МДК.02.02 Организация администрирования компьютерных сетей

3-курс

Занятие 07, 08

Технология NAT

Технология NAT

Изначально было задумано 2 в степени 32 или 4 294 967 296 IPv4 адресов.

Много это или нет? Кажется, что да.

Однако с распространением персональных вычислений, мобильных устройств и быстрым ростом интернета вскоре стало очевидно, что 4,3 миллиарда адресов IPv4 будет недостаточно.

Долгосрочным решением было IPv6, но требовались более быстрое решение для устранения нехватки адресов.

И этим решением стал NAT (Network Address Translation).

Технология NAT

Сети обычно проектируются с использованием частных IP- адресов.

Это адреса **10.0.0.0/8, 172.16.0.0/12** и **192.168.0.0/16**.

Эти частные адреса используются внутри организации или площадки, чтобы позволить устройствам общаться локально, и они не маршрутизируются в интернете.

Чтобы позволить устройству с приватным IPv4-адресом обращаться к устройствам и ресурсам за пределами локальной сети, приватный адрес сначала должен быть переведен на общедоступный публичный адрес.

Технология NAT

И вот как раз NAT переводит приватные адреса, в общедоступные.

Это позволяет устройству с частным адресом IPv4 обращаться к ресурсам за пределами его частной сети.

NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных IPv4-адресов.

Один общедоступный IPv4-адрес может быть использован сотнями, даже тысячами устройств, каждый из которых имеет частный IPv4-адрес.

NAT имеет дополнительное преимущество, заключающееся в добавлении степени конфиденциальности и безопасности в сеть, поскольку он скрывает внутренние IPv4-адреса из внешних сетей.

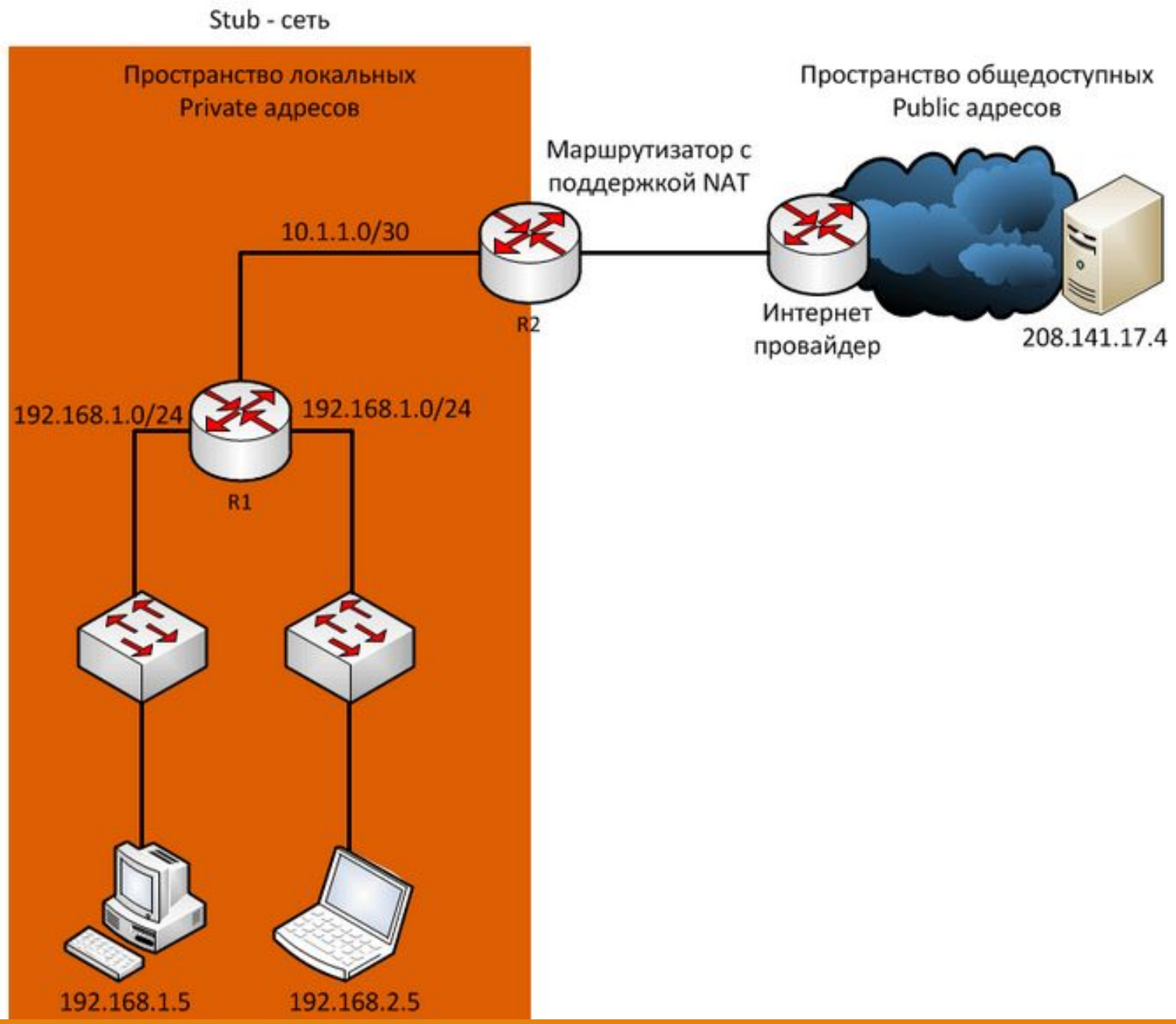
Технология NAT

Маршрутизаторы с поддержкой NAT могут быть настроены с одним или несколькими действительными общедоступными IPv4-адресами.

Эти общедоступные адреса называются пулом NAT.

Когда устройство внутренней сети отправляет трафик из сети наружу, то маршрутизатор с поддержкой NAT переводит внутренний IPv4-адрес устройства на общедоступный адрес из пула NAT.

Для внешних устройств весь трафик, входящий и выходящий из сети, выглядит имеющим общедоступный IPv4 адрес.


Stub - сеть
Пространство локальных
Private адресов
Пространство общедоступных
Public адресов
Маршрутизатор с
поддержкой NAT
10.1.1.0/30
R2
Интернет
провайдер
208.141.17.4
192.168.1.0/24
192.168.1.0/24
R1
192.168.1.5
192.168.2.5

Технология NAT

Маршрутизатор NAT обычно работает на границе Stub-сети.

Stub-сеть – это тупиковая сеть, которая имеет одно соединение с соседней сетью, один вход и выход из сети.

Когда устройство внутри Stub-сети хочет связываться с устройством за пределами своей сети, пакет пересылается пограничному маршрутизатору.

Пограничный маршрутизатор выполняет NAT-процесс, переводя внутренний частный адрес устройства на публичный, внешний, маршрутизируемый адрес.

Терминология NAT

Терминология NAT

В терминологии NAT внутренняя сеть представляет собой набор сетей, подлежащих переводу.

Внешняя сеть относится ко всем другим сетям.

При использовании NAT, адреса IPv4 имеют разные обозначения.

Эти обозначения зависят от того, находятся ли они в частной сети или в общедоступной сети (в интернете), и является ли трафик входящим или исходящим.

Терминология NAT

NAT включает в себя четыре типа адресов:

- **Внутренний локальный адрес (Inside local address)**;
- **Внутренний глобальный адрес (Inside global address)**;
- **Внешний местный адрес (Outside local address)**;
- **Внешний глобальный адрес (Outside global address)**;

При определении того, какой тип адреса используется, важно помнить, что терминология NAT всегда применяется с точки зрения устройства с транслированным адресом.

