

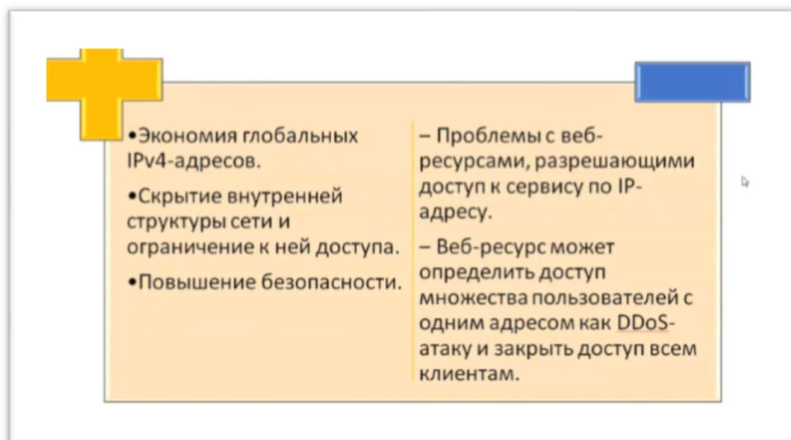
ТРАНСЛЯЦИЯ СЕТЕВЫХ АДРЕСОВ

1. Определение и назначение технологии NAT. Типы адресов в NAT.

NAT (Network Address Translation) - трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах. NAT используется чаще всего для осуществления доступа устройств из корпоративной (частной) сети в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети. Для преобразования частных адресов в глобальные (маршрутизируемые в Интернете) применяют NAT.

Помимо возможности доступа в глобальную сеть Интернет, NAT имеет ещё несколько положительных сторон. Так, например, трансляция сетевых адресов позволяет скрыть внутреннюю структуру сети и ограничить к ней доступ, что повышает безопасность. Также эта технология позволяет экономить глобальные IPv4-адреса, так как под одним глобальным адресом в Интернет может выходить множество устройств.

Технология NAT обеспечивает преобразование частных адресов в публичные. Это позволяет устройству с частным IPv4-адресом получать доступ к ресурсам за пределами корпоративной сети. NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных адресов IPv4. Один общедоступный IPv4-адрес может использоваться сотнями и тысячами устройствами, каждое из которых имеет уникальный частный IPv4-адресс.



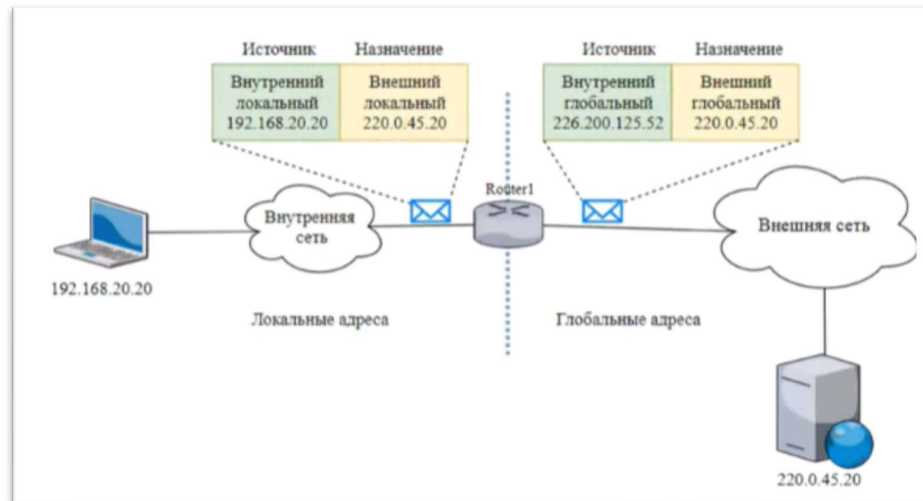
<ul style="list-style-type: none">• Экономия глобальных IPv4-адресов.• Скрытие внутренней структуры сети и ограничение к ней доступа.• Повышение безопасности.	<ul style="list-style-type: none">– Проблемы с веб-ресурсами, разрешающими доступ к сервису по IP-адресу.– Веб-ресурс может определить доступ множества пользователей с одним адресом как DDoS-атаку и закрыть доступ всем клиентам.
--	---

Терминология NAT

- **Внутренняя сеть** – это набор сетей, IP-адреса которых подлежат трансляции. **Внешняя сеть** относится ко всем другим сетям.

Типы адресов в технологии NAT.

- **внутренний локальный адрес** – адрес устройства, который транслируется с помощью NAT;
- **внутренний глобальный адрес** – адрес, полученный в результате трансляции NAT;
- **внешний локальный адрес** – адрес устройства во внешней сети до трансляции NAT;
- **внешний глобальный адрес** – это адрес устройства во внешней сети.



2. Различия в видах трансляции IP-адресов.

Виды трансляции

- **Static NAT (статический NAT)** – преобразование IP-адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети;
- **Dynamic NAT (динамический NAT)** – преобразование внутреннего адреса/ов в один из группы внешних адресов;
- **Port Address Translation (PAT)** или Overloading – преобразование несколько внутренних адресов в один внешний.

