



Проверка работоспособности и устранение основных неполадок протокола NAT (Network Address Translation, преобразование сетевых адресов)

Данный документ содержит флэш-анимацию.

Интерактивный документ. В данном документе приводится анализ используемого устройства Cisco.

Содержание

Введение

Предварительные условия

- Требования

- Используемые компоненты

- Условные обозначения

Как отключить протокол NAT

Учебный пример с флэш-анимацией. Запрос "ICMP-эхо" удается отправить на хост, но не работает Telnet

Учебный пример с флэш-анимацией. Запрос "ICMP-эхо" не удается отправить за NAT

Пример проблемной ситуации. Запрос "ICMP-эхо" работает только для одного маршрутизатора из двух

- Краткое описание проблемы

Пример проблемной ситуации: Внешние сетевые устройства не взаимодействуют с внутренними маршрутизаторами

- Краткое описание проблемы

Контрольные таблицы для устранения неполадок

- Преобразование не установлено в таблице преобразований

- Не используется правильная запись о преобразовании

- Протокол NAT работает правильно, но проблемы с соединением остались

- Заключение

Дополнительные сведения

Введение

При наличии проблем IP-соединения в среде NAT часто бывает трудно определить причину возникновения этой проблемы. Ответственность за это часто по ошибке возлагается на протокол NAT, тогда как на самом деле причина кроется глубже. Это документ показывает, как проверить работу протокола NAT с помощью средств, имеющихся в маршрутизаторах Cisco. В этом документе также объясняется, как выполнять элементарный поиск и устранение неисправностей протокола NAT и описывается, как не допустить частых ошибок во время поиска и устранения неисправностей с NAT.

Предварительные условия

Требования

В данном документе не выдвигаются никаких особых требований.

Используемые компоненты

Сведения в данном документе не ограничиваются определенными версиями ПО или устройств.

Данные для этого документа были получены при тестировании указанных устройств в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, запускались с чистой (заданной по умолчанию) конфигурацией. Если сеть работает в реальных условиях, при использовании каждой команды следует адекватно оценивать ее потенциальное воздействие.

Условные обозначения

Дополнительные сведения о применяемых в документе обозначениях см. в документе Условные обозначения, используемые в технической документации Cisco.

Как отключить протокол NAT

Отключение протокола NAT облегчает поиск причин возникновения проблем IP-соединения. Чтобы удостовериться, что протокол NAT функционирует должным образом, выполните следующие действия:

1. В соответствии с конфигурацией, четко определите, что должен делать протокол NAT. На этом шаге можно определить наличие проблемы с конфигурацией. Дополнительные сведения о настройке NAT см. в разделе Настройка преобразования сетевых адресов (NAT). Начало работы.
2. Убедитесь, что в таблице преобразований существуют правильные преобразования.
3. Чтобы убедиться в том, что преобразование происходит, используйте команды **show** и **debug**.
4. Подробно проверьте, что происходит с пакетом данных, и убедитесь, что у маршрутизаторов имеются правильные данные маршрутизации для пересылки пакета.

Ниже приводятся примеры нескольких проблемных ситуаций, в которых используются вышеупомянутые действия для определения причин проблем.

Учебный пример с флэш-анимацией. Запрос "ICMP-эхо" удается отправить на хост, но не работает Telnet

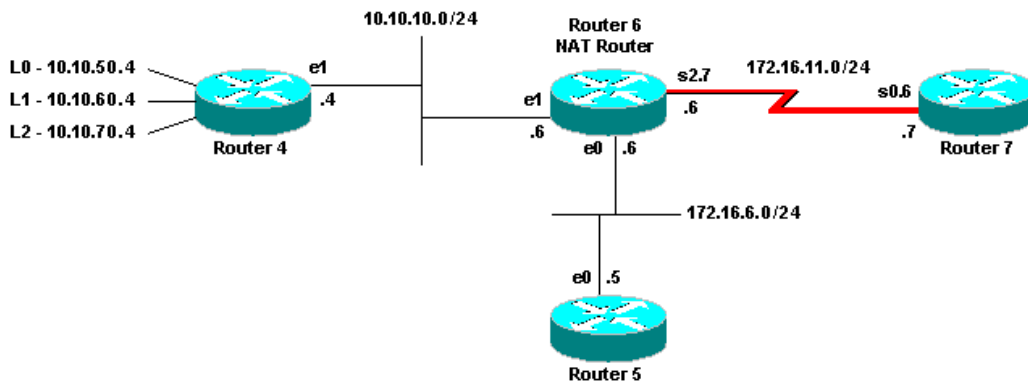
Щелкните здесь [↗](#), чтобы просмотреть 7-минутный анимационный ролик о том, почему устройство может отправить запрос "ICMP-эхо" на хост, но при этом не работает функция Telnet.

