МВД России
Санкт-Петербургский университет

А. И. Локнов, И. Н. Васильева

СИСТЕМЫ И СЕТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Учебно-методическое пособие

Санкт-Петербург
2023

План-график 2023, поз. 64

УДК 004.7
ББК 32.88
Л73

Л73 Системы и сети передачи информации: учебно-методическое пособие / Локнов А. И., Васильева И. Н. — Санкт-Петербург: СПбУ МВД России, 2023. — 72 с.

Авторский коллектив:
Локнов А. И. — введ., т. 1–13, 16–17, закл.; *Васильева И. Н.* — т. 14–15

ISBN 978-5-91837-674-4

Учебно-методическое пособие подготовлено в соответствии с программой учебной дисциплины «Системы и сети передачи информации». В учебно-методическом пособии содержатся методические рекомендации по подготовке к семинарским и практическим занятиям. Практические задания позволяют развивать у обучающихся профессиональные компетенции, связанные с умением работать с интерактивными модулями с целью систематизации теоретического материала, с программными средствами тестирования параметров соединения в компьютерных сетях, эмуляторами для моделирования сети.

Предназначено для научно-педагогических работников, курсантов и слушателей образовательных организаций системы МВД России, обучающихся по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

УДК 004.7
ББК 32.88

Рецензенты:
Еськов А. В., доктор технических наук, профессор
(Краснодарский университет МВД России);
Симаков А. А., кандидат технических наук, доцент
(Омская академия МВД России)

ISBN 978-5-91837-674-4

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Одной из основных целей совершенствования профессиональной подготовки обучающихся по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере является приобретение ими компетенций и опыта создания и использования средств сетевых технологий. В результате выполнения практических заданий курсанты систематизируют теоретический материал через выполнение интерактивных упражнений, узнают об утилитах диагностики TCP/IP, об эмуляторах, о современных тенденциях развития сетевых технологий, подготовятся к тестированию по учебной дисциплине.

Настоящее учебно-методическое пособие разработано с учетом федеральных государственных образовательных стандартов; его структура соответствует структуре дисциплины «Системы и сети передачи информации» для специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере. Учебно-методическое пособие также можно использовать в рамках преподавания дисциплин «Средства и системы обработки информации», «Информатика и информационные технологии в правоохранительной деятельности», «Основы кибербезопасности», «Системы и сети передачи данных».

Использование данного учебного пособия в образовательном процессе направлено на развитие у обучающихся профессиональных компетенций, связанных с умением виртуально моделировать сети, осуществлять самоконтроль и самооценку собственных знаний по компьютерным сетям. Курсанты овладевают компетенциями в области использования интерактивных и виртуальных сред (NetEmul, Cisco Packet Tracer, Oracle VirtualBox).

Раздел I. ОСНОВЫ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Тема 1. Общие принципы построения вычислительных сетей (лекция)

Цели занятия:

1. Получение обучающимися знаний по основам сетей передачи данных.
2. Расширение научных представлений обучающихся о системах и сетях передачи информации.
3. Изучение программных средств для создания сети.
4. Развитие мышления и творческой активности обучающихся.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. История развития вычислительных сетей.
2. Общие принципы построения вычислительных сетей.
3. Классификация компьютерных сетей.

Изучение систем и сетей передачи данных, как и любой процесс познания, развивается по спирали. Не представляется возможным сразу осознать сложные процессы, происходящие в компьютерных сетях. Правильным подходом будет являться первоначальное изучение общих принципов с их последующим детальным рассмотрением в конкретных методах, технологиях и конструкциях.

Чтобы лучше понять эволюцию сетей передачи данных, необходимо проанализировать лекционный материал об истории развития компьютерных сетей. Это поможет понять основную сущность достижений в данной отрасли науки и техники.

Для уяснения существующих тенденций и оценки перспективности направлений развития нужно подвергнуть анализу материал о классификации и основных архитектурах вычислительных сетей. Особенно следует уделить внимание различию глобальных и локальных сетей, их характеристикам, территории распространения, расстоянию между узлами, средствам телекоммуникационных систем, скорости передачи данных.

Практический материал для занятия

Задание 1. Определите, какие из представленных на рис. 1 типов топологии сетей относятся к неполносвязной топологии.

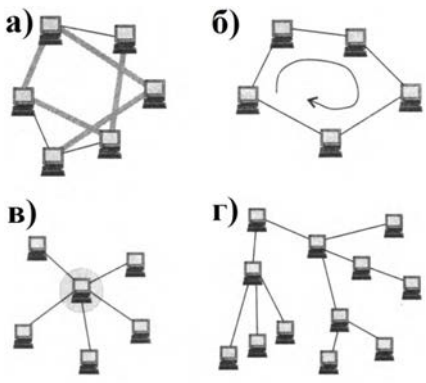


Рис. 1.1. Типы топологии сетей

Задание 2. Дайте характеристику информационно-телекоммуникационной сети «Интернет» в соответствии с общепринятыми критериями классификации сетей передачи данных.

Задание 3. Какой из нижеперечисленных терминов наиболее полно отражает определение сетевой технологии:

а) приложение, состоящее из нескольких частей, каждая из которых может выполняться на отдельном компьютере сети;

б) сеть передачи данных, в одном или нескольких узлах которой размещено периферийное оборудование;

в) согласованный набор программных и аппаратных средств, а также механизмов передачи данных по линиям связи, достаточный для построения вычислительной сети.

Вопросы для самоконтроля:

1. Назовите основные предпосылки создания вычислительных сетей.
2. Охарактеризуйте сущность локальных и глобальных вычислительных сетей.
3. Назовите подходы к структуризации вычислительных сетей.
4. В чем сущность принципа соответствия логической и физической структур вычислительных сетей?

Тема 2. Коммуникация пакетов и каналов

Практическое занятие: Эмулятор NetEmul. Ознакомление с интерфейсом программы NetEmul. Соединение ЭВМ в сеть

Цели занятия:

1. Закрепление знаний обучающихся по коммуникации пакетов и каналов.
2. Расширение научных представлений обучающихся о коммуникации пакетов и каналов.
3. Изучение и практическая работа с программными средствами для создания сети.
4. Развитие мышления и творческой активности обучающихся.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Изучение эмулятора NetEmul для исследования работы компьютерных сетей.
2. Выполнение практического задания по ознакомлению с интерфейсом программы NetEmul. Соединение ЭВМ в сеть.

Изучение эмулятора NetEmul для исследования работы компьютерных сетей

Для проведения практического занятия выбрано программное обеспечение NetEmul[1]. Данная программа создана для визуализации работы компьютерных

[1] NetEmul. Сайт программы для визуализации возникающих в сети процессов, связанных с передачей служебной и пользовательской информации. URL: http://netemul.sourceforge.net/ruindex.html (дата обращения: 11.02.2023).

сетей и облегчения понимания происходящих в ней процессов. Кроме обучения, программа открывает широкие возможности для экспериментов и их наглядного отображения[2]. Программное обеспечение предназначено для обучающихся, изучающих компьютерные сети, в качестве наглядного пособия для получения навыков работы в данной области. Также программу могут использовать преподаватели для проверки знаний обучающихся. Использование NetEmul предполагает наличие начальных знаний компьютерных сетей и принципов их работы. Программа отвечает основному требованию для проведения практических занятий — позволяет моделировать компьютерные сети. Помимо этого, она обладает рядом преимуществ, основные из которых — визуализация работы компьютерных сетей; точная и детальная настройка каждого компонента сети; программа свободно распространяется и является бесплатной.

Интерфейс программы NetEmul

Для начала необходимо установить программу, запустить и русифицировать её командой *Сервис–Настройки (Setting)*[3], как показано на рис. 2.1.

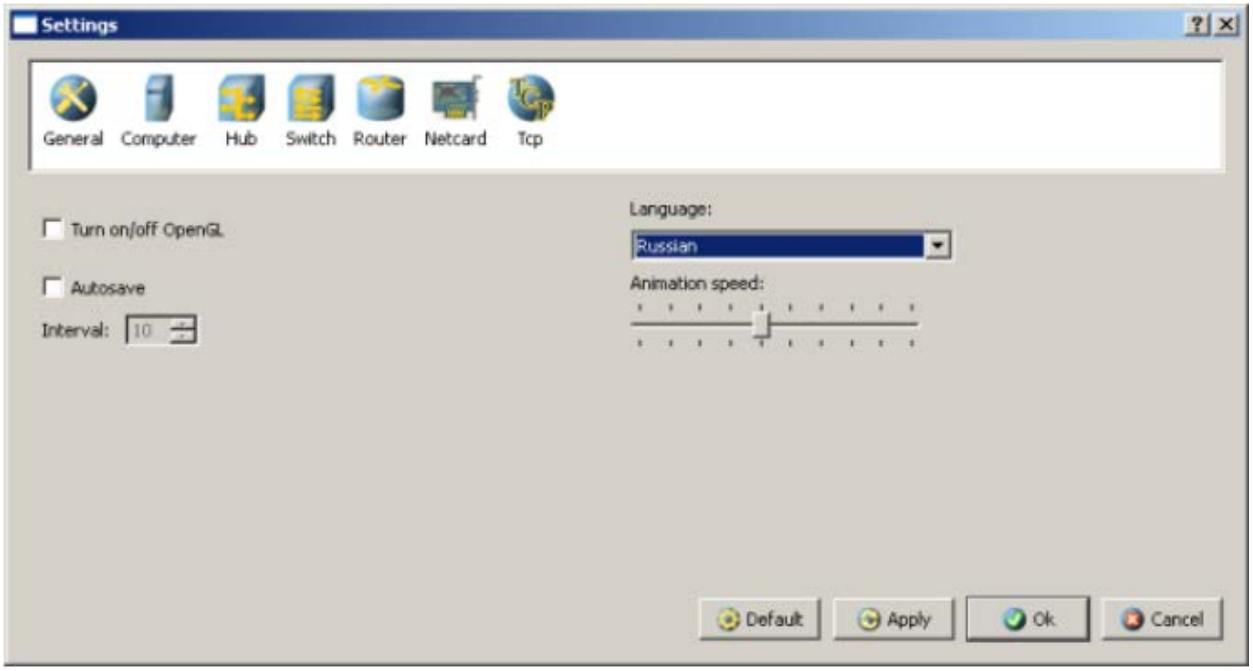


Рис. 2.1. Русификация интерфейса программы

В главном окне программы все элементы размещаются на рабочей области (на *Сцене*). На всей свободной области сцены, размеченной сеткой, можно ставить устройства, при этом они не должны пересекаться.

На *Панели устройств* размещены все необходимые для построения сети инструменты, а также кнопка отправки сообщений и *Запустить/Остановить.* На *Панели параметров* указаны свойства объектов. Для выделенного объекта появляются только те свойства, которые характерны для него (рис. 2.2).

---

[2] Компьютерные сети : учебное пособие. В 2 ч. / Н. П. Табачук; [науч. ред. В. А. Казинец]. Ч. 1. — Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2019. — 127 с.

[3] Национальный Открытый Университет «ИНТУИТ». Официальный сайт. URL: https://intuit.ru/studies/courses/3688/930/lecture/20109 (дата обращения: 11.02.2023).

