Технология PAT

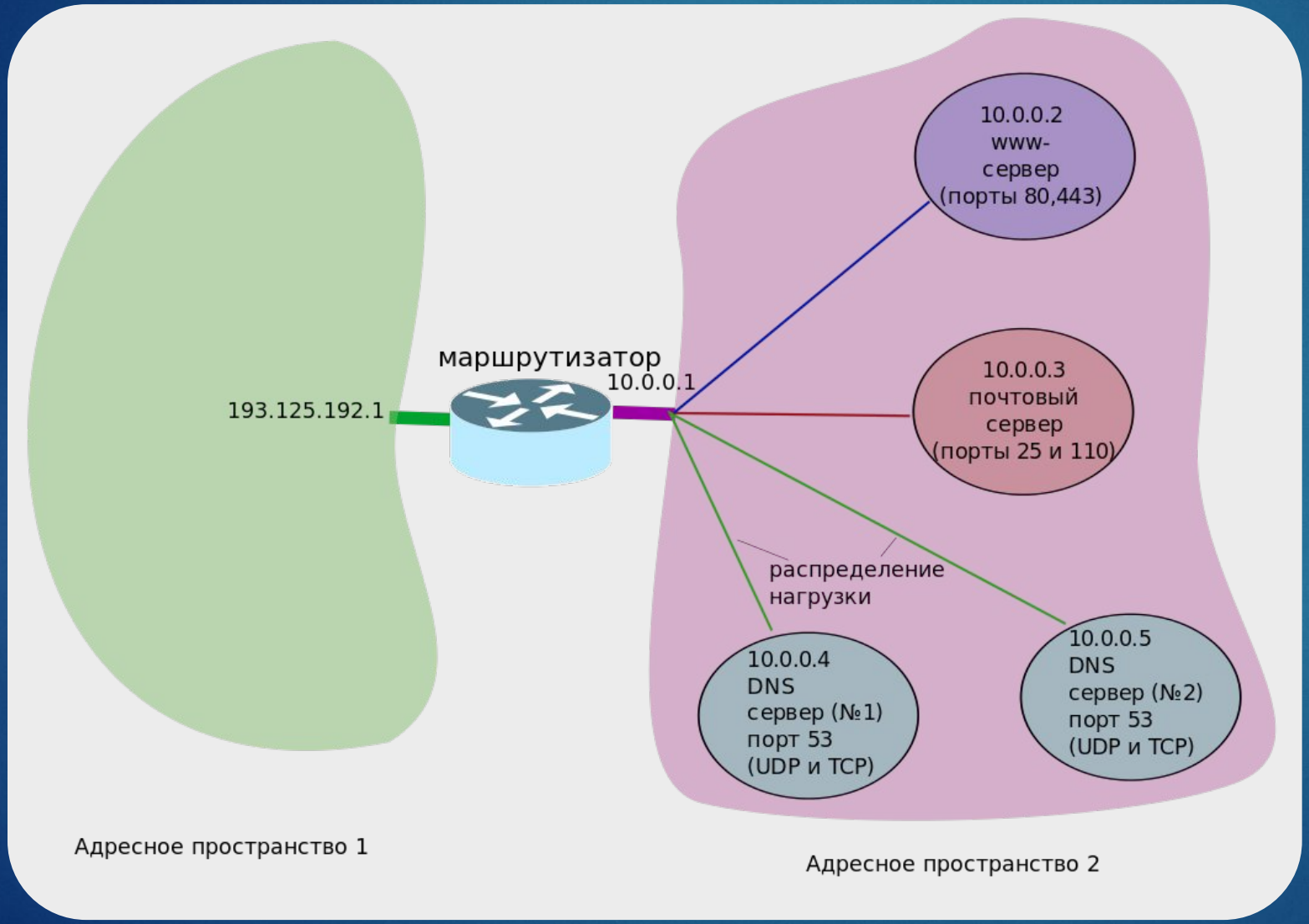
Определение

- Трансляция порт-адрес (Port address translation, PAT) — технология трансляции сетевого адреса в зависимости от порта получателя. Является частным случаем NAT. Позволяет выводить в Интернет до 65535 хостов локальной сети под одним реальным адресом, видимым из интернета. PAT решает проблему глобальной нехватки белых адресов в интернете, экономя общее адресное пространство.