Учебный пример с флэш-анимацией. Запрос "ICMP-эхо" не удается отправить за NAT

Щелкните здесь [↗](#), чтобы просмотреть 10-минутный анимационный ролик о том, почему устройство не может отправить запрос "ICMP-эхо" за NAT.

Пример проблемной ситуации. Запрос "ICMP-эхо" работает только для одного маршрутизатора из двух

На этой схеме сети 4-ый маршрутизатор получает ответ на запрос "ICMP-эхо" от 5-го маршрутизатора (172.16.6.5), но не от 7-го (172.16.11.7).



Ни на одном из маршрутизаторов не запущен ни один протокол маршрутизации, а для 4-ого маршрутизатора 6-ой задан как шлюз по умолчанию. 6-ой маршрутизатор настраивается с помощью протокола NAT следующим образом:

6-ой маршрутизатор

```
interface Ethernet0
ip address 172.16.6.6 255.255.255.0
ip directed-broadcast
ip nat outside
media-type 10BaseT
!
interface Ethernet1
ip address 10.10.10.6 255.255.255.0
ip nat inside
media-type 10BaseT
!
interface Serial2.7 point-to-point
ip address 172.16.11.6 255.255.255.0
ip nat outside
frame-relay interface-dlci 101
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
!
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4
```

Сначала следует убедиться в правильном функционировании протокола NAT. Согласно известной вам конфигурации, IP-адрес 4-ого маршрутизатора (10.10.10.4) должен статически преобразовываться в 172.16.6.14. На 6-ом маршрутизаторе можно использовать команду **show ip nat translation**, чтобы удостовериться, что это преобразование действительно существует в таблице преобразований.

```
router-6# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.6.14        10.10.10.4       ---                ---
```

Теперь необходимо убедиться, что преобразование происходит, когда 4-ый маршрутизатор выдает IP-трафик. Для этого на 6-ом маршрутизаторе можно использовать два метода: выполнить команду NAT **debug** или проследить статистику NAT с помощью команды **show ip nat statistics**. Так как команды **debug** должны использоваться в крайнем случае, начинать следует с команды **show**.

Смысл этих действий состоит в том, чтобы отследить число обращений и узнать, растет ли оно по мере отправки трафика с 4-ого маршрутизатора. Это число увеличивается каждый раз, когда преобразование из таблицы используется для преобразования адреса. В первую очередь обнулите статистику, затем выведите ее на экран, попытайтесь послать запрос "ICMP-эхо" с 4-ого маршрутизатора на 7-ой, а затем снова посмотрите статистику.

```
router-6# clear ip nat statistics
```

```

router-6#
router-6# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Ethernet0, Serial2.7
Inside interfaces:
Ethernet1
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 7 pool test refcount 0
pool test: netmask 255.255.255.0
start 172.16.11.70 end 172.16.11.71
type generic, total addresses 2, allocated 0 (0%), misses 0
router-6#

```

После использования команды **ping 172.16.11.7** на 4-ом маршрутизаторе статистика NAT на 6-ом маршрутизаторе будет следующей:

```

router-6# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Ethernet0, Serial2.7
Inside interfaces:
Ethernet1
Hits: 5 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 7 pool test refcount 0
pool test: netmask 255.255.255.0
start 172.16.11.70 end 172.16.11.71
type generic, total addresses 2, allocated 0 (0%), misses 0

```

Из сообщений команды **show** видно, что число обращений выросло на 5. В случае успешного выполнения команды **ping** на маршрутизаторе Cisco число обращений должно увеличиться на 10. Пять эхо-сигналов ICMP (Internet Control Message Protocol, межсетевой протокол контрольных сообщений), переданных с исходного маршрутизатора (4-ого), должны быть преобразованы, и пять ответных эхо-пакетов с маршрутизатора назначения (7-ого) также должны быть преобразованы, то есть общее число обращений должно быть равно десяти. Пять обращений теряются, скорее всего, из-за эхо-ответов, которые либо не были преобразованы, либо не были отправлены с 7-ого маршрутизатора.

