connecté à Gw1.sciences. Il est alors nécessaire de définir au niveau du routeur une correspondance entre l'adresse IPv4 193.54.12.32 et une adresse IPv6 définie dans une plage d'adresses spécifiquement réservée au mécanisme de NAT-PT. Cette plage d'adresses appelée préfixe NAT devra avoir une longueur de 96 bits afin de pouvoir faire correspondre l'ensemble des adresses

[1] **IPv6-ADIRE** : Projet lancé par le ministère de l'Education Nationale, de la Recherche et de l'Enseignement Supérieur visant à déployer IPv6 sur des réseaux de production.

IPv4 existantes. Ainsi lorsque le routeur recevra un paquet dont l'adresse destination sera comprise dans ce préfixe alors il appliquera le mécanisme de NAT-PT. Dans notre exemple il translatera donc l'adresse destination 2001:660:4503:1::1 en 193.54.12.32. Afin de simplifier au maximum, nous considérerons que l'adresse source sera également translatée statiquement vers une adresse IPv4 prédéfinie.

1.2 - Translation dynamique

La translation statique est utile pour communiquer avec un poste précis mais il est inconcevable de mettre en place statiquement une table permettant d'accéder à tout l'Internet. Dans ce contexte il était donc nécessaire de mettre en œuvre un second mécanisme permettant de remplir dynamiquement la table de correspondance au fur et à mesure des besoins. Pour se faire la solution consiste à utiliser les réponses aux requêtes DNS traversant le routeur pour mettre à jour les correspondances. L'utilisation de la translation dynamique nécessite donc la mise en place d'une entrée statique permettant de communiquer avec le serveur de noms.

Voici les différentes étapes permettant la création d'une entrée dynamique (cf. Figure 2 : Scénario d'utilisation du mécanisme NAT-PT) :

1 : Le poste IPv6 émet une requête de résolution de noms de type AAAA pour www.google.fr. L'adresse destination utilisée est 2001:660:4503:1::1.

2 : Le routeur reçoit le paquet et s'aperçoit que l'adresse destination fait partie du préfixe NAT. Le paquet est donc translaté selon l'entrée statique correspondante et la requête de type AAAA et transformée en une requête de type A et une seconde de type AAAA.

3 : Le serveur de noms répond aux deux requêtes. Si il retourne une adresse IPv6 alors cette adresse est communiquée au client qui pourra alors accéder directement au site (sans NAT-PT). Dans le cas inverse le routeur utilisera l'adresse IPv4 retournée pour ajouter dynamiquement une entrée dans la table NAT. L'adresse IPv6 correspondante sera constituée du préfixe NAT suivie de l'adresse IPv4 convertie en caractères hexadécimaux (66.249.85.104=42F9.5568).

4 : Le routeur translatera ainsi la réponse de type A en réponse de type AAAA avec comme résultat à la requête, l'adresse constituée précédemment (2001:660:4503:1:42F9:5568).

5 : La communication peut avoir lieu puisqu'une entrée dans la table NAT a été créée.

