Министерство науки и высшего образования Российской Федерации

Калужский филиал
федерального государственного бюджетного образовательного
учреждения высшего образования
**«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»**
(КФ МГТУ им. Н.Э. Баумана)

Е.В.Красавин

Домашняя работа по дисциплине «Компьютерные сети и интернет технологии»: учебное пособие

Калуга – 2024

УДК 004.62
ББК 32.972.1
Б435

Рецензенты:

Доцент кафедры «Системы обработки информации» КФ МГТУ им. Н.Э.Баумана канд. техн.наук, доц. В.О.Трешневская

Исполнительный директор АО «Биметалл», доктор техн.наук В.В.Прасицкий

Утверждено Методической комиссией КФ МГТУ им.Н.Э.Баумана (протокол №__ от _____ г., рег. Номер ___/_____)

Красавин Е.В

Домашняя работа по дисциплине «Компьютерные сетии интернет технологии»: учебное пособие / Е.В.Красавин – Калуга: КФ МГТУ им. Н.Э.Баумана, 2024. -57 с.

В учебном пособии приведены теоретические сведения и характеристика исходных данных для выполнения домашней работы, рекомендации по их выполнению, требования к оформлению, рекомендуемые источники информации.

Учебное пособие предназначено для студентов КФ МГТУ им. Н.Э.Баумана, обучающихся по направлению подготовки 09.03.04 «Программная инженерия».

Оглавление

ВВЕДЕНИЕ

Настоящая домашняя работа составлена в соответствии с программой проведения лабораторных работ по дисциплине «Компьютерные сети и интернет технологии» на кафедре «Программное обеспечение ЭВМ, информационные технологии» факультета информатики и управления Калужского филиала МГТУ им. Н.Э. Баумана.

Домашняя работа предназначена для студентов 4-го курса направления подготовки 09.03.04 «Программная инженерия» и содержит цели и задачи домашней работы, основные теоретические сведения, дается описание порядка выполнения и методические указания, приведены контрольные вопросы и форма отчета по домашней работе.

Выполнение домашней работы позволит студентам получить и закрепить знания, умения и навыки, достижения которых является результатом освоения дисциплины «Компьютерные сети и интернет технологии».

ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ВЫПОЛНЕНИИ ЛАБОРАТОРНЫХ РАБОТ

При выполнении домашних работ необходимо руководствоваться требованиями Инструкции по охране труда для пользователей персональных компьютеров (ПК) ИОТ 020-2018.

ОПИСАНИЕ ВИРТУАЛНОЙ ЛАБОРАТОРИИ CISCO PACKET TRACER

Cisco Packet Tracer – это симулятор телекоммуникационных сетей, он позволяет строить работоспособные модели сети, настраивать маршрутизаторы и коммутаторы (преимущественно производства фирмы Cisco Systems), в произвольных топологиях с поддержкой разных протоколов. В симуляторе реализованы серии маршрутизаторов Cisco 800, 1800, 1900, 2600, 2800, 2900 и коммутаторов Cisco Catalyst 2950, 2960, 3560, а также межсетевой экран ASA 5505. Беспроводные устройства представлены маршрутизатором Linksys WRT300N, точками доступа и сотовыми вышками. Кроме того, есть серверы DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP и EMAIL, рабочие станции, различные модули к компьютерам и маршрутизаторам, IP-фоны, смартфоны, хабы, а также облако, эмулирующее глобальные сети. Объединять сетевые устройства можно с помощью различных типов кабелей, таких как прямые и обратные патч-корды, оптические и коаксиальные кабели, последовательные кабели и телефонные пары.

Cisco Packet Tracer позволяет создавать довольно сложные макеты сетей, что зачастую нереально сделать на реальном оборудовании, проверять на работоспособность топологии. Однако, реализованная функциональность устройств ограничена и не предоставляет всех возможностей реального оборудования, но зато приспособлена для понимания основных концепций устройства вычислительных сетей.

Вы можете официально скачать и использовать Cisco Packet Tracer бесплатно. Вам нужна учетная запись Cisco Network Academy для загрузки и использования Cisco Packet Tracer. Вы можете создать учетную запись Cisco Network Academy бесплатно.

В Packet Tracer 7 добавлена функция аутентификации пользователей. Пользователь Сетевой академии должен выполнить вход при первом запуске Packet Tracer. Пользователи без учетной записи Сетевой академии смогут сохранять топологии не более трех раз.

Пользователь без учетной записи Сетевой академии может нажать кнопку гостевого входа, чтобы записаться на бесплатный курс для самостоятельного изучения «Введение в Packet Tracer» и получить учетную запись netacad.com для полного доступа к Packet Tracer. Курс «Введение в Packet Tracer» поможет вам ознакомиться с основными функциями Packet Tracer.

Чтобы создать учетную запись Cisco Network Academy, перейдите на страницу https://www.netacad.com/ru/courses/packet-tracer/introduction-packet-tracer из любого веб-браузера по вашему выбору, и вы должны увидеть следующую страницу. Теперь нажмите «Зарегистрируйтесь уже сегодня!», чтобы загрузить Packet Tracer.

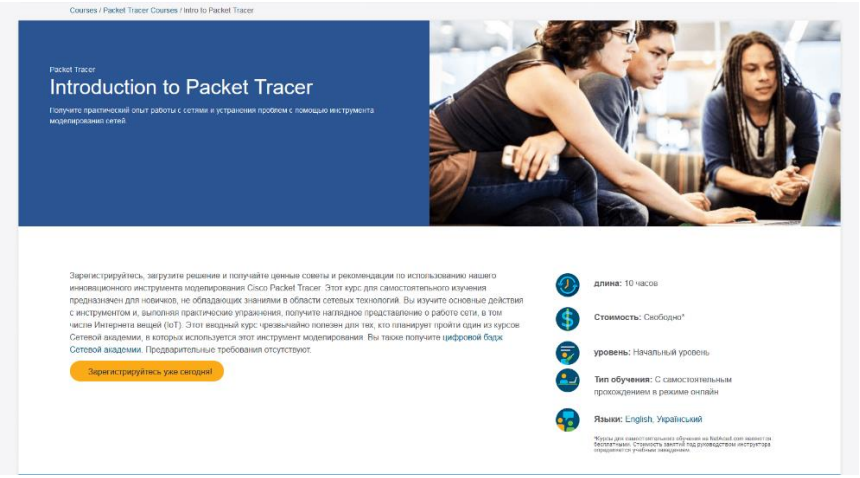


Рис. 1. Окно создания учетной записи

В выпадающем меню нужно нажать кнопку English. Должна открыться страница регистрации. Заполните данные и нажмите Отправить, как показано на скриншоте ниже.

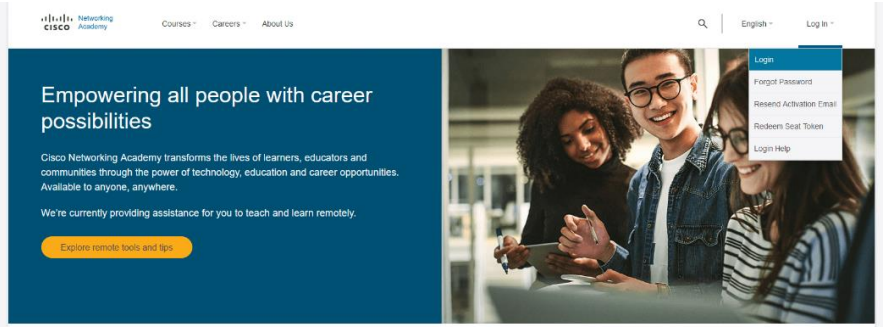


Рис.2. Окно создания учетной записи

После того как вы зарегистрировались и подтвердили свою учетнуюзапись, перейдите по адресу https://www.netacad.com/, и вы должны увидеть следующую страницу. Нажмите Log In -> Login, как видно на скриншоте.

После того как вы зашли, нужно нажать в верхнем меню Resource ->Download Packet Tracer.

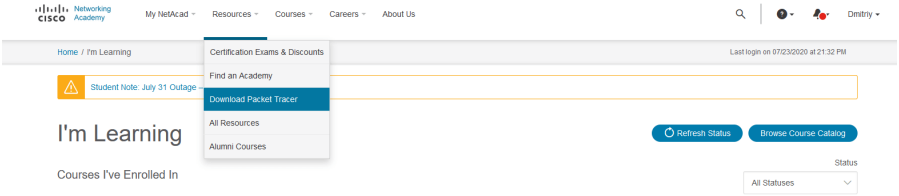


Рис.3. Окно загрузки

На этой странице в разделе Downloads нужно выбрать и скачать необходимую версию - для Windows, Linux, MacOS, Android или iOS.

