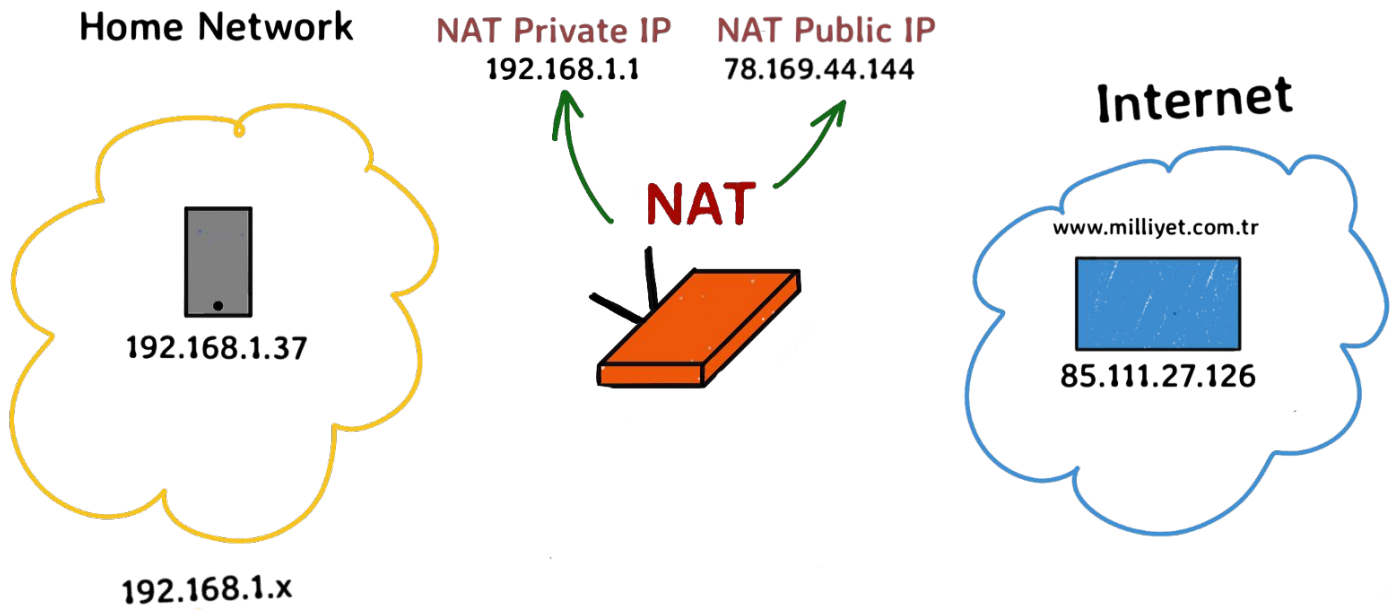
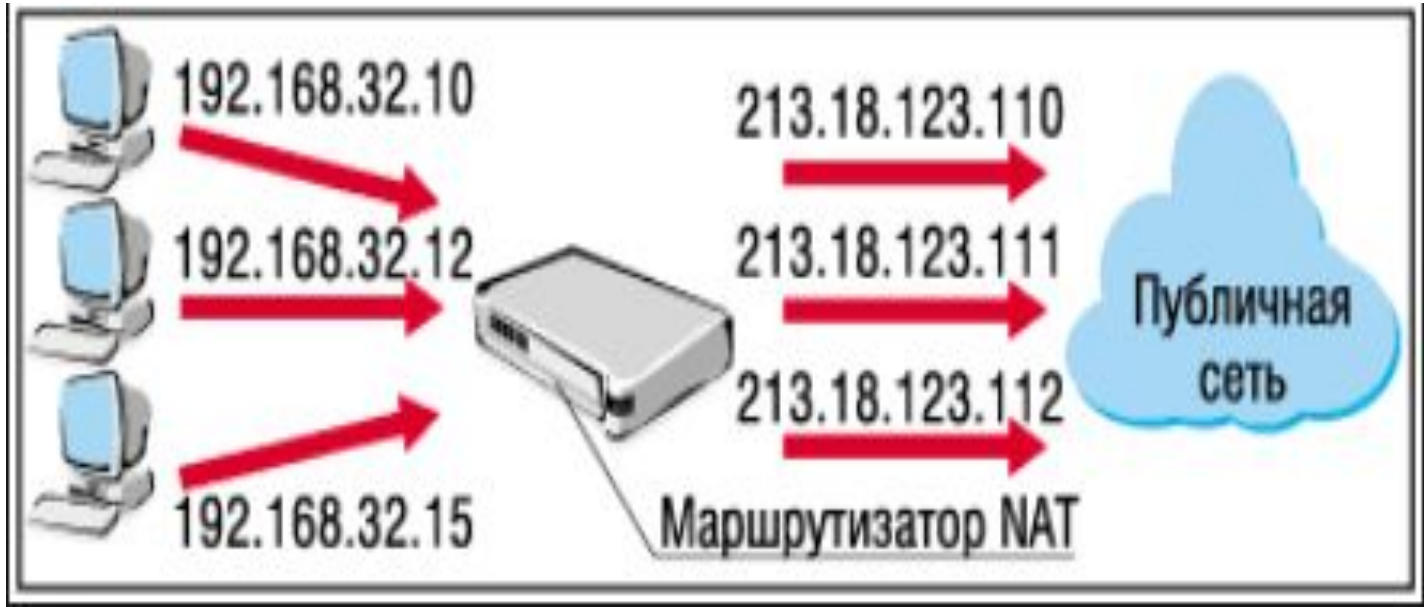
Протокол NAT