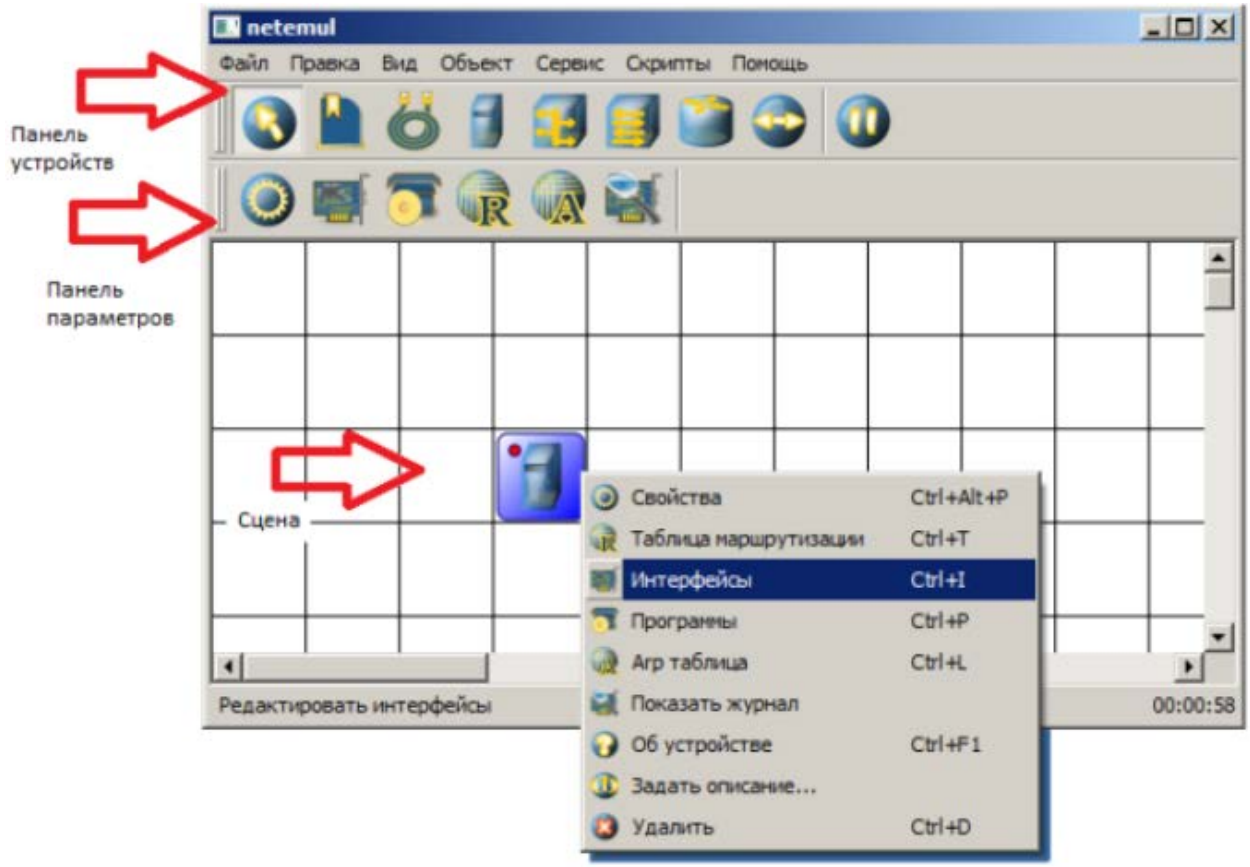


Рис. 2.2. Интерфейс программы Netemul

На рис. 2.3 изображен интерфейс программы.

Интерфейс состоит из:

— главного меню программы;

— панели устройств;

— панели параметров;

— сцены — рабочей области программы.

Главное меню программы NetEmul служит для настройки работы самой программы. Главное меню состоит из пунктов: *Файл, Правка, Вид, Объект, Сервис, Скрипты, Помощь.*

С помощью пункта *Файл* можно создать новый проект, сохранить или загрузить его, а также запустить предпросмотр получившейся модели сети и распечатать ее.

Пункт *Правка* служит для отмены или возврата действия пользователя.

Пункт *Вид* используется для включения или отключения панелей программы.

Пункт *Объект* полностью копирует функции контекстного меню, которое вызывается по нажатию правой кнопки мыши. Важно отметить, что данный пункт становится активным лишь после того, как будет выделен какой-либо из объектов на сцене.

Пункт *Сервис* позволяет просмотреть общую статистику для всей сети, в которой указывается количество каждого из устройств и общий трафик.

Пункт *Помощь* содержит сведения об авторах и краткую справку по использованию программы NetEmul.

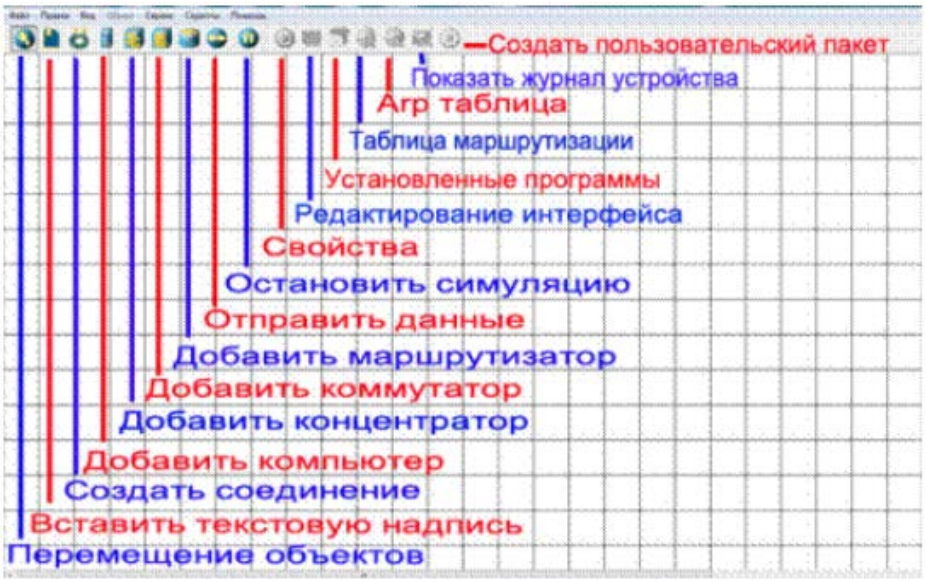


Рис. 2.3. Функциональное предназначение инструментов программы NetEmul

Панель устройств предназначена для добавления и перемещения ряда сетевых устройств. Описание пунктов панели (слева направо):

— перемещение объектов — позволяет перемещать устройства по сцене;

— текстовая надпись — позволяет добавить текстовую заметку на сцену;

— кабель (создать соединение) — позволяет соединять устройства в сети;

— добавить компьютер — установка персонального компьютера на сцену;

— добавить концентратор — установка сетевого концентратора (hub) на сцену;

— добавить коммутатор — установка сетевого коммутатора (switch) на сцену;

— добавить маршрутизатор — установка сетевого маршрутизатора (router) на сцену;

— отправить данные — используется для проверки работоспособности сети;

— остановить симуляцию — останавливает запущенную передачу данных в сети.

Панель параметров предназначена для настройки отдельно взятого устройства в сети. Важно отметить, что у каждого из сетевых устройств используются собственные настройки, поэтому не все пункты будут активны для каждого из устройств в сети. Описание пунктов панели (слева направо):

— показать свойства — вызывает диалоговое окно со свойствами сетевого устройства (например, для компьютера — это шлюз; для концентратора и коммутатора — количество портов и MAC-адреса в сети; для маршрутизатора — количество портов и включение или выключение маршрутизации);

— редактирование интерфейсов — пункт меню, с помощью которого задаются IP-адреса и маски подсети; используется для настройки компьютера и маршрутизатора.

— установленные программы — с помощью данного пункта можно присвоить компьютеру и маршрутизатору свойство сервера или клиента;

— таблица маршрутизации — с помощью данного пункта можно задать правила маршрутизации;

— ARP-таблица — позволяет задать соответствие между IP-адресами и MAC-адресами устройства;

— журнал устройства — с помощью данного пункта можно просмотреть подробный журнал событий устройства в сети, где отображаются проходящие через него пакеты при передаче данных.

2. Выполнение практического задания по ознакомлению с интерфейсом программы NetEmul. Соединение ЭВМ в сеть

Цель работы: ознакомиться с основами работы с программным эмулятором NetEmul. Научиться строить простейшие модели локальных вычислительных сетей. Уяснить разницу в построении сетей передачи данных на концентраторах и коммутаторах[4].

Теоретический материал

Запуск эмулятора NetEmul

Для запуска эмулятора NetEmul необходимо либо воспользоваться соответствующим пунктом главного меню операционной системы, либо выполнить в терминале команду netemul.

Порядок выполнения практического задания

С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую:

1. Номер учебного взвода.
2. ФИО курсантов, выполняющих работу.
3. Номер варианта согласно номеру курсанта (одного из курсантов группы) в журнале (см. табл. 2.1).

Таблица 2.1

Варианты задания (указаны согласно номеру курсанта в журнале)

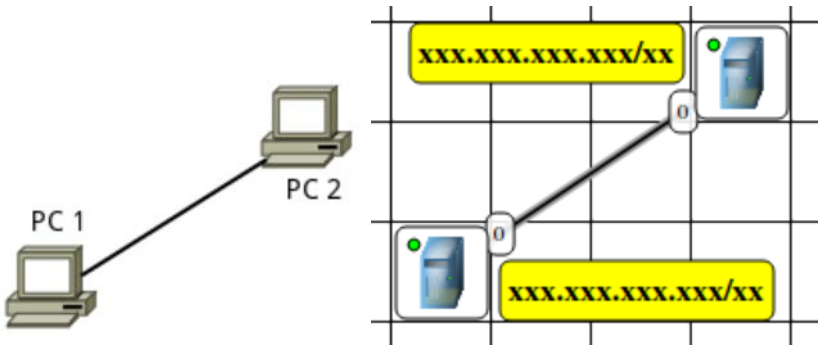
№	Адрес сети/маска	№	Адрес сети/маска	№	Адрес сети/маска
1	10.0.1.0/27	11	10.1.1.64/27	21	10.2.1.128/27
2	10.0.2.32/27	12	10.1.2.96/27	22	10.2.2.160/27
3	10.0.3.64/27	13	10.1.3.128/27	23	10.2.3.192/27
4	10.0.4.96/27	14	10.1.4.160/27	24	10.2.4.224/27
5	10.0.5.128/27	15	10.1.5.192/27	25	10.2.5.0/27
6	10.0.6.160/27	16	10.1.6.224/27	26	10.2.6.32/27
7	10.0.7.192/27	17	10.1.7.0/27	27	10.2.7.64/27
8	10.0.8.224/27	18	10.1.8.32/27	28	10.2.8.96/27
9	10.0.9.0/27	19	10.1.9.64/27	29	10.2.9.128/27
10	10.0.0.32/27	20	10.1.0.96/27	30	10.2.0.160/27

Соединение двух ЭВМ напрямую

1. Выбрать исходные данные для выполнения работы согласно своему варианту.

2. Добавить на рабочее поле эмулятора два компьютера (см. рис. 2.4), использовав кнопку «Добавить компьютер» на панели инструментов.

[4] Компьютерные сети передачи данных: лабораторный практикум / С. С. Владимиров. — СПб.: СПбГУТ, 2016. — 24 с.



а б

Рис. 2.4. Схема модели локальной вычислительной сети при соединении двух ЭВМ напрямую: а — в общем виде; б — в NetEmul

3. Соединить добавленные компьютеры, как показано на рис. 2.4. Для этого:

а) нажать кнопку «Создать соединение» на панели инструментов;

б) навести указатель на один из компьютеров;

в) зажав левую кнопку мыши (далее — ЛКМ), перевести курсор на второй компьютер — за курсором от первого компьютера должна тянуться прямая линия;

г) отпустить ЛКМ — после этого должно появиться окно начальных настроек с выбором соединяемых интерфейсов;

д) подтвердить соединение между интерфейсами eth0 и eth0, нажав «Соединить»;

е) если все сделано правильно, то компьютеры теперь соединены, на каждом конце соединения показан номер используемого интерфейса (в данном случае — 0), а индикатор соединения на иконке компьютера сменил цвет с красного на желтый (соединение есть, но интерфейсы не настроены).

4. Настроить компьютеры, задав каждому IP-адрес и маску подсети в соответствии с вариантом. Для этого:

а) выбрать инструмент «Перемещение объектов» на панели инструментов;

б) выделить первый компьютер щелчком ЛКМ;

в) вызвать контекстное меню щелчком ПКМ и выбрать пункт «Интерфейсы»;

г) в появившемся окне указать в соответствующих полях IP-адрес и маску подсети;

д) подтвердить ввод последовательным нажатием кнопок «Применить» и «ОК»;

е) если все сделано правильно, то индикатор соединения на иконке компьютера должен сменить цвет с желтого на зеленый (соединение есть, и интерфейсы настроены);

ж) добавить возле каждого компьютера надпись с его IP-адресом и маской подсети, как показано на рис. 2.4.