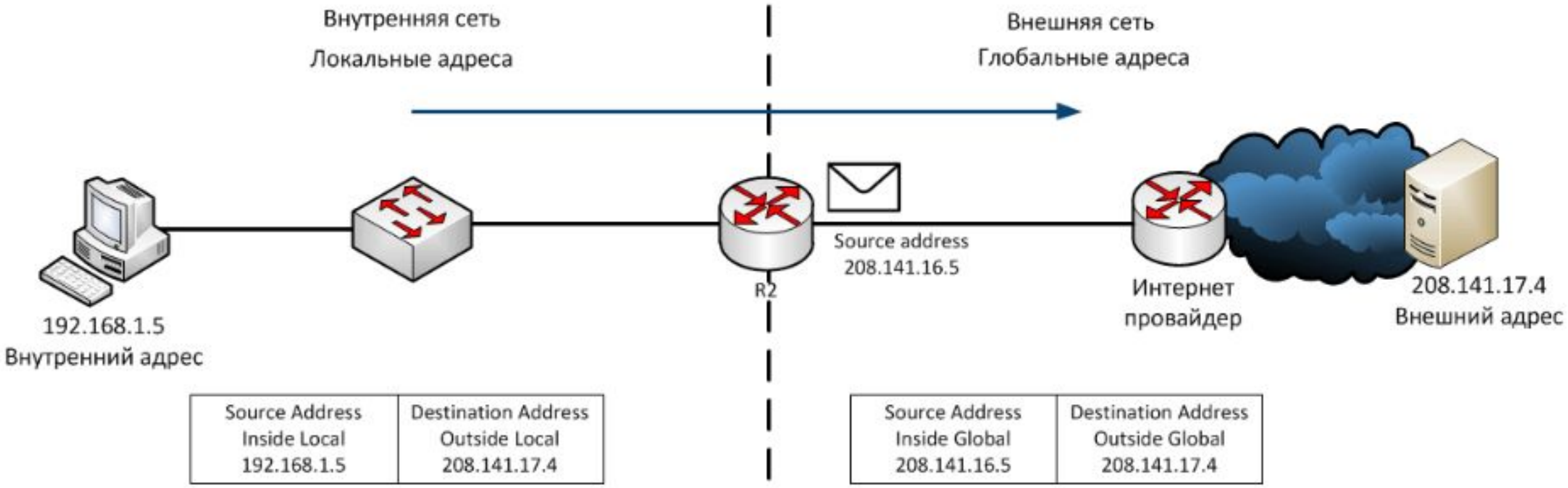
Терминология NAT

То есть:

- **Внутренний адрес (Inside address)** - адрес устройства, которое транслируется NAT;
- **Внешний адрес (Outside address)** - адрес устройства назначения;
- **Локальный адрес (Local address)** - это любой адрес, который отображается во внутренней части сети;
- **Глобальный адрес (Global address)** - это любой адрес, который отображается во внешней части сети;

Рассмотрим это на примере схемы.

Терминология NAT



Терминология NAT

На рисунке ПК имеет внутренний локальный (**Inside local**) адрес 192.168.1.5.

С его точки зрения веб-сервер имеет внешний (**outside**) адрес 208.141.17.4.

Когда с ПК отправляются пакеты на глобальный адрес веб-сервера, внутренний локальный (**Inside local**) адрес ПК транслируется в 208.141.16.5 (**inside global**).

Адрес внешнего устройства обычно не переводится, поскольку он является общедоступным адресом IPv4.

Терминология NAT

Необходимо отметить, что ПК имеет разные локальные и глобальные адреса.

В отличие от ПК, веб-сервер имеет одинаковый публичный IP адрес.

С его точки зрения трафик, исходящий из ПК поступает с внутреннего глобального адреса 208.141.16.5.

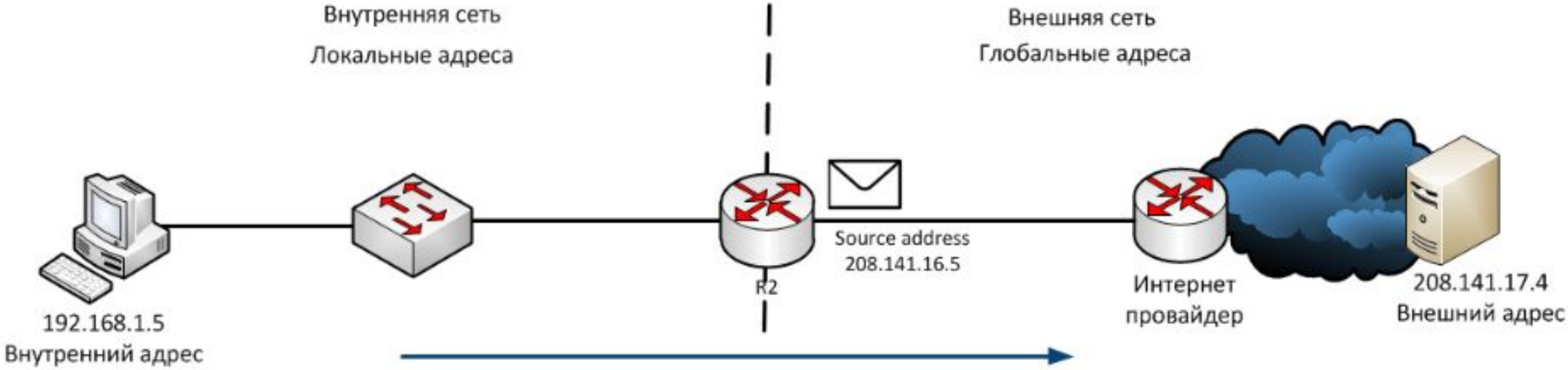
Маршрутизатор с NAT является точкой демаркации между внутренней и внешней сетями и между локальными и глобальными адресами.

Терминология NAT

Термины, **inside** и **outside**, объединены с терминами **local** и **global**, чтобы ссылаться на конкретные адреса.

На рисунке маршрутизатор настроен на предоставление NAT и имеет пул общедоступных адресов для назначения внутренним хостам.

На следующем рисунке показано как сообщение отправляется с внутреннего ПК на внешний веб-сервер, через маршрутизатор с поддержкой NAT, а также как сообщение высылается и переводится в обратную сторону.



Source Address Inside Local 192.168.1.5	Destination Address Outside Local 208.141.17.4

Source Address Inside Global 208.141.16.5	Destination Address Outside Global 208.141.17.4

Destination Address Inside Local 192.168.1.5	Source Address Outside Local 208.141.17.4

Destination Address Inside Global 208.141.16.5	Source Address Outside Global 208.141.17.4

NAT таблица маршрутизатора			
ПК		Веб-сервер	
Inside Global	Inside Local	Outside Local	Outside Global
208.141.17.4	192.168.1.5	208.141.16.5	208.141.16.5

Терминология NAT

Внутренний локальный адрес (**Inside local address**) – адрес источника, видимый из внутренней сети.

На рисунке адрес 192.168.1.5 присвоен ПК – это и есть его внутренний локальный адрес.

Внутренний глобальный адрес (**Inside global address**) – адрес источника, видимый из внешней сети.

На рисунке, когда трафик с ПК отправляется на веб-сервер по адресу 208.141.17.4, маршрутизатор переводит внутренний локальный адрес (**Inside local address**) на внутренний глобальный адрес (**Inside global address**).

В этом случае роутер изменяет адрес источника IPv4 с 192.168.1.5 на 208.141.16.5.

Терминология NAT

Внешний глобальный адрес (**Outside global address**) – адрес адресата, видимый из внешней сети.

Это глобально маршрутизируемый IPv4-адрес, назначенный хосту в Интернете.

На схеме веб-сервер доступен по адресу 208.141.17.4.

Чаще всего внешние локальные и внешние глобальные адреса одинаковы.

Внешний локальный адрес (**Outside local address**) – адрес получателя, видимый из внутренней сети.

В этом примере ПК отправляет трафик на веб-сервер по адресу 208.141.17.4

Терминология NAT

Рассмотрим весь путь прохождения пакета.

ПК с адресом 192.168.1.5 пытается установить связь с веб-сервером 208.141.17.4.

Когда пакет прибывает в маршрутизатор с поддержкой NAT, он считывает IPv4 адрес назначения пакета, чтобы определить, соответствует ли пакет критериям, указанным для перевода.

В этом примере исходный адрес соответствует критериям и переводится с 192.168.1.5 (**Inside local address**) на 208.141.16.5. (**Inside global address**).