Рис.4. Окно выбора версии

Устанавливаем и запускаем. При первом запуске мы увидим окно где нужно еще раз залогиниться под учетной записью netacad. Чтобы войти без учетной записи нужно нажать кнопку Guest Login в правом нижнем углу и подождать окончания таймера, после чего нажать кнопку Confirm Guest.

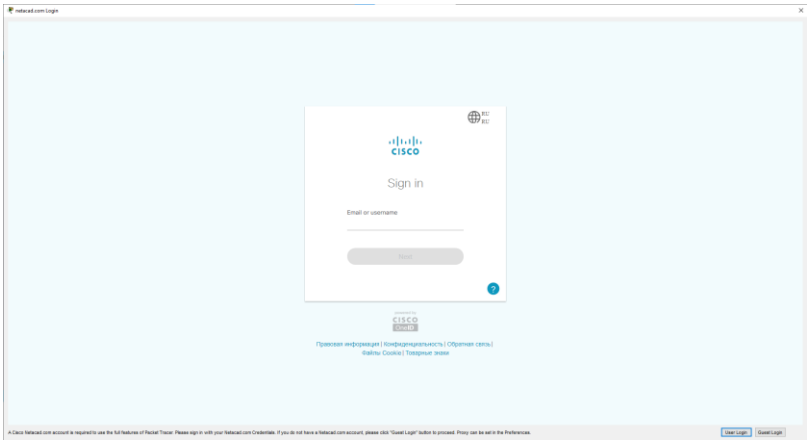


Рис.5. Окно авторизации

Можно начинать работать.

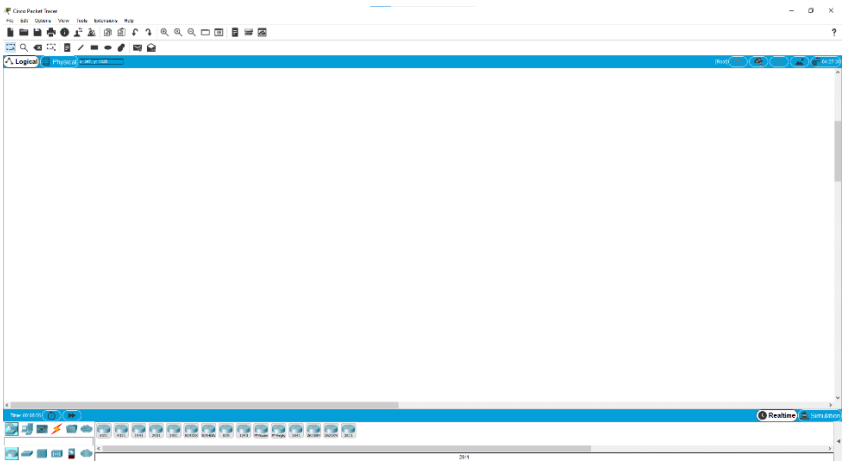


Рис.6. Окно программы

Окно программы и его структура представлены ниже.

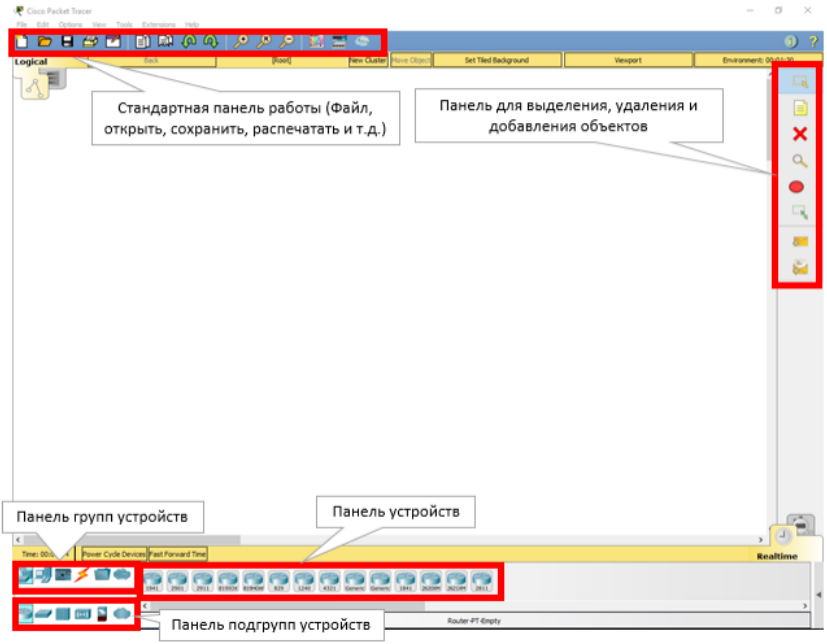


Рис.7. Элементы интерфейса

ЦЕЛИ И ЗАДАЧИ ДОМАШНЕЙ РАБОТЫ

Целью выполнения лабораторной работы является формирование практических навыков работы с сетевыми адаптерами.

Основными задачами выполнения лабораторной работы являются:

- Создание компьютерной сети в рабочей области логической топологии
- Настраивание на компьютерах и локальном сервере ip-адресов
- Создание сегментов локальной сети посредством vlan на коммутаторе и sub-интерфейсов на маршрутизаторе
- Подключение локальной сети к провайдеру
- Настройка перегруженного NAT
- Настройка access-листа
- Настройка статического NAT

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

СОЗДАНИЕ КОМПЬЮТЕРНОЙ СЕТИ В РАБОЧЕЙ ОБЛАСТИ ЛОГИЧЕСКОЙ ТОПОЛОГИИ

NAT — технологии трансляции сетевых адресов, позволяющей узлам из частной сети прозрачным для пользователей образом получать доступ к узлам внешней сети.

Что такое NAT

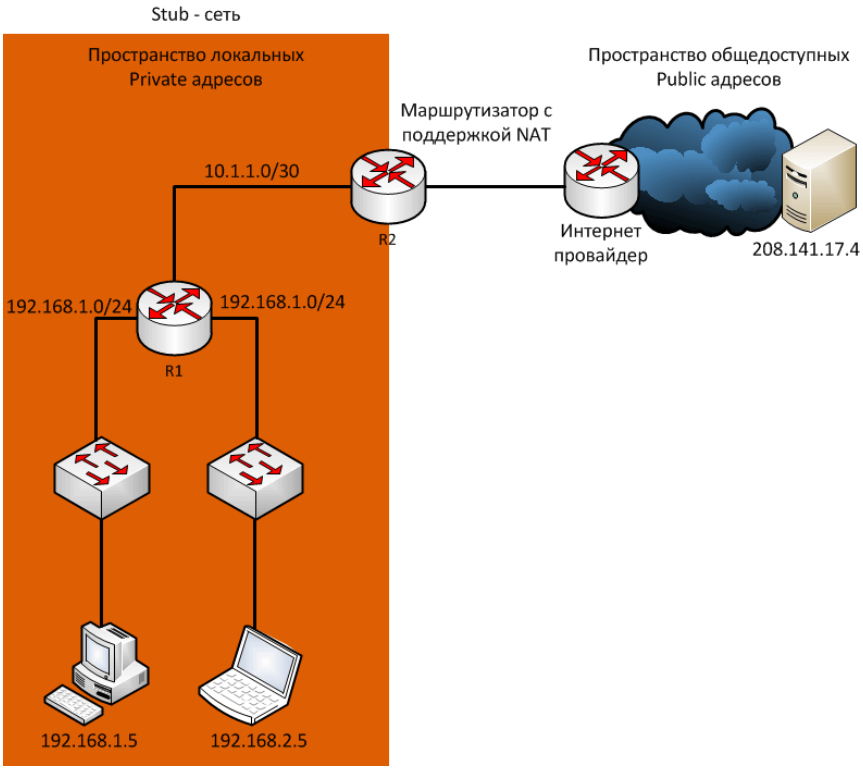
Сети обычно проектируются с использованием частных IP адресов. Это адреса 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. Эти частные адреса используются внутри организации или площадки, чтобы позволить устройствам общаться локально, и они не маршрутизируются в интернете. Чтобы позволить устройству с приватным IPv4-адресом обращаться к устройствам и ресурсам за пределами локальной сети, приватный адрес сначала должен быть переведен на общедоступный

публичный адрес.

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.

