

# Comment le mode NAT traite-t-il les fragments ICMP

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Cas 1](#)

[Cas 2](#)

[Cas 3](#)

[Résumé](#)

[Informations connexes](#)

## [Introduction](#)

Ce document explique comment la traduction d'adresses de réseau (NAT) gère les fragments ICMP (Internet Control Message Protocol) lorsque vous configurez la surcharge NAT. Pour plus d'informations sur la surcharge NAT, reportez-vous à la [FAQ NAT](#).

La gestion des fragments ICMP dépend de l'état de la table de traduction NAT et de l'ordre dans lequel le routeur NAT reçoit les fragments ICMP. Nous allons examiner trois cas différents, dans lesquels nous envoyons deux requêtes ping de 172.16.0.1 à 172.17.1.2 avec une longueur de 3600 octets chacun (trois fragments IP).

## [Conditions préalables](#)

### [Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

### [Components Used](#)

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

### [Conventions](#)

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

## Cas 1

Dans ce scénario, nous voyons NAT créer une entrée de traduction entièrement étendue dans la table de traduction. Une fois cela fait, et il n'y a aucune autre adresse utilisable dans le pool NAT, NAT supprime tous les fragments reçus avant le premier fragment (fragment 0) d'un paquet.

Au début, une seule adresse du pool effectue une surcharge ; la table de traduction NAT est vide ; et la configuration NAT apparaît comme suit :

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

Examinons ce qui se passe lorsque des paquets commencent à arriver au routeur NAT.

1. Le fragment 0 du paquet 1 arrive et la NAT crée une entrée de traduction entièrement étendue. NAT traduit et transfère ensuite le fragment 0 du paquet 1. La table de traduction apparaît désormais comme suit :

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24320	172.16.0.1:24320	172.17.1.2:24320	172.17.1.2:24320

Notez le numéro 24320 dans le tableau de traduction ci-dessus. Il s'agit de la valeur de l'identificateur ICMP incluse dans l'en-tête ICMP du datagramme IP. Seul le fragment 0 du datagramme IP contient cet en-tête ICMP. Pour déterminer si plusieurs fragments font partie d'un même paquet, NAT doit suivre la valeur de l'identificateur IP, qui se trouve dans l'en-tête IP de tous les fragments du datagramme IP d'origine. Si plusieurs fragments ont la même valeur d'ID IP que le fragment 0, qui a créé la traduction étendue, NAT traduit ces fragments en utilisant la même entrée de traduction étendue. Référez-vous à [RFC 791](#) pour plus d'informations sur le champ d'identification IP. Référez-vous à [RFC 792](#) pour plus d'informations sur le champ d'identification ICMP.

2. Le paquet 1 fragment 2 et le paquet 1 fragment 1 arrivent. Puisque ces fragments font partie du même paquet qui contient le fragment 0 (qui a créé la traduction), NAT utilise l'entrée de traduction ci-dessus pour traduire et transférer ces fragments. Le périphérique de destination reçoit tous les fragments du paquet 1 et envoie une réponse.
3. Le fragment 1 du paquet 2 arrive. Comme il s'agit d'un nouveau paquet, sa valeur d'ID IP ne correspond à rien qui a été enregistré par NAT. Par conséquent, NAT ne peut pas utiliser la traduction existante. Il ne peut pas non plus créer une nouvelle traduction, car elle possède déjà une entrée de traduction entièrement étendue et n'a pas l'identificateur ICMP pour en créer une autre. NAT supprime le fragment 1 du paquet 2.
4. Le fragment 0 du paquet 2 arrive. NAT peut utiliser la traduction ci-dessus puisque l'identificateur ICMP correspond. (Toutes les requêtes ping d'un même ensemble de requêtes ping utilisent le même numéro d'identification ICMP.) À ce stade, NAT enregistre l'ID IP de ce paquet. NAT traduit et transfère le fragment 0 du paquet 2.
5. Le fragment 2 du paquet arrive. La traduction NAT peut désormais utiliser la traduction ci-dessus, car sa valeur d'ID IP correspond à la NAT enregistrée à l'étape précédente. NAT traduit et transfère le fragment 2 du paquet. Le périphérique de destination reçoit uniquement les fragments 0 et 2 (le fragment 1 est manquant), donc il n'envoie aucune réponse.

## Cas 2

Dans ce scénario, nous voyons que si des fragments autres que le premier fragment (fragment 0) arrivent en premier, NAT crée une traduction simple tant qu'il y a une adresse dans le pool NAT qui n'a pas déjà été utilisée dans une traduction entièrement étendue.

