

смотрим мужика

<https://www.youtube.com/watch?v=L1JtmAiSaFQ>

NAT (Network Address Translation) - трансляция сетевых адресов - технология замены ip адресов и портов в заголовке ip пакетов.

NAT (Network Address Translation) – трансляция сетевых адресов

Технология преобразования IP-адресов внутренней (частной) сети в IP-адреса внешней сети (Интернет)

Цель создания – преодоление нехватки адресов IPv4

Внешние и внутренние IP-адреса

Внешние IP-адреса

- Применяются в сети Интернет
- Должны быть уникальными
- Распределяются ICANN
- Адресов IPv4 не хватает для всех устройств в Интернет (количество адресов IPv4 примерно 4 млрд.)

Внутренние IP-адреса

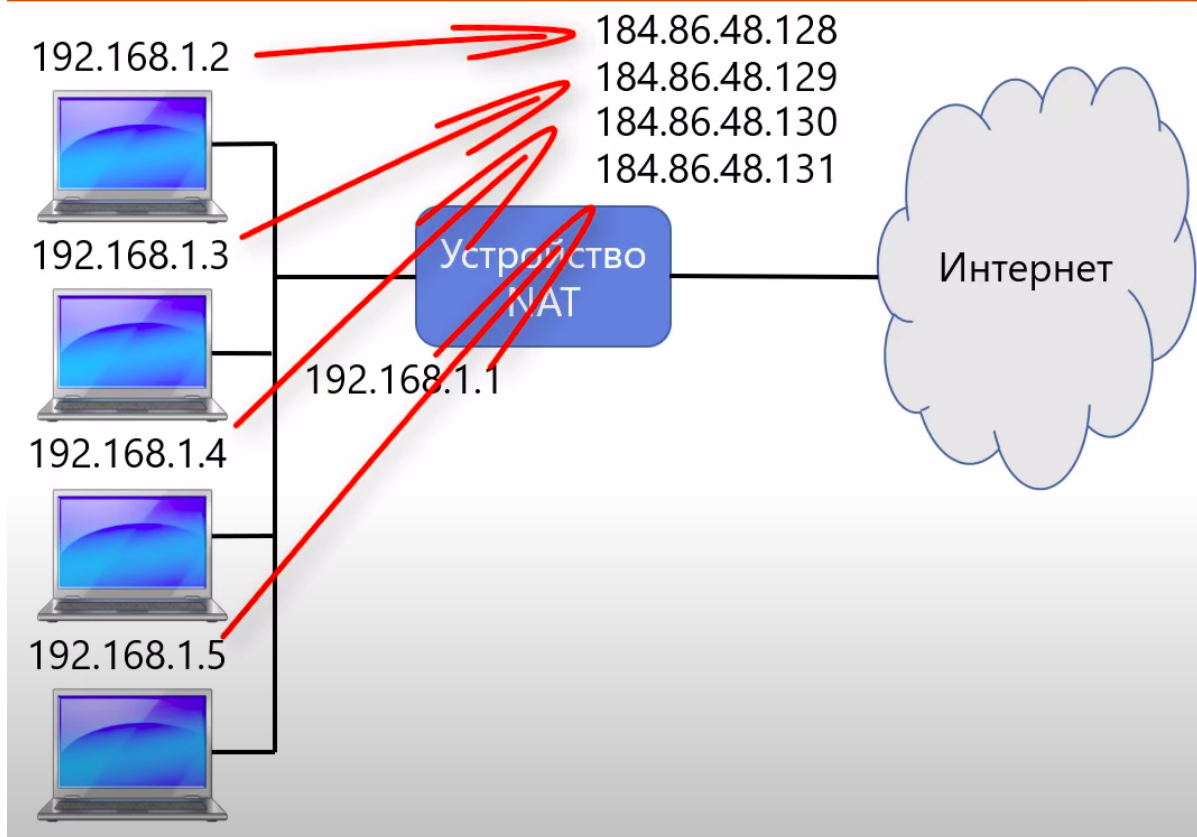
- Диапазон частных сетей (RFC 1918): 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Не маршрутизируются в Интернет
- Могут использоваться без обращения в ICANN
- Допускается использование одинаковых адресов в разных сетях (т.к. они не будут видны в Интернет)

Типы NAT

Статический: отображение один к одному

В этом случае нужно иметь столько же адресов, сколько и компов во внутренней сети.