Проверьте, можно ли найти какую-либо причину, по которой 7-ой маршрутизатор мог не отправить ответные эхо-пакеты 4-ому маршрутизатору. Прежде всего необходимо узнать, что NAT делает с пакетами. 4-ый маршрутизатор посылает эхо-пакеты ICMP с адресом источника 10.10.10.4 и адресом назначения 172.16.11.7. После выполнения протокола NAT пакет, полученный 7-ым маршрутизатором, будет иметь адрес источника 172.16.6.14 и адрес получателя 172.16.11.7. Маршрутизатору 7 требуется дать ответ на адрес 172.16.6.14, а поскольку последний напрямую не подключен к 7-ому маршрутизатору, для ответа ему нужен маршрут для этой сети. Убедитесь в существовании маршрута, проверив таблицу маршрутизации 7-ого маршрутизатора.

```

router-7# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 4 subnets
C       172.16.12.0 is directly connected, Serial0.8
C       172.16.9.0 is directly connected, Serial0.5
C       172.16.11.0 is directly connected, Serial0.6
C       172.16.5.0 is directly connected, Ethernet0

```

Как видите, в таблице маршрутизации 7-ого маршрутизатора нет маршрута для адреса 172.16.6.14. После добавления этого маршрута эхо-запросы будут успешно выполняться.

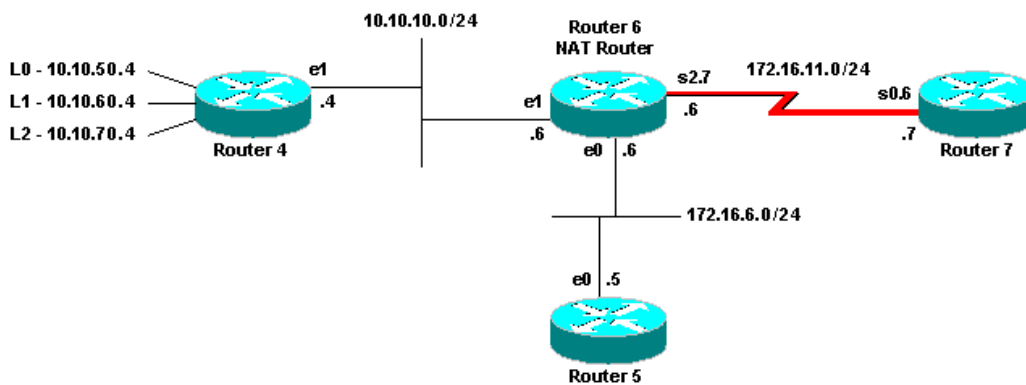
Краткое описание проблемы

Сначала вы определили, какие операции должен был совершить протокол NAT. Далее было проверено существование и правильность статической записи протокола NAT в таблице преобразований. Проверка статистики операций протокола NAT показала, что преобразование действительно имело место. Затем была обнаружена неполадка, которая привела к необходимости проверки данных маршрутизации на 7-ом маршрутизаторе. Проверка показала, что 7-му маршрутизатору был необходим маршрут к внутреннему глобальному адресу 4-ого маршрутизатора.

Обратите внимание, что в этих простых лабораторных условиях полезно отследить статистику операций NAT с помощью команды **show ip nat statistics**. Однако в более сложной среде NAT с несколькими выполняющимися преобразованиями, команда **show** не будет столь полезна. В таком случае, возможно, понадобится использовать на маршрутизаторе команду **debug**. В следующем сценарии проблемной ситуации показано использование команд **debug**.

Пример проблемной ситуации. Внешние сетевые устройства не могут взаимодействовать с внутренними маршрутизаторами

В данном сценарии 4-ый маршрутизатор может отправить запрос "ICMP-эхо" как на 5-ый, так и на 7-ой маршрутизаторы с помощью команды **ping**, но устройства в сети 10.10.50.0 не могут установить связь с 5-ым или 7-ым маршрутизатором (в испытательной лаборатории этот процесс эмулируется путем отправки, с помощью команды **ping**, запроса "ICMP-эхо" с интерфейса обратной связи с IP-адресом 10.10.50.4). Взгляните на схему сети.



6-ой маршрутизатор

```
interface Ethernet0
ip address 172.16.6.6 255.255.255.0
ip directed-broadcast
ip nat outside
media-type 10BaseT
!
interface Ethernet1
ip address 10.10.10.6 255.255.255.0
ip nat inside
media-type 10BaseT
!
interface Serial2.7 point-to-point
ip address 172.16.11.6 255.255.255.0
ip nat outside
frame-relay interface-dlci 101
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
!
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4
```

Во-первых, четко определите требования к работе протокола NAT. Согласно конфигурации 6-ого маршрутизатора, адрес 10.10.50.4 должен быть динамически преобразован в первый доступный адрес при "проверке" пула NAT. Этот пул состоит из адресов 172.16.11.70 и 172.16.11.71. Из того, что было выяснено по этой проблеме выше, можно сделать вывод, что пакеты, полученные 5-ым и 7-ым маршрутизаторами, имеют исходный адрес 172.16.11.70 или 172.16.11.71. Эти адреса находятся в той же подсети, что и 7-ой маршрутизатор, поэтому у 7-ого маршрутизатора должен быть напрямую подключенный маршрут, однако 5-ому маршрутизатору понадобится маршрут к подсети, если он еще не настроен.