Терминология NAT

Роутер добавляет это сопоставление локального в глобальный адрес в таблицу NAT и отправляет пакет с переведенным адресом источника в пункт назначения.

Веб-сервер отвечает пакетом, адресованным внутреннему глобальному адресу ПК (208.141.16.5).

Роутер получает пакет с адресом назначения 208.141.16.5 и проверяет таблицу NAT, в которой находит запись для этого сопоставления.

Он использует эту информацию и переводит обратно внутренний глобальный адрес (208.141.16.5) на внутренний локальный адрес (192.168.1.5), и пакет перенаправляется в сторону ПК.

Типы NAT

Типы NAT

Существует три типа трансляции NAT:

- **Статическая адресная трансляция** (**Static NAT**) – сопоставление адресов один к одному между локальными и глобальными адресами;
- ***Динамическая адресная трансляция*** (**Dynamic NAT**) – сопоставление адресов “многие ко многим” между локальными и глобальными адресами;
- **Port Address Translation** (**PAT**) – многоадресное сопоставление адресов между локальными и глобальными адресами с использованием портов.

Также этот метод известен как **NAT Overload**;

Типы NAT

Static NAT

Статический NAT использует сопоставление локальных и глобальных адресов один к одному.

Эти сопоставления настраиваются администратором сети и остаются постоянными.

Когда устройства отправляют трафик в Интернет, их внутренние локальные адреса переводятся в настроенные внутренние глобальные адреса.

Для внешних сетей эти устройства имеют общедоступные IPv4-адреса.

Типы NAT

Статический NAT особенно полезен для веб-серверов.

Также статический NAT применяется для устройств, которые должны иметь согласованный адрес, доступный из Интернета, как например веб-сервер компании.

Статический NAT требует наличия достаточного количества общедоступных адресов для удовлетворения общего количества одновременных сеансов пользователя.

Типы NAT

Статическая NAT таблица выглядит так:

Static NAT Table	
Inside Local Address	Inside Global Address
192.168.1.2	208.165.17.5
192.168.1.3	208.165.17.6
192.168.1.4	208.165.17.7

Типы NAT

Dynamic NAT

Динамический NAT использует пул публичных адресов и назначает их по принципу «первым пришел, первым обслужен».

Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT назначает доступный общедоступный IPv4-адрес из пула.

Подобно статическому NAT, динамический NAT требует наличия достаточного количества общедоступных адресов для удовлетворения общего количества одновременных сеансов пользователя.

Типы NAT

Динамическая NAT таблица выглядит так:

Static NAT Table	
Inside Local Address	Inside Global Address
192.168.1.2	208.165.17.5
Available	208.165.17.6
Available	208.165.17.7
Available	208.165.17.8

Типы NAT

Port Address Translation (PAT)

PAT транслирует несколько частных адресов на один или несколько общедоступных адресов.

Это то, что делают большинство домашних маршрутизаторов.

Интернет-провайдер назначает один адрес маршрутизатору, но несколько членов семьи могут одновременно получать доступ к Интернету.

Это наиболее распространенная форма NAT.

Типы NAT

С помощью PAT несколько адресов могут быть сопоставлены с одним или несколькими адресами, поскольку каждый частный адрес также отслеживается номером порта.

Когда устройство инициирует сеанс **TCP/IP**, оно генерирует значение порта источника **TCP** или **UDP** для уникальной идентификации сеанса.

Когда NAT-маршрутизатор получает пакет от клиента, он использует номер своего исходного порта, чтобы однозначно идентифицировать конкретный перевод NAT.

Типы NAT

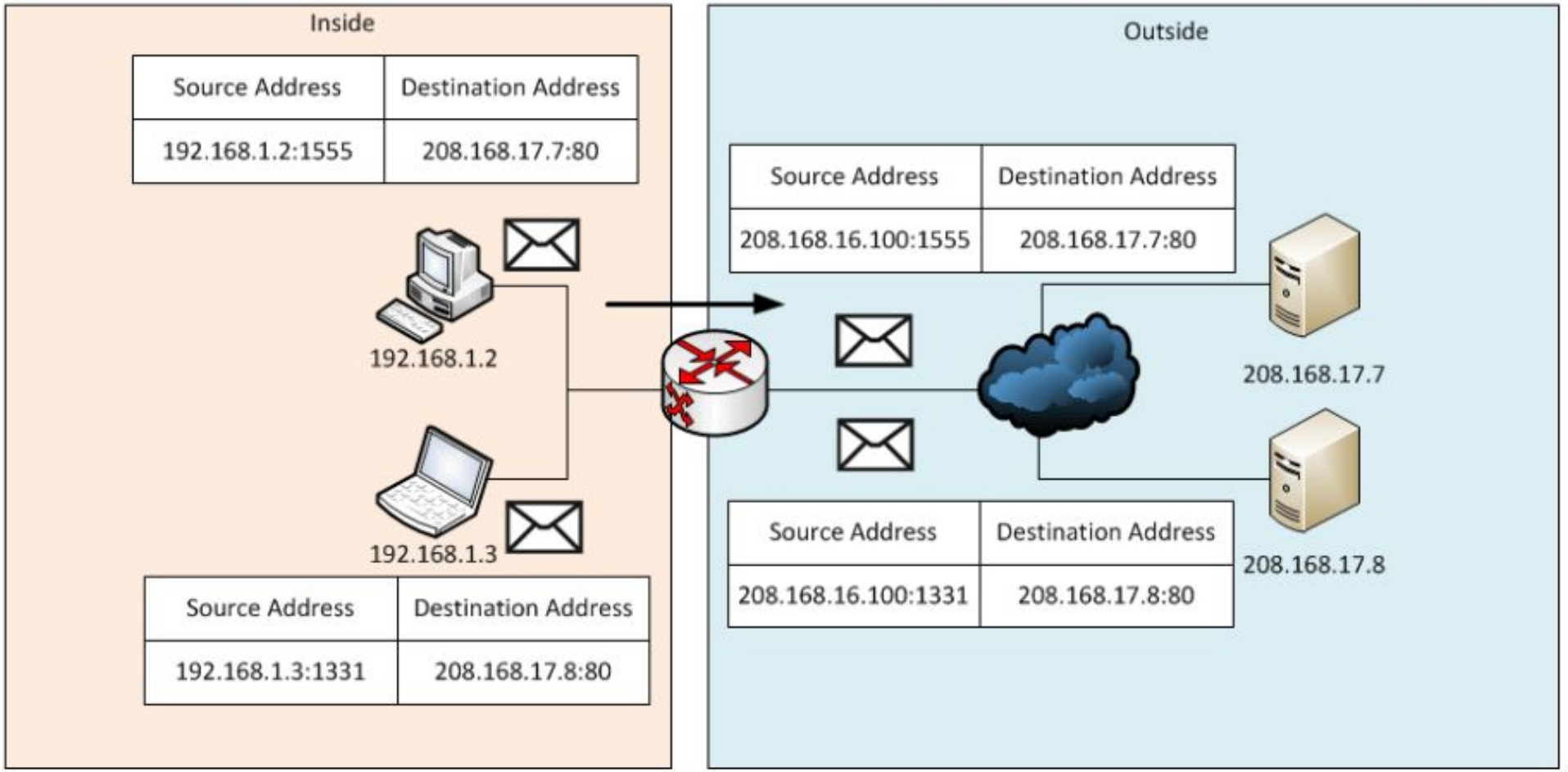
PAT гарантирует, что устройства используют разный номер порта TCP для каждого сеанса.

Когда ответ возвращается с сервера, номер порта источника, который становится номером порта назначения в обратном пути, определяет, на какое устройство маршрутизатор перенаправляет пакеты.

Следующий рисунок иллюстрирует процесс **PAT**.

PAT добавляет уникальные номера портов источника во внутренний глобальный адрес, чтобы различать переводы.

