Министерство науки и высшего образования Российской Федерации

Томский государственный университет
систем управления и радиоэлектроники

Ф. Н. Захаров, К.А. Ярков

СИСТЕМЫ БЕСПРОВОДНОЙ СВЯЗИ

Учебно-методическое пособие для практических и лабораторных работ
студентов всех форм обучения, обучающихся по техническим направлениям

Томск
2024

УДК 621.39
ББК 32.884.1
З–38

Рецензенты:
Аникин А.С., доцент кафедры радиотехнических систем,
канд. техн. наук

Захаров, Фёдор Николаевич, Ярков, Кирилл Алексеевич
З–38 Системы беспроводной связи : Учебно-методическое пособие для практических и лабораторных работ студентов всех форм обучения, обучающихся по техническим направлениям / Захаров Ф. Н., Ярков К. А. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2024 – 69 с.

Методические указания составлены с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО).

В учебно-методическом пособии рассмотрены вопросы построения беспроводных локальных сетей по стандарту IEEE 802.11 (Wi-Fi), а также ряд вопросов оптимизации работы локальных сетей. В частности, описаны технология разделения локальной сети на подсети с использованием виртуальных локальных сетей (VLAN), технология трансляции сетевых адресов (преобразование частных IP-адресов в глобальные IP-адреса) и методы повышения безопасности коммутаторов на основе анализа MAC-адресов подключенных устройств. В каждом разделе содержатся задания для практических и лабораторных работ.

Одобрено на заседании кафедры РТС, протокол № 4 от 16.11.2023

УДК 621.39
ББК 32.884.1

Оглавление

1 Введение

Многие пользователи регулярно пользуются услугами и устройствами беспроводных локальных сетей (Wireless LAN – WLAN). На текущий момент времени растёт тенденция использования портативных устройств, таких как ноутбуки, планшеты, смартфоны. Также сейчас активно развиваются концепции «умного дома», большинство устройств которого подключаются «по воздуху». В связи с этим возникла потребность беспроводного подключения во всех людных местах: на работе, дома, в гостинице, в кафе или книжном магазине. С ростом количества беспроводных устройств, которые подключаются через сеть WLAN, выросла популярность беспроводных сетей.

Ниже представлена упрощённая схема работы локальной сети коммерческого предприятия.

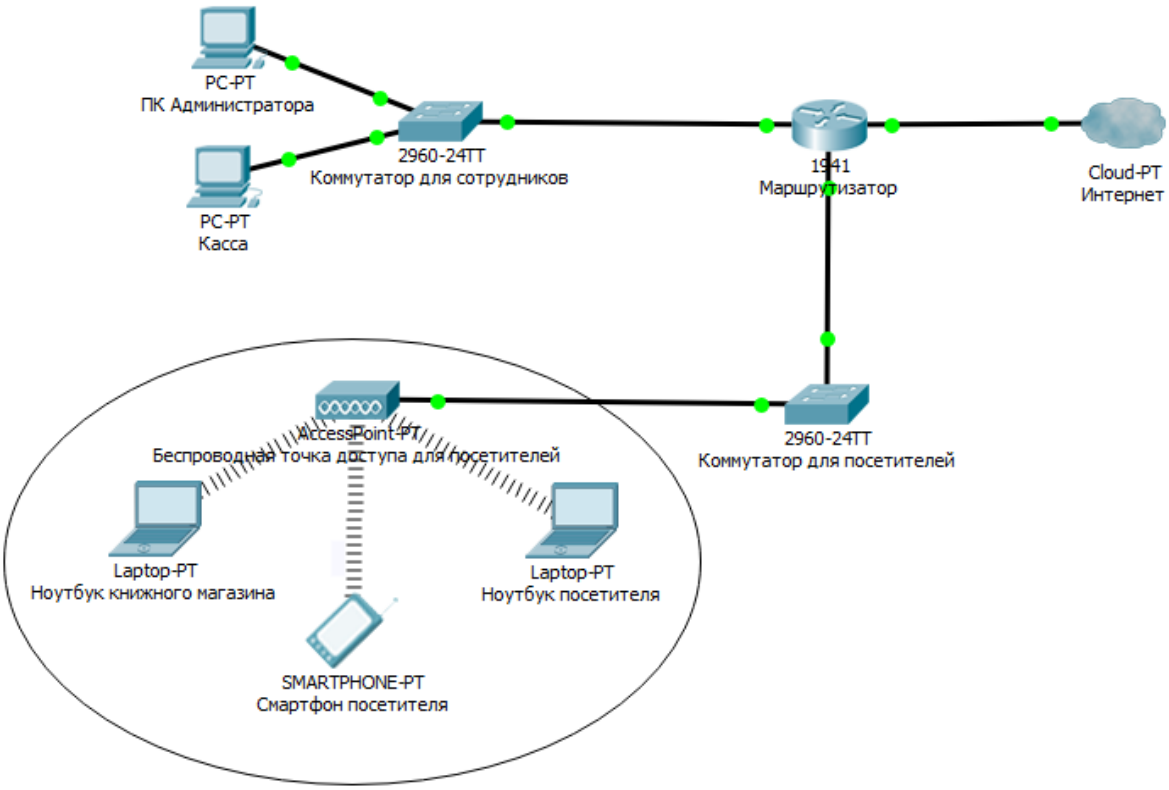


Рисунок 1 – Пример топологии локальной сети

Портативные компьютеры посетителей взаимодействуют с устройством WLAN, называемым беспроводной точкой доступа (Access Point). Точка доступа использует радиоканал для отправки и получения фреймов (отдельных, законченных HTML-документов, которые вместе с другими HTML-документами могут быть отображены в окне браузера) от клиентского устройства, например, компьютера. Кроме того, точка доступа подключена к той же сети Ethernet, что и устройства, обеспечивающие работу магазина, следовательно, и покупатели, и сотрудники могут искать информацию на дистанционных веб-сайтах.

Методические указания посвящены изучению технологий беспроводных локальных сетей по стандарту IEEE 802.11 (Wi-Fi).

2 Беспроводные локальные сети

2.1 Сравнение беспроводных локальных сетей с локальными сетями

Беспроводные локальные сети во многом похожи с локальными сетями, например, оба типа сетей позволяют устройствам взаимодействовать между собой. Для обеих разновидностей сетей работает стандарт IEEE (IEEE 802.3 для сетей Ethernet и IEEE 802.11 – для беспроводных сетей). В обоих стандартах описан формат фреймов сети (заголовок и концевик), указано, что заголовок должен иметь длину 6 байтов и содержать MAC-адреса отправителя и получателя. Оба стандарта указывают, как именно устройства в сети должны определять, когда можно передавать фрейм в среду, а когда нельзя.

Основное отличие двух типов сетей состоит в том, что для передачи данных в беспроводных сетях используется технология излучения энергии (или технология излучения радиоволн), а в сетях Ethernet используется передача электрических импульсов по медному кабелю (или импульсов света в оптическом волокне). Для передачи радиоволн не нужна специальная среда работы, обычно говорят, что «связь происходит по воздуху», чтобы подчеркнуть, что никакой физической сети не надо. В действительности любые физические объекты на пути радиосигнала (стены, металлические конструкции и т.п.) являются препятствием, ухудшающим качество радиосигнала.

2.2 Стандарты беспроводных локальных сетей

Разработкой и поддержкой стандарта 802.11 занимается комитет Wi-Fi Alliance. Термин Wi-Fi (Wireless Fidelity) используется в качестве общего имени для стандарта 802.11, а также всех последующих спецификаций, относящихся к беспроводным локальным сетям (wireless LAN).

Стандарт IEEE 802.11. активно развивается и включает в себя множество спецификаций. Стандарт 802.11a рассчитан на работу в частотном диапазоне 5 ГГц. Скорость передачи данных до 54 Мбит/с, то есть примерно в пять раз быстрее сетей 802.11b. Это наиболее широкополосный стандарт из семейства. К его недостаткам относят большую потребляемую мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (100 м). Стандарт 802.11b благодаря ориентации на диапазон 2,4 ГГц завоевал наибольшую популярность у производителей оборудования. В качестве базовой радиотехнологии в нем используется метод расширенного спектра прямого распространения DSSS (Direct Sequence Spread Spectrum), который отличается высокой устойчивостью к искажению данных, помехам, в том числе преднамеренным, а также к обнаружению. Поскольку оборудование 802.11b, работающее на максимальной скорости 11 Мбит/с, имеет меньший

радиус действия, чем на более низких скоростях, то им предусмотрено автоматическое понижение скорости при ухудшении качества сигнала. Пропускная способность (теоретическая 11 Мбит/с, реальная – от 1 до 6 Мбит/с) отвечает требованиям большинства приложений. Расстояния – до 300 м, но на практике – до 160 м.

Спецификация 802.11d устанавливает универсальные требования к физическому уровню (процедуры формирования каналов, псевдослучайные последовательности частот и т.д.). Спецификация 802.11e позволит создавать мультисервисные беспроводные сети для корпораций и индивидуальных потребителей. При сохранении полной совместимости с действующими стандартами 802.11a и 802.11b она расширяет их функциональность за счет обслуживания потоковых мультимедиа-данных и гарантированного качества услуг. Спецификация 802.11f описывает протокол обмена служебной информацией между точками доступа IAPP (Inter-Access Point Protocol). Спецификация 802.11h предусматривает возможность дополнения действующих спецификаций алгоритмами эффективного выбора частот для офисных и уличных беспроводных сетей, а также средствами управления использованием спектра, контроля излучаемой мощности и генерации соответствующих отчетов.

Стандарт 802.11g является стандартом, регламентирующим метод построения wireless LAN, функционирующих в не лицензируемом частотном диапазоне 2,4 ГГц. Максимальная скорость передачи данных в беспроводных сетях 802.11g составляет 54 Мбит/с. Оборудование, поддерживающее этот стандарт, обеспечивает одновременное подключение к сети устройств стандартов 802.11g и 802.11b, поскольку он представляет собой развитие последнего и обратно совместим с ним. В числе преимуществ 802.11g отмечается низкая потребляемая мощность, большие расстояния (до 300 м) и высокая проникающая способность сигнала.

Существует несколько технологий беспроводных сетей, использующих как радио-, так и инфракрасные волны. Основное преимущество таких сетей – возможность объединения разного оборудования.

2.3 Основные устройства и условные знаки в работе с Wi-Fi

1. Точка доступа – это беспроводной «удлинитель» проводной сети. Графическое изображение точки доступа приведено на рисунке 2.

Рисунок 2 – Графическое изображение точки доступа

2. Маршрутизатор (рисунок 3) – это более «умное» устройство, которое не просто принимает и передает данные, но и перераспределяет их согласно различным установленным правилам и выполняет заданные команды.

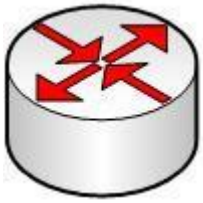


Рисунок 3 – Графическое изображение маршрутизатора

3. Облако (рисунок 4) – настроенная часть сети.

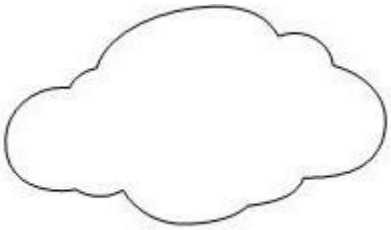


Рисунок 4 – Графическое изображение настроенной части сети

4. Wi-Fi соединение (рисунок 5).

Рисунок 5 – Графическое изображение Wi-Fi соединения

2.4 Основные способы использования Wi-Fi

Беспроводные сети могут иметь две логические топологии:

1) *Точка - точка доступа* (Infrastructure) - *звездообразная* - применяется в устройствах стандарта 802.11 b/g и RadioLAN. Здесь точка доступа (узловой передатчик) играет роль концентратора, поскольку все компьютеры соединяются через нее, а не взаимодействуют друг с другом напрямую. При

такой топологии несколько сетевых адаптеров могут быть объединены одной точкой доступа, либо несколько точек доступа соединены с одной точкой доступа. Этот режим применяется для создания локальной беспроводной сети из нескольких пользователей, для соединения этой сети с проводной сетью (например, для выхода в Интернет), для соединения между собой нескольких проводных сетей.

2) *Точка - точка* (Ad-hoc). Два сетевых адаптера либо две точки доступа соединяются между собой. Метод применяется для непосредственного соединения двух компьютеров либо при организации радио-моста между двумя проводными сетями. Эта топология используется в устройствах HomeRF (Home Radio Freqiuently – домашний радиодиапазон) и применяется в устройствах Bluetooth. Такие устройства напрямую соединяются друг с другом и не требуют никаких узловых передатчиков или других устройств, подобных концентратору, для взаимодействия друг с другом.

Способы использования Wi-Fi

1. **Wi-Fi мост** (рисунок 6) – соединение двух точек доступа по Wi-Fi.

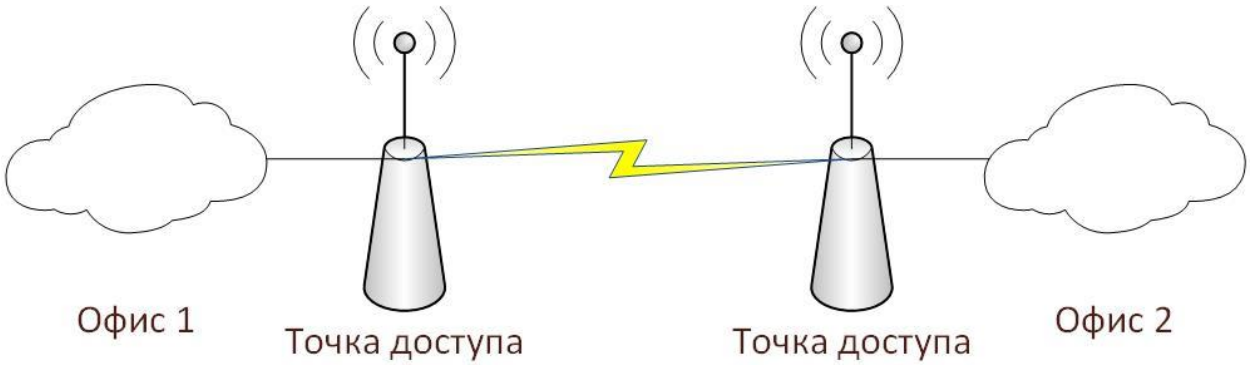


Рисунок 6 – Wi-Fi мост

2. **Wi-Fi маршрутизатор или роутер** (рисунок 7) – подключение всех устройств к роутеру по Wi-Fi (вся сеть подключена беспроводным способом).

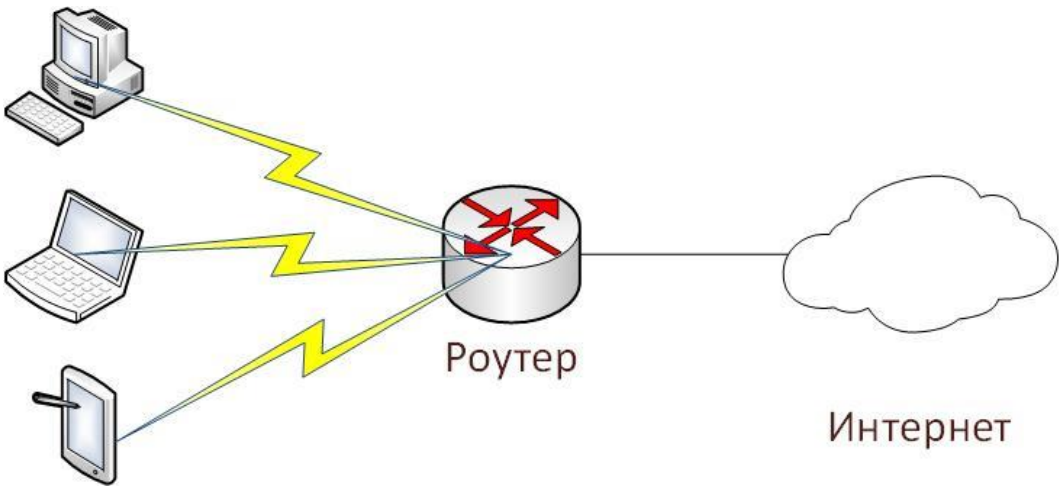


Рисунок 7 – Wi-Fi роутер

3. **Wi-Fi точка доступа** (рисунок 8) – подключение части сети для беспроводной работы.

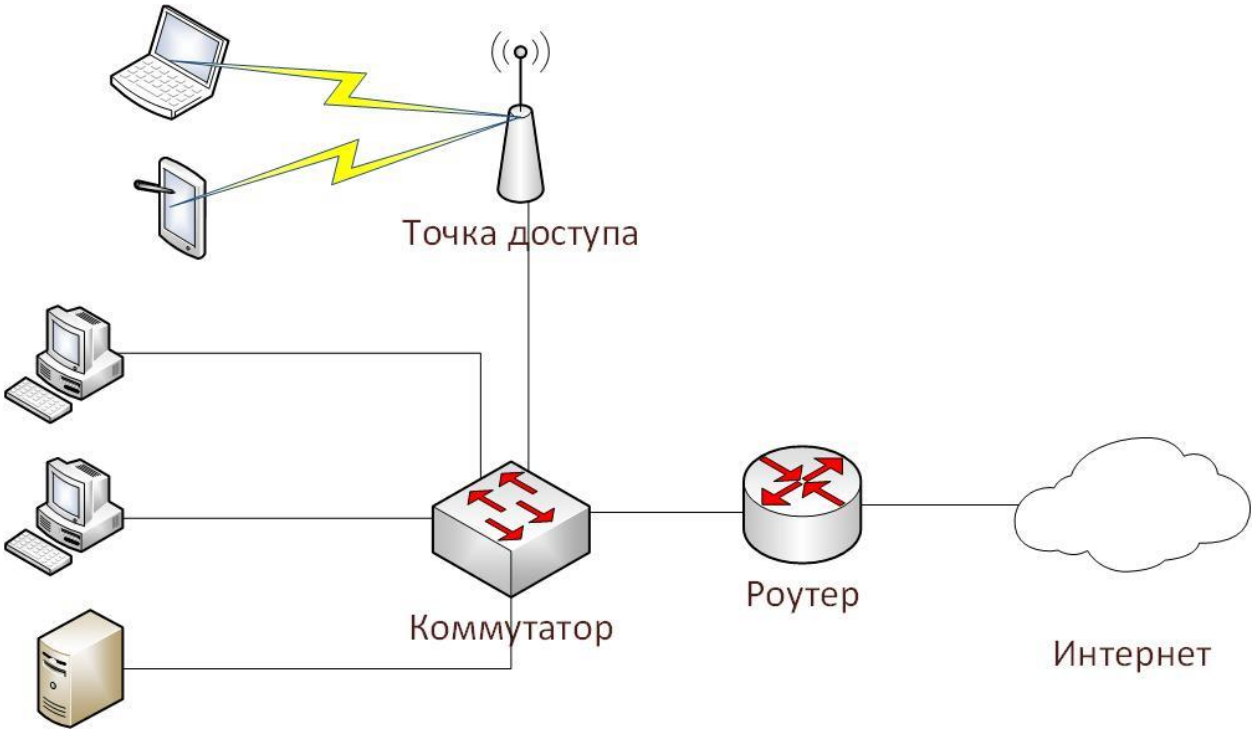


Рисунок 8 – Wi-Fi точка доступа

Таким образом, оборудование беспроводных сетей включает в себя узловые передатчики (точки беспроводного доступа Access Point) и беспроводные адаптеры для каждого абонента. Точки доступа выполняют роль концентраторов, обеспечивающих связь между абонентами и между собой, а также функцию мостов, осуществляющих связь с кабельной локальной сетью и с Интернет. Несколько близкорасположенных точек доступа образуют зону доступа Wi-Fi (Hotspot), в пределах которой все абоненты, снабженные беспроводными адаптерами, получают доступ к сети.

Метод доступа к такой сети – множественный доступ с предотвращением коллизий CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Сеть строится по сотовому принципу. В сети предусмотрен механизм роуминга, то есть поддерживается автоматическое подключение к точке доступа и переключение между точками доступа при перемещении абонентов, хотя строгих правил роуминга стандарт не устанавливает.

2.5 Сервисы Wi-Fi

Стандарт IEEE 802.11 предусматривает, что все беспроводные сети (wireless LAN) должны предоставлять девять типов сервисов (услуг). Их можно разделить на две категории: сервисы распределения (пять из девяти) и станционные (четыре сервиса).

Сервисы распределения связаны с управлением станциями, находящимися в данной соте, и взаимодействием с внешними станциями.