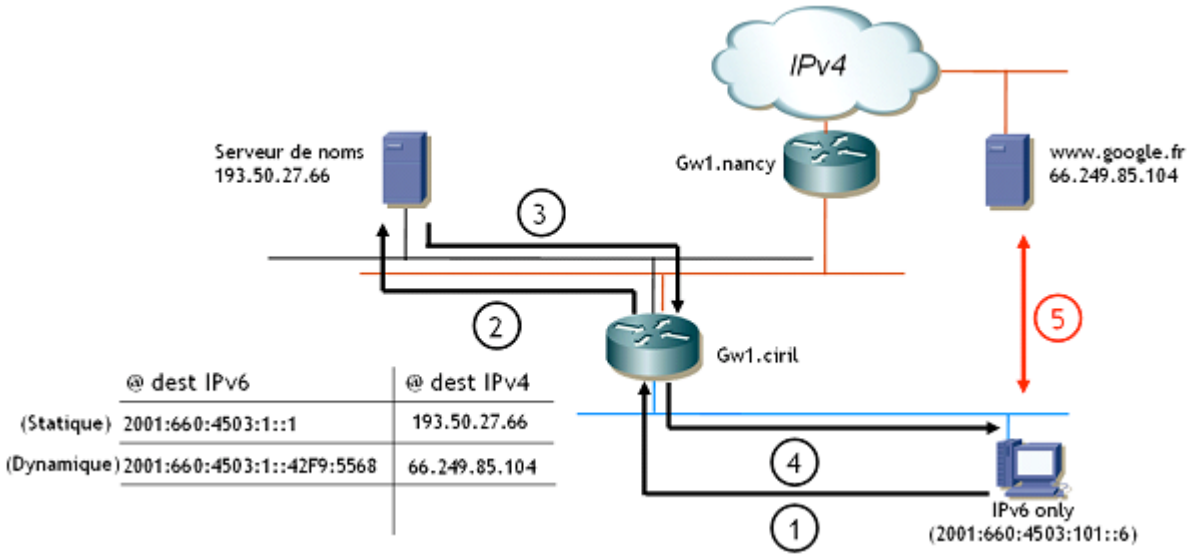


Figure 2 : Scénario d'utilisation du mécanisme NAT-PT

2 – Mise en oeuvre de l'implémentation CISCO

2.1 – Disponibilité dans l'IOS

Voici les versions minimums requises pour pouvoir bénéficier du mécanisme de transition NAT-PT :

NAT Protocol Translation	12.2(13)T, 12.3, 12.3(2)T, 12.4
Support for DNS ALG (translation dynamique)	12.2(13)T, 12.3, 12.3(2)T, 12.4
Support for port address translation (PAT) or overload (NAPT-PT)	12.3(2)T, 12.4

2.2 – Configuration

La première étape consiste à définir le préfixe de 96 bits qui sera utilisé pour identifier le trafic IPv6 devant être natté.

```
ipv6 nat prefix 2001:660:4503:1::/96
```

Il est ensuite nécessaire de définir une entrée statique dans la table de translation afin de pouvoir contacter le serveur DNS IPv4. Cette règle est indispensable pour réaliser par la suite les translations dynamiques.

```
ipv6 nat v4v6 source 193.50.27.66 2001:660:4503:1::1
```

D'après cette règle, tous les paquets émis par le poste 193.50.27.66 (ici le serveur de noms IPv4) seront translatés en IPv6 comme émis par le poste 2001:660:4503:1::1. De plus, l'adresse IPv6 sera translaté conformément à cette règle lorsqu'elle apparaîtra dans le champs destination d'un paquet. Cette directive permet donc à un poste IPv6 d'interroger le serveur de noms IPv4.

La dernière étape consiste à définir la ou les règles NAT permettant de réaliser les translations dynamiques.

```
ipv6 nat v6v4 source list natpt-list interface Loopback0 overload
!
ipv6 access-list natpt-list
   permit ipv6 2001:660:4503:102::/64
```

Cette directive autorise l'opération de NAT-PT conformément à l'access list natpt-list en surchargeant l'adresse de l'interface IPv4 Loopback0. Dans ce cas précis tous les postes du réseau 2001:660:4503:102::/64 sont autorisés à accéder au service NAT-PT et ainsi communiquer avec des équipements IPv4. A ce stade de la configuration, il ne reste alors plus qu'à activer le service pour l'ensemble des interfaces concernées (interfaces IPv4 et IPv6).

```
interface FastEthernet0.100
 encapsulation dot1Q 100
 ip address 193.50.80.58 255.255.255.224
 ip broadcast-address 193.50.80.63
 ipv6 nat
!
```

```
interface FastEthernet0.166
 encapsulation dot1Q 166
 ipv6 address 2001:660:4503:102::1/64
 ipv6 enable
 ipv6 nat
!
```

3 – Résultats

L'ensemble des tests réalisés dans le but de valider le bon fonctionnement du mécanisme de translation a permis d'évaluer les performances et les limites d'une telle solution.

