

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ
БЕЛАРУСЬ**

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

ЕРМОЛАЕВА ЕКАТЕРИНА АЛЕКСАНДРОВНА

Настройка и проверка NAPT

Отчет по лабораторной работе № 13,

вариант 18

(“Компьютерные сети”)

студентки 2-го курса 14-ой группы

Преподаватель

Бубен И. В.

2021

СОДЕРЖАНИЕ

Шаг 1. Подсоединение устройств	3
Шаг 2. Настройка основной конфигурации маршрутизатора 2	3
Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза	4
Шаг 4. Настройка правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов	4
Шаг 5. Проверка работоспособности сети	5
Шаг 6. Создание маршрута по умолчанию	7
Шаг 7. Создание статического маршрута	8
Шаг 8. Определение пула используемых публичных IP-адресов	9
Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам	9
Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов	9
Шаг 11. Назначение интерфейсов	9
Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP	10
Шаг 13. Проверьте работоспособность NAT	10
Шаг 14. Краткий реферат по NAT и NAT	11

Вариант	Адреса для узлов	Маршрутизатор 1	Маршрутизатор 2	IP-адрес Loopback 1
18	10.162.140.0/24	176.141.0.1/30	176.141.0.2/30	172.16.1.18/32

Устройство	Имя узла	Маска подсети порта FastEthernet 0/0	Тип интерфейса	IP-адрес порта Serial 0/0	IP-адрес Loopback 1
Маршрутизатор 1	Gateway	10.162.140.0/24	DTE	176.141.0.1/30	
Маршрутизатор 2	ISP	нет	DCE	176.141.0.2/30	172.16.1.18/32
Коммутатор 1	Switch 1				

Шаг 1. Подсоединение устройств

- Подсоедините интерфейс Serial 0/0 маршрутизатора 1 к интерфейсу Serial 0/0 маршрутизатора 2 с помощью последовательного кабеля.
- Подсоедините интерфейс Fa0/0 маршрутизатора 1 к интерфейсу Fa0/1 коммутатора 1 с помощью прямого кабеля.
- Подсоедините оба узла к порту Fa0/2 и Fa0/3 коммутатора с помощью прямых кабелей.
- Как уже было принято, подписать устройства сети.

Шаг 2. Настройка основной конфигурации маршрутизатора 2

Задайте в настройках конфигурации маршрутизатора 2 имя узла (ISP), задайте IP-адреса для интерфейсов согласно вашему варианту задания. Сохраните конфигурацию.

Конфигурация последовательного интерфейса:

```
ISP(config)#interface serial0/0
ISP(config-if)#ip address 176.141.0.2 255.255.255.252
```

Конфигурация Loopback интерфейса:

```
ISP(config)#interface loopback 1
```

```
ISP(config-if)#
```

```
%LINK-5-CHANGED: Interface Loopback1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
```

```
ISP(config-if)#ip address 172.16.1.18 255.255.255.255
```

Сохранение конфигурации:

```
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза

Задайте в настройках основной конфигурации маршрутизатора 1 имя узла (Gateway), задайте IP-адреса для интерфейсов. Сохраните конфигурацию.

Конфигурация последовательного интерфейса:

```
Gateway(config)#interface serial0/0
Gateway(config-if)#ip address 176.141.0.1 255.255.255.252
```

Конфигурация интерфейса FastEthernet:

```
Gateway(config)#interface fa0/0
Gateway(config-if)#ip address 10.162.140.1 255.255.255.0
```

Сохранение конфигурации:

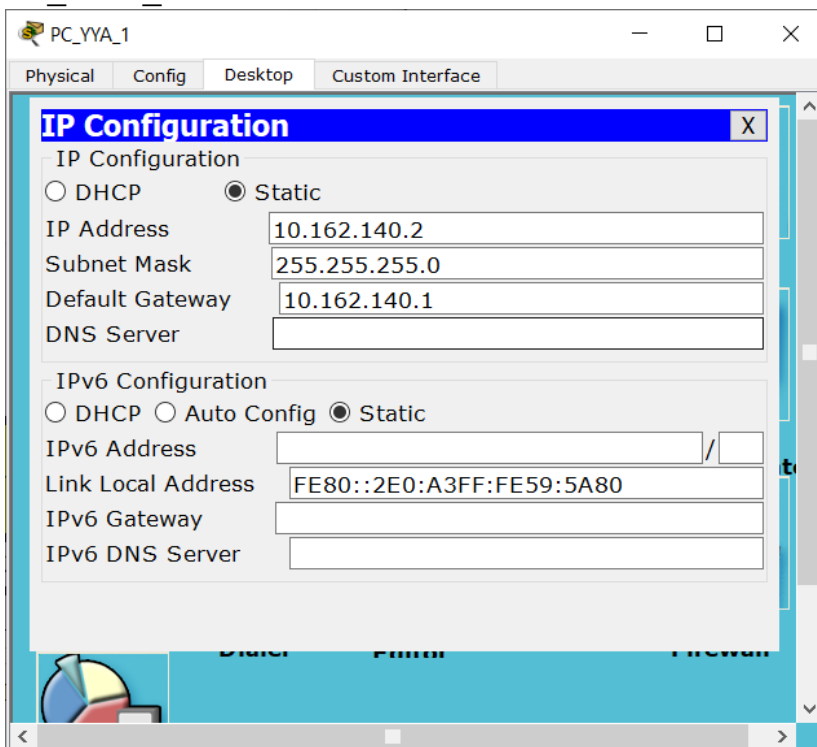
```
Gateway#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Шаг 4. Настройка правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов

Присвойте каждому узлу соответствующий IP-адрес, маску подсети и шлюз по умолчанию. Оба узла должны получить внутренние частные IP-адреса в сети 10.10.10.0/24 (вам необходимо задать адреса согласно вашему варианту задания). Шлюзом по умолчанию должен быть IP-адрес интерфейса FastEthernet маршрутизатора с именем Gateway.

Конфигурация узлов:

PC_YYA_1:



PC_YYA_2:

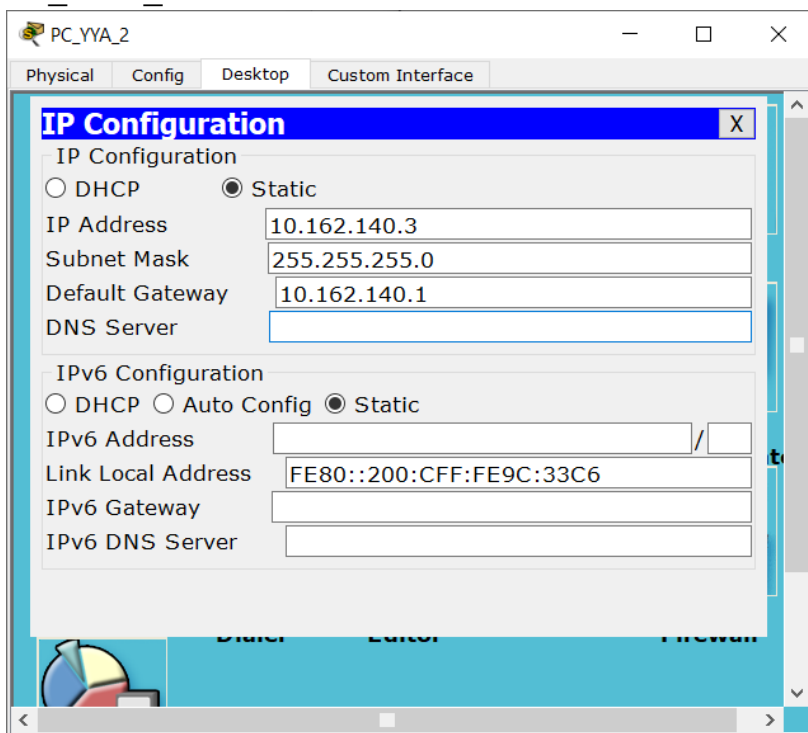
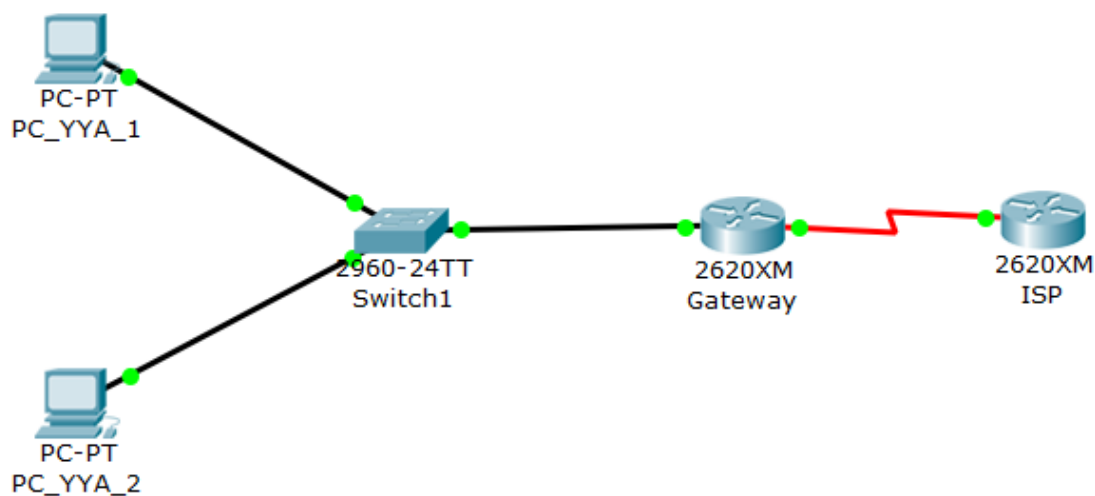


Схема построенной сети:



Шаг 5. Проверка работоспособности сети

1. С присоединенных узлов отправьте эхо-запрос на интерфейс FastEthernet маршрутизатора, используемого в качестве шлюза по умолчанию.

Ответьте на следующие вопросы.

а). Успешно ли выполнен эхо-запрос с узла 1? Да, успешно.

Результат отправки эхо-запроса с узла 1:

```
PC>ping 10.162.140.1

Pinging 10.162.140.1 with 32 bytes of data:

Reply from 10.162.140.1: bytes=32 time=13ms TTL=255
Reply from 10.162.140.1: bytes=32 time=0ms TTL=255
Reply from 10.162.140.1: bytes=32 time=0ms TTL=255
Reply from 10.162.140.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.162.140.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

b) Успешно ли выполнен эхо-запрос с узла 2? Да, успешно.

Результат отправки эхо-запроса с узла 2:

```
PC>ping 10.162.140.1

Pinging 10.162.140.1 with 32 bytes of data:

Reply from 10.162.140.1: bytes=32 time=0ms TTL=255
Reply from 10.162.140.1: bytes=32 time=0ms TTL=255
Reply from 10.162.140.1: bytes=32 time=0ms TTL=255
Reply from 10.162.140.1: bytes=32 time=0ms TTL=255

Ping statistics for 10.162.140.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Если ответы на оба вопроса отрицательны, выполните поиск и устранение ошибок в конфигурации маршрутизатора и узлов. Тестируйте соединение до тех пор, пока эхо-запросы не будут успешными.

3. Отправьте эхо-запросы на IP-адрес маршрутизатора ISP. Какой получили результат. Поясните свой ответ.

Результат отправки эхо-запросов:

```
PC>ping 176.141.0.2

Pinging 176.141.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 176.141.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 176.141.0.2

Pinging 176.141.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 176.141.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Можем увидеть, что эхо-запросы не были выполнены успешно, так как в таблице маршрутизации на ISP маршрутизаторе еще нет записи о маршруте до сети, в которой находятся узлы.

Шаг 6. Создание маршрута по умолчанию

- С маршрутизатора, использующегося в качестве шлюза по умолчанию, создайте статический маршрут к маршрутизатору поставщика услуг Интернета в сети 0.0.0.0 0.0.0.0 с помощью команды `ip route`. Это вызовет трафик к любому неизвестному адресу назначения через поставщика услуг Интернета путем настройки шлюза «последней надежды» на маршрутизаторе, использующемся в качестве шлюза по умолчанию.

Под шлюзом «последней надежды» подразумевается маршрут по умолчанию, т. е. шлюз, на который пересылаются все пакеты, адресованные в сети, конкретных маршрутов до которых нет в таблице маршрутизации. Настройка шлюза «последней надежды»:

```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 176.141.0.2
```

- Проверьте маршрут по умолчанию по таблице маршрутизации маршрутизатора Gateway. Находится ли статический маршрут в таблице маршрутизации?

Таблица маршрутизации маршрутизатора Gateway:

```
Gateway#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 176.141.0.2 to network 0.0.0.0

    10.0.0.0/24 is subnetted, 1 subnets
C      10.162.140.0 is directly connected, FastEthernet0/0
    176.141.0.0/30 is subnetted, 1 subnets
C      176.141.0.0 is directly connected, Serial0/0
S*    0.0.0.0/0 [1/0] via 176.141.0.2
```

Можем убедиться, что заданный статический маршрут появился в таблице маршрутизации.

- Попробуйте отправить эхо-запрос с одной с рабочих станций на IP-адрес последовательного интерфейса маршрутизатора поставщика услуг Интернета. Успешно ли выполнен эхо-запрос?

Результат отправки эхо-запроса:

```
PC>ping 176.141.0.2
```

```
Pinging 176.141.0.2 with 32 bytes of data:
```

```
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.
```

```
Ping statistics for 176.141.0.2:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Как видим, эхо-запрос вновь отправлен неуспешно, так как на ISP маршрутизаторе все еще нет записи о маршруте до сети, в которой находятся узлы. Т. е. запрос доходит до маршрутизатора, но он не может отослать узлу ответ.

Шаг 7. Создание статического маршрута

Создайте статический маршрут от маршрутизатора ISP к частной сети, присоединенной к маршрутизатору Gateway. Создайте статический маршрут с помощью команды ip route.

Настройка статического маршрута:

```
ISP(config)#ip route 10.162.140.0 255.255.255.0 176.141.0.1
```

- *Отправьте эхо-запрос с узла 1 на адрес интерфейса loopback маршрутизатора ISP. Успешно ли выполнен эхо-запрос?*

Результат отправки запроса:

```
PC>ping 172.16.1.18
```

```
Pinging 172.16.1.18 with 32 bytes of data:
```

```
Reply from 172.16.1.18: bytes=32 time=21ms TTL=254  
Reply from 172.16.1.18: bytes=32 time=4ms TTL=254  
Reply from 172.16.1.18: bytes=32 time=5ms TTL=254  
Reply from 172.16.1.18: bytes=32 time=6ms TTL=254
```

```
Ping statistics for 172.16.1.18:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 4ms, Maximum = 21ms, Average = 9ms
```

Как видим, эхо-запрос был выполнен успешно, так как теперь таблица маршрутизации маршрутизатора ISP содержит запись о маршруте до сети, в которой находятся узлы.

Таблица маршрутизации ISP маршрутизатора:


```
ISP#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

10.0.0.0/24 is subnetted, 1 subnets
S    10.162.140.0 [1/0] via 176.141.0.1
172.16.0.0/32 is subnetted, 1 subnets
C    172.16.1.18 is directly connected, Loopback1
176.141.0.0/30 is subnetted, 1 subnets
C    176.141.0.0 is directly connected, Serial0/0
```

- Если эхо-запрос не выполнен, проверьте правильность конфигурации маршрутизатора и узла и повторите тестирование связи.

Шаг 8. Определение пула используемых публичных IP-адресов

Для определения пула используемых публичных IP-адресов используйте команду `ip nat pool`.

Определение пула публичных адресов:

```
Gateway(config)#ip nat pool public_access 176.141.0.1 176.141.0.1
netmask 255.255.255.252
```

Публичные IP-адреса - это IP-адреса, доступные и используемые для адресации в глобальной внешней сети (Интернете).

Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам

Для определения списка доступа, соответствующего внутренним частным адресам используйте команду `access-list`.

Определение списка доступа:

```
Gateway(config)#access-list 1 permit 10.162.140.0 0.0.0.255
```

Частные IP-адреса - это IP-адреса, которые используются для адресации внутри частной сети.

Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов

Для определения NAT используйте команду `ip nat inside source`.

Определение NAT:

```
Gateway(config)#ip nat inside source list 1 pool public_access overload
```

Этой командой мы задаем правило динамической трансляции частных адресов на публичные (в нашем случае это все адреса частной сети 10.162.140.0/24 на один публичный адрес 176.141.0.1/30).

Шаг 11. Назначение интерфейсов

Активные интерфейсы маршрутизатора следует определить в качестве внутреннего или внешнего интерфейса в отношении к NAT. Для этого используйте команду `ip nat inside` или `ip nat outside`.

В отношении к NAT внутренним будет интерфейс, смотрящий в частную сеть, а внешним - интерфейс, смотрящий во внешнюю глобальную сеть. Определение последовательного интерфейса в качестве внешнего:

```
Gateway(config)#interface serial0/0
Gateway(config-if)#ip nat outside
```

Определение интерфейса FastEthernet в качестве внутреннего:

```
Gateway(config)#interface fastethernet0/0
Gateway(config-if)#ip nat inside
```

Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP

Отправьте эхо-запросы с узлов 1 и 2 на адрес 172.16.1.18.

Результат отправки эхо-запросов:

```
PC>ping 172.16.1.18
```

```
Pinging 172.16.1.18 with 32 bytes of data:
```

```
Reply from 172.16.1.18: bytes=32 time=26ms TTL=254
Reply from 172.16.1.18: bytes=32 time=1ms TTL=254
Reply from 172.16.1.18: bytes=32 time=1ms TTL=254
Reply from 172.16.1.18: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 172.16.1.18:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 26ms, Average = 7ms
```

```
PC>ping 172.16.1.18
```

```
Pinging 172.16.1.18 with 32 bytes of data:
```

```
Reply from 172.16.1.18: bytes=32 time=10ms TTL=254
Reply from 172.16.1.18: bytes=32 time=8ms TTL=254
Reply from 172.16.1.18: bytes=32 time=1ms TTL=254
Reply from 172.16.1.18: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 172.16.1.18:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 5ms
```

Оба запроса прошли успешно.

Шаг 13. Проверьте работоспособность NAPT

Для отображения статистики NAPT введите в приглашение привилегированного режима EXEC маршрутизатора Gateway команду `show ip nat statistics`. Проанализируйте полученную информацию и дайте ответ на следующие вопросы.

Результат выполнения команды *`show ip nat statistics`*:

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0
Inside Interfaces: FastEthernet0/0
Hits: 8 Misses: 8
Expired translations: 8
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.252
   start 176.141.0.1 end 176.141.0.1
   type generic, total addresses 1 , allocated 0 (0%), misses 0
```

1. Сколько активных преобразований выполнено?

0 преобразований

```
Total translations: 0 (0 static, 0 dynamic, 0 extended)
```

2. Сколько адресов имеется в пуле?

1 адрес

```
total addresses 1
```

3. Сколько адресов уже выделено?

0 адресов

```
allocated 0 (0%)
```

Если эхо-запрос выполнен успешно, отобразите преобразование NAT на маршрутизаторе Gateway с помощью команды show ip nat translations.

Выполнение эхо-запроса от PC_YYA_1 на адрес 172.16.1.18:

```
PC>ping 172.16.1.18
```

```
Pinging 172.16.1.18 with 32 bytes of data:
```

```
Reply from 172.16.1.18: bytes=32 time=2ms TTL=254
Reply from 172.16.1.18: bytes=32 time=3ms TTL=254
Reply from 172.16.1.18: bytes=32 time=5ms TTL=254
Reply from 172.16.1.18: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 172.16.1.18:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

Он выполнен успешно. Результат выполнения команды **show ip nat translations**:

```
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 176.141.0.1:25     10.162.140.2:25   172.16.1.18:25     172.16.1.18:25
icmp 176.141.0.1:26     10.162.140.2:26   172.16.1.18:26     172.16.1.18:26
icmp 176.141.0.1:27     10.162.140.2:27   172.16.1.18:27     172.16.1.18:27
icmp 176.141.0.1:28     10.162.140.2:28   172.16.1.18:28     172.16.1.18:28
```

Как видим, частный адрес 10.162.140.2 был транслирован на публичный адрес 176.141.0.1. Значит, трансляция адресов настроена верно.

Шаг 14. Краткий реферат по NAT и NAPT

Преобразование сетевых адресов (Network Address Translation - NAT) - это процесс, который изменяет IP-адрес в заголовке IP-пакета, когда он проходит через устройство маршрутизации. Преобразование адресов методом NAT

может производиться почти любым маршрутизирующим устройством (маршрутизатором, сервером доступа, межсетевым экраном). NAT позволяет использовать один набор IP-адресов для трафика в локальной сети, а другой набор IP-адресов - для внешнего трафика. Одной из главных причин использования технологии NAT является дефицит IP-адресов. Использование NAT решает эту проблему, поскольку частные IP-адреса используются внутри автономной сети, и это не вызывает конфликтов с IP-адресами, используемыми в других не связанных с ней сетях. Также использование NAT повышает безопасность локальной сети, поскольку предоставляет возможность скрыть внутренние IP-адреса и не дать возможности злоумышленникам составить представление о структуре и масштабах корпоративной сети, а также о структуре и интенсивности исходящего и входящего трафика.

Идея технологии NAT состоит в следующем. Пусть сеть предприятия образует тупиковый домен, узлам которого присвоены частные адреса. На маршрутизаторе, связывающем сеть предприятия с внешней сетью, установлено программное обеспечение NAT. Это NAT-устройство динамически отображает набор частных адресов $\{IP^*\}$ на набор глобальных адресов $\{IP\}$, полученных предприятием от поставщика услуг и присвоенных внешнему интерфейсу маршрутизатора предприятия.

Традиционная технология NAT подразделяется на Basic NAT (технология базовой трансляции сетевых адресов, использующая для отображения только IP-адреса) и NAT (технология трансляции сетевых адресов и портов, использующая в дополнение к IP-адресам еще и так называемые транспортные идентификаторы, в качестве которых чаще всего выступают TCP-и UDP-порты). Трансляция адресов может осуществляться статически или динамически. В первом случае частный IP-адрес отдельного узла всегда преобразуется в один и тот же глобальный адрес. Также благодаря этому этот глобальный адрес никогда не получит другой локальный узел. При динамическом преобразовании NAT-устройство транслирует частные адреса на адреса из заданного доступного пула внешних глобальных адресов.