Характеристики NAT

NAT (*Network Address Translation* – преобразование сетевых адресов) обеспечивает преобразование частных адресов в публичные адреса. Это позволяет устройству с частным IPv4-адресом получать доступ к ресурсам вне своей частной сети, включая ресурсы, найденные в Интернете. В сочетании с частными IPv4-адресами, NAT продемонстрировал свою целесообразность в отношении экономии публичных IPv4-адресов. Один публичный IPv4-адрес может совместно использоваться сотнями, даже тысячами устройств, для каждого из которых настроен уникальный частный IPv4-адрес.



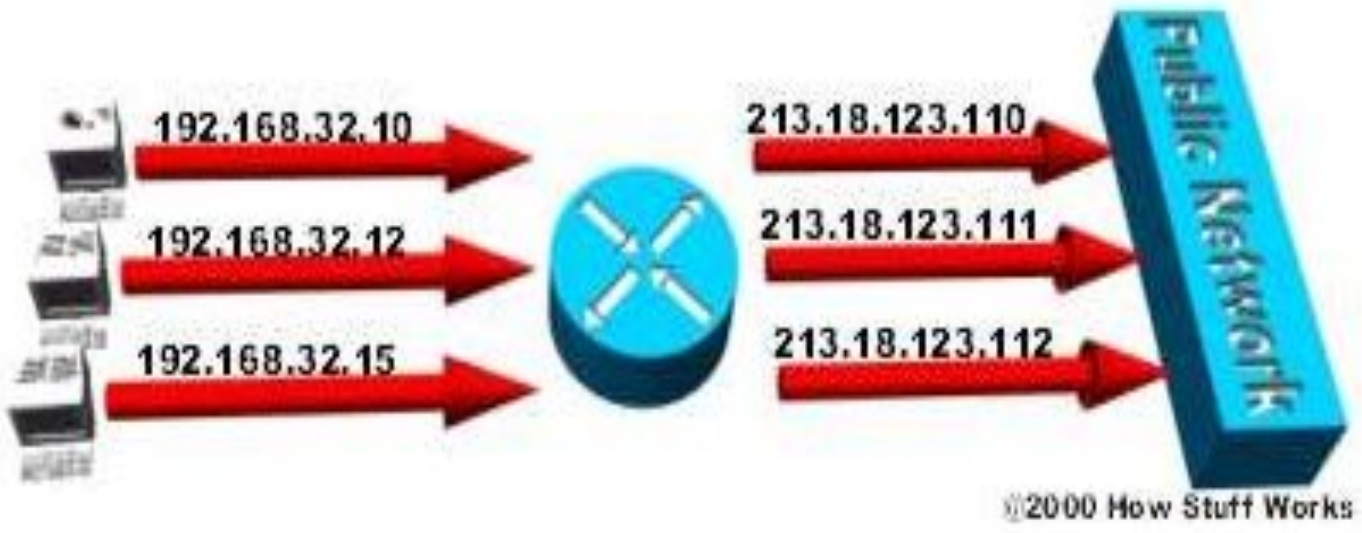
ПРИНЦИП РАБОТЫ СИСТЕМЫ NAT

Система NAT похожа на секретаря в большом офисе. Допустим, вы дали ему инструкцию не соединять вас ни с кем, кто бы ни звонил по телефону, пока вы не дадите разрешение