



**РАНХиГС**  
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА  
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ  
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

# НАСТРОЙКА ТРАНСЛЯЦИИ СЕТЕВЫХ АДРЕСОВ (**NAT**) В ОС **LINUX**

ВЫПОЛНИЛА СТУДЕНТКА ГРУППЫ **31КС-17**: БОЙКО МАРГО

ПРЕДМЕТ: ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

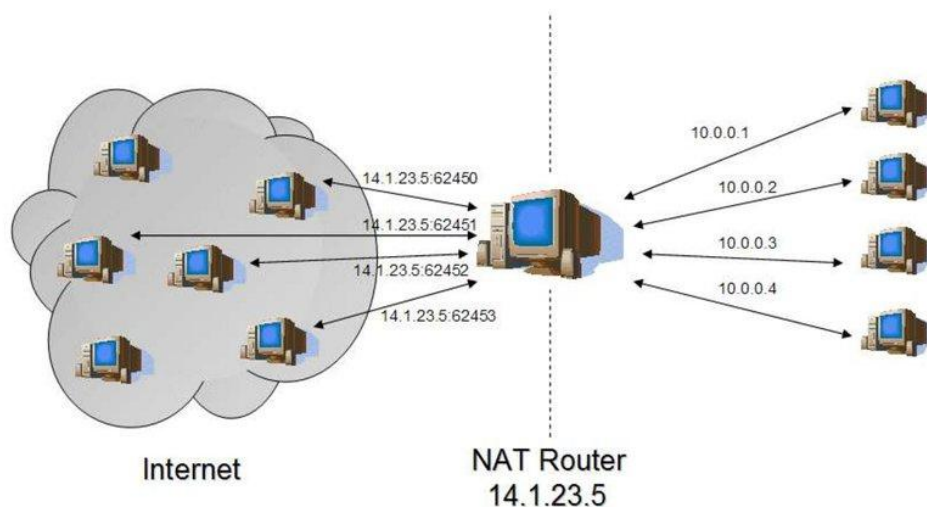
ПРЕПОДАВАТЕЛЬ: БАБАЕВА НАЗИЯТ АГАБЕКОВНА

МОСКВА, **2019**

# ЧТО ТАКОЕ NAT?

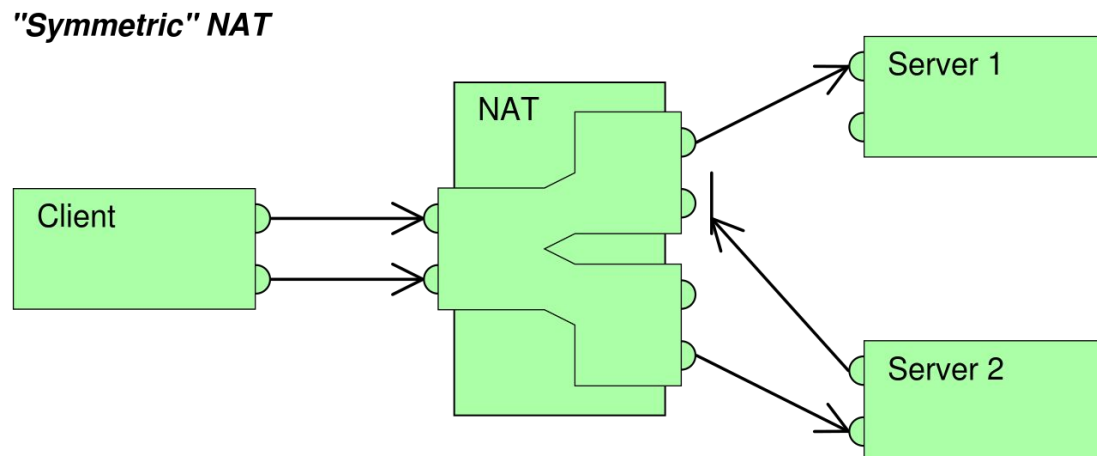
**Network Address Translation** — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