NAT Table with PAT			
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
208.168.16.100:1555	192.168.1.2:1555	208.168.17.7:80	208.168.17.7:80
208.168.16.100:1331	192.168.1.3:1331	208.168.17.8:80	208.168.17.8:80



Типы NAT

Поскольку маршрутизатор обрабатывает каждый пакет, он использует номер порта (1331 и 1555, в этом примере), чтобы идентифицировать устройство, с которого выслан пакет.

Адрес источника (**Source Address**) – это внутренний локальный адрес с добавленным номером порта, назначенным TCP/IP.

Адрес назначения (**Destination Address**) – это внешний локальный адрес с добавленным номером служебного порта.

В этом примере порт службы 80: HTTP.

Типы NAT

Для исходного адреса маршрутизатор переводит внутренний локальный адрес во внутренний глобальный адрес с добавленным номером порта.

Адрес назначения не изменяется, но теперь он называется внешним глобальным IP-адресом.

Когда веб-сервер отвечает, путь обратный.

В этом примере номера портов клиента 1331 и 1555 не изменялись на маршрутизаторе с NAT.

Это не очень вероятный сценарий, потому что есть высокая вероятность того, что эти номера портов уже были прикреплены к другим активным сеансам.

Типы NAT

PAT пытается сохранить исходный порт источника.

Однако, если исходный порт источника уже используется, PAT назначает первый доступный номер порта, начиная с начала соответствующей группы портов **0-511, 512-1023** или **1024-65535**.

Когда портов больше нет, и в пуле адресов имеется более одного внешнего адреса, PAT переходит на следующий адрес, чтобы попытаться выделить исходный порт источника.

Этот процесс продолжается до тех пор, пока не будет доступных портов или внешних IP-адресов.

Типы NAT

То есть если другой хост может выбрать тот же номер порта 1444.

Это приемлемо для внутреннего адреса, потому что хосты имеют уникальные частные IP-адреса.

Однако на маршрутизаторе NAT номера портов должны быть изменены.

В противном случае пакеты из двух разных хостов выйдут из него с тем же адресом источника.

Поэтому PAT назначает следующий доступный порт (1445) на второй адрес хоста.

Некоторые итоги

Некоторые итоги

Подведем итоги в сравнении NAT и PAT.

Как видно из таблиц, NAT переводит IPv4-адреса на основе 1:1 между частными адресами IPv4 и общедоступными IPv4-адресами.

Однако PAT изменяет как сам адрес, так и номер порта.

NAT перенаправляет входящие пакеты на их внутренний адрес, ориентируясь на входящий IP адрес источника, заданный хостом в общедоступной сети, а с PAT обычно имеется только один или очень мало публично открытых IPv4-адресов, и входящие пакеты перенаправляются, ориентируясь на NAT таблицу маршрутизатора.

Некоторые итоги

Если рассматривать пакеты IPv4, содержащие данные, отличные от TCP или UDP, то эти пакеты не содержат номер порта уровня 4.

PAT переводит наиболее распространенные протоколы, переносимые IPv4, которые не используют TCP или UDP в качестве протокола транспортного уровня.

Наиболее распространенными из них являются ICMPv4.

Каждый из этих типов протоколов по-разному обрабатывается PAT.

Некоторые итоги

Например, сообщения запроса ICMPv4, эхо-запросы и ответы включают идентификатор запроса **Query ID**.

ICMPv4 использует Query ID для идентификации эхо-запроса с соответствующим ответом.

Идентификатор запроса увеличивается с каждым отправленным эхо-запросом.

PAT использует идентификатор запроса вместо номера порта уровня 4.

Преимущества и недостатки NAT

Преимущества и недостатки NAT

NAT предоставляет множество **преимуществ**, в том числе:

- NAT сохраняет зарегистрированную схему адресации, разрешая приватизацию интрасетей.

При PAT внутренние хосты могут совместно использовать один общедоступный IPv4-адрес для всех внешних коммуникаций.

В этом типе конфигурации требуется очень мало внешних адресов для поддержки многих внутренних хостов;

- NAT повышает гибкость соединений с общедоступной сетью.

Многочисленные пулы, пулы резервного копирования и пулы балансировки нагрузки могут быть реализованы для обеспечения надежных общедоступных сетевых

Преимущества и недостатки NAT

- NAT обеспечивает согласованность для внутренних схем адресации сети.

Изменение общей схемы адресов IPv4 требует переадресации всех хостов в существующей сети.

Стоимость переадресации хостов может быть значительной.

NAT позволяет существующей частной адресной схеме IPv4 оставаться, позволяя легко изменять новую схему общедоступной адресации.

Это означает, что организация может менять провайдеров и не нужно менять ни одного из своих внутренних клиентов;

Преимущества и недостатки NAT

- NAT обеспечивает сетевую безопасность.

Поскольку частные сети не рекламируют свои адреса или внутреннюю топологию, они остаются достаточно надежными при использовании в сочетании с NAT для получения контролируемого внешнего доступа.

Однако нужно понимать, что NAT не заменяет фаерволы;

Преимущества и недостатки NAT

Но у NAT есть некоторые **недостатки**.

Тот факт, что хосты в Интернете, по-видимому, напрямую взаимодействуют с устройством с поддержкой NAT, а не с фактическим хостом внутри частной сети, создает ряд проблем:

- Один из недостатков использования NAT связан с производительностью сети, особенно для протоколов реального времени, таких как **VoIP**.

NAT увеличивает задержки переключения, потому что перевод каждого адреса IPv4 в заголовках пакетов требует времени;

Преимущества и недостатки NAT

- Другим недостатком использования NAT является то, что сквозная адресация теряется.

Многие интернет-протоколы и приложения зависят от сквозной адресации от источника до места назначения.

Некоторые приложения не работают с NAT.

Приложения, которые используют физические адреса, а не квалифицированное доменное имя, не доходят до адресатов, которые транслируются через NAT-маршрутизатор.

Иногда эту проблему можно избежать, реализуя статические сопоставления NAT;

Преимущества и недостатки NAT

- Также теряется сквозная трассировка IPv4.

Сложнее трассировать пакеты, которые подвергаются многочисленным изменениям адресов пакетов в течение нескольких NAT-переходов, что затрудняет поиск и устранение неполадок;

- Использование NAT также затрудняет протоколы туннелирования, такие как IPsec, поскольку NAT изменяет значения в заголовках, которые мешают проверкам целостности, выполняемым IPsec и другими протоколами туннелирования;

Преимущества и недостатки NAT

- Службы, требующие инициирования TCP-соединений из внешней сети, или stateless протоколы, например, использующие UDP, могут быть нарушены.

Если маршрутизатор NAT не настроен для поддержки таких протоколов, входящие пакеты не могут достичь своего адресата;

Настройка статического NAT (Static NAT)