Станционные сервисы имеют отношение к управлению активностью внутри одной соты.

Пять сервисов распределения предоставляются базовой станцией и имеют дело с мобильностью станций при их входе в соту или выходе из нее:

1) *Ассоциация*. Используется мобильными станциями для подключения к базовым станциям (БС). Мобильная станция передает идентификационную информацию и сообщает о своих возможностях (поддерживаемой скорости передачи данных, необходимости PCF-услуг, или опроса) и требованиях по управлению электропитанием. Базовая станция может принять или отвергнуть мобильную станцию. Если последняя принята, она должна пройти идентификацию.

2) *Дизассоциация*. По инициативе мобильной или базовой станции может быть произведена дизассоциация, то есть разрыв отношений. Это требуется при выключении станции или ее уходе из зоны действия БС. Впрочем, базовая станция также может быть инициатором дизассоциации, если, например, она временно выключается для проведения технического обслуживания.

3) *Реассоциация*. С помощью этого сервиса станция может сменить БС. Очевидно, данная услуга используется при перемещении станции из одной соты в другую. Если она проходит корректно и без сбоев, то при переходе никакие данные не теряются.

4) *Распределение*. С помощью этой услуги определяется маршрутизация кадров (единицы данных, которыми обмениваются компьютеры в сети Ethernet), посылаемых базовой станции. Если адрес назначения является локальным с точки зрения БС, то кадры следуют просто напрямую (передаются в эфире). В противном случае их необходимо пересылать по проводной сети.

5) *Интеграция*. Если кадру нужно пройти через сеть, не подчиняющуюся стандарту 802.11 и использующую другую схему адресации и/или формат кадра, то на помощь приходит данный сервис. Он реализует трансляцию форматов.

Оставшиеся четыре сервиса — это внутренние услуги соты. Они предоставляются после прохождения ассоциации. Ниже перечислены станционные сервисы:

6) *Идентификация*. Поскольку беспроводные коммуникации подразумевают очень легкое подключение к сети и возможность приема/отправки данных любыми станциями, попавшими в зону действия БС, то возникает необходимость идентификации. Только после идентификации станции разрешается обмен данными. После принятия мобильной станции в ряды текущих абонентов соты базовая станция посылает специальный кадр запроса, позволяющий понять, знает ли станция присвоенный ей секретный ключ (пароль). Подтверждение осуществляется путем шифрования кадра

запроса и отсылки его назад базовой станции. Если шифрование выполнено корректно, мобильная станция получает нормальные права доступа к сети.

7) *Деидентификация*. Если станция, работавшая в сети, покидает ее, она должна произвести деидентификацию. После выполнения данного сервиса она больше не сможет использовать ячейку.

8) *Конфиденциальность*. Чтобы сохранить передаваемые по сети данные, их необходимо шифровать. Данный сервис осуществляет операции по шифрации и дешифрации информации. Применяется алгоритм RC4, изобретенный Рональдом Ривестом (Ronald Rivest).

9) *Доставка данных*. Именно этот сервис является ключевым во всей работе сети, поскольку стандарт 802.11 существует для обмена данными.

3 Настройка беспроводной сети

3.1 Практическая работа. Настройка модели сети

Создать модель локальной сети, состоящей из обычного домашнего Wi-Fi маршрутизатора и маршрутизатора, который имитирует провайдера Интернета (рисунок 9). Использовать интерфейс Fast Ethernet. Добавим ещё пользовательское устройство, например ноутбук. Установим модуль Wi-Fi (WPC300N) в ноутбук.

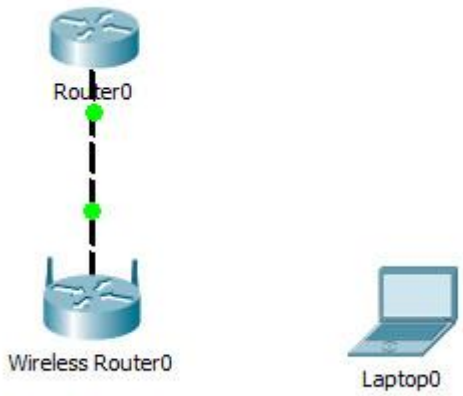


Рисунок 9 – Модель сети

1) Настройки маршрутизатора провайдера ***Router0*** (жирным выделено то, что необходимо ввести с клавиатуры:

```
Router>en
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#int fa0/0
Router (config-if)#ip address 210.210.0.1 255.255.255.252
Router (config-if)#no shutdown

Router (config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Router (config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
```

Введённые команды обозначают следующее:

1) **En** – enable. Расширенный доступ к конфигурации

2) **Conf t** – Configuration terminal. Открывает терминал настройки

3) **int fa0/0** – interface fastEthernet0/0. Переходим к настройки указанного порта (в нашем случае к fastEthernet0/0)

4) **ip address 210.210.0.1 255.255.255.252** – задаётся IP адрес и его маска. Адрес – 210.210.0.1 (допустим, это адрес нам дал провайдер), маска – /30.

5) **no shut** – no shutdown. Включить, настроенный нами, интерфейс

6) **End** – завершения настройки.

7) **wr mem** – write memory. Сохранение конфигураций.

2) Настройки домашнего Wi-Fi маршрутизатора ***Wireless Router0*** выполняется с помощью веб интерфейса.

2.1) Настройка внешнего интерфейса во вкладке Setup показана на рисунке 10.

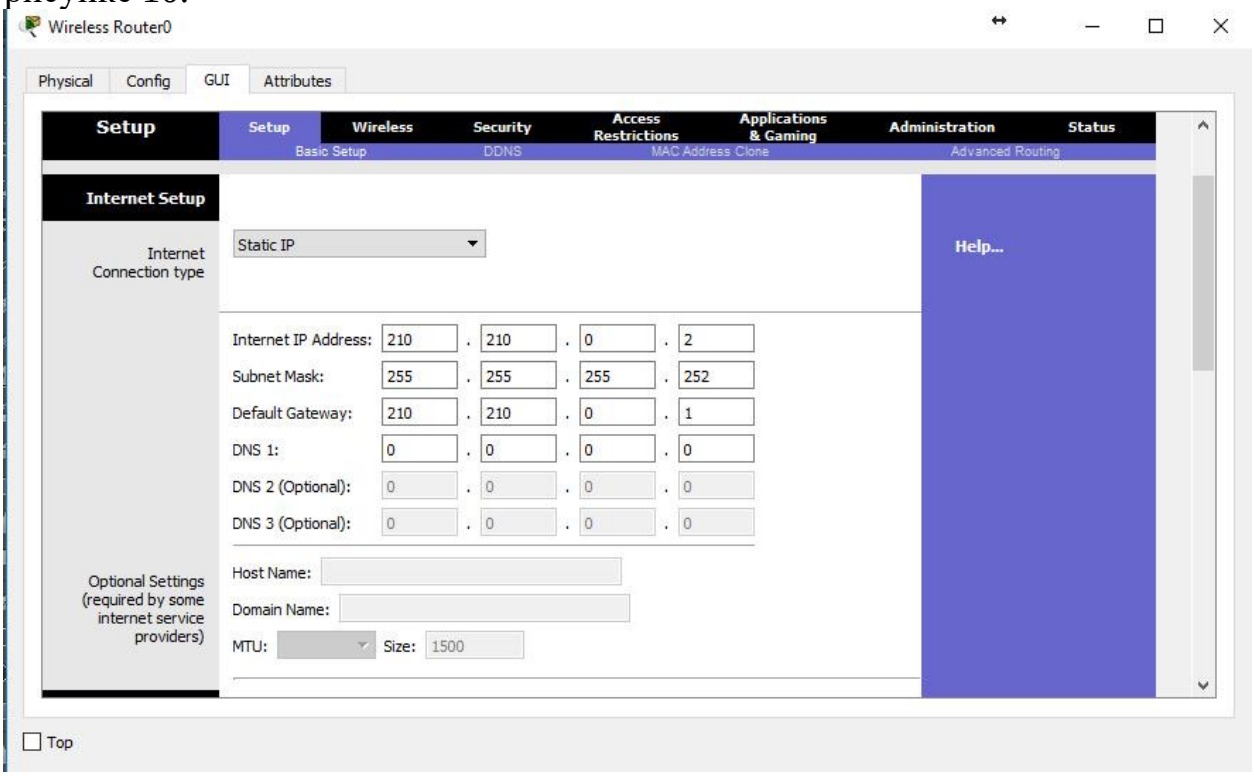


Рисунок 10 – Настройка внешнего интерфейса домашнего Wi-Fi маршрутизатора

2.2) Настройка локальной сети (Network Setup)

Выбираем по умолчанию ip-адрес 192.168.0.1, маска 24-битная 255.255.255.0, разрешён DHCP-сервер, начало раздачи с адреса 192.168.0.100 (см. рисунок 11). После чего незабываем сохранить настройки, нажать на кнопку внизу формы Save Settings.

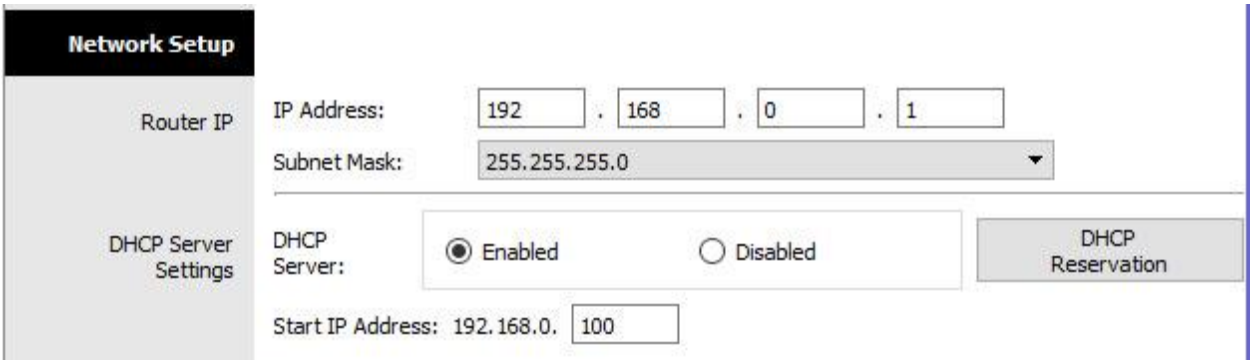


Рисунок 11 – Настройка локальной сети

Настройки во вкладке Wireless (рисунок 12), т.е. wi-fi. Выбираем основные настройки вайфая: режим (mode), мы выбираем смешанный (mixed); идентификатор сети (SSID) — netskills; ширина канала (Radio Band) — auto; частоту — 1-2.412HGz; видимость сети (SSID Broadcast) — видимая (enable). Сохраняем настройки.

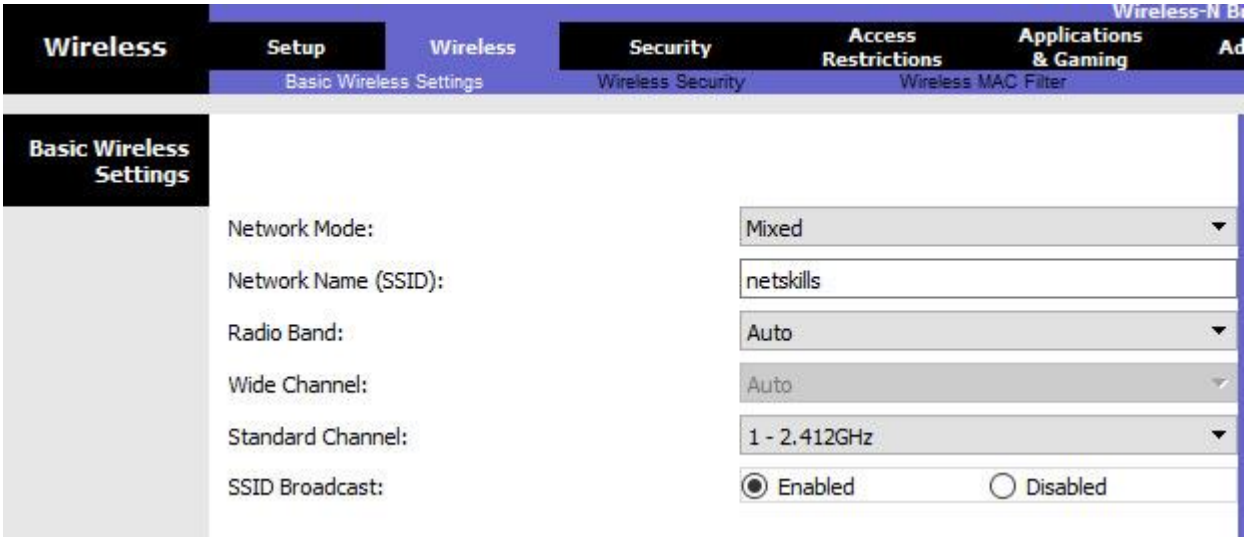


Рисунок 12 – Настройки во вкладке Wireless

Переходим ко вкладке Wireless Security (рисунок 13). Выбираем режим шифрования WPA2 Personal, алгоритм шифрования AES, ключевое слово для выбранного режима шифрования не менее 8 символов. Сохраняем.

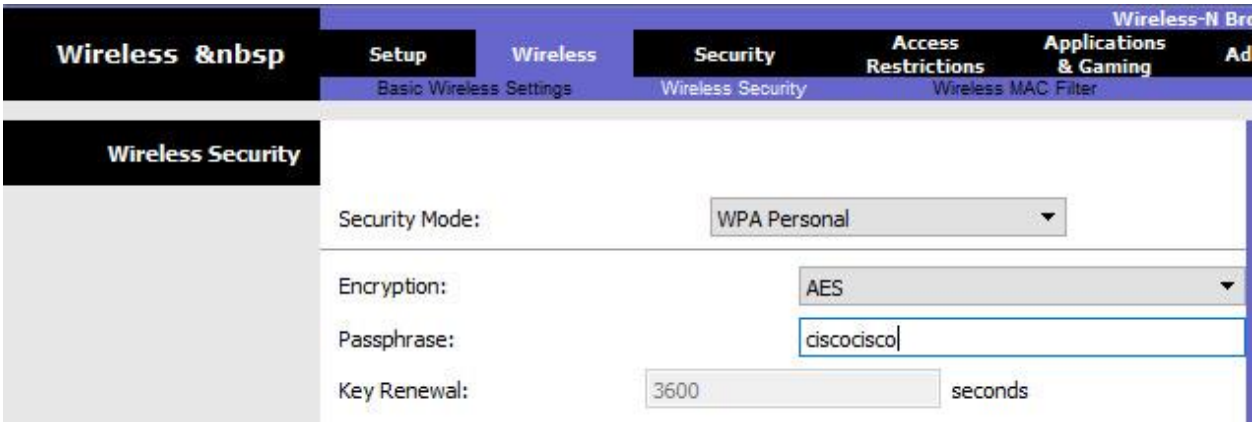


Рисунок 13 – Настройки во вкладке Wireless Security

3) Настройка Wi-Fi адаптера на ноутбуке. Вкладка Desktop->PC Wireless->Connect. Смотрим доступные нам сети. Нажимаем кнопку Connect для подключения к сети netskills.

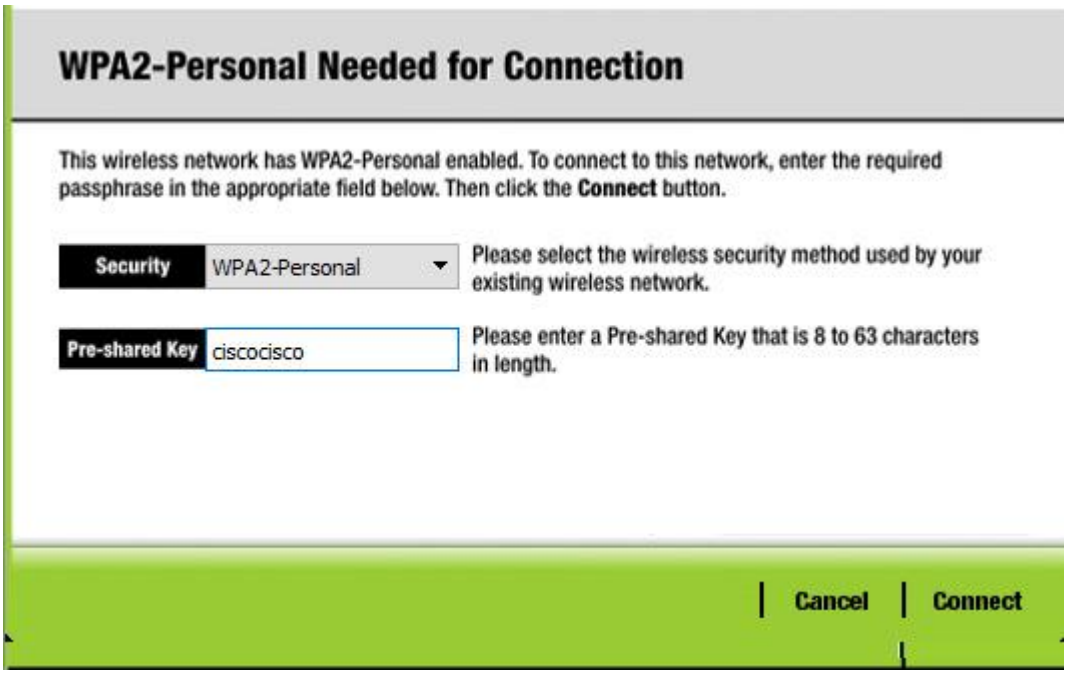


Рисунок 14 – Настройка Wi-Fi адаптера на ноутбуке

Если настройки произведены верно, то появится пунктирная линия между Wi-Fi маршрутизатором и ноутбуком как на рисунке 15.

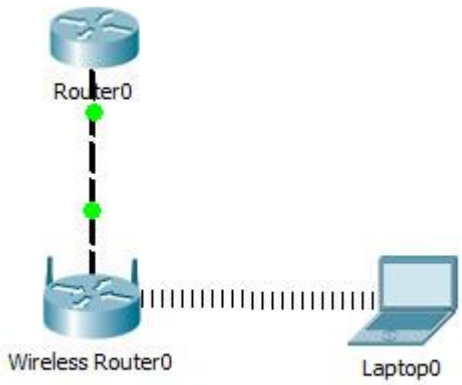


Рисунок 15 – Настроенная Wi-Fi сеть

Введём на ноутбуке в командной строке команду ipconfig, чтобы проверить правильность настроек. Из рисунка 16 видно, что DHCP-сервер присвоил правильный IP-адрес 192.168.0.100 Пропингуем шлюз (Wi-Fi маршрутизатор) и пропингуем адрес интернет провайдера. На рисунке видно, что в обоих случаях пинг идёт.

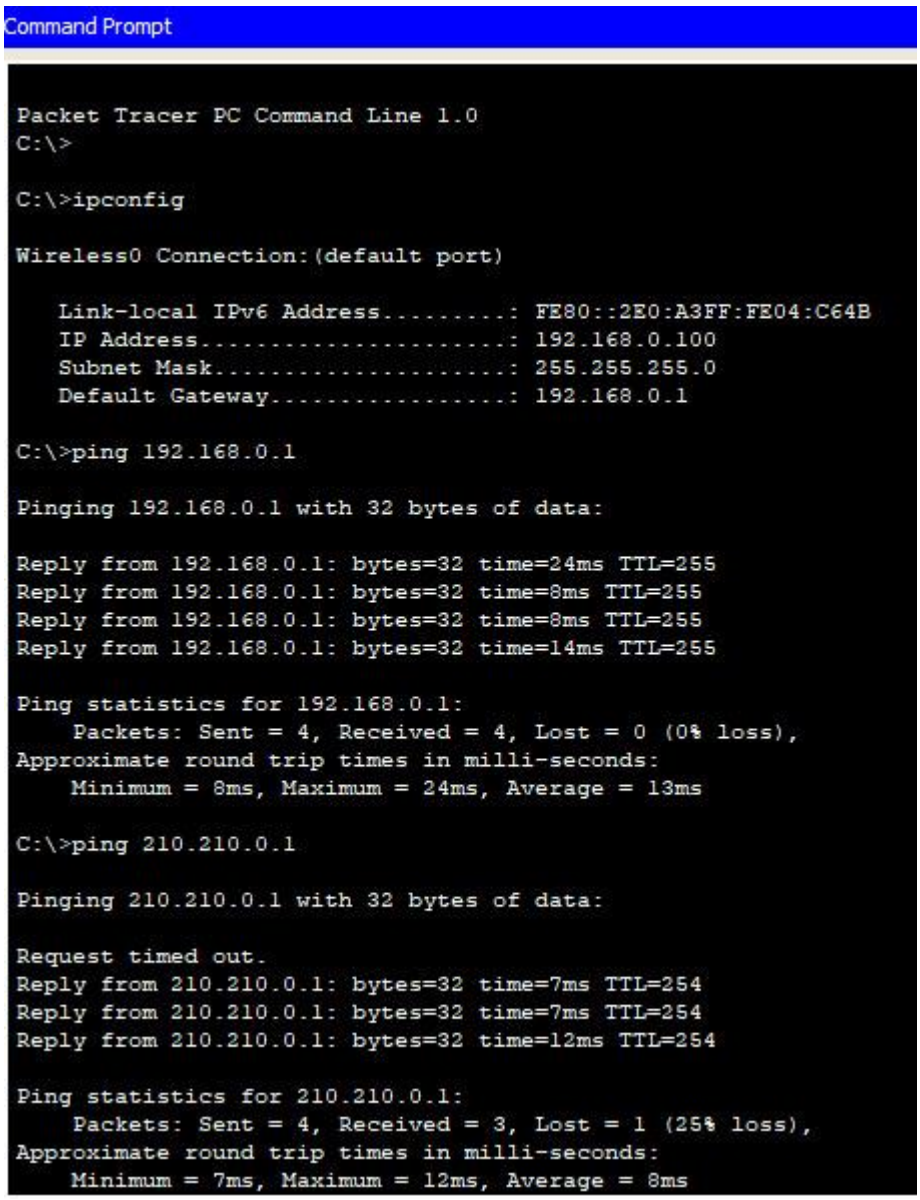


Рисунок 16 – Проверка соединения

3.2 Практическая работа. Создание простейшей сети

Цель работы: создать простейшую сеть, топология которой представлена на рисунке 17, а адресация устройств в таблице 1.