Маршрутизаторы с поддержкой NAT могут быть настроены с одним или несколькими действительными общедоступными IPv4-адресами. Эти общедоступные адреса называются пулом NAT. Когда устройство из 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.

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, и он выполняет NAT-процесс, переводя внутренний частный адрес устройства на публичный, внешний, маршрутизируемый адрес.

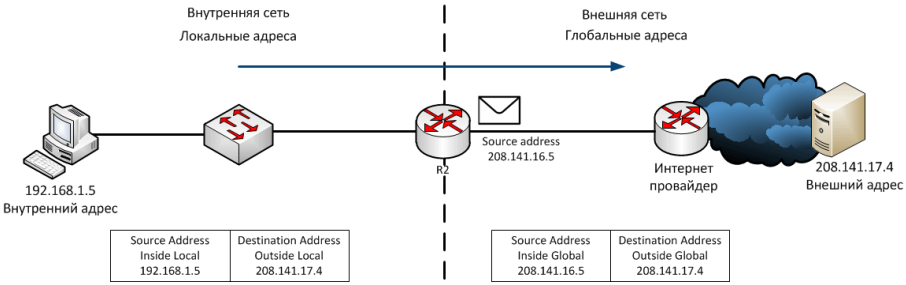
В терминологии NAT внутренняя сеть представляет собой набор сетей, подлежащих переводу. Внешняя сеть относится ко всем другим сетям.

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);

Рассмотрим это на примере схемы.

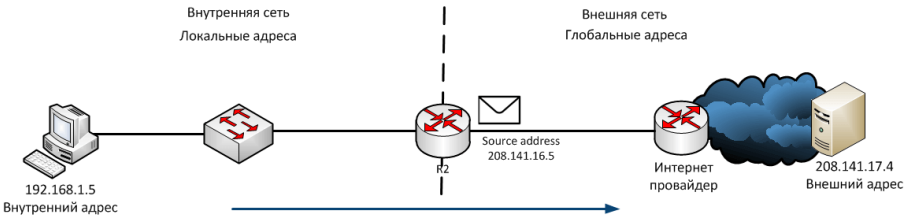


На рисунке ПК имеет внутренний локальный (**Inside local**) адрес 192.168.1.5 и с его точки зрения веб-сервер имеет внешний (**outside**) адрес 208.141.17.4. Когда с ПК отправляются пакеты на глобальный адрес веб-сервера, внутренний локальный (**Inside local**) адрес ПК транслируется в 208.141.16.5 (**inside global**). Адрес внешнего устройства обычно не переводится, поскольку он является общедоступным адресом IPv4.

Стоит заметить, что ПК имеет разные локальные и глобальные адреса, тогда как 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.

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



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

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.

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

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

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**;

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. Статический NAT особенно полезен для веб-серверов или 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.

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

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.

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

Port Address Translation (PAT)

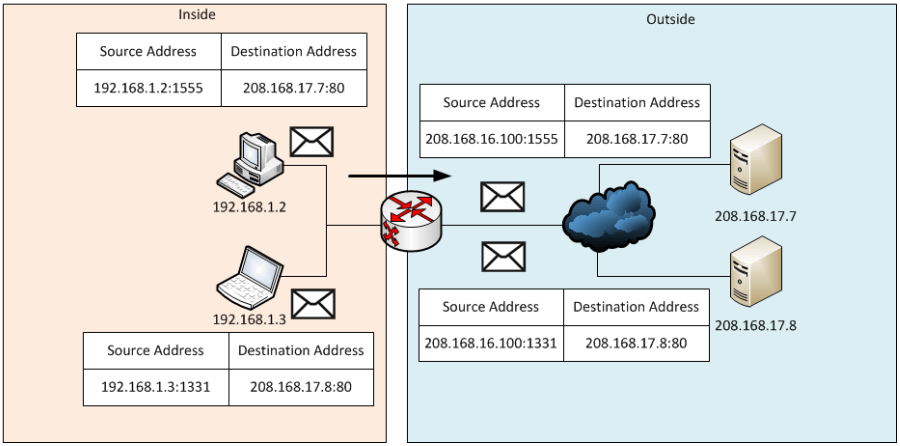
PAT транслирует несколько частных адресов на один или несколько

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.

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. 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, какое устройство маршрутизатор перенаправляет пакеты.

Картинка 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



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.

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 хорошая вероятность того, что эти номера портов уже были

прикреплены к другим активным сеансам. 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.

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.

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 подключений;
- NAT обеспечивает согласованность для внутренних схем адресации сети. В сети, не использующей частные IPv4-адреса и NAT, 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;

- 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;

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;
- 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;
- 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;
- 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;

Для создания списка правил, запрещающих или разрешающих использование ресурсов сети: доступа к интернету, телефонии, видеосвязи и т.д. используется Access Control List (ACL). ACL работает с IP-пакетами, но может узнать тип конкретного пакета, проанализировать порты TCP (Transmission Control Protocol) и UDP (User Datagram Protocol)

Access Control List или ACL — список управления доступом, который определяет, кто или что может получать доступ к объекту, и какие именно операции разрешено или запрещено выполнять субъекту. Списки контроля доступа являются основой систем с избирательным управлением доступа

ACL может работать с разнообразными протоколами локальных сетей: AppleTalk, а также IP и IPX (internetwork packet exchange). Для фильтрации такого трафика ACL работает на стыке, когда оборудование граничит с локальной сетью и интернетом, то есть когда необходимо «почистить» трафик от ненужных данных.

Разновидности ACL

Существует рефлексивный, динамический и ограниченный по времени ACL. Рассмотрим каждый из них подробнее.

Динамический (Dynamic ACL)

С его помощью можно реализовать следующее:

- предположим, у администратора есть маршрутизатор, имеющий подключение к определенному серверу;
- стоит задача закрыть доступ этому маршрутизатору из глобальной сети, но сохранить при этом к ней доступ небольшой группе людей;
- администратор выполняет настройку списка с правилами по предоставлению доступа;
- этот список устанавливается на входящее направление;
- клиенты локальной сети, которым необходимо подключиться, используют Telnet (teletype network) – сетевой протокол для реализации текстового терминального интерфейса по сети;
- в итоге, Dynamic ACL открывает доступ к серверу, и клиент может на него зайти, к примеру, через HTTP (HyperText Transfer Protocol – протокол передачи гипертекста).

Согласно настройкам по умолчанию, спустя определенное время, доступ снова закрывается, и для входа необходимо подключаться повторно. Ограниченный по времени (Time-based ACL)

Стандартный ACL, открывающий доступ в определенное «окно времени». Задать это «окно» может администратор, используя специальное расписание, активирующее/закрывающее списки доступа. К примеру, можно запретить HTTP-доступ к интернету на протяжении всего рабочего дня. А сразу после его окончания открывать доступ.

Рефлексивный (Reflexive ACL)

Подразумевается, что через частную сеть открыт узел, который отправляет TCP-запрос в глобальную сеть и в то же время ждет TCP-ответа. То есть, канал в это время должен быть открытым для исходящих пакетов данных, чтобы установилось соединение. Если канал будет закрытым, подключиться не удастся, и злоумышленники

смогут проникнуть в локальную сеть с целью воровства данных.

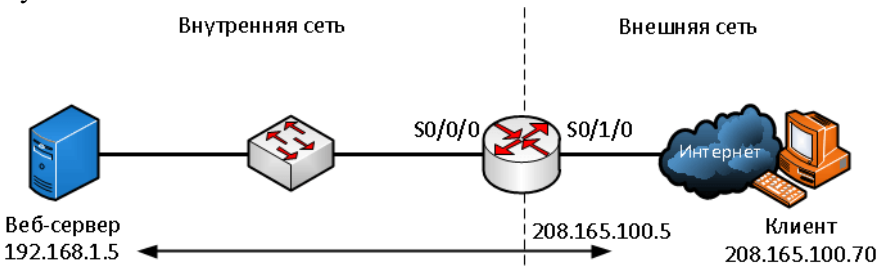
Рефлексивные ACL полностью блокируют доступ (deny any), но формируют дополнительный ACL, способный распознавать параметры пользовательских сессий, которые были сгенерированы из локальной сети. На основе этих параметров ACL открывает им доступ.

В итоге получается, что из глобальной сети подключиться к локальной не смогут, а сгенерированная группа пользователей сможет получать ответы.

Настройка статического NAT (Static NAT)

Напомним, что 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.

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



Статическая NAT таблица	
Inside Global	Inside Local
208.165.100.5	192.168.1.5

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.

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.