Le premier test mis en oeuvre a consisté à vérifier le bon fonctionnement de la résolution de nom pour un équipement IPv4.

```
[root@sargas ~]# dig @2001:660:4503:1::1 -t AAAA free.fr
[...]
;; QUESTION SECTION:
;free.fr.                   IN      AAAA

;; ANSWER SECTION:
free.fr.            0       IN      AAAA    2001:660:4503:1::d5e4:2a

;; AUTHORITY SECTION:
free.fr.            0       IN      NS      freens1-a.free.fr.
free.fr.            0       IN      NS      freens1-1.free.fr.

;; ADDITIONAL SECTION:
freens1-a.free.fr.  0       IN      AAAA    2001:660:4503:1::d5e4:52
freens1-1.free.fr.  0       IN      AAAA    2001:660:4503:1::d5e4:c6
[...]
```

On remarque donc que l'adresse retournée est comme prévue constituée du préfixe NAT (2001:660:4503:1::/96) suivi de l'adresse IPv4 du site convertie en hexadécimal (213.228.0.42 = 0xD5E4002A). Ce test est donc conforme en tout point aux résultats attendus.

Nous avons ensuite naturellement essayé de contacter un équipement uniquement IPv4 en réalisant un ping6.

```
orval:/home/vincent# ping6 free.fr
PING free.fr(www1.free.fr) 56 data bytes
64 bytes from www1.free.fr: icmp_seq=1 ttl=56 time=5.95 ms
64 bytes from www1.free.fr: icmp_seq=2 ttl=56 time=6.40 ms
64 bytes from www1.free.fr: icmp_seq=3 ttl=56 time=7.13 ms
64 bytes from www1.free.fr: icmp_seq=4 ttl=56 time=6.76 ms
64 bytes from www1.free.fr: icmp_seq=5 ttl=56 time=5.88 ms
```

Ce test a également été couronné de succès mais il a permis de révéler un premier problème lié à l'implémentation faite par Cisco du mécanisme de NAT-PT et plus particulièrement au comportement du proxy DNS (DNS-ALG). La lenteur entre chaque réponse nous a amené à étudier de plus près les messages échangés. Nous avons ainsi remarqué que les résolutions inverses faites dans le domaine ip6.arpa pour résoudre l'adresse « pingée » posaient problèmes. En effet le routeur NAT translate la réponse dans le domaine ip6.int (cf. Annexe A). Dans ces conditions, cette dernière n'est pas acceptée et l'application attend une autre réponse. Ce problème explique donc la lenteur du ping

réalisé. L'option '–n' de la commande ping6 nous a permis d'empêcher les tentatives de résolutions inverses.

Les tests suivants ont finalement consisté à vérifier la possibilité d'accéder à divers services IPv4 en utilisant le mécanisme de NAT-PT. Mis à part le problème déjà évoqué, l'implémentation faite par Cisco s'est alors très bien comportée. Cependant le fonctionnement de l'ensemble des applications utilisées a posé une seconde difficulté. En effet les applications testées (Firefox, IE, …etc) ne prévoient pas une utilisation uniquement IPv6. Il en résulte systématiquement des interrogations DNS pour des ressources IPv4 qui ralentissent considérablement l'exécution du programme (cf. Annexe B pour plus de détail) puisque celles-ci sont bloquées par le routeur NAT-PT.

Conclusion

Etant donné les différents problèmes soulevés lors des tests de la mise en oeuvre du mécanisme de NAT-PT, il parait difficile d'envisager l'utilisation de ce mécanisme dans un réseau de production. Pour cela, il faudra inévitablement bénéficier d'applications et/ou de systèmes permettant une utilisation uniquement IPv6 sans forcément passer par de longues phases de configuration.

Références

RFC :

[1] RFC 2766 : Network Address Translation - Protocol Translation (NAT-PT)

[2] RFC 3142 : An IPv6-to-IPv4 Transport Relay Translator

[3] RFC 2694 : DNS extensions to Network Address Translators (DNS-ALG)

Documents :

Implementing IPv6 for Cisco IOS Software
http://www.cisco.com/application/pdf/en/us/guest/products/ps5187/c2001/ccmigration_09186a00801d7f16.pdf