Чтобы убедиться в том, что в таблице маршрутизации 5-ого маршрутизатора действительно есть адрес 172.16.11.0, можно использовать команду **show ip route**:

```
router-5# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 4 subnets
C 172.16.9.0 is directly connected, Serial1
S 172.16.11.0 [1/0] via 172.16.6.6
C 172.16.6.0 is directly connected, Ethernet0
C 172.16.2.0 is directly connected, Serial0
```

Чтобы убедиться в том, что в таблице маршрутизации 7-ого маршрутизатора адрес 172.16.11.0 записан как адрес непосредственно подключенной подсети, можно использовать команду **show ip route**:

```
router-7# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
C    172.16.12.0 is directly connected, Serial0.8
C    172.16.9.0 is directly connected, Serial0.5
C    172.16.11.0 is directly connected, Serial0.6
C    172.16.5.0 is directly connected, Ethernet0
S    172.16.6.0 [1/0] via 172.16.11.6
```

Теперь, после явного указания действий для протокола NAT, необходимо проверить, что он работает корректно. Начните с проверки таблицы преобразования NAT и убедитесь, что ожидаемое преобразование существует. Так как рассматриваемое преобразование создается динамически, необходимо в первую очередь отправить IP-трафик с соответствующего адреса. После отправки запроса "ICMP-эхо" с помощью команды **ping** с адреса 10.10.50.4 на адрес 172.16.11.7, в таблице преобразований 6-ого маршрутизатора будет отображаться следующая информация:

```
router-6# show ip nat translation
Pro Inside global      Inside local      Outside local     Outside global
--- 172.16.6.14        10.10.10.4       ---              ---
--- 172.16.11.70      10.10.50.4       ---              ---
```

Поскольку ожидаемое преобразование содержится в таблице преобразований, то мы знаем, что преобразование для эхо-пакетов ICMP выполняется правильно, но что можно сказать об ответных эхо-пакетах? Как упоминалось ранее, можно отслеживать статистику NAT, но в сложной среде это не дает особого эффекта. Другой вариант – запустить отладку протокола NAT на маршрутизаторе NAT (6-ой маршрутизатор). В этом случае, во время выполнения команды **ping** с адреса 10.10.50.4 на адрес 172.16.11.7, необходимо выполнить команду **debug ip nat** на 6-ом маршрутизаторе. Результат выполнения команды **debug** показан ниже.

Примечание. При использовании на маршрутизаторе любой команды **debug**, возможна перегрузка маршрутизатора, что приведет к его неработоспособности. Всегда будьте очень внимательны и, если возможно, никогда не прибегайте к использованию команды **debug** при работе с критически важными маршрутизаторами без участия специалиста Службы технической поддержки Cisco.

```
router-6# show log
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 39 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 39 messages logged
  Trap logging: level informational, 33 message lines logged
```

```
Log Buffer (4096 bytes):
```

```
05:32:23: NAT: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [70]
05:32:23: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [70]
05:32:25: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [71]
05:32:25: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [71]
05:32:27: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [72]
05:32:27: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [72]
05:32:29: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [73]
05:32:29: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [73]
05:32:31: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [74]
05:32:31: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [74]
```

Как видно из приведенных выше результатов применения команды **debug**, первая строка показывает преобразование исходного адреса 10.10.50.4 в 172.16.11.70. Вторая строка показывает адрес назначения 172.16.11.70, преобразованный обратно в 10.10.50.4. Эта схема повторяется во всех дальнейших результатах работы команды **debug**. Это говорит о том, что 6-ой маршрутизатор преобразует пакеты в обоих направлениях.