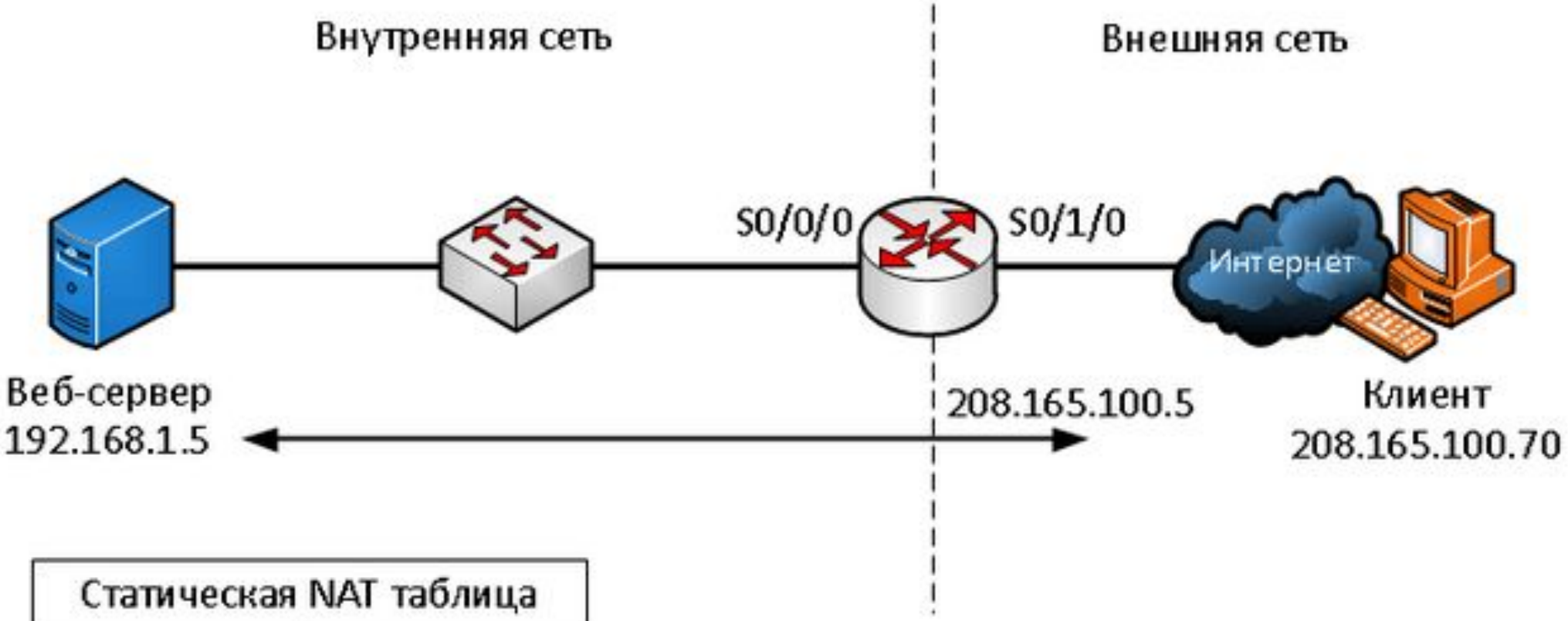
Настройка статического NAT (Static NAT)

Статический NAT представляет собой сопоставление внутреннего и внешнего адреса один к одному.

Он позволяет внешним устройствам инициировать подключения к внутренним с использованием статически назначенного общего адреса.

Внутренний веб-сервер может быть сопоставлен с определенным внутренним глобальным адресом, чтобы он был доступен из внешних сетей.

Настройка статического NAT (Static NAT)



Статическая NAT таблица	
Inside Global	Inside Local
208.165.100.5	192.168.1.5

Настройка статического NAT (Static NAT)

На схеме показана внутренняя сеть, содержащая веб-сервер с частным адресом IPv4.

Маршрутизатор сконфигурирован со статическим NAT, чтобы позволить устройствам из внешней сети обращаться к веб-серверу.

Клиент из внешней сети обращается к веб-серверу с использованием общедоступного IPv4-адреса.

Статический NAT переводит общедоступный IPv4-адрес в частный.

Настройка статического NAT (Static NAT)

При настройке статических трансляций NAT выполняются две основные задачи:

1. Создание сопоставления между внутренним локальным (**inside local**) адресом и внутренними глобальными (**inside global**) адресами. Например, внутренний локальный адрес 192.168.1.5 и внутренний глобальный адрес 208.165.100.5 на схеме настроены как статическая NAT трансляция.
2. После того как сопоставление настроено, интерфейсы, участвующие в трансляции должны быть настроены как внутренние (**inside**) и наружные (**outside**) относительно NAT. На схеме интерфейс маршрутизатора Serial 0/0/0 является внутренним, а Serial 0/1/0 – внешним.

Настройка статического NAT (Static NAT)

Пакеты, поступающие на внутренний интерфейс маршрутизатора **Serial 0/0/0** из настроенного внутреннего локального адреса **IPv4 (192.168.1.5)**, транслируются и затем перенаправляются во внешнюю сеть.

Пакеты, поступающие на внешний интерфейс **Serial 0/1/0**, адресованные настроенному внутреннему глобальному адресу **IPv4 (208.165.100.5)**, переводятся на внутренний локальный адрес **(192.168.1.5)** и затем перенаправляются внутрь сети.

Настройка статического NAT (Static NAT)

Настройка проходит в несколько шагов:

1. Создать статическую трансляцию между внутренним локальным и внешним глобальным адресами. Для этого используем команду **ip nat inside source static [локальный _IP глобальный_IP]**. Чтобы удалить трансляцию нужно ввести команду **no ip nat inside source static**. Если нам нужно сделать трансляцию не адреса в адрес, а адреса в адрес интерфейса, то используется команда **ip nat inside source static [локальный _IP тип_интерфейса номер_интерфейса]**.
2. Определим внутренний интерфейс. Сначала зайти в режим конфигурации интерфейса, используя команду **interface [тип номер]** и ввести команду **ip nat inside**.
3. Таким же образом определить внешний интерфейс, используя команду **ip nat outside**.

Настройка статического NAT (Static NAT)

Пример:

```
Router(config)# ip nat inside source static 192.168.1.5 208.165.100.5
Router(config)# interface serial0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)# interface serial0/1/0
Router(config-if)#ip nat outside
```

Настройка статического NAT (Static NAT)

В результате трансляции будут проходить так:

1. Клиент хочет открыть соединение с веб-сервером. Он отправляет пакет на веб-сервер, используя общедоступный IPv4-адрес назначения 208.165.100.5. Это внутренний глобальный адрес веб-сервера.

2. Первый пакет, который роутер получает от клиента на внешнем интерфейсе NAT, заставляет его проверять свою таблицу NAT. Адрес IPv4 адресата находится в таблице NAT он транслируется.

3. Роутер заменяет внутренний глобальный адрес назначения 208.165.100.5 внутренним локальным 192.168.1.5 и пересылает пакет к веб-серверу.

Настройка статического NAT (Static NAT)

4. Веб-сервер получает пакет и отвечает клиенту, используя внутренний локальный адрес источника 192.168.1.5.

5. Роутер получает пакет с веб-сервера на свой внутренний интерфейс NAT с адресом источника внутреннего локального адреса веб-сервера, 192.168.1.5. Он проверяет NAT таблицу для перевода внутреннего локального адреса во внутренний глобальный, меняет адрес источника с 192.168.1.5 на 208.165.100.5 и отправляет его из интерфейса Serial 0/1/0 в сторону клиента

6. Клиент получает пакет, и обмен пакетами продолжается. Роутер выполняет предыдущие шаги для каждого пакета.

Проверка статического NAT

Полезной командой для проверки работы NAT является команда **show ip nat translations**.

Эта команда показывает активные трансляции NAT.

Статические переводы, в отличие от динамических переводов, всегда находятся в таблице NAT.

```
Router#show ip nat translations
Pro   Inside global   Inside local  Outside local    Outside global
---   208.165.100.5    192.168.1.5  208.165.100.70      208.165.100.70
```

Проверка статического NAT

Другой полезной командой является команда **show ip nat statistics**. Она отображает информацию об общем количестве активных переводов, параметрах конфигурации NAT, количестве адресов в пуле и количестве адресов, которые были выделены.

```
Router#show ip nat statistics

Total active translations: 1 (1 static, 0 dynamic; 0 extended)

Peak translations: 2, occurred 00:00:21 ago

Outside interfaces:

   Serial0/1/0

Inside interfaces:

   Serial0/0/0

Hits:7 Misses:0
```

Проверка статического NAT

Чтобы убедиться, что трансляция NAT работает, лучше всего очистить статистику из любых прошлых переводов, используя команду **clear ip nat statistics** перед тестированием.