Annexe A : Capture ping6

Cette capture illustre le problème des résolutions inverses avec l'implémentation Cisco du mécanisme NAT-PT rencontré lors d'un « ping6 » vers un poste IPv4. On remarque que le premier paquet (Frame 3) est une requête de résolution inverse dans le domaine ip6.arpa pour l'adresse pingée. Le second paquet correspond à la réponse mais indique que la requête correspondante est une résolution dans le domaine ip6.int. La réponse n'est pas prise en compte et la requête est réitérée (Frame 8) au bout d'un temps. Ce timeout ainsi que le nombre de tentatives de résolutions peuvent être spécifiés grâce aux options **timeout** et **attempts** dans le fichier resolv.conf.

```
# /etc/resolv.conf
nameserver 2001:660:4503:1::1
options timeout:5
options attempts: 2
```

Frame 3 (152 bytes on wire, 152 bytes captured)

Internet Protocol Version 6

    Version: 6

    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d

    Destination address: 2001:660:4503:1::1

User Datagram Protocol, Src Port: 32783 (32783), Dst Port: domain (53)

Domain Name System (query)

    Questions: 1

    Answer RRs: 0

    Authority RRs: 0

    Additional RRs: 0

    Queries

        a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.arpa: type PTR, class IN

            Name: a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.arpa

            Type: PTR (Domain name pointer)

            Class: IN (0x0001)

Frame 4 (279 bytes on wire, 279 bytes captured)

Internet Protocol Version 6

    Version: 6

    Source address: 2001:660:4503:1::1

    Destination address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d

User Datagram Protocol, Src Port: domain (53), Dst Port: 32783 (32783)

Domain Name System (response)

    Questions: 1

    Answer RRs: 1

    Authority RRs: 2

    Additional RRs: 2

    Queries

```
        a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int: type PTR,
class IN
            Name: a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int
            Type: PTR (Domain name pointer)
            Class: IN (0x0001)
    Answers
        a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int: type PTR,
class IN, www1.free.fr
            Name: a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int
            Type: PTR (Domain name pointer)
            Class: IN (0x0001)
            Time to live: 0 time
            Data length: 14
            Domain name: www1.free.fr



Frame 8 (151 bytes on wire, 151 bytes captured)
Internet Protocol Version 6
    Version: 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::1
User Datagram Protocol, Src Port: 32784 (32784), Dst Port: domain (53)
Domain Name System (query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int: type PTR,
class IN
            Name: a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int
            Type: PTR (Domain name pointer)
            Class: IN (0x0001)



Frame 9 (279 bytes on wire, 279 bytes captured)
Internet Protocol Version 6
    Version: 6
    Source address: 2001:660:4503:1::1
    Destination address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
User Datagram Protocol, Src Port: domain (53), Dst Port: 32784 (32784)
Domain Name System (response)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
    Queries
```

```
        a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int: type PTR,
class IN
            Name: a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int
            Type: PTR (Domain name pointer)
            Class: IN (0x0001)
    Answers
        a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int: type PTR,
class IN, www1.free.fr
            Name: a.2.0.0.4.e.5.d.0.0.0.0.0.0.0.0.1.0.0.0.3.0.5.4.0.6.6.0.1.0.0.2.ip6.int
            Type: PTR (Domain name pointer)
            Class: IN (0x0001)
            Time to live: 0 time
            Data length: 14
            Domain name: www1.free.fr



Frame 10 (118 bytes on wire, 118 bytes captured)
Internet Protocol Version 6
    Version: 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::d5e4:2a
Internet Control Message Protocol v6
    Type: 128 (Echo request)



No.     Time        Source                Destination           Protocol Info
     11 7.654620    2001:660:4503:1::d5e4:2a 2001:660:4503:101:2b0:d0ff:fee2:cc2d ICMPv6
Echo reply


Frame 11 (126 bytes on wire, 126 bytes captured)
Internet Protocol Version 6
    Version: 6
    Source address: 2001:660:4503:1::d5e4:2a
    Destination address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
Internet Control Message Protocol v6
    Type: 129 (Echo reply)
```