5. Проверить работоспособность построенной модели локальной вычислительной сети (далее — ЛВС), передав пакеты от одного компьютера до другого. Для этого:

а) выбрать инструмент «Отправить данные» на панели инструментов;

б) под курсором (на рабочем поле программы) должен появиться красный круг;

в) навести курсор с красным кругом на передающий компьютер и нажать ЛКМ;

г) в появившемся окне «Отправка» указать: протокол TCP, размер данных 5 KB;

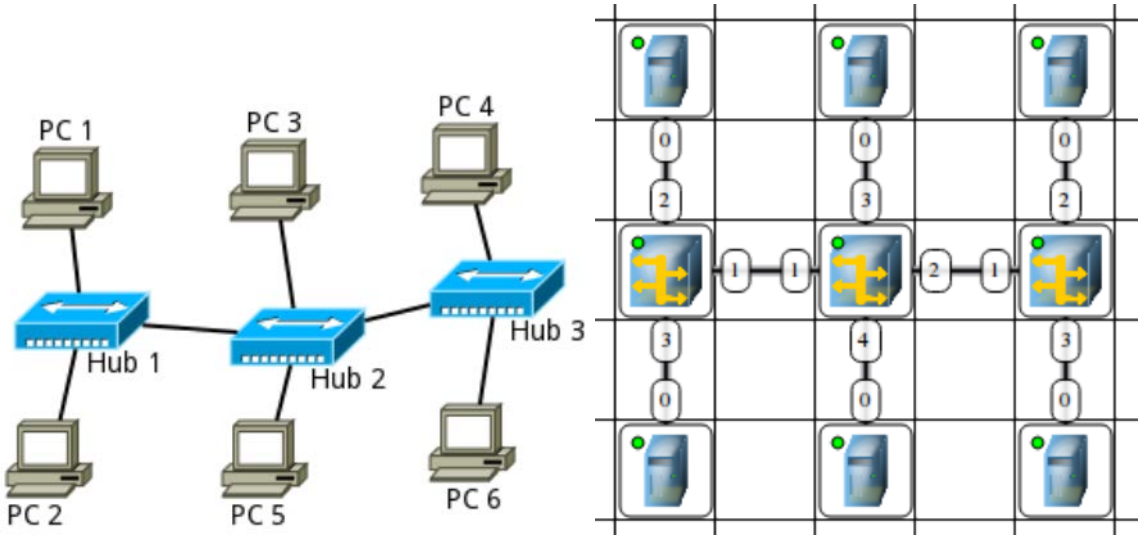
д) нажать «Далее» — окно пропадет, а кружок под курсором сменит цвет на зеленый;

е) навести курсор с зеленым кругом на принимающий компьютер и нажать ЛКМ;

ж) в появившемся окне подтвердить интерфейс на принимающем компьютере eth0, нажав «Отправка»;

з) проследить за перемещением пакетов.

Построение ЛВС на концентраторах



а б

Рис. 2.5. Схема модели локальной вычислительной сети на основе концентраторов: а — в общем виде; б — в NetEmul

1. Выбрать исходные данные для выполнения работы согласно своему варианту.

2. Добавить на рабочее поле эмулятора шесть компьютеров и три концентратора, как показано на рис. 2.5.

3. Соединить устройства, как показано на рис. 2.5.

4. Настроить компьютеры, задав каждому IP-адрес и маску подсети в соответствии с вариантом.

5. Добавить возле каждого компьютера надпись с его IP-адресом и маской подсети.

6. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) от одного компьютера до другого. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе концентраторов.

Построение локальной вычислительной сети на коммутаторах

1. Выбрать исходные данные для выполнения работы согласно своему варианту.

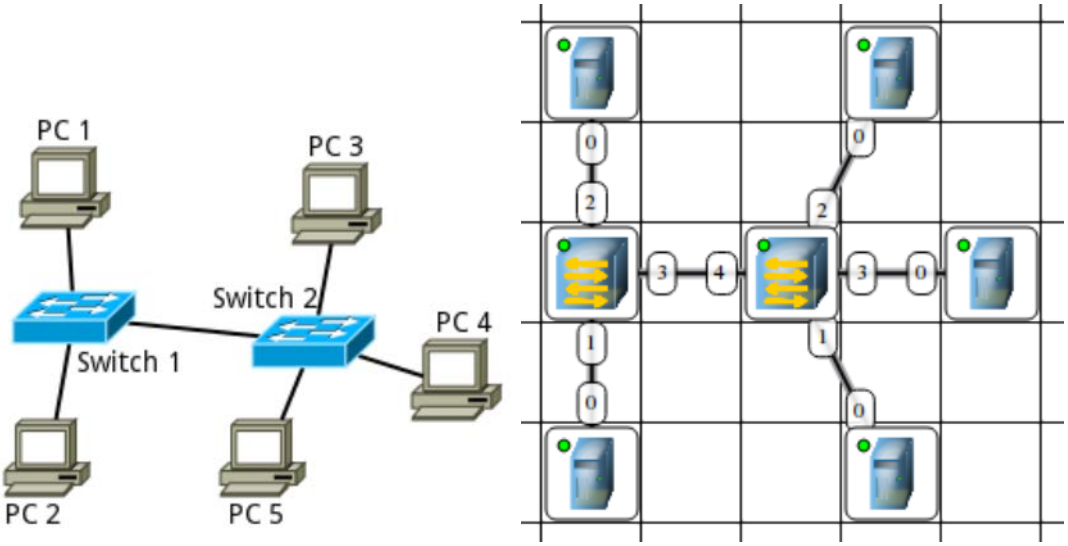
2. Добавить на рабочее поле эмулятора пять компьютеров и два коммутатора, как показано на рис. 2.6.

3. Соединить устройства, как показано на рис. 2.6.

4. Настроить компьютеры, задав каждому IP-адрес и маску подсети в соответствии с вариантом.

5. Добавить рядом с каждым компьютером надпись с его IP-адресом и маской подсети.

6. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) от одного компьютера до другого. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе коммутаторов.



а *б*

Рис. 2.6. Схема модели локальной вычислительной сети на основе коммутаторов: а — в общем виде; б — в NetEmul

После выполнения работы продемонстрировать преподавателю работоспособность построенной модели.

Проект сохранить для отчета.

Форма представления и содержание отчета: отчет в формате PDF выполняется согласно правилам оформления (приложение 1) и предоставляется преподавателю вместе с файлом проекта. Отчет выполняется один на группу.

Содержание отчета:

1. Титульный лист (оформляется согласно приложению 2).
2. Цель работы.
3. По каждому пункту практического занятия должна быть приведена схема модели с указанием IP-адресов устройств и номеров интерфейсов.
4. По каждому пункту практического занятия должны быть приведены выводы по работе.

Вопросы для самоконтроля:

1. Что такое IP-адрес?
2. Что такое маска подсети?
3. Как работает концентратор?
4. Как работает коммутатор?

Тема 3. Архитектура и стандартизация сетей

Семинар: Стандартизация сетей

Семинар посвящён изучению стандартизации сетей. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся по основным терминам и определениям архитектуры и стандартизации сетей.
2. Расширение научных представлений обучающихся об основных принципах архитектуры и стандартизации сетей.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Открытая система.
2. Организации, разрабатывающие стандарты в области компьютерных сетей.
3. История развития стандартизации сетей.
4. Стандартизация интернета.
5. Стандартные стеки коммуникационных протоколов.
6. Соответствие популярных стеков протоколов модели OSI.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Обсуждение основных терминов и определений архитектуры и стандартизации сетей. Педагогический работник актуализирует теоретические знания обучающихся о том, что представляет собой стандартизация сетей на современном этапе развития информационных технологий.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению

наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь стандартизации сетей с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Изучить содержание лекции «Общая характеристика модели OSI. Декомпозиция задачи сетевого взаимодействия».
2. Проработать материал главы 4 «Стандартизация и классификация сетей» учебного пособия[5].
3. Изучить основные термины и определения архитектуры и стандартизации сетей.
4. Уяснить смысл и содержание основных терминов и определений; уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Поясните порядок передачи данных между уровнями модели OSI.

Задание 2. Перечислите назначение и функции уровней модели OSI.

Вопросы для самоконтроля:

1. Приведите пример декомпозиции задачи.
2. В чём сущность многоуровневого подхода?
3. Что такое стек протоколов?
4. Дайте понятие протокольной сущности.

Практическое занятие (эмулятор NetEmul): Использование маршрутизаторов. Статическая маршрутизация

Цель работы: ознакомиться с работой маршрутизаторов. Научиться формировать статические маршруты и прописывать их в таблицы маршрутизации сетевых устройств.

Теоретический материал

Запуск эмулятора NetEmul

Для запуска эмулятора NetEmul необходимо либо воспользоваться соответствующим пунктом главного меню операционной системы, либо выполнить в терминале команду netemul.

Порядок выполнения практического задания

С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую:

1. Номер группы.
2. ФИО курсантов, выполняющих работу.

[5] Компьютерные сети. Принципы, технологии, протоколы: учебное пособие / В. Олифер, Н. Олифер. — СПб.; М.; Екатеринбург: Питер, 2021. — 1005 с.

Построение модели сети

1. Выбрать исходные данные для выполнения работы согласно своему варианту. Варианты заданий взять из табл. 3.1.

Таблица 3.1

Варианты задания (указаны согласно номеру курсанта в журнале)

Вариант задания	*Диапазон адресов 1*	*Диапазон адресов 2*
1	10.1.0.0/16	192.168.1.0/24
2	172.20.2.0/24	192.168.0.0/16
3	10.3.0.0/24	172.16.0.0/12
4	192.168.4.0/24	10.4.0.0/16
5	172.30.5.0/24	10.0.0.0/8
6	10.6.0.0/16	192.168.0.0/16
7	10.7.0.0/24	172.17.7.0/24
8	172.18.8.0/24	192.168.0.0/16
9	192.168.9.0/24	10.0.0.0/8
10	192.168.10.0/24	10.10.0.0/16
11	172.21.11.0/24	192.168.0.0/16
12	10.12.0.0/16	192.168.0.0/16
13	192.168.13.0/24	10.13.0.0/16
14	172.24.0.0/12	10.14.0.0/16
15	10.15.0.0/24	192.168.0.0/16
16	192.168.16.0/24	10.16.0.0/16
17	172.27.17.0/24	10.0.0.0/24
18	10.18.0.0/16	192.168.0.0/16
19	192.168.19.0/24	10.19.0.0/24
20	192.168.20.0/24	172.20.1.0/24
21	172.21.1.0/24	10.0.0.0/16
22	172.23.22.0/24	10.10.0.0/16
23	192.168.0.0/16	172.23.23.0/24
24	10.24.0.0/16	192.168.24.0/24
25	172.27.0.0/16	10.25.1.0/24
26	192.168.26.0/24	10.26.1.0/24
27	10.27.0.0/24	172.17.110.0/24
28	172.28.0.0/24	192.168.0.0/16
29	10.29.0.0/16	192.168.0.0/16
30	172.29.30.0/24	10.30.0.0/16

2. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 3.1. В свойствах каждого маршрутизатора необходимо указать количество интерфейсов, равное 4.

3. Настроить интерфейсы компьютеров и маршрутизаторов, задав каждому IP-адрес и маску подсети в соответствии с вариантом. Добавить рядом с каждым компьютером и интерфейсом роутера надписи с их IP-адресом и маской подсети.

4. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) от одного устройства до другого в пределах одной подсети.

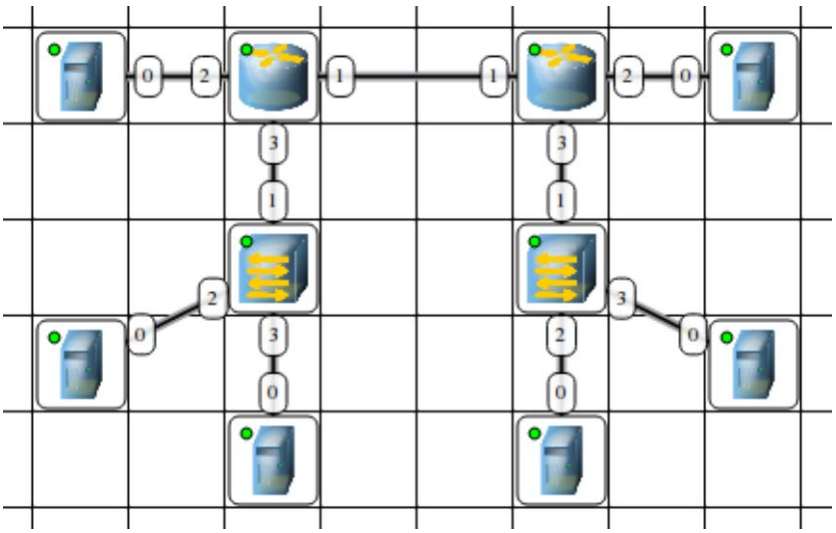


Рис. 3.1. Связь сетей посредством маршрутизаторов

Формирование таблицы статической маршрутизации

1. Задать на каждом компьютере маршрут «по умолчанию» (IP сети = 0.0.0.0; маска подсети = 0.0.0.0).