Настройка динамического NAT (Dynamic NAT)

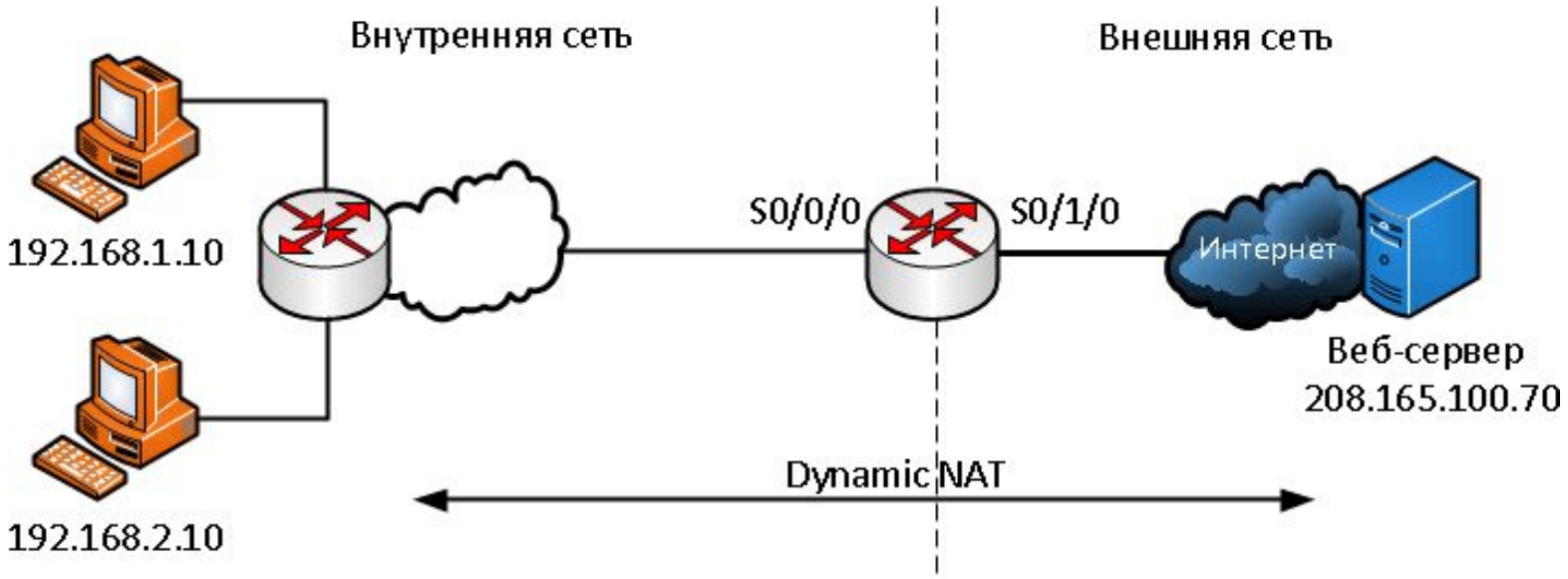
Настройка динамического NAT (Dynamic NAT)

В то время пока статический NAT постоянное сопоставление между внутренним локальным и внутренним глобальным адресом, динамический NAT позволяет автоматически сопоставлять внутренние локальные и глобальные адреса (которые обычно являются публичными IP-адресами).

Динамический NAT использует группу или пул публичных адресов IPv4 для перевода.

Динамический NAT, как и статический NAT, требует настройки внутреннего и внешнего интерфейсов, участвующих в NAT.

Настройка динамического NAT (Dynamic NAT)



NAT Pool	
Inside Local Address Pool	Inside Local Address Pool
208.165.100.5	192.168.1.10
208.165.100.6	192.168.2.10
208.165.100.7	Available
...	...
208.165.100.15	Available

Настройка динамического NAT (Dynamic NAT)

Рассмотрим на примере этой схемы.

Видим внутреннюю сеть с двумя подсетями 192.168.1.0/24 и 192.168.2.0/24 и пограничным маршрутизатором, на котором настроен динамический NAT с пулом публичных адресов 208.165.100.5 - 208.165.100.15.

Пул публичных адресов (**inside global address pool**) доступен для любого устройства во внутренней сети по принципу «первым пришел – первым обслужили».

Настройка динамического NAT (Dynamic NAT)

С динамическим NAT один внутренний адрес преобразуется в один внешний адрес.

При таком типе перевода должно быть достаточно адресов в пуле для одновременного предоставления для всех внутренних устройств, которым необходим доступ к внешней сети.

Если все адреса в пуле были использованы, то устройство должно ждать доступного адреса, прежде чем оно сможет получить доступ к внешней сети.

Настройка динамического NAT (Dynamic NAT)

Рассмотрим настойку по шагам:

1. Определить пул которые будут использоваться для перевода, используя команду **ip nat pool [имя начальный_ip конечный_ip]**. Этот пул адресов обычно представляет собой группу публичных общедоступных адресов. Адреса определяются указанием начального IP-адреса и конечного IP-адреса пула. Ключевые слова **netmask** или **prefix-length** указывают маску.

2. Нужно настроить стандартный **access-list (ACL)**, чтобы определить только те адреса, которые будут транслироваться. Введем команду **access-list [номер_ACL] permit source [wildcard_маска]**. Про стандартные access-list'ы можно прочитать в этой статье (а про расширенные в этой). ACL который разрешает очень много адресов может привести к непредсказуемым результатам, поэтому в конце листа есть команда **deny all**.

Настройка динамического NAT (Dynamic NAT)

3. Необходимо привязать ACL к пулу, и для этого используется команду **ip nat inside source list [номер_ACL] number pool [название_пула]**. Эта конфигурация используется маршрутизатором для определения того, какие устройства (список) получают адреса (пул).

4. Определить, какие интерфейсы находятся внутри, по отношению к NAT, то есть любой интерфейс, который подключен к внутренней сети.

5. Определить, какие интерфейсы находятся снаружи, по отношению к NAT, то есть любой интерфейс, который подключен к внешней сети.

Настройка динамического NAT (Dynamic NAT)

Пример:

```
Router(config)# ip nat pool MerionNetworksPool 208.165.100.5 208.165.100.15 netmask 255.255.255.0
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 pool MerionNetworksPool
Router(config)# interface serial0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)# interface serial0/1/0
Router(config-if)#ip nat outside
```

Настройка динамического NAT (Dynamic NAT)

Как это будет работать на нашей схеме:

1. Компьютеры с адресами 192.168.1.10 и 192.168.2.10 отправляют пакеты в сторону сервера по публичному адресу 208.165.100.70

2. Маршрутизатор принимает первый пакет от хоста 192.168.1.10. Поскольку этот пакет был получен на интерфейсе, сконфигурированном как внутренний интерфейс NAT, маршрутизатор проверяет конфигурацию NAT, чтобы определить, должен ли этот пакет быть транслирован. ACL разрешает этот пакет, и роутер проверяет свою таблицу NAT. Поскольку для этого IP-адреса нет записи трансляции, роутер определяет, что исходный адрес 192.168.1.10 должен быть переведен динамически.

Настройка динамического NAT (Dynamic NAT)

Роутер выбирает доступный глобальный адрес из пула динамических адресов и создает запись перевода, 208.165.200.5. Исходный IPv4-адрес источника (192.168.1.10) является внутренним локальным адресом, а переведенный адрес является внутренним глобальным адресом (208.165.200.5) в таблице NAT. Для второго хоста 192.168.2.10 маршрутизатор повторяет эту процедуру, выбирая следующий доступный глобальный адрес из пула динамических адресов, создает вторую запись перевода - 208.165.200.6.

3. После замены внутреннего локального адреса источника в пакетах маршрутизатор перенаправляет пакет.

Настройка динамического NAT (Dynamic NAT)

4. Сервер получает пакет от первого ПК и отвечает, используя адрес назначения 208.165.200.5. Когда сервер получает пакет от второго ПК, то в ответе в адресе назначения будет стоять 208.165.200.6.

5. Когда роутер получает с адресом назначения 208.165.200.5, то он выполняет поиск в таблице NAT и переводит адрес назначения во внутренний локальный адрес 192.168.1.10 и направляет в сторону ПК. То же самое происходит с пакетом, направленным ко второму ПК.

6. Оба ПК получают пакеты, и обмен пакетами продолжается. Для каждого следующего пакета выполняются предыдущие шаги.

Проверка динамического NAT

Для проверки также используется команда **show ip nat** отображает все статические переводы, которые были настроены, и любые динамические переводы, которые были созданы трафиком.

Добавление ключевого слова **verbose** отображает дополнительную информацию о каждом переводе, включая то, как давно запись была создана и использовалась.

