

Как NAT обрабатывает фрагменты ICMP

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Пример 1](#)

[Случай 2](#)

[Случай 3](#)

[Сводка](#)

[Дополнительные сведения](#)

Введение

Этот документ объясняет как преобразование сетевых адресов (NAT) регулирует части протокола Internet Control Message Protocol (ICMP) когда вы установите перегрузку трансляции сетевых адресов. Для получения информации о Перегрузке трансляции сетевых адресов обратитесь к [часто задаваемым вопросам NAT](#).

Обработка фрагментов ICMP зависит от состояния Таблицы преобразования сетевых адресов (NAT) и заказа, в котором маршрутизатор NAT получает фрагменты ICMP. Рассмотрим три различных случая отправки двух пинговых пакетов с адреса 172.16.0.1 на адрес 172.17.1.2; размер каждого пакета составляет 3600 байтов (три IP-фрагмента).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Пример 1

В этом сценарии NAT создает полную запись расширенной трансляции в таблице трансляции. После этого и отсутствия в пуле NAT возможных для использования адресов, NAT будет отбрасывать любые фрагменты, полученные до первого фрагмента (фрагмент 0) пакета.

Поскольку мы запускаем, только один адрес в пуле выполняет перегрузку; Таблица преобразования сетевых адресов (NAT) пуста; и конфигурация NAT появляется как:

```
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
```

Давайте посмотрим, что случается, когда пакеты начинают поступать на маршрутизатор NAT.

1. Приходит фрагмент 0 пакета 1, и NAT создает полностью расширенную запись трансляции. NAT тогда преобразовывает и передает пакет 1 фрагмент 0. Таблица преобразования теперь появляется как:

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

Обратите внимание на число 24320 в таблице преобразования вверху. Это значение идентификатора ICMP включенное в заголовке ICMP датаграммы IP. Только фрагмент 0 IP-датаграммы содержит такой заголовок ICMP. Чтобы определить, являются ли несколько фрагментов частью одного и того же пакета, NAT должен отслеживать значение идентификатора IP, помещаемого в IP-заголовки всех фрагментов из исходной IP-датаграммы. Если несколько фрагментов имеют то же значение опознавания IP как фрагмент 0, который создал расширенную трансляцию, NAT преобразовывает эти фрагменты с помощью той же записи расширенной трансляции. См. [RFC 791](#) для получения дополнительной информации о поле идентификации IP. См. [RFC 792](#) для получения дополнительной информации о поле идентификации ICMP.
2. Получены фрагменты 2 и 1 пакета 1. Так как данные фрагменты являются частью одного пакета, содержащего фрагмент 0 (определяет преобразование), описанная выше запись преобразования используется протоколом NAT для преобразования и пересылки данных фрагментов. Целевое устройство получает все фрагменты для пакета 1 и передает ответ.
3. Получение фрагмента 2 пакета 1. Так как это - новый пакет, его значение опознавания IP не совпадает ни с чем, что было зарегистрировано NAT. Поэтому NAT не может использовать существующее преобразование. Также она не может создать новую трансляцию, поскольку уже имеет полностью расширенную запись трансляции и не имеет идентификатора ICMP, чтобы создать еще одну. NAT отброшен фрагмент 1 пакета 2.
4. Получен пакет 2, фрагмент 0. NAT может использовать вышеуказанное преобразование, так как идентификатор ICMP соответствует. (Весь пинг внутри обычного набора пинга использует такой же номер идентификатора ICMP.) На этом этапе NAT делает запись идентификатора IP этого пакета. NAT транслирует и пересылает фрагмент 0 пакета 2.
5. Прибывает фрагмент 2 пакета 2. Теперь NAT может использовать представленную

выше обработку, так как IP идентификационное значение согласовывается с одним NAT, записанным в предыдущем шаге. NAT преобразовывает и передает пакет 2 фрагмента 2. Устройство назначения получает только фрагменты 0 и 2 (фрагмент 1 отсутствует), поэтому ответ не посылается.

Случай 2

В этом сценарии, мы видим что если все части за исключением первой части (части 0) прибывают первыми, то NAT создает простое преобразование пока адрес в области NAT которая уже не была использована в полностью расширенной трансляции.