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 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**

```
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
```

В результате трансляции будут проходить так:

1. Клиент хочет открыть соединение с веб-сервером. Клиент 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.
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
```

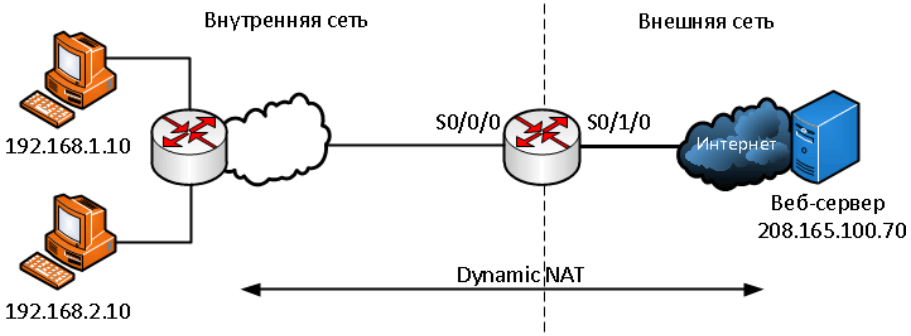
Другой полезной командой является команда **show ip nat statistics**. Она отображает информацию об общем количестве активных переводов, параметрах конфигурации NAT, количестве адресов в пуле и количестве адресов, которые были выделены.

```
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
```

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)

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.



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

Рассмотрим на примере этой схемы. Мы тут имеем 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». 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.

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**.
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.

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
```

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. R2 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.
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.

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.

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)

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.

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

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.

Рассмотрим настойку PAT для пула адресов по шагам:

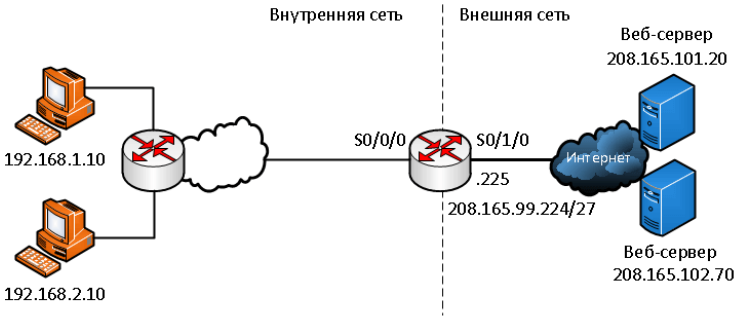
1. Определить пул адресов глобальных адресов, которые будут использоваться для PAT трансляции, используя команду **ip nat pool [имя начальный_ip конечный_ip] netmask [маска] | prefix-length [длина_префикса]**.
2. Создать стандартный access-list, разрешающий адреса, которые должны быть переведены. Используется команда **access-list [номер_ACL] permit source [wildcard_маска]**.

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**

Пример настройки для схемы, что использовалась ранее, только теперь мы будем использовать 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

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:

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**.

Конфигурация похожа на динамический NAT, за исключением того, что вместо пула адресов мы используем адрес интерфейса с вешним IP адресом. NAT пул не определяется.

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
```

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
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.

3. 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. 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.
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
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

Проверка Port Address Translation (PAT)

Для проверки PAT используются такие же команды, что и для обычного NAT. Команда **show ip nat translations** отображает переводы IP адресов вместе с портами и команда **show ip nat statistics** показывает информацию о количестве и типе активных переводов, параметрах конфигурации NAT, количестве адресов в пуле и количестве выделенных адресов.

```
Router#show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:07 ago
Outside interfaces:
        Serial0/1/0
Inside interfaces:
        Serial0/0/0
Hits:4 Misses:0
CEF Translated packets: 4, CEF Punted packets:0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool MerionNetworksPool2 refcount 2
pool MerionNetworksPool2: netmask 255.255.255.0
        start 208.165.100.5 end 208.165.100.15
        type generic, total addressers 10, allocated 1(10%),
misses 0
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Также для поиска проблем можно использовать дебаг, который запускается командой **debug ip nat**, который отображает информацию о каждом пакете, который транслируется маршрутизатором. Также можно использовать команду **debug ip nat detailed**, которая генерирует описание каждого пакета. Эта команда также предоставляет информацию о различных ошибках, например, таких как неспособность выделить глобальный адрес. Однако эта команда более требовательна к ресурсам устройства.

```
Router#debug ip nat
IP NAT debugging is on
Router#
*Aug 24 16:20:331:670: NAT*: s=192.168.1.10->208.165.99.225 d=208.165.101.20 [3730]
*Aug 24 16:20:331:682: NAT*: s=208.165.101.20 d=208.165.99.225 ->192.168.1.10 [4156]
*Aug 24 16:20:331:698: NAT*: s=192.168.1.10->208.165.99.225 d=208.165.101.20 [3731]
*Aug 24 16:20:331:702: NAT*: s=192.168.1.10->208.165.99.225 d=208.165.101.20 [3732]
*Aug 24 16:20:331:710: NAT*: s=208.165.101.20 d=208.165.99.225 ->192.168.1.10 [4157]
```

В выводе используются следующие символы и значения:

- ***** (звездочка) – звездочка с NAT указывает, что перевод происходит по пути с быстрым переключением (fast-switched path). Первый пакет в разговоре всегда медленнее, остальные пакеты проходят путь с быстрым переключением.
- **s=** - IP адрес источника
- **a.b.c.d ? w.x.y.z** - это значение указывает, что адрес источника a.b.c.d переводится на w.x.y.z.
- **d=** - IP адрес назначения
- **[xxxx]** - значение в скобках - это идентификационный номер IP.