на такие действия. Позже вы звоните потенциальному клиенту и оставляете ему сообщение о том, чтобы он вам перезвонил. Вы сообщаете секретарю, что ждете звонка от клиента и приказываете обеспечить соединение, когда тот позвонит.

Клиент набирает главный телефонный номер офиса, потому что ему известен только этот номер. Клиент сообщает секретарю, что он хочет связаться с вами, секретарь сверяется по справочной таблице, где указано ваше имя и ваш добавочный телефонный номер. Секретарь знает, что вы разрешили скоммутировать этого клиента, поэтому коммутирует вызывающую сторону на ваш добавочный номер.

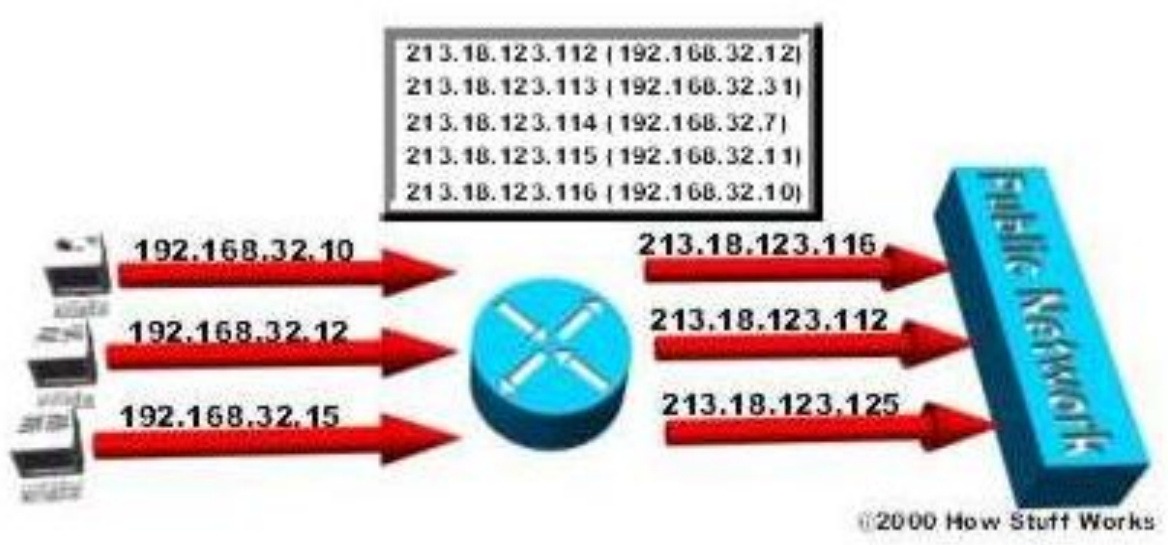
Способы работы NAT

Статический NAT - Отображение незарегистрированного IP адреса на зарегистрированный IP адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.