При статическом NAT после отправки сообщения с устройства внутренней сети маршрутизатор преобразует внутренний локальный адрес во внутренний глобальный адрес. Статический NAT особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес, доступный из глобальной сети. Также статический NAT может применяться для устройств, которые должны быть доступны для авторизованного персонала вне сети, например, доступ по SSH к настройкам сетевого оборудования. Основное требование при использовании статического NAT - доступность достаточного количества адресов.

Динамический NAT использует пул публичных адресов и назначает их в порядке очереди. Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT назначает доступный общедоступный IPv4-адрес из пула.

PAT иногда называется Overloading сопоставляет несколько частных адресов IPv4 с одним общедоступным адресом IPv4. В большинстве случаев домашние маршрутизаторы используют именно эту технологию трансляции IPv4-адресов. Интернет-провайдер назначает маршрутизатору один адрес, но несколько устройств, подключенных к одному домашнему маршрутизатору, могут одновременно иметь доступ к Интернету.

3. Последовательность действий и пример конфигурации статического NAT. Способы проверки конфигурации NAT

Для конфигурации статического NAT необходимо выполнить следующие действия:

- 1) спланировать сопоставление внутренних локальных IPv4-адресов и внутренних глобальных;

Наименование устройства	Внутренний локальный адрес	Внутренний глобальный адрес
ЮТ0	172.20.0.114	122.20.0.19
ЮТ4	172.20.0.130	122.20.0.20
ЮТ6	172.20.0.146	122.20.0.21

- 2) осуществить конфигурацию статического NAT с помощью команды
`ip nat inside source static Внутренний_локальный_адрес`
`Внутренний_глобальный_адрес;`

```
Router3(config)#ip nat inside source static 172.20.0.114 122.20.0.19
```

```
Router3(config)# ip nat inside source static 172.20.0.130 122.20.0.20
```

```
Router3(config)# ip nat inside source static 172.20.0.146 122.20.0.21
```

```
Router3(config)#ip nat inside source static 172.20.0.147 122.20.0.21
```

- 3) определить какие интерфейсы маршрутизатора относятся к внутренней сети; осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внутренней сети с помощью команды `ip nat inside`; определить какие интерфейсы маршрутизатора относятся к внешней сети;осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внешней сети с помощью команды `ip nat outside`.

```
Router3(config)#interface Port-channel2
Router3(config-if)#ip nat outside
Router3(config-if)#interface GigabitEthernet0/0/0
Router3(config-if)#ip nat outside
Router3(config-if)#interface GigabitEthernet0/0.404
Router3(config-subif)#ip nat inside
Router3(config-subif)#interface GigabitEthernet0/0.405
Router3(config-subif)#ip nat inside
```

Дополнение:

Отличия inside и outside

• `ip nat inside ...`:

- Транслирует **source IP address** в пакете, который направляется из внутренней сети (**inside**) во внешнюю (**outside**).
- Транслирует **destination IP address** в пакете, который направляется из внешней сети (**outside**) во внутреннюю (**inside**).

• `ip nat outside ...`:

- Транслирует **source IP address** в пакете, который направляется из внешней сети (**outside**) во внутреннюю (**inside**).
- Транслирует **destination IP address** в пакете, который направляется из внутренней сети (**inside**) во внешнюю (**outside**).

- 4)изменение конфигурации маршрутизатора

```
Router3(config-router)#no network 172.20.0.112 0.0.0.15 area 1
```

```
Router3(config-router)#no network 172.20.0.128 0.0.0.15 area 1
```

```
Router3(config-router)#no network 172.20.0.144 0.0.0.15 area 1
```

```
Router3(config-router)# network 122.20.0.56 0.0.0.3 area 1
```

```
Router3(config-router)# network 122.20.0.16 0.0.0.15 area 1
```

```
Router3(config-router)# network 122.20.0.68 0.0.0.3 area 1
```

Проверка конфигурации NAT:

- `show ip nat translations`
- `show ip nat statistics`

4. Последовательность действий и пример конфигурации динамического NAT

Для конфигурации динамического NAT необходимо выполнить следующие действия.

1. Определить пул адресов, которые будут использоваться для трансляции, помощью команды

ip nat pool имя_пула начальный_IP-адрес конечный_IP-адрес netmask маска_подсети.