2. Задать на каждом маршрутизаторе статические маршруты до удалённых от него сетей.

3. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) между удаленными друг от друга сетями. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе маршрутизаторов.

После выполнения работы продемонстрировать преподавателю работоспособность построенной модели.

Проект сохранить для отчета.

Форма представления и содержание отчета: отчет в формате PDF выполняется согласно правилам оформления (приложение 1) и предоставляется преподавателю вместе с файлом проекта. Отчет выполняется один на группу.

Содержание отчета:

1. Титульный лист (оформляется согласно приложению 2).
2. Цель работы.
3. По каждому пункту практического занятия должна быть приведена схема модели с указанием IP-адресов устройств и номеров интерфейсов.
4. По каждому пункту практического занятия должны быть приведены выводы по работе.

Вопросы для самоконтроля:

1. Охарактеризуйте функции уровней модели OSI.
2. Дайте сравнительную характеристику методов коммутации.
3. Как работает маршрутизатор?
4. Назовите принципы статической маршрутизации.

Тема 4. Технологии физического уровня

Семинар: Технологии первичных сетей

Семинар посвящён изучению технологии первичных сетей. Занятия проводятся в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся по технологиям первичных сетей.
2. Расширение научных представлений обучающихся об организации первичных сетей PHD и SDH; об организации первичных сетей DWDM и OTM.
4. Развитие мышления и творческой активности обучающихся.
5. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
6. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Организация первичных сетей PHD.
2. Организация первичных сетей SHD.
3. Организация первичных сетей OTN.
4. Организация первичных сетей DWDM.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания обучающихся об основных принципах организации первичных сетей.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь технологии первичных сетей с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Изучить содержание лекции «Линии связи. Принципы организации первичных сетей».

2. Проработать материал главы 8 «Технологии первичных сетей PHD и SDH», главы 9 «Технологии первичных сетей DWDM и OTM» учебного пособия[6].

3. Изучить особенности технологии первичных сетей.

4. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Наиболее полно ответьте на поставленные вопросы. Ответы обоснуйте. Чем логическое кодирование отличается от физического? С какой целью в технологиях PDH и SDH используется чередование байтов? В чём заключаются функции мультиплексора?

Задание 2. Приведите примеры мультиплексирования телефонного узла на 400 каналов. В чём заключается сложность выведения потока?

Вопросы для самоконтроля:

1. Адреса какого типа используются в таблицах коммутации SDH?
2. Что унаследовала технология OTN от технологии SDH?
3. Каковы особенности трибутарного слота OTN?

[6] Компьютерные сети: учебное пособие.

Раздел II. ЛОКАЛЬНЫЕ СЕТИ

Тема 5. Технология Ethernet

Семинар: Использование различных типов кадров Ethernet

Семинар посвящён изучению использования различных типов кадров Ethernet. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся по технологии Ethernet.
2. Расширение научных представлений обучающихся о применении различных типов кадров и стандартов технологии Ethernet.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Форматы кадров технологии Ethernet.
2. Неблокирующие коммутаторы технологии Ethernet.
3. Спецификация Fast Ethernet.
4. Спецификация Gigabit Ethernet.
5. Стандарт 10G Ethernet.
6. Стандарты 100G Ethernet и 40G Ethernet.
7. Стандарты 400G, 200G Ethernet и 50G Ethernet.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания обучающихся о технологии Ethernet.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь технологии Ethernet с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Изучить содержание лекции «Ethernet в локальных сетях».

2. Проработать материал главы 10 «Ethernet в локальных сетях» учебного пособия[7].

3. Изучить особенности технологии Ethernet.

4. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Имеется таблица продвижения моста (табл. 5.1).

Таблица 5.1

Таблица продвижения моста

Порт	*MAC-адрес*
1	f8:f2:1e:0c:3a:b8
2	d0:94:66:4c:37:bf

На порт 2 поступает кадр с адресом назначения ac:1f:6b:64:c7:d6 и адресом источника f8:f2:1e:0c:3a:b8. Какое действие выполнит мост?

а) передаст его на все порты и не станет корректировать записи;

б) передаст его на все порты и заменит первую запись таблицы продвижения на MAC-адрес f6:f2:1e:0c:3a:b6, порт 2;

в) отбросит кадр.

Задание 2. В сети на коммутаторах образовалась петля. Какие меры необходимо принять, чтобы предотвратить негативные последствия:

а) разорвать петлю логическим переводом порта в неактивное состояние.

б) активировать протокол STP;

в) установить более скоростные порты Ethernet;

г) разорвать петлю физическим отсоединением порта.

Ответ обоснуйте.

Вопросы для самоконтроля:

1. В чём заключаются преимущества и недостатки разделяемой среды?

2. Имеется MAC-адрес 02:25:86:64:ca:e4. К какому типу он относится?

3. Приведите примеры коммутаторов отечественного производства. Каковы их особенности?

4. Как можно назначить некоторый коммутатор корневым?

Тема 6. Локальные сети на основе разделяемой среды

Семинар: Беспроводные локальные сети

Семинар посвящён изучению беспроводных локальных сетей. Занятие проводится в интерактивной форме учебной дискуссии.

[7] Компьютерные сети. Принципы, технологии, протоколы.

Цели занятия:

1. Закрепление знаний обучающихся в области локальных сетей на основе разделяемой среды.

2. Расширение научных представлений обучающихся о практическом использовании локальных сетей на основе разделяемой среды.

3. Развитие мышления и творческой активности обучающихся.

4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.

5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Технологии физического уровня беспроводных сетей.
2. Особенности среды беспроводных локальных сетей.
3. Беспроводные локальные сети IEEE 802.11.
4. Персональные сети и технология Bluetooth.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания обучающихся о локальных сетях на основе разделяемой среды.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь локальных сетей на основе разделяемой среды с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 21 «Технологии физического уровня беспроводных сетей», главы 22 «Беспроводные локальные и персональные сети» учебного пособия[8].

2. Изучить особенности локальных сетей на основе разделяемой среды.

3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

[8] Компьютерные сети. Принципы, технологии, протоколы.

Практический материал для занятия:

Задание 1. Настройте на ноутбуке доступ к созданной беспроводной сети. Остановите все беспроводные подключения, в частности Wi-Fi, сотовую связь и Bluetooth. Какой инструмент для этого используется?

Задание 2. Создайте на ноутбуке беспроводную локальную сеть. Осуществите подключение с других устройств к этой сети. Получите сведения о беспроводной сети. Результат продемонстрируйте преподавателю.

Вопросы для самоконтроля:

1. Дайте общую характеристику технологии физического уровня беспроводных сетей.
2. Назовите основные особенности беспроводных локальных сетей IEEE 802.11.
3. Какие рабочие диапазоны частот существуют у стандартов семейства IEEE 802.11?
4. Какие версии технологии Bluetooth используются для передачи данных?

Тема 7. Коммутируемые локальные сети

Семинар: Логическая структуризация сети с помощью мостов и коммутаторов

Семинар посвящён изучению логической структуризации сети с помощью мостов и коммутаторов. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области коммутируемых локальных сетей.
2. Расширение научных представлений обучающихся о практическом использовании коммутируемых локальных сетей.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Алгоритм покрывающего дерева.
2. Фильтрация трафика.
3. Агрегирование линий связи в локальных сетях.
4. Виртуальные локальные сети.
5. Ограничения коммутаторов.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический

работник актуализирует теоретические знания обучающихся о коммутируемых локальных сетях.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь логической структуризации сети с помощью мостов и коммутаторов с общими принципами коммутируемых локальных сетей.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 11 «Отказоустойчивые и виртуальные локальные сети» учебного пособия[9].
2. Изучить особенности коммутируемых локальных сетей.
3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Вопросы для самоконтроля:

1. Сформулируйте понятие виртуальной локальной сети (VLAN).
2. Назовите основные особенности быстрого и эффективного выполнения логической структуризации сетей.
3. Как происходит логическая структуризация сети при подключении к коммутатору компьютера и сегмента сети?

[9] Компьютерные сети. Принципы, технологии, протоколы.

Раздел III. СЕТИ TCP/IP

Тема 8. Адресация в сетях TCP/IP

Семинар: Схема работы DNS

Семинар посвящён изучению схемы работы DNS. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области адресации в сетях TCP/IP.
2. Расширение научных представлений обучающихся о практическом использовании адресации в сетях TCP/IP.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Пространство DNS-имен.
2. Сервер, клиент и протокол DNS.
3. Иерархическая организация службы DNS.
4. Итеративная и рекурсивная процедуры разрешения имени.
5. Корневые серверы и обратная зона.
6. Протокол DHCP.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания обучающихся об адресации в сетях TCP/IP.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь схемы работы DNS с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Изучить содержание лекции «Типы адресов стека TCP/IP. Адресация и технология CIDR».

2. Проработать материал главы 13 «Адресация в стеке протоколов TCP/IP» учебного пособия[10].

3. Изучить особенности адресации в сетях TCP/IP.

4. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Структура сети неизвестна, но в распоряжении инженера имеется таблица соответствия IP-адресов и DNS-имён нескольких узлов сети (табл. 8.1).

Таблица 8.1

Таблица соответствия IP-адресов и DNS-имён

IP-адрес узла	125.1.0.05	125.1.0.06	125.1.0.07	125.1.0.07		
DNS-имя узла	w1.nsd.ru	w2.nsd.ru	w3.nsd.ru	w4.nsd.ru	w5.nsd.ru	w6.nsd.ru

Что можно сказать об IP-адресах узлов, имеющих DNS-имена w5.nsd.ru и w5.nsd.ru?

Задание 2. На учебном курсе факультета обучается 96 курсантов. Каждый из них имеет собственный ноутбук. В учебном корпусе оборудована специализированная аудитория, в которой развернута компьютерная сеть, имеющая 30 коннекторов для подключения компьютеров. Во время практических занятий курсанты отрабатывают задачи в этой аудитории, подключая свои ноутбуки к сети. Сколько IP-адресов должно быть у администратора сети, чтобы все курсанты могли подключаться к ней, не выполняя процедуру конфигурирования своих ноутбуков? Ответ обоснуйте.

Вопросы для самоконтроля:

1. Дайте определение DNS.
2. Назовите две основные схемы разрешения DNS-имен.
3. Что такое корневые серверы?
4. Охарактеризуйте понятие «Обратная зона».

Практическое занятие (эмулятор NetEmul): Разрешение адресов по протоколу ARP. APR-спуфинг

Цель работы: Ознакомиться с механизмом работы протокола ARP. Научиться формировать и отправлять пользовательские пакеты. Ознакомиться с журналом работы сетевого устройства в эмуляторе. Научиться проводить сетевую атаку вида ARP-спуфинг.

[10] Компьютерные сети. Принципы, технологии, протоколы.

Теоретический материал

Запуск эмулятора NetEmul

Для запуска эмулятора NetEmul необходимо либо воспользоваться соответствующим пунктом главного меню операционной системы, либо выполнить в терминале команду netemul.

Протокол ARP

ARP (Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса сетевого устройства по известному IP-адресу. Наибольшее распространение ARP получил благодаря распространенности сетей IP, построенных поверх Ethernet, поскольку в подавляющем большинстве случаев при таком сочетании используется ARP. В семействе протоколов IPv6 протокола ARP не существует, его функции возложены на ICMPv6. Описание протокола было опубликовано в ноябре 1982 г. в RFC 826. ARP был спроектирован для случая передачи IP-пакетов через сегмент Ethernet. При этом общий принцип, предложенный для ARP, был использован и для сетей других типов. Существуют следующие типы сообщений ARP: запрос ARP (ARP-request) и ответ ARP (ARP-reply). Система-отправитель при помощи запроса ARP запрашивает физический адрес системы-получателя. Ответ (физический адрес узла-получателя) приходит в виде ответа ARP. Принцип работы протокола: узел (хост A), которому нужно выполнить отображение IP-адреса на MAC-адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес (хост B), и рассылает запрос широковещательно (в поле «MAC-адрес назначения» заголовка Ethernet указывается широковещательный MAC-адрес FF:FF:FF:FF:FF:FF). Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел (хост B) формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель (хост A) указывает свой локальный адрес.

Схема работы показана на рис. 8.1.

При получении ARP-ответа хост A записывает в кэш ARP запись с соответствием IP-адреса хоста B и MAC-адреса хоста B, полученного из ARP-ответа. Время хранения такой записи ограничено. По истечении времени хранения хост A посылает повторный запрос, теперь уже адресно, на известный MAC-адрес хоста B. В случае, если ответ не получен, снова посылается широковещательный запрос.

Структура кадра ARP с учетом заголовка Ethernet показана на рис. 8.2.

Значения полей заголовка кадра ARP приведены в табл. 8.1.

Самопроизвольный ARP (gratuitous ARP) — такое поведение ARP, когда ARP-ответ присылается, если в этом (с точки зрения получателя) нет особой необходимости. Самопроизвольный ARP-ответ — это пакет-ответ ARP, присланный без запроса. Он применяется для определения конфликтов IP-адресов в сети: как только станция получает адрес по DHCP или адрес присваивается вручную, рассылается ARP-ответ gratuitous ARP.

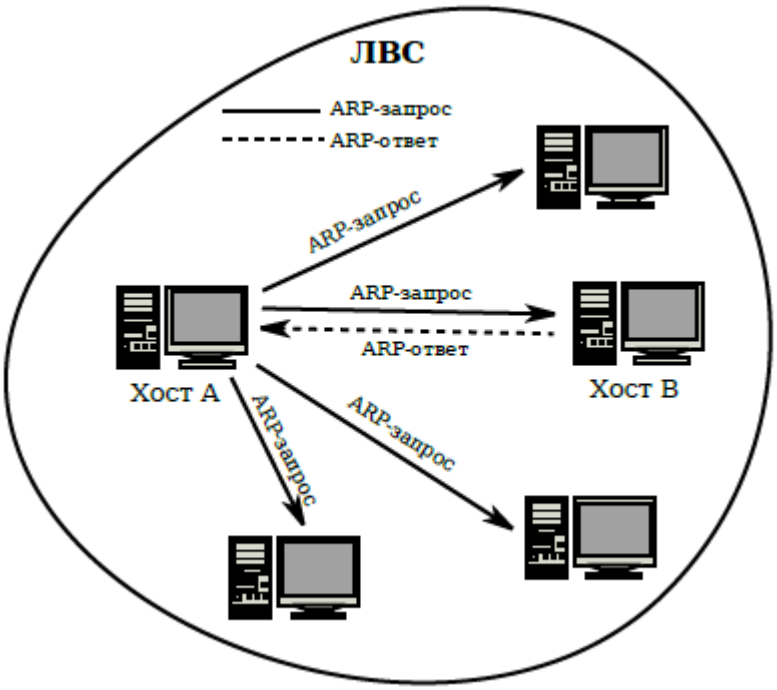


Рис. 8.1. Схема работы протокола ARP

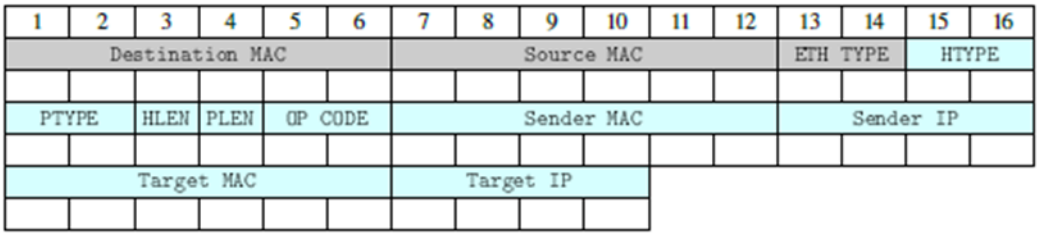


Рис. 8.2. Кадр протокола ARP

Таблица 8.1

Значения полей заголовка кадра ARP

Поле	Значение
HTYPE	Номер протокола передачи канального уровня (0x0001 для протокола Ethernet)
PTYPE	Код протокола сетевого уровня (0x0800 для протокола IPv4)
HLEN	Длина физического адреса в байтах. Адреса Ethernet имеют длину 6 байт
PLEN	Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта
OP CODE	Код операции: 0x01 в случае ARP-запроса и 0x02 в случае ARP-ответа
Sender MAC	Физический адрес отправителя
Sender IP	Сетевой адрес отправителя
Target MAC	Физический адрес получателя. При запросе поле заполняется нулями
Target IP	Сетевой адрес получателя

Самопроизвольный ARP может быть полезен в следующих случаях:
— обновление ARP-таблиц, в частности, в кластерных системах;
— информирование коммутаторов;
— извещение о включении сетевого интерфейса.

Несмотря на эффективность самопроизвольного ARP, он является особенно небезопасным, поскольку с его помощью можно уверить удаленный узел

в том, что MAC-адрес какой-либо системы, находящейся с ней в одной сети, изменился, и указать, какой адрес используется теперь.

Сетевая атака ARP-спуфинг

Сетевая атака ARP-спуфинг (ARP-spoofing) основана на использовании самопроизвольного ARP. Чтобы перехватить сетевые пакеты, которые атакуемый хост (A) отправляет на хост B, атакующий хост (C) формирует ARP-ответ, в котором ставит в соответствие IP-адресу хоста B свой MAC-адрес. Далее этот пакет отправляется на хост A. В том случае, если хост A поддерживает самопроизвольный ARP, он модифицирует собственную ARP-таблицу и помещает туда запись, где вместо настоящего MAC-адреса хоста B стоит MAC-адрес атакующего хоста C. Теперь пакеты, отправляемые хостом A на хост B, будут передаваться хосту C.

Схема атаки показана на рис. 8.3.

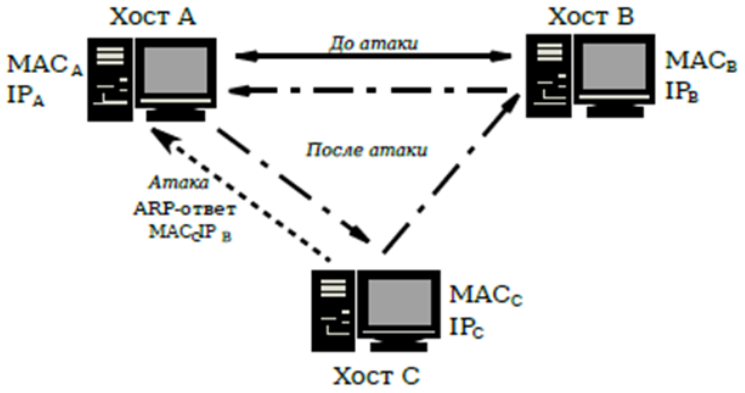


Рис. 8.3. Схема сетевой атаки ARP-спуфинг

Порядок выполнения практического задания

С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую:

1. Номер учебного взвода.
2. ФИО курсантов, выполняющих работу.
3. Номер варианта согласно номеру курсанта (одного из курсантов группы) в журнале (табл. 8.2).

Таблица 8.2

Варианты задания (указаны согласно номеру курсанта в журнале)

№	Адрес сети/маска	№	Адрес сети/маска	№	Адрес сети/маска
1	10.0.1.0/27	11	10.1.1.64/27	21	10.2.1.128/27
2	10.0.2.32/27	12	10.1.2.96/27	22	10.2.2.160/27
3	10.0.3.64/27	13	10.1.3.128/27	23	10.2.3.192/27
4	10.0.4.96/27	14	10.1.4.160/27	24	10.2.4.224/27
5	10.0.5.128/27	15	10.1.5.192/27	25	10.2.5.0/27
6	10.0.6.160/27	16	10.1.6.224/27	26	10.2.6.32/27
7	10.0.7.192/27	17	10.1.7.0/27	27	10.2.7.64/27
8	10.0.8.224/27	18	10.1.8.32/27	28	10.2.8.96/27
9	10.0.9.0/27	19	10.1.9.64/27	29	10.2.9.128/27
10	10.0.0.32/27	20	10.1.0.96/27	30	10.2.0.160/27

Построение модели сети

1. Выбрать исходные данные для выполнения работы согласно своему варианту. Полученную согласно варианту сеть с маской /27 разбить на две подсети с маской /28 каждая.

2. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 8.4. В свойствах маршрутизатора необходимо указать количество интерфейсов, равное 2.

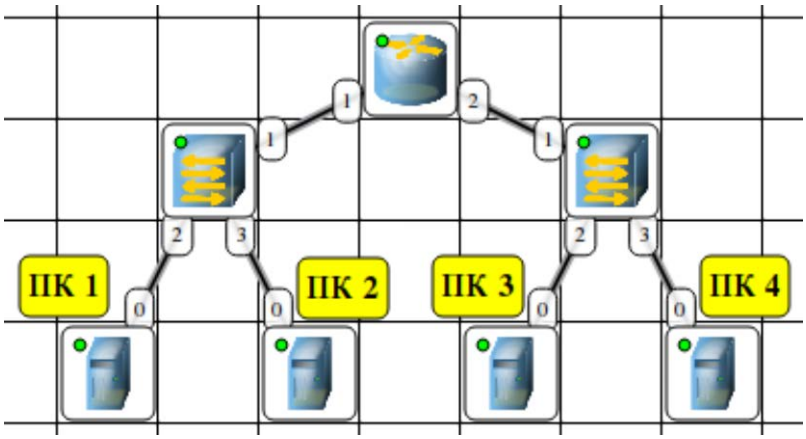


Рис. 8.4. Сеть для изучения протокола ARP

3. Настроить интерфейсы компьютеров и маршрутизаторов, задав каждому IP-адрес и маску подсети (слева — первая подсеть в заданной сети, справа — вторая подсеть). Добавить рядом с каждым компьютером и интерфейсом роутера надписи с их IP-адресом и маской подсети.

4. Настроить на компьютерах маршруты «по умолчанию» (IP сети = 0.0.0.0; маска подсети = 0.0.0.0). Можно воспользоваться «Таблицей маршрутизации» либо вызвать свойства компьютера двойным щелчком, указать шлюз по умолчанию и включить маршрутизацию.

5. Включить маршрутизацию на маршрутизаторе.

6. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) от компьютера в левой подсети до компьютера в правой подсети.

7. Задать каждому компьютеру имя-описание, воспользовавшись пунктом контекстного меню «Задать описание».

Определение MAC-адреса с помощью ARP-запроса

1. Запустить для компьютеров 1 и 2 журналы пакетов (пункт меню «Показать журнал»).

2. Очистить ARP-таблицу компьютера 1.

3. Выделить компьютер 1 и с помощью инструмента «Конструктор пакетов» сформировать пакет ARP-запроса для определения MAC-адреса компьютера 2. Помните, что ARP-запрос рассылается широковещательно (MAC-адрес получателя в заголовке Ethernet — FF:FF:FF:FF:FF:FF), а MAC-адрес искомого узла в заголовке ARP приравнивается к нулевому 00:00:00:00:00:00. MAC-адрес компьютера 1 указан в окне «Интерфейсы» для компьютера 1.

4. Запустить ARP-запрос, проследить за ним и за сгенерированным для него ARP-ответом по схеме сети и журналам компьютеров 1 и 2.

5. Открыть ARP-таблицу компьютера 1 и убедиться, что запись добавилась в таблицу.

6. Сохранить скриншот экрана (с открытыми журналами) для отчета.

Реализация атаки ARP-спуфинг

1. Запустить для компьютеров 1 и 2 журналы пакетов (пункт меню «Показать журнал»). При необходимости очистить их.

2. Очистить ARP-таблицу компьютера 1.

3. Выделить компьютер 2 и с помощью инструмента «Конструктор пакетов» сформировать пакет ARP-ответа, в котором будут указаны

– MAC отправителя — MAC компьютера 2;
– IP отправителя — IP интерфейса роутера в левой подсети;
– MAC получателя — MAC компьютера 1;
– IP получателя — IP компьютера 1.

4. Запустить ARP-ответ, проследить за ним. Может возникнуть окно с сообщением о дублировании IP-адресов в сети — это происходит в том случае, если из-за действий коммутатора пакет-атаку получает и роутер. Окно быстро закрыть.

5. Сразу же запустить передачу пакетов (UDP, 5 KB) от компьютера 1 на компьютер 3. Убедиться, что пакеты вначале приходят на компьютер 2 и лишь потом (если на компьютере 2 включена маршрутизация) отправляются на компьютер 3 (через маршрутизатор).

6. Сохранить скриншот экрана (с открытыми журналами) для отчета.

После выполнения работы продемонстрировать преподавателю работоспособность построенной модели.

Проект сохранить для отчета.

Форма представления и содержание отчета: отчет в формате PDF выполняется согласно правилам оформления (приложение 1) и предоставляется преподавателю вместе с файлом проекта. Отчет выполняется один на группу.

Содержание отчета:

1. Титульный лист (оформляется согласно приложению 2).
2. Цель работы.
3. Разбиение заданной сети /27 на две подсети /28.
4. Схема модели с указанием IP-адресов устройств и номеров интерфейсов.
5. Скриншоты с результатами разрешения адреса и сетевой атаки.
6. По каждому пункту практического занятия должны быть приведены выводы по работе.

Вопросы для самоконтроля:

1. Что такое протокол ARP?
2. Каков формат пакета ARP?
3. Охарактеризуйте самопроизвольный ARP.
4. Что такое MAC-адрес?
5. Что такое ARP-спуфинг?

Тема 9. Протокол межсетевого взаимодействия

Практическое занятие (эмулятор NetEmul): Динамическая маршрутизация по протоколу RIP. Получение сетевых настроек по DHCP

Цель работы: ознакомиться с механизмом динамической маршрутизации по протоколу RIP. Научиться настраивать компьютеры и серверы для автоматизации получения компьютерами сетевых настроек.

Теоретический материал

Запуск эмулятора NetEmul

Для запуска эмулятора NetEmul необходимо либо воспользоваться соответствующим пунктом главного меню операционной системы, либо выполнить в терминале команду netemul.

Порядок выполнения практического задания

С помощью инструмента «Вставить текстовую надпись» добавить на рабочее поле эмулятора надпись, содержащую:

1. Номер учебного взвода.
2. ФИО курсантов, выполняющих работу.
3. Номер варианта согласно номеру курсанта (одного из курсантов группы) в журнале (табл. 9.1).

Таблица 9.1

Варианты задания (указаны согласно номеру курсанта в журнале)

№	Адрес сети/маска	№	Адрес сети/маска	№	Адрес сети/маска
1	10.0.1.0/26	11	10.1.1.128/26	21	10.2.1.0/26
2	10.0.2.64/26	12	10.1.2.192/26	22	10.2.2.64/26
3	10.0.3.128/26	13	10.1.3.0/26	23	10.2.3.128/26
4	10.0.4.192/26	14	10.1.4.64/26	24	10.2.4.192/26
5	10.0.5.0/26	15	10.1.5.128/26	25	10.2.5.0/26
6	10.0.6.64/26	16	10.1.6.192/26	26	10.2.6.64/26
7	10.0.7.128/26	17	10.1.7.0/26	27	10.2.7.128/26
8	10.0.8.192/26	18	10.1.8.64/26	28	10.2.8.192/26
9	10.0.9.0/26	19	10.1.9.128/26	29	10.2.9.0/26
10	10.0.0.64/26	20	10.1.0.192/26	30	10.2.0.64/26

Построение модели сети

1. Выбрать исходные данные для выполнения работы согласно своему варианту. Полученную согласно варианту сеть с маской /26 разбить на 8 подсетей с маской /29 каждая.

2. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 9.1.

3. Распределить полученные ранее адреса сетей между сетями SR1–SR5 и SH11–SH13. Добавить рядом с каждой сетью надпись с ее IP-адресом.

4. Настроить интерфейсы маршрутизаторов, задав каждому IP-адрес и маску подсети в соответствии с выбранным распределением.

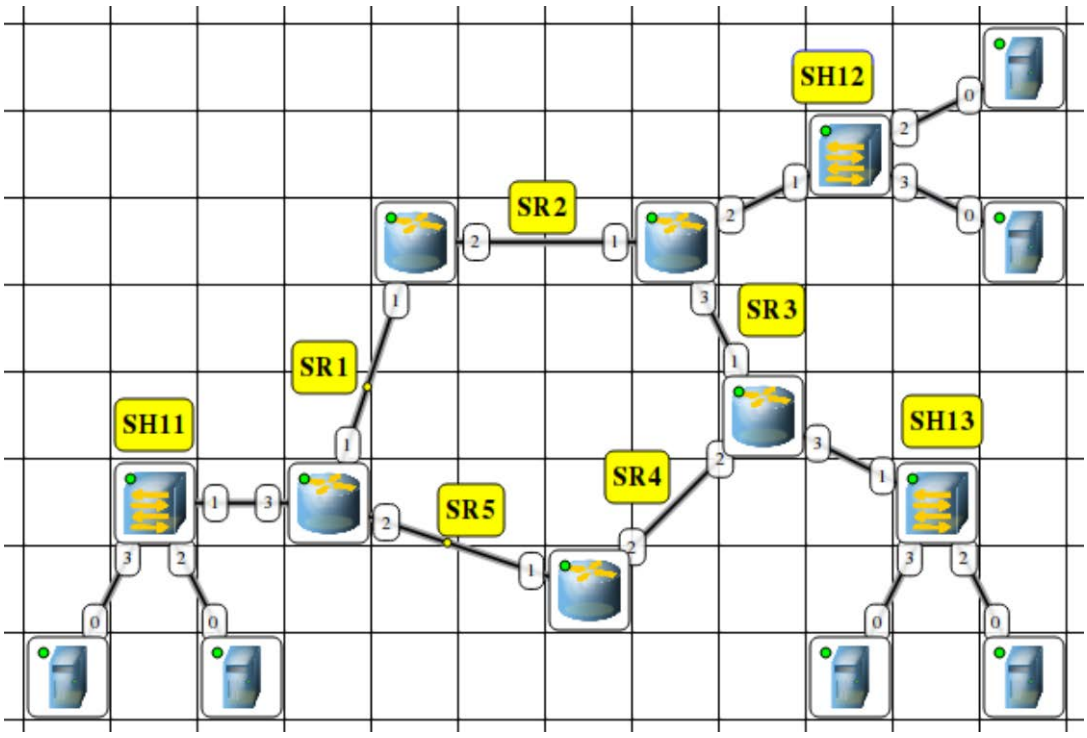


Рис. 9.1. Модель сети для изучения работы протоколов RIP и DHCP

Настройка динамической маршрутизации по протоколу RIP

1. На каждом маршрутизаторе добавить и запустить программу RIP. Пункт контекстного меню «Программы». Кнопка «Добавить». Поставить флаг для активации программы.

2. Включить маршрутизацию на маршрутизаторе.

3. Открыть журнал одного из маршрутизаторов. Проследить за перемещением пакетов протокола RIP по сети.

4. Поочередно открыть таблицы маршрутизации каждого маршрутизатора и убедиться, что таблица заполнилась.

Настройка автоматического получения сетевых настроек по протоколу DHCP

1. На маршрутизаторах, которые отвечают за сети SH11–SH13, добавить и запустить программу DHCP-сервер. Не забудьте поставить флаг для активации программы.

2. В настройках каждого DHCP-сервера указать интерфейс, «смотрящий» в сторону сети SH, тип адресов — динамические, диапазон адресов, выделяемых для динамической адресации, маску подсети и IP-адрес шлюза.

3. На каждом компьютере добавить и запустить программу DHCP-клиент. Поставить флаг для активации программы.

4. В настройках каждого DHCP-клиента указать интерфейс, который должен автоматически получать сетевые настройки.

5. Открыть диалог настройки интерфейсов каждого компьютера и убедиться, что стоит флаг «Получать настройки автоматически».

6. Дождаться, пока все компьютеры получат сетевые настройки.

7. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) между компьютерами в разных подсетях.

После выполнения работы продемонстрировать преподавателю работоспособность построенной модели.

Проект сохранить для отчета.

Формат письма:

Тема: номер учебного взвода, дисциплина, номер работы, ФИО первого курсанта в группе.

Тело: номер учебного взвода. Дисциплина. Номер работы. ФИО курсантов.

Содержание отчета:

1. Заголовок согласно приложению.
2. Цель работы.
3. Схема модели с указанием IP-адресов устройств и номеров интерфейсов.
4. По каждому пункту практического занятия должны быть приведены выводы по работе.

Форма представления и содержание отчета: отчет в формате PDF выполняется согласно правилам оформления (приложение 1) и представляется преподавателю вместе с файлом проекта. Отчет выполняется один на группу.

Содержание отчета:

1. Титульный лист (оформляется согласно приложению 2).
2. Цель работы.
3. Схема модели с указанием IP-адресов устройств и номеров интерфейсов.
4. По каждому пункту практического занятия должны быть приведены выводы по работе.

Вопросы для самоконтроля:

1. Охарактеризуйте протокол RIP.
2. Охарактеризуйте протокол DHCP.

Тема 10. Базовые протоколы TCP/IP

Семинар: Управление окном приёма

Семинар посвящён изучению протоколов транспортного уровня TCP и UDP. Занятия проводятся в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области базовых протоколов TCP/IP.
2. Расширение научных представлений обучающихся о протоколах транспортного уровня TCP и UDP.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Сегменты и поток байтов.
2. Система буферов при дуплексной передаче.
3. Накопительный принцип квитирования.
4. Параметры управления потоком в TCP.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания о маршрутизации в IP сетях.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь управления окном приёма с базовыми протоколами TCP/IP.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 15 «Протоколы транспортного уровня TCP и UDP» учебного пособия[11].
2. Изучить особенности протоколов транспортного уровня TCP и UDP.
3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Вопросы для самоконтроля:

1. Охарактеризуйте сущность метода квитирования.
2. Назовите основные особенности метода скользящего окна.
3. Перечислите различия между методом квитирования и методом скользящего окна.

[11] Компьютерные сети. Принципы, технологии, протоколы.

Тема 11. Маршрутизация в IP-сетях

Семинар: Классификация протоколов маршрутизации. Построение таблицы маршрутизации

Семинар посвящён изучению классификации протоколов маршрутизации и особенностям построения таблицы маршрутизации. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области маршрутизации в IP-сетях.
2. Расширение научных представлений обучающихся о маршрутизации в IP-сетях.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Протокол RIP.
2. Протокол OSPF.
3. Маршрутизация в неоднородных сетях.
4. Протокол BGP.
5. Протокол IGMP.
6. Программно определяемые сети SDN.
7. Виртуализация сетевых функций: NFV.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания о маршрутизации в IP сетях.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь протоколов маршрутизации и таблицы маршрутизации с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 15 «Протоколы транспортного уровня TCP и UDP», главы 16 «Протоколы маршрутизации и технология SDN» учебного пособия[12].

2. Изучить особенности маршрутизация в IP-сетях.

3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Приведите перечень протоколов маршрутизации и дайте им краткие характеристики.

Задание 2. Перечислите пять основных недостатков традиционной маршрутизации, которые послужили причинами создания SDN. Поясните их содержание.

Вопросы для самоконтроля:

1. Приведите примеры маршрутизаторов отечественного производства. Каковы их особенности?

2. К какому типу относится протокол OSPF?

3. Может ли работать маршрутизатор, не имея таблицы маршрутизации?

4. Какие параметры сети учитывают метрики, поддерживаемые протоколом OSPF?

[12] Компьютерные сети. Принципы, технологии, протоколы.

Раздел IV. ТЕХНОЛОГИИ ГЛОБАЛЬНЫХ СЕТЕЙ

Тема 12. Технология IP в глобальных сетях

Семинар: Организация и услуги глобальных сетей

Семинар посвящён изучению организации и услуг глобальных сетей. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области технологии IP в глобальных сетях.
2. Расширение научных представлений обучающихся о технологии IP в глобальных сетях.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Сети операторов связи.
2. Организация Интернета.
3. Многослойное представление технологий и услуг глобальных сетей.
4. Облачные сервисы.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания о технологии IP в глобальных сетях.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь организации и услуг глобальных сетей с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 18 «Организация и услуги глобальных сетей» учебного пособия[13].

2. Изучить особенности технологии IP в глобальных сетях.

3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Изобразите структурную схему глобальной сети.

Задание 2. Создайте папку с облачным хранением данных. Включите совместный доступ, ограничив пользователей только режимом просмотра. Ограничьте время действия ссылки одним днём. Результат продемонстрируйте преподавателю.

Вопросы для самоконтроля:

1. Какие услуги предоставляют операторы связи?
2. Как строятся взаимоотношения между операторами связи?
3. Охарактеризуйте организацию Интернета.
4. В чем разница между технологиями «IP поверх OTN» и «IP поверх DWDM»?

Тема 13. Технологии удалённого доступа

Семинар: Схемы удалённого доступа. Мультиплексирование информации

Семинар посвящён изучению схемы удалённого доступа и мультиплексированию информации. Занятия проводятся в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области технологии удалённого доступа.
2. Расширение научных представлений обучающихся о технологии удалённого доступа.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Организация удалённого доступа «проблема последней мили».
2. Коммутируемый аналоговый доступ.
3. Модемы.
4. Технология ADSL.
5. Пассивные оптические сети.
6. Технология MPLS.

[13] Компьютерные сети. Принципы, технологии, протоколы.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания о технологии удалённого доступа.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь схемы удалённого доступа, мультиплексирования информации с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 19 «Транспортные технологии глобальных сетей», главы 20 «Технология MPLS» учебного пособия[14].
2. Изучить особенности технологии удалённого доступа.
3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. В чём принципиальное отличие доступа через ADSL от коммутируемого доступа. Изобразите схему отличия условий работы ADSL-модемов от обычных модемов.

Задание 2. Скорость передачи данных через ADSL-соединение равна 128000 бит/с. Через данное соединение передают файл размером 625 кбайт. Определить время передачи файла в секундах.

Задание 3. Скорость передачи данных через ADSL-соединение равна 512 000 бит/с. Передача файла через это соединение заняла 1 минуту. Определить размер файла в килобайтах.

Задание 4. С помощью модема установлена связь с другим компьютером со скоростью соединения 19 200, с коррекцией ошибок и сжатием данных.

Можно ли при таком соединении файл размером 2,6 кбайт передать за 1 секунду? Обоснуйте свой ответ.

Всегда ли при таком соединении файл размером 2,3 кбайт будет передаваться за 1 секунду? Обоснуйте свой ответ.

[14] Компьютерные сети. Принципы, технологии, протоколы.

Можно ли при таком соединении оценить время передачи файла размером 4 Мб? Если можно, то каким образом?

Вопросы для самоконтроля:

1. Что понимается под термином «Проблема последней мили»?
2. Что такое «Пассивная оптическая сеть»?
3. Охарактеризуйте суть технологии MPLS.
4. Поясните, каким образом можно повысить скорость технологии ADSL.

Раздел V. ТЕХНОЛОГИИ ПРИКЛАДНОГО УРОВНЯ

Тема 14. Защита сетевого трафика

Семинар: Атаки на транспортную инфраструктуру сети

Семинар посвящён изучению атак на транспортную инфраструктуру сети. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области защиты сетевого трафика.
2. Расширение научных представлений обучающихся о защите сетевого трафика.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.
5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. TCP-атака: затопление SYN-пакетами.
2. TCP-атака: подделка TCP-сегмента.
3. TCP-атака: сброс TCP-соединения.
4. ICMP-атаки.
5. UDP-атаки.
6. IP-атаки.
7. Атаки на DNS.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания о защите сетевого трафика.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь уязвимостей и методов защиты транспортной инфраструктуры сети с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Изучить содержание лекции «Сервис защищённого канала. Шифрование в протоколе IPSec».

2. Проработать материал главы 29 «Атаки на транспортную инфраструктуру сети» учебного пособия[15].

3. Изучить уязвимости и методы защиты транспортной инфраструктуры сети.

4. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Установите соответствие следующих терминов на русском языке (ущерб; уязвимость; вредоносное ПО; доступность; целостность; подмена содержимого пакета; распределенная атака, «отказ в обслуживании») и английском языке (Denial of Service; availability; integrity; vulnerability; malware; impact; spoofing; DDoS).

Задание 2. Что означает данный список доступа: access-list 2 permit 93.8.25.2 0.0.0.0 access-list 2 deny 93.8.25.0 0.0.0.255?

Вопросы для самоконтроля:

1. Назовите разновидности TCP-атак.
2. Что является целью сетевой разведки?
3. В чём суть сканирования сети и сканирования портов?
4. Какие существуют методы защиты служб DNS?

Практическое занятие: Моделирование атаки MAC-spoofing (в среде Cisco Packet Tracer)

Краткие теоретические сведения

Одна из наиболее простых в реализации сетевых атак ― MAC-spoofing (подмена MAC-адреса). Это атака канального (L2) уровня, заключающаяся в том, что на сетевой карте изменяется MAC-адрес на совпадающий с адресом другого устройства в сети.

В таблице MAC-адресов коммутатора запись с атакованным MAC-адресом будет соотнесена с интерфейсом, на котором в последний раз был идентифицирован фрейм с данным MAC-адресом в качестве источника.

Как результат — до поступления фрейма с атакуемого устройства все данные коммутатор в соответствии со своей таблицей MAC-адресов будет пересылать на атакующее устройство.

Подобная атака может привести к нестабильной работе сети, недоступности узла, вывести из строя важный элемент инфраструктуры. Например, если в качестве атакуемого устройства будет контроллер домена, его недоступность приведет к невозможности регистрации (входа) пользователей в сети.

Подмена может осуществляться нарушителем и в иных целях, например, для обхода блокировок доступа на уровне сетевых идентификаторов (MAC filtering).

[15] Компьютерные сети. Принципы, технологии, протоколы.

Атаку можно предотвратить при помощи функции port-security коммутатора. Функцию port-security поддерживают коммутаторы Cisco, аналогичные функции есть также и у коммутаторов других производителей.

Для каждого порта можно ограничивать количество и/или задавать список MAC-адресов, которые на нем могут появляться.

В случае нарушения безопасности возможны различные сценарии поведения коммутатора, которые задаются следующими режимами:

— protect — фреймы с неизвестным MAC-адресом отправителя отбрасываются, как и фреймы с безопасных MAC-адресов, если число этих адресов превышает установленные ограничения; оповещения о нарушении безопасности нет;

— restrict — идентичен режиму protect за тем исключением, что коммутатор отправляет оповещение о нарушении по SNMP, кроме того, записывает информацию в syslog (если настроен) и ведет счетчик нарушений;

— shutdown — помимо оповещений и записи в syslog, порт-интерфейс переводится в состояние error-disabled и немедленно выключается.

Указания по выполнению практического задания

Практическое задание выполняется в среде эмулятора сетевого оборудования Cisco Packet Tracer.

Cisco Packet Tracer — самый известный симулятор оборудования компании Cisco. Симулятор имитирует работу оригинального программного обеспечения (ПО), но им не является. ПО симулятора содержит существенные упрощения и реализует не все функциональные возможности операционной системы (ОС). Это относится как к системному ПО сетевого оборудования, так и к эмуляции конечных точек. Поэтому эмулятор можно использовать только для воспроизведения внешнего поведения исследуемых объектов.

Несмотря на существенные ограничения, в среде Cisco Packet Tracer можно смоделировать атаку типа MAC-spoofing и рассмотреть меры противодействия ей.

Технология выполнения

Задание 1. Создайте модель сети из трех конечных устройств, изучите работу коммутатора с MAC-адресами.

1. Создайте виртуальную машину под управлением ОС Windows (32-разрядная версия), назначив ей не менее 2 Гб оперативной памяти. Создайте для машины общую папку, поместите в нее установочный файл Cisco Packet Tracer 6.3, полученный от преподавателя.

2. Установите на виртуальной машине Cisco Packet Tracer, после установки зайдите в него, использовав гостевой вход **Guest Login**. Через 15 секунд нажмите **Confirm Guest**.

3. Выбирая нужные устройства и интерфейсы на нижней панели инструментов Cisco Packet Tracer (рис. 14.1), постройте следующую модель сети: два конечных устройства (компьютера) соединены медным проводом через коммутатор (рис. 14.2). В качестве коммутатора выбирайте устройство **2960**.

Для создания сетевого интерфейса на нижней панели выберите тип.

Интерфейсы (значок в виде молнии), а затем сплошную прямую линию (медный провод Copper Straight-Through). Затем щелкните мышью на значке

подключаемого к сети компьютера, выберите FastEthernet0 и затем щелкните на значке коммутатора. В открывшемся окне выберите название интерфейса (например, FastEthernet0/1 для первого компьютера).

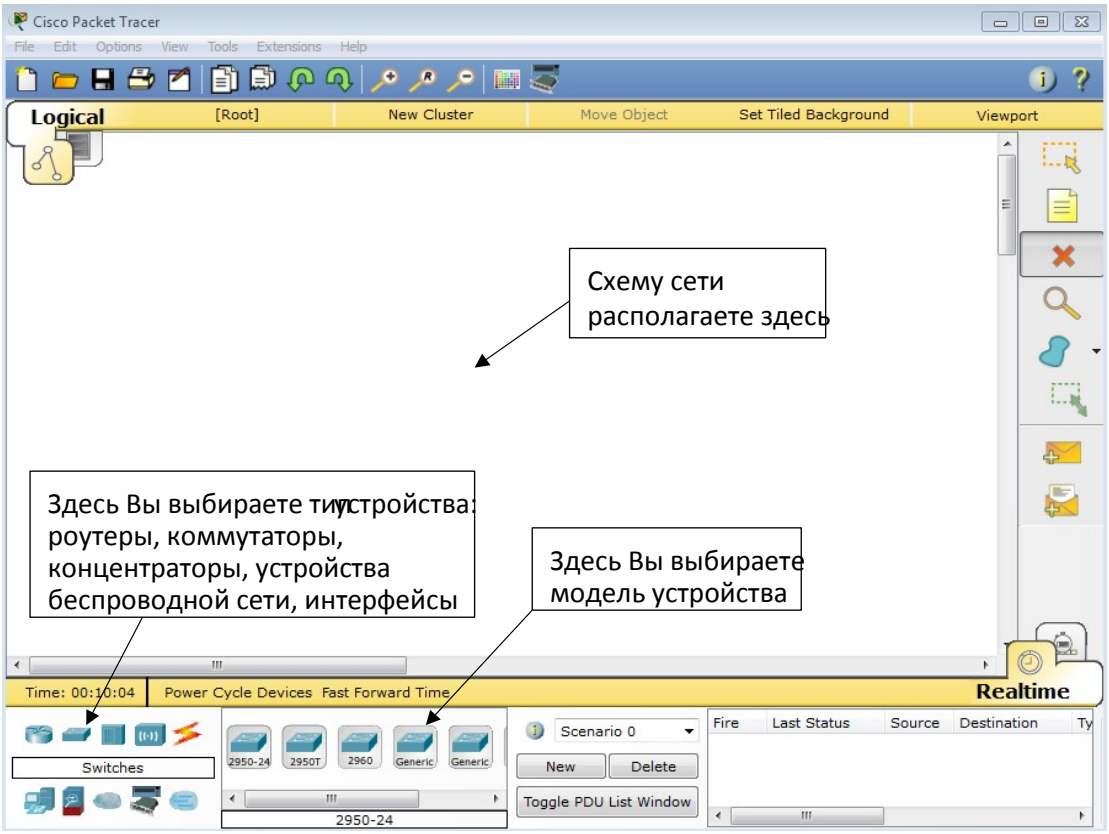


Рис. 14.1. Интерфейс программы Cisco Packet Tracer

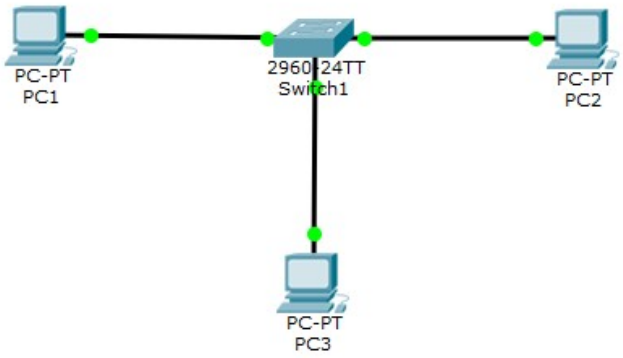


Рис. 14.2. Схема простейшей сети

Задайте для конечных точек (компьютеров) сети статическую IP-адресацию. Все адреса должны принадлежать одной подсети, например, 192.168.X.Y с маской 255.255.255.0, где X — номер варианта, Y — номер компьютера в сети.