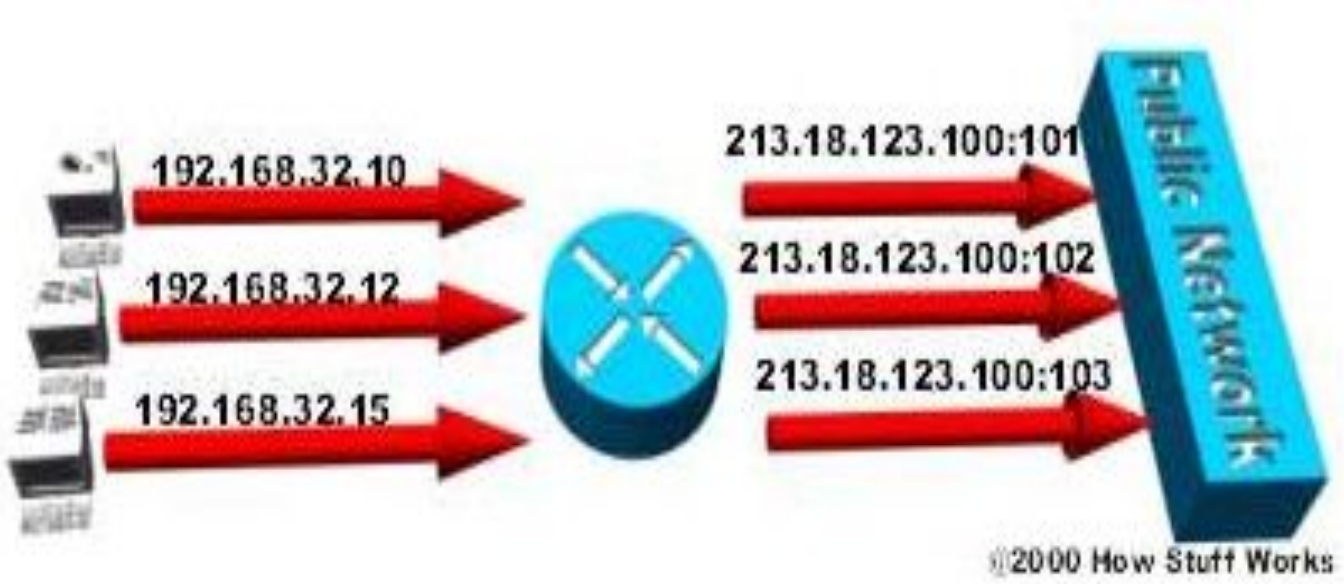
В статическом NAT, компьютер с адресом 192.168.32.10 будет всегда транслироваться в адрес 213.18.123.110:

Динамический NAT - Отображает незарегистрированный IP адрес на зарегистрированный адрес от группы зарегистрированных IP адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.



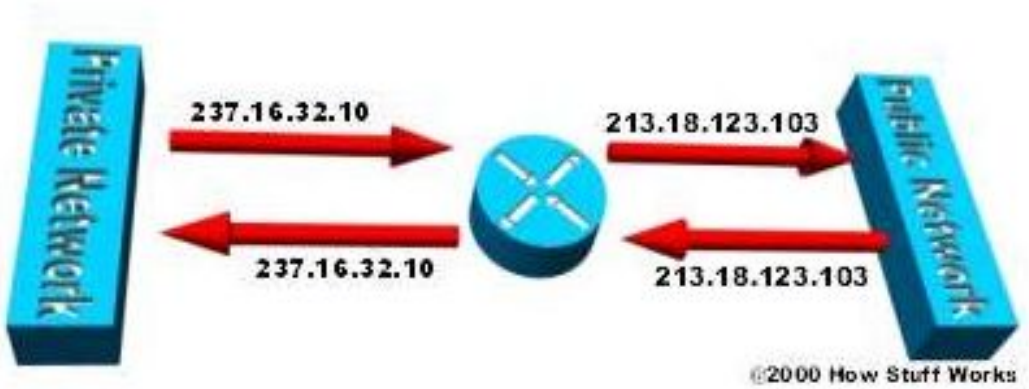
В динамическом NAT, компьютер с адресом 192.168.32.10 транслируется в первый доступный адрес в диапазоне от 213.18.123.100 до 213.18.123.150

Перегрузка(Overload) - форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP адрес, используя различные порты. Известен также как PAT (Port Address Translation)



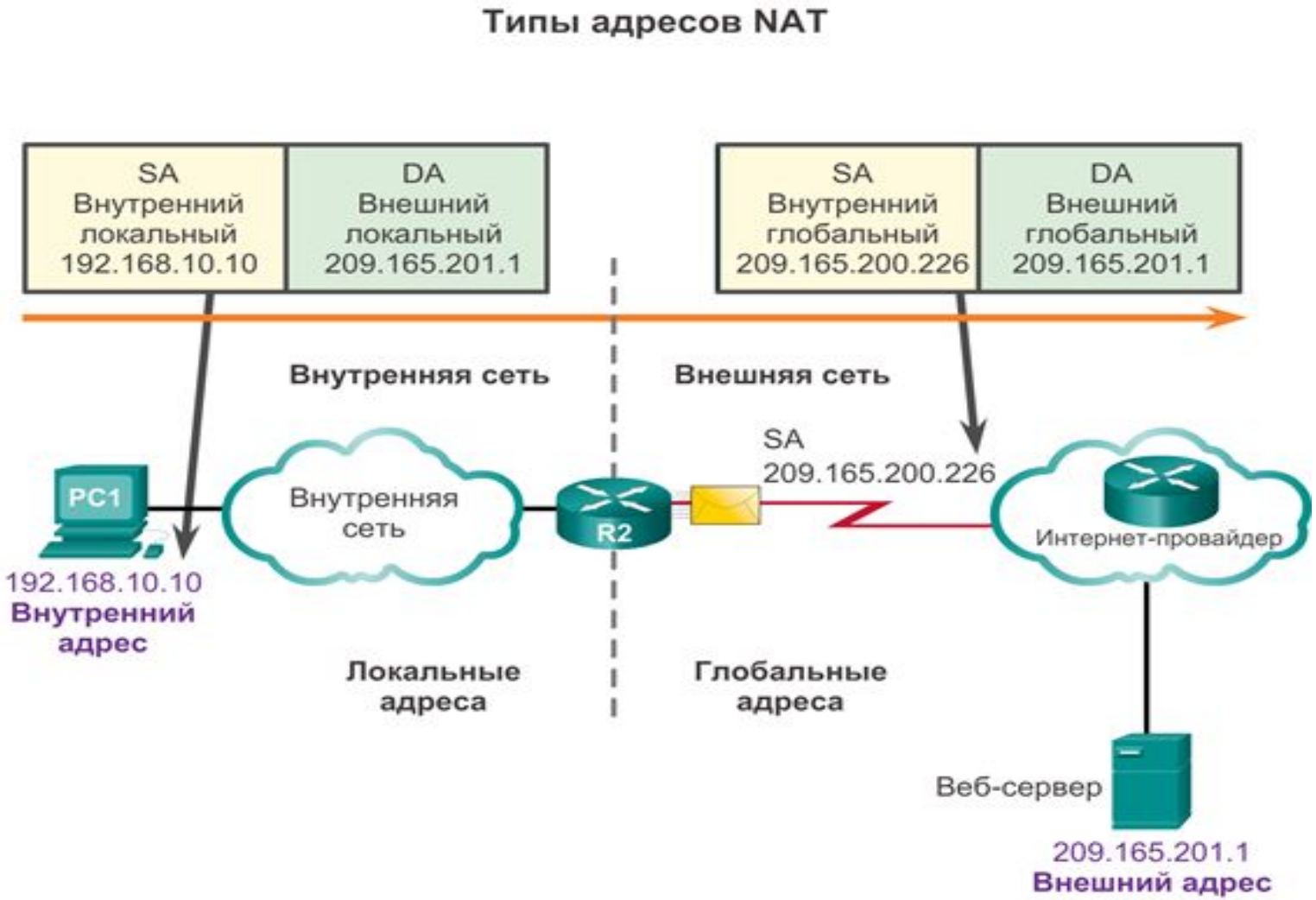
При перегрузке, каждый компьютер в частной сети транслируется в тот же самый адрес (213.18.123.100), но с различным номером порта

- **Перекрытие** - Когда IP адреса, используемые в вашей внутренней сети, также используются в другой сети, маршрутизатор должен держать таблицу поиска этих адресов так, чтобы он мог перехватить и заменить их зарегистрированными уникальными IP адресами. Важно отметить, что NAT маршрутизатор должен транслировать "внутренние" адреса в зарегистрированные уникальные адреса, а также должен транслировать "внешние" зарегистрированные адреса в адреса, которые являются уникальными для частной сети. Это может быть сделано либо через статический NAT, либо вы можете использовать DNS и реализовать динамический NAT.



Внутренний диапазон IP (237.16.32.xx) является также зарегистрированный диапазоном, используемым другой сетью. Поэтому, маршрутизатор транслирует адреса, чтобы избежать потенциального конфликта . Он также будет транслировать зарегистрированные глобальные IP адреса обратно к незарегистрированным локальным адресам , когда пакеты посылаются во внутреннюю сеть

Типы адресов NAT

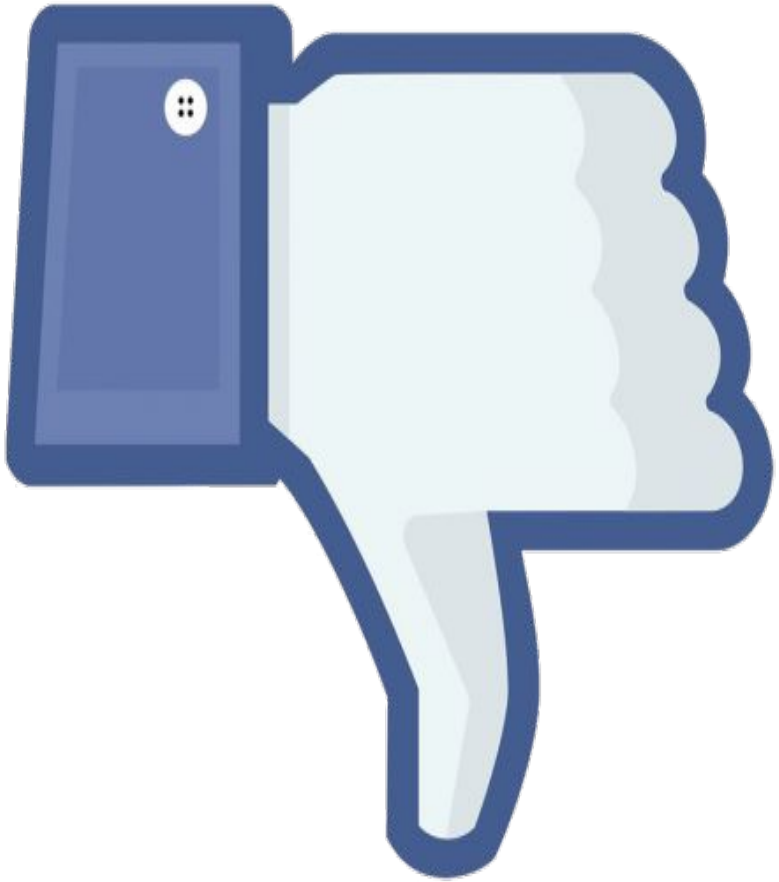


- **Внутренний локальный адрес** — это адрес источника, видимый из внутренней сети. На рисунке PC1 назначен IPv4-адрес 192.168.10.10. Это внутренний локальный адрес PC1.
- **Внутренний глобальный адрес** — это адрес источника, видимый из внешней сети. На рисунке, когда PC1 отправляет трафик веб-серверу с адресом 209.165.201.1, R2 преобразует внутренний локальный адрес во внутренний глобальный адрес. В этом случае R2 меняет исходный IPv4-адрес с 192.168.10.10 на 209.165.200.226. В терминологии NAT, внутренний локальный адрес 192.168.10.10 преобразуется во внутренний глобальный адрес 209.165.200.226.
- **Внешний глобальный адрес** — это адрес назначения, видимый из внешней сети. Это глобально маршрутизируемый IPv4-адрес, назначенный узлу в Интернете. Например, вебсервер доступен по IPv4-адресу 209.165.201.1. В большинстве случаев внешний локальный и внешний глобальный адреса совпадают.
- **Внешний локальный адрес** — это адрес назначения, видимый из внутренней сети. В этом примере PC1 отправляет трафик веб-серверу с IPv4-адресом 209.165.201.1. В редких случаях этот адрес может отличаться от глобально маршрутизируемого адреса назначения.

Преимущества NAT:

- **Позволяет сэкономить IP-адреса** 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.
- **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.
- **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 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.

Недостатки NAT:



- **Старые протоколы**. Протоколы, разработанные до массового внедрения NAT, не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP).
- **Идентификация пользователей**. Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.
- **Иллюзия DoS-атаки**. Если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT приводит к проблеме с подключением к серверу некоторых пользователей из-за превышения допустимой скорости подключений. Частичным решением проблемы является использование *пула адресов*(группы адресов), для которых осуществляется трансляция.
- **Пиринговые сети**. В NAT-устройствах, не поддерживающих технологию Universal Plug & Play, в некоторых случаях, необходима дополнительная настройка при работе с пиринговыми сетями и некоторыми другими программами, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие.

Школа системного администратора.

Подготовительный курс.

Глава 1: сетевые технологии.

Урок: NAT.