Теперь рассмотрим более подробно, что же именно должно происходить. 4-ый маршрутизатор посылает пакет с адреса 10.10.50.4 на адрес 172.16.11.7. 6-ой маршрутизатор выполняет протокол NAT для пакета и пересылает его с адреса 172.16.11.70 на 172.16.11.7. 7-ой маршрутизатор посылает ответ с исходным адресом 172.16.11.7 и адресом назначения 172.16.11.70. 6-ой маршрутизатор выполняет NAT для пакета, в результате чего получается пакет с исходным адресом 172.16.11.7 и адресом назначения 10.10.50.4. На этом этапе 6-ой маршрутизатор должен отправить пакет на адрес 10.10.50.4, основываясь на информации в его таблице маршрутизации. Чтобы убедиться, что 6-ой маршрутизатор имеет необходимый маршрут в своей таблице, необходимо использовать команду **show ip route**.

```
router-6# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/24 is subnetted, 5 subnets
C 172.16.8.0 is directly connected, Serial1
C 172.16.10.0 is directly connected, Serial2.8
C 172.16.11.0 is directly connected, Serial2.7
C 172.16.6.0 is directly connected, Ethernet0
C 172.16.7.0 is directly connected, Serial0
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Ethernet1
```

Краткое описание проблемы

Во-первых, было четко определено, какой протокол NAT предполагалось выполнить. Во-вторых, было проверено наличие необходимых правил преобразования в таблице преобразования. В-третьих, использовалась команда **debug** или **show**, которая позволила убедиться, что преобразование действительно имело место. Наконец, был подробно рассмотрен процесс передачи пакета, а также действия маршрутизатора по его пересылке или отправке ответа.

Контрольные таблицы для устранения неполадок

Теперь, когда указана процедура поиска причин неисправностей при установлении соединения, будет представлено несколько контрольных таблиц для устранения типичных неполадок.

Преобразование не установлено в таблице преобразований

Если обнаруживается, что соответствующее преобразование не установлено в таблице преобразований, убедитесь в следующем:

- Настройка осуществлена правильно. Использование протокола NAT для выполнения требуемых действий иногда может быть весьма неочевидным. Дополнительные сведения о настройке протокола NAT см. в документе Настройка преобразования сетевых адресов (NAT). Начало работы.
- Не существует списков входящего доступа, на основании которых отклонялись бы пакеты, входящие в маршрутизатор NAT.
- У маршрутизатора NAT есть соответствующий маршрут в таблице маршрутизации, если пакет идет изнутри наружу. Дополнительные сведения см. в документе Порядок работы протокола NAT.
- Список доступа, на который ссылается команда NAT, разрешает использование всех необходимых сетей.
- В пуле NAT имеется достаточно адресов. Это будет проблемой, только если протокол NAT не настроен для перегрузки.
- Интерфейсы маршрутизатора правильно определены как внутренний или внешний протокол NAT.
- В случае преобразования полезной нагрузки пакетов DNS (Domain Name System, система доменных имен) следует убедиться, что преобразование делается для адреса, указанного в IP-заголовке пакета. Если это не выполняется, то протокол NAT не проверяет полезную нагрузку пакета.

Не используется запись о правильном преобразовании

Если запись о правильном преобразовании в таблице преобразований есть, но не используется, проверьте следующее:

- Убедитесь, что не существует списков входящего доступа, на основании которых отклоняются пакеты, входящие в маршрутизатор NAT.
- Для пакетов, которые передаются из внутренней сети во внешнюю, следует убедиться в наличии маршрута к получателю, так как эта проверка выполняется до преобразования. Дополнительные сведения см. в документе Порядок работы протокола NAT.

Протокол NAT работает правильно, но проблемы при подключении остались

Если протокол NAT функционирует правильно, устранение неполадок с соединением следует начать со следующих действий:

- Проверьте возможность соединения на втором уровне.
- Проверьте данные маршрутизации на третьем уровне.
- Найдите те фильтры пакетов, которые могут быть причиной неполадок.

Заключение

Перечисленные выше проблемы показывают, что причиной неполадок IP-соединения не всегда является протокол NAT. В большинстве случаев, причина неполадок заключается не в протоколе NAT, и необходимо дальнейшее исследование. В данном документе содержится описание основных действий, которые необходимо предпринять для устранения неисправностей и проверки работы протокола NAT. Данные шаги включают следующее:

- Четко определите требуемые от протокола NAT действия.
- Убедитесь, что в таблице преобразований существуют нужные преобразования.

- Чтобы убедиться в том, что преобразование происходит, используйте команды **show** и **debug**.
- Подробно проверьте, что происходит с пакетом данных, и убедитесь, что у маршрутизаторов имеются правильные данные маршрутизации для пересылки пакета.

Дополнительные сведения

- [Страница поддержки протокола NAT](#)
- [Техническая поддержка – Cisco Systems](#)

© 1992-2010 Cisco Systems, Inc. Все права защищены.

Дата генерации PDF файла: Jan 05, 2010

<http://www.cisco.com/support/RU/customer/content/10/107600/13.shtml>