Статический NAT

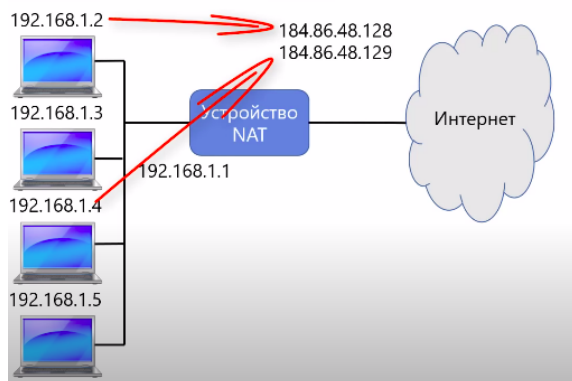


Получается, что у нас фиксированное отображение внутренних ip-адресов во внешние.

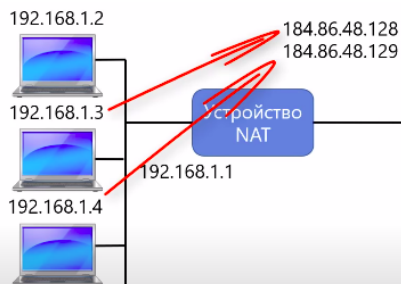
Динамический: отображение внутренних адресов на группу внешних адресов

У нас есть несколько внешних ip-адресов, которые поочередно используются разными компьютерами из внутренней сети.

Динамический NAT



Например, этот и этот комп используют эти адреса. Через некоторое время этот комп использует этот адрес, этот комп - этот (дадада)



Один ко многим (masquerading): отображение внутренних адресов на один внешний адрес

Преобразование выполняется с помощью таблицы NAT

Использует комбинацию IP-адрес + порт

Вид таблицы NAT

Внутренний IP	Внутренний порт	Внешний IP	Внешний порт
192.168.1.2	50300	184.86.48.128	49127
192.168.1.3	52001	184.86.48.128	49128
192.168.1.2	49238	184.86.48.128	49129

Пример.

Пусть комп с ip 192.168.1.2 решил зайти на сайт www.asozykin.ru. Он отправляет пакет, в котором в адресе отправителя указывается ip адрес компа из внутренней сети. В поле "порт" указывается динамический порт, выданный браузеру ОС.

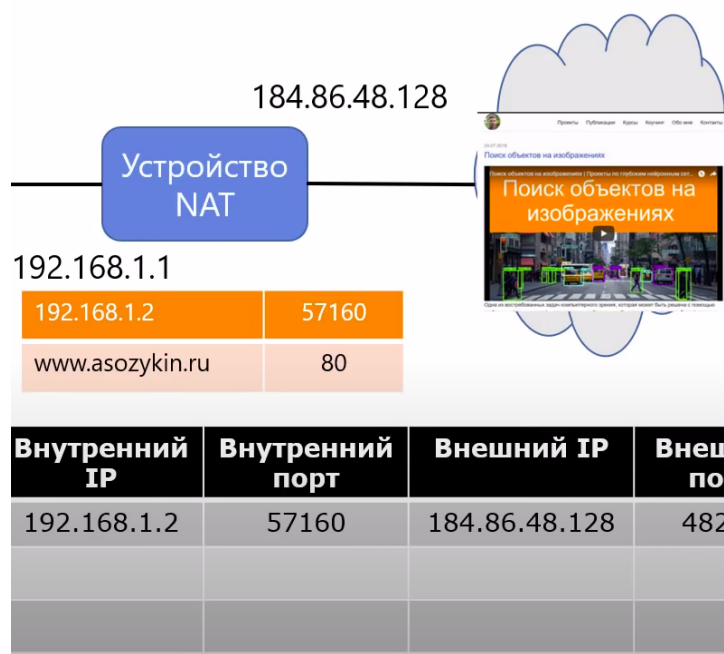
192.168.1.1

192.168.1.2	57160
www.asozykin.ru	80

Пакет предназначен для 80-го порта адреса веб-сайта.