## Принцип работы NAT



# ТИПЫ NAT

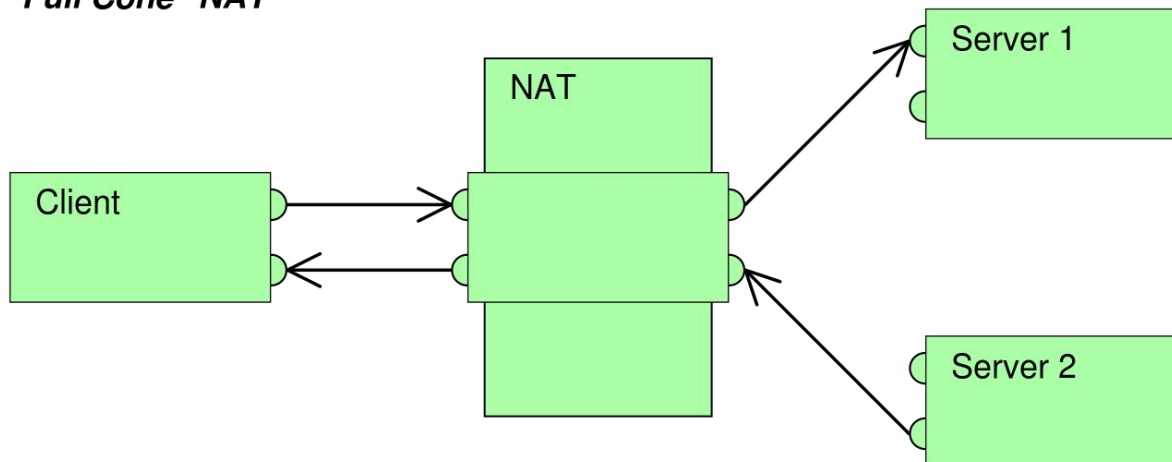
**Симметричный NAT (Symmetric NAT)** — трансляция, при которой каждое соединение, инициируемое парой «внутренний адрес: внутренний порт» преобразуется в свободную уникальную случайно выбранную пару «публичный адрес: публичный порт». При этом инициация соединения из публичной сети невозможна.



# ТИПЫ NAT

**Cone NAT, Full Cone NAT** — однозначная (взаимная) трансляция между парами «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт». Любой внешний хост может инициировать соединение с внутренним хостом (если это разрешено в правилах межсетевого экрана).