Annexe B : Capture HTTP

Cette capture illustre le problème soulevé lors de l'utilisation d'applications telles qu'un navigateur WEB avec le mécanisme de NAT-PT. Le premier paquet (frame 23) correspond à une requête de résolution de nom IPv6 pour l'adresse du serveur HTTP interrogé. Le paquet suivant correspond à la réponse du serveur. Alors que le navigateur connaît déjà l'adresse (IPv6) du serveur WEB à interroger il va cependant réaliser une requête de type A (pour une ressource IPv4). Cette requête étant bloquée au niveau du routeur NAT-PT par le proxy DNS (DNS-ALG) le poste va réitérer plusieurs fois la demande de résolution IPv4 (frame 25, 31, 36, 42) puis va se résigner à utiliser l'adresse IPv6 pour accéder au serveur HTTP (Frame 74) plus de 20 secondes après avoir reçu la réponse à la requête de type AAAA.

```
Frame 23 (92 bytes on wire, 92 bytes captured)
    Time since reference or first frame: 3.535739000 seconds
Internet Protocol Version 6
    Version: 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::1
User Datagram Protocol, Src Port: 32813 (32813), Dst Port: domain (53)
Domain Name System (query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ciril.fr: type AAAA, class IN
            Name: www.ciril.fr
            Type: AAAA (IPv6 address)
            Class: IN (0x0001)

Frame 24 (352 bytes on wire, 352 bytes captured)
    Time since reference or first frame: 3.538713000 seconds
Internet Protocol Version 6
    Source address: 2001:660:4503:1::1 (2001:660:4503:1::1)
    Destination address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
User Datagram Protocol, Src Port: domain (53), Dst Port: 32813 (32813)
Domain Name System (response)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 5
    Queries
        www.ciril.fr: type AAAA, class IN
            Name: www.ciril.fr
            Type: AAAA (IPv6 address)
```

```
            Class: IN (0x0001)
    Answers
        www.ciril.fr: type AAAA, class IN, addr 2001:660:4503:1::1
            Name: www.ciril.fr
            Type: AAAA (IPv6 address)
            Class: IN (0x0001)
            Time to live: 0 time
            Data length: 16
            Addr: 2001:660:4503:1::1


Frame 25 (92 bytes on wire, 92 bytes captured)
       Time since reference or first frame: 3.564700000 seconds
Internet Protocol Version 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::1 (2001:660:4503:1::1)
User Datagram Protocol, Src Port: 32813 (32813), Dst Port: domain (53)
Domain Name System (query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ciril.fr: type A, class IN
            Name: www.ciril.fr
            Type: A (Host address)
            Class: IN (0x0001)

Frame 31 (92 bytes on wire, 92 bytes captured)
       Time since reference or first frame: 8.575314000 seconds
Internet Protocol Version 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::1 (2001:660:4503:1::1)
User Datagram Protocol, Src Port: 32815 (32815), Dst Port: domain (53)
Domain Name System (query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ciril.fr: type A, class IN
            Name: www.ciril.fr
            Type: A (Host address)
            Class: IN (0x0001)

Frame 36 (92 bytes on wire, 92 bytes captured)
```

```
       Time since reference or first frame: 13.584690000 seconds
Internet Protocol Version 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::1 (2001:660:4503:1::1)
User Datagram Protocol, Src Port: 32817 (32817), Dst Port: domain (53)
Domain Name System (query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ciril.fr: type A, class IN
            Name: www.ciril.fr
            Type: A (Host address)
            Class: IN (0x0001)

Frame 42 (92 bytes on wire, 92 bytes captured)
       Time since reference or first frame: 18.594658000 seconds
Internet Protocol Version 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::1 (2001:660:4503:1::1)
User Datagram Protocol, Src Port: 32819 (32819), Dst Port: domain (53)
Domain Name System (query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ciril.fr: type A, class IN
            Name: www.ciril.fr
            Type: A (Host address)
            Class: IN (0x0001)

Frame 74 (94 bytes on wire, 94 bytes captured)
    Time since reference or first frame: 23.604877000 seconds
Internet Protocol Version 6
    Source address: 2001:660:4503:101:2b0:d0ff:fee2:cc2d
    Destination address: 2001:660:4503:1::1 (2001:660:4503:1::1)
Transmission Control Protocol, Src Port: 32793 (32793), Dst Port: www (80)
    Source port: 32793 (32793)
    Destination port: www (80)
    Sequence number: 0    (relative sequence number)
    Header length: 40 bytes
```