Но! Т.к. адреса из внутренней сети не могут использоваться в Интернете, то устройству nat нужно заменить ip-адрес из внутренней сети в заголовке пакета в адресе отправителя на ip адрес из внешней сети.

Как это делает устройство nat?



После того, как устройство nat получило пакет, оно записывает внутренний ip-адрес и внутренний порт в таблицу nat и генерирует пару "внешний ip адрес и внешний порт" для замены в пакете. Т.к у нас только 1 внешний ip адрес, то именно он записывается в поле "внешний ip". Данные в поле "внешний порт" генерируется случайно.

Преимущества и недостатки nat

Преимущества NAT:

- Позволяет преодолеть нехватку адресов IPv4
- Легко развернуть и использовать
- Скрывает структуру сети от внешнего мира

Недостатки NAT:

- Нарушение фундаментального принципа построения IP-сетей: каждый компьютер может соединиться с любым другим
- Нет возможности подключиться к компьютерам во внутренней сети из внешнего мира
- Плохо работают протоколы не устанавливающие соединения
- Некоторые прикладные протоколы работают неправильно (FTP)
- Нет единого стандарта NAT, много разных вариантов

Решение проблем с nat

Решение проблем с NAT

Статическое отображение IP-адресов:

- Внутренний IP ↔ Внешний IP
- Требуется несколько внешних IP-адресов

Статическое отображение портов:

- Порт 80 → Внутренний адрес Web-сервера и порт 80
- Порт 25 → Внутренний адрес почтового сервера и порт 25
- Порт 21 → Внутренний адрес FTP сервера и порт 21

Технология NAT Traversal:

- Позволяет устанавливать соединение с компьютерами во внутренней сети
- RFC 3489 и другие варианты

→ Используется VoIP приложениями (Skype)

Итоги

Трансляция сетевых адресов (NAT)

- Преобразование IP-адресов внутренней (частной) сети в IP-адреса внешней сети (Интернет)
- Реализуется на маршрутизаторах, межсетевых экранах и др.

Преимущества

- Частично решает проблему нехватки адресов IPv4
- Легко развернуть и использовать
- Повышает безопасность внутренней сети

Недостатки

- Нет возможности подключиться из Интернет к компьютерам во внутренней сети
- Плохо работают многие сетевые протоколы (FTP, Skype и т.п.)

Configuring Static NAT

```
R1>
R1>
R1>
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip nat ?
    inside    Inside address translation
    outside   Outside address translation
    pool       Define pool of addresses
R1(config)#ip nat inside ?
    source    Source address translation
R1(config)#ip nat inside s
R1(config)#ip nat inside source ?
    list      Specify access list describing local addresses
    static    Specify static local->global mapping
R1(config)#ip nat inside source s
R1(config)#ip nat inside source static ?
    A.B.C.D   Inside local IP address
    tcp       Transmission Control Protocol
    udp       User Datagram Protocol
R1(config)#ip nat inside source static 172.16.16.1 ?
    A.B.C.D   Inside global IP address
R1(config)#ip nat inside source static 172.16.16.1 64.100.50.1 ?
    <cr>
R1(config)#ip nat inside source static 172.16.16.1 64.100.50.1
R1(config)#inter
R1(config)#interface Se
R1(config)#interface Serial0/0/0
R1(config-if)#ip nat out
R1(config-if)#ip nat outside
R1(config-if)#ex
R1(config)#inter
R1(config)#interface G
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip nat in
R1(config-if)#ip nat inside
R1(config-if)#ex
R1(config)#|
```

То есть настраиваем одной командой

```
R1(config)#ip nat inside source static 172.16.16.1 64.100.50.1
```

А затем интерфейсы настраиваем как на фотке.