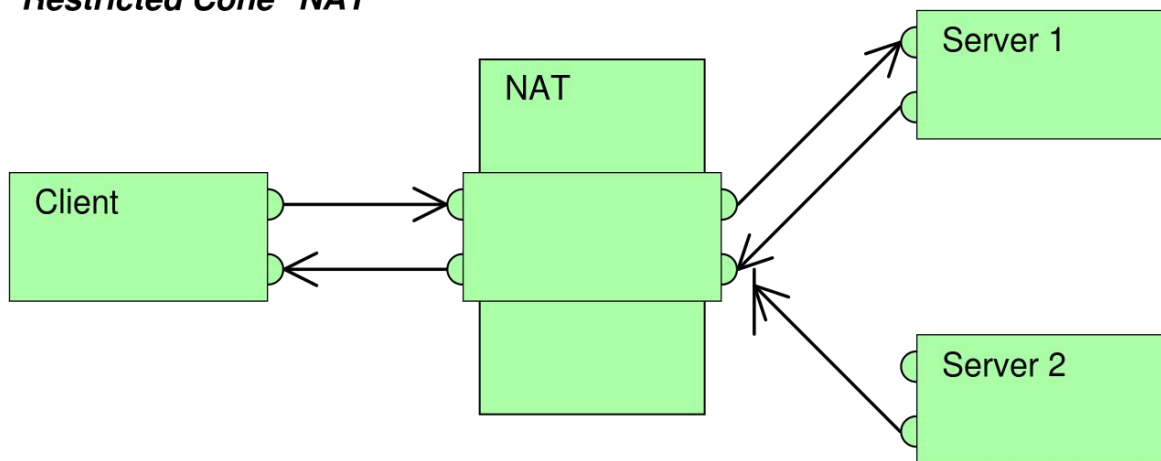
*"Full Cone" NAT*



# ТИПЫ NAT

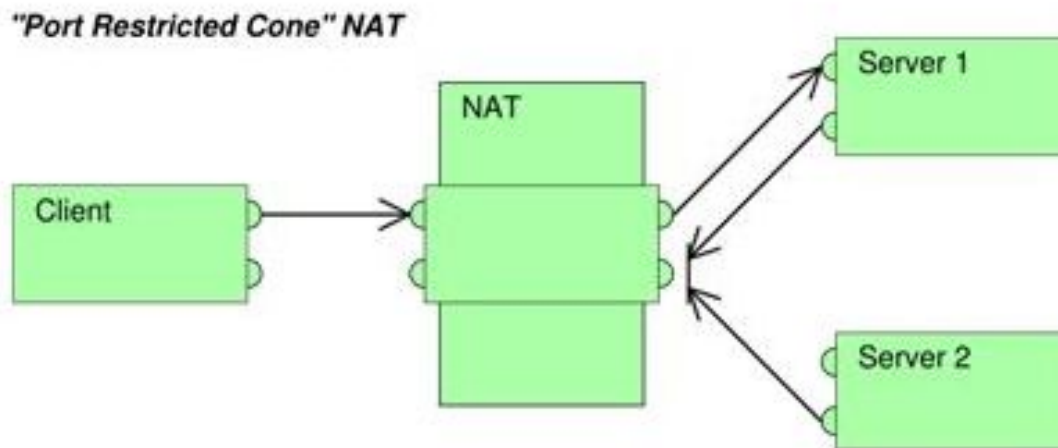
**Address-Restricted cone NAT, Restricted cone NAT** — постоянная трансляция между парой «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт». Любое соединение, инициированное с внутреннего адреса, позволяет в дальнейшем получать ему пакеты с любого порта того публичного хоста, к которому он отправлял пакет(ы) ранее.

*"Restricted Cone" NAT*



# ТИПЫ NAT

**Port-Restricted cone NAT** — трансляция между парой «внутренний адрес: внутренний порт» и «публичный адрес: публичный порт», при которой входящие пакеты проходят на внутренний хост только с одного порта публичного хоста — того, на который внутренний хост уже посылал пакет.



# ФУНКЦИИ NAT

- 1.** Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.
- 2.** Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.
- 3.** Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомлённых посетителей можно будет попасть по адресу <http://example.org:54055>, но на внутреннем сервере, находящемся за NAT, он будет работать на обычном 80-м порту. Повышение безопасности и сокрытие «непубличных» ресурсов.

# ПОРЯДОК ПРИМЕНЕНИЯ NAT

- 1.** На рабочих станциях указанный шлюз по умолчанию или gateway
- 2.** Преобразует служебные заголовки, формирует идентичный IP-пакет
- 3.** Публикация локальных ресурсов во внешней IP-сети
- 4.** Экономическая выгода вследствие приобретения единственного IP-подключения, а не IP-сети.
- 5.** Соккрытие от внешнего наблюдателя структуры внутренней IP-сети.
- 6.** Организация системы с распределенной нагрузкой.
- 7.** При общем доступе через NAT прозрачно открывается доступ к внутренней структуре с защитой без использования межсетевого экрана и т. п.
- 8.** Через NAT корректно работают многие сетевые протоколы. Конструктивные реализации (общий доступ — это и есть подключение NAT) есть аппаратная реализация NAT (интегрированы межсетевые экраны).



# ВЫВОД

**Анализируя функционал и порядок применения, можно сделать вывод, что NAT может быть использован во многих компаниях и организациях, так как данная система позволяет не только уменьшить используемое адресное пространство, выделенное для компаний, но и увеличить защищенность сети за счет функционирования данной системы как межсетевого экрана.**

# ИСТОЧНИКИ

- [https://ru.wikipedia.org/wiki/NAT#Программная\\_реализация\\_NAT](https://ru.wikipedia.org/wiki/NAT#Программная_реализация_NAT)
- Студент группы 872 Военного Института Правительственной Связи: Славнов Вадим

СПАСИБО ЗА  
ВНИМАНИЕ!