Задачи

1. Создание простейшей сети в рабочей области логической топологии
2. Конфигурирование сетевых устройств
3. Тестирование связи между сетевыми устройствами

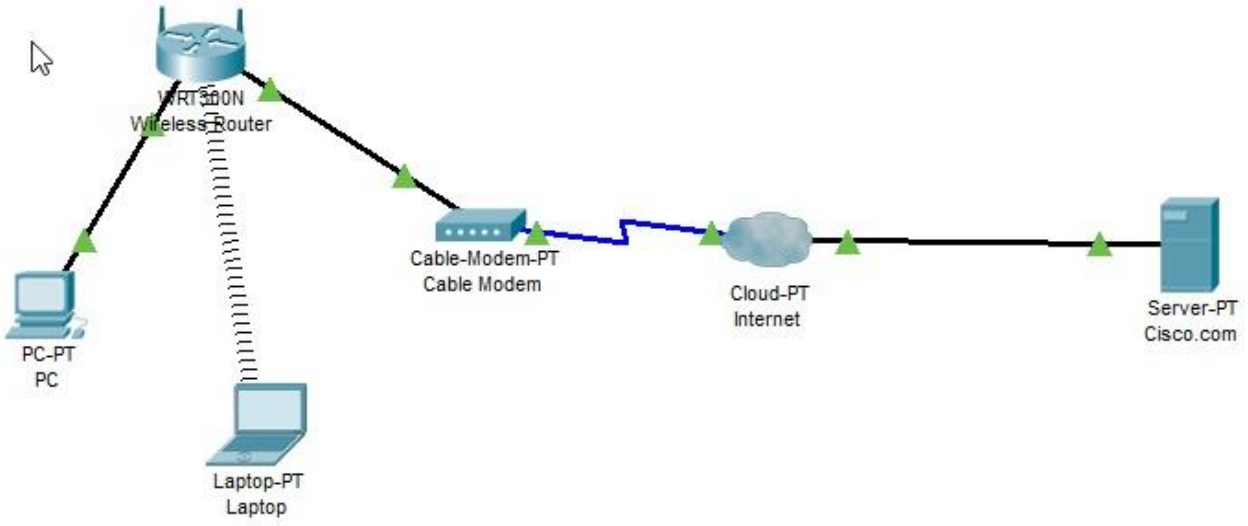


Рисунок 17 – Топология проектируемой сети

Таблица 1. Таблица адресации

Устройство	**Интерфейс**	**IP адрес**	**Маска подсети**	**Шлюз по умолчанию**
PC	Ethernet0	DHCP		192.168.0.1
Wireless Router	LAN	192.168.0.1	255.255.255.0	
	Internet	DHCP		
Cisco.com Server	Ethernet0	208.67.220.220	255.255.255.0	
Laptop	Wireless0	DHCP		

1) Выстраивание топологии сети

1.1) 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.

1.2) Измените отображаемые имена устройств сети.

Чтобы изменить отображаемые имена сетевых устройств, щелкните значок устройства в рабочем пространстве Packet Tracer Logical, затем щелкните вкладку Config в окне конфигурации устройства. На вкладке «Конфигурация» введите новое имя устройства в поле «Отображаемое имя», как показано на рисунке 18.

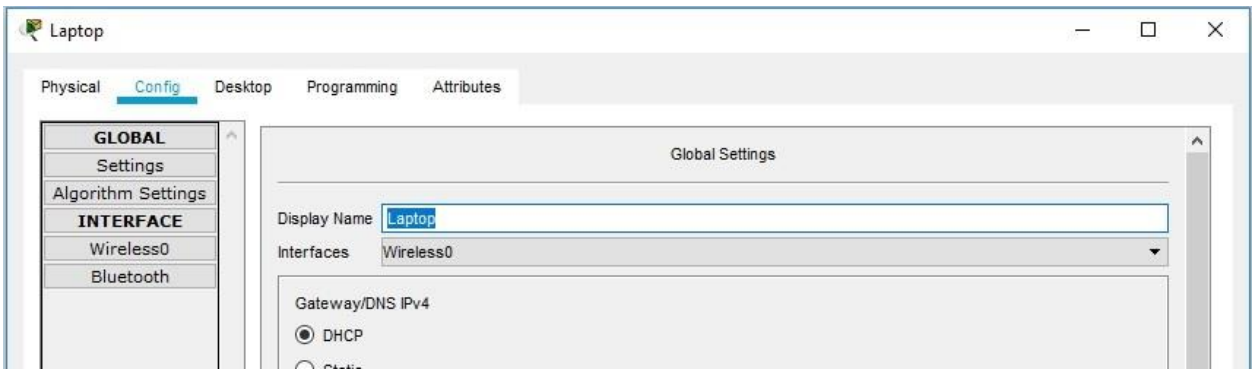


Рисунок 18 – Настройка отображаемого имени устройства

1.3) 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 беспроводному маршрутизатору ПК понадобится медный прямой кабель. Выберите медный прямой кабель в окне «Выбор устройства» и прикрепите его к интерфейсу FastEthernet0 на ПК и интерфейсу Ethernet 1 беспроводного маршрутизатора.

Для подключения беспроводного маршрутизатора к кабельному модему потребуется медный **прямой** кабель. Выберите медный прямой кабель в окне «Выбор устройства» и прикрепите его к **Интернет-интерфейсу** беспроводного маршрутизатора и интерфейсу порта 1 кабельного модема.

Для подключения к интернет-облаку кабельного модема потребуется коаксиальный кабель. Выберите коаксиальный кабель в окне «Выбор устройства» и прикрепите его к интерфейсу порта 0 кабельного модема и коаксиальному интерфейсу интернет-облака.

Для подключения к серверу Cisco.com для облака Internet необходим медный прямой кабель. Выберите медный прямой кабель в окне «Выбор устройства» и прикрепите его к интерфейсу Ethernet облака Интернета и интерфейсу FastEthernet0 на сервере Cisco.com.

2) Настройка беспроводного маршрутизатора

2.1) Создание беспроводной сети на беспроводном маршрутизаторе

Нажмите значок Wireless Router на рабочем пространстве Packet Tracer Logical, чтобы открыть окно конфигурации устройства. В окне конфигурации Wireless Router нажмите вкладку GUI, чтобы просмотреть параметры конфигурации для Wireless Router. Затем щелкните вкладку Wireless в графическом интерфейсе, чтобы просмотреть настройки беспроводной сети. Единственным параметром, который необходимо изменить по умолчанию, является имя сети (SSID). Здесь введите имя «HomeNetwork», как показано на рисунке 19.

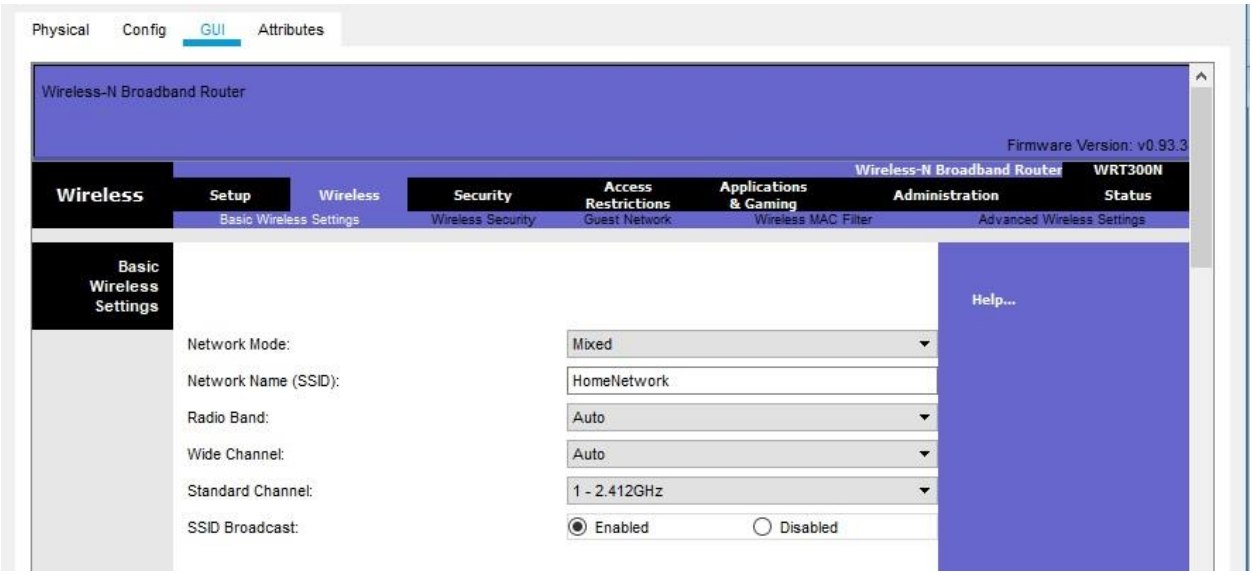


Рисунок 19 – Настройка беспроводной сети

2.2) Настройка подключения к Интернету на беспроводном маршрутизаторе

Нажмите вкладку «Настройка» в графическом интерфейсе Wireless Router. В настройках сервера DHCP убедитесь, что выбрана кнопка «Включено» и настройте статический IP-адрес DNS-сервера как 208.67.220.220, как показано на рисунке 20.

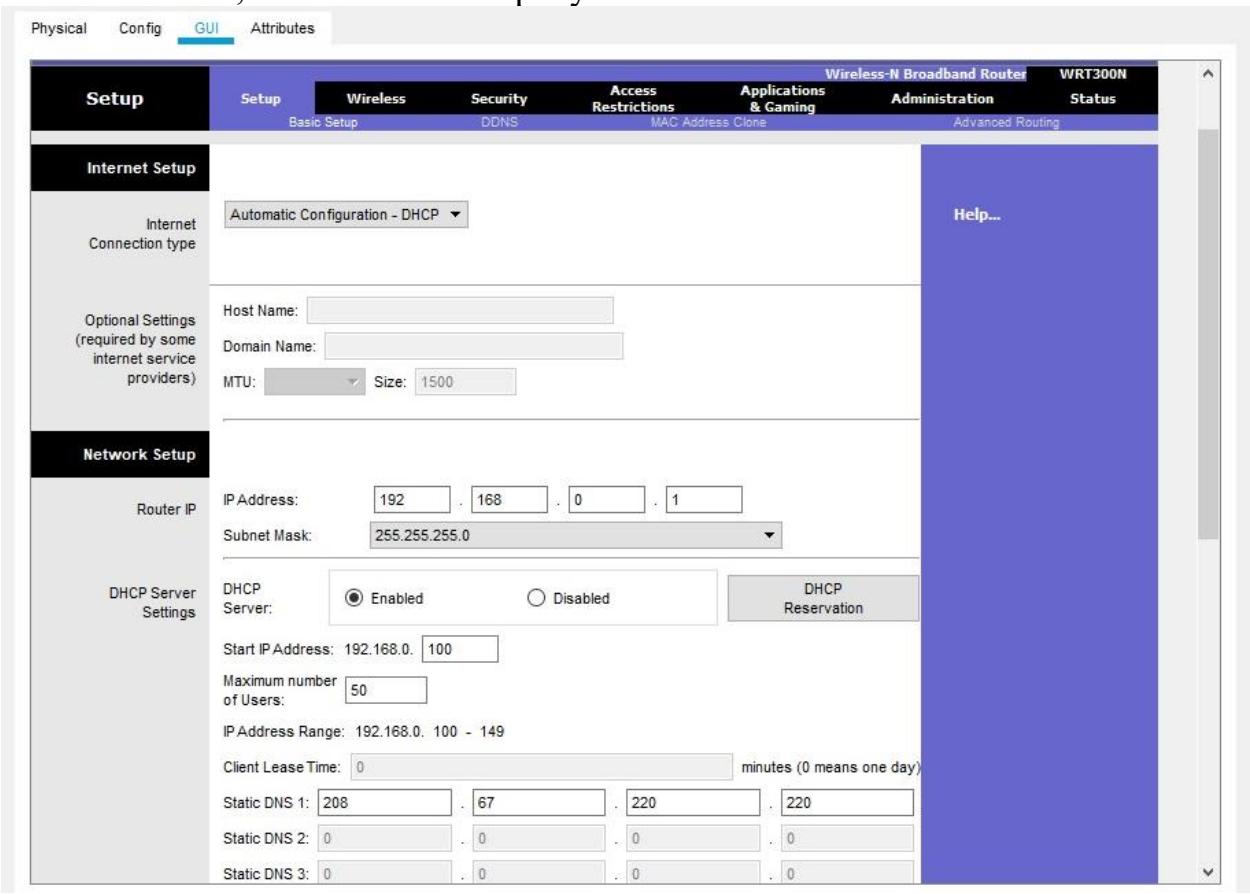


Рисунок 20 – Настройка подключения к Интернету на беспроводном маршрутизаторе

2.3) Сохраните настройки.

3) Настройка ноутбука

Нажмите значок «Ноутбук» на рабочем месте Packet Tracer Logical, а в окнах конфигурации ноутбука выберите вкладку «Физические». На вкладке «Физик» вам нужно будет удалить медный модуль Ethernet и заменить его на модуль Wireless WPC300N. Для этого сначала выключите ноутбук, нажав кнопку питания на боковой панели ноутбука. Затем удалите установленный в данный момент медный модуль Ethernet, щелкнув модуль на боковой панели ноутбука и перетащите его в панель MODULES слева от окна ноутбука. Затем установите модуль Wireless WPC300N, щелкнув по нему в панели MODULES и перетащив его в пустой порт модуля на стороне ноутбука. Включите ноутбук снова, снова нажав кнопку питания ноутбука. С установленным беспроводным модулем следующая задача — подключить ноутбук к беспроводной сети.

Перейдите на вкладку «Рабочий стол» в верхней части окна конфигурации ноутбука и выберите значок «Беспроводная сеть ПК». После того, как параметры адаптера ноутбука Wireless-N станут видны, выберите вкладку «Подключить». Беспроводная сеть «HomeNetwork» должна быть видна в списке беспроводных сетей, как показано на рисунке 21. Выберите сеть и нажмите вкладку «Подключиться», расположенную под информацией о сайте.

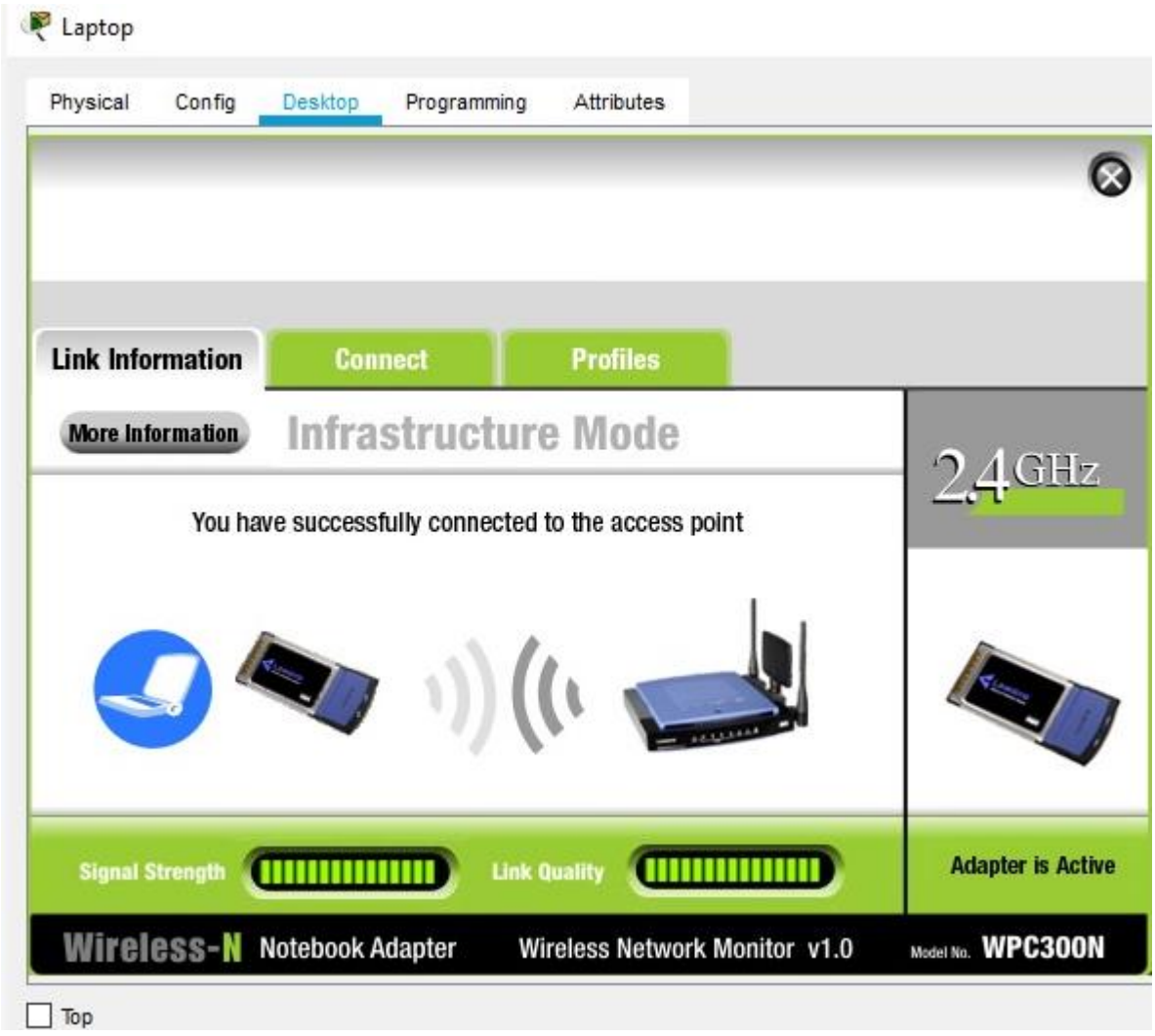


Рисунок 21 – Настройка ноутбука

4) Настройка ПК

Нажмите значок ПК на рабочем пространстве Packet Tracer Logical и выберите вкладку «Рабочий стол», а затем значок «Конфигурация IP». В окне IP-конфигурации выберите переключатель DCHP, как показано на рисунке 22, чтобы ПК использовал DCHP для приема IPv4-адреса с беспроводного маршрутизатора. Закройте окно настройки IP.