Про статический нат:

- <https://www.practicalnetworking.net/series/nat/static-nat/>
- <https://linkmeup.gitbook.io/sdsm/5.-acl-i-nat/01-nat>

Configuring Dynamic NAT

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip ac
R2(config)#ip access-list ?
    extended  Extended Access List
    standard  Standard Access List
R2(config)#ac
R2(config)#access-list ?
    <1-99>      IP standard access list
    <100-199>   IP extended access list
R2(config)#access-list 1 ?
    deny       Specify packets to reject
    permit     Specify packets to forward
    remark     Access list entry comment
R2(config)#access-list 1 per
R2(config)#access-list 1 permit ?
    A.B.C.D    Address to match
    any        Any source host
    host       A single host address
R2(config)#access-list 1 permit 172.16.0.0 ?
    A.B.C.D    Wildcard bits
    <cr>
R2(config)#access-list 1 permit 172.16.0.0 0.0.255.255 ?
    <cr>
R2(config)#access-list 1 permit 172.16.0.0 0.0.255.255
R2(config)#ip nat ?
    inside     Inside address translation
    outside    Outside address translation
    pool       Define pool of addresses
R2(config)#ip nat pool ?
    WORD       Pool name
R2(config)#ip nat pool POOL ?
    A.B.C.D    Start IP address
R2(config)#ip nat pool POOL 209.165.76.196 209.165.76.199 ?
    netmask    Specify the network mask
R2(config)#ip nat pool POOL 209.165.76.196 209.165.76.199 n
R2(config)#ip nat pool POOL 209.165.76.196 209.165.76.199 netmask 255.255.255.252
R2(config)#|
```

```
R2(config)#inter
R2(config)#interface Serial0/0/0
R2(config-if)#ip nat pu
R2(config-if)#ip nat ou
R2(config-if)#ip nat outside
R2(config-if)#ex
R2(config)#interface S
R2(config)#interface Serial0/0/1
R2(config-if)#ip nat ins
R2(config-if)#ip nat inside
R2(config-if)#ex
R2(config)#|
```

Про динамический нат:

- <https://study-ccna.com/dynamic-nat/>
- <https://habr.com/ru/articles/131712/> про wildcards
- <https://geckich.blogspot.com/2011/12/wildcard-mask.html> wildcards + calc

Configuring Port Forwarding on a Wireless Router

Всё по инструкции как написано.

Почитать вот [это](#).

Проброс портов обычно используется для того, чтобы получить доступ к информации и данным на другом устройстве, которое подключено к той же сети по Wi-Fi-роутеру.

Для каких целей используется переадресация портов? Допустим, вы хотите подсоединиться к компьютеру, который транслирует видеосигнал, чтобы смотреть транслируемое видео или создаёте сервер для общей игры в Интернете. В некоторых случаях нужно открыть доступ к ПК, если вы хотите обмениваться трафиком через торрент-приложения.

Verifying and Troubleshooting NAT Configurations

Port Status Summary Table for R2
Device Name: R2
Device Model: 2911
Hostname: R2

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Down	--	<not set>	<not set>	0002.1685.9501
GigabitEthernet0/1	Down	--	<not set>	<not set>	0002.1685.9502
GigabitEthernet0/2	Down	--	<not set>	<not set>	0002.1685.9503
Serial0/0/0	Up	--	209.165.76.194/27	<not set>	<not set>
Serial0/0/1	Up	--	10.4.1.1/30	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0040.0825.CD65

R2
Physical Config CLI Attributes
IOS Command Line Interface

```

route      IP routing table
ssh        Information on SSH
R2#show ip nat
% Incomplete command.
R2#show ip nat?
nat
R2#show ip nat
% Incomplete command.
R2#show ip nat?
nat
R2#show ip nat ?
statistics Translation statistics
translations Translation entries
R2#show ip nat st
R2#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside interfaces: Serial0/0/0
Inside interfaces: Serial0/0/1
Hits: 0 Misses: 4
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 101 pool R2POOL refCount 0
pool R2POOL: netmask 255.255.255.224
start 209.165.76.195 end 209.165.76.223
type generic, total addresses 29 , allocated 0 (0%), misses 0
R2#

```

перенастроим интерфейсы

```

R2(config)#inter
R2(config)#interface Ser
R2(config)#interface Serial0/0/0
R2(config-if)#ip nat ou
R2(config-if)#ip nat outside
R2(config-if)#ex
R2(config)#interface ser
R2(config)#interface serial0/0/1
R2(config-if)#ip nat ins
R2(config-if)#ip nat inside

```

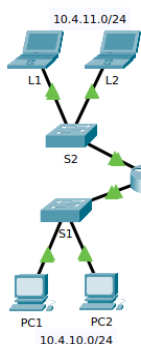
Посмотрим сюда

```

R2#show access-lists
Extended IP access list 101
  10 permit ip 10.4.10.0 0.0.0.255 any (2 match(es))

```

и на компы



Первые 2 числа меняются, а последние 2 - нет. А в выводе команды в wild card bits не меняются первые 3 числа- что неверно. Поэтому надо удалить этот access list и написать новый нормальный.

```
R2(config)#access-list ?
<1-99>      IP standard access list
<100-199>   IP extended access list
R2(config)#access-list 101 ?
deny        Specify packets to reject
permit      Specify packets to forward
remark      Access list entry comment
R2(config)#access-list 101 p
R2(config)#access-list 101 permit ?
ahp         Authentication Header Protocol
eigrp       Cisco's EIGRP routing protocol
esp         Encapsulation Security Payload
gre         Cisco's GRE tunneling
icmp        Internet Control Message Protocol
ip          Any Internet Protocol
ospf        OSPF routing protocol
tcp         Transmission Control Protocol
udp         User Datagram Protocol
R2(config)#access-list 101 permit ip ?
A.B.C.D     Source address
any         Any source host
host        A single source host
R2(config)#access-list 101 permit ip ?
A.B.C.D     Source address
any         Any source host
host        A single source host
R2(config)#access-list 101 permit ip 10.4.10.0 0.0.1.255 ?
A.B.C.D     Destination address
any         Any destination host
host        A single destination host
R2(config)#access-list 101 permit ip 10.4.10.0 0.0.1.255 any ?
dscp        Match packets with given dscp value
precedence  Match packets with given precedence value
<cr>
R2(config)#access-list 101 permit ip 10.4.10.0 0.0.1.255 any |
```

Implementing Static and Dynamic NAT

Настроим

```
R2>
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip ac
R2(config)#ip access-list ?
    extended  Extended Access List
    standard  Standard Access List
R2(config)#ip access-list s
R2(config)#ip access-list standard ?
    <1-99>    Standard IP access-list number
    WORD      Access-list name
R2(config)#ip access-list standard R2NAT ?
    <cr>
R2(config)#ip access-list standard R2NAT |
```

```
R2(config)#ip access-list ?
    extended  Extended Access List
    standard  Standard Access List
R2(config)#ip access-list s
R2(config)#ip access-list standard ?
    <1-99>    Standard IP access-list number
    WORD      Access-list name
R2(config)#ip access-list standard R2NAT ?
    <cr>
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)#?
    <1-2147483647> Sequence Number
    default        Set a command to its defaults
    deny           Specify packets to reject
    exit           Exit from access-list configuration
    no             Negate a command or set its default
    permit         Specify packets to forward
    remark         Access list entry comment
R2(config-std-nacl)#pr
R2(config-std-nacl)#pe
R2(config-std-nacl)#permit 192.168.10.0 ?
    A.B.C.D  Wildcard bits
    <cr>
R2(config-std-nacl)#permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
R2(config-std-nacl)#|
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat ?
    inside    Inside address translation
    outside   Outside address translation
    pool       Define pool of addresses
R2(config)#ip nat pool R2POOL ?
    A.B.C.D    Start IP address
R2(config)#ip nat pool R2POOL 209.165.202.129 209.165.202.129 ?
    netmask    Specify the network mask
R2(config)#ip nat pool R2POOL 209.165.202.129 209.165.202.129 net
R2(config)#ip nat pool R2POOL 209.165.202.129 209.165.202.129 netmask
255.255.255.252 ?
    <cr>
R2(config)#ip nat pool R2POOL 209.165.202.129 209.165.202.129 netmask
255.255.255.252
R2(config)#
```

```
IOS Command Line Interface

pool      Define pool of addresses
R2(config)#ip nat in
R2(config)#ip nat inside ?
    source Source address translation
R2(config)#ip nat inside so
R2(config)#ip nat inside source ?
    list Specify access list describing local addresses
    static Specify static local->global mapping
R2(config)#ip nat inside source 1
R2(config)#ip nat inside source list ?
    <1-199> Access list number for local addresses
    WORD Access list name for local addresses
R2(config)#ip nat inside source list R2NAT ?
    interface Specify interface for global address
    pool Name pool of global addresses
R2(config)#ip nat inside source list R2NAT int
R2(config)#ip nat inside source list R2NAT p
R2(config)#ip nat inside source list R2NAT pool ?
    WORD Name pool of global addresses
R2(config)#ip nat inside source list R2NAT pool R2POOL ?
    overload Overload an address translation
    <cr>
R2(config)#ip nat inside source list R2NAT pool R2POOL o
R2(config)#ip nat inside source list R2NAT pool R2POOL overload ?
    <cr>
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
R2(config)#
```

Copy Paste

теперь настроим интерфейсы

```
R2(config)#inter
R2(config)#interface Serial0/1/0
R2(config-if)#ip nat o
R2(config-if)#ip nat outside
R2(config-if)#ex
R2(config)#int
R2(config)#interface F
R2(config)#interface FastEthernet0/0
R2(config-if)#ip nat o
R2(config-if)#ip nat outside
R2(config-if)#ex
R2(config)#interface Ser
R2(config)#interface Serial0/0/0
R2(config-if)#ip nat in
R2(config-if)#ip nat inside
R2(config-if)#ex
R2(config)#interface Serial0/0/1
R2(config-if)#ip nat un
R2(config-if)#ip nat in
R2(config-if)#ip nat inside
R2(config-if)#ex
```


На маршрутизаторе R2 настройте стандартный ACL-список с именем R2NAT, который использует 3 правила, разрешающих в указанном порядке пр

создадим статическое преобразование

```
R2(config)#ip nat in
R2(config)#ip nat inside sou
R2(config)#ip nat inside source st
R2(config)#ip nat inside source static 192.168.20.254 ?
    A.B.C.D  Inside global IP address
R2(config)#ip nat inside source static 192.168.20.254
209.165.202.130 ?
    <cr>
R2(config)#ip nat inside source static 192.168.20.254
209.165.202.130
R2(config)#
```

```
R2#show ip nat s
R2#show ip nat statistics
Total translations: 12 (1 static, 11 dynamic, 11 extended)
Outside Interfaces: FastEthernet0/0 , Serial0/1/0
Inside Interfaces: Serial0/0/0 , Serial0/0/1
Hits: 101  Misses: 103
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list R2NAT pool R2POOL refCount 4
pool R2POOL: netmask 255.255.255.252
start 209.165.202.129 end 209.165.202.129
type generic, total addresses 1 , allocated 1 (100%),
misses 0
/// R2#
Fastethernet0/0 определен не верно
переделаем
```

```
R2#show ip nat s
R2#show ip nat statistics
Total translations: 12 (1 static, 11 dynamic, 11 extended)
Outside Interfaces: FastEthernet0/0 , Serial0/1/0
Inside Interfaces: Serial0/0/0 , Serial0/0/1
Hits: 101  Misses: 103
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list R2NAT pool R2POOL refCount 4
pool R2POOL: netmask 255.255.255.252
start 209.165.202.129 end 209.165.202.129
type generic, total addresses 1 , allocated 1 (100%),
misses 0
R2#
```

Полезные ссылки

- <https://linkmeup.gitbook.io/sdsm/5.-acl-i-nat/01-nat>
- <https://habr.com/ru/articles/121806/> про acl-листы