По умолчанию данные о переводах истекают через 24 часа, если таймеры не были переконфигурированы с помощью команды **ip nat translation timeout [время_в_секундах]** в режиме глобальной конфигурации.

Проверка динамического NAT

Чтобы очистить динамические записи до истечения времени ожидания, можно использовать команду **clear ip nat translation**.

Полезно очищать динамические записи при тестировании конфигурации NAT.

Эту команду можно использовать с ключевыми словами и переменными, чтобы контролировать, какие записи очищаются.

Конкретные записи можно очистить, чтобы не прерывать активные сеансы.

Только динамические переводы удаляются из таблицы.

Статические переводы не могут быть удалены из таблицы.

Проверка динамического NAT

Также можно использовать команду **show ip nat statistics** которая отображает информацию об общем количестве активных переводов, параметрах конфигурации NAT, количестве адресов в пуле и количестве переведенных адресов.

Поскольку у нас здесь используются листы контроля доступа ACL, то для их проверки можно использовать команду **show access-lists**.

Настройка Port Address Translation (PAT)

Настройка Port Address Translation (PAT)

PAT (также называемый **NAT overload**) сохраняет адреса во внутреннем глобальном пуле адресов, позволяя маршрутизатору использовать один внутренний глобальный адрес для многих внутренних локальных адресов.

Другими словами, один открытый IPv4-адрес может использоваться для сотен и даже тысяч внутренних частных IPv4-адресов.

Когда несколько внутренних локальных адресов сопоставляются с одним внутренним глобальным адресом, номера портов **TCP** или **UDP** каждого внутреннего узла различают локальные адреса.

Настройка Port Address Translation (PAT)

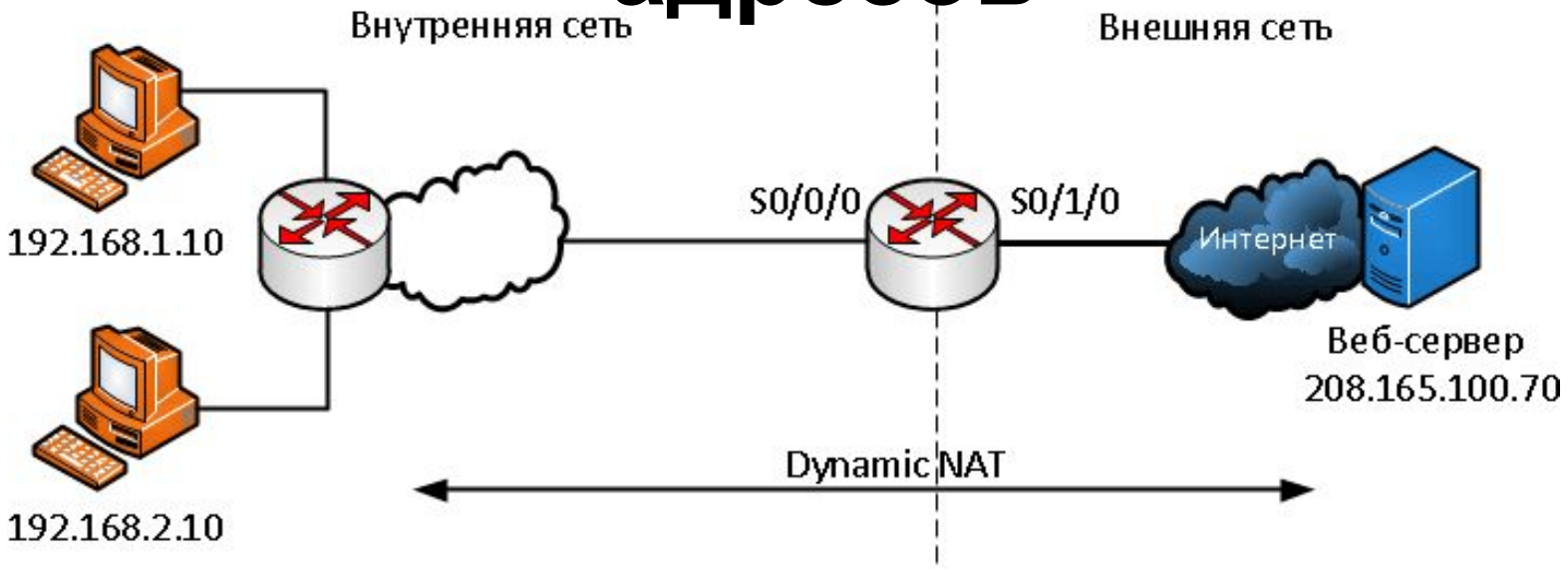
Общее количество внутренних адресов, которые могут быть переведены на один внешний адрес, теоретически может составлять 65 536 на каждый IP-адрес.

Однако на практике число внутренних адресов, которым может быть назначен один IP-адрес, составляет около 4000.

Существует два способа настройки PAT, в зависимости от того, как провайдер выделяет общедоступные IPv4-адреса.

В первом случае интернет-провайдер выделяет более одного публичного IPv4-адреса организации, а в другом он выделяет один общедоступный IPv4-адрес, который требуется для организации для подключения к интернет-провайдеру.

Настройка PAT для пула публичных IP-адресов



NAT Pool	
Inside Local Address Pool	Inside Local Address Pool
208.165.100.5	192.168.1.10
208.165.100.6	192.168.2.10
208.165.100.7	Available
...	...
208.165.100.15	Available

Настройка PAT для пула публичных IP-адресов

Если нам доступно более одного общедоступного IPv4-адреса, то эти адреса могут быть частью пула, который используется PAT.

Это похоже на динамический NAT, за исключением того, что в этом случае недостаточно общих адресов для взаимного сопоставления внутренних адресов.

Небольшой пул адресов распределяется между большим количеством устройств.

Основное различие между этой конфигурацией и конфигурацией для динамического NAT, заключается в том, что используется ключевое слово **overload**, которое включает PAT.

Настройка PAT для пула публичных IP-адресов

Рассмотрим настойку PAT для пула адресов по шагам:

1. Определить пул глобальных адресов, которые будут использоваться для PAT трансляции, используя команду **ip nat pool [имя начальный_ip конечный_ip] netmask [маска] | prefix-length [длина_префикса]**.

2. Создать стандартный **access-list**, разрешающий адреса, которые должны быть переведены.

Используется команда **access-list [номер_ACL] permit source [wildcard_маска]**.

Настройка PAT для пула публичных IP-адресов

3. Включим PAT, используя волшебное слово **Overload**.

Вводим команду **ip nat inside source list [номер_ACL] number pool [название_пула] overload**.

4. Определяем, какие интерфейсы находятся внутри, по отношению к NAT, а какие снаружи.