Создание компьютерной сети в рабочей области логической топологии

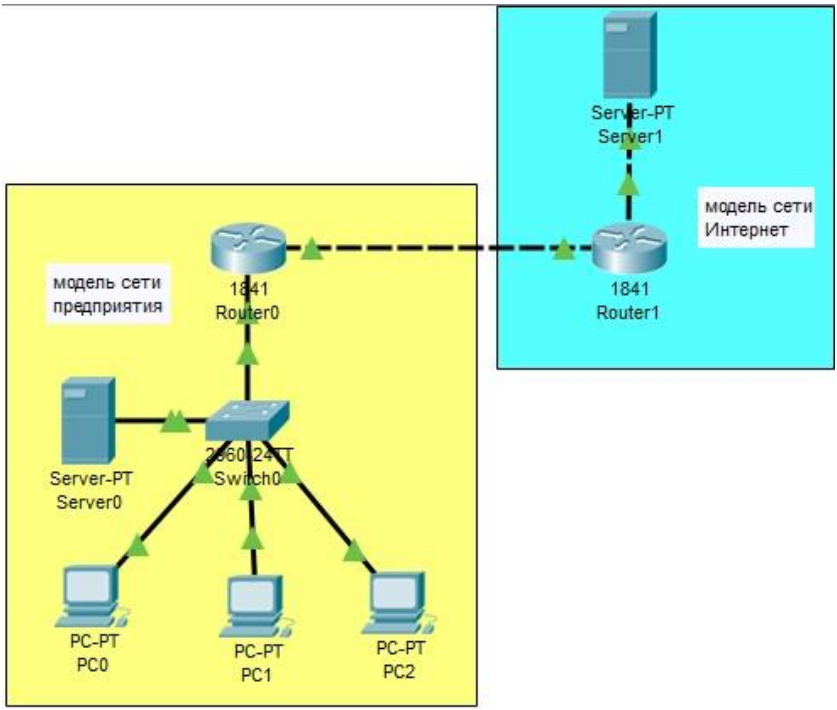


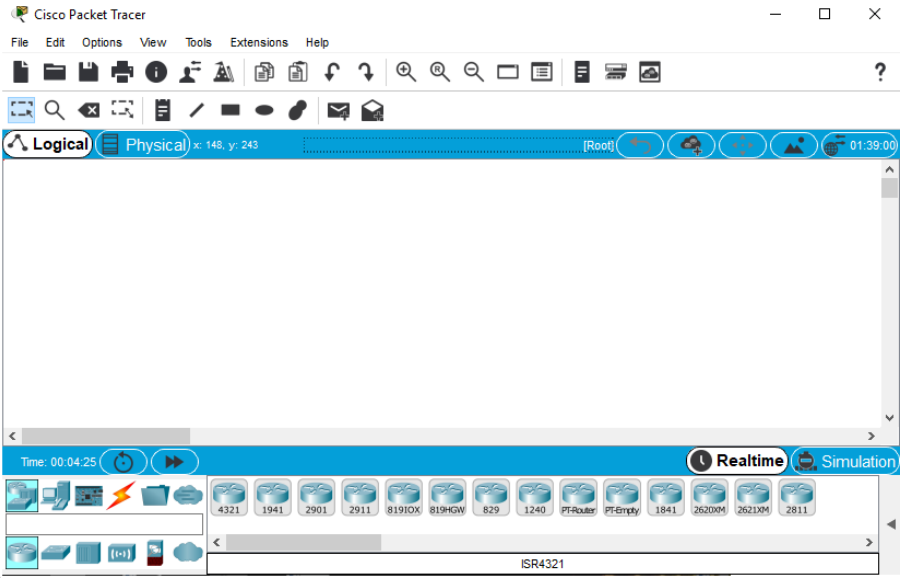
Таблица адресации

Устройство	Интерфейс	IP адрес	Маска подсети	Шлюз по умолчанию
PC0	FastEthernet0	192.168.2.2	255.255.255.0	192.168.2.1
PC1	FastEthernet0	192.168.2.3	255.255.255.0	192.168.2.1
PC2	FastEthernet0	192.168.2.4	255.255.255.0	192.168.2.1
Server0	FastEthernet0	192.168.3.2	255.255.255.0	192.168.3.1
Server1	FastEthernet0	213.234.20.2	255.255.255.252	213.234.20.1
Router0	FastEthernet0/0	213.234.10.2	255.255.255.252	213.234.10.1
	FastEthernet0/1.2	192.168.2.1	255.255.255.0	-
	FastEthernet0/1.3	192.168.3.1	255.255.255.0	-
Router1	FastEthernet0/0	213.234.10.1	255.255.255.252	-
	FastEthernet0/0	213.234.20.1	255.255.255.252	-

Запускаем Packet Tracer

а. Запустите Packet Tracer на вашем ПК или ноутбуке.

Дважды щелкните значок «Пакет трассировщика» на рабочем столе или перейдите в каталог, содержащий исполняемый файл Packet Tracer, и запустите пакетный трассировщик. Пакет Tracer должен открываться с пустой рабочей областью логической топологии по умолчанию, как показано на рисунке. Здесь я использую новую на сегодня версию программы 7.2.1., хотя можно пользоваться и старыми 🙂



Выстраиваем топологию

а. Добавьте сетевые устройства в рабочее пространство.

Используя окно выбора устройства, добавьте сетевые устройства в рабочее пространство, как показано на диаграмме топологии.

Чтобы поместить устройство в рабочую область, сначала выберите тип устройства из окна «Выбор типа устройства». Затем щелкните нужную модель устройства в окне «Выбор устройства». Наконец, нажмите на местоположение в рабочей области, чтобы поместить ваше устройство в это место. Если вы хотите отменить свой выбор, нажмите на значок «Отмена» для этого устройства. Кроме того, вы можете

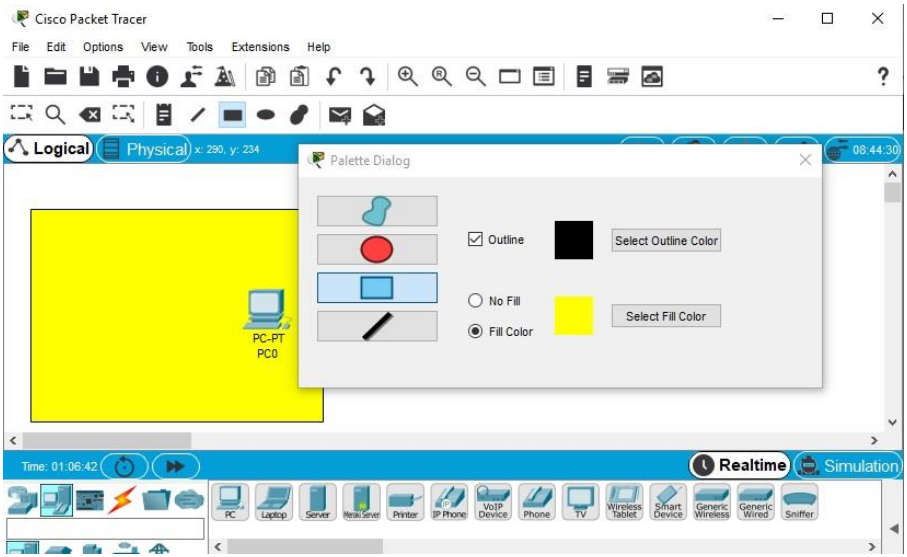
щелкнуть и перетащить устройство из окна «Выбор конкретного устройства» в рабочее пространство.

б. Добавьте сетевые устройства в рабочее пространство.

Используя поле выбора устройства, добавьте сетевые устройства в рабочее пространство, как показано на диаграмме топологии. Чтобы поместить устройство в рабочую область, сначала выберите тип устройства из окна «Выбор типа устройства». Затем щелкните нужную модель устройства в окне «Выбор устройства». Наконец, нажмите на местоположение в рабочей области, чтобы поместить ваше устройство в это место. Если вы хотите отменить свой выбор, нажмите на значок «Отмена» для этого устройства. Кроме того, вы можете щелкнуть и перетащить устройство из окна «Выбор конкретного устройства» в рабочее пространство.

с. Выделите разными цветами заливки участки компьютерной сети.

Чтобы выделить разными цветами заливки участки компьютерной сети, щелкните значок прямоугольника на панели инструментов, в появившемся диалоговом окне установите переключатель и флажок как показано на рисунке. Выберите с помощью кнопок нужный цвет границы и цвет заливки. В рабочей области Packet Tracer Logical удерживая левую кнопку мыши обведите соответствующий сегмент сети.



д. Добавить физическую проводку между устройствами в рабочей области

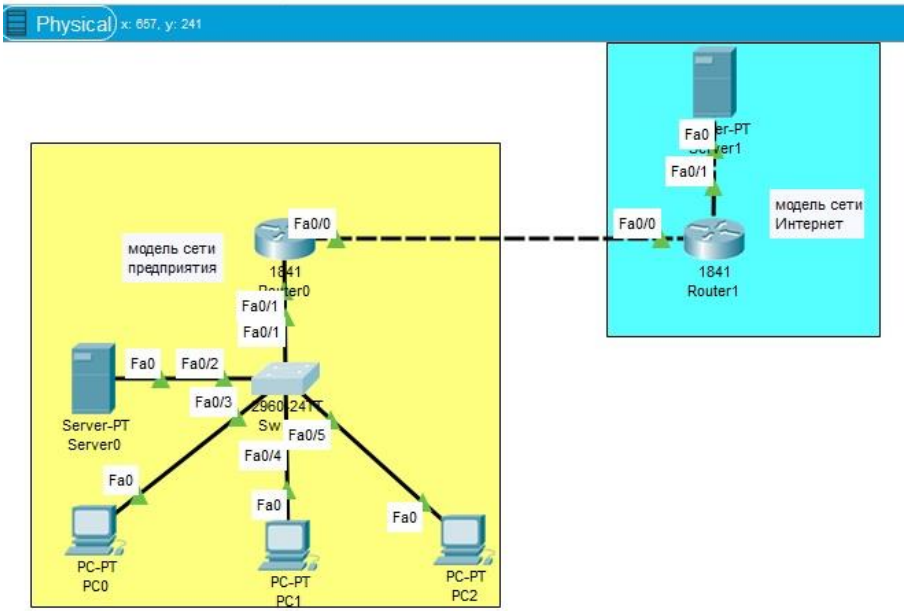
Используя поле выбора устройства, добавьте физическую проводку между устройствами в рабочей области, как показано на диаграмме топологии.

Для подключения к коммутатору ПК понадобится медный прямой кабель. Выберите **медный прямой кабель** в окне «Выбор устройства» и прикрепите его к интерфейсу FastEthernet0 на ПК (PC0) и интерфейсу FastEthernet0/3 коммутатора. Аналогичным образом прикрепите компьютер PC1 к интерфейсу FastEthernet0/4 коммутатора, компьютер PC2 к интерфейсу FastEthernet0/5 коммутатора. Сервер (Server0) прикрепите к интерфейсу FastEthernet0/2 коммутатора.

Для подключения маршрутизатора Router0 к маршрутизатору Router1 используйте **перекрёстный медный кабель**. Выберите перекрёстный медный кабель в окне «Выбор устройства» и прикрепите его к интерфейсу FastEthernet0/0 маршрутизатора Router0, а другим концом к прикрепите к интерфейсу FastEthernet0/0 маршрутизатора

R0uter1.