Пример

- Маршрутизатор имеет два интерфейса (например, адрес 193.125.192.1, на который поступают запросы и для которого производится трансляция, и адрес 10.0.0.1, который обращён в сторону сети с серверами). При этом IP-пакеты, поступающие на маршрутизатор, в зависимости от адреса порта получателя транслируются с различными адресами — порты 80 и 443 направляются на один сервер (10.0.0.2), порты 25 и 110 на второй (10.0.0.3), 53 на третий (10.0.0.4). Соответствующим же образом производится и трансляция ответов серверов (в этом случае заменяется адрес отправителя). В соответствии с этим есть два типа сети: внутренняя (nat inside) и внешняя (nat outside). У пакетов, приходящих из наружной сети, меняется адрес получателя, у пакетов из внутренней — отправителя.

Пример трансляции



Наружу виден 1 IP-адрес, обслуживающий порты 25,53,80,110,443

Аналогии PAT

- Устройство PAT похоже на секретаря в офисе, который имеет один внешний телефонный номер. Все исходящие звонки, сделанные из офиса, будут с одного номера. Однако входящие звонки должны быть переданы определенному сотруднику секретарем, который будет спрашивать клиента, с кем тот хочет говорить; до этих офисных разветвлений нельзя подключиться извне прямо.

Связи между NAT и PAT

- PAT является подмножеством NAT и тесно связана с концепцией NAT. В PAT только один выставляемый публично IP-адрес и много внутренних хостов. Входящие пакеты с открытой сети маршрутизируются к своим назначениям во внутреннюю сеть по ссылкам в таблице, сохраненной внутри устройства PAT, который отслеживает внутренние и внешние пары портов.
- Когда происходит трансляция PAT, и внутренний адрес IP и номер порта связи модифицируются; устройство PAT выбирает номера портов, которые будут видны хостам внешней сети. Таким образом, PAT оперирует и на 3 (сетевой), и на 4 (транспортный) уровнях модели OSI , тогда как базовый NAT оперирует только на уровне 3.

Различия между NAT и PAT

NAT

Пул внутренних глобальных адресов	Внутренний локальный адрес
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Внутренний глобальный адрес	Внутренний локальный адрес
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

Как показано на рисунке, NAT преобразует IPv4-адреса, исходя из схемы 1:1для частных IPv4-адресов и публичных IPv4-адресов. В то же время, PAT меняет и адрес, и номер порта.

Использование PAT

- Программные брандмауэры (файерволы) и устройства широкополосного сетевого доступа (например, ADSL роутеры) являются примерами сетевых технологий, которые могут содержать реализацию PAT. Когда конфигурируются эти устройства, внешней сетью является Интернет, а внутренней сетью является LAN .

Преимущества PAT

- Позволяет сэкономить IP-адреса
- Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу.
- Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов.

Недостатки PAT

- 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).
- Масштабируемость. Поскольку доступно только ограниченное количество номеров для портов, устройство PAT может в итоге иметь недостаточно места в таблице трансляции. Хотя доступны тысячи портов, и они быстро высвобождаются для нового использования, некоторые сетевые связи отнимают много портов почти одновременно, в одну логическую транзакцию
- Сложность с файерволом. Так как внутренние адреса являются скрытыми за одним публичным доступным адресом, невозможно для внешних машин инициировать соединение с конкретной машиной внутри, без специальной настройки в брандмауэре, для передачи соединения на конкретный порт. Это значительно влияет на приложения, такие как VOIP, видеоконференции, и другие peer-to-peer приложения.