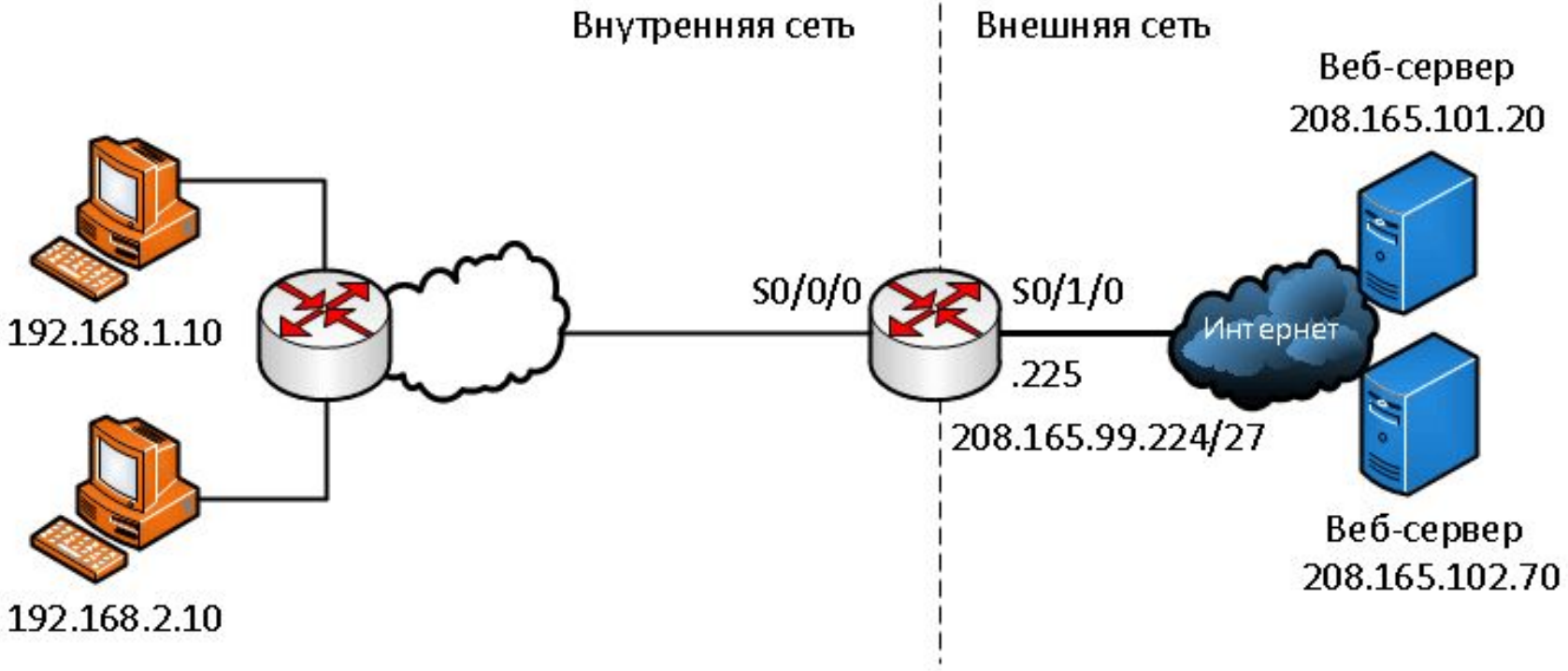
Используем команду **ip nat inside** и **ip nat outside**.

Настройка PAT для пула публичных IP-адресов

Пример настройки PAT:

```
Router(config)# ip nat pool MerionNetworksPool2 208.165.100.5 208.165.100.15 netmask 255.255.255.0
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 pool MerionNetworksPool2 overload
Router(config)# interface serial0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)# interface serial0/1/0
Router(config-if)#ip nat outside
```

Настройка PAT для одного публичного IPV4-адреса



NAT Pool			
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
208.165.200.225:1444	192.168.1.10:1444	208.165.101.20:80	208.165.101.20:80
208.165.200.225:1445	192.168.2.10:1444	208.165.102.70:80	208.165.102.70:80

Настройка PAT для одного публичного IPV4-адреса

На схеме показана топология реализации PAT для трансляции одного IP публичного адреса.

В этом примере все хосты из сети 192.168.0.0/16 (соответствующие ACL), которые отправляют трафик через маршрутизатор, будут переведены на адрес IPv4 208.165.99.225 (адрес IPv4 интерфейса S0 /1/0).

Трафик будет идентифицироваться по номерам портов в таблице NAT.

Настройка PAT для одного публичного IPV4-адреса

Настройка:

1. Создать лист access-list разрешающий адреса, которые нужно транслировать – **access-list [номер_ACL] permit source [wildcard_маска]**.

2. Настроить преобразование адреса источника в адрес интерфейса, через команду **ip nat inside source list [номер_ACL] interface [тип номер] overload**

3. Определить внешние и внутренние интерфейсы через команды **ip nat inside** и **ip nat outside**.

Настройка PAT для одного публичного IPV4-адреса

Пример:

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# ip nat source list 1 interface serial0/1/0 overload
Router(config)# interface serial0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)# interface serial0/1/0
Router(config-if)#ip nat outside
```

Настройка PAT для одного публичного IPV4-адреса

Процесс PAT не изменятся при использовании одного адреса, или пула адресов.

Рассмотрим процесс PAT по шагам:

1. На схеме два разных ПК связываются с двумя разными веб-серверами.

Первый ПК имеет адрес источника 192.168.1.10 и использует TCP порт 1444, а второй ПК имеет адрес источника 192.168.2.10 и по совпадению использует то же TCP порт 1444

Настройка PAT для одного публичного IPV4-адреса

2. Пакет с первого ПК сначала достигает роутера и он, используя PAT, изменяет исходный IPv4-адрес на 208.165.99.225 (**inside global address**).

В таблице NAT нет других устройств с портом 1444, поэтому PAT использует тот же номер порта и пакет отправляется в направлении сервера по 208.165.101.20.

Настройка PAT для одного публичного IPV4-адреса

4. Далее пакет со второго компьютера поступает в маршрутизатор, где PAT настроен на использование одного глобального IPv4-адреса для всех переводов - 208.165.99.225.

Подобно процессу перевода для первого ПК, PAT изменяет исходящий адрес второго ПК на внутренний глобальный адрес 208.165.99.225.

Однако второй ПК имеет тот же номер порта источника, что и текущая запись PAT первого ПК, поэтому PAT увеличивает номер порта источника до тех пор, пока он не станет уникальным в своей таблице.

Настройка PAT для одного публичного IPV4-адреса

В этом случае запись исходного порта в таблице NAT и пакет для второго ПК получает 1445 порт.

Хотя оба ПК используют один и тот же внутренний глобальный адрес 208.165.99.225 и тот же номер порта источника – 1444, измененный номер порта для второго ПК (1445) делает каждую запись в таблице NAT уникальной.

Это станет очевидным при отправке пакетов с серверов обратно клиентам.

Настройка PAT для одного публичного IPV4-адреса

4. Сервера отвечают на запросы от компьютеров, и используют исходный порт из принятого пакета в качестве порта назначения и исходный адрес как адрес назначения. Может казаться, что они общаются одним и тем же хостом по адресу 208.165.99.225, однако, это не так – они имеют разные порты.

5. Когда пакеты возвращаются на роутер, он находит уникальную запись в своей таблице NAT с использованием адреса назначения и порта назначения каждого пакета. В случае пакета от первого сервера адрес назначения 208.165.99.255 имеет несколько записей, но только одну с портом назначения 1444. Используя эту запись в своей таблице, роутер изменяет адрес IPv4 адресата пакета на 192.168.1.10, не меняя порт назначения. Затем пакет перенаправляется на первый ПК

Настройка PAT для одного публичного IPV4-адреса

6. Когда пакет от второго сервера прилетает на маршрутизатор, он выполняет аналогичный перевод.

Адрес IPv4 назначения 208.165.99.225 имеет несколько записей, однако используя порт назначения 1445, роутер может однозначно идентифицировать запись трансляции.

Адрес IPv4 назначения будет изменен на 192.168.2.10 и в этом случае порт назначения также должен быть изменен до исходного значения 1444, которое хранится в таблице NAT.

После этого пакет высылается на второй ПК.

Контрольные вопросы

1. Назовите

Список литературы:

1. Беленькая М. Н., Малиновский С. Т., Яковенко Н. В. Администрирование в информационных системах. Учебное пособие. - Москва, Горячая линия - Телеком, 2011.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санк-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санк-Петербург, 2003.

Список ссылок:

http://polpoz.ru/umot/lokalenaya-sete-ooo-nadejnij-kontakt/10.png
https://wiki.merionet.ru/images/nat-na-palcax-chto-eto/1.PNG
https://wiki.merionet.ru/images/nat-na-palcax-chto-eto/2.PNG
https://wiki.merionet.ru/images/nat-na-palcax-chto-eto/3.PNG
https://wiki.merionet.ru/images/nat-na-palcax-chto-eto/4.PNG
https://wiki.merionet.ru/images/nat-na-palcax-chto-eto/5.PNG
https://wiki.merionet.ru/images/nat-na-palcax-chto-eto/6.PNG
https://wiki.merionet.ru/images/nastrojka-nat-na-cisco/1.PNG
https://wiki.merionet.ru/images/nastrojka-nat-na-cisco/2.PNG
https://wiki.merionet.ru/images/nastrojka-nat-na-cisco/3.PNG

Благодарю за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru