МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Методические указания
по выполнению лабораторных работ по дисциплине
для студентов дневного и заочного отделения,
обучающихся по направлениям
09.04.02 «Информационные системы и технологи»,
09.04.03 «Прикладная информатика»

Севастополь
СевГУ
2023

УДК 004.7:004.056.5(076.5)
ББК 32.973.202я73
Б399

Р е ц е н з е н т :
К. В. Кротов - доцент кафедры «Информационные системы»,
д-р техн. наук, доцент

Составитель: В. С. Чернега

Б399 Безопасность компьютерных сетей : методические указания к выполнению лабораторных работ по дисциплине для студентов дневного и заочного отделения, обучающихся по направлениям 09.04.02 «Информационные системы и технологи», 09.04.03 «Прикладная информатика» / Севастопольский государственный университет ; сост. В. С. Чернега. – Севастополь : СевГУ, 2023. – 74 с. – Текст : электронный.

Цель указаний: помочь студентам в изучении и исследовании способов обеспечения безопасности доступа к ресурсам сети, конфигурации инфокоммуникационного оборудования для реализации безопасной работы в проводных и беспроводных локальных компьютерных сетях.

Предназначены для выполнения лабораторных работ по дисциплине «Безопасность компьютерных сетей» для студентов дневной и заочной форм обучения.

УДК 004.7:004.056.5(076.5)
ББК 32.973.202я73

Методические указания рассмотрены и рекомендованы к изданию на заседании кафедры «Информационные системы», протокол № 9 от 26 апреля 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время компьютерные сети используются практически во всех сферах человеческой деятельности, что привлекает различного рода злоумышленников, которые стремятся похитить конфиденциальную информацию, либо нарушить штатное функционирование сети. Поэтому проблема безопасности компьютерных сетей является весьма актуальной.

Для обеспечения эффективной защиты информации в компьютерной сети проектирование и внедрение системы защиты должно осуществляться в три этапа: анализ рисков; разработка политики безопасности; реализация политики безопасности.

В процессе изучения дисциплины «Безопасность компьютерных сетей» студенты-магистранты должны изучить уязвимости и угрозы безопасности, ознакомиться с принципами построения и реализации политики безопасности, способами защиты ресурсов компьютерных сетей.

Целью лабораторных работ по данной дисциплине является углубление теоретических знаний в области безопасности компьютерных сетей, а также приобретение практических навыков исследования функционирования локальных проводных и беспроводных компьютерных сетей, выявления слабых мест, разработка сценариев конфигурирования сетевого оборудования для повышения безопасности отдельных сегментов компьютерных сетей.

Выполнение лабораторных работ осуществляется в виртуальной среде эмулирования компьютерных сетей Cisco Packet Tracer (CPT). Интерфейсы конфигурация сетевого оборудования в среде CPT практически не отличаются от интерфейсов конфигурации реального сетевого оборудования.

Выполнение лабораторных работ по дисциплине «Безопасность компьютерных сетей» предполагает знание дисциплины «Инфокоммуникационные системы и сети», которая входит в учебный план подготовки бакалавров по направлениям «Информационные системы и технологии» и «Прикладная информатика». Предполагается, что студенты знакомы с системой Cisco Packet Tracer. Для студентов, не работавших ранее с этой системой, предусмотрено выполнение лабораторной работы по изучению среды CPT и приобретению практических навыков исследования компьютерных сетей в этой среде.

Лабораторная работа 1
ИЗУЧЕНИЕ СИСТЕМЫ МОДЕЛИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ CISCO PACKET TRACER

1 ЦЕЛЬ РАБОТЫ

Целью работы является изучение системы моделирования компьютерных сетей, исследование способов построения локальных компьютерных сетей (ЛКС) и конфигурации коммуникационного оборудования, а также приобретение практических навыков конфигурации и исследования функционирования ЛКС.

2 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

В качестве лабораторной установки используется персональный компьютер с установленной свободно распространяемой системой моделирования компьютерных сетей Packet Tracer, позволяющей осуществлять моделирования компьютерных сетей, построенных на оборудовании корпорации Cisco. Симулятор Cisco Packet Tracer поддерживает интерфейс командной строки Cisco IOS для конфигурирования устройств. С помощью этой программы можно создавать, настраивать, изучать сети и устранять неполадки, используя виртуальное оборудование и модели соединений.

Packet Tracer позволяет моделировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, концентраторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д. Интерактивное взаимодействие пользователей с симулятором дает весьма правдоподобное ощущение настройки реальной сети.

Среда Packet Tracer позволяет настраивать оборудование, используемое в сети, удобным для пользователя образом. Предусмотрено управление сетевыми устройствами с помощью команд операционной системы Cisco IOS, за счет графического интерфейса или использования интерфейса командной строки CLI (Command Line Interface). Несмотря на то, что на данном сетевом симуляторе реализованы не все функции операционной системы Cisco IOS, функциональность, которую обеспечивает программа симуляции, хватает для построения большинства типов сетевых систем и понимания технологических принципов их конфигурации и функционирования.

Packet Tracer поддерживает режим визуализации, с помощью которого пользователь может отследить перемещение данных по сети, появление и изменение параметров пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения пакетов. Таким образом, анализ событий,

происходящих в сети, позволяет понять и исследовать механизм ее работы и обнаружить неисправности.

На основе Cisco Packet Tracer пользователь может строить не только логическую, но и физическую модель сети и, следовательно, получать навыки проектирования. Созданную в учебной среде схему сети можно наложить на чертеж реально существующего здания. С учетом физических ограничений в тех или иных помещениях можно спроектировать размещение устройств, длину и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

2.1 Рабочее окно симулятора Cisco Packet Tracer

При запуске программы Cisco Packet Tracer на экране компьютера появляется главное окно симулятора (рисунок 2.1).

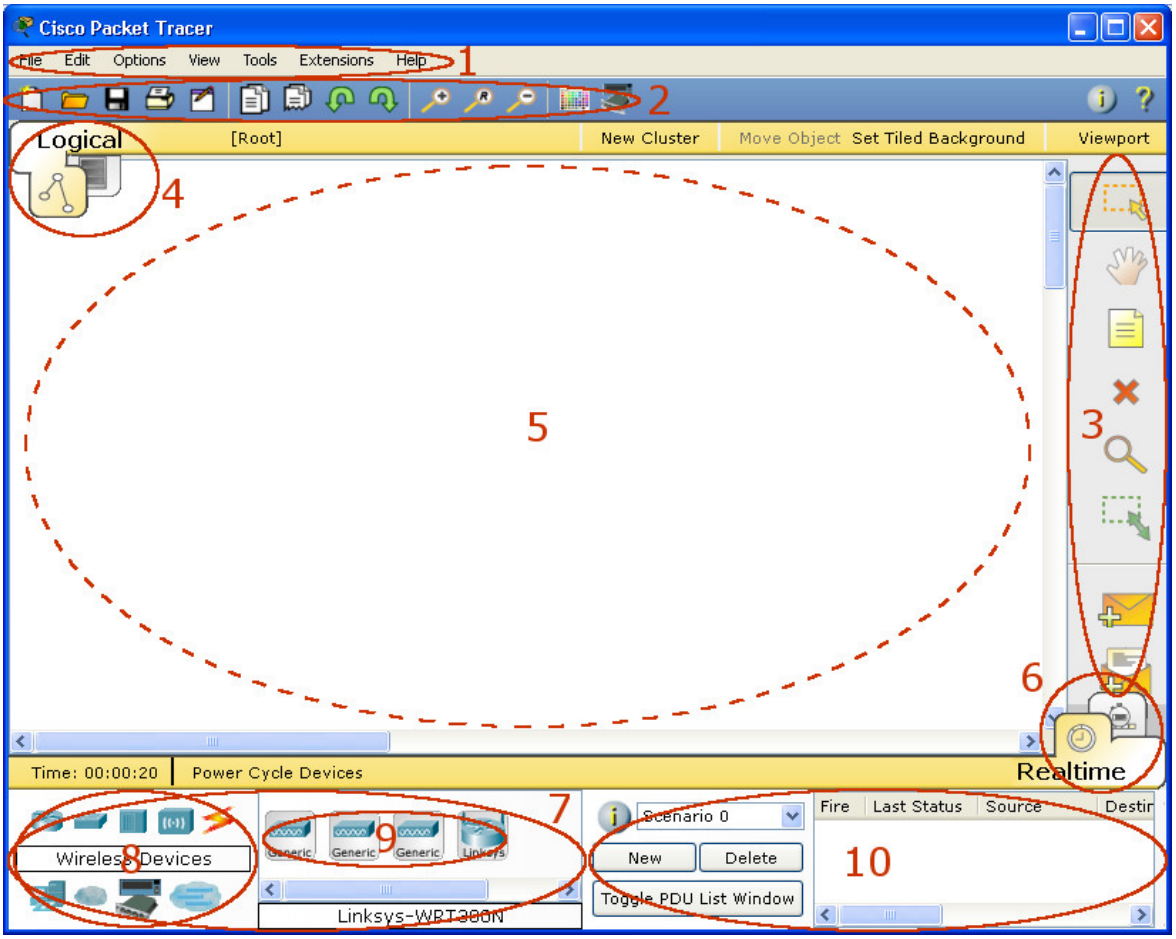


Рисунок 2.1 – Главное окно программы Cisco Packet Tracer

Основными составляющими симулятора являются следующие.

1. Главное меню программы:

– Файл – содержит операции открытия / сохранения документов;

- Правка – стандартные операции «копировать / вырезать, отменить / повторить»;
- Настройки/Параметры – параметры анимации, профиль пользователя;
- Вид – масштаб рабочей области и панели инструментов;
- Инструменты – цветовая палитра и окно пользовательских устройств;
- Расширения – мастер проектов, многопользовательский режим;
- Помощь/Справка – справочная информация.

2. Панель инструментов, часть которых дублирует пункты меню (содержит кнопки быстрого вызова команд из меню *File* и *Edit* а так же команд *Zoom, Drawing Palette и Custom Devices Dialog*).

3. Панель инструментов рабочей области содержит наиболее часто используемые операции, применяемые при построении модели сети: инструменты выделения, удаления, перемещения, масштабирования объектов, а также формирование произвольных пакетов.

4. Навигационная панель позволяет переключать рабочую область между логической и физической топологией сети. Физическая топология подразумевает расположение устройств в городе, районе, офисе. Здесь можно посмотреть, как топологию сети всего города, так и расположение устройств в офисе.

5. Рабочая область занимает большую часть окна программы. Здесь происходит конструирование виртуальной сети, где размещаются устройства и строятся связи между ними. Двойной клик по любому устройству открывает окно его конфигурации. Окно конфигурации устройств состоит из 3-х вкладок:

- *Phusical* – внешний вид устройства и позволяет добавлять/убирать модули. Модули нельзя добавлять/извлекать при включенном устройстве. Перед их сменой следует отключить питание устройства, а после замены или добавления интерфейса снова включить.;
- *Config* – эта вкладка не открывается, пока устройство не загрузилось. Здесь осуществляется графическое конфигурирование оборудования Cisco без применения командной строки, но для информативности внизу отображаются команды, которые выполняются при конфигурации;
- *CLI/Desktop* – в зависимости от устройства позволяет получить доступ к командной строке IOS либо к рабочему столу Linux.

6. Панель симуляции/реального времени. После запуска программа находится в логическом режиме реального времени, можно строить сеть и смотреть, как она работает. Данная панель позволяет переключаться в режим симуляции и обратно. В этом режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет наглядно видеть, по какому интерфейсу в данный момент перемещается пакет, какой протокол используется и т.д. В режиме симуляции *Simulation* (правая клавиша внизу) можно не только отслеживать движение кадров (в виде конвертов) и используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован.

7. Блок выбора сетевых компонентов. Окно выбора устройств либо способов связи, размещаемых в рабочей области. Состоит из двух составных частей: области выбора типа устройства и области выбора конкретной модели устройства.

8. Окно типа устройств. Позволяет выбрать и моделировать большое количество устройств различного назначения: маршрутизаторы, коммутаторы (в том числе и мосты), хабы и повторители, конечные устройства – ПК, серверы, принтеры, IP-телефоны; безпроводные устройства: точки доступа и безпроводные маршрутизаторы; другие устройства – Internet-облако, DSL-модем и кабельный модем, а также разнообразные линии связи от консольного кабеля до оптической линии.

9. Окно моделей устройств. Область выбора конкретной модели устройства указанного типа. В частности, Packet Tracer может моделировать следующие телекоммуникационные устройства: маршрутизаторы типов 1841, 2620XM, 2621XM, 2811; коммутаторы типов 2959-24, 2950T, 2960, 3560; беспроводные устройства типа Linksys-WRT300N и др.

10. Окно пользовательских пакетов. Окно управляет пакетами, которые были созданы в сети во время сценария симуляции.

2.2 Оборудование и линии связи в Cisco Packet Tracer

2.2.1 Маршрутизаторы

Маршрутизаторы (рисунок 2.2) используется для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например, выбор маршрута (пути) с наименьшим числом транзитных узлов. Работают на сетевом уровне модели OSI.

Рисунке 2.2 – Панель выбора маршрутизаторов

2.2.2 Коммутаторы

Коммутаторы (рисунок 2.3) – это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор передаёт пакеты на основании внутренней таблицы – таблицы коммутации, следовательно, трафик идёт только на тот MAC-адрес, которому он предназначается, а не повторяется на всех портах (как на концентраторе).

Рисунок 2.3 – Панель выбора коммутаторов

2.2.3 Беспроводные устройства

Основными узлами беспроводных Wi-Fi-сетей, осуществляющими ретрансляцию кадров, являются точки доступа (рисунок 2.4).

Рисунок 2.4 – Панель выбора беспроводных устройств

2.2.4 Конечные устройства

Здесь располагаются непосредственно конечные узлы, хосты, сервера, принтеры, телефоны и другое оборудование (рисунок 2.5).

Рисунок 2.5 – Панель выбора конечных устройств

2.2.5 Линии связи

В качестве линий связи, соединяющих телекоммуникационные устройства между собой, могут быть использованы консольный кабель, коаксиальный кабель или витая пара и оптоволокно (рисунок 2.6). Дополнительно можно указать тип кабельного соединения: прямое или кроссоверное. В таблице 1 приведено описание предлагаемых кабельных линий связи.

Рисунок 2.6 – Панель выбора линий связи

Таблица 2.1 – Типы линий связи

Тип кабеля	Описание
Console	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Скорость соединения обеих сторон должна быть одинаковая, передаваться может любой поток данных.
Copper straight-through	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, которые функционируют на разных уровнях OSI. Сигнал передается напрямую из одного конца в другой, а именно с 1-го контакта на 1-й, с 2-го на 2-й и т. д. Используется между ПК и хабом, ПК и DSL-модемом, хабом и коммутатором.
Copper cross-over	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Используется для соединения двух ПК напрямую, т. е. без хаба или коммутатора. Таким образом, можно подключить только 2 компьютера одновременно.
Fiber	Оптоволоконный кабель используется для соединения между оптическими портами.
Phone	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты.
Coaxial	Коаксиальный кабель используется для соединения между коаксиальными портами.
Serial Data Circuit Equipment/Data Terminal Equipment (DCE/DTE)	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке «часов» рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становится DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

2.2.6 Эмуляция Интернета

В этом блоке (рисунок 2.7) располагаются устройства, используемые при эмуляция глобальных сетей, в частности модемы различных типов, в частности, (DSL или кабельные), «облако» и проч.

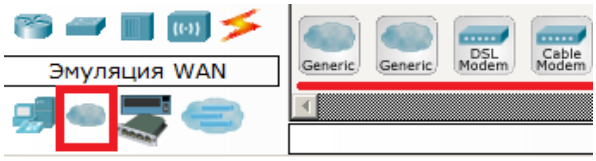


Рисунок 2.7 – Панель выбора топологии сети

2.2.7 Пользовательские устройства

Вид панели выбора пользовательских устройств изображен на рисунке 2.8.

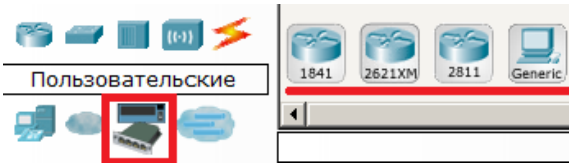


Рисунок 2.8 – Панель выбора пользовательских устройств

2.2.8 Облако для многопользовательской работы

Вид панели выбора облака для многопользовательской работы представлен на рисунке 2.9.

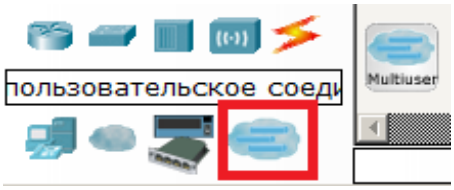


Рисунок 2.9 – Панель выбора облака для многопользовательской работы

3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО СОЗДАНИЮ И НАСТРОЙКЕ ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Для создания сети необходимо на рабочую область перенести требуемые оконечные устройства *(End Devices)* пользователей – компьютеры, ноутбуки, серверы, принтеры и другие устройства.

После размещения необходимого оборудования пользователей можно аналогичным образом разместить на рабочей области активное сетевое оборудование, сгруппированное в следующих типах устройств: *маршрутизаторы (Routers)*, *коммутаторы (Switches)*, *концентраторы (Hubs)*, *беспроводные устройства (Wireless Devices)* и др.

Для подключения оконечных устройств к узлу (коммутатору или маршрутизатору) следует выбрать тип соединения *Copper Straight-Through* (прямой медный кабель) и подвести его к компьютеру и щелкнуть левой кнопки мыши (ЛКМ). Затем щелкнуть ЛКМ по интерфейсу Fast Ethernet0 компьютера. Таким образом имитируется подключение штекера RJ-45 кабеля к данному гнезду соответствующего устройства. Второй конец прямого кабеля подключается аналогично к одному из гнезд интерфейсов коммутатора FastEthernet0/X. Здесь первая цифра означает номер модуля устройства, а X – номер интерфейса в соответствующем модуле. Подобным образом необходимо соединить все устройства. Обратите внима-

ние, что при создании нового соединения занятые порты устройства не отображаются во всплывающем окне.

Если создавать соединение с использованием автоматического выбора типа соединения (*Automatically Choose Connection Type*), то всплывающие окна появляться не будут, а Packet Tracer сам определит тип соединения и используемые порты (но эту возможность использовать не рекомендуется, поскольку с методической позиции студент должен представлять, какие порты и как соединяются). Следует заметить, что если между собой соединяются однотипные сетевые устройства (компьютер-компьютер, коммутатор-коммутатор и т.д.), то соединение нужно производить перекрестным кабелем *Copper Cross-Over* (подумайте, почему?).

После завершения соединения устройств сети Packet Tracer сигнализирует о наличии соединений на физическом и канальном уровнях двумя зелеными периодически мигающими квадратиками (кружочками или треугольничками) на концах каждого соединения (мигание означает активность линии). При отсутствии соединения квадратики/кружочки/треугольники становятся красными. Это можно проверить, выключив питание одного из компьютеров. Для этого выполните щелчок левой кнопкой мыши на одном из компьютеров и перейдите в открывшемся окне на вкладку *Физическая конфигурация (Physical)*. Выполните щелчок ЛКМ по кнопке питания на изображении компьютера, обратите внимание, что находящийся над ней индикатор погас. После включения устройства квадратик/треугольник/кружочек на линии связи возле устройства не сразу изменяет цвет на зеленый. Это обусловлено необходимостью некоторого времени на распознавание устройства коммутатором.

При создании беспроводного сегмента сети и подключения его к проводной сети (рисунок 3.1) необходимо добавить на рабочую область *Точку доступа (Access Point-PT),* предварительно выбрав в Панели типов устройств *Беспроводные устройства (Wireless Devices)*, а также добавить из группы *Оконечные устройств (End Devices) Ноутбук (Laptop-PT)*.

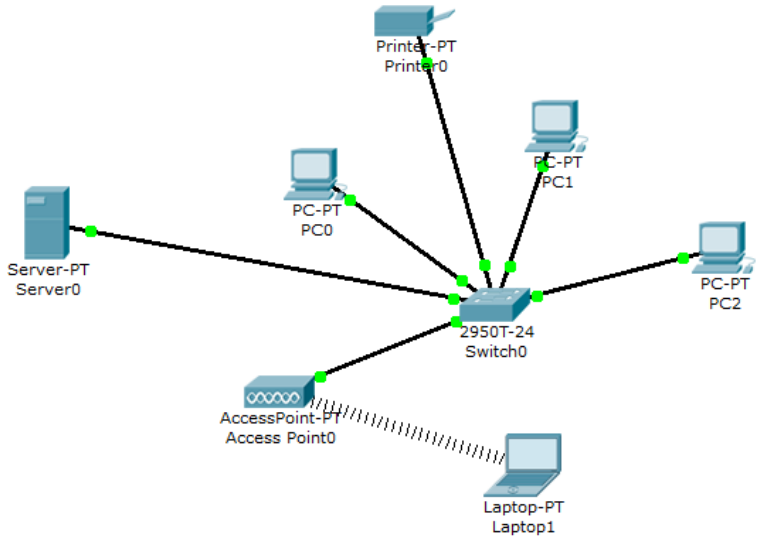


Рисунок 3.1 – Завершенная топология локальной компьютерной сети

Поскольку ноутбук в данном симуляторе, по умолчанию, оснащен только проводным интерфейсом, нужно заменить его на беспроводный. Для этого необходимо выполнить щелчок левой кнопкой мыши на ноутбуке и перейти на вкладку *Физическая конфигурация (Physical)*. Чтобы увидеть изображение ноутбука, следует протянуть линейку прокрутки вниз.

Затем нужно отключить питание ноутбука, выполнив щелчок ЛКМ на кнопке питания, при этом погаснет индикатор питания. Дальше необходимо перетащить мышью модуль с проводным интерфейсом в *Список модулей (MODULES)* слева от изображения ноутбука. А после этого, перетащить верхний модуль с беспроводным интерфейсом *Linksys-WPC300N* из *Списка модулей (MODULES)* в разъем ноутбука, в котором был установлен модуль с проводным интерфейсом. После включения питания ноутбука на схеме сети будет видно, что ноутбук связался с точкой доступа по радиоканалу.

При необходимости добавить в создаваемую локальную сеть сервер и сетевой принтер их следует выбрать из группы *Оконечные устройств (End Devices)* на Панели типов устройств *Сервер (Server-PT)* и *Принтер (Printer-PT)*. Оба устройства по умолчанию оснащены проводными интерфейсами *Fast Ethernet*, работающими со скоростью 100 Мбит/с. Подсоединение принтера к порту (интерфейсу) коммутатора осуществляется аналогично соединению с ПК. Если устройства, подлежащие соединению, имеют разнотипные по скорости интерфейсы, то следует на одном из устройств заменить интерфейсный модуль на совместимый. Например, изъять модуль FastEthernet и заменить его на Gigabit Ethernet, работающим со скоростью 1000 Мбит/с, либо наоборот. Процесс замены модуля выполняется так же, как это делалось для ноутбука.

Обратите внимание, что при подсоединении сервера к коммутатору целесообразно использовать гигабитные порты, например, *Gigabit Ethernet 1/1*. В этом случае пакеты между коммутатором и сервером будут проходить на скорости в 10 раз большей скорости между коммутатором и остальными устройствами сети, что является оправданным, так как сервер обычно используется несколькими устройствами одновременно.

После физического соединения между собой всех сетевых устройств следующим шагом является **конфигурирование** устройств. Сетевые имена устройств (PC0, Switch, Server и др.) задаются системой моделирования автоматически при построении схемы сети. Их, при желании, можно изменять прямо в рабочей области или в окне конфигурирования устройств. Устройства Packet Tracer поддерживают стек сетевых протоколов TCP/IP, причем поддерживается и IPv4 (в настоящее время наиболее распространенной), и IPv6 (переход к которой уже начался). В данной работе задавать устройствам адреса следует по протоколу IPv4.

Назначение имен и IP-адресов ПК, принтера и сервера происходит одинаковым образом, поэтому приведем последовательность действий по конфигурированию этих параметров на примере ПК. Выполните щелчок по изображе-

нию устройства левой кнопкой мыши, при этом откроется окно конфигурирования устройств, выберите его вкладку *Конфигурация (Config)*.

Из списка слева выберите команду *Настройки (Settings)* для перехода к окну, в котором можно ввести/изменить сетевое имя устройства. Здесь также можно указать IP-адреса *шлюза (Gateway)* сети, в которую входит данное устройство, и *DNS-сервера*, на котором находятся соответствия имен пользовательских устройств сети и их IP-адресов, и указать будет ли назначаться им адрес автоматически (с использованием сервера, работающего по протоколу *Dynamic Host Configuration Protocol – DHCP-сервера*) или вручную (*Static*).

Сетевой шлюз (Gateway) представляет собой сетевой интерфейс, через который сетевые пакеты от устройств одной сети передаются в другие сети и пакеты от устройств других сетей поступают в данную сеть. Поскольку в данной работе моделируется только одна сеть, адрес шлюза задавать не нужно. Исследование работы *Доменной системы имен (Domain Name System – DNS)* и конфигурирование DNS-сервера будет выполнено на последующих лабораторных занятиях. Без конфигурирования такого сервера можно посылать пакеты с помощью утилиты ping, используя в качестве ее аргумента только IP-адрес удаленного компьютера. После конфигурирования DNS-сервера появляется дополнительная возможность связи с удаленным устройством по его сетевому имени.

Для задания устройству сетевого (IP) адреса нужно из списка слева выбрать тип сетевого интерфейса устройства (например, *Fast Ethernet*). При этом откроется окно установки адресов. В поле *IP-адрес (IP Address)* для компьютера с сетевым именем *PC1* введите адрес 192.168.0.1, далее выполните щелчок в поле *Маска подсети (Subnet Mask)*, программа автоматически введет маску 255.255.255.0. Ее нужно оставить без изменений. Обратите внимание, что на этой вкладке выводится MAC-адрес устройства, а также скорость и режим передачи данных (100 Мбит/с и полный дуплекс).

Выполните аналогичным способом конфигурирование остальных пользовательских устройств созданной локальной сети, задав им IP-адреса и маски, приведенные в таблице 3.1. Обратите внимание, что сетевой интерфейс сервера имеет тип *Gigabit Ethernet* и работает на скорости 1000 Мбит/с.

Таблица 3.1 – Адресная информация для конфигурирования пользовательских устройств локальной компьютерной сети на рисунке 3.1.

Устройство	Сетевое имя	IP-адрес	Маска подсети
ПК-1	PC1	192.168.0.1	255.255.255.0
ПК-2	PC2	192.168.0.2	255.255.255.0
ПК-3	PC3	192.168.0.3	255.255.255.0
Ноутбук	Laptop1	192.168.0.4	255.255.255.0
Сетевой принтер	Printer0	192.168.0.5	255.255.255.0
Сервер	Server0	192.168.0.6	255.255.255.0

Конфигурирование адресов для ноутбука имеет особенности, поскольку мы оснастили его беспроводным интерфейсом. По умолчанию окно конфигу-

рирования интерфейса открывается с установленной настройкой автоматического задания IP-адреса и маски подсети устройствам (*DHCP*). Но поскольку в данной сети отсутствует DHCP-сервер, следует переключить установку в режим ручного задания адресов (*Static*) и задать IP-адрес и маску подсети описанным выше способом. Обратите внимание на наличие настроек *аутентификации (Authentication)* устройств при беспроводном подключении к точке доступа передачу точке доступа пароля, по которому она будет подключать устройство, и настроек *шифрования*, передаваемых по беспроводной сети данных (*Encryption*). Учитывая простоту несанкционированного подключения к беспроводной сети, на практике эти возможности являются часто используемыми. Пока оставьте их отключенными (*Disabled*).

В списке интерфейсов беспроводной точки доступа присутствуют два интерфейса: *Port 0* проводной интерфейс Fast Ethernet, связывающий точку доступа с коммутатором, и беспроводный интерфейс *Port 1*. Здесь так же, как и для беспроводного адаптера, есть поля для настройки аутентификации и шифрования, включая указание ключевой (парольной) фразы, которую должен передать беспроводный адаптер для подключения к точке доступа.

Все выполняемые в графическом интерфейсе настройки сопровождаются соответствующими им командами IOS в окне Equivalent IOS Command.

Для **проверки связи** между устройствами созданной модели локальной сети можно использовать утилиту ping. Для этого выполните щелчок левой кнопкой мыши, например, на ПК и перейдите на вкладку *Рабочий стол (Desktop)*. На нем будут доступны дополнительные инструменты для настройки данного устройства (их доступность зависит от физического конфигурирования устройства: наличия тех либо иных модулей или устройств). Нам понадобится инструмент *Command Prompt (Окно командной строки)*, в котором можно запустить утилиту ping с IP-адресом устройства сети, связь с которым проверяется в качестве ее аргумента.

Система моделирования Cisco Packet Tracer может функционировать также и в режиме симуляции работы сети, в котором можно анимировать прохождение пакетов. Переход в режим симуляции осуществляется путем нажатия комбинации клавиш **Shift+S**, или, щелчком мыши на иконке симуляции в правом нижнем углу рабочего окна. Затем нужно исключить все сетевые протоколы, кроме ICMP. Для этого следует нажать на кнопку Edit Filters (Изменить фильтры) и убрать все флажки, за исключением ICMP и ARP.

Исследования прохождения пакетов ICMP от Laptop 0 на Server 0 можно выполнить двумя способами.

1-й способ.

Кликнуть по иконке Laptop 0, откроется соответствующее окно в котором активировать Command Prompt и ввести и запустить команду Ping.

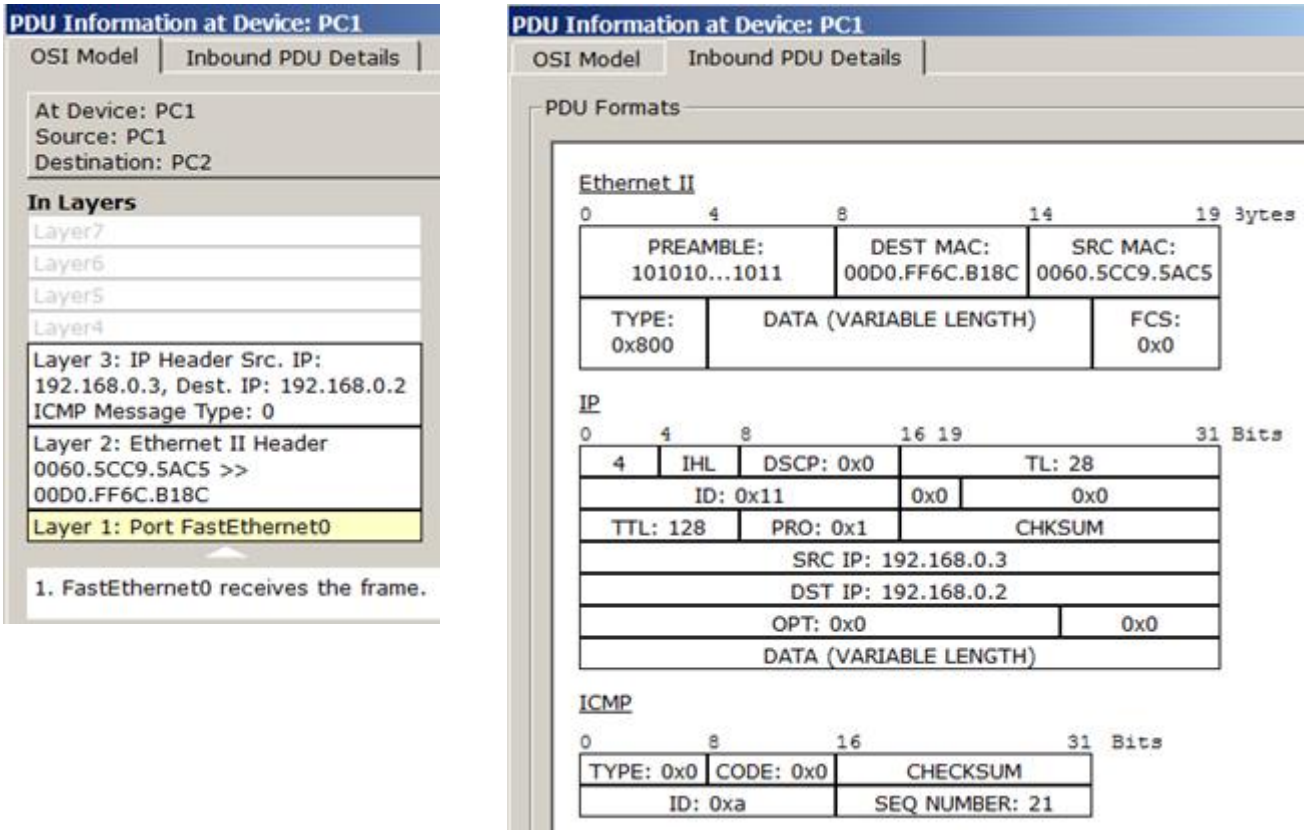
2-й способ.

Кликнуть на иконки конвертов в правой стороне рабочего окна. А затем последовательно кликнуть сначала на компьютер-источник (например, Laptop0), тем самым обозначив его в качестве отправителя и источника паке-

тов, и затем на тестируемое конечное устройство (например, Server 0), обозначив его получателем пакетов.

Запустить продвижение пакетов в сеть пошагово путем нажатия на кнопку Capture/Forward (Вперёд) в окне симуляции. Если нажать на кнопку Auto Capture/Play (воспроизведение), то можно увидеть весь непрерывный цикл прохождения пакета по сети. В Event List (Список событий) отображается весь процесс пингования.

Щелчок мышью на конверте можно получить дополнительную информацию о движении пакета по сети. При этом на первой вкладке отображается **модель OSI** (рисунок 3.2, а).



а) б)

Рисунок 3.2 - Мониторинг движения пакета на модели OSI

На вкладке OSI Model (Модель OSI) представлена информация об уровнях OSI, на которых работает данное сетевое устройство. На другой вкладке можно посмотреть структуру пакета (рисунок 3.2,б).

4 ПРОГРАММА РАБОТЫ

1. Повторить теоретический материал курса «Инфокоммуникационные системы и сети», относящиеся к теме «Виртуальные локальные сети».
2. Составить схему локальной компьютерной сети, изображенной на рисунке 3.1.
3. Выполнить конфигурацию оборудования локальной сети в соответствии с таблицей 3.1 и проверить пингованием возможность передачи пакетов между любыми оконечными пунктами сети.
4. Проверить и записать содержимое ARP-таблиц персональных компьютеров и ноутбуков.
5. Выполнить в режиме симулирования (Simulation) пингование между персональными компьютерами сети и другими оконечными устройствами и записать типы используемых пакетов и последовательность обмена пакетами между всеми устройствами сети.
6. Исследовать в режиме симуляции формат заголовков передаваемых кадров и пакетов.
7. Составить схему компьютерной сети с разделение ее на виртуальные локальные подсети (VLAN). Сеть расположена на двух этажах здания, на каждом из которых установлен собственный этажный коммутатор. Связь между этажами обеспечивается магистральным коммутатором. В каждой VLAN имеется локальный сервер. Компьютеры виртуальных подсетей размещены как на первом, так и на втором этажах. Обобщенная схема сети и параметры конфигурации приведены в конце методических указаний в приложении 1.
8. Состав определяется таблицей вариантов (приложение 1) вариантом (номер по определяется последней цифрой номера зачетной книжки). Условием правильного функционирования сети является отсутствие связи между хостами, принадлежащими разным VLAN.
9. Выполнить в режиме симулирования (Simulation) пингование между оконечными устройствами подсетей и записать типы используемых пакетов и последовательность обмена пакетами между всеми устройствами сети.
10. Составить выводы по работе.

5 СОДЕРЖАНИЕ ОТЧЕТА

5.1. Титульный лист.
5.2. Цель и программа лабораторной работы.
5.3. Исходные данные в соответствии с индивидуальным вариантом.
5.4. Скриншоты с топологией локальных сетей.
5.5. Команды и скриншоты этапов настройки локальных сетей.
5.6. Скриншоты результатов тестирования сетей.

5.7. Структура заголовков исследуемых кадров и пакетов.
5.8. Выводы.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

6.1. Какие сетевые устройства эмулирует программа Packet Tracer?
6.2. Чем различаются между собой узловые устройства сетей: повторители (Hubs), коммутаторы (Switches), маршрутизаторы (Routers)?
6.3. В чем состоит отличие прямого кабеля Ethernet (Straight-Through) от перекрестного (Cross Over)?
6.4. Какие порты имеет персональный компьютер, для чего они предназначены и каковы их параметры?
6.5. Какие порты имеет коммутатор и для чего они предназначены?
6.6. Как формируется таблица коммутации?
6.7. Чем канальный кадр отличается от сетевого пакета?
6.8. Для чего предназначен протокол ARP и что происходит в сети при запуске процедуры ARP?
6.9. Каким образом при моделировании функционирования сети можно посмотреть содержимое заголовков кадров и пакетов?
6.10. Какую функцию выполняет точка доступа в беспроводной сети?
6.11. Что такое порт по умолчанию, где он расположен и для чего применяется?
6.12. Какие параметры задаются сетевому компьютеру при его конфигурации?

Лабораторная работа 2

ИССЛЕДОВАНИЕ СПОСОБОВ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ И КОНФИГУРАЦИИ СЕТЕВОГО ОБОРУДОВАНИЯ

1 ЦЕЛЬ РАБОТЫ

Углубление теоретических знаний в области построения компьютерных локальных сетей и конфигурации телекоммуникационного оборудования, исследование процессов передачи пакетов в сети среде Packet tracer в реальном времени и в режиме симуляции, закрепление практических навыков конфигурации и моделирования беспроводных локальных компьютерных сетей.

2 ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

В практической деятельности по внедрению компьютерных сетей встречаются ситуации, в которых принципиально невозможна прокладка кабеля. Это, как правило, старинные здания либо очень дорогие интерьеры, где стоимость прокладки кабельной сети непомерно высока, или важна скорость установки и запуска сети (временные сети на выставках, семинарах и т.п.). В такой ситуации проблема решается путем развертывания беспроводной локальной компьютерной сети **WLAN** (*Wireless Local Area Network*).

Беспроводные решения широко применяются также в корпоративных компьютерных сетях для объединения удаленных локальных сетей в случае отсутствия между ними проводных или волоконно-оптических каналов или необходимости их резервирования.

2.1. Топологии беспроводных локальных компьютерных сетей

В зависимости от способа построения, вида связей между узлами, количества компьютеров в сети и расстояния между ними, топологически беспроводные локальные сети разделяются на сети трех видов:

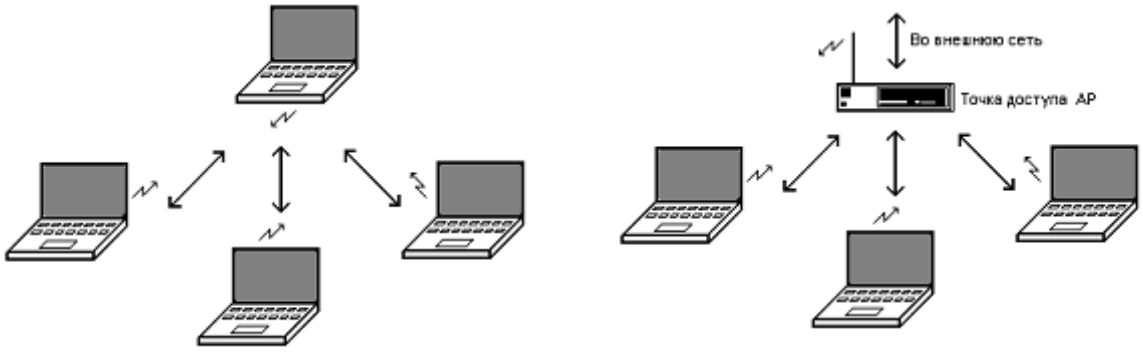
1) сеть без базовой станции — внеплановая сеть (*Ad Hoc*);
2) сеть с точкой доступа (*Infrastructure Network*);
3) ячеистая сеть (*Mesh Network*).

Компьютер пользователя, оснащенный беспроводным интерфейсом (радиоадаптером), обычно называют клиентской станцией.

Компьютерные сети, состоящие обычно из переносных компьютеров (ноутбуков), оснащенных беспроводными интерфейсами, создаваемые на сравнительное короткое время для пользователей, которые пообщаются некоторое

время и разойдутся, получили обозначение **Ad HOC** (от лат. *ad hoc — на данный случай, для этой цели*). Их также называют "внеплановыми", т.к. при создании таких сетей заранее не разрабатываются какие-либо планы места их расположения. В неплановой сети Ad HOC количество компьютеров невелико и расстояние между ними измеряется несколькими десятками метров, а базовая станция отсутствует (рисунок 2.1,а). Беспроводная сеть Ad HOC является **одноранговой**, то есть все компьютеры этой сети равноправны и отсутствует выделенный пункт управления, регламентирующий работу сети.

Сети Ad HOC называют также сетями с независимой базовой зоной обслуживания **IBSS** (*Independent Basic Service Set*). Клиентские станции в данных сетях непосредственно взаимодействуют друг с другом, пока они находятся в пределах устойчивой радиосвязи, т.е. передача информации осуществляется в режиме "точка-точка". В заголовках передаваемых кадров содержатся физические адреса (MAC-адреса) станции назначения и станции отправителя, а также идентификатор IBSS, который является логическим адресом компьютерной сети Ad HOC. Важнейшее достоинство сетей IBSS — простота, так как нет необходимости создания сетевой инфраструктуры, каждый клиентский компьютер должен быть оснащен только беспроводным адаптером. Основными недостатками режима Ad Hoc являются ограниченный диапазон действия компьютерной сети и невозможность подключения к внешней сети (например, к Интернету).



а) б)

Рисунок 2.1 – Топологии беспроводных локальных компьютерных сетей:
а) топология *Ad HOC*; топология *Infrastructure Network*

В сетях *Infrastructure Network* клиентские компьютеры взаимодействуют друг с другом не напрямую, а через промежуточную базовую станцию — **точку доступа AP** (*Access Point*), которая выполняет в беспроводной сети роль своеобразного концентратора (аналогично тому, как это происходит в традиционных кабельных сетях). При взаимодействии клиентов с точкой доступа заголовок каждого кадра содержит MAC-адреса узла-отправителя, узла-получателя и логический адрес самой точки доступа.

Через точку доступа возможен также выход во внешние проводные сети. В компьютерной сети может быть несколько AP, объединенных проводной сетью Ethernet. Фактически такая сеть представляет собой набор базовых станций с неперекрывающимися зонами охвата.