• Пример 1

```
Router1(config)#ip nat pool NATadmin 122.20.0.3 122.20.0.14  
netmask 255.255.255.240
```

• Пример 2

```
Router1(config)#ip nat pool NAT1 122.20.0.34 122.20.0.46 netmask  
255.255.255.240
```

2. Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды *access-list номерACL permit IPадрес внутренней_сети обратная_маска внутренней_сети*

```
Router1(config)#access-list 15 permit 172.20.0.0 0.0.0.15
```

```
Router1(config)#access-list 15 permit 172.20.0.16 0.0.0.153
```

3. Установить связь созданного ACL с пулом с помощью команды

ip nat inside source list номер_ACL pool имя_пула. Эта конфигурация используется маршрутизатором для определения того, какие устройства (номер ACL) получают, какие адреса (имя пула).

```
Router1(config)#ip nat inside source list 15 pool NAT1
```

4. Определить какие интерфейсы маршрутизатора относятся к внутренней сети, на интерфейсах с указанием их подключения к внутренней сети с помощью *ip nat inside*. И какие относятся к внешней сети с помощью команды *ip nat outside*.

```
Router1(config)#interface GigabitEthernet0/0/0
```

```
Router1(config-if)#ip nat outside
```

```
Router1(config)#interface GigabitEthernet0/1.7
```

```
Router1(config-if)#ip nat inside
```

*Для очистки динамических записей NAT используется команда режима *clear ip nat translation*

5. Изменение конфигурации маршрутизации

```
Router1(config)#interface GigabitEthernet0/1.100
```

```
Router1(config-subif)#encapsulation dot1Q 100
```

```
Router1(config-subif)#ip address 122.20.0.33 255.255.255.240
```

```
Router1(config)#router ospf 111
```

```
Router1(config-router)#no network 172.20.0.0 0.0.0.15 area 1
```

```
Router1(config-router)#no network 172.20.0.16 0.0.0.15 area 1
```

```
Router1(config-router)#no network 172.20.0.32 0.0.0.15 area 1
```

```
Router1(config-router)#network 122.20.0.0 0.0.0.15 area 1
```

```
Router1(config-router)#network 122.20.0.32 0.0.0.15 area 1
```

```
Router1(config-router)#network 122.20.0.60 0.0.0.3 area 1
```

```
Router1(config-router)#network 122.20.0.64 0.0.0.3 area 1
```

Проверка конфигурации NAT:

– show ip nat translations

- Sh ip nat statistics

Отключение функции демонстрации процесса преобразования на маршрутизаторе

- Debug ip nat

5. Последовательность действий и пример конфигурации РАТ для диапазона публичных IP-адресов. = (динамический)

1. Определить пул глобальных адресов, которые будут использоваться для трансляции, с помощью команды

ip nat pool имя_пула начальный_IP-адрес конечный_IP-адрес netmask маска_подсети.

```
Router2(config)#ip nat pool NAT1 122.20.0.73 122.20.0.74 netmask  
255.255.255.252
```

2. Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды *access-list номерACL permit IPадрес внутренней сети обратная маска внутренней сети*.

```
Router2(config)#access-list 14 permit 172.20.0.96 0.0.0.15
```

3. Установить связь созданного ACL с пулом и типом NAT с помощью команды *ip nat inside source list номер_ACL pool имя_пула overload*.

```
Router2(config)#ip nat inside source list 14 pool NAT1 overload
```

4. Определить какие интерфейсы маршрутизатора относятся к внутренней сети – *ip nat inside*. к внешней сети с помощью команды *ip nat outside*

```
Router2(config)# interface GigabitEthernet0/0.401
```

```
Router2(config-if)# ip nat inside
```

```
Router2(config)# interface Port-channel1
```

```
Router2(config-if)# ip nat outside
```

5. Изменение конфигурации маршрутизации

```
Router2(config)# interface Loopback1
```

```
Router2(config-subif)# ip address 122.20.0.73 255.255.255.255
```

```
Router2(config)# interface Loopback2
```

```
Router2(config-subif)# ip address 122.20.0.74 255.255.255.255
```

```
Router2(config)# router ospf 111
```

```
Router2(config-router)#no network 172.20.0.96 0.0.0.15 area 1
```

```
Router2(config-router)# network 122.20.0.0 0.0.0.15 area 1
```

```
Router2(config-router)# network 122.20.0.68 0.0.0.3 area 1
```

```
Router2(config-router)# network 122.20.0.52 0.0.0.3 area 1
```

```
Router2(config-router)# network 122.20.0.72 0.0.0.3 area 1
```

Проверка конфигурации ПАТ

- Show ip nat translations
- Show ip nat stat

6. Последовательность действий и пример конфигурации ПАТ для одного публичного IP-адреса.

1, Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды *access-list номерACL permit IPадрес_внутренней_сети_обратная_маска_внутренней_сети*.

```
Router2(config)#access-list 15 permit 172.20.0.64 0.0.0.15
```

```
Router2(config)#access-list 15 permit 172.20.0.80 0.0.0.15
```

2. Конфигурация ПАТ с указанием номера списка контроля доступа и типа и номера интерфейса, IP-адрес которого будет использован для трансляции, с помощью команды *ip nat inside source list номер_ACL interface tun_номер overload*.

```
Router2(config)#ip nat inside source list 15 interface  
GigabitEthernet0/2/0 overload
```

3. Определить какие интерфейс к внутренней сети и к внутренней сети с помощью команды *ip nat inside*. И *ip nat outside*

```
Router2(config)#interface GigabitEthernet0/2/0
```

```
Router2(config-if)# ip nat outside
```

```
Router2(config)# interface GigabitEthernet0/0.400
```

```
Router2(config-if)# ip nat inside
```

```
Router2(config)# interface GigabitEthernet0/0.401
```

```
Router2(config-if)# ip nat inside
```