Поскольку мы запускаем, существует только один адрес в пуле NAT, Таблица преобразования сетевых адресов (NAT) пуста, и конфигурация появляется как:

```
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. Получение фрагмента 1 пакета 1. NAT не может сформировать полностью расширенное преобразование в таблице преобразования, так как в этом ее фрагменте не содержится информация об отступе ICMP. Однако, так как полностью расширенные преобразования отсутствуют, NAT вводит простое преобразование. NAT тогда преобразовывает и передает пакет 1 фрагмент 1. Транслируемое значение появляется

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

2. Прибывает пакет 1 фрагмент 0. Поскольку данные опознавания ICMP включены в этот фрагмент, NAT вводит запись полностью расширенной трансляции:

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
```

тогда делает запись сведений ident IP, и преобразовывает и передает пакет 1 фрагмент 0.

3. Получение фрагмента 2 пакета 1. Поскольку этот фрагмент имеет те же сведения ident IP, которых NAT сделал запись в шаге 2, NAT использует полностью расширенную трансляцию для перевода и передача пакетов 1 фрагмент 2. Устройство назначения принимает все пакеты и отвечает. На На этой стадии все команды "ping" прошли успешно до того момента, пока таблица преобразования NAT не была очищена или не превысила время ожидания.

Случай 3

В этом сценарии, мы видим что если все части за исключением первой части (части 0) прибывают первыми, то NAT создает простое преобразование пока адрес в области NAT которая уже не была использована в полностью расширенной трансляции. Если расширенная трансляция в таблице NAT уже использует адрес, вы рискуете NAT, преобразовывающим каждый из адресов источника фрагмента к другому адресу.

Как только мы начинаем, больше чем один адрес в области NA выполняет перегрузку, таблица преобразования уже имеет расширенное преобразование в этом месте и её конфигурация является следующей:

```
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
```

Таблица преобразования появляется как:

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. Получение фрагмента 1 пакета 1. NAT не может создать элемент таблицы полностью расширенной трансляции, так как он не имеет Данных опознавания ICMP в этом фрагменте, и он не может создать запись простой трансляции для адреса 10.10.10.3, так как существует существующая расширенная запись для этого IP-адреса. NAT выбирает следующий свободный IP-адрес (10.10.10.4) и создает простую трансляцию. NAT тогда преобразовывает и передает пакет 1 фрагмент 1. Таблица преобразования

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. Прибывает пакет 1 фрагмент 0. Поскольку в данный фрагмент входят опознавательные данные ICMP, преобразование NAT вводит запись полностью расширенного преобразования для адреса 10.10.10.3 и записывает опознавательные данные IP для данного пакета. NAT тогда преобразовывает и передает пакет 1 фрагмент 0. Таблица преобразования теперь появляется как:

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. Получение фрагмента 2 пакета 1. Так как информация, определяющая IP, совпадает с одним из NAT, записанных на шаге 2, NAT использует полностью расширенную трансляцию, созданную на шаге 2, для трансляции и переадресации фрагмента 2 пакета 1. В это время устройство получателя получает все фрагменты пакета 1, но у фрагмента 0 и фрагмента 2 адрес источника был преобразован в 10.10.10.3, а у фрагмента 1 - в 10.10.10.4. Поэтому, целевое устройство не может собрать пакеты и послать ответ.
4. Получен пакет 2, фрагмент 0. NAT или использует вышеупомянутую полностью расширенную трансляцию или создает новую полностью расширенную трансляцию в зависимости от значения поля идентификатора ICMP фрагмента. В любом случае NAT делает запись сведений ident IP. NAT тогда преобразовывает и передает пакет 2 фрагмента 0.
5. Прибывает фрагмент 2 пакета 2. Его опознавательные данные IP совпадают с записью NAT на шаге 4, поэтому NAT использует второе полностью расширенное преобразование, выполненное на шаге 4. NAT преобразует и переадресует фрагмент 2 пакета 2.
6. Получение фрагмента 2 пакета 1. Его сведения ident IP совпадают с тем, что NAT, зарегистрированный в шаге 4, таким образом, NAT использует вторую полностью расширенную трансляцию, созданную в шаге 4. NAT преобразовывает и передает пакет 2 фрагмента 1. Устройство назначения получает все три фрагмента пакета 2 из одного источника (10.10.10.3), повторно монтирует пакет и отвечает.

Отбросит ли NAT фрагмент ICMP или передаст дальше, зависит от ряда факторов, таких как порядок, в котором маршрутизатор NAT получает фрагменты, и состояние таблицы преобразования на текущий момент. При определенных условиях NAT преобразовывает фрагменты по-другому, который лишает возможности целевое устройство повторно собирать пакет.

[Дополнительные сведения](#)

- [Страница поддержки NAT](#)
- [Страница поддержки IP-маршрутизации](#)
- [Техническая поддержка - Cisco Systems](#)