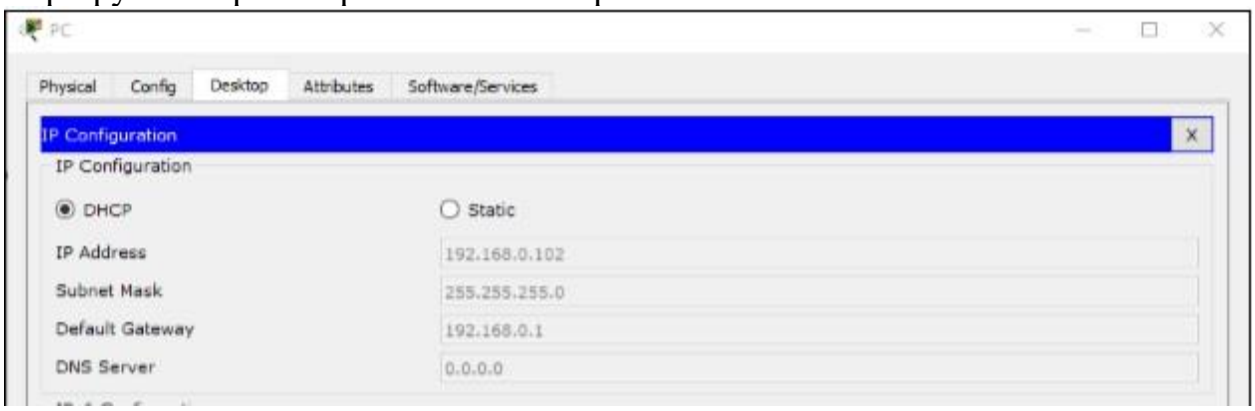


Рисунок 22 – Настройка автоматического получения IP-адреса на ПК

Нажмите на значок командной строки. Убедитесь, что ПК получил IPv4-адрес, выпустив команду ipconfig / all из команды, как показано на рисунке 23. ПК должен получить IPv4-адрес в диапазоне 192.168.0.x.

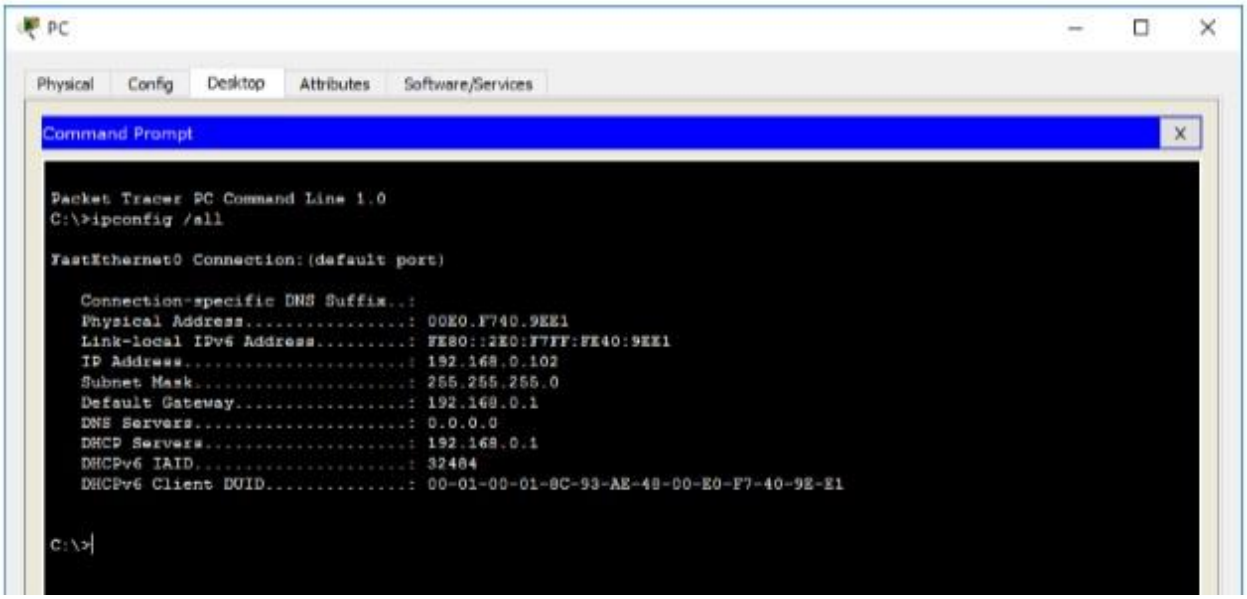


Рисунок 23 – Проверка сетевых настроек ПК

5) Настройка облака Интернета

5.1) При необходимости установите сетевые модули. Нажмите значок «Интернет-облако» в рабочей области «Трассировщик пакетов» и затем перейдите на вкладку «Физические». Для облачного устройства потребуется два модуля, если они еще не установлены. PT-CLOUD-NM-1CX, который предназначен для подключения кабельного модема и PT-CLOUD-NM-1CFE, который предназначен для подключения медного Ethernet-кабеля. Если эти модули отсутствуют, отключите физические облачные устройства, нажав на кнопку питания и перетащите

каждый модуль на пустой порт модуля на устройстве, а затем снова включите устройство.

5.2) Определите тип поставщика.

На вкладке «Конфигурация» нажмите «FastEthernet8» в «INTERFACE» на левой панели. В окне конфигурации FastEthernet8 выберите «Кабель» в качестве сети поставщика, как показано на рисунке 24.

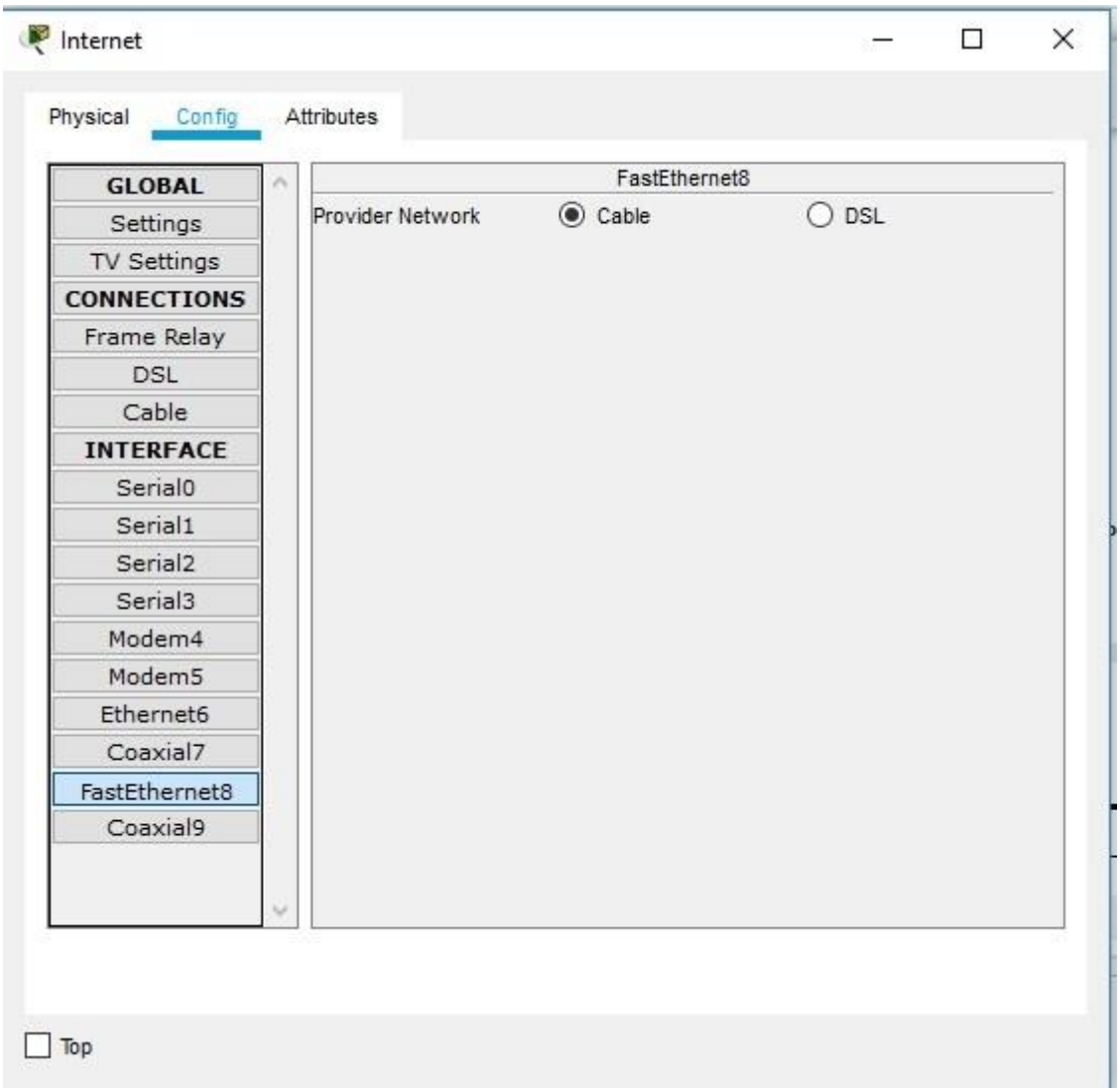


Рисунок 24 - Определите тип поставщика

5.3) Идентификация портов From и To

Перейдите на вкладку «Конфигурация» в окне «Облако». В левой панели нажмите «Кабель» под разъемами CONNECTIONS. В первом раскрывающемся списке выберите Coaxial7, а во втором выпадающем списке выберите «FastEthernet8», затем нажмите кнопку Add, чтобы добавить их как «От порта» и «В порт», как показано на рисунке 25.

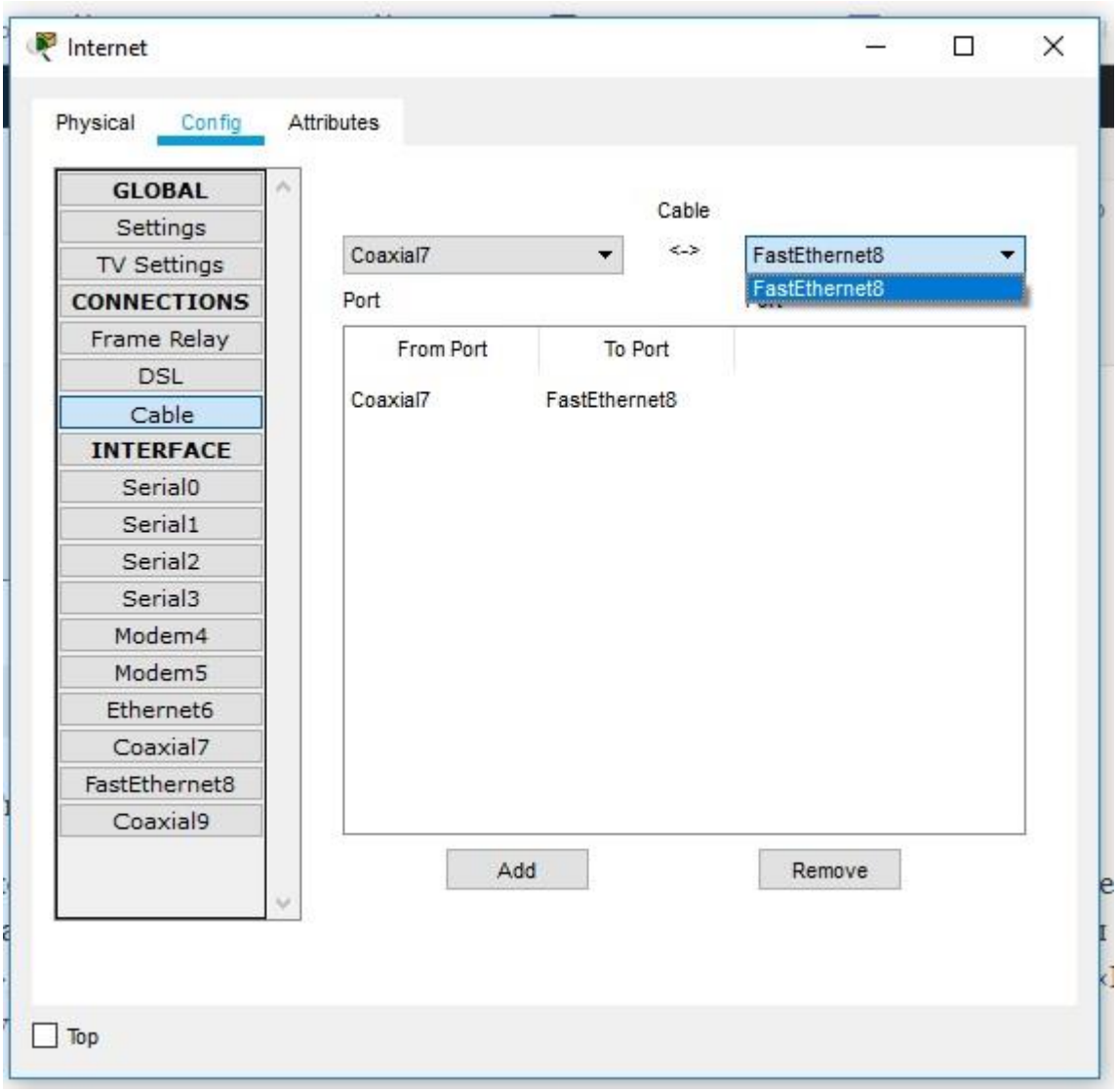


Рисунок 25 – Идентификация портов From и To

6) Настройка сервера Cisco.com

6.1) Настройте сервер Cisco.com как сервер DHCP

Нажмите значок сервера Cisco.com в рабочем пространстве Packet Tracer Logical и выберите вкладку «Службы». Выберите DHCP из списка «УСЛУГИ» на левой панели.

В окне конфигурации DHCP настройте DHCP, как показано на рисунке, со следующими настройками.

- Нажмите «Вкл.», чтобы включить службу DCHP.
- Имя пула: DHCPpool
- Шлюз по умолчанию: 208.67.220.220
- DNS-сервер: 208.67.220.220
- Запуск IP-адреса: 208.67.220.1
- Маска подсети 255.255.255.0
- Максимальное количество пользователей: 50

Нажмите «Добавить», чтобы добавить пул.

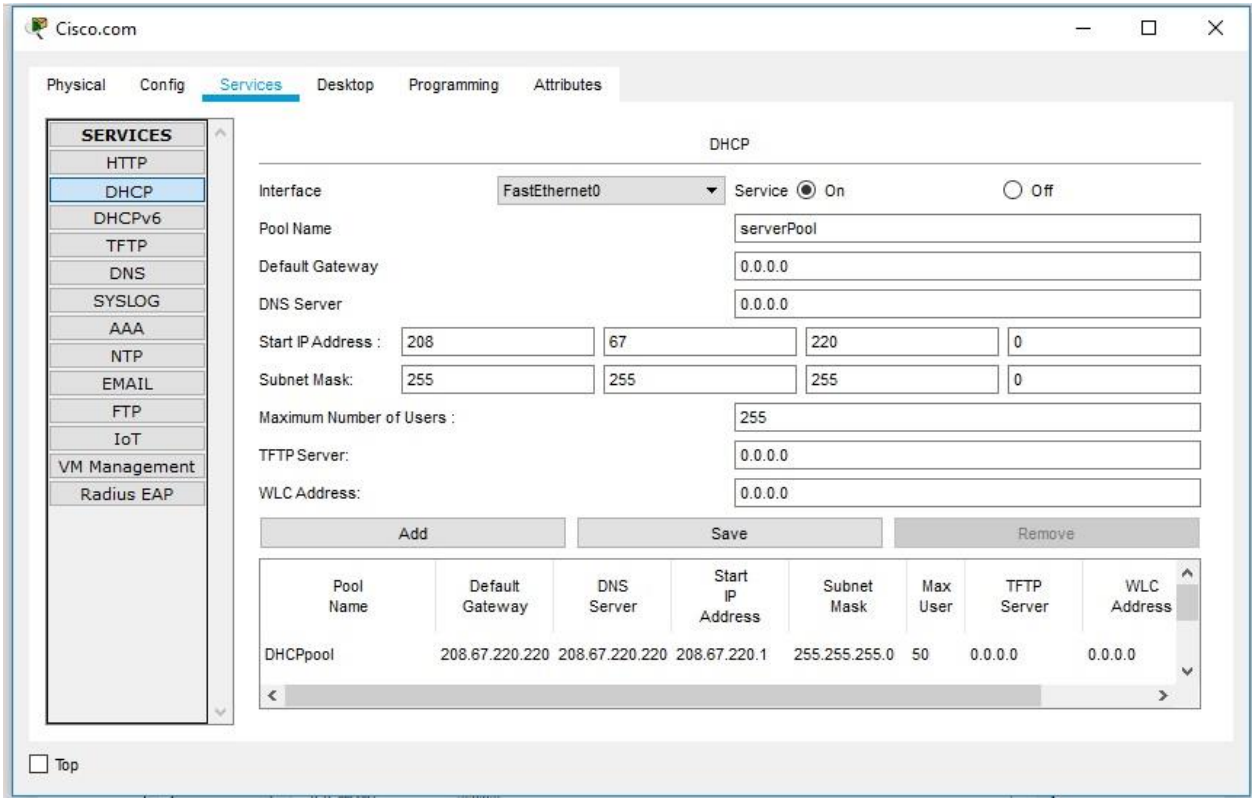


Рисунок 26 – Настройка сервера Cisco.com как сервер DHCP

6.2) Настройте сервер Cisco.com как DNS-сервер для предоставления имени домена для разрешения адреса IPv4.

На вкладке «Службы» выберите DNS из служб, перечисленных на левой панели.

Настройте службу DNS, используя следующие настройки, как показано на рисунке 27.

- Нажмите «Вкл.», чтобы включить службу DNS
- Имя: Cisco.com
- Тип: A Запись
- Адрес: 208.67.220.220

Нажмите «Добавить», чтобы добавить настройки службы DNS

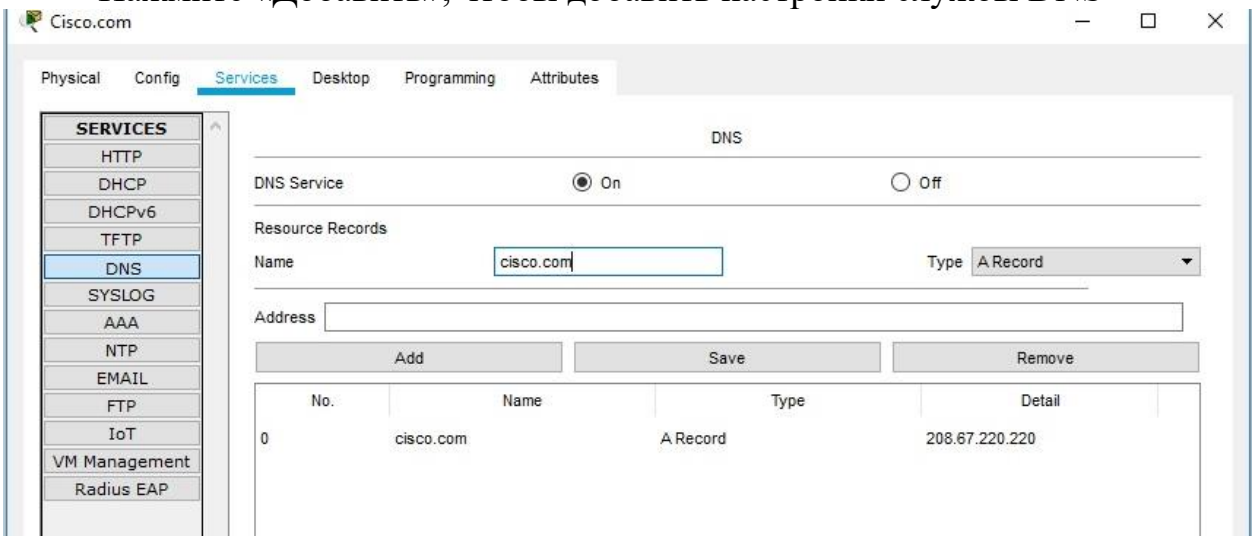


Рисунок 27 – Настройка сервера Cisco.com как DNS-сервера

6.3) Настройте глобальные настройки сервера Cisco.com.