Au début, il n'y a qu'une seule adresse dans le pool NAT, la table de traduction NAT est vide et la configuration apparaît comme suit :

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

1. Le fragment 1 du paquet arrive. NAT ne peut pas créer une traduction entièrement étendue dans la table de traduction, car elle ne contient pas les informations d'identification ICMP dans ce fragment. Cependant, comme il n'y a pas de traductions entièrement étendues en place, NAT entre une traduction simple. NAT traduit et transfère ensuite le paquet 1 fragment 1. L'entrée de traduction s'affiche comme suit :

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---

2. Le fragment 0 du paquet 1 arrive. Puisque les informations d'identification ICMP sont incluses dans ce fragment, NAT entre une entrée de traduction complète étendue :

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---
icmp	10.10.10.3:24321	172.16.0.1:24321	172.17.1.2:24321	172.17.1.2:24321

NAT enregistre ensuite les informations d'identification IP, traduit et transfère le fragment 0 du paquet 1.

3. Le fragment 2 du paquet 1 arrive. Comme ce fragment possède les mêmes informations d'identification IP que la NAT enregistrée à l'étape 2, la NAT utilise la traduction entièrement étendue pour traduire et transférer le fragment 2 du paquet 1. Le périphérique de destination reçoit tous les fragments et les réponses. À ce stade, toutes les requêtes ping aboutissent jusqu'à ce que la table de traduction NAT soit effacée ou expire.

## Cas 3

Dans ce scénario, nous voyons que si des fragments autres que le premier fragment (fragment 0) arrivent en premier, NAT crée une traduction simple tant qu'il y a une adresse dans le pool NAT qui n'a pas déjà été utilisée dans une traduction entièrement étendue. Si une traduction étendue de la table NAT utilise déjà l'adresse, vous courez le risque de traduire NAT chacune des adresses source de fragment en une adresse différente.

Au début, plusieurs adresses du pool NAT effectuent une surcharge, la table de traduction a déjà une traduction étendue en place et la configuration est la suivante :

```
ip nat pool POOL1 10.10.10.3 10.10.10.5 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

La table de traduction apparaît comme suit :

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

1. Le fragment 1 du paquet arrive. La NAT ne peut pas créer une entrée de table de traduction

entièrement étendue car elle ne contient pas les informations d'identification ICMP dans ce fragment et elle ne peut pas créer une entrée de traduction simple pour l'adresse 10.10.10.3, car il existe une entrée étendue existante pour cette adresse IP. NAT sélectionne l'adresse IP libre suivante (10.10.10.4) et crée une traduction simple. NAT traduit et transfère ensuite le paquet 1 fragment 1. La table de traduction apparaît désormais comme suit :

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

2. Le fragment 0 du paquet 1 arrive. Puisque les informations d'identification ICMP sont incluses dans ce fragment, NAT entre une entrée de traduction complète étendue pour l'adresse 10.10.10.3 et enregistre les informations d'identification IP pour ce paquet. NAT traduit et transfère ensuite le fragment 0 du paquet 1. La table de traduction apparaît désormais comme suit :

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322
icmp	10.10.10.3:24323	172.16.0.1:24323	172.17.1.2:24323	172.17.1.2:24323

3. Le fragment 2 du paquet 1 arrive. Puisque ses informations d'identification IP correspondent à la NAT enregistrée à l'étape 2, la NAT utilise la traduction entièrement étendue créée à l'étape 2 pour traduire et transférer le paquet 1 fragment 2. À ce stade, le périphérique de destination reçoit tous les fragments du paquet 1, mais les fragments 0 et 2 ont fait traduire leur adresse source en 10.10.10.3 et le fragment 1 en 10.10.10.4. Par conséquent, le périphérique de destination ne peut pas réassembler le paquet et n'envoie aucune réponse.
4. Le fragment 0 du paquet 2 arrive. NAT utilise la traduction complète ci-dessus ou crée une nouvelle traduction complète en fonction de la valeur du champ ID ICMP de fragment. Dans les deux cas, NAT enregistre les informations d'identification IP. NAT traduit et transfère ensuite le fragment 0 du paquet 2.
5. Le fragment 2 du paquet arrive. Ses informations d'ID IP correspondent à ce que NAT a enregistré à l'étape 4. La NAT utilise donc la deuxième traduction entièrement étendue créée à l'étape 4. NAT traduit et transfère le fragment 2 du paquet.
6. Le fragment 1 du paquet 2 arrive. Ses informations d'ID IP correspondent à ce que NAT a enregistré à l'étape 4. La NAT utilise donc la deuxième traduction entièrement étendue créée à l'étape 4. NAT traduit et transfère le fragment 1 du paquet 2. Le périphérique de destination reçoit les trois fragments du paquet 2 de la même source (10.10.10.3), de sorte qu'il réassemble le paquet et répond.

## Résumé

Le fait que NAT abandonne ou transfère un fragment ICMP dépend de plusieurs éléments, tels que l'ordre dans lequel le routeur NAT reçoit les fragments et l'état de la table de traduction à ce moment-là. Dans certaines conditions, la traduction NAT traduit les fragments différemment, ce qui rend impossible pour le périphérique de destination de réassembler le paquet.

## Informations connexes

- [Page de support NAT](#)
- [Page de support pour le routage IP](#)

- [Support technique - Cisco Systems](#)