Для подключения к серверу (Server1) для маршрутизатора Router1 необходим медный прямой кабель. Выберите медный прямой кабель в окне «Выбор устройства» и прикрепите его к интерфейсу FastEthernet0/1 маршрутизатора и интерфейсу FastEthernet0 на сервере с именем Server1. Проверьте по рисунку правильность подключений.



Дальнейший ход лабораторной работы полностью представлен в видео:

https://www.youtube.com/watch?v=xNDYghAKQw0

1. Настроим на компьютерах и локальном сервере IP-адреса.

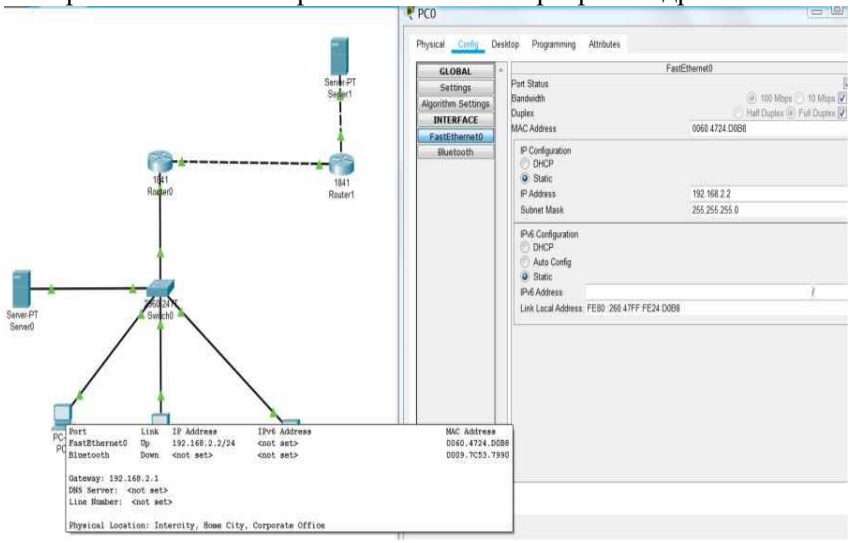


Рис. 1 Настройка IP адресов на локальных PC

Выделяем локальный сервер в отдельный сегмент:

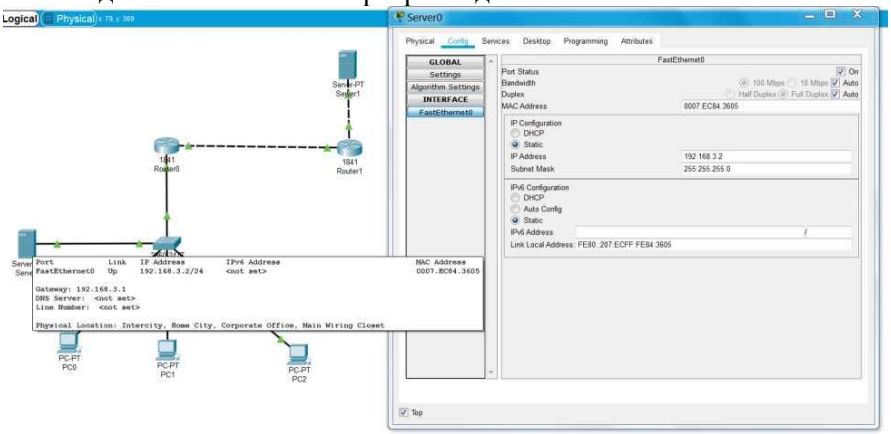


Рис. 2 Настройка IP адреса локального сервера

2. Создадим сегменты локальной сети посредством vlan на коммутаторе:

Vlan 2 - для пользовательских машин, vlan 3 для сервера.

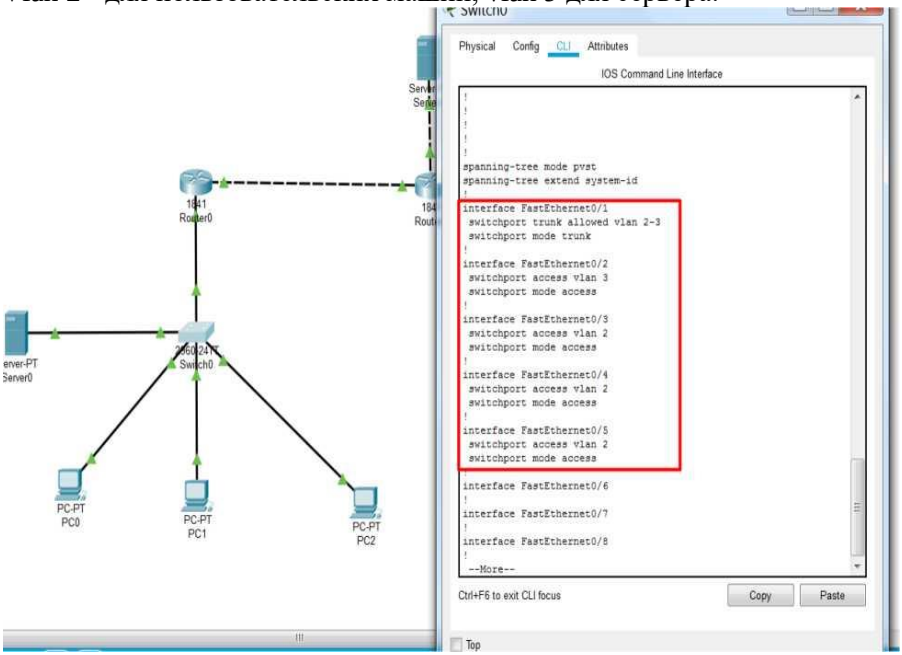


Рис.3 Создание сегментов

Теперь создадим соответствующие sub-интерфейсы для соответствующих vlan’ое на роутере.

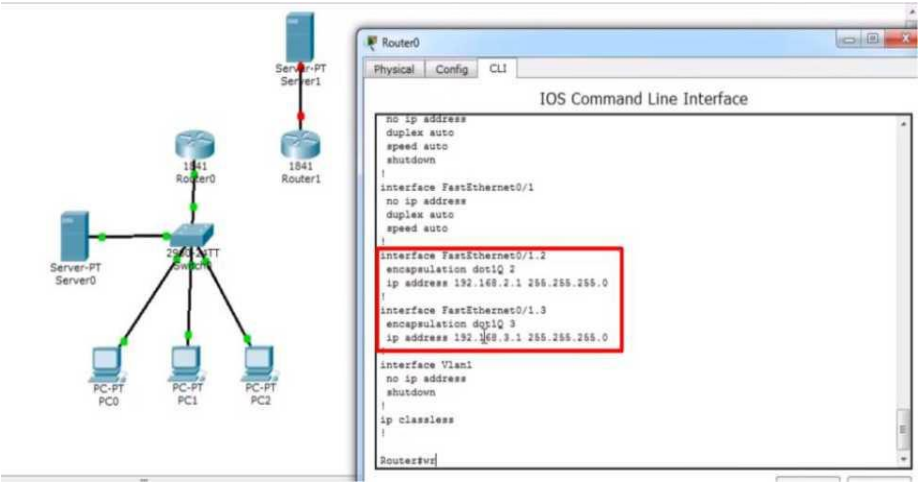


Рис. 4 Создание sub-интерфейсов

Пропингуем сервер и другой PC, чтобы убедиться, что локальная сеть настроена
правильно:

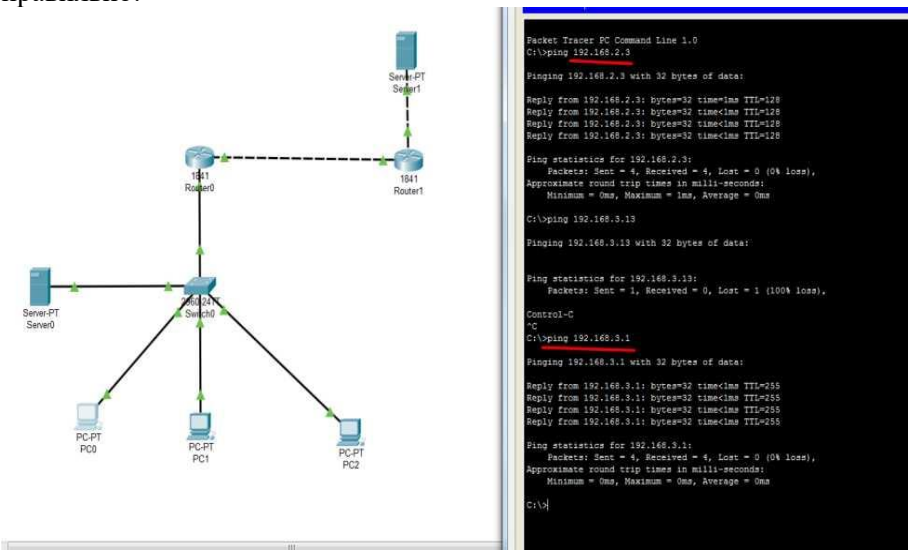


Рис. 5. Пинги в локальной сети

3. Теперь мы захотели подключить нашу локальную сеть к сети Интернет, симулировав провайдера посредством роутера и сервера, приняв, что провайдер нам выделил статический IP-адрес. Также настроим сервер.