Выберите вкладку «Конфигурация». Нажмите «Настройки» в левой панели. Настройте глобальные настройки сервера следующим образом:

- Выберите Статический
- Шлюз: 208.67.220.1
- DNS-сервер: 208.67.220.220

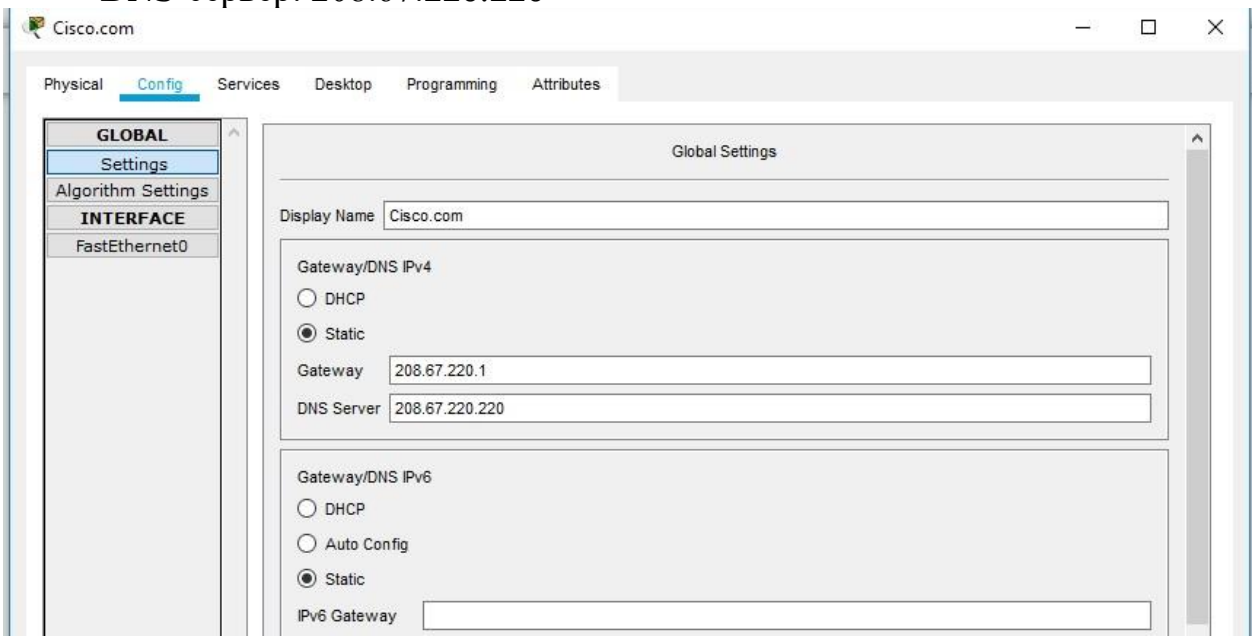


Рисунок 28 – Глобальные настройки сервера Cisco.com

6.4) Настройте параметры интерфейса FastEthernet0 сервера Cisco.com.

Нажмите «FastEthernet» в левой панели вкладки «Конфигурация». Настройте параметры интерфейса FastEthernet на сервере следующим образом:

- Выберите «Статический» при настройке IP-адреса
- IP-адрес: 208.67.220.220
- Маска подсети: 255.255.255.0

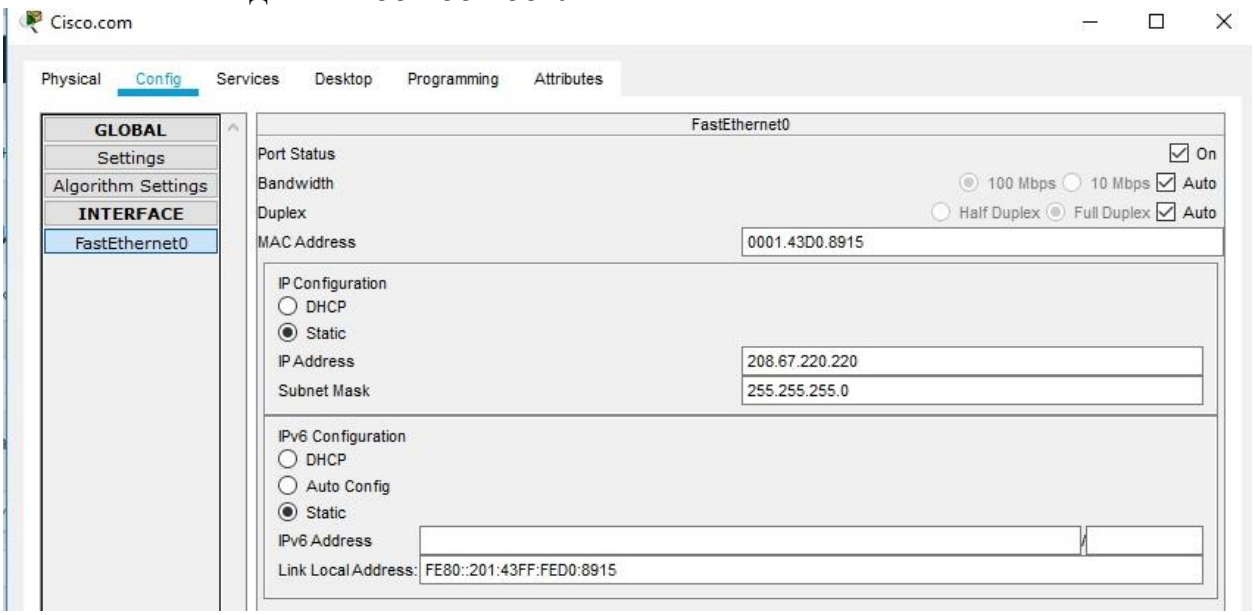


Рисунок 29 – Параметры интерфейса FastEthernet0 сервера Cisco.com

7) Проверка подключения

7.1) Убедитесь, что ПК получает информацию о конфигурации IPv4 от DHCP. Нажмите на ПК в рабочем пространстве Packet Tracer Logical, а затем выберите вкладку Desktop в окне конфигурации ПК. Нажмите значок командной строки (см. рисунок 30).

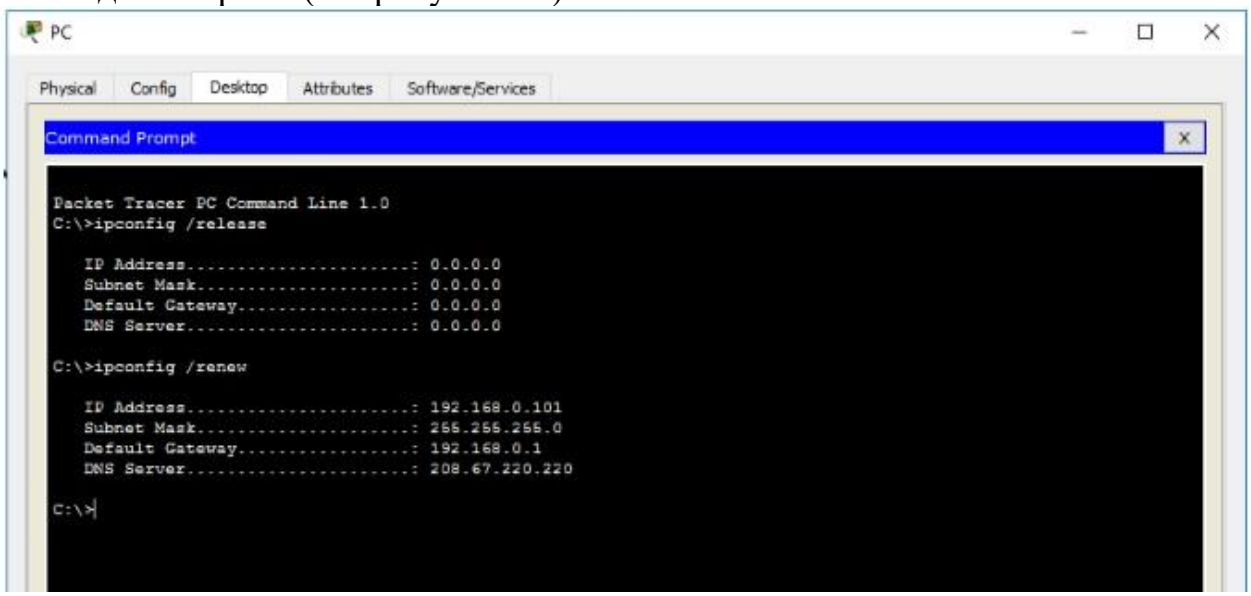


Рисунок 30 – Обновление настроек IPv4 на ПК

7.2) Проверить подключение к серверу Cisco.com с ПК

Из командной строки, выдающей команду ping Cisco.com. Для возврата ping может потребоваться несколько секунд. Необходимо получить четыре ответа, как показано на рисунке 31.

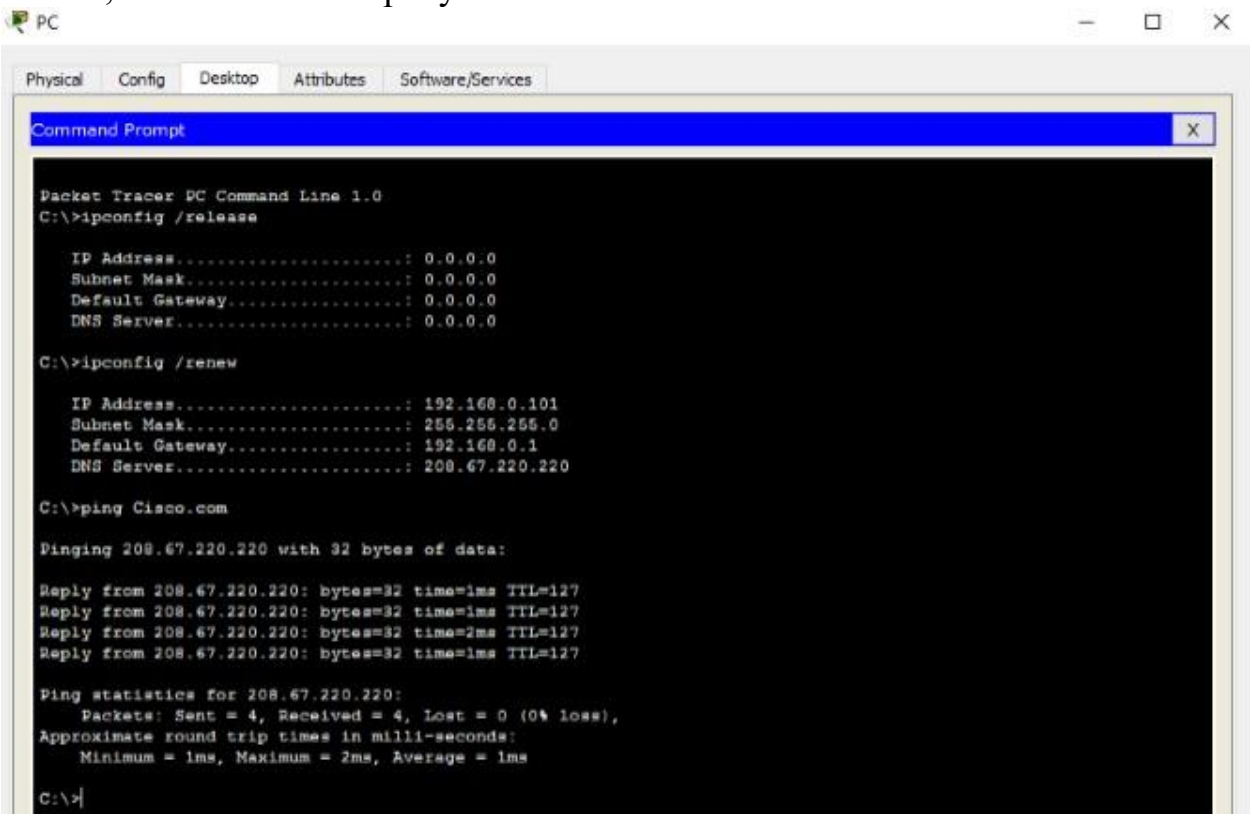


Рисунок 31 - Проверка подключения к серверу Cisco.com с ПК

3.3 Лабораторная работа. Создание беспроводной сети

1) Собрать сеть согласно топологии, изображенной на рисунке 31.

2) Настроить вручную (без использования DHCP сервера) IP-адреса на всех сетевых устройствах. IP-адреса и маска подсети для каждого устройства указаны на рисунке. Вместо символа XX указать последние две цифры зачетки или студенческого билета.

3) Прописать статические маршруты к удаленным сетям на маршрутизаторе (команда «ip route *Номер удаленной сети Маска удаленной сети IP-следующего маршрутизатора*»)

3) Проверить наличие связи между устройствами (команда ping).

4) На проверку сдать файл Packet Tracer с настроенной сетью.

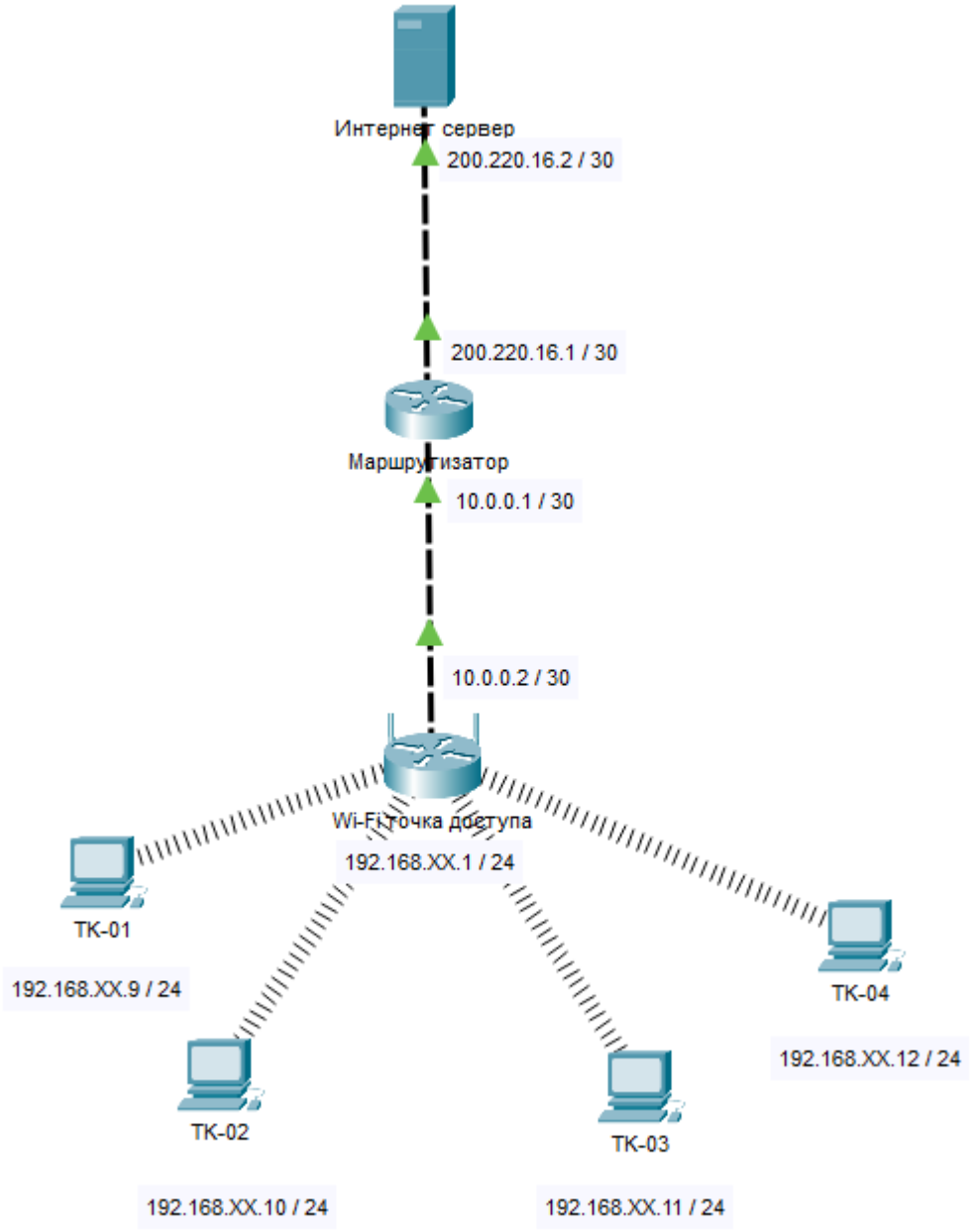


Рисунок 31 – Топология проектируемой сети

4 Технология VLAN

4.1 Принцип работы VLAN

VLAN – это технология, которая позволяет строить виртуальные сети с независимой от физических устройств топологией. Например, можно объединить в одну сеть отдел компании, сотрудники которого работают в разных зданиях и подключены к разным коммутаторам. Или, наоборот, создать отдельные сети для устройств, подключённых к одному коммутатору, если этого требует политика безопасности.

Компьютеры в локальной сети соединяются между собой с помощью сетевого оборудования — коммутаторов. По умолчанию все устройства, подключённые к портам одного коммутатора, могут взаимодействовать, обмениваясь сетевыми пакетами. Любой компьютер может направить широковещательный пакет, адресованный всем устройствам в этой сети, и все остальные компьютеры, подключённые к коммутатору, получат его. Все слышат всех.

Большое количество широковещательных пакетов, отправляемых устройствами, приводит к снижению производительности сети, поскольку вместо полезных операций коммутаторы заняты обработкой данных, адресованных сразу всем.

Чтобы снизить влияние широковещательных рассылок на производительность, сеть разделяют на изолированные сегменты. При этом каждый широковещательный пакет будет распространяться только в пределах сегмента, к которому подключен компьютер-отправитель.

Добиться такого результата можно, подключив разные сегменты к разным физическим коммутаторам, не соединённым между собой, либо соединить их через маршрутизаторы, которые не пропускают широковещательные рассылки.

На рисунке 32 имеется четыре изолированных сегмента сети, каждый из которых подключён к отдельному физическому коммутатору. Взаимодействие между сегментами происходит через маршрутизаторы.

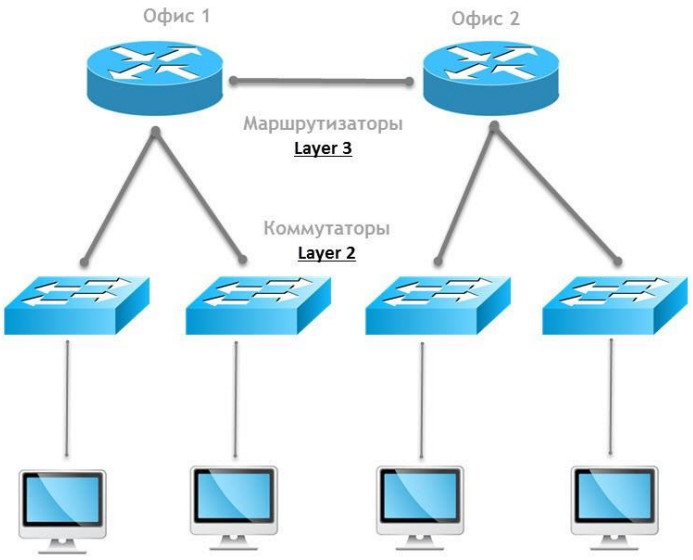


Рисунок 32 – Изоляция сегментов с использованием маршрутизаторов

VLANы позволяют изолировать сегменты сети с помощью одного физического коммутатора (см. рисунок 33). При этом функционально всё будет выглядеть полностью аналогично, но для каждого офиса используется один коммутатор с поддержкой VLAN.

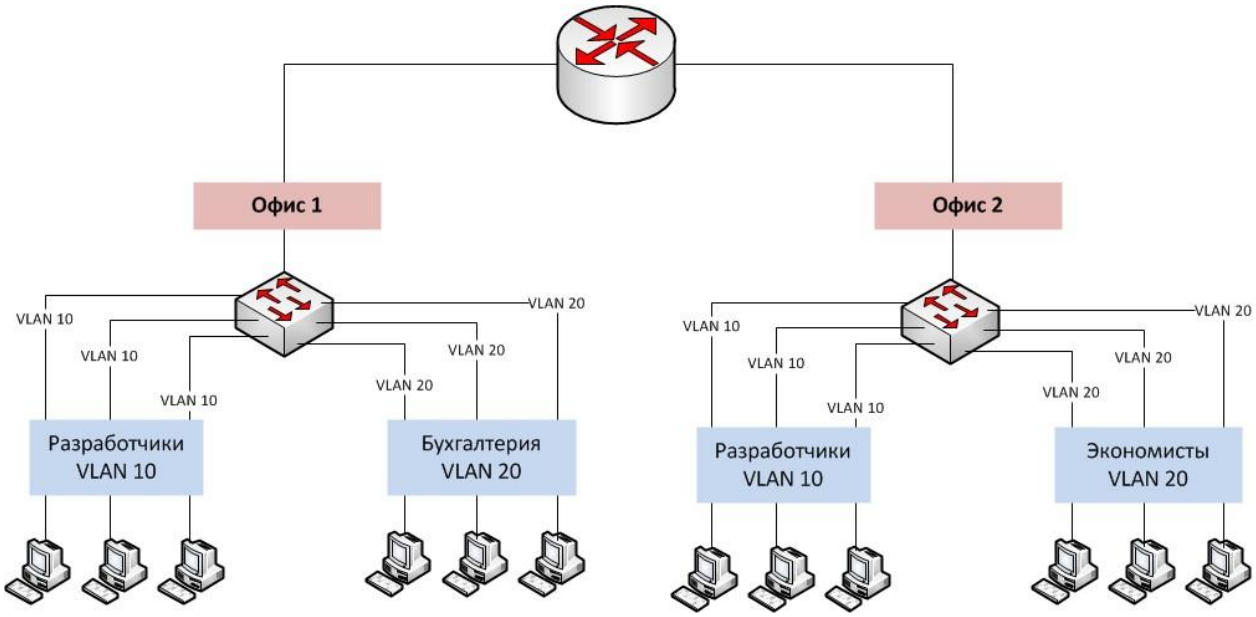


Рисунок 33 – Изоляция сегментов с использованием технологии VLAN

В основе технологии VLAN лежит стандарт IEEE 802.1Q. Он позволяет добавлять в Ethernet-трафик информацию о принадлежности передаваемых данных к той или иной виртуальной сети — теги VLAN. С их помощью коммутаторы и маршрутизаторы могут выделить из общего потока передаваемых по сети кадров те, что относятся к конкретному сегменту.