Существует два режима взаимодействия с точками доступа: **BSS** *(Basic Service Set*) и **ESS** (*Extended Service Set*). В режиме BSS все рабочие станции (клиенты) связываются между собой только через точку доступа (сервер), которая может выполнять также роль моста к внешней сети (рисунок 2.1,б).

Как видно из рисунка 2.1,б, расстояние между компьютерными станциями увеличивается, как минимум, вдвое. Одна точка доступа обеспечивает обслуживание от 15 до 250 абонентов, в зависимости от конфигурации сети и технологии доступа. Увеличить емкость сети можно просто, добавив новые точки доступа, при этом не только расширяется зона обслуживания, но и снижается вероятность перегрузки.

Группа клиентских станций вместе с точкой доступа образуют некоторую **ячейку**, внутри которой осуществляется связь компьютеров между собой. Для идентификации ячейки BSS ей присваивается уникальный идентификатор **SSID** (*Service Set IDentifier*) или другими словами — имя сети. Этот параметр задаётся при настройке точки доступа и обычно передаётся ею в эфир. Настройки большинства точек доступа позволяют отключить широковещание SSID, что затрудняет несанкционированное подключение к сети посторонних пользователей, однако, возможность подключения клиентов, знающих SSID, сохранится.

В **расширенном режиме** ESS существует инфраструктура нескольких базовых сетей BSS, причем сами точки доступа взаимодействуют друг с другом через некоторую систему, называемую **системой распределения DS** (*Distribution System*), позволяющую направлять трафик от одной BSS к другой (рисунок 2.2).

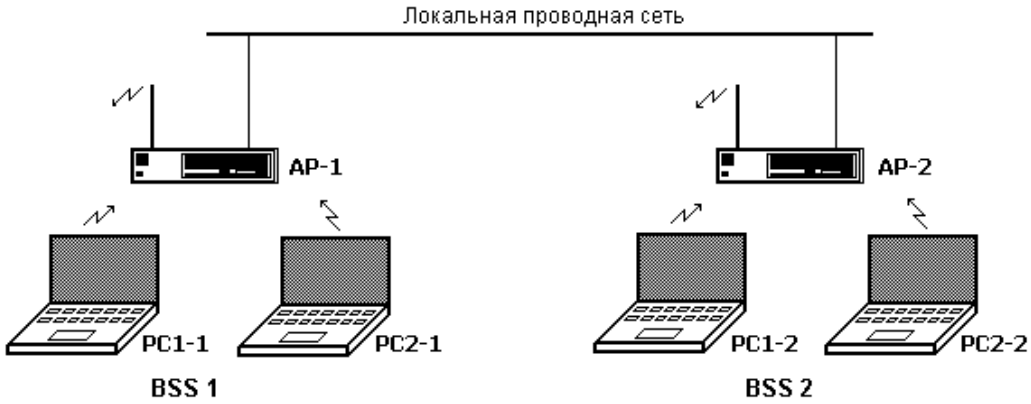


Рисунок 2.2 – Беспроводная локальная компьютерная сеть
с расширенной инфраструктурой

Связь базовых сетей с DS осуществляется посредством точек доступа AP-1 и AP-2. Между собой точки доступа соединяются с помощью сегментов кабельной сети, либо радиомостов, т.е. система распространения представляет собой либо совокупность устройств AP, либо сегмент локальной сети. Каждая базовая станция ESS должна обладать одинаковым идентификатором SSID. Для уменьшения взаимных помех соседние точки доступа обычно настраиваются на различные частотные каналы.

Ячеистые сети (*Mesh Network*) — это беспроводные компьютерные сети, состоящие из множества специальных точек доступа (*Mesh Point*), которые могут взаимодействовать друг с другом в режиме Ad HOC, образуя таким образом опорную сетевую инфраструктуру. В ячеистой сети Mesh-точка доступа образует собственную ячейку, внутри которой все клиентские компьютеры работают на одной и той же несущей частоте. И если в обычных сетях независимые ячейки практически не взаимодействуют между собой, то в ячеистых сетях такое взаимодействие является обязательным условием существования сети. Очевидно, что соседние Mesh-точки доступа должны располагаться в зоне достижимости друг друга, в противном случае они не смогут обмениваться кадрами.

2.2. Виды кадров, используемых в сетях 802.11

Кадры в беспроводных локальных сетях формируются на MAC-уровне, а на физическом уровне к ним прибавляется только заголовок этого уровня. На MAC-уровень от верхнего уровня поступают пакеты приложений. Если размер пакетов превышает предельно допустимую длину кадра, то осуществляется их фрагментация. Формат кадра и структура заголовка для физического уровня показаны на рисунке 2.3.

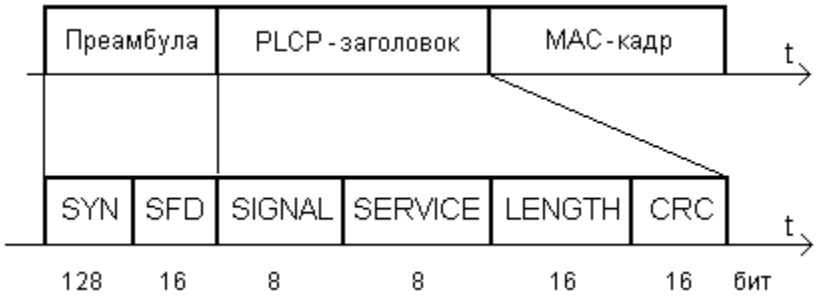


Рисунок 2.3 — Формат кадра физического уровня

Перед передачей MAC-кадра в канал к нему добавляется заголовок физичского уровня, состоящий из преамбулы длиною 144 бита и собственно заголовка **PLCP** (*Physical Layer Convergence Protocol*) размером 48 битов. Преамбула служит для обеспечения тактовой и цикловой синхронизации передающей и приемной частей. Она состоит из синхронизирующей битовой последовательности **SYN** вида 1010…, которая завершается маркерной кодовой комбинацией **SFD** (*Start Frame Delimiter*) вида F3A0h, сигнализирующей о начале кадра.

PLCP-заголовок содержит поле SIGNAL с информацией о скорости передачи и способе модуляции, поле SERVICE с дополнительными сведениями о наличии вариантов расширений и поле LENGTH, в котором указана длина временного интервала в микросекундах, необходимого для передачи следующей за заголовком части кадра. Все поля заголовка кодируются помехоустойчивым циклическим кодом с образующим полиномом 16-й степени. Результат кодиро-

вания помещается в поле контрольной последовательности CRC. Все биты заголовка передаются со скоростью 1 Мбит/с. Остальная часть кадра может передаваться с другой допустимой данным стандартом скоростью, которая указывается в полях SIGNAL и SERVICE.

На MAC-уровне стандарта 802.11 применяются кадры трех типов:

- **служебные** (*Management Frames*) — обеспечивают соединения в сетях, аутентификацию, а также сообщают о состоянии оборудования;
- **информационные** (*Data Frames*) — выполняют транспортирование пользовательских данных;
- **управляющие** (*Control Frames*) — поддерживают передачу кадров данных при нормальном обмене информацией между станциями стандарта 802.11.

Форматы всех трех типов кадров похожи на основной формат, применяемый в сетях 802.11. Все они имеют заголовки с множеством полей, используемых подуровнем MAC. Названные три типа кадров расширяют и используют специфические участки кадра для своих целей.

Структура MAC-кадра основного формата показана на рисунке 2.4. Поле "Управление кадром" (*Frame Control*) занимает два байта и содержит 11 вложенных подполей, которые выполняют следующие функции:

"Версия протокола" (2 бита) — указывает версию протокола MAC-подуровня. Подполе имеет значение 0 (используется только одна версия), остальные значения зарезервированы.

- "Тип" (2 бита) — указывает тип MAC-кадра: информационный, служебный или управляющий.

Управление кадром	Продол-житель-ность/ID	Адрес 1	Адрес 2	Адрес 3	Управле-ние оче-редностью	Адрес 4	Данные	КПК
2 байта	2	6	6	6	2	6	0 - 2312	4

Рисунок 2.4 — Основной формат MAC-кадра сети 802.11

- "Подтип" (4 бита) — уточняет тип и подтип кадра (например, "запрос на соединение", "ответ на запрос", "зондирующий запрос", "аутентификация", кадры RTS или CTS, ACK и др.). Далее располагаются однобитовые подполя, выполняющие следующие функции.
- Один бит "К DS" и один бит "От DS" — индицируют о направлении движения кадра: к междоменной системе распределения DS (например, Ethernet) или от нее. Координационная функция MAC присваивает биту "К DS" значение 1, если кадр предназначен распределительной системе, и единичное значение биту "От DS", если кадр исходит от распределительной системы.
- MF (*More Fragments*) — информирует о том, что далее следует еще один фрагмент.
- "Повтор" — отмечает повторно посылаемый фрагмент.

• "Управление питанием" — указывает на режим энергопотребления рабочей станции: «1" — режим пониженного потребления, "0» — активный режим. В кадрах точки доступа этот бит всегда сброшен в "0".

• "Продолжение" (*More Data*) — свидетельствует о том, что у отправителя имеются еще кадры для пересылки.

• W — является индикатором использования шифрования в поле данных кадра по алгоритму WEP (*Wired Equivalent Protocol*).

• O (*Order*) — информирует приемник о том, что кадры с этим битом должны обрабатываться строго по порядку.

Последующие поля кадра идентифицируются следующим образом.

• "Продолжительность / ID" (2 байта) — используется по-разному, в зависимости от того, получает ли доступ к среде рабочая станция, работающая в энергосберегающем режиме, находится ли среда в режиме сосредоточенной координации PCF периода свободного от конкуренции (CFP), или доступ к среде получает станция с распределенной функцией координации DCF (детальнее функции PCF и DCF рассматриваются в третьем разделе). В частности, для рабочей станции с DCF здесь указывается время передачи данных и ожидания ответа.

• "Адрес 1, 2" — содержат адреса рабочих станций отправителя и получателя соответственно, а поля "Адрес 3 и 4" входят в состав кадра только при соединении двух сетей через распределительную систему DS. В этом случае третий адрес обозначает адрес точки доступа сети отправителя, а четвертый — получателя.

• "Управление очередностью" — содержит порядковый номер и номер фрагмента кадра. Из 16 доступных бит 12 идентифицируют кадр, а 4 — фрагмент.

• "КПК" — контрольная последовательность кадра (CRC), 32-разрядная комбинация, полученная в результате помехоустойчивого циклического кодирования.

Кадр данных содержит в заголовке все поля основного формата MAC-кадра и собственно пользовательскую информацию, длина которой может достигать 2312 байтов.

Служебные кадры (*Management Frames*) по своему функциональному назначению подразделяются на следующие типы:

- сигнальный (маячковый) кадр;
- кадры запроса и ответа на зондирование;
- кадры аутентификации и деаутентификации;
- кадры запроса на ассоциирование либо реассоциирование;
- кадры ответа на ассоциирование либо реассоциирование;
- кадр диссоциирования;
- кадр индикации объявленного трафика.

Наряду с типовыми полями, присущими базовому кадру, служебные MAC-кадры содержат дополнительные структуры данных, состоящие из так называемых информационных элементов **IE** (*Information Elements*) и фиксированных полей (*Fixed Fields*). Целью введения таких структур является обеспечения гибкости при расширении возможностей служебных кадров.

Стандартом 802.11 определено шесть типов **управляющих кадров.**

1. PS-Poll (*Power Saving-Polling*) — опрос после выхода из экономичного режима. В кадре требуется передача кадра, прибывшего, когда станция находилась в режиме энергосбережения, и в данный момент размещенного в буфере точки доступа.
2. RTS (*Request To Send*) — запрос на резервирование среды.
3. CTS (*Clear To Send*)— ответ на кадр запроса RTS.
4. ACK (*Acknowledge)*— подтверждение успешной передачи кадра.
5. CF-End (*Contention Free-End*) окончание периода, свободного от конкуренции.
6. CF-End +CF-ACK — конец периода, свободного от конкуренции и подтверждение приема последнего кадра.

Управляющие кадры (*Control Frames*) имеют формат, сходный с форматом информационных кадров, за одним исключением: в управляющем кадре отсутствуют поля адресов базовых станций, поскольку таким кадрам нет необходимости выходить за пределы базовой зоны обслуживания.

3 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

В качестве лабораторной установки используется персональный компьютер с установленной системой моделирования компьютерных сетей Packet Tracer. Работа с этой системой подробно описана в предыдущей работе

В работе исследуются процессы построения, конфигурирования и моделирования компьютерной сети, схема которой изображена на рисунке 3.1. В качестве клиентских устройств используются стационарные компьютеры (PC0 и PC1), а также мобильные устройства (Laptop0, Laptop1 и планшетный компьютер Tablet PC0). Беспроводные устройства подключаются к сети по беспроводному каналу с помощью точки доступа Access Poit0, работающей по стандарту 802.11N. Локальная компьютерная сеть имеет обеспечиваемый маршрутизатором Router0 выход в публичную сеть, фрагмент которой моделируется маршрутизатором Интернет-провайдера Router1 и сервером Server0.

Следует учитывать, в исходном состоянии в ноутбуке отсутствует беспроводный интерфейс. Для его инсталляции необходимо вначале изъять модуль проводного интерфейса сети Ethernet, а взамен его установить модуль, обеспечивающий обмен кадрами по стандарту 802.11.

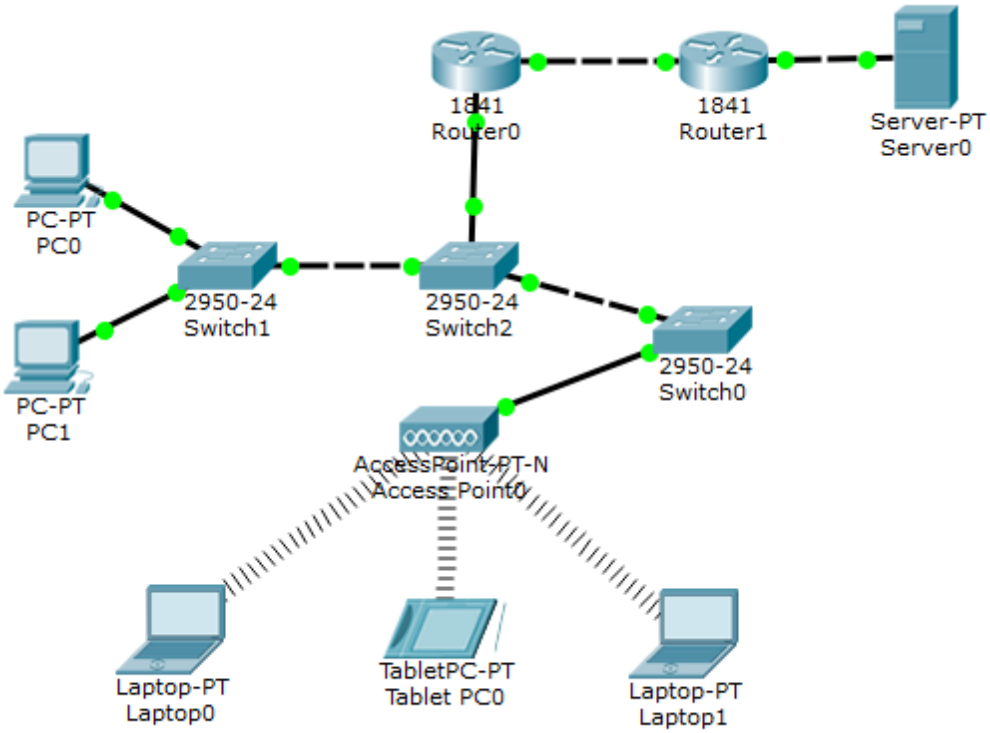


Рисунок 3.1 – Схема исследуемой локальной компьютерной сети

4 ПРОГРАММА И МЕТОДИКА ИССЛЕДОВАНИЯ

4.1. Повторить теоретический материал по построению локальных компьютерных сетей и конфигурации телекоммуникационного оборудования, статической маршрутизации, а также стандарты построения беспроводных локальных сетей стандарта 802.11.

4.2. Составить схему локальной сети, изображенной на рисунке 3.1 и выполнить конфигурацию телекоммуникационного оборудования, обеспечивающего доступ с любого клиентского компьютера доступ к внешнему серверу. Способ формирования адресов изложен в примечании.

4.3. Исследовать функционирование сети путем взаимного пингования в реальном режиме (Realtime).

4.4. Проверить функционирование сети путем взаимного пингования в режиме симуляции (Simulation Mode).

4.5. Исследовать состав таблиц маршрутизации и разрешения адресов на маршрутизаторах и таблиц коммутации на коммутаторах и динамику их изменения в процессе пингования с различных клиентских компьютеров.

4.6. Исследовать состав заголовков пакетов всех используемых протоколов.

4.7. Ознакомиться с параметрами конфигурации беспроводных клиентских сетевых устройств.

4.8. Сформулировать выводы по результатам работы.

ПРИМЕЧАНИЕ:

Адреса клиентских компьютеров формируются в виде: 192.168.X.У, где X – предпоследняя цифра, а У – последняя цифра номера зачетной книжки. Вместо нуля ставится число 10.

Адреса внешней сети задается в виде ХУ.ХУ.ХУ.ZZ, где X и У – предпоследняя и последняя цифра номера зачетной книжки. Если У равен нулю, то эта цифра в формировании адреса не участвует. Значение Z выбирается произвольным от 1 до 254.

Адрес сервера задается в виде 172.16.X.У, где X – предпоследняя цифра, а У – последняя цифра номера зачетной книжки. Вместо нуля ставится число 10.

5 СОДЕРЖАНИЕ ОТЧЕТА

5.1. Титульный лист.
5.2. Цель и программа лабораторной работы.
5.3. Исходные данные в соответствии с индивидуальным вариантом.
5.4. Скриншот с топологией локальной сети.
5.5. Команды и скриншоты этапов настройки локальной сети.
5.6. Скриншоты результатов тестирования сети.
5.7. Структура заголовков исследуемых пакетов.
5.8. Выводы.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

6.1. В чем состоит отличие функционирование маршрутизатора от коммутатора второго уровня?

6.2. Чем статическая маршрутизация отличается от динамической?

6.3. Поясните принцип трансляции частных адресов в публичные.

6.4. Для чего предназначена точка доступа и как происходит передача кадров при обмене данными между двумя беспроводными клиентскими устройствами?

6.5. Чем отличается работа точки доступа от беспроводного маршрутизатора?

6.6. Каковы топологии беспроводных локальных компьютерных сетей используются в настоящее время? Проведите сравнительный анализ этих топологий.

6.7. Что означает понятие «шлюз по умолчанию», где он располагается и для чего используется?

6.8. Проведите сравнительную характеристику беспроводных сетей стандартов IEEE 802.11a,b-n.

6.9. За счет чего повышается скорость передачи данных по беспроводным сетям при неизменной полосе пропускания канала?

6.10. Какие типы кадров используются в беспроводных локальных сетях и каково их назначение?

6.11. Поясните назначение и структуру преамбулы в начале кадра.

6.12. Расскажите о назначении полей в заголовке основного формата MAC-кадра.

Лабораторная работа 3

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ И БЕЗОПАСНОСТИ ДАННЫХ В БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

1 ЦЕЛЬ РАБОТЫ

Углубление теоретических знаний в области построения защищенных беспроводных компьютерных локальных сетей и конфигурации телекоммуникационного оборудования, обеспечивающего требуемую степень защиты информации, исследование способов защиты передачи пакетов в беспроводной сети в среде Packet Tracer в реальном времени и в режиме симуляции, закрепление практических навыков конфигурации и моделирования беспроводных локальных компьютерных сетей.

2 ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

2.1 Характеристика уязвимостей беспроводных сетей

В связи с тем, что сигналы беспроводных устройств излучаются в свободное пространство в большинстве случаев во всех направлениях, они могут быт приняты (перехвачены) любым субъектом, обладающим приемным устройством используемого в беспроводных сетях диапазона частот, а передаваемые сообщения могут быть использованы в злонамеренных целях. К основным уязвимостям беспроводных локальных компьютерных сетей (БКЛС) относятся следующие.

Вещание радиомаяка. Точка доступа передает с определенным периодом широковещательные сообщения, чтобы оповещать окрестные беспроводные узлы о своем присутствии. Эти широковещательные сообщения содержат основную информацию о точке беспроводного доступа, включая, как правило, идентификатор (название) сети SSID (Service Set Identifier), и приглашают беспроводные узлы зарегистрироваться в данной области. Любая рабочая станция, находящаяся в режиме ожидания, может назначить себе SSID и добавить себя в соответствующую сеть. Многие модели точек доступа позволяют отключать содержащую SSID часть этого вещания, чтобы несколько затруднить беспроводное подслушивание, но SSID, тем не менее, посылается при подключении, поэтому все равно существует небольшое окно уязвимости.

Обнаружение WLAN. Для обнаружения беспроводных сетей WLAN используются специальные инструментальные средства, например, утилита NetStumber. Эта утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней система шифрования WEP. Применение внешней антенны на портативном компьютере делает возможным обнаружение сетей WLAN во время обхода нужного района или поездки по городу. Надежным ме-

тодом обнаружения WLAN является обследование офисного здания с переносным компьютером в руках.