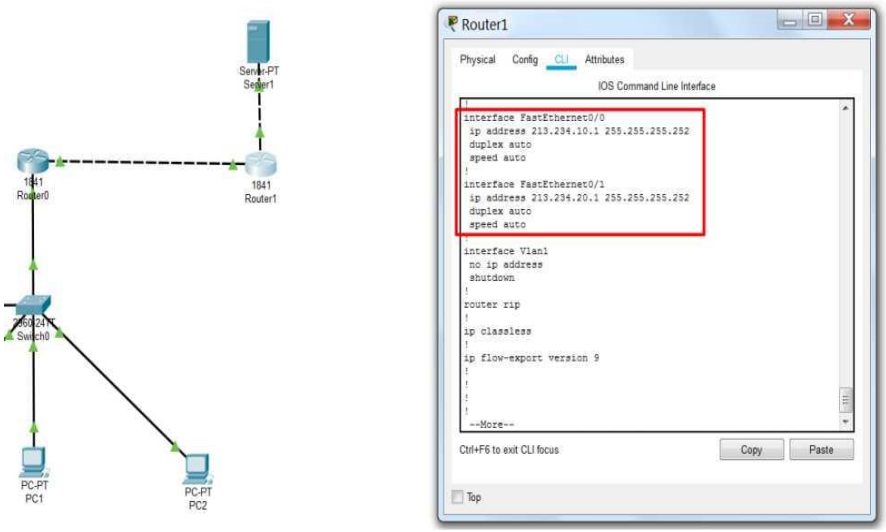


Рис. 6 Настройка роутера провайдера.

Получаем, что на роутере провайдера мы имеем: один белый IP-адрес который смотрит в сторону роутера нашей локальной сети, другой в сторону публичного сервера.

Пропишем на нашем роутере IP-адрес интернета, который нам выделил провайдер 213.234.10.2 и установим адрес шлюза провайдера.

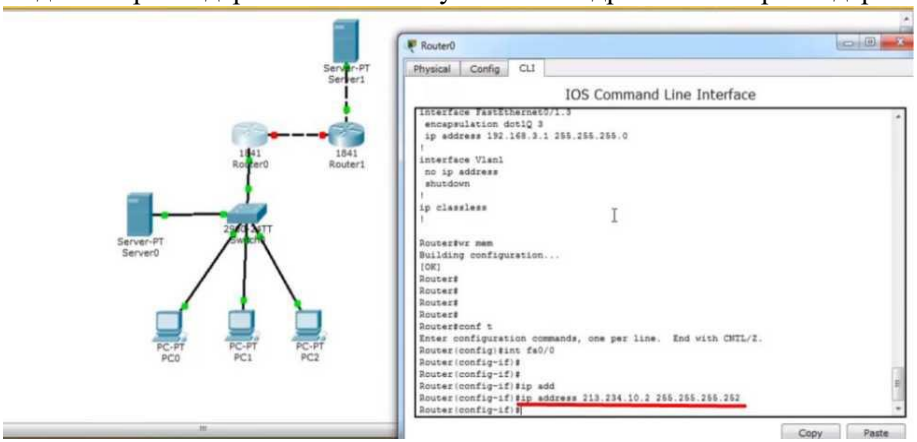


Рис. 7 Настройка IP-адреса интернета на локальном роутере

Убедимся, что наш роутер установил связь с интернет-провайдером и соответственно с публичным сервером, пропинговав их.

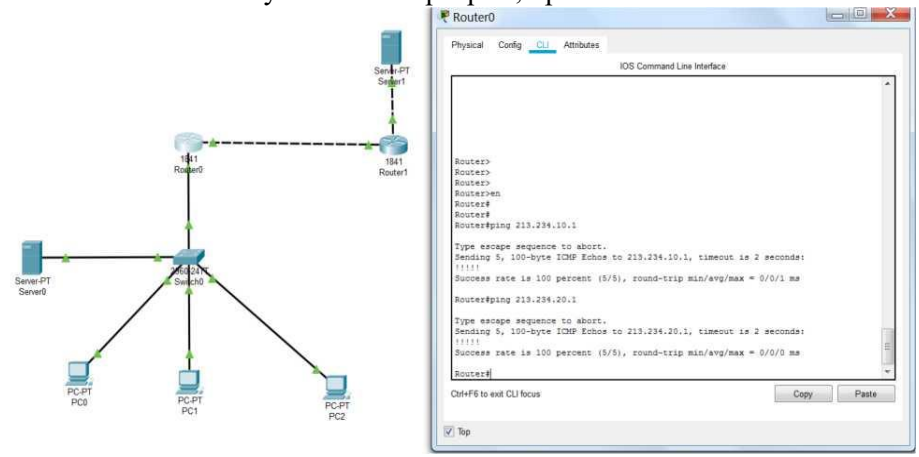


Рис.8 Пинги роутра к провайдеру и публичному серверу

Теперь попробуем связаться с публичным сервером с локального PC, пинг не пройдёт, потому что мы используем серые IP-адреса и наш роутер не знает про эту сеть.

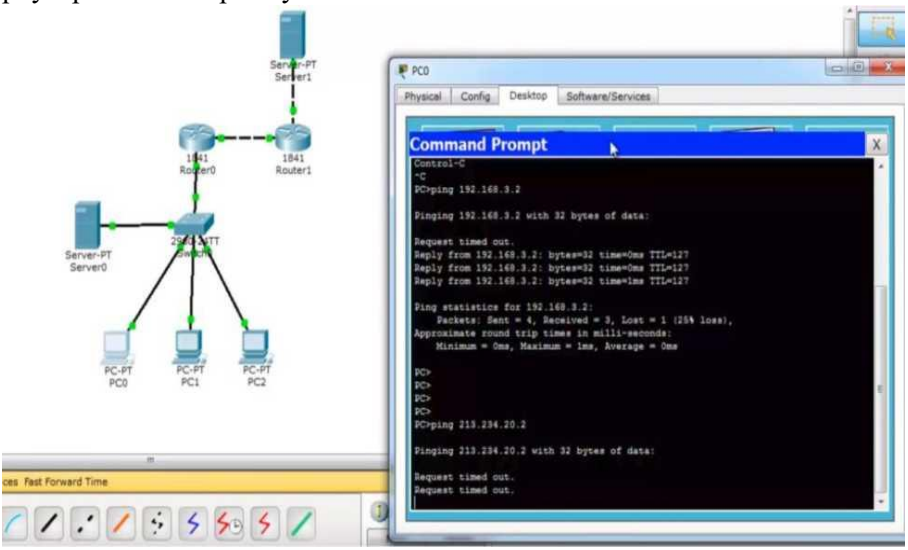


Рис. 9 Локальная сеть не видит интернет.

4. С помощью технологии NAT мы обеспечим доступ локальных компьютеров и сервера в сеть Интернет.

Для начала на локальном роутере настроим какой интерфейс будет являться для NAT внешним, а какой внутренним.

R o u t e внешний	FastEthernetO/O	213.234.10.2
	FastEthernetO/1.2	192,168.2.1
	FastEthernetO/1.3	192.168.3.1

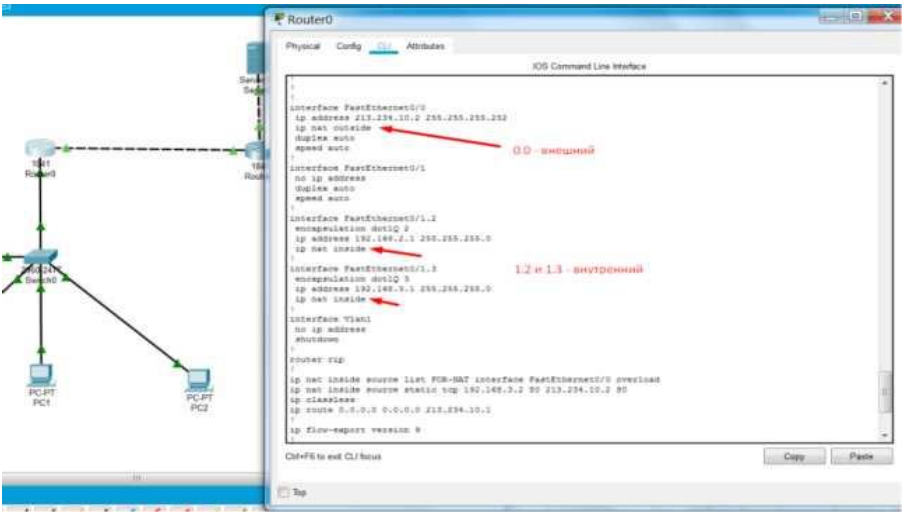


Рис. 10 Настройка NAT локального роутера.

5. Затем мы создаём access-list которые будут характеризовать, какой именно траффик мы будем «натить».

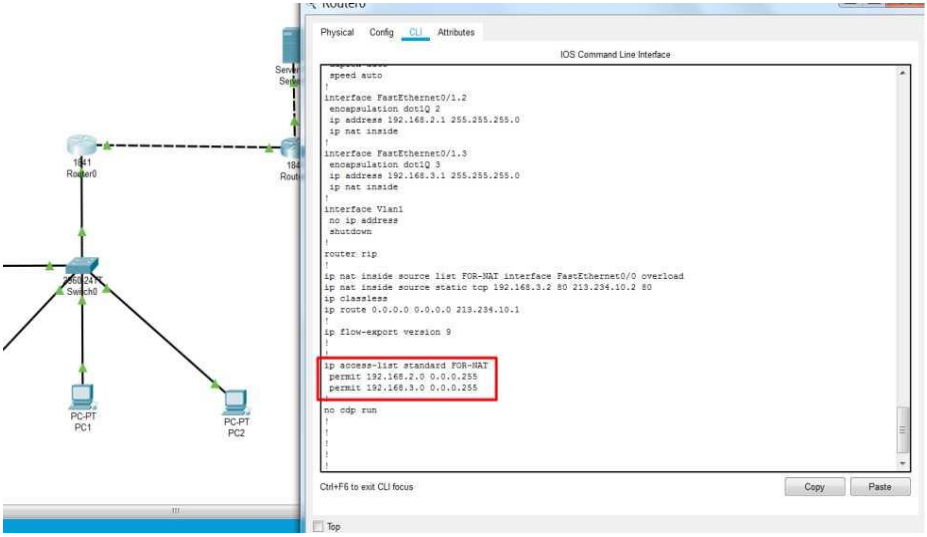


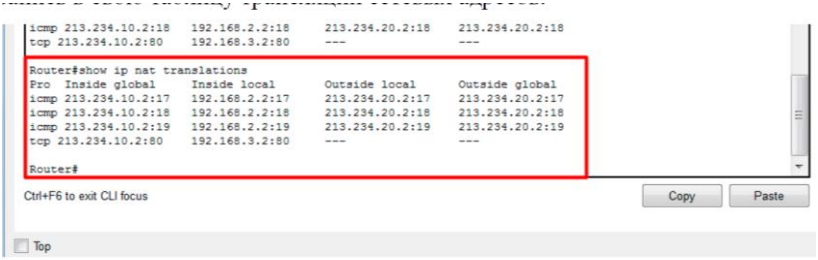
Рис. 11. Создание access-list для NAT

Последней командой ip nat inside source list FOR-NAT interface FastEthernet0/0 overload завершаем настройку роутера.

6. Как работает NAT:

Наш пользователь работает в домашней сети на хосте 192.168.2.2 и запрашивает веб-страницу с веб-сервера (порт 80) с IP-адресом 213.234.20.2. Хост 192.168.2.2 присваивает (произвольно) номер исходного порта 18 и посылает дейтаграмму в локальную сеть. NAT-маршрутизатор получает дейтаграмму, генерирует для нее новый номер исходного порта, в нашем случает такой же 18 порт, заменяет исходный IP-адрес соответствующим IP-адресом, расположенным на стороне ГВС (213.234.10.2) и заменяет старый номер исходного порта 18 новым — 18. При генерировании нового номера исходного порта NAT-маршрутизатор может выбрать любой, которого пока нет в таблице трансляции сетевых адресов. Механизм NAT в маршрутизаторе также

добавляет запись в свою таблицу трансляции сетевых адресов.



Веб-сервер, совершенно не представляющий, что прибывшая к нему дейтаграмма с HTTP-запросом уже подверглась обработке на NAT- маршрутизаторе, посылает в ответ дейтаграмму, где адрес получателя — это IP- адрес NAT-маршрутизатора, а порт назначения имеет номер 18. Когда дейтаграмма прибывает на NAT-маршрутизатор, тот делает выборку из таблицы трансляции сетевых адресов. При этом он использует целевой IP-адрес и номер порта назначения, чтобы получить подходящий IP-адрес (192.168.2.2) и номер порта назначения (18) для браузера, работающего в домашней сети. Затем маршрутизатор переписывает адрес назначения дейтаграммы и номер порта назначения и пересылает ее в домашнюю сеть.

ПОРЯДОК ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

1. Разработать модель подключения сети к одному провайдеру, настроить NAT, добавить ACL правила. Сеть создать с использованием Switch 2960 и Router 1841 при помощи CISCO PACKET TRACER:

- Активное оборудование должно быть настроено согласно

заданию

- Должны использоваться индивидуальные диапазоны IP-адресов, выделенные каждому студенту

- Сеть должна выход в интернет со всех компьютеров предприятия и доступ из интернета к локальному серверу предприятия.

- Сеть предприятия имеет адреса в формате:
  10.11.N.0;
  Локальный сервер предприятия
  10.11.N+1.2;
  где N –вариант по журналу. Маска 24.

- сеть Интернет, симулировав провайдера посредством роутера и сервера, приняв, что провайдер нам выделил статический IP-адрес
  195.111.G.92 , шлюз по умолчанию 195.111.G.91
  а адрес сервера провайдера
  195.111.G+10.92

где G –индекс группы. Маска 24

2. Ответить на контрольные вопросы и оформить отчет.

ФОРМА ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ, ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ

Отчет на защиту предоставляется в электронном или печатном виде.

Структура отчета (на отдельном листе(-ах)): титульный лист, формулировка задания, ответы на контрольные вопросы, описание процесса выполнения лабораторной работы со скриншотами, выводы.

К отчету прилагается файл с созданной сетью в формате Cisco Packet Tracer (с расширением pkt). Файл должен содержать:

- Визуальную схему сети
- Используемую в сети адресацию в виде надписей
- Сетевое и конечное оборудование в соответствии с заданием
- Линии связи между оборудованием

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

1 Классифицируйте виды NAT.
2 Опишите различия между входящим и исходящим трафиком.
3 Опишите способы применения ACL.
4 Приведите пример записи ACL.
5 Приведите способы подключения к маршрутизатору.
6 Предложите вариант настройки Static NAT.

ОСНОВНАЯ ЛИТЕРАТУРА

1. Сергеев, А.Н. Основы локальных компьютерных сетей [Электронный ресурс]: учебное пособие / А.Н. Сергеев. — Санкт-Петербург : Лань, 2016. — 184 с. – Режим доступа: URL: https://e.lanbook.com/book/87591
2. Топорков, С.С. Компьютерные сети для продвинутых пользователей [Электронный ресурс]: учебное пособие / С.С. Топорков. — Москва : ДМК Пресс, 2009. — 192 с. – Режим доступа: URL: https://e.lanbook.com/book/1170

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

3. Ачилов Р.Н. Построение защищенных корпоративных сетей [Электронный ресурс]: учебное пособие / Р.Н.Ачилов. – Москва : ДМК Пресс, 2013. – 250 с. Режим доступа: URL: https://e.lanbook.com/book/66472
4. Ибе О. Компьютерные сети и службы удаленного доступа [Электронный ресурс]: справочник / О.Ибе. - – Москва : ДМК Пресс, 2007. – 336 с. Режим доступа: URL: https://e.lanbook.com/book/1169

ЭЛЕКТРОННЫЕ РЕСУРСЫ:

5. Научная электронная библиотека http://eLIBRARY.RU
6. Электронно-библиотечная система http://e.lanbook.com
7. Компьютерные сети и технологии http://www.xnets.ru