Технология VLAN даёт возможность организовать функциональный эквивалент нескольких LAN-сетей без использования набора из коммутаторов и кабелей, которые понадобились бы для их реализации в физическом виде.

Физическое сетевое оборудование заменяется виртуальным. Отсюда термин Virtual LAN.

4.2 Возможности VLAN

Используя виртуальные локальные сети, можно создавать конфигурации для решения различных задач:

1) Объединить в единую сеть группы компьютеров, подключённых к разным коммутаторам (см. рисунок 34). Компьютеры в VLAN 1 будут взаимодействовать между собой, хотя подключены к разным физическим коммутаторам, при этом сети VLAN 1 и VLAN 2 будут невидимы друг для друга.

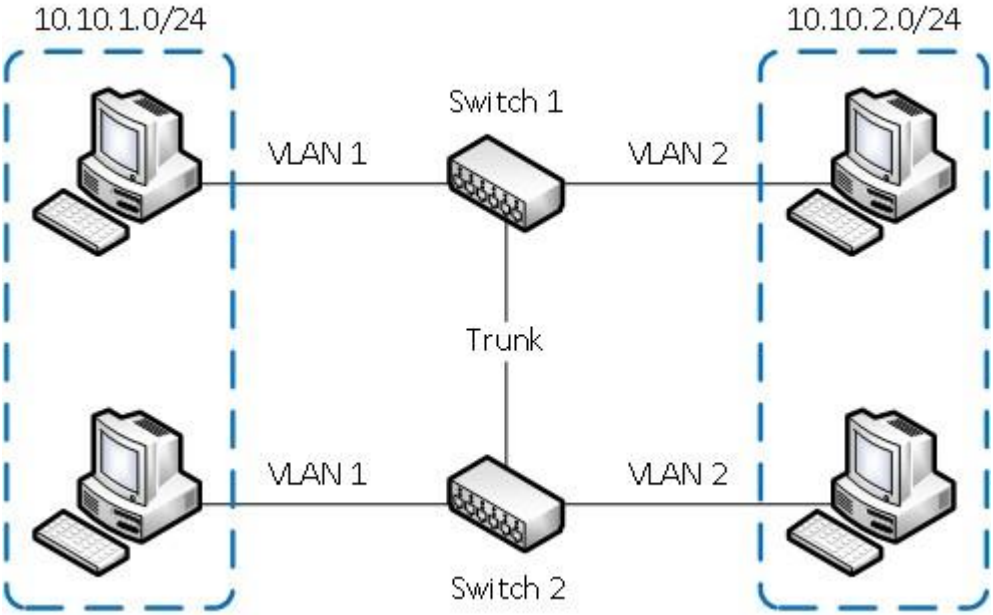


Рисунок 34

2) Разделить на разные сети компьютеры, подключённые к одному коммутатору (рисунок 35). При этом устройства в VLAN 1 и VLAN 2 не смогут взаимодействовать между собой.

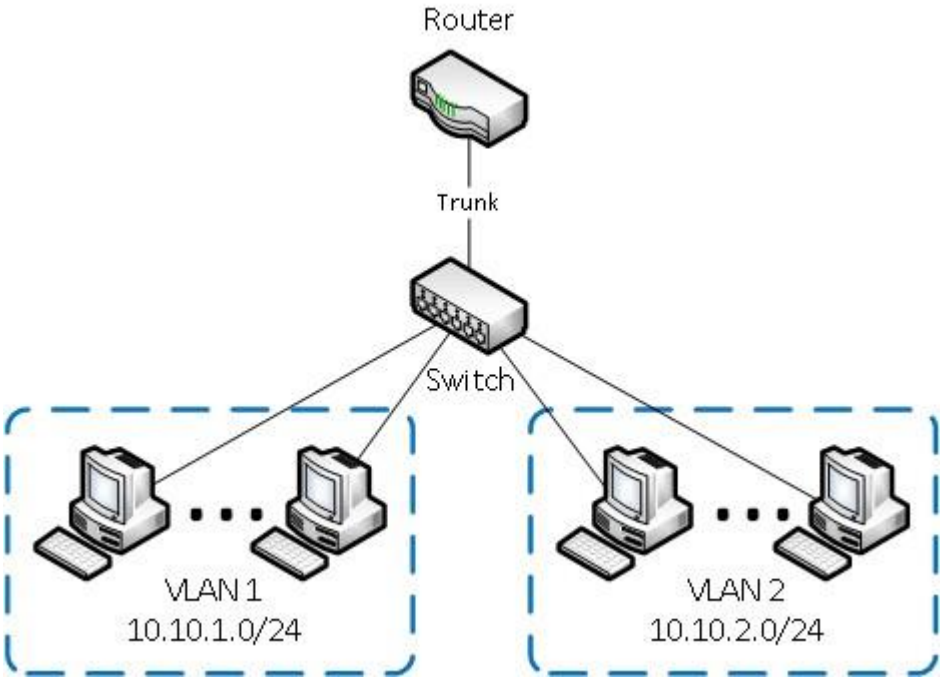


Рисунок 35

3) Разделить гостевую и корпоративную беспроводную сеть компании (рисунок 36). Гости смогут подключаться к интернету, но не получат доступа к сети компании.

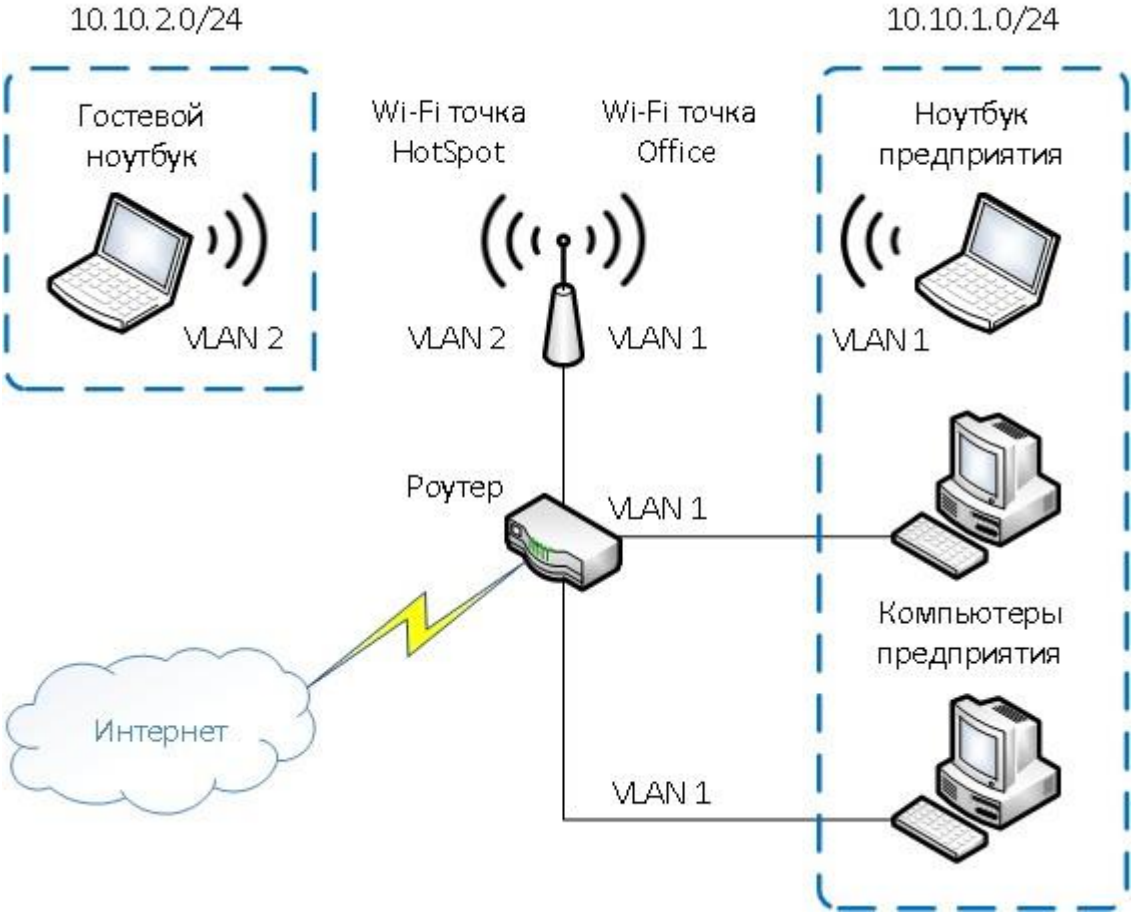


Рисунок 36

Преимущества VLAN

- Сокращение числа широковещательных запросов, которые снижают пропускную способность сети.
- Повышение безопасности каждой виртуальной сети. Работники одного отдела офиса не смогут отслеживать трафик отделов, не входящих в их VLAN, и не получат доступ к их ресурсам.
- Возможность разделять или объединять отделы или пользователей, территориально удаленных друг от друга. Это позволяет привлекать к рабочему процессу специалистов, не находящихся в здании офиса.
- Создать новую виртуальную сеть можно без прокладки кабеля и покупки коммутатора.
- Позволяет объединить в одну сеть компьютеры, подключенные к разным коммутаторам.
- Упрощение сетевого администрирования. При переезде пользователя VLAN в другое помещение или здание сетевому администратору нет необходимости перекоммутировать кабели, достаточно со своего рабочего места перенастроить сетевое оборудование. А в случае использования динамических VLAN регистрация пользователя в «своём» VLAN на новом месте выполнится автоматически.

4.3 Практическая работа. Настройка VLAN на коммутаторе

Общая идея настройки VLAN на коммутаторах заключается в том, чтобы задать разрешенные номера VLAN для каждого порта коммутатора. Все оконечные устройства, подключенные к коммутатору, передают Ethernet кадры без метки VLAN (тега). Это так называемый нетегированный трафик. Если на порту коммутатора, к которому подключено оконечное устройство, настроен VLAN с некоторым номером, то в кадры Ethernet, приходящие на этот порт, будет добавляться метка (тег) с номером этого VLAN'а. Такие порты коммутатора называются **access port**, т.е. порт, принадлежащий одному VLAN'у и принимающий нетегированный трафик. При передаче кадра с меткой VLAN оконечному устройству через access порт коммутатор удаляет метку и кадр становится нетегированым.

В случае, если через порт коммутатора нужно передать тегированный (т.е. кадры с меткой VLAN) трафик для одного изи нескольких VLAN, то такой порт настраивают в режим **trunk** и указывают номера разрешенных VLAN, которые нужно передавать через этот порт. **Trunk port** – порт передающий тегированный трафик одного или нескольких VLAN'ов.

Коммутаторы Cisco используют протокол 802.1Q для работы с технологией VLAN.

Порядок настройки

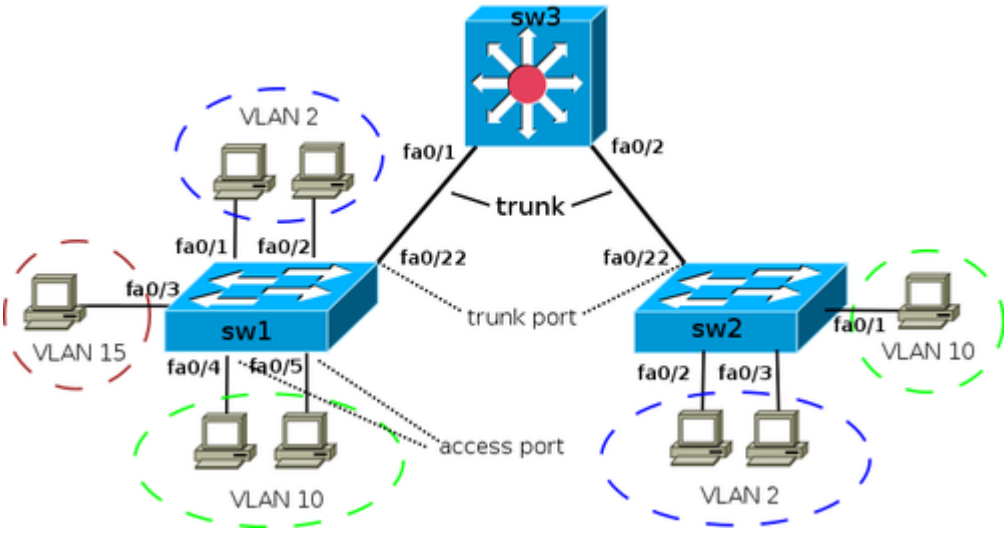


Рисунок 37 – Сеть с VLANами на коммутаторах Cisco

1) Создание VLAN с заданным номером и задание имени для него:

```
sw1(config)# vlan 2
sw1(config-vlan)# name test
```

2) Настройка access портов

Назначение порта коммутатора в VLAN:

```
sw1(config)# interface fa0/1
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 2
```

Назначение диапазона портов с fa0/4 до fa0/5 в vlan 10:

```
sw1(config)# interface range fa0/4 - 5
sw1(config-if-range)# switchport mode access
sw1(config-if-range)# switchport access vlan 10
```

Просмотр информации о VLAN'ах:

```
sw1# show vlan brief
VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21,
```

```
                                                Fa0/22, Fa0/23, Fa0/24

2    test                             active    Fa0/1, Fa0/2

10   VLAN0010                         active    Fa0/4, Fa0/5

15   VLAN0015                         active    Fa0/3
```

Справка

VLAN можно создать на коммутаторе с помощью команды vlan. Кроме того, VLAN автоматически создается на коммутаторе в момент добавления в него интерфейсов в режиме access.

В схеме, которая используется для демонстрации настроек, на коммутаторах sw1 и sw2, нужные VLAN будут созданы в момент добавления access-портов в соответствующие VLAN:

```
sw1(config)# interface fa0/3
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 15
% Access VLAN does not exist. Creating vlan 15
```

На коммутаторе sw3 access-портов нет. Поэтому необходимо явно создать все необходимые VLAN:

```
sw3(config)# vlan 2,10,15
```

3) Настройка транка (trunk)

Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим транка. Создание статического транка:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport mode trunk
```

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк. Указать перечень разрешенных VLAN для транкового порта fa0/22:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan 1-2,10,15
```

Добавление ещё одного разрешенного VLAN:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan add 160
```

Удаление VLAN из списка разрешенных:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan remove 160
```

5) Настройка маршрутизации между VLAN`ми

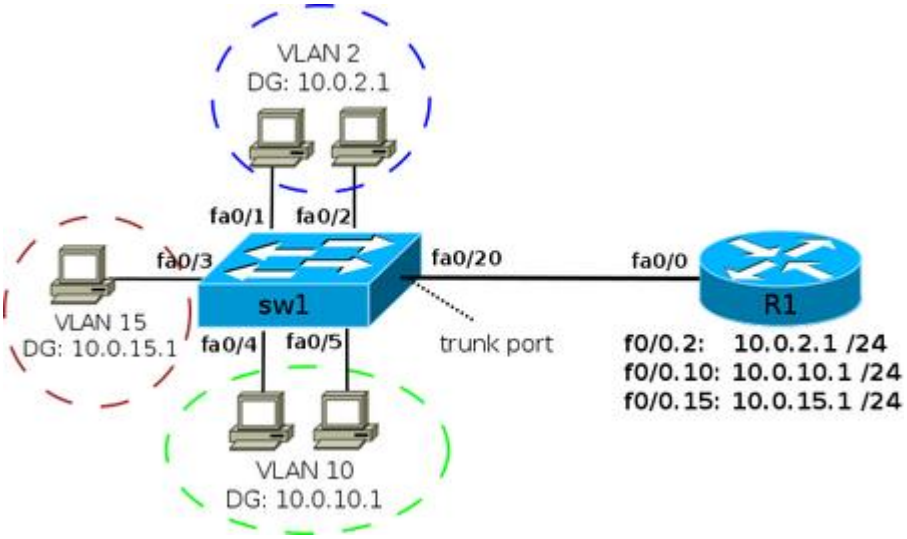


Рисунок 38 – Передача трафика между VLANами с помощью маршрутизатора

Передача трафика между VLAN может осуществляться с помощью маршрутизатора. Для того чтобы маршрутизатор мог передавать трафик из одного VLAN в другой (из одной сети в другую), необходимо, чтобы в каждой сети у него был интерфейс. Для того чтобы не выделять под сеть каждого VLAN отдельный физический интерфейс, создаются логические подынтерфейсы на физическом интерфейсе для каждого VLAN.

На коммутаторе порт, ведущий к маршрутизатору, должен быть настроен как тегированный порт (транк).

Изображенная на рисунке 38 схема, в которой маршрутизация между VLAN выполняется на маршрутизаторе, часто называется **router on a stick**.

IP-адреса шлюза по умолчанию для VLAN (эти адреса назначаются на подынтерфейсах маршрутизатора R1):

VLAN	IP-адрес
VLAN 2	10.0.2.1 /24
VLAN 10	10.0.10.1 /24
VLAN 15	10.0.15.1 /24

Для логических подынтерфейсов необходимо указывать то, что интерфейс будет получать тегированный трафик и указывать номер VLAN соответствующий этому интерфейсу. Это задается командой в режиме настройки подынтерфейса: `encapsulation dot1q <vlan-id>`

Создание логического подынтерфейса для VLAN 2:

```
R1(config)# interface fa0/0
R1(config-if)# no shutdown
```

```
R1(config-if)# interface fa0/0.2
R1(config-subif)# encapsulation dot1q 2
R1(config-subif)# ip address 10.0.2.1 255.255.255.0
```

Создание логического подынтерфейса для VLAN 10:

```
R1(config)# interface fa0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 10.0.10.1 255.255.255.0
```

На **коммутаторе** порт, ведущий к маршрутизатору, должен быть настроен как статический транк:

```
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

4.4 Лабораторная работа. Настройка сети малого офиса

Задание на работу

1. Собрать сеть, согласно схеме ниже (рисунок 39).

2. Настроить разделение сети на сегменты в соответствии с номерами VLAN на схеме. На коммутаторе Sw1 портам fa0/1-4 назначить VLAN 10, остальные порты отключить командой shutdown.

На коммутаторе Sw2:

- портам fa0/1-2 (подключить к Sw1 и Точке доступа 1) назначить VLAN 10,
- порту fa0/3 (подключить к Точке доступа 2) назначить VLAN 20,
- порту fa0/4 (подключить к Точке доступа 3) назначить VLAN 30,
- порт fa0/5 (подключить к R1) перевести в режим trunk и разрешить трафик для VLAN 10, 20, 30,
- остальные порты отключить.

3. Настроить маршрутизацию между VLANми на маршрутизаторе.

4. Настроить автоматическую раздачу IP-адресов по протоколу DHCP для сотрудников, клиентов и гостей.

Настройка DHCP на маршрутизаторе для сети 192.168.10.1/24 осуществляется следующим образом:

```
R1(config)#ip dhcp pool POOL_vlan10
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#exit
```

Для сетей 192.168.20.1/24 и 192.168.30.1/24 настройка аналогичная.

4) Для трех точек доступа настроить беспроводные сети следующим образом:

Wi-Fi сеть для сотрудников:
SSID: worker
Пароль: 123
Метод аутентификации: WPA2-PSK
Метод шифрования: AES
Номер частотного канала: 11

Wi-Fi сеть для клиентов:
SSID: client
Пароль: client456
Метод аутентификации: WPA-PSK
Метод шифрования: AES
Номер частотного канала: 11

Wi-Fi сеть для гостей:
SSID: guest
Пароль: guest789
Метод аутентификации: WPA-PSK
Метод шифрования: AES
Номер частотного канала: 1

5) На маршрутизаторе провайдера в режиме глобальной конфигурации прописать команду:

```
ip route 192.168.0.0 255.255.0.0 200.45.XX.2
```

где XX – порядковый номер студента в списке группы.

6) Проверить связь между устройствами.

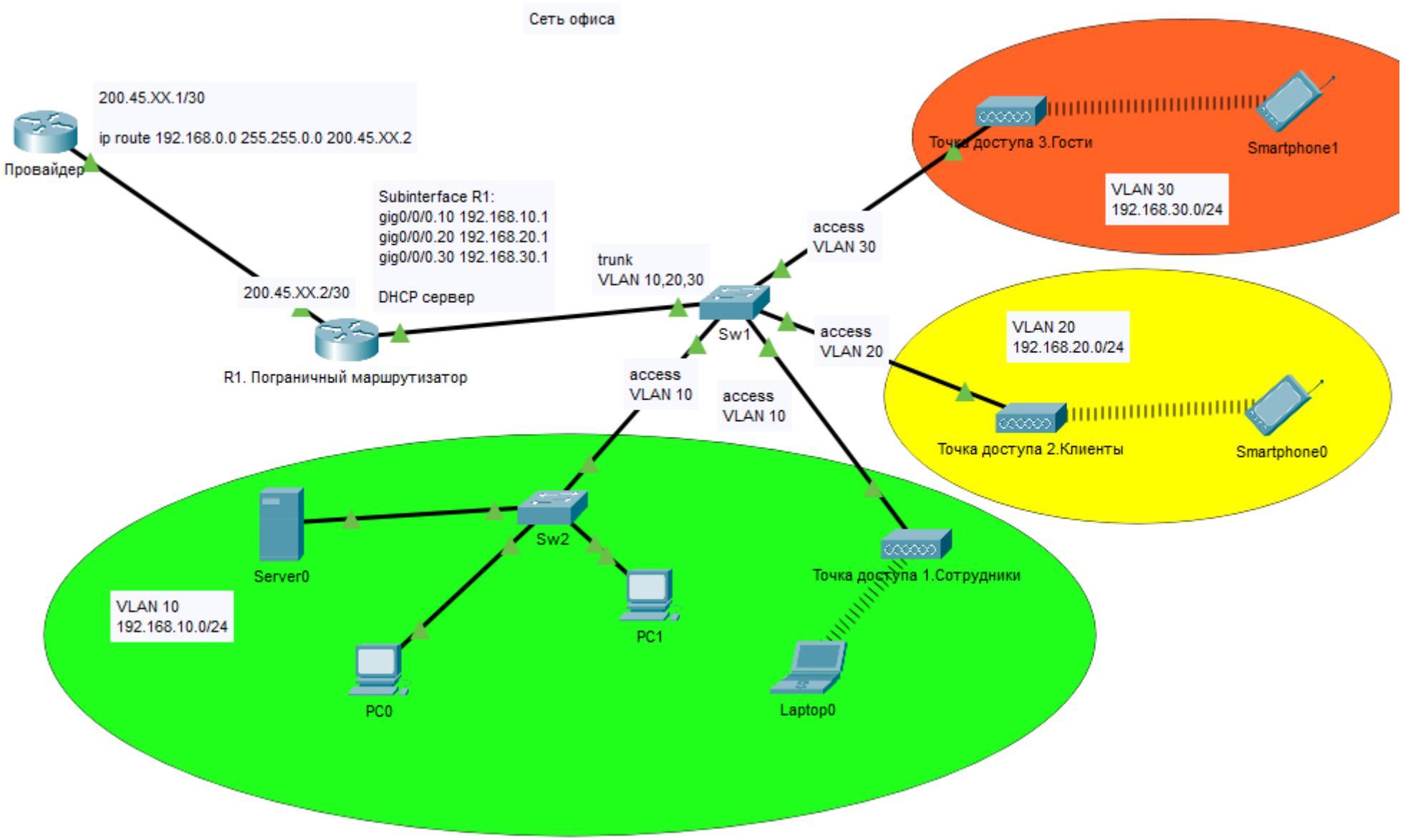


Рисунок 39 – Топология сети

5 Технология трансляции адресов (NAT)

5.1 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.

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 (рисунок 40). Stub-сеть – это тупиковая сеть, которая имеет одно соединение с соседней сетью, один вход и выход из сети.

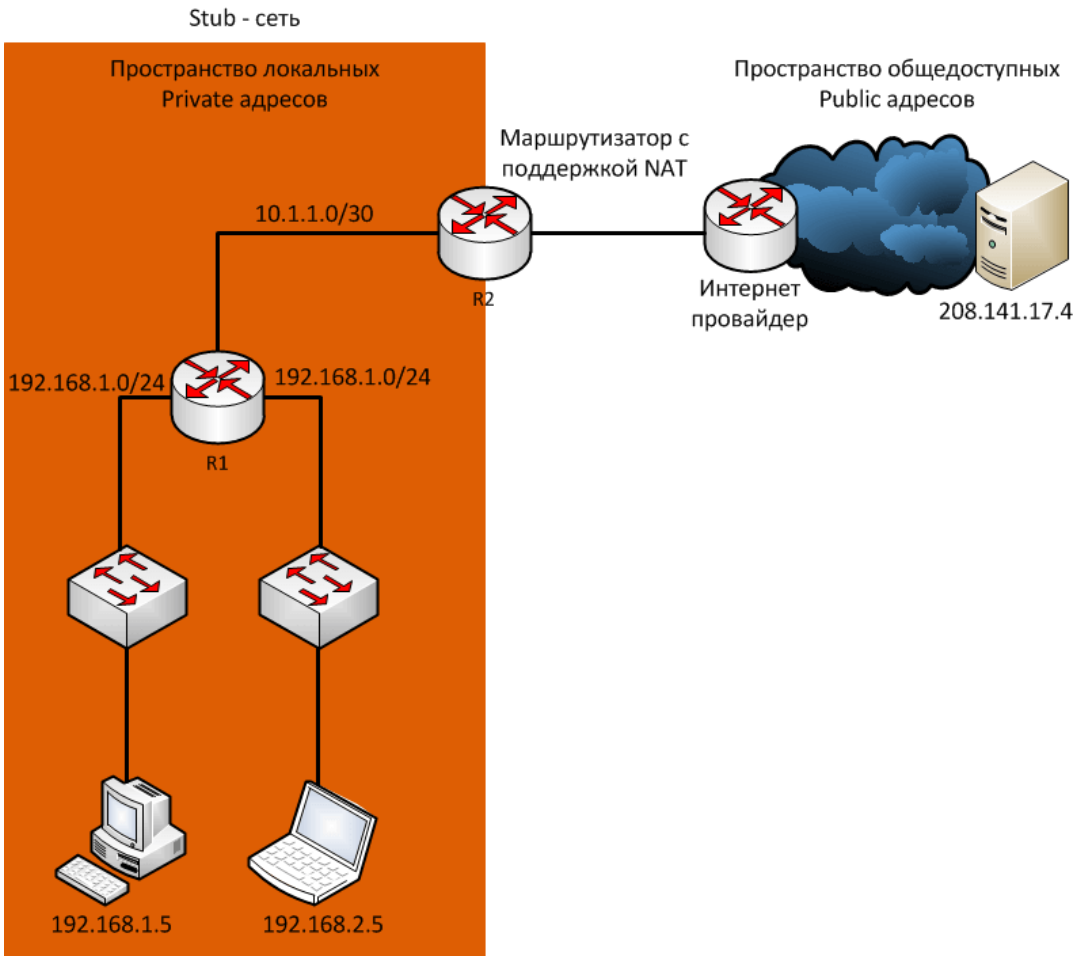


Рисунок 40 – Stub-сеть

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.

5.2 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, основанные на том, находятся ли они в частной сети или в общедоступной сети (в интернете), и является ли трафик входящим или исходящим.

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:

- **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, изображенной на рисунке 41.

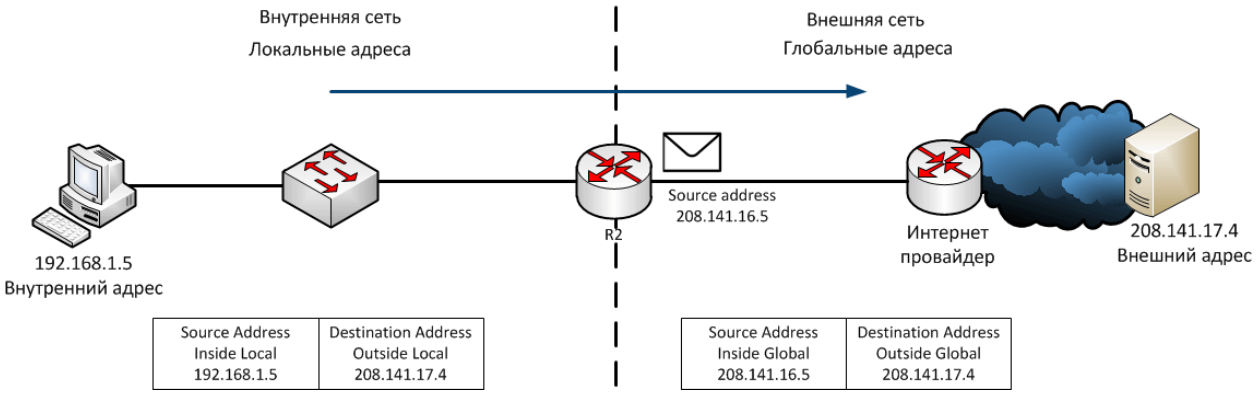


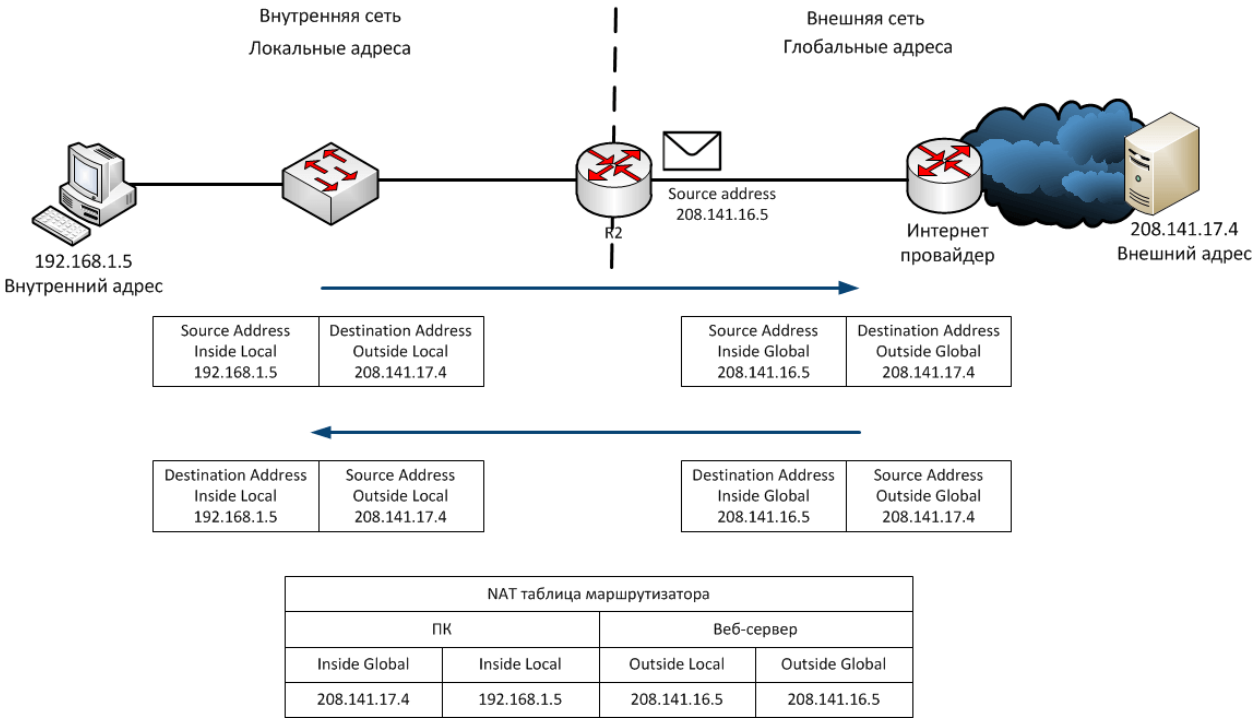
Рисунок 41 – Адреса для технологии NAT

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 42 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

Рисунок 42 – Трансляция адресов технологии 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.

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.

5.3 Типы NAT

Существует три типа трансляции NAT:

1. Статическая адресная трансляция (Static NAT) - сопоставление адресов один к одному между локальными и глобальными адресами;
2. Динамическая адресная трансляция (Dynamic NAT) - сопоставление адресов «многие ко многим» между локальными и глобальными адресами;
3. Port Address Translation (PAT) - многоадресное сопоставление адресов между локальными и глобальными адресами с использованием портов. Также этот метод известен как NAT Overload.

5.3.1 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, как показано на рисунке 43.

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

Рисунок 43 - Статическая NAT таблица

5.3.2 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, как показано на рисунке 44.

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

Рисунок 44 - Динамическая NAT таблица

5.3.3 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.

Рисунок 45 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

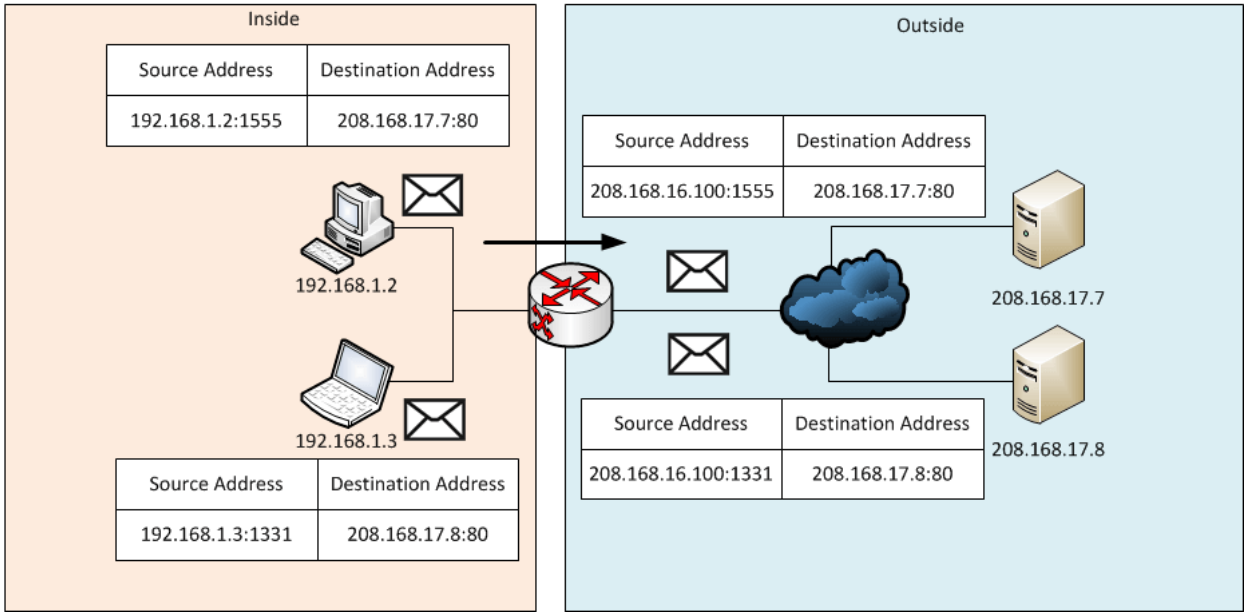


Рисунок 45 – Процесс PAT

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.

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.

А что относительно пакетов IPv4, содержащих данные, отличные от TCP или UDP? 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. 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.

5.4 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;

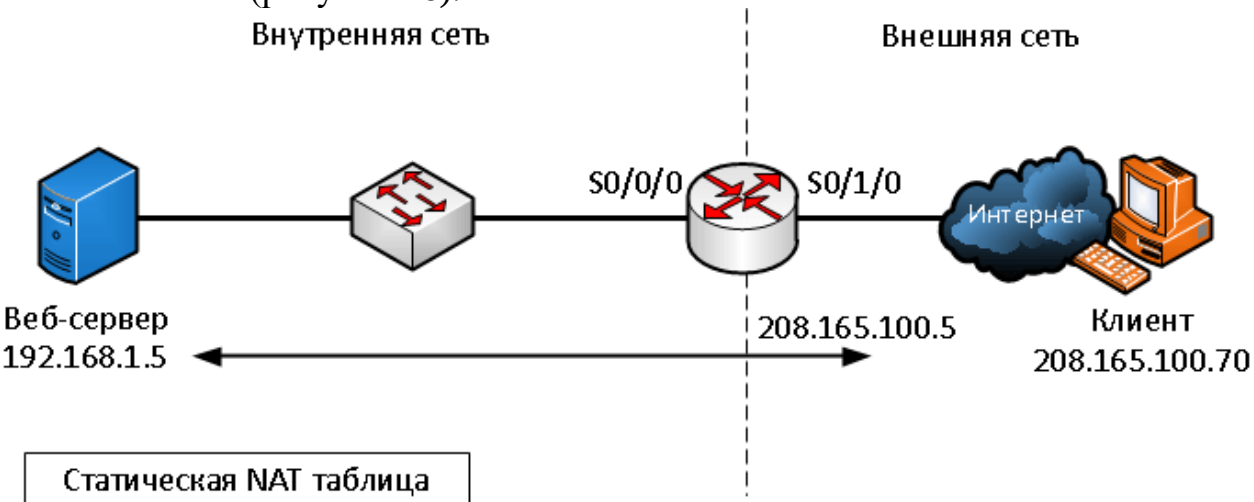
Но у NAT есть некоторые недостатки. Тот факт, что хосты в Интернете, по-видимому, напрямую взаимодействуют с устройством с поддержкой NAT, а не с фактическим хостом внутри частной сети, создает ряд проблем:

- 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;

5.5 Практическая работа. 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.

Например, внутренний веб-сервер может быть сопоставлен с определенным внутренним глобальным адресом, чтобы он был доступен из внешних сетей (рисунок 46).



Статическая NAT таблица	
Inside Global	Inside Local
208.165.100.5	192.168.1.5

Рисунок 46 – Статический NAT

На схеме (рисунок 46) 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**

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
```

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.

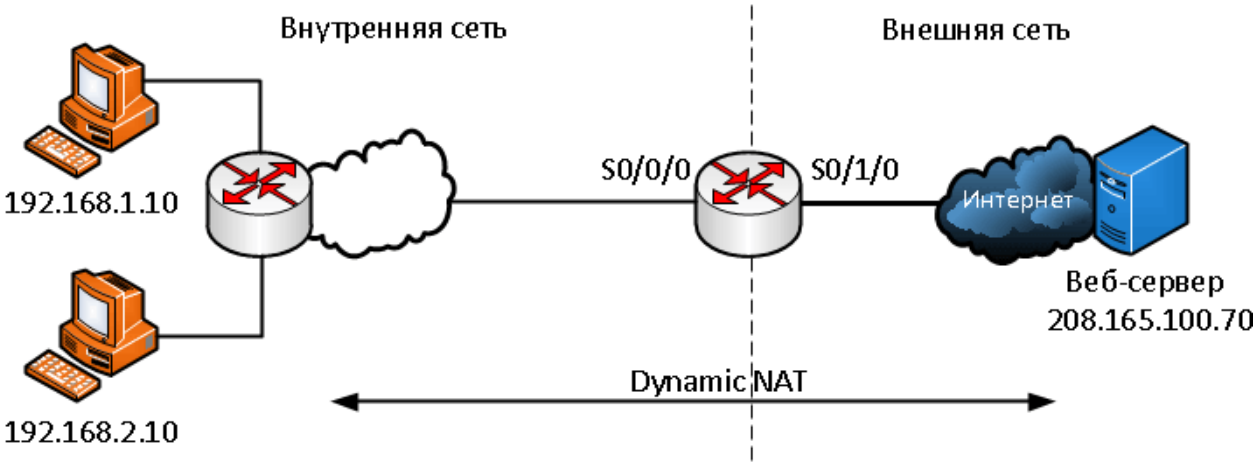
```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:21 ago
Outside interfaces:
        Serial0/1/0
Inside interfaces:
        Serial0/0/0
Hits:7 Misses:0
```

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

5.6 Практическая работа. Настройка динамического NAT (Dynamic NAT)

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.

Рассмотрим работу динамического NAT на примере схемы, изображенной на рисунке 47. Мы 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.



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

Рисунок 47 – Динамический NAT

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 источнике [5] (а про расширенные в источнике [6]). 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**.

5.6 Практическая работа. 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:

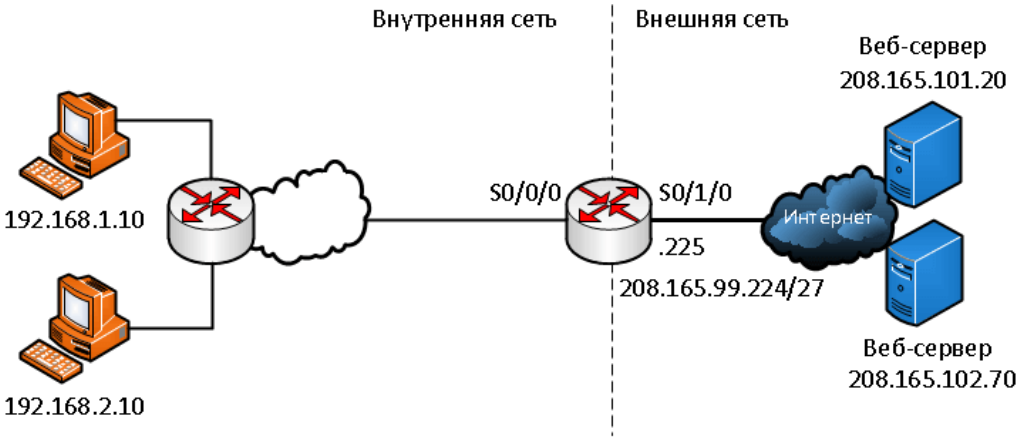
1. Определить пул адресов глобальных адресов, которые будут использоваться для PAT трансляции, используя команду **ip nat pool [имя начальный_ip конечный_ip] netmask [маска] | prefix-length [длина_префикса]**.
2. Создать стандартный access-list, разрешающий адреса, которые должны быть переведены. Используется 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 (рисунок 39), 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

На схеме (рисунок 48) 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.



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

Рисунок 48 - Топология реализации PAT для одного публичного 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**.

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 inside 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.

5.8 Лабораторная работа. Настройка сети с технологией PAT

Задание лабораторной работы

Создать простую сеть с использование технологии PAT (перегруженный NAT). Схема сети представлена на рисунке 49. Вся работа будет выполняться в программе Cisco Packet Tracer.

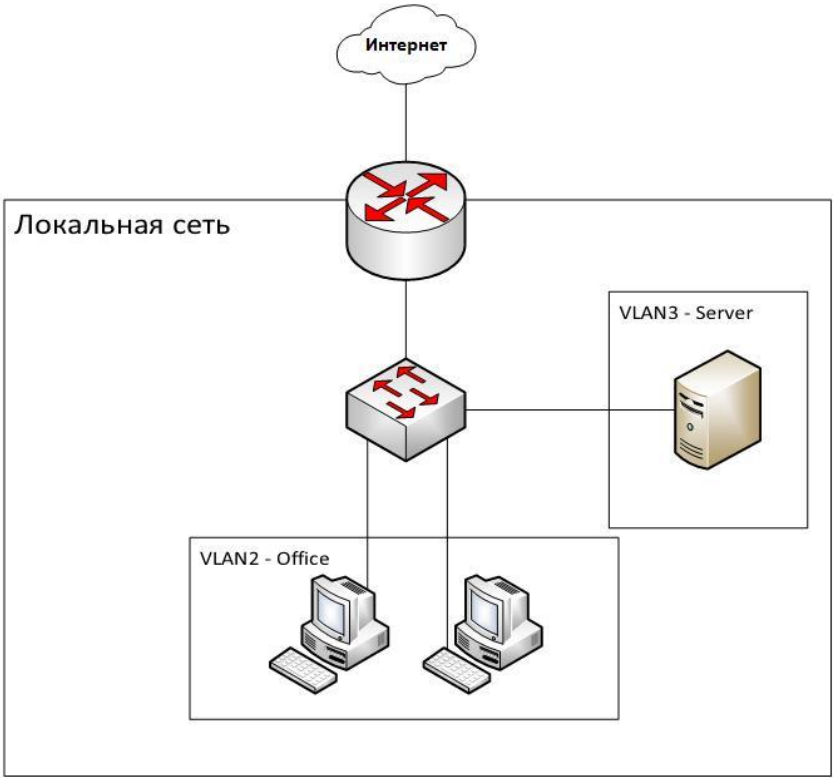


Рисунок 49 – Схема сети

Выполнение лабораторной работы

1) Создать на рабочей панели Packet Tracer 2 ПК, сервер, коммутатор и 2 маршрутизатора и соединить все устройства как показано на рисунке 50.

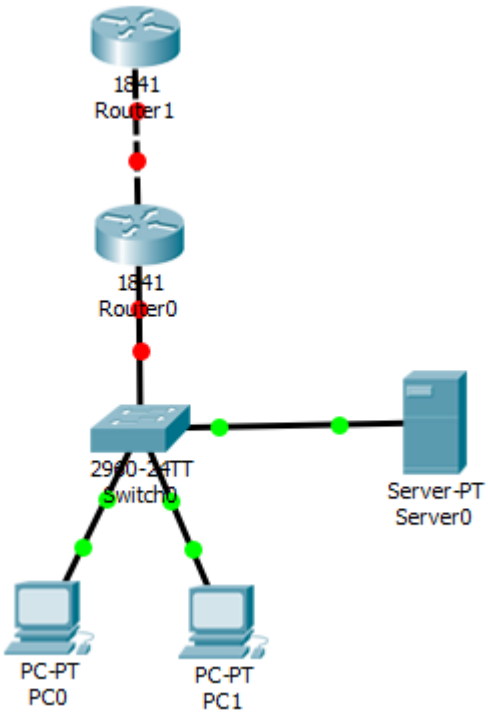


Рисунок 50 – Схема сети

2) На коммутаторе настроить 2 сети VLAN, чтобы схема работы получилась, такая, как на рисунке 51.

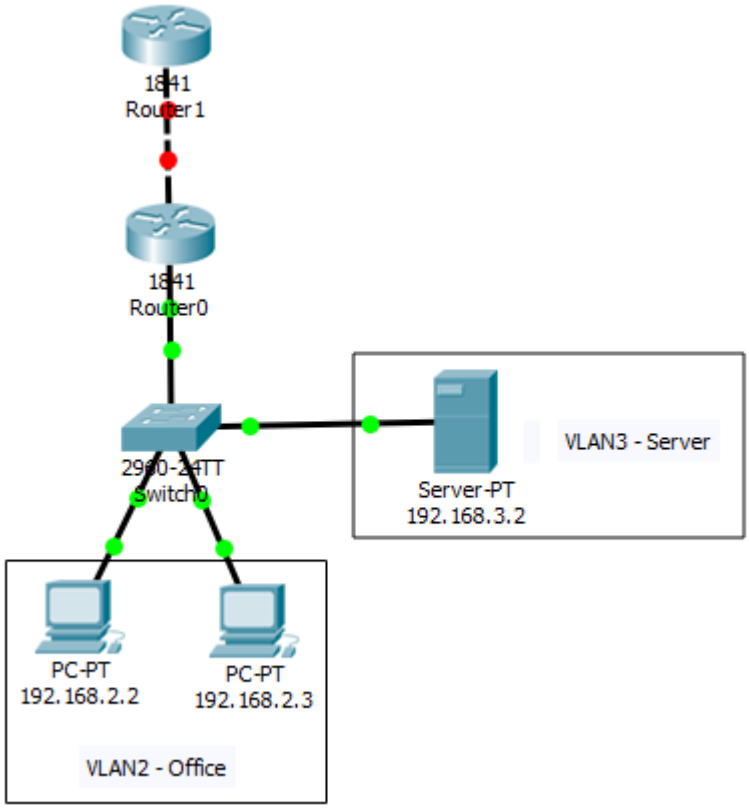


Рисунок 51 – Схема сети с настроенными VLAN

3) Настроить на Router0 маршрутизацию между VLAN. Проверить связь между ПК и сервером.

4) Настроить маршрутизаторы. На Router1 выставить на порту, который связан с Router0 кросс-кабелем, белый IP адрес. Например, 120.120.53.1. На Router0 выставить белый IP из той же сети (например, 120.120.53.2). Таким образом мы смоделировали ситуацию подключения Интернета от провайдера. Проверить связь с удаленным маршрутизатором (120.120.53.1). Связь должна отсутствовать. Объясните почему.

5) Теперь настроим PAT с access листом. Это нужно для того, чтобы мы могли расширить нашу сеть и подключить несколько VLAN. Обратите внимание на нашу схему. По ней можно увидеть то, что локальная сеть заканчивается на нулевом маршрутизаторе. На нём же начинается выход в интернет по публичному IP. Поэтому, именно на нём мы и будем настраивать PAT. Для начала нам нужно определить какой интерфейс для PAT будет внешним, а какой внутренним. Внешний интерфейс – это тот, который выходит в сеть Интернет, а внутренний – который внутри локальной сети. То есть, в нашем случае, внешний – fa0/0, а внутренних два, так как два отдела (fa0/0.2 и fa0/0.3).

6) Настроим нулевой маршрутизатор для работы с PAT. Исходя из пункта 5, введём следующие команды:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int fa0/1.2
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/1.3
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#end
Router#wr mem
```

7) Создадим на этом-же роутере access лист для того, чтобы роутер «понимал» что ему натить. Введём следующие команды:

```
Router>en
Router#conf t
Router(config)#ip access-list standard TEST_TUSUR
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.3.0 0.0.0.255
Router(config-std-nacl)#end
```

8) Проверить настройки можно командой **show run**. Для старта работы PAT потребуется ввести ещё одну команду в настройках конфигураций:

```
ip nat inside source list TEST_TUSUR int fa0/0 overload
```

9) Проверяем подключение к Интернету.

Описание команд:

ip access-list standard TEST_TUSUR – создаём стандартный access лист с именем TEST_TUSUR

permit 192.168.2.0 0.0.0.255 – добавляем адреса сетей с обратной маской сети

ip nat inside source list TEST_TUSUR int fa0/0 overload – начинаем путь NAT изнутри (из инсайда) по access листу под названием TEST_TUSUR на интерфейсе int fa0/0. Overload указывает на тип NAT, а именно перегруженный NAT, то есть PAT.

6 Безопасность портов коммутатора

6.1 Настройка Cisco Port-Security

Port-Security – это функция коммутатора, при помощи которой мы можем указать каким устройствам можно пропускать трафик через определенные порты. Устройство определяется по его **MAC**-адресу.

Эта функция предназначена для защиты от несанкционированного подключения к сети и атак, направленных на переполнение таблицы MAC-адресов. При помощи нее мы можем указывать конкретные адреса, с которых разрешен доступ или указывать максимальное количество MAC-адресов, которые могут передавать трафик через порт.

Типы Port-Security

Существует несколько способов настройки port-security:

- **Статические MAC-адреса** – MAC-адреса, которые вручную настроены на порту, из режима конфигурации порта при помощи команды **switchport port-security mac-address [MAC-адрес]**. MAC-адреса, сконфигурированные таким образом, сохраняются в таблице адресов и добавляются в текущую конфигурацию коммутатора.
- **Динамические MAC-адреса** - MAC-адреса, которые динамически изучаются и хранятся только в таблице адресов. MAC-адреса, сконфигурированные таким образом, удаляются при перезапуске коммутатора.
- **Sticky MAC-адреса** - MAC-адреса, которые могут быть изучены динамически или сконфигурированы вручную, затем сохранены в таблице адресов и добавлены в текущую конфигурацию.

6.2 Sticky MAC-адреса

Если необходимо настроить port-security со **sticky** MAC-адресами, которые преобразуются с из динамически изученных адресов и добавляются в текущую конфигурацию, то необходимо настроить так называемое sticky изучение. Для того чтобы его включить необходимо на интерфейсе коммутатора выполнить команду **switchport port-security mac-address sticky** из режима конфигурации интерфейса.

Когда эта команда введена, коммутатор преобразует все динамически изученные MAC-адреса (включая те, которые были динамически изучены до того, как было включено sticky обучение) к sticky MAC-адресам. Все sticky MAC-адреса добавляются в таблицу адресов и в текущую конфигурацию.

Также sticky адреса можно указать вручную. Когда sticky MAC-адреса настроены при помощи команды **switchport port-security mac-address sticky [MAC-адрес]**, все указанные адреса добавляются в таблицу адресов и текущую конфигурацию.

Если sticky MAC-адреса сохранены в файле конфигурации, то при перезапуске коммутатора или отключении интерфейса интерфейс не должен будет переучивать адреса. Если же sticky адреса не будут сохранены, то они будут потеряны.

Если sticky обучение отключено при помощи команды **no switchport port-security mac-address sticky** , то эти адреса будут оставаться в таблице адресов, но удалятся из текущей конфигурации.

Обратите внимание, что port-security не будут работать до тех пор, пока не будет введена команда, включающая его - **switchport port-security**

6.3 Нарушение безопасности

Нарушением безопасности являются следующие ситуации:

- Максимальное количество MAC-адресов было добавлено в таблицу адресов для интерфейса, а устройство, MAC-адрес которого отсутствует в таблице адресов, пытается получить доступ к интерфейсу.
- Адрес, полученный или сконфигурированный на одном интерфейсе, отображается на другом интерфейсе в той же VLAN.

На интерфейсе может быть настроен один из трех режимов реагирования при нарушении:

- **Protect** - когда количество MAC-адресов достигает предела, разрешенного для порта, пакеты с неизвестными исходными адресами отбрасываются до тех пор, пока не будет удалено достаточное количество MAC-адресов или количество максимально допустимых адресов для порта не будет увеличено. Уведомление о нарушении безопасности отсутствует в этом случае.
- **Restrict** – то же самое, что и в случае Protect, однако в этом случае появляется уведомление о нарушении безопасности. Счетчик ошибок увеличивается
- **Shutdown** – стандартный режим, в котором нарушения заставляют интерфейс немедленно отключиться и отключить светодиод порта. Он также увеличивает счетчик нарушений. Когда порт находится в этом состоянии (**error-disabled**), его можно вывести из него введя команды **shutdown и no shutdown** в режиме конфигурации интерфейса.

Чтобы изменить режим нарушения на порту коммутатора, используется команда **port-security violation {protect | restrict |shutdown}** в режиме конфигурации интерфейса.

Таблица 2. Режимы реагирования при нарушении

Режим реагирования	**Передача траффика**	**Отправка сообщения syslog**	**Отображение сообщения об ошибке**	**Увеличение счетчика нарушений**	**Выключение порта**
Protect	Нет	Нет	Нет	Нет	Нет
Restrict	Нет	Да	Нет	Да	Нет
Shutdown	Нет	Нет	Нет	Да	Да

6.4 Практическая работа. Настройка Port-Security

Первым шагом при настройке Port-Security необходимо включить данную функцию на необходимом порту коммутатора.

```
S1#configure terminal
S1(config)#interface fastEthernet 0/11
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
```

Таким образом, мы включили на интерфейсе эту функцию со значениями по умолчанию, а именно:

- Максимум 1 MAC адрес на порту
- Режим запоминания динамический (в оперативной памяти, без sticky)
- Действие при появлении второго MAC адреса – отключение порта

Это легко проверить, если подключить компьютер к 11-му порту, пропинговать что-то, а потом сменить MAC и снова попробовать пропинговать. Порт отключится и перейдёт в состояние err-disable. Чтобы снова включить порт, надо его потушить и включить:

```
S1(config)#interface fastEthernet 0/11
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed
state to up
```

Текущие настройки port security можно увидеть с помощью команды:

```
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
---------------------------------------------------------------------
        Fa0/11        1          1                 0         Shutdown
---------------------------------------------------------------------
```

Из таблички видно, что максимум 1 MAC и он уже изучен, действие – Shutdown.

Если коммутатор перезагрузить, то запомненный MAC забудется и надо будет его заново изучать, чтобы этого избежать, надо включить «липкое» заучивание MAC-ов. Заодно давайте увеличим количество с одного до пяти:

```
S1(config)#interface fastEthernet 0/11
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security maximum 5
```

Если мы хотим статически вручную перечислить адреса, то вместо слова sticky (или параллельно с ним – отдельной строчкой) мы можем их перечислять командой:

```
S1(config-if)#switchport port-security mac-address 1234.abcd.1234
```

Но предположим, что мы не добавляли MAC статически, а просто включили sticky режим. Пробуем пропинговать с компьютера, после чего смотрим конфиг:

```
S1#show running-config
Building configuration...
Current configuration : 1185 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
…
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.4276.96B5
…
```

Что мы видим? Строка «switchport port-security mac-address sticky 0001.4276.96B5» говорит о том, что адрес компьютера запомнился и «прилип к порту», как будто мы сами его туда вбили статически. Если теперь сохранить конфиг, то после перезагрузки адрес не пропадёт и коммутатор не надо будет заново обучать.

6.5 Лабораторная работа. Настройка параметров безопасности коммутатора локальной сети

Задачи

1. Настройка топологии и инициализация устройств в соответствии со схемой сети (рисунок 52) и таблицей адресации

2. Конфигурация основных параметров устройств и проверка соединения

3. Конфигурирование и проверка доступа с помощью протокола SSH на коммутаторе

S1_ФАМИЛИЯ

– Настройте доступ по протоколу SSH.
– Измените параметры SSH.
– Проверьте конфигурацию SSH.

4. Настройка и проверка параметров безопасности для S1_ФАМИЛИЯ

– Настройте и проверьте общие функции безопасности.
– Настройте и проверьте функцию безопасности порта

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	172.16.XX.1	255.255.255.0	–
S1_ФАМИЛИЯ	VLAN XX	172.16.XX.11	255.255.255.0	172.16.XX.1
PC-A	NIC	172.16.XX.3	255.255.255.0	172.16.XX.1

Рисунок 52 – Схема сети

7 Контрольные вопросы

1. В каких частотных диапазонах работает Wi-Fi?
2. Перечислите основные устройства, используемые для построения беспроводных сетей.
3. Опишите основные способы использования Wi-Fi.
4. Перечислите основные этапы настройки домашней беспроводной сети.
5. Перечислите основные этапы настройки беспроводной сети малого офиса.
6. В каких случаях и для чего применяется технология VLAN?
7. Опишите принцип работы технологии VLAN.
8. Чем access порт коммутатора отличается от trunk порта?
9. В каких случаях применяется технология трансляции адресов (NAT)?
10. Какой тип NAT чаще всего используется в домашних сетях и сетях малых предприятий?
11. Назовите принципиальное отличие PAT от NAT.
12. Для чего настраивается на коммутаторе Cisco Port-Security?

Список рекомендуемой литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. Санкт-Петербург: Питер. 2020. 1008 с.

2. Таненбаум Э.С., Фимстер Н., Уэзеролл Д. Компьютерные сети. 6-е изд. СПб.: Питер, 2023. 992 с.

3. Технологии современных беспроводных сетей Wi-Fi: учебное пособие / Е.В. Смирнова, А.В. Пролетарский, Е.А. Ромашкина, С.А. Балюк, А.М. Суворов; под общ. ред. А. В. Пролетарского. Москва: Издательство МГТУ им. Н.Э. Баумана, 2017. 446 с.

4. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд.: Пер. с англ. М.: ООО «И.Д. Вильямс», 2015. 736 с.

5. Стандартные листы контроля доступа (ACL): [Электронный ресурс]. URL: https://wiki.merionet.ru/articles/standartnye-listy-kontrolya-dostupa-acl/ (Дата обращения 18.09.2023).

6. Расширенные листы контроля доступа (Extended ACL): [Электронный ресурс]. URL: https://wiki.merionet.ru/articles/rasshirennye-listy-kontrolya-dostupa-extended-acl/ (Дата обращения 18.09.2023).

Заключение

В учебно-методическом пособии рассмотрены вопросы построения беспроводных локальных сетей по стандарту IEEE 802.11 (Wi-Fi), а также ряд вопросов оптимизации работы локальных сетей. В частности, описаны технология разделения локальной сети на подсети с использованием виртуальных локальных сетей (VLAN), технология трансляции сетевых адресов (преобразование частных IP-адресов в глобальные IP-адреса) и методы повышения безопасности коммутаторов на основе анализа MAC-адресов подключенных устройств.

В каждом разделе содержатся задания для практических и лабораторных работ, которые выполняются в программе сетевого моделирования Cisco Packet Tracer.