Подслушивание. Подслушивание ведут для сбора информации о сети, которую предполагается атаковать впоследствии. Перехватчик может использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое используется для обычного доступа к этой сети. Беспроводные сети по своей природе позволяют соединять с физической сетью компьютеры, находящиеся на некотором расстоянии от нее, как если бы эти компьютеры находились непосредственно в сети. Например, подключиться к беспроводной сети, располагающейся в здании, может человек, сидящий в машине на стоянке рядом. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

Ложные точки доступа в сеть. Опытный атакующий может организовать ложную точку доступа с имитацией сетевых ресурсов. Абоненты, ничего не подозревая, обращаются к этой ложной точке доступа и сообщают ей свои важные реквизиты, например аутентификационную информацию. Этот тип атак иногда применяют в сочетании с прямым «глушением» истинной точки доступа в сеть.

Отказ в обслуживании. Полную парализацию сети может вызвать атака типа DoS (Denial of Service) — отказ в обслуживании. Ее цель состоит в создании помехи при доступе пользователя к сетевым ресурсам. Беспроводные системы особенно восприимчивы к таким атакам. Физический уровень в беспроводной сети — абстрактное пространство вокруг точки доступа. Злоумышленник может включить устройство, заполняющее весь спектр на рабочей частоте помехами и нелегальным трафиком — такая задача не вызывает особых трудностей. Сам факт проведения DoS-атаки на физическом уровне в беспроводной сети трудно доказать.

Атаки типа «человек-в-середине». Атаки этого типа выполняются на беспроводных сетях гораздо проще, чем на проводных, так как в случае проводной сети требуется реализовать определенный вид доступа к ней. Обычно атаки «человек-в-середине» используются для разрушения конфиденциальности и целостности сеанса связи. Атаки MITM более сложные, чем большинство других атак: для их проведения требуется подробная информация о сети. Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Он использует возможность прослушивания и нелегального захвата потока данных с целью изменения его содержимого, необходимого для удовлетворения некоторых своих целей, например для спуфинга IP-адресов, изменения MAC-адреса для имитирования другого хоста и т. д.

Анонимный доступ в Интернет. Незащищенные беспроводные ЛВС обеспечивают хакерам наилучший анонимный доступ для атак через Интернет. Хакеры могут использовать незащищенную беспроводную ЛВС организации для выхода через нее в Интернет, где они будут осуществлять противоправные действия, не оставляя при этом своих следов. Организация с незащищенной

ЛВС формально становится источником атакующего трафика, нацеленного на другую компьютерную систему, что связано с потенциальным риском правовой ответственности за причиненный ущерб жертве атаки хакеров.

2.2 Требования к защите информации в сетях

При передаче данных по инфокоммуникационным сетям должны выполняться следующие условия:

- аутентичность (гарантия того, что данные получены от легального источника);
- конфиденциальность (данные должны быть надежно зашифрованы);
- целостность (данные получателю должны поступить в том виде, какими они были отправлены источником, т.е. не должны быть изменены третьим лицом).

Особо остро стоит проблема выполнения этих условий в беспроводных сетях.

2.3 Способы обеспечения безопасности в беспроводных сетях

Первым протоколом обеспечения безопасности, для сетей WiFi является протокол **WEP** (*Wired Equivalent Privacy*). Цель введения данного протокола — сделать беспроводные сети такими же безопасными, как и проводные. Процедура WEP кроме шифрования данных, передаваемых по радиоканалу, предназначена также для обеспечения:

- *конфиденциальности* — предотвращение элементарного прослушивания содержимого сообщений;
- *контроля доступа* — защита сети от несанкционированного доступа к её ресурсам;
- *целостности данных* — обнаружение искажений и изменений в принятом кадре.

Шифрование потока данных обеспечивает конфиденциальность информации, передаваемой между двумя станциями в сети. В процедуре WEP используется симметричное шифрование. Оба устройства должны применять одинаковые ключи, иначе передача данных между пользователями сети невозможна. Способ распределения ключей между пользователями сети стандартом не регламентируется.

В протоколе WEP используется симметричный способ шифрования RC4 с 40-битным или 104-битным ключом. При включении WEP все станции (как клиентские, так и точки доступа) получают свой ключ, который применяется для шифрования данных до передачи их в канал. Если станция получает пакет, не зашифрованный соответствующим ключом, пакет исключается из трафика. Этот метод служит для защиты от несанкционированного доступа и перехвата данных.

При использовании протокола WEP возможны два типа взаимной аутентификации беспроводных устройств: **открытая система** и **совместно используемый ключ**. При аутентификации *Open System* к беспроводной сети может подключиться любое устройство с соответствующим значением SSID. Ключи WEP в процессе аутентификации не проверяются. Аутентификация с совместно используемым ключом типа *Shared Key* требует, чтобы точка доступа и беспроводный адаптер имели одинаковый ключ WEP.

Процесс аутентификации в режиме *Shared Key* выглядит следующим образом.

1. Пользователь (клиент) отправляет начальный аутентификационный запрос точке доступа.

2. В ответ на запрос клиентского устройства на подключение к сети, точка доступа *WiFi* посылает случайно сформированное незашифрованное тестовое сообщение (*challenge text*) длиной 128 бит.

3. Клиент копирует этот текст, затем зашифровывает его своим ключом WEP и возвращает точке доступа.

4. Точка доступа расшифровывает сообщение с помощью своего ключа WEP и, если результат совпадает с исходным сообщением, разрешает доступ.

Тип аутентификации *Shared Key* значительно безопаснее, чем Open System, поэтому, если нет специальных противопоказаний, следует использовать именно *Shared Key Authentication*.

На практике протокол WEP оказался не столь надежным, как ожидалось. Основным его недостатком является использование статического ключа для шифрования данных. Злоумышленник может тем или иным способом узнать этот ключ и получить доступ к беспроводной сети. В дальнейшем на смену WEP пришли более надежные протоколы WPA и 802.11x. Тем не менее, протокол WEP продолжает широко использоваться, так как не все устройства поддерживают новые протоколы безопасности.

Протокол **WPA** (WiFi *Protected Access*) обеспечивает более надежный тип защиты. В отличие от WEP, в нем для более безопасного шифрования используется протокол TKIP (*Temporary Key Integrity Protocol*).

Существует два варианта протокола:

- **WPA-Personal** (Personal Key) или сокращенно WPA-PSK;
- **WPA-Enterprise**.

Следующим вариантом повышения защищенности стал протокол **WPA2.** Основное отличие в WPA2 заключается в том, что в нем применяется улучшенный стандарт шифрования AES (*Advanced Encryption Standard*) вместо TKIP. AES способен защищать сверхсекретную информацию, поэтому это хороший вариант для обеспечения безопасности WiFi дома или в компании.

Впоследствии был разработан протокол WPA2-PSK. Он на настоящее время считается лучшим способом для защиты сетей беспроводного доступа.

WPA2 Enterprise – применяется усложненный способ аутентификации с использованием специального RADIUS-сервера для выдачи паролей. Используется динамический ключ, индивидуальный для каждого работающего клиента в

данный момент. Этот ключ может периодический обновляться по ходу работы без разрыва соединения, и за его генерацию отвечает дополнительный компонент — сервер авторизации, и почти всегда это RADIUS-сервер.

WPA3 ─ введены новые функции для упрощения настройки безопасности WiFi, обеспечения более надежной аутентификации и повышения криптографической устойчивости для высокочувствительных данных.

Протокол IEEE 802.1x обеспечивает авторизацию устройства, запросившего подключение к сети, осуществляя передачу пакетов в соответствии с протоколом расширенной аутентификации **EAP** (*Extensible Authentication Protocol*). Алгоритм аутентификации EAP поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и её пользователей с возможностью динамической генерации ключей шифрования. Стандарт 802.1x регламентирует управление доступом к сети не только на основе идентификационных данных устройств и пользователей, но и с учетом параметров протоколов верхних уровней, реализуя таким образом соответствующие политики сетевой безопасности

В стандарте 802.1x реализована эффективная процедура для защиты сети от несанкционированного доступа, для контроля клиентских потоков информации, а также для использования динамического распределения ключей доступа. Этот стандарт использует протокол EAP, который применяется как в проводных, так и в беспроводных сетях, поддерживает аутентификацию группы станций/пользователей (множественную аутентификацию) и аутентификацию типа "открытый ключ".

В структуре стандарта 802.1x можно выделить три функциональные составные части:

1) пользователь или клиент/проситель (*Supplicant*), который желает быть авторизован;

2) точка доступа (аутентификатор);

3) сервер аутентификации, обычно это RADIUS-сервер.

Перечисленные составляющие являются программными компонентами, устанавливаемыми на устройствах сети.

Сервер аутентификации **RADIUS** (*Remote Authentication Dial-In User Service*) представляет собой программу, реализующую сервис протокола клиент-сервер. Данный сервер предназначен для авторизации, аутентификации и ведения учетных записей (*Authorization, Authentication и Accounting* **— AAA**). Первоначально он использовался для регистрации клиентов в сервере сетевого доступа, связь с которыми осуществлялась по коммутируемой линии. Протокол RADIUS часто используется в различных сетевых устройствах для аутентификации пользователей, так как такие устройства имеют обычно ограниченные аппаратные ресурсы и не могут хранить в памяти информацию о большом числе пользователей.

Традиционно сервер RADIUS размещается на стороне провайдера и применяется поставщиками услуг доступа в Интернет для выполнения задач AAA. Процедура AAA содержит следующие три фазы:

1) **аутентификации** (*Authentication*) **—** проверяется имя пользователя и пароль в базе данных, а после проверки идентификационной информации начинается процесс авторизации;
2) **авторизации** (*Authorization*) **—** определяется, было ли дано разрешение на запрос доступа к ресурсам, а также назначается IP-адрес для клиента, выполняющего доступ по коммутируемой линии (*Dial-Up*);
3) **ведения учетной записи** (*Accounting*) **—** выполняется сбор информации об используемых ресурсах для оценки, аудита, учета времени сеанса или учета стоимости затрат.

Перед началом процедуры аутентификации и авторизации аутентификатор (точка доступа) создает логический порт для клиентских устройств. Этот порт основан на идентификаторе ассоциации (**AID**) и имеет два пути прохождения данных: неконтролируемый и контролируемый. Неконтролируемый путь позволяет проходить по сети всему трафику аутентификации, формируемого в соответствии со стандартом 802.1x, а контролируемый блокирует обычный трафик до тех пор, пока не будет успешно реализована аутентификация клиента в точке доступа.

Для распределения ключей между клиентами локальной сети разработан соответствующий протокол раздачи ключей в 802.1x, получивший название **EAPoL** (EAP over LANs). Процедура доступа клиента к сети согласно протоколу 802.1x происходит следующим образом.

1. Клиент (клиентский беспроводный адаптер) ассоциируется с аутентификатором точки доступа.

2. Беспроводная точка (Аутентификатор) обнаруживает кадр ассоциирования и выделяет порт для данного клиента. Порт устанавливается в неавторизованное состояние, в результате чего пропускается только служебный трафик стандарта 802.1x, а остальной трафик блокируется.

3. Аутентификатор посылает клиенту кадр с EAP-запросом идентификации, чтобы убедиться в идентичности клиента.

4. Получив от данного клиента пакет EAP-ответа, в котором содержатся идентификационные данные клиента (логин, пароль), точка доступа перенаправляет пакет серверу аутентификации.

5. Если логин и пароль пользователя были верными, сервер аутентификации передает сообщение клиенту о том, что аутентификация прошла успешно. Теперь точка доступа открывает контролируемый порт для клиента, через который он может получить доступ к сервисам сети.

Корпорация Cisco Systems, разработала и предлагает для своих беспроводных сетей, помимо упомянутых, следующие проприетарные протоколы:

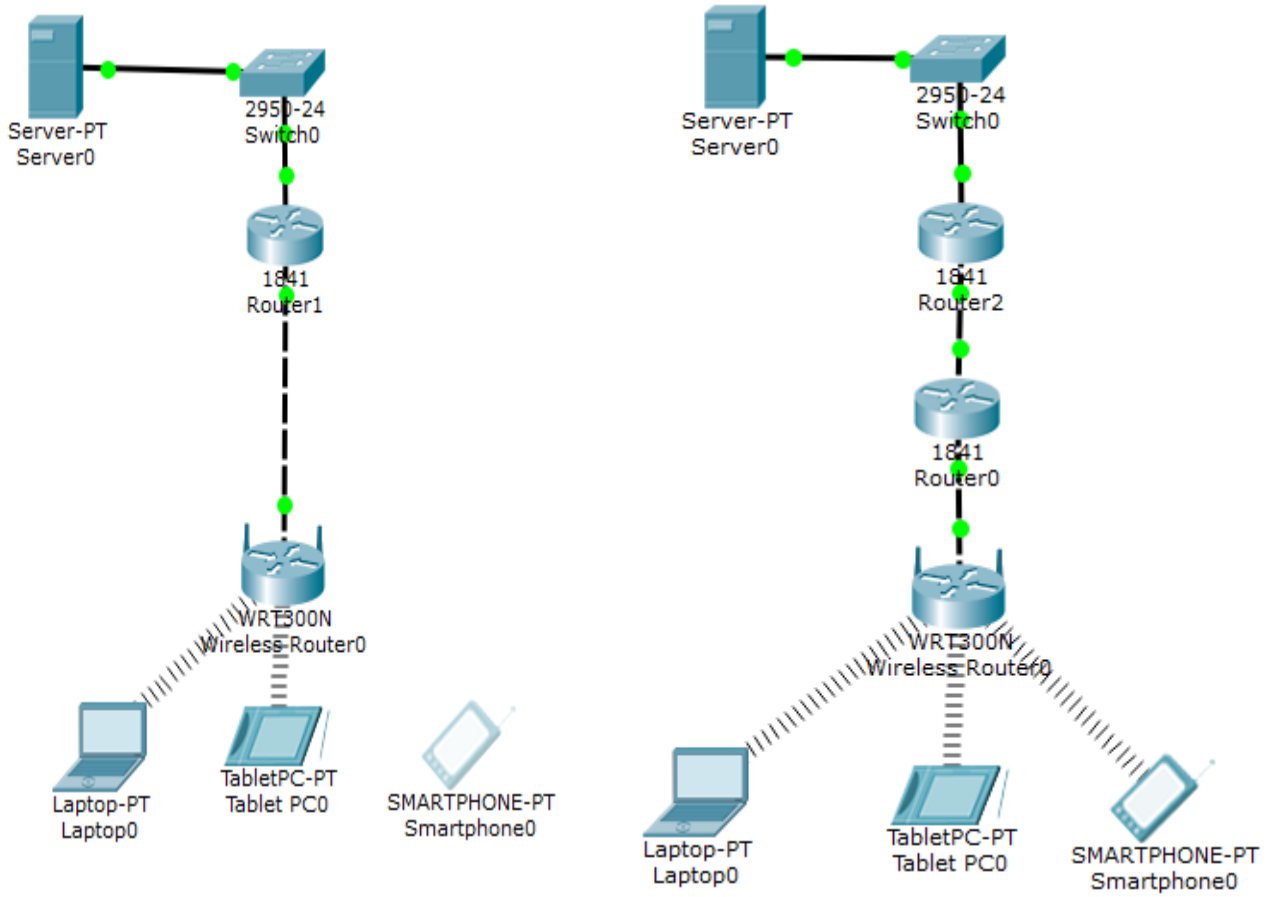
- **EAP-TLS** (*Extensible Authentication Protocol ─Transport Layer Security***)** обеспечивает аутентичность путем двустороннего обмена цифровыми сертификатами;

- **PEAP** — предусматривает обмен цифровыми сертификатами и дополнительную проверку имени и пароля по специально созданному шифрованному туннелю.

3 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

В качестве лабораторной установки используется персональный компьютер с установленной свободно распространяемой системой моделирования компьютерных сетей Packet Tracer, позволяющей осуществлять моделирования компьютерных сетей, построенных на оборудовании корпорации Cisco.

В работе исследуются процессы построения, конфигурирования и моделирования беспроводной компьютерной сети, схема которой изображена на рисунке 3.1. В качестве клиентских устройств используются мобильные устройства Laptop0 (Note book), планшетный компьютер Tablet PC0 и мобильный телефон (Smartphone0).



а) б)

Рисунок 3.1 – Схемы исследуемых беспроводных компьютерных сетей

Беспроводные устройства подключаются к сети по беспроводному каналу с помощью беспроводного маршрутизатора Wireless Router0 типа WRT300N, работающего по стандарту 802.11N. Локальная компьютерная сеть имеет обес-

печиваемый маршрутизатором Router0 выход в публичную сеть, фрагмент которой моделируется маршрутизаторами Интернет-провайдера Router1, Router2 и сервером Server0.

4 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ РЕЖИМОВ КОНФИГУРАЦИИ БЕСПРОВОДНОЙ ТОЧКИ ДОСТУПА

Практически на всех беспроводных WiFi маршрутизаторах имеются органы управления (флажки, кнопки, выпадающее меню), которые задают режимы функционирования устройства. Они позволяют выполнять следующие настройки.

Wireless enable – установка флажка будет означать включение беспроводной сети на роутере.

Network Mode – выбор типа беспроводной сети. Вы можете выбрать стандарт беспроводной связи, который будет использоваться.

Network Name (SSID) – имя точки доступа. Основное имя точки доступа беспроводной связи, которое будет закреплено за роутером. Вы так же можете включить дополнительные параметры.

Radio Band – полоса частот используемого канала. Стандартной (по умолчанию) является частота 20 МГц.

SSID Broadcast – режим публичного показа точки доступа в сети. Если Вы хотите скрыть передачу информации о точке, выключите этот параметр.

AP Isolation –Эта функция изолирует все беспроводные клиенты и беспроводные устройства в вашей сети друг от друга. Беспроводные устройства смогут соединяться с роутером, но не между собой. Для использования этой функции выберите Enabled. По умолчанию AP Isolation отключена.
Если данная функция включена, клиенты беспроводной сети, подключенные с одним и тем же SSID, не смогут общаться между собой.
BSSID – Идентификатор набора сервисов сети. По умолчанию равен мак адресу точки доступа/роутера.
Standard Channel – Номер канала. По умолчанию доступно 13 каналов, наиболее популярные 1,6,12. В случае если рядом где либо работает уже какая-либо сеть Wi-Fi, постарайтесь указать канал по номеру находящимся дальше от работающей сети.
Network Mode – режим работы: **Mixed** – новый формат кадрой, представленный в стандарте 802.11n. Он использует защитный механизм, который позволяет 802.11n-устройствам сосуществовать с устаревшими 802.11 a/b/g-устройствами, включая те, которые не принадлежат вашей Wi-Fi-сети.
Greenfield – В отличие от предыдущего режима HT-mixed, устройства, работающие в режиме Greenfield, предполагают, что рядом нет устаревших 802.11

a/b/g-станций, использующих тот же или соседние каналы. Устройства 802.11 a/b/g не могут осуществлять связь с Greenfield-устройствами, т.к. одновременное использование будет создавать коллизии, что приведет к проблемам для обеих сторон.

Channel BandWidth – Пропускная способность канала. Для сетей 802.11n выберите 20/40

Guard Interval – Защитный интервал.

Security Mode – Режим защиты в 802.11 (WEP, WPA, WPA Enterprise).

Beacon Interval – Маячковый интервал. Время между оповещениями точки доступа окружающих о своей доступности (по аналогии можно вспомнить скорость вращения окна внутри настоящего маяка). Чем меньше интервал, тем чаще посылается информация в информационное пространство.

Data Beacon Rate (DTIM) – Интервал отправки сообщения Delivery Traffic Indication Message по умолчанию равен 1.

DTIM – это обратный счетчик, уведомляющий клиентов следующего окна о необходимости прослушивания широковещательных и многоадресных сообщений.

Fragment Threshold – Размер пакета до тех пор, пока он не будет фрагментирован на мелкие пакеты.

RTS Threshold – Пороговое значение RTS (Request To Send) запроса.

RTS/CTS запросы – механизм в беспроводной сети, отсылающий RTS к точке доступа, которая посылает **CTS ответ**. Это помогает им общаться в режиме большого насыщения беспроводными сетями. В целях повышения стабильности этот параметр уменьшают до 1500 или 500.

TX Power – Мощность передатчика беспроводного сигнала. Если Вы подключаетесь к роутеру с близкого расстояния, снизьте мощность до 30–40%.

Short Preamble – Тип преамбулы. Это тип информации используемой при согласовании, изменении скорости и других важных процессов. Рекомендуется устанавливать Long если необходимо повысить качество надежности соединения.

Tx Burst – Технология увеличения общей скорости работы беспроводной сети.

Country Region Code – Выбор набора частот. Определяется регионом, где используется беспроводный маршрутизатор.

Country Code – Код текущей выбранной страны.

5 ПРОГРАММА И МЕТОДИКА ИССЛЕДОВАНИЯ

5.1. Повторить теоретический материал, относящийся к принципам передачи данных и способам защиты в беспроводных локальных компьютерных сетях.

5.2. Составить схемы исследуемых сетей (рисунок 3.1а и 3.1б) и выполнить конфигурацию параметров оборудования, обеспечивающего доступ каждого из мобильных клиентов к внешнему серверу. При конфигурации

оборудования сетей предусмотреть трансляцию адресов при обращении к внешнему серверу.

5.3. Открыть графический интерфейс настройки беспроводного маршрутизатора GUI — (*Graphical User Interface*), ознакомиться с параметрами настройки маршрутизатора WRT300N и выполнить необходимые настройки.

5.4. Пояснить роль каждого параметра, диапазон его значений, механизм влияния на защиту сети.

5.5. Проверить возможность доступа к серверу с каждого оконечного устройства при открытой аутентификации в реальном режиме и режиме симуляции.

5.6. Скопировать и исследовать форматы заголовков кадров, участвующих в обмене информацией.

5.7. Активировать протокол аутентификации WEP и проверить доступ к серверу с каждого оконечного устройства.

5.8. Активировать последовательно протоколы аутентификации повышенной защищенности WPA и WPA2 Enterprise всех доступных модификаций и проверить доступ к серверу с каждого оконечного устройства.

5.9. Составить отчет по результатам выполненной работы.

6 СОДЕРЖАНИЕ ОТЧЕТА

6.1. Титульный лист.

6.2. Цель и программа лабораторной работы.

6.3. Исходные данные в соответствии с индивидуальным вариантом.

6.4. Скриншот с топологией локальной сети.

6.5. Команды и скриншоты этапов настройки локальной сети.

6.6. Форматы кадров, участвующих в обмене информацией.

6.7. Скриншоты результатов тестирования сети.

6.8. Структура заголовков исследуемых пакетов.

6.9. Выводы.

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

7.1. Чем поясняются уязвимости проводных и беспроводных компьютерных сетей?

7.2. Перечислите и поясните категории информационной безопасности.

7.3. Что означает понятие «политика информационной безопасности» (ПИБ), какие существуют уровни политики безопасности и каковы требования к ПИБ?

7.4. Каковы угрозы безопасности и уязвимости характерны для беспроводных компьютерных сетей?

7.5. Расскажите о способах обеспечения безопасности в беспроводных компьютерных сетях.
7.6. Поясните принцип симметричного шифрования данных. Каковы преимущества и недостатки такого способа шифрования?
7.7. Поясните последовательность действий для получения доступа клиентом к беспроводной сети.
7.8. Как обеспечивается безопасность в компьютерной сети по протоколу WEP? В чем состоит недостаток этого протокола защиты?
7.9. Какие дополнительные меры повышения безопасности приняты в протоколе WPA2?
7.10. Расскажите об особенностях обеспечения безопасности работы в беспроводной сети, реализованных в протоколе IEEE 802.1x.
7.11. Расскажите о назначении сервера RADIUS и о фазах процедуры AAA.
7.12. В чем состоит отличие функционирование маршрутизатора от коммутатора второго уровня?
7.13. Чем статическая маршрутизация отличается от динамической?
7.14. Поясните принцип трансляции частных адресов в публичные.
7.15. Для чего предназначена точка доступа и как происходит передача кадров при обмене данными между двумя беспроводными клиентскими устройствами?
7.16. Чем отличается работа точки доступа от беспроводного маршрутизатора?
7.17. Каковы топологии беспроводных локальных компьютерных сетей используются в настоящее время? Проведите сравнительный анализ этих топологий.
7.18. Что означает понятие «шлюз по умолчанию», где он располагается и для чего используется?

Лабораторная работа 4
ИССЛЕДОВАНИЕ СПОСОБОВ ЗАЩИТЫ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ НА КАНАЛЬНОМ УРОВНЕ

1 ЦЕЛЬ РАБОТЫ

Углубление и закрепление теоретических знаний в области безопасности локальных компьютерных сетей и исследование механизмов защиты в локальных компьютерных сетях (ЛКС) на основе коммутаторов от атак канального уровня типа MAC-flooding и MAC-spoofing. Формирование навыков моделирования компьютерных сетей и конфигурирования коммуникационного оборудования при обеспечении защиты локальных сетей.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Безопасность функционирования корпоративной локальной компьютерной сети является залогом надежной и стабильной работы организации/предприятия. Защита ресурсов компьютерной сети осуществляется на всех уровнях эталонной модели взаимодействия открытых систем (OSI). Второй уровень сетевой модели OSI получил название «Канальный уровень» (*Data Link layer*) либо уровень передачи данных. Канальный уровень эталонной модели регламентирует передачу данных узлам, находящимся в том же сегменте локальной сети. На канальном уровне возможно реализация процедур обнаружения и исправления ошибок, возникших на физическом уровне. Регламентация процессов передачи данных на канальном уровне осуществляется несколькими протоколами. Наиболее широко на канальном уровне используются протоколы Ethernet для локальных сетей, *Point-to-Point Protocol* (PPP) для установления прямой связи между двумя оконечными точками, HDLC (*High-Level Data Link Control*), используемый преимущественно в глобальных сетях. Независимой неделимой информационной единицей канального уровня является кадр (*Frame*). Устройствам, работающим на канальном уровне, назначаются уникальные идентификаторы, функции которых выполняют функцию аппаратные адреса. В локальных компьютерных сетях одной из основных процедур канального уровня является управление доступом к общей среде. В связи с этим аппаратный адрес получил название MAC (*Medium Access Control*)-адрес. Независимой неделимой информационной единицей канального уровня является кадр (*Frame*). Управляющая информация, в состав которой входят и MAC-адреса источника и получателя, размещаются в заголовке кадра.

Злоумышленник, узнавший каким-то образом пароль, может получить доступ в сеть. Такой злоумышленник называется неавторизованным пользователем. Казалось бы, что от таких пользователей уже нельзя защититься. Однако существуют способы дополнительной защиты доступа к ресурсам сети.

Одним из механизмов защиты ЛКС от проникновения в сеть неавторизованных пользователей является механизм *port security*, реализованный на большинстве коммутаторов. Механизм *port security* позволяет осуществлять фильтрацию кадров, поступающих на отдельные порты коммутатора ЛКС, на основе MAC-адреса источника. Процедура **Port-security** обеспечивает контроль доступа неавторизованных устройств к сети, проверяя MAC-адрес источника принятого кадра и MAC-адрес назначения отправленного кадра.

При активизации данного защитного механизма на порту коммутатора создается список ассоциированных (разрешенных) с ним MAC-адресов. При поступлении на порт коммутатора с активизированной функцией *port security* кадров, MAC-адреса которых не принадлежат данному списку, коммутатор запускает заданную пользователем функцию защиты порта и автоматически выполняет заданное действие. При этом сам порт коммутатора может переходить в режим отключения (shutdown).

Существует два метода построения списка разрешенных MAC адресов: метод **статического назначения** и метод **динамического изучения**. Метод статического назначения разрешенных MAC-адресов применяется на коммутаторах доступа корпоративных сетей, центров обработки данных и т.д. При этом на порту коммутатора указывается конкретный MAC-адрес. Кроме этого, для подавления атаки MAC-flooding при настройке коммутатора также необходимо указать, что на порту коммутатора, к которому подключен пользователь, может быть, например, не больше одного MAC-адреса, а в случае, если появляется более одного, перевести порт в отключенное состояние и отправить сообщение администратору о нарушении безопасности (например, на syslog-сервер).

Метод динамического изучения адресов определяет максимальное количество MAC-адресов, ассоциируемых коммутатором с конкретным портом в течение некоторого времени. Такой способ построения таблицы адресов, как правило, целесообразно применять на уровне доступа ЛКС или в сетях филиалов. При нарушении безопасности – при поступлении на защищаемый порт коммутатора кадра с запрещенным MAC-адресом – возможно одно из трех событий: порт отключается (режим защиты **shutdown**), кадр отвергается коммутатором (режим защиты **protect**), кадр отвергается коммутатором, увеличивается счетчик нарушений порта и генерируется SNMP-сообщение (режим защиты **restrict**).

В компьютерных сетях, в которых часто происходит изменение сетевой инфраструктуры, рекомендуется ограничиваться одним MAC-адресом для порта коммутатора и использовать режим **protect**, в серверных группах – статически задавать списки MAC-адресов и использовать режим **shutdown**, в VoIP-сегментах – ограничиваться двумя или тремя MAC-адресами с активизацией режима **restrict**. Дополнительным механизмом формирования списка MAC адресов является механизм **sticky**. Он позволяет добавить статически заданные или динамически выученные MAC-адреса в конфигурационный файл ОС коммутатора.

При конфигурации портов с использованием функции Port-Security применяются следующие команды:

switchport port-security ─ Включить функцию port-security на порту.
no switchport port-security ─ Отключить эту функцию.

switchport port-security mac-address {sticky | <*mac-address*> [vlan <*vlan-id*>]}
no switchport port-security {sticky | <*mac-address*> [vlan <*vlan-id*>]} ─ Задается максимальное количество MAC-адресов для текущего порта. Если применена команда **vlan <*vlan-list*>**, порог будет распространяться на указанные VLAN**.** Команда **no** восстанавливает конфигурацию по умолчанию ─ 1 MAC для порта.

switchport port-security violation {protect | recovery | restrict | shutdown}

no switchport port-security violation ─ Выбрать действие при анализе нового MAC-адреса, если превышено заданное максимальное число адресов. **protect ─** не изучать новый MAC, не отправлять уведомление; **recovery ─** изучить новый MAC; **restrict ─** не изучать новый MAC, отправить уведомление **trap** и запись в системный журнал **syslog**; **shutdown ─** выключить порт. Команда **no** восстанавливает конфигурацию по-умолчанию **─ shutdown.**

clear port-security {all | configured | dynamic | sticky} [[address <*mac-addr*> | interface <*interface-id*>] [vlan <*vlan-id*>]] ─ Очистить таблицу изученных MAC адресов: **all ─** все, **dynamic ─** изученных динамически; **configured ─** добавленных вручную; добавленных функцией **sticky.**

show port-security [interface <*interface-id*>] [address | vlan] ─ Отобразить информацию о конфигурации port-security.

Пример конфигурации Port-Security

Для предотвращения подмены MAC одного пользователя другими, установить на портах коммутатора доступа процедуру **port-security**. Процедура будет разрешать доступ только авторизованным устройствам и отправлять оповещение администратору при попытке изучения неизвестного адреса.

Сценарий конфигурации имеет следующий вид.

Switch(config)#interface Ethernet 1/0/1-1/0/24
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#exi

При попытках получить доступ к ресурсам сети или нарушить ее функционирование неавторизированные пользователи (злоумышленники) используют несколько видов атак с участием информации о MAC-адресах кадров. В названиях этих атак применяется аббревиатура MAC. Наиболее часто на канальном уровне встречаются атаки MAC-flooding и MAC-spoofing.

Атака **MAC-flooding** относится к классу разведывательных атак. Этот вид несанкционированного доступа может использоваться также и в качестве DoS-атаки. Атакующая машина загружает коммутатор огромным количеством кадров с неверными MAC-адресами отправителя. Коммутаторы имеют ограниченную память для таблицы коммутации, содержащей записи MAC→порт (например, в коммутаторе Catalyst 2960 в таблице коммутации помещается 8192 записей). Поэтому при атаке MAC-flooding таблица будет быстро заполнена некорректными MAC-адресами, пришедшими от атакующей рабочей станции. Фактически коммутатор в такой ситуации начинает функционировать, как простой концентратор (хаб). Т.е., при поступлении легального трафика, из-за отсутствия соответствующих записей в таблице коммутации, пакеты будут направляться на все порты коммутатора. В результате этого атака может вызвать перегрузку каналов коммутатора и отказа в пересылке кадров получателям. В некоторых случаях может произойти утечка информации, так как злоумышленник может «прослушать» весь сетевой трафик и получить конфиденциальную информацию.

Атака канального уровня **MAC-spoofing** состоит в том, что на сетевой карте злоумышленника изменяется MAC-адрес, что позволяет ему обойти список контроля доступа к серверам или маршрутизаторам, замаскировать свой компьютер, либо захватить трафик необходимого ему устройства.

Следует отметить, что всё это действенно только для VLAN, в котором находится злоумышленник, т.е. после переполнения данной таблицы атакующий сможет прослушивать весь сетевой трафик, который «проходит» через коммутатор.

3 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

Лабораторная установка состоит из персонального компьютера с инсталлированной системой моделирования компьютерных сетей Cisco Packet Tracer. бъектом исследования является локальная компьютерная сеть, построенная на основе коммутаторов, схема которой изображена на рисунке 3.1.

Локальная сеть состоит из двух виртуальных локальных сетей, построенных на основе коммутаторов второго уровня SW4-2 и SW4-3, объединенных маршрутизирующим коммутатором третьего уровня SW4-1и двух внутренних серверов. Интерфейсы (порты) коммутатора SW4-1 Fa0/2 и Fa0/3 являются магистральными (транковыми), а Fa0/4 и Fa0/5 – портами доступа. Магистральные линии связи обозначены жирными линиями, а линии доступа – тонкими.

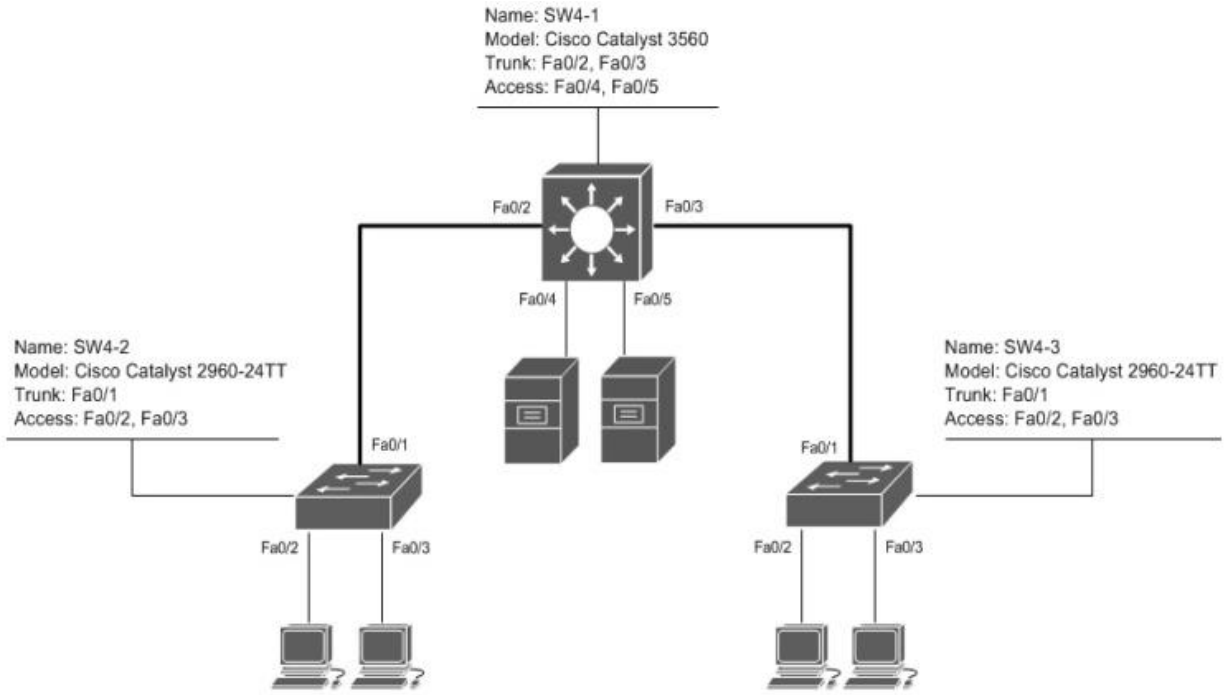


Рисунок 3.1 ─ Схема исследуемой локальной компьютерной сети

.

4 ПРОГРАММА И МЕТОДИКА ВЫПОЛНЕНИЯ РАБОТЫ

4.1. Изучить теоретический материал, относящийся к компьютерным атакам, осуществляемым на различных уровнях эталонной модели взаимодействия компьютерных систем (выполняется в процессе домашней подготовки).

4.2. Построить в окне эмулятора Packet Tracer схему сегмента компьютерной сети, изображенной на рисунке 3.1.

4.3. Осуществить конфигурацию оборудования сети, обеспечивающей защиту сети от атак типа MAC-flooding и MAC-spoofing.

4.4. Выполнить конфигурацию коммутатора канального уровня SW4-3, обеспечивающей механизм защиты типа port security в динамическом режиме для рабочих станций. Для этого необходимо осуществить следующие настройки:

```
switch# conf t
switch(config)#interface range fa0/2-3
switch(config-if-range)#switchport mode access
switch(config-if-range)#switchport port-security !-- включение защиты порта
switch(config-if-range)#switchport port-security maximum 1
!-- указание количества адресов на порту
switch(config-if-range)#switchport port-security violation protect
!-- указание режима protect  ( violation - нарушение)
switch#show port-security !-- просмотра установок, сделанных на портах
```

4.5. Выполнить аналогичные настройки реализации механизма защиты port security на коммутаторе SW4-2.

4.6. Произвести конфигурацию коммутатора третьего уровня SW4-1, обеспечивающую механизм защиты port security в статическом режиме с привязкой к заданному MAC-адресу для порта FastEthernet0/4. Для этого необходимо реализовать следующий сценарий:

```
interface fa0/4
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address xxxx.yyyy.zzzz
switchport port-security violation shutdown
!-- выключение при нарушении безопасности
```

4.7. На коммутаторе 3-го уровня SW4-1 выполнить дополнительную настройку реализации механизма port security в статическом режиме с опцией sticky для порта FastEthernet0/5. Для этого необходимо реализовать следующий сценарий:

```
interface fa0/5
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

4.8. Исследовать функционирование механизма обеспечения безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-spoofing. Для этого установить MAC-адрес рабочей станции, подключенной к порту коммутатора со статическим методом формирования списка MAC-адресов, несоответствующий требованиям политики безопасности. Убедиться в переводе порта коммутатора в режим shutdown или protect.

4.9. Исследовать функционирование механизма обеспечения безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-flooding. Для этого на порт коммутатора с динамическим методом формирования списка разрешенных MAC-адресов подключить коммутатор с несколькими рабочими станциями. Убедиться в переводе порта коммутатора в режим shutdown или protect.

4.10. Оформить отчет и сформулировать выводы по результатам проведенных исследований.

5 СОДЕРЖАНИЕ ОТЧЕТА

5.1. Титульный лист.
5.2. Цель и программа лабораторной работы.
5.3. Исходные данные в соответствии с индивидуальным вариантом.
5.4. Скриншот с топологией локальной сети.
5.5. Команды и скриншоты этапов настройки локальной сети.
5.6. Скриншоты результатов тестирования сети.
5.7. Выводы.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

6.1. В чем состоит отличие канального уровня от сетевого и транспортного?
6.2. Чем отличаются меду собой коммутаторы 2-го и 3-го уровней?
6.3. В чем состоит суть DoS атаки?
6.4. Как осуществляется DDoS атака?
6.5. В чем состоит суть MAC-flooding атаки?
6.6. Что представляет собой таблица коммутации и каким образом она формируется в коммутаторе? Каков ее размер?
6.7. К каким нежелательным последствиям может привести MAC-flooding атака?
6.8. В чем состоит суть MAC-spoofing атаки?
6.9. Расскажите о особенностях механизма port security?
6.10. Чем отличается способ статического назначения адресов от динамического?
6.11. Чем отличается режим защиты protect от режима защиты restrict?
6.12. Какие возникают аномалии в работе сети при попытках проникновения в сеть?
6.13. В чем состоит суть сигнатурного анализа при защите сетей от атак?
6.14. Из каких компонентов состоит система обнаружения вторжений?
6.15. Какие функции выполняет межсетевой защитный экран (брандмауэр)?
6.16. Как организована защита сети на базе сервера RADIUS?

Лабораторная работа 5

ИССЛЕДОВАНИЕ СПОСОБОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ СПИСКОВ КОНТРОЛЯ ДОСТУПА

1 ЦЕЛЬ РАБОТЫ

Исследование методов защиты от несанкционированного доступа к сетевым ресурсам и способов составления списков ограничения доступа, приобретение практических навыков составления стандартных и расширенных списков доступа, а также конфигурации сетевого оборудования.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

2.1 Общая характеристика списков контроля доступа

Для защиты локальной компьютерной сети (ЛКС), подключенной к сети Интернет, от потенциальных угроз на стыке ЛКС и глобальной сети устанавливается защитный сетевой экран (брандмауэр, файервол). Он выполняется зачастую в виде самостоятельного устройства, в котором функции защиты с целью повышения быстродействия, реализуются аппаратным способом. Однако существуют и программные брандмауэры, построенные на основе специально выделенных компьютеров (прокси-серверы) или маршрутизаторов, но быстродействие таких защитных экранов существенно ниже. И в аппаратных и программных защитных экранах контроль входящих и исходящих пакетов осуществляется на основе списков доступа ***ACL* (*Access Control Lists*)**, которые являются своеобразными фильтрами пакетов. Они позволяют запретить или разрешить определенным хостам доступ к ресурсам сети. Например, в корпоративной сети администраторы могут запретить доступ к внутреннему серверу или в Интернет определенным пользователям, а остальным наоборот – разрешить.

Списки доступа позволяют фильтровать трафик на входе и выходе интерфейсов маршрутизаторов. На входе весь поступающий трафик подвергается фильтрации. Нежелательные пакеты отбрасываются и уже только потом остальные пакеты маршрутизируются. Если же ACL настроены на выходе интерфейса, то трафик фильтруется сразу же после процесса маршрутизации. Списки доступа позволяет использовать маршрутизатор как межсетевой экран (файрвол, брандмауэр) для запрета или ограничения доступа к внутренней сети из внешней, например, сети Интернет. Брандмауэр, как правило, помещается в точках соединения между двумя сетями.

Списки доступа содержат набор инструкций (директив, предписаний) какие порты и адреса блокировать, а какие наоборот разрешить. Этих инструкций в списке может быть от единиц до нескольких десятков. В конце списка всегда содержится неявная инструкция по блокировке всего трафика. Данная инструк-

ция добавляется автоматически самой системой. В настройках она не видна, но нужно учитывать ее наличие.

На настоящее время существуют 3 типа списков доступа: 1) стандартные; 2) расширенные и 3) именованные списки.

Стандартные списки позволяют проверять только IP адрес отправителя. Стандартные списки доступа рекомендуется устанавливать как можно ближе к отправителю. Стандартные и расширенные списки доступа обязательно нумеруются. Номера стандартных списков могут принимать значение от 0 до 99.

Расширенные списки управления доступом *extended ACL* (*extended Access Control List*) используются чаще, чем стандартные, поскольку они обеспечивают большие возможности контроля. Расширенные списки предписывают проверку как адреса отправителя, так и адреса получателя. Они могут также проверять конкретные протоколы, номера портов и другие параметры. Это придает им большую гибкость в задании проверяемых условий. Пакету может быть разрешена отправка или отказано в передаче в зависимости от того, откуда он был выслан и куда направлен. Расширенным спискам доступа назначаются номера от 100 до 199.

Именованные списки аналогичны стандартным и расширенным ACL, но вместо номеров используются имена списков. Стандартные и расширенные списки редактировать нельзя. К примеру, нельзя в середину списка вставить команду или удалить ее. Для этого нужно сначала **деактивировать список на самом интерфейсе**, а затем полностью его удалить и настроить заново. Именованные списки позволяет редактировать вновь созданные списки. Все введенные команды нумеруются, что позволяет легко добавлять и удалять команды.

2.2 Правила составления списков доступа

Правила построения и назначения списков доступа для различных протоколов имеют свою специфику, однако, можно выделить два этапа работы с любыми списками доступа. Сначала, создается список доступа, а затем выполняется привязка его к соответствующему интерфейсу, линии связи или логической операции, выполняемой маршрутизатором (роутером).

Каждое предписание в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с директивами, имеющих один и тот же номер (или имя). Порядок задания директив в списке играет важную роль. Проверка пакета на соответствие списку производится последовательным применением предписаний из данного списка (в том порядке, в котором они были внесены). В конце каждого списка системой IOS добавляется неявное правило, состоящее в том, что если пакет удовлетворяет какому-либо предписанию, то дальнейшие проверки его на соответствие следующим директивам в списке НЕ ПРОИЗВОДЯТСЯ. Таким образом, пакет, который не соответствует ни одному из введенных предписаний, отвергается.

Для одного списка можно определить несколько директив. Каждая из них должна ссылаться на имя или на номер списка для того, чтобы все они были связаны с одним и тем же списком. Количество директив может быть произвольным, и ограничено лишь объемом имеющейся памяти. Однако, чем больше в списке директив, тем труднее понять логику работы списка и контролировать ее. Поэтому рекомендуется тщательно заносить всю информацию о списках в специальный журнал.

Как уже упоминалось выше, порядок строк в списке доступа очень важен, поскольку невозможно изменить этот порядок или исключить какие-либо строки из существующего списка доступа. По этой причине целесообразно предварительно создавать списки доступа (например, на tftp-сервере) и загружать их целиком в маршрутизатор, а не пытаться редактировать их на маршрутизаторе. Если список доступа с данным номером (именем) существует, то строки списка с тем же номером (именем) будут добавляться к существующему списку в конец его.

Списки управления доступом представляют собой перечень особых **директив** (предписаний): «**разрешит**ь» (*permit*) и «**запретить**» (*deny*). Эти директивы применяются к адресам или протоколам верхних уровней (3-7). Предписание «разрешить» означает, что все пакеты, отвечающие определенным условиям, будут пропущены, т.е. им будет разрешено дальнейшее перемещение по сети. Директива «запретить» указывает, что пакет, имеющий определенные характеристики, необходимо удалить. Списки доступа могут применяться для запрещения продвижения пакетов через определенный интерфейс маршрутизатора в ту или другую сторону, для ограничения доступа некоторых пользователей и устройств к сетевым ресурсам, для указания способа шифрования, а также для указания приоритетности обработки пакетов.

Каждая из директив в списке доступа читается процессором маршрутизатора по порядку, т.е. очередной пакет, проходящий через соответствующий порт, будет последовательно сравниваться со всеми критериями **(**адресом источника, адресом получателя или номером порта**) в списке доступа с начала списка до конца.** Если пакет не соответствует условию первой директивы, то он проверяется на соответствие второй директиве из списка управления доступом. А если параметры пакета соответствуют следующему условию, которое представляет собой директиву разрешения доступа, то ему разрешается отправка на интерфейс получателя. Таким образом, при первом обнаружении соответствия остальные директивы не рассматриваются. Поэтому, если была записана директива, разрешающая передачу всех данных, то все последующие директивы не проверяются. Следует особо подчеркнуть, что **в конце каждого списка выполняется неявное правило "deny all"** (запретить все), поэтому при назначении списков на интерфейс нужно следить, чтобы явно разрешить все виды необходимого трафика через интерфейс (не только пользовательского, но и служебного, например, обмен информацией по протоколам динамической маршрутизации).

Для создания **стандартного списка доступа** для маршрутизаторов Cisco применяется команда **access-list**, которая вводится в следующем формате:

access-list <номер_списка> {deny|permit} <адрес отправителя> [маска шаблона адреса] [log]

Маска шаблона (англ. *wildcard mask*) указывает маршрутизатору на те биты в шаблоне адреса отправителя, которые следует сравнивать с поступившим в порт маршрутизатора адресом отправителя, и те, которые нужно проигнорировать. Как и маска в схеме адресации протокола IP, маска шаблона в списке доступа состоит из 32-х битов, записанных в точечно-десятичной форме. Например, маска шаблона 0.0.0.255 соответствует двоичному представлению 00000000.00000000.00000000.11111111. Однако **запись маски шаблона** в списках доступа, в отличие от метода записи маски адреса на сетевых интерфейсах, **записана инверсно**, т.е. единицами отмечены биты адреса, которые НЕ будут проверяться. **Нулевые биты** в маске списка доступа предписывают маршрутизатору **необходимость сравнения** соответствующих битов IP-адреса в проверяемом пакете с аналогичными битами в шаблоне адреса. Соответственно, единичные биты указывают на то, что сравнение производить не нужно. Таким образом, маска 0.0.0.0 вынуждает маршрутизатор сравнивать все 32 бита адреса пакета на соответствие их битам шаблона, заданного в списке доступа.

Ключевое слово "**log**" инициирует выдачу записи о совпадении пакета с данным предписанием на консоль и в системный лог-файл. Часто используемое описание фильтра, которому удовлетворяет любой адрес 0.0.0.0 255.255.255.255, имеет специальное обозначение "any":

access-list <access-list-number> {deny | permit} any

В **расширенном списке** перед полем адреса источника можно указывать **тип протокола**, а после адреса источника указываются (при необходимости) адрес хоста назначения и порт. Общий формат расширенного списка доступа имеет следующий вид:

access-list номер-списка {permit | deny} {протокол} {адрес источника} [маска-источника][адрес получателя] [маска-получателя] [оператор номер порта] [established] [log]

Параметры списка могут принимать значения:
оператор — lt, gt, eq, neq (меньше чем, больше чем, равно, не равно); established — разрешает прохождение ответного TCP-потока (от web-сервера) во внутреннюю сеть, если он использует установленное из внутренней сети соединение (т. е. если бит АСК в заголовке сегмента установлен). Частные случаи списков доступа могут иметь вид:

access-list access-list-number {deny|permit} протокол any any

или

access-list access-list-number {deny | permit} протокол host source host destination

Если в качестве протокола указано "tcp" или "udp", то описания source- и destination-wildcard могут включать номера портов для данных протоколов с

ключевыми словами "eq" (*equal*) — равно, neq (*not equal*) — не равно, "lt" (*less than*) — меньше чем, "gt" (*greater then*) — больше чем, "range" — указание диапазона номеров портов. Для протокола "tcp", возможно также применение слова "established" для выделения только установленных tcp-сессий. Ключевое слово "host source" эквивалентно записи: "source 0.0.0.0".

При использовании именованных списков в список добавляется оператор, указывающий на стандартный (*standard*) или расширенный (*extended*) список доступа. Синтаксис такого списка имеет вид:

ip access-list {standard | extended} <имя ACL>}

Пример формирования стандартного списка.

Запретить прохождение через маршрутизатор пакетов с рабочей станции с IP-адресом 235.12.60.23 и пропустить все остальные.

В связи с тем, что запрет осуществляется только по адресу источника, используем стандартный список доступа, присвоив ему номер 4.

access-list 4 deny host 235.12.60.23
access-list 4 permit any

При составлении сценариев конфигурации маршрутизаторов следует помнить, что команды всех видов списков доступа вводятся в режиме конфигурирования маршрутизатора, который индицируется промптом: Router(config)#.

Для того чтобы список доступа начал выполнять свою функцию, он должен быть применен к интерфейсу с помощью команды

Router(config-if)#ip access-group номер-списка-доступа in|out

Список доступа может быть применен как входной (in) либо как выходной (out). Когда список доступа применяется как входной, то маршрутизатор получает входной пакет и сверяет содержащийся в нем адрес с элементами списка. Маршрутизатор разрешает пакету маршрутизироваться на интерфейс назначения, если пакет удовлетворяет разрешающим элементам списка, либо отбрасывает пакет, если он соответствует условиям запрещающих элементов списка. Если список доступа применяется как выходной, то маршрутизатор получает входной пакет, пересылает его на интерфейс назначения и только тогда проверяет содержащийся в пакете адрес согласно элементам списка доступа этого интерфейса. Далее маршрутизатор либо разрешает отправку пакета через выходной интерфейс, либо отбрасывает его согласно разрешающим и запрещающим директивам списка соответственно. Так, созданный ранее список, например, с номером 77 применяется к интерфейсу Ethernet 0 маршрутизатора как входной список следующими командами:

Router(config)#int Ethernet 0
Router(config-if)#ip access-group 77 in

Этот же список применяется к интерфейсу Ethernet 0 маршрутизатора как выходной список с помощью команд

Router(config-if)#ip access-group 77 out

Отменить список на интерфейсе можно с помощью команды **no.**

Router(config-if)#no ip access-group 77 out

Рассмотрим принцип создания более сложных списков доступа. Пусть имеем сеть, изображенную на рисунке 2.1.

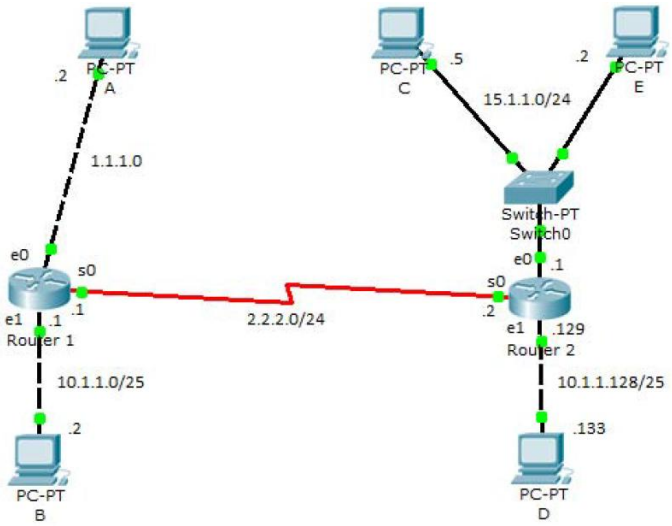


Рисунок 2.1 – Пример топологии сети для создания сложных списков доступа

Разрешим все пакеты, исходящие из сети 10.1.1.0/25 (10.1.1.0 255.255.255.128), но запретим все пакеты, поступающие из сети 10.1.1.128 /25 (10.1.1.128 255.255.255.128) по последовательному интерфейсу S0. Пусть также необходимо запретить все пакеты, исходящие из сети 15.1.1.0 /24 (15.1.1.0 255.255.255.0), за исключением пакетов от единственного хоста с адресом 15.1.1.5. Все остальные пакеты разрешаем. Списку присвоим номер 2. Последовательность команд для выполнения поставленной задачи будет следующая:

Router(config)#**access-list 2 deny 10.1.1.128 0.0.0.127**
Router(config)#**access-list 2 permit 15.1.1.5 0.0.0.0**
Router(config)#**access-list 2 deny 15.1.1.0 0.0.0.255**
Router(config)#**access-list 2 permit 0.0.0.0 255.255.255.255**

Отметим отсутствие разрешающего элемента для сети 10.1.1.0 255.255.255.128. Его роль выполняет последний элемент **access-list 2 permit 0.0.0.0 255.255.255.255.**

Удостоверимся, что поставленная задача выполнена.

1. Разрешить все пакеты, исходящие из сети 10.1.1.0 255.255.255.128. Последняя строка в списке доступа удовлетворяет этому критерию. Нет необходимости в явном виде разрешать эту сеть в нашем списке доступа так, как в списке нет строк, соответствующей этой сети за исключением последней разрешающей строки permit 0.0.0.0 255.255.255.255.

2. Запретить все пакеты, исходящие из сети 10.1.1.128 255.255.255.128. Первая строка в списке выполняет этот критерий. Инверсная маска 0.0.0.127 для этой сети предписывает, что не нужно брать в рассмотрение последние семь бит четвертого октета адреса, которые назначены для адресации компьютера в данной подсети. Маска для этой сети 255.255.255.128, которая указывает, что последние семь бит четвертого октета определяют адресацию компьютера в данной сети.

3. Запретить все пакеты, исходящие из сети 15.1.1.0 255.255.255.0, за исключением пакетов от единственного хоста с адресом 15.1.1.5. Это требование удовлетворяется второй и третьей строкой нашего списка доступа. Важно отметить, что список доступа осуществляет это требование не в том порядке как оно определено. Обязательно следует помнить, что список доступа обрабатывается сверху вниз и **при первом совпадении обработка пакетов прекращается**. Поэтому вначале запрещаются все пакеты, исходящие из сети 15.1.1.0 255.255.255.0 и лишь затем разрешаются пакеты с адресом 15.1.1.5. Если в командах, определяющих список доступа, переставить вторую и третью команды, то вся сеть 15.1.1.0 будет запрещена до разрешения хоста 15.1.1.5. То есть, адрес 15.1.1.5 сразу же в начале будет запрещен более общим критерием **deny 15.1.1.0 0.0.0.255.**

4. Разрешить все остальные пакеты. Последняя команда разрешает все адреса, которые не соответствуют первым трем командам.

Таким образом, последовательность действий для реализации списка доступа может быть записана в следующем виде.

1. Определить критерии и ограничения для доступа.

2. Реализовать их с помощью команд access-list, создав список доступа с определенным номером.

3. Применить список к определенному интерфейсу либо как входящий, либо как исходящий.

Следует заметить, что в общем случае стандартный список доступа нужно помещать как можно ближе к точке назначения, а не к источнику пакетов. Если список помещен вблизи источника пакетов, то очень вероятно, что доступ к устройствам, на которых не осуществляется никакая конфигурация доступа, будет затруднен.

Конкретизируем политику безопасности для сети на рисунке 2.1. Наша цель создать политику для компьютера A (адрес 1.1.1.2 сеть 1.1.1.0/24), которая изо всех устройств локальной сети 15.1.1.0/24, в которую входит компьютер C (15.1.1.5), разрешит доступ к компьютеру A только компьютеру C. Требуется также создать политику, запрещающую удаленный доступ к компьютеру A из любого устройства локальной сети 10.1.1.128 / 25 компьютера D (10.1.1.133). Весь остальной трафик мы разрешаем. На рисунке 2.1 компьютер PC5 (15.1.1.5) играет роль произвольного, отличного от компьютера C, представителя локальной сети 15.1.1.0/24.

Размещение списка критично для реализации такой политики. Возьмем созданный ранее список с номером 2. Если список сделать выходным на последовательном интерфейсе S0 маршрутизатора 2, то задача для компьютера A бу-

дет выполнена, однако возникнут ограничения на трафик между другими локальными сетями. Аналогичную ситуацию получим, если сделаем этот список входным на последовательном интерфейсе маршрутизатора 1. Если мы поместим этот список как выходной на интерфейс Ethernet0 маршрутизатора 1, то задача будет выполнена безо всяких побочных эффектов.

Именованные ACL

К именованным ACL обращаются по имени, а не по номеру, что дает наглядность и удобство для обращения. Для создания именованного ACL имеется команда

Router(config)#**ip access-list standard|extended** ACL_name

и далее команды для создания элементов списка

Router(config-ext-nacl)#**permit|deny** IP_protocol source_
IP_address
wildcard_mask [protocol_information] destination_IP_address
wildcard_mask [protocol_information] [log]

Для завершения создания списка следует дать команду **exit**.

Имя именованного списка чувствительно к регистру. Команды для создания неименованного списка аналогичные командам для создания элементов нумерованного списка, но сам процесс создания отличен. Вы должны использовать ключевое слово ip перед главным ACL оператором и тем самым войти в режим конфигурации именно для этого именованного списка. В этом режиме вы начинаете с ключевых слов permit или deny и не должны вводить access-list в начале каждой строки.

Привязка именованных ACL к интерфейсу осуществляется командой

Router(config)#**interface** type [slot_№] port_№
Router(config-if)#**ip access-group** ACL_name **in|out**

Именованный ACLs возможно редактировать. Для этого надо набрать команду, которая была использована для его создания

Router(config)#**ip access-list standard|extended** ACL_name

С помощью клавиш с вертикальными стрелками следует найти строку списка, которую нужно изменить. Изменить ее, используя горизонтальные стрелки. Нажать ввод. Новая строка добавится в конец списка. Старая не уничтожится. Для ее удаления следует ввести **no** в начале строки. Для редактирования же числовых ACLs необходимо его уничтожить и создать заново или изменить список офлайн и загрузить в устройство с помощью telnet.

Пример именованного списка доступа.

Создается стандартный список доступа с именем Internet_filter и расширенный список доступа с именем marketing_group:

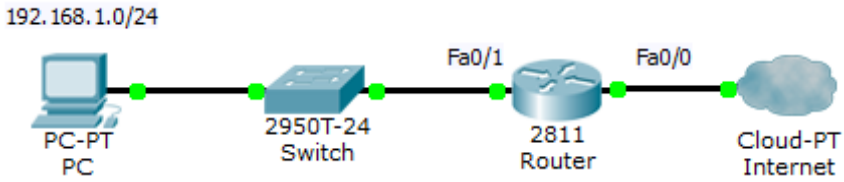
```
Router(config)#interface Ethernet0/5
Router(config-if)#ip address 2.0.5.1 255.255.255.0
Router(config)#ip access-group Internet_filter out
Router(config-if)#ip access-group marketing_group in
Router(config)#ip access-list standard Internet_filter
Router(config-ext-nacl)#permit 1.2.3.4
Router(config-ext-nacl)#deny any
Router(config)#ip access-list extended marketing_group
Router(config-ext-nacl)#permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Router(config-ext-nacl)#deny tcp any any
Router(config-ext-nacl)#permit icmp any any
Router(config-ext-nacl)#deny udp any 171.69.0.0 0.0.255.255 lt 1024
Router(config-ext-nacl)#deny ip any any log
```

Reflexive ACL – зеркальные списки контроля доступа

Зеркальные (reflexive) ACL – это расширение технологии extended ACL, которое позволяет организовать пропуск трафика из Интернета в локальную сеть только в ответ на предварительно сделанный запрос из локальной сети в Интернет. Зеркальные списки ACL можно задать **только** с помощью расширенных именованных списков ACL для протокола IP. Их нельзя определить с помощью нумерованных или стандартных списков ACL для протокола IP или с помощью списков ACL для других протоколов.

Суть фильтрации пакетов состоит в следующем: на выходной интерфейс локальной сети прикрепляется ACL, который пропускает исходящий трафик. Одновременно автоматически формируется встречный ACL для пропуска входящего трафика. Благодаря этому разрешается получать ответы из Интернета только на свои запросы. Ключевые слова, используемые в Reflexive ACL – это **reflect** для исходящего трафика и **evaluate** для входящего.

Пример. Пусть имеется локальная компьютерная сеть с адресом 192.168.1.0/24. Из нее нужно организовать доступ в Интернет всем клиентским компьютерам сети по протоколам http, pop и smtp.



Вначале необходимо создать именованный расширенный список для исходящего трафика, например, с именем IN-TO-OUT, а затем для входящего трафика список именем OUT-TO-IN. При этом следует учитывать, что сообщения для указанных сервисов (http, pop и smtp) передаются по протоколу TCP. Сценарий, реализующий заданные условия, имеет следующий вид.

```
R1(config)#ip access-list extended IN-TO-OUT
```

```
R1(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 any eq www reflect BACK-WWW
R1(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 any eq pop3 reflect BACK-POP
R1(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 any eq smtp reflect BACK-SMTP
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended OUT-TO-IN
R1(config-ext-nacl)#evaluate BACK-WWW
R1(config-ext-nacl)#evaluate BACK-POP
R1(config-ext-nacl)#evaluate BACK-SMTP
```

Здесь BACK-WWW, BACK-POP и BACK-SMTP – имена зеркальных списков доступа. Параметр **reflect name** используется для создания рефлексивного списка доступа.

Затем эти списки связываются с внешним fa0/0 и внутренним fa0/1 интерфейсами маршрутизатора.

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group OUT-TO-IN in
R1(config)#interface fa0/1
R1(config-if)#ip access-group IN-TO-OUT out
R1(config-if)#
```

Список IN-TO-OUT разрешает выход трафика изнутри наружу. Пропускается трафик на порты 25, 80 и 110, параллельно формируются зеркальные ACL с именами BACK-WWW, BACK-POP и BACK-SMTP, которые пропускают обратный трафик. Весь трафик извне фильтруется ACL с именем OUT-TO-IN, который по умолчанию ничего не пропускает, но когда появляются зеркальные записи, то трафик начинает пропускаться.

Предположим, что пользователь обращается с адреса 192.168.1.100 к веб страничке на сервере 123.123.123.123 при обращении выбирается случайный порт отправителя (например, 1235), порт получателя используется стандартный – 80. Когда пакет проходит через маршрутизатор, он проверяется IN-TO-OUT и на основании первой строчки списка выводится в канал. Одновременно в ACL с именем BACK-WWW автоматически на время добавляется зеркальная запись:

```
permit tcp host 123.123.123.123 eq 80 host 192.168.1.100 eq 1235
```

То есть, в настоящий момент весь трафик из интернета вовнутрь будет заблокирован, за исключением ответа от веб-сервера на наш запрос. Преимущество Reflexive ACL перед established заключается в том, что при established пользуется только флагом в TCP сегменте, а Reflexive реально отслеживает соединения. Флаг можно подделать, в этом случае входящий трафик начнет пропускаться. Конечно, его вряд ли кто-то примет, но можно устроить, например, DOS атаку. Но самое важное преимущество, с помощью established в принципе

нельзя организовать пропуск протоколов, отличных от TCP. Например, протоколов, базирующихся на UDP, или ICMP трафик. Зеркальные же ACL успешно справляются с этими задачами.

ACL обрабатываются сверху вниз. Наиболее часто повторяющийся трафик должен быть обработан в начале списка. Как только обрабатываемый списком пакет удовлетворяет элементу списка, обработка этого пакета прекращается. Стандартные ACLs следует помещать ближе к точке назначения, где трафик должен фильтроваться. Выходные (out) расширенные ACLs следует помещать как можно ближе к источнику фильтруемых пакетов, а входные следует помещать ближе к точке назначения, где трафик должен фильтроваться.

Ограничение доступа виртуального терминала к VTY при помощи ACL.

ACL можно применять не только для фильтрации трафика, но и для ограничения адресов, с которых можно подключиться с помощью виртуально терминала к маршрутизатору по telnet или ssh.

Сначала создается стандартный ACL, в котором перечисляются адреса и сети, из который доступ по telnet надо разрешить. Теперь его необходимо применить непосредственно на **line vty 0 4**, то есть, на линии виртульного терминала, к которым происходит подключение. Таким образом, не важно, через какой интерфейс маршрутизатора telnet-пакеты попадут на роутер, они будут отфильтрованы когда доберутся собственно до vty.

На маршрутизаторе создается стандартный список доступа **VTY_ACCESS**:

```
Router(config)#ip access-list standard VTY_ACCESS
Router(config-std-nacl)#permit 15.15.1.0 0.0.0.255
```

Устанавливается ограничение доступа к **VTY** на маршрутизаторе:

```
Router(config)#line vty 0 4
Router(config-line)#access-class VTY_ACCESS in
```

Теперь по telnet можно подключиться только из сети 15.15.1.0.
Обратите внимание, что ACL применяется на интерфейсе командой access-group, а на vty – командой access-class.

3. ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

В качестве лабораторной установки используется персональный компьютер с инсталлированной программой Cisco Packet Tracer, позволяющей осуществлять моделирования компьютерных сетей, построенных на оборудовании корпорации Cisco. Подробно описание пакета моделирования и работы с ним приведено в лабораторной работе №1. Схема первой объединенной компьютерной сети изображена на рисунке 3.1. Она состоит из трех сетей, соединенных посредством маршрутизаторов последовательными линиями связи. В пер-

вой сети расположены серверы, вторая и третья сети являются сетями рабочих групп.

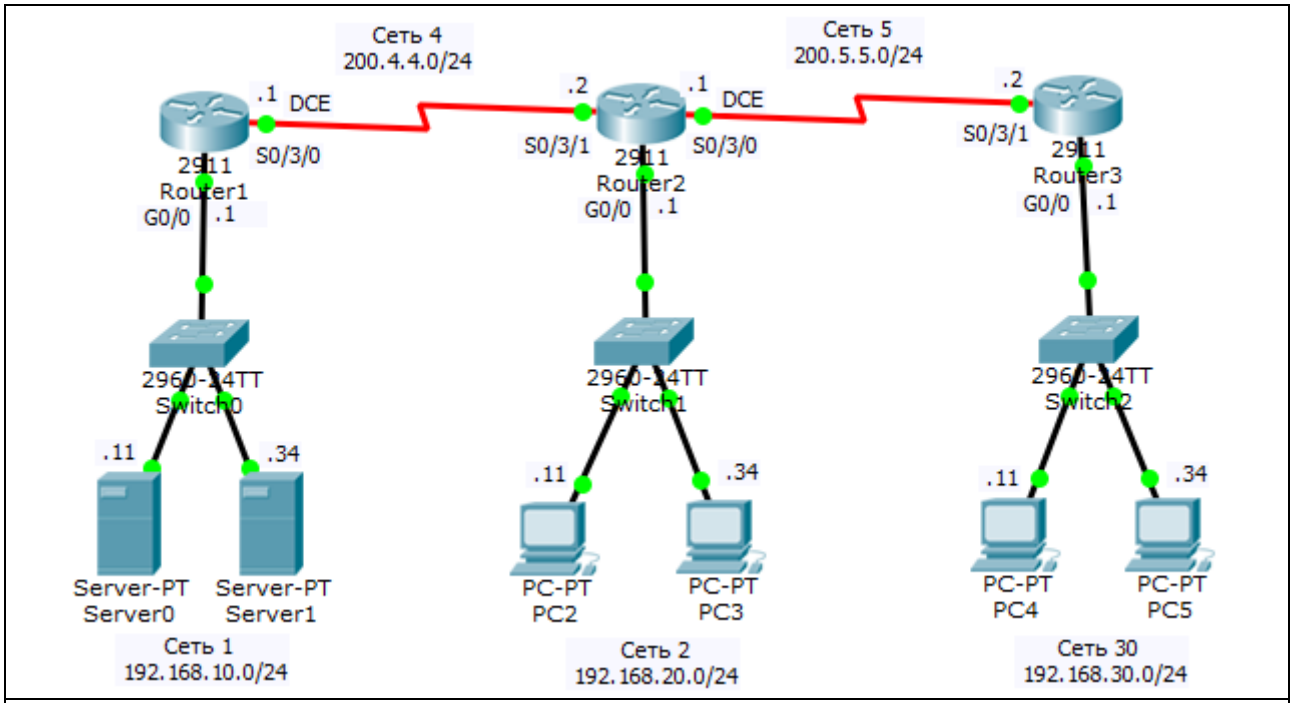


Рисунок 3.1 – Схема компьютерной сети с серверами

4. ПРОГРАММА ВЫПОЛНЕНИЯ РАБОТЫ

4.1. Изучить теоретический материал, относящийся к составлению и применению списков доступа (выполняется в процессе домашней подготовки).

4.2. Создать в рабочем окне Packet Tracer схему сети, изображенную на рисунке 3.1.

4.3. Произвести первоначальную настройку сетевого оборудования для обеспечения взаимной достижимости всех компьютеров этих сетей, используя статическую маршрутизацию. Проверить взаимную достижимость компьютеров.

4.4. Составить и настроить стандартный список контроля доступа таким образом, чтобы серверы Сети 1 были доступны только руководителям рабочих групп Сети 2 с адресом 192.168.20.11 сети 3 с адресом 192.168.30.11, а все остальные персональные компьютеры Сети 2 и Сети 3 не имели бы доступа к серверам. *Список* доступа следует установить на *интерфейс* G0/0 маршрутизатора Router1.

4.5. Продублировать схему сети (рисунок 3.1) и удалить списки доступа на маршрутизаторе. Конфигурацию серверов, компьютеров и маршрутизаторов оставить прежнюю.

4.6.Сконфигурировать оборудования таким образом, чтобы доступ к серверам имел только администратор.

4.7. Проверить путем пингования, что требования, изложенные в п.4.3 и 4.4 выполнены.

4.8. Переконфигурировать оборудования таким образом, чтобы пользователи рабочих станций PC0-PC2 имели доступ к файл-серверу и к HTTP (порт80) и FTP (порт21) серверам. При этом предусмотреть функционирование DNS (порт 53) сервера.

4.9. Сформулировать выводы по результатам исследований.

Примечание: проверить правильность конфигурации телекоммуникационного оборудования и обнаружить ошибки конфигурации можно путем использования приложения А.

5. СОДЕРЖАНИЕ ОТЧЕТА

Отчет о выполненной работе должен содержать:

5.1. Титульный лист.
5.2. Схему исследуемой сети и программу работы.
5.3. Скрипты настроек сетевого оборудования.
5.4. Скриншоты результатов исследования функционирования сети.
5.5. Выводы по результатам выполненной работы.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

6.1. Для чего предназначен сетевой экран и какие существуют виды защитных экранов?
6.2. Чем пакетный фильтр отличается от брандмауэра?
6.3. Что представляют собой списки контроля доступа?
6.4. Какие адреса являются критерием для разрешения/запрещения пакета?
6.5. С какой целью применяются ACL?
6.6. Как задать элемент ACL и что такое инверсная маска?
6.7. Как маршрутизатор обрабатывает элементы ACL?
6.8. Какой элемент всегда неявно присутствует в ACL?
6.9. Как ACL применить к интерфейсу и затем его отменить?
6.10. Чем отличается входной ACL от выходного?
6.11. Где в сети рекомендуется размещать ACL?
6.12. Какими тремя командами можно проверить содержимое ACL и привязку к интерфейсу.
6.13. Что фильтруют расширенные ACL?
6.14. Какую дополнительную функциональность имеют расширенные ACL по сравнению со стандартными?

6.15. Можно ли, используя расширенные ACL, наложить ограничения на трафик к определённой TCP/IP службе?
6.16. Опишите процедуру создания именованного ACL.
6.17. Как отредактировать конкретную строку в числовом ACL?
6.18. Как отредактировать конкретную строку в именованном ACL?
6.19. Чем отличается форматы команд для ввода элементов числового и именованного ACL?

Лабораторная работа 6
ИССЛЕДОВАНИЕ ПРИНЦИПОВ ОРГАНИЗАЦИИ VPN-СОЕДИНЕНИЯ И НАСТРОЙКИ GRE-ТУННЕЛЯ

1 Цель работы

Углубление теоретических знаний в области защиты данных в компьютерных сетях, изучение принципов организации VPN-соединения и исследование работы протокола туннелирования GRE в симуляторе компьютерных сетей Cisco Packet Tracer, приобретение практических навыков моделирования процессов защиты информации.

2 Краткие теоретические сведения

2.1. Принципы организации VPN

Виртуальные частные сети VPN (*Virtual Private Network*) – технология, позволяющая организовывать виртуальные сети поверх существующих реальных сетей. Другими словами, VPN — это служба, которая создает зашифрованное соединение клиента с VPN-сервером через обычное интернет-соединение путем создания защищенного «туннеля».

Туннель представляет собой канал между двумя коммуникационными устройствами, по которому передаётся данные, причем специфика построения канала не оказывает влияние на передаваемые данные. В процессе туннелирования создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции с использованием различных протоколов. При туннелировании данные упаковываются вместе со служебными заголовками в новый пакет для обеспечения конфиденциальности и целостности всей передаваемой информации.

Существует два типа VPN туннелей:

1) Remote access VPN – туннель организуется между приложением на компьютере клиента и каким-либо устройством, которое выступает в качестве сервера (рисунок 2.1).

Этот туннель используется для подключения, в частности, удалённых работников к корпоративной сети предприятия по защищённому каналу. В этом случае работник может находиться в любом месте, где есть интернет, а программное обеспечение на его компьютере построит туннель до маршрутизатора компании, по которому будут передаваться данные пользователя.

2) Site-to-site VPN – представляет собой два устройства (например, маршрутизаторы), между которыми создан постоянный туннель. В этом случае пользователи находятся за устройствами в своих локальный сетях и на их компьютерах не требуется установки какого-либо специального программного обеспечения (рисунок 2.2).

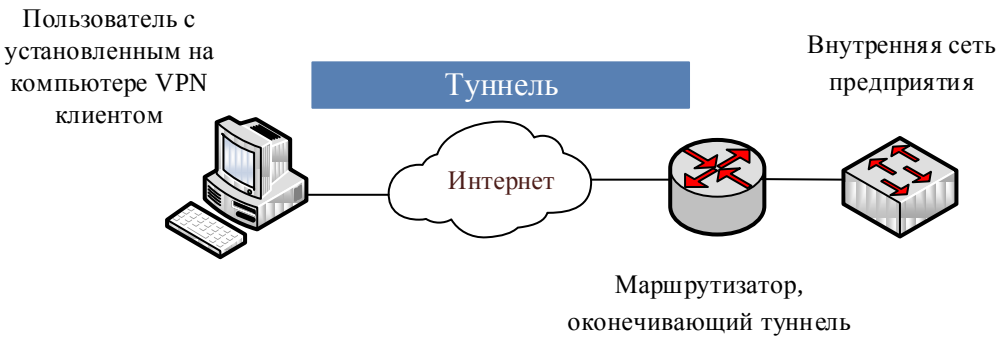


Рисунок 2.1 – Схема туннелирования Remote access VPN

Такой тип туннеля используется в случае необходимости стационарного соединения между двумя удалёнными филиалами, или филиалом и центральным офисом. В этом случае сотрудники без специального ПО работают в локальной сети офиса, а на границе этой сети стоит маршрутизатор, который незаметно для пользователя создаёт туннель с удалённым маршрутизатором и передаёт на него полезный трафик.

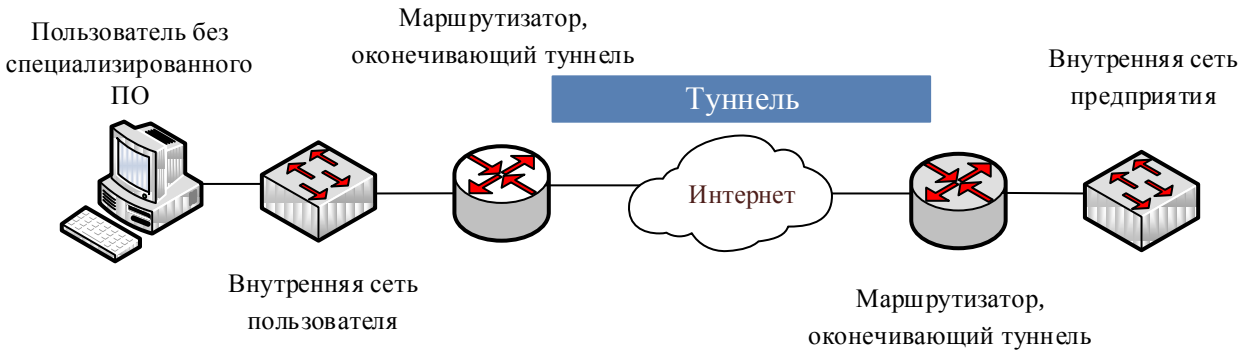


Рисунок 2.2 – Схема туннелирования Site-to-site VPN

В туннеле обычно используется три прослойки протоколов:

1) **протокол доставки** или транспортирующий протокол (например, IP). Это протокол, на котором построена существующая реальная сеть, то есть, он изначально не связан с VPN-ом, но используется для транспортировки инкапсулированных пакетов, содержащих внутри себя зашифрованную, или открытую информацию, относящуюся ко внутренней сети туннеля;

2) **протокол инкапсуляции**, несущий протокол (например, GRE - Generic Routing Encapsulation) – используется как прослойка между транспортирующим протоколом и внутренним транспортируемым протоколом;

3) **инкапсулированный протокол** (например, IP, IPX, IPSec) – это собственно пакеты внутритуннельной сети. Пользователь, подключенный к VPN-у, отправляет пакеты, которые на входе в туннель становятся инкапсулированными, например, в GRE, который, в свою очередь, инкапсулируется в транспортирующий протокол.

Таким образом, общий порядок инкапсуляции, в случае использования site-to-site VPN следующий: пользователь отправляет обычный IP пакет. Он до-

ходит до устройства, на котором поднят туннель, устройство вставляет этот полезный пакет в поле «data» протокола инкапсуляции (GRE). Пакет GRE в свою очередь инкапсулируется в поле «data» протокола доставки (обычно IP). После чего из устройства выходит с виду обычный, например, IP пакет, в котором, в поле с полезными данными содержится GRE-пакет, в котором, в свою очередь, содержится другой внутренний IP пакет (рисунок 2.3). Это позволяет использовать независимую адресацию внутри туннеля и снаружи туннеля.

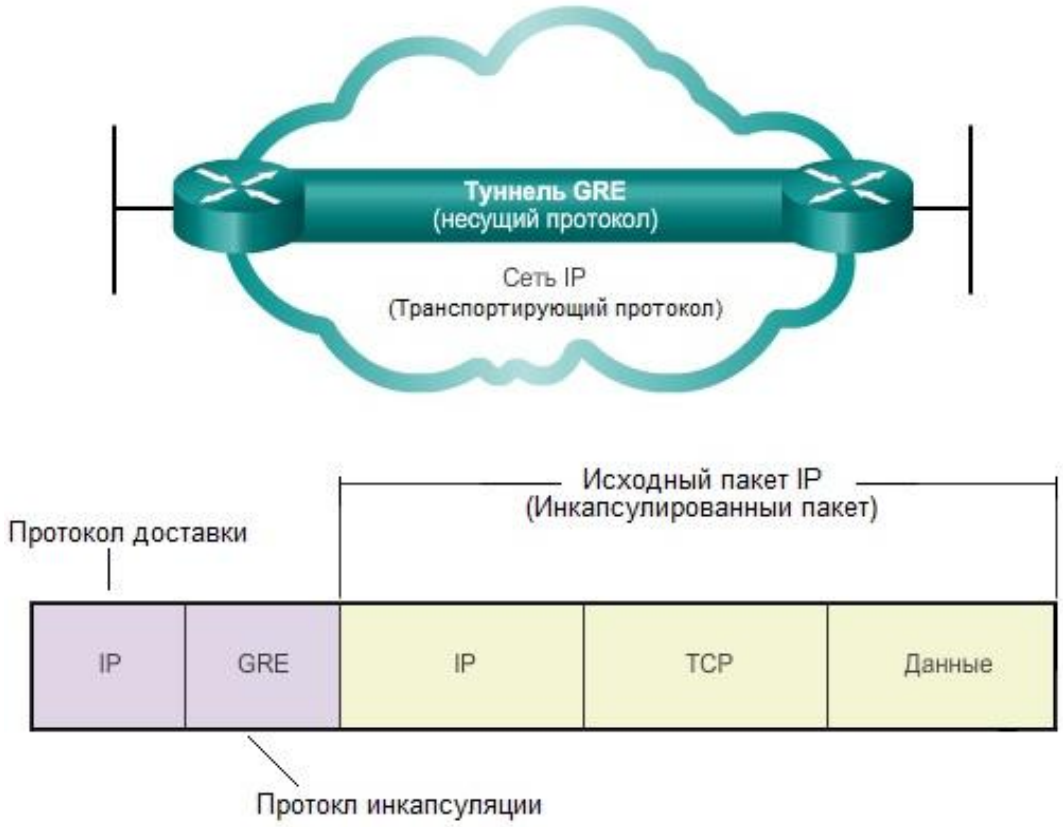


Рисунок 2.3 – Универсальная инкапсуляция при маршрутизации

Когда устройство назначения получает такой пакет, оно разворачивает его, извлекая из него GRE, а потом и внутренний IP пакет. После чего внутренний пакет направляется получателю. В данной ситуации отправитель и получатель ничего не знают о наличии туннеля, и работают так, как будто бы его нет. При этом в транспортирующем протоколе используется одна адресация (например, публичные IP адреса), а в транспортируемом протоколе могут использоваться приватные адреса, что не мешает ему транспортироваться через интернет (так как маршрутизация осуществляется для внешнего, транспортирующего пакета).

2.2 Особенности протокола универсальной инкапсуляции GRE

Протокол универсальной инкапсуляции при маршрутизации GRE (*Generic Routing Encapsulation*) является базовым, незащищённым протоколом создания туннелей для site-to-site VPN. Это протокол туннелирования пакетов, разработанный компанией Cisco. Основная его задача – создавать поверх обычного заголовка сетевого уровня новый IP-заголовок, который будет содержать в себе измененный IP-адрес (рисунок 2.3). Протокол GRE предназначен для управления процессом передачи многопротокольного и группового IP-трафика между двумя и более площадками, между которыми связь может обеспечиваться только по IP. Он может инкапсулировать пакеты протоколов различного типа в IP-туннеле.

Интерфейс туннеля поддерживает заголовки для следующих протоколов:

- инкапсулированный протокол (или «протокол-пассажир»), например IPv4, IPv6, AppleTalk, DECnet или IPX;
- протокол инкапсуляции (или несущий протокол), в данном случае GPE;
- протокол доставки (транспортирующий протокол), например IP, который передаёт данные протокола инкапсуляции.

2.3 Характеристики GRE

Протокол туннелирования GRE позволяет инкапсулировать пакеты протоколов различного типа внутри IP-туннелей и создавать виртуальный канал «точка-точка» между маршрутизаторами Cisco поверх IP-сети. Туннелирование IP с помощью GRE позволять расширять сеть с использованием однопротокольной магистральной среды. Это обеспечивается путем соединения между собой различных многопротокольных подсетей в однопротокольной магистральной среде. Структура заголовков протокола GRE показана на рисунке 2.4.

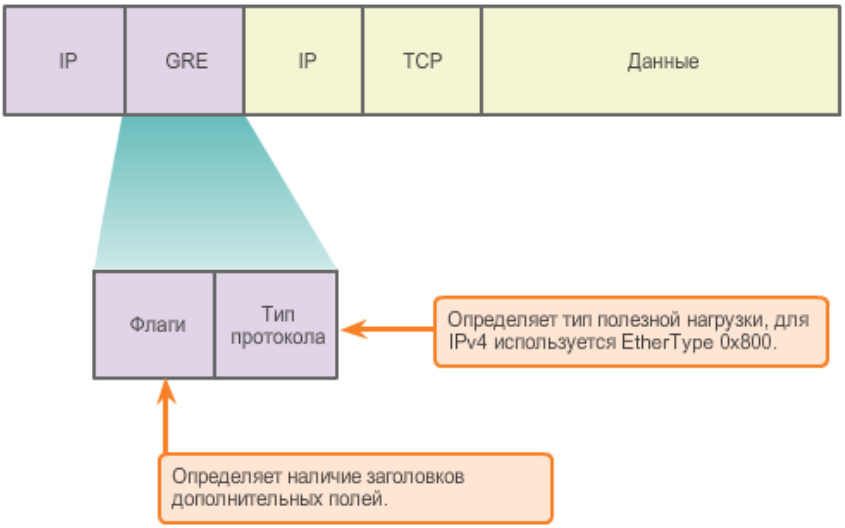


Рисунок 2.4 – Структура заголовков протокола GPE

К особенностям протокола GRE относится:

- протокол GRE относится к протоколам сетевого уровня и не использует порты;

- во внешнем заголовке IP в поле протокола доставки используется значение 47, указывающее на то, что за ним будет следовать заголовок GRE;

- протоколом не предусмотрено отслеживание состояния соединения и по умолчанию в нем не содержится механизмов управления потоком;

- для защиты полезной нагрузки в протоколе GRE отсутствуют какие-либо криптостойкие механизмы безопасности;

- заголовок GRE вместе с заголовком IP туннелированного сообщения создаёт, по крайней мере, 24 байта дополнительной служебной информации для туннелированных пакетов.

2.4 Настройка туннеля GRE

GRE используется для создания туннеля VPN между двумя узлами, положение которого показано на рисунке 2.5. Для реализации туннеля GRE сетевой администратор должен сначала узнать IP-адреса начальной и конечной точек туннеля. После этого для настройки туннеля GRE следует выполнить следующую процедуру:

1) создать интерфейс туннеля с помощью команды **interface tunnel number**;
2) указать IP-адрес источника туннеля;
3) указать IP-адрес назначения туннеля;
4) указать IP-адрес для интерфейса туннеля;
5) указать на интерфейсе туннеля в качестве используемого режима режим GRE (режим GRE является режимом по умолчанию для интерфейса туннеля в программном обеспечении Cisco IOS).

Рисунок 2.5 – Адресация интерфейсов туннеля GPE

На рисунке 2.6 приведен пример базовой настройки туннеля GRE для маршрутизаторов R1 и R2.

Настройка R1:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Настройка R2:

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Рисунок 2.6 – Базовая настройка туннеля GPE для маршрутизаторов

Для минимальной настройки требуется указать адреса источника и назначения туннеля. Подсеть IP также необходимо настроить таким образом, чтобы обеспечить связь по IP через канал туннеля. Для обоих интерфейсов туннеля в качестве источника туннеля указан локальный интерфейс serial S0/0/0, а в качестве назначения туннеля – интерфейс serial S0/0/0 маршрутизатора, с которым устанавливается туннель. IP-адрес назначается интерфейсам туннеля на обоих маршрутизаторах. Настройка протокола OSPF также позволяет обмениваться маршрутами через туннель GRE.

Описания отдельных команд для туннеля GRE приведены в таблице 1.

Таблица 1 – Команды для настройки туннеля GRE

Команда	Описание
tunnel mode gre ip	Указывает, что режимом работы интерфейса туннеля является GRE по IP
tunnel source *interface*	Указывает номер интерфейса источника туннеля
tunnel destination *ip_address*	Указывает адрес назначения туннеля
ip address *ip_address mask*	Указывает IP-адрес интерфейса туннеля

При настройке туннелей GRE может оказаться трудно запомнить, какие сети IP связаны с физическими интерфейсами, а какие – с интерфейсами туннеля. Следует помнить, что перед созданием туннеля GRE физические интерфейсы уже настроены. Команды **tunnel source** и **tunnel destination** указывают на IP-адреса предварительно настроенных физических интерфейсов. Команды **ip**

address на интерфейсах туннеля определяют сеть IP, созданную специально для туннеля GRE.

2.5 Проверка туннеля GRE

Для наблюдения и устранения неполадок в туннелях GRE можно использовать несколько команд. При проверке работоспособности интерфейса туннеля применяется команда **show ip interface brief**, а для контроля состояния туннеля GRE ─ команда **show interface tunnel**. Протокол канального уровня в интерфейсе туннеля GRE активен до тех пор, пока существует маршрут до адреса назначения туннеля. Перед реализацией туннеля GRE между IP-адресами физических интерфейсов на противоположных сторонах потенциального туннеля GRE должна уже существовать связь по IP. Транспортный протокол туннелирования отображается в выходных данных.

Если настроен протокол OSPF на обмен маршрутами по туннелю GRE, то с помощью команды **show ip ospf neighbor** можно проверить, что через интерфейс туннеля установлены отношения смежности OSPF.

Преимущества протокола GRE:

- может быть использован для туннелирования трафика, отличного от IP, по сети IP, позволяя расширить сеть путем подключения различных многопротокольных подсетей через однопротокольную магистральную среду;
- поддерживает процесс туннелирования групповой рассылки IP (IP multicast), т.е. в туннеле можно использовать протоколы маршрутизации, что позволяет обеспечивать динамический обмен данными о маршрутизации в виртуальной сети;
- на практике часто создаются туннели GRE «IPv6 по IPv4», где IPv6 является инкапсулированным протоколом, а IPv4 – транспортирующим протоколом.

Недостатки протокола GRE: не обеспечивает шифрования и таким образом не дает никаких гарантий безопасности при передаче данных. Поэтому данные, отправляемые по туннелю GRE, не защищены. Если требуется безопасная передача данных, то необходимо настроить сети VPN с IPsec или с SSL.

3 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

В качестве лабораторной установки используется персональный компьютер с установленной программной системой моделирования компьютерных сетей Packet Tracer версии 6 и выше. Работа с системой Packet Tracer детально описана в методических указаниях к лабораторным работам №1.

4 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНОЙ РАБОТЫ

Как отмечалось выше, протокол GRE не обеспечивает никакой безопасности передаваемых данных – это site-to-site VPN-туннель в чистом виде. Используется обычно такой туннель, когда есть специфичные задачи, связанные с маршрутизацией и нет требований к безопасности. Кроме того, чистый GRE туннель не нагружает оборудование.

Протокол GRE инкапсулируется напрямую в IP, минуя TCP или UDP, в IP пакете есть специальное поле «Protocol type», в котором содержится число, обозначающее протокол, инкапсулированный в данный IP пакет, для GRE protocol type равен 47. В связи с этим, если в сети есть GRE туннели, то стоит внимательно относиться к написанию расширенных списков контроля доступа (ACL), так как permit tcp any any и permit udp any any приведут к запрету на GRE из-за того, что он инкапсулируется напрямую в пакет, надо писать либо permit ip any any либо permit gre any any.

Как видно из рисунка 2.3, исходный пакет IP инкапсулируется в GRE, который затем инкапсулируется во внешний IP (протокол доставки). При этом заголовок GRE и заголовок внешнего IP пакета добавляют 24 байта, соответственно, уменьшая размер пакета на эту величину.

В примере, приведенном ниже, будем рассматривать GRE в IPv4, но GRE может успешно работать и с другими инкапсулируемыми и транспортными протоколами, например, IPv6.

Рассмотрим топологию, представленную на рисунке 4.1. Пусть имеется две частные локальные сети: LAN1 за маршрутизатором R1 с адресацией 192.168.0.0/24 и LAN2 – за маршрутизатором R3, с адресацией 192.168.1.0/24. В каждой сети есть по одному клиентскому компьютеру PC1 и PC2. Между маршрутизаторами имеются две публичные сети 1.0.0.0/8 и 2.0.0.0/8, а также маршрутизатор R2, который моделируют сеть Интернет. В сетях используется динамическая маршрутизация.

Выполним трассировку с компьютера PC1 до компьютера PC2:

```
PC1>tracert 192.168.1.2
Tracing route to 192.168.1.2 over a maximum of 30 hops:
  1   0 ms     0 ms     0 ms     192.168.0.1
  2   0 ms     0 ms     0 ms     1.1.1.2
  3   0 ms     0 ms     0 ms     2.2.2.2
  4   1 ms     0 ms     0 ms     192.168.1.2
```

Как видно, пакет проходит через все маршрутизаторы последовательно, вплоть до компьютера адресата. Теперь создадим GRE туннель между R1 и R3 со внутренней адресацией 10.10.10.0/24.

Создадим интерфейс Tunnel0, в нём укажем с помощью ip address внутреннюю адресацию туннеля – тот есть это адреса инкапсулированного IP, а с помощью команд tunnel source и tunnel destination указываются параметры

транспортного протокола IP (внешнего). Появилась новая сеть, которая виртуально соединяет напрямую два маршрутизатора R1 и R3 (без лишнего хопа на R2).

```
R1(config)#interface tunnel 0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 10.10.10.1 255.255.255.0
R1(config-if)#tunnel source FastEthernet0/1
R1(config-if)#tunnel destination 2.2.2.2
```

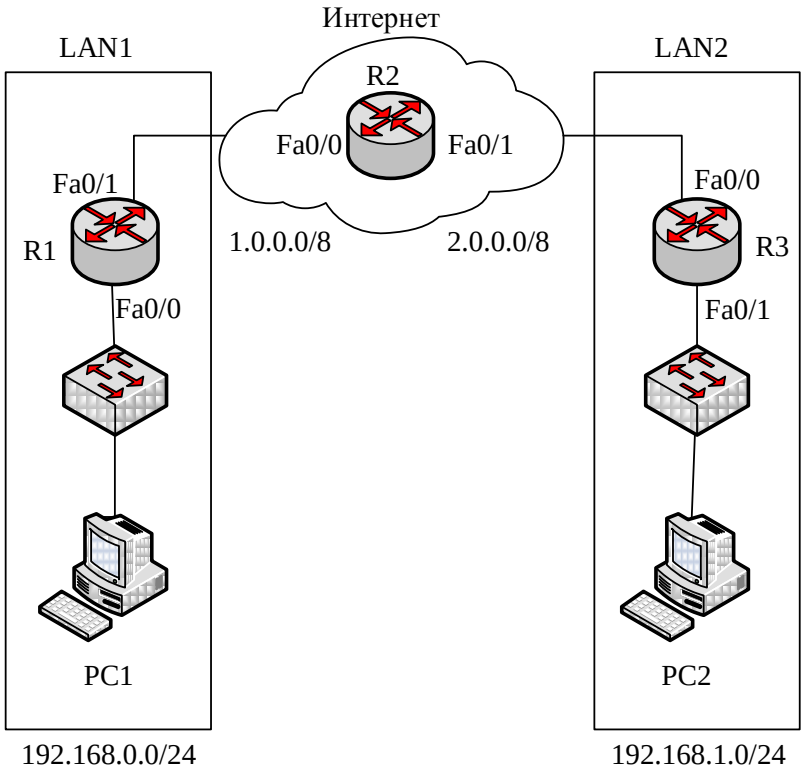


Рисунок 4.1 – Топология сети для изучения принципов работы протокола GRE

Настроим вторую сторону туннеля – на R3. Для примера создадим интерфейс Tunnel1:

```
R3(config)#interface tunnel 1
R3(config-if)#tunnel mode gre ip
R3(config-if)#ip address 10.10.10.2 255.255.255.0
R3(config-if)#tunnel source FastEthernet0/0
R3(config-if)#tunnel destination 1.1.1.1
```

Теперь выполним трассировку с маршрутизатора R1 противоположного конца туннеля – на R3:

```
R1#traceroute 10.10.10.2
Type escape sequence to abort.
Tracing the route to 10.10.10.2
  1   10.10.10.2      1 msec    0 msec    0 msec
```

Как видно, трассировка проходит внутри туннеля и нет лишнего хопа в виде R2. Посмотрим таблицу маршрутизации на R1:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    1.0.0.0/8 is directly connected, FastEthernet0/1
R    2.0.0.0/8 [120/1] via 1.1.1.2, 00:00:12, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/2] via 1.1.1.2, 00:00:12, FastEthernet0/1
```

Видно, что новая сеть отображается, как непосредственно подключенная к интерфейсу Tunnel 0. Если сейчас попробовать сделать трассировку с компьютера 1 до компьютера 2, то она не пойдёт по туннелю. Это связано с тем, что на маршрутизаторе R1 нет соответствующего маршрута. Просматривая свою таблицу маршрутизации, R1 отправит пакеты на PC2 по тому же маршруту, как и раньше – в обход туннеля. Чтобы исправить ситуацию необходимо прописать с двух сторон на R1 и R3 статические маршруты, в которых явно указываются, что в сети 192.168.0.0 и 192.168.1.0 надо доставлять трафик через туннель.

На R1:

```
R1(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.2
```

На R3:

```
R3(config)#ip route 192.168.0.0 255.255.255.0 10.10.10.
```

Теперь трафик пойдёт через GRE туннель. Проверим это, выполнив трассировку с PC1 до PC2:

```
tracert 192.168.1.2
Tracing route to 192.168.1.2 over a maximum of 30 hops:
  1   0 ms     0 ms     0 ms     192.168.0.1
  2   0 ms     0 ms     0 ms     10.10.10.2
  3   1 ms     0 ms     1 ms     192.168.1.2
Trace complete.
```

Как видно, из результатов трассировки, теперь на пути всего два хопа: 192.168.0.1 – R1, шлюз PC1, который заворачивает трафик в туннель. Далее,

транспортный (внешний) IP пакет с GRE внутри проходит на R2, затем на R3 и только тут из пакета декапсулируется внутренний IP – это и есть второй хоп – 10.10.10.2, затем пакет по локальной сети идёт адресату – на 192.168.1.2, если добавить в интернете ещё несколько маршрутизаторов, то трассировка не изменится, в ней по-прежнему будет два хопа до адресата.

5 ПРОГРАММА ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

1. Повторить теоретический материал, касающийся конфигурации оборудования при создании локальных сетей.

2. В Cisco Packet Tracer построить сеть согласно топологии, приведенной на рисунке 4.1.

3. Выполнить адресацию узлов в сети согласно данным, приведенных в таблице 5.1.

Таблица 5.1 – Таблица адресации

Устройство/подсеть	IP-адрес сети	Маска подсети	Примечание
LAN1	192.168.N.0	255.255.255.0	IP-адреса локальных сетей
LAN2	192.168.(N+1).0	255.255.255.0	
R1	192.168.N.0	255.255.255.0	IP-адреса сетей, подключенных к маршрутизаторам
	(N+1).0.0.0	255.0.0.0	
R2	(N+1).0.0.0	255.0.0.0	
	(N+2).0.0.0	255.0.0.0	
R3	192.168.(N+1).0	255.255.255.0	
	(N+2).0.0.0	255.0.0.0	
Tunnel	N.N.N.0	255.255.255.0	IP-адрес сети туннеля
PC1	192.168.N.2	255.255.255.0	
PC2	192.168.(N+1).2	255.255.255.0	

N – номер варианта (определяется по последней цифре зачетной книжки)

4. Настроить динамическую маршрутизацию в построенной сети по протоколу OSPF или RIP. Проверить, что компьютеры PC1 и PC2 пингуются.

5. Выполнить трассировку с компьютера PC1 до компьютера PC2.

6. Создать GRE туннель между R1 и R3 со внутренней адресацией N.N.N.0/24 (N – номер варианта).

7. Настроить статическую маршрутизацию, чтобы трафик между маршрутизаторами R1 и R3 шел по туннелю.

8. Выполнить трассировку с маршрутизатора R1 противоположного конца туннеля – на R3.

9. Снова выполнить трассировку с компьютера PC1 до компьютера PC2.

10. Исследовать результат действия команд:

- show running-config;
- show ip interface brief;
- show interface tunnel;
- show ip ospf/rip neighbor.

6 СОДЕРЖАНИЕ ОТЧЕТА

6.1. Титульный лист.
6.2. Цель и программа лабораторной работы.
6.3. Исходные данные в соответствии с индивидуальным вариантом.
6.4. Скриншот с топологией локальной сети.
6.5. Команды и скриншоты этапов настройки локальной сети.
6.6. Скриншоты результатов тестирования сети.
6.7. Выводы по результатам работы

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

7.1. Чем отличаются частные сети от публичных?
7.2. Какие уязвимости характерны для незащищенных сетей?
7.3. Каким образом злоумышленник может получить доступ к сети?
7.4. Какие действия выполняются при конфигурации локальной сети?
7.5. Чем маршрутизатор отличается от коммутатора третьего уровня?
7.6. Что означают записи Fa1/2, S0/0/0?
7.7. Что называется туннелированием в сети и зачем оно выполняется?
7.8. Какие существуют типы VPN туннелей и в каких случаях они применяются?
7.9. Какие три прослойки используются в VPN туннеле и какие процедуры они регламентируют?
7.10. Какие необходимо выполнить настройки для создания туннеля GRE?
7.11. Какие дополнительные поля добавляются к пакету при GRE туннелировании?
7.12. Каким образом осуществляется защита при GRE туннелировании?
7.13. Как можно осуществить проверку работоспособности интерфейса туннеля GRE?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 08.04.2023).
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 08.04.2023).
3. Аппаратные и программные средства защиты информации : учебное пособие / Душкин А. В., Кольцов А., Кравченко А. – Воронеж : Научная книга, 2016. - 232 с. - URL: https://znanium.com/catalog/product/923168 (дата обращения: 08.04.2023).– Режим доступа: по подписке. — ISBN 978-5-4446-0746-6. - Текст : электронный.
4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Юрайт, 2023. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138 (дата обращения: 08.04.2023).
5. Чернега, В. С. Компьютерные сети : учебное пособие для студентов направления "Компьютерные науки" вузов / В. С. Чернега, Б. Платтнер. - Севастополь : СевНТУ, 2006. - 499 с. : ил ; 21 см. - Библиография: с. 489-491. - Предметный указатель: с. 492-499. - ISBN 966-7473-98-8 (в пер.). - Текст : непосредственный.

Приложение 1

Топология исследуемой сети

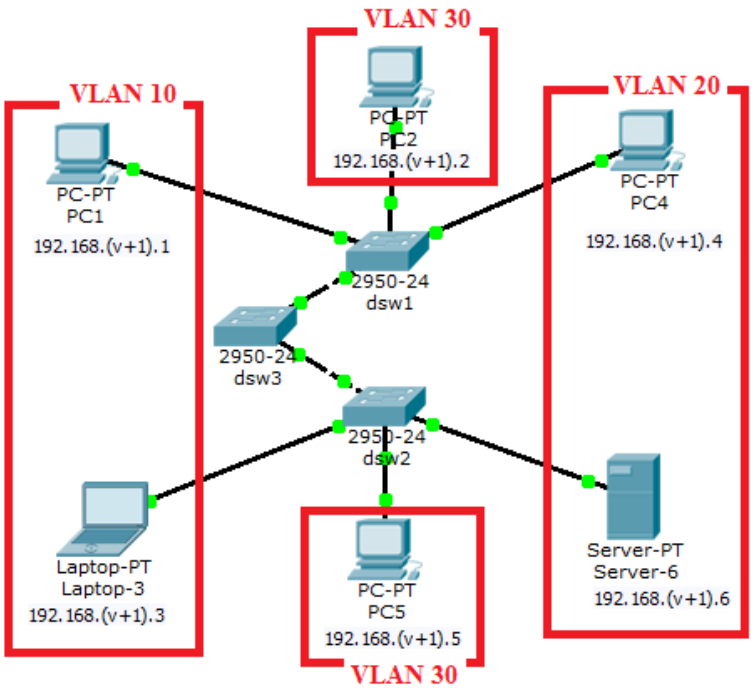


Рисунок П1 – Топология исследуемой локальной компьютерной сети

Таблица вариантов исследуемой локальной компьютерной сети

Вариант	Количество				
	PC	серверов	ноутбуков	коммутаторов	VLAN
1	2	2	2	3	2
2	4	3	2	3	3
3	6	3	3	3	3
4	4	2	2	3	2
5	5	3	4	3	3
6	5	4	4	3	4
7	6	3	3	3	3
8	4	3	3	3	3
9	3	2	3	3	2
10	4	4	2	3	4

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Методические указания

Составитель: **Чернега** Виктор Степанович

В авторской редакции

Изд. № 136/2023. Объем 4,75 п.л. Усл. печ. л. 4,42. Уч.-изд. л. 4,66.
РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»