Например, зададим для первой машины IP-адрес 192.168.1.1, для второй — 192.168.1.2, а для третьей — 192.168.1.3; все адреса находятся в одной подсети 192.168.1.0/24 (маска 255.255.255.0).

Для того чтобы получить доступ к настройкам устройства, щелкните на нем мышью, а затем перейдите на вкладку *Config*. Для задания IP-адреса выберите вкладку *FastEthernet0* группы INTERFACE (рис. 14.3).

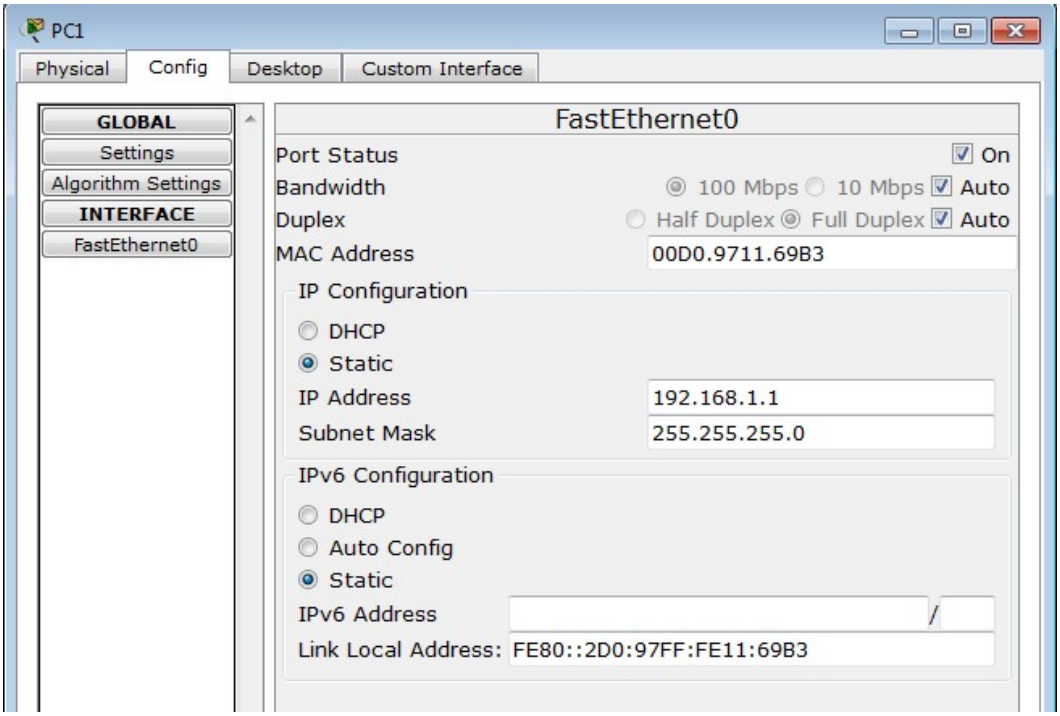


Рис. 14.3. Пример сетевых настроек первого компьютера

Итак, все узлы физически подключены к одному коммутатору и находятся в одной IP-сети (192.168.1.0/24).

4. Проверьте содержимое таблицы MAC-адресов на коммутаторе.

Откройте окно свойств коммутатора, щелкнув на нем мышью. Перейдите на вкладку CLI и нажмите кнопку Enter для активации командной строки управления коммутатором. Должно появиться приветствие вида Switch>.

После приветствия введите команду sh mac-address-table.

Таблица MAC-адресов пока не заполнена (рис. 14.4).

5. Проверьте возможность установки сетевого соединения между узлами.

Для моделирования сетевого взаимодействия в режиме реального времени откройте свойства первого компьютера, перейдите на вкладку *Desktop* и откройте окно командной строки **Command Prompt**. Пошлите ping-запрос ко второму компьютеру, введя команду ping с его IP-адресом (рис. 14.5). В случае успешного соединения пакеты не будут потеряны.

Проверьте наличие связи между всеми компьютерами, «пропинговав» с каждого из них два других. Убедитесь, что существует связь между всеми тремя компьютерами.

Сделайте скриншот одного из командных окон.

6. Повторно проверьте содержимое таблицы MAC-адресов на коммутаторе. Теперь таблица должна содержать MAC-адреса всех компьютеров (рис. 14.6). Сделайте скриншот этой таблицы для отчета.

7. Сохраните настроенную модель сети в файл с вашим ФИО, выполнив команду **File/Save**.

8. Сохраните настроенную модель сети в файл с новым именем (ваше ФИО_MAC_spoofing), выполнив команду **File/Save as**. Последующие изменения будем производить и сохранять уже в этом файле.

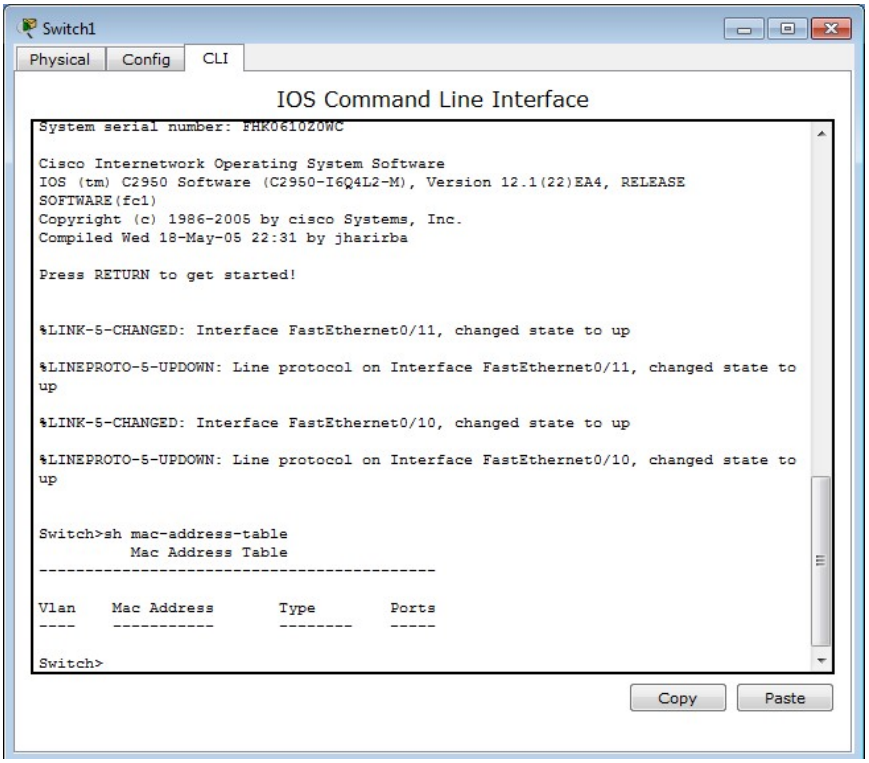


Рис. 14.4. Начальное состояние таблицы MAC-адресов на коммутаторе (таблица пуста)

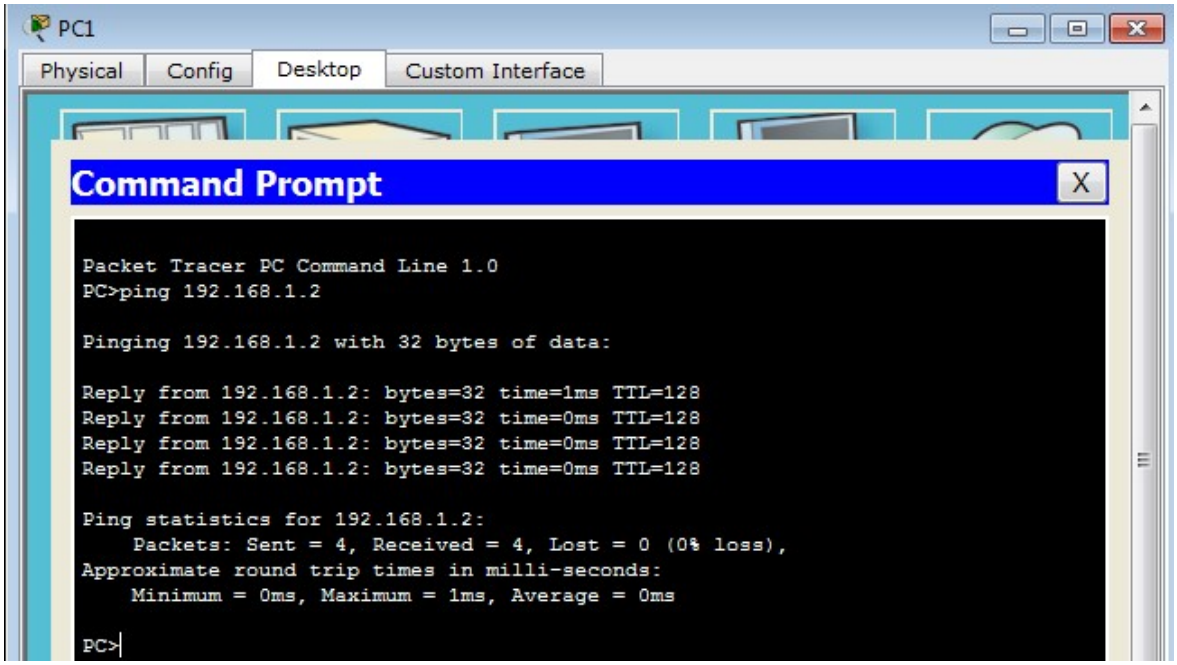


Рис. 14.5. Проверка связи первого компьютера со вторым

```
Switch>sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.9711.69b3    DYNAMIC     Fa0/1
   1    00d0.ffdd.0060    DYNAMIC     Fa0/3
   1    00d0.ffdd.0062    DYNAMIC     Fa0/2
Switch>
```

Рис. 14.6. Пример таблицы MAC-адресов устройств в сети

Задание 2. Реализуйте атаку MAC-spoofing, подменив MAC-адрес компьютера злоумышленника.

1. Выберите компьютер, который будет играть роль компьютера злоумышленника. Пусть, например, это будет компьютер 3.

2. Выберите другой компьютер — «жертву». Пусть, например, это будет компьютер 2.

3. Определите MAC-адрес компьютера-«жертвы». Поскольку таблица MAC-адресов содержит только названия интерфейсов, посмотрите, к какому порту коммутатора подключен компьютер-«жертва».

На схеме сети посмотреть названия интерфейсов можно, наведя указатель мыши на значок зеленой точки рядом с коммутатором (но не нажимая на нее!). В рассматриваемом примере интерфейс, с помощью которого компьютер 2 подключен к коммутатору, — Fa0/2. Согласно рис. 14.6, получаем, что MAC-адрес этого компьютера — 00d0.ffdd.0062.

Установите это значение в качестве MAC-адреса компьютера 3, играющего роль злоумышленника (Свойства, вкладка *Config/ FastEthernet0*).

Значение адреса можно скопировать из окна командной строки коммутатора.

4. «Пропингуйте» теперь с машины злоумышленника оставшийся компьютер (компьютер 1). Затем попробуйте «пропинговать» с оставшегося компьютера (компьютер 1) компьютер-«жертву» (компьютер 2). Компьютер-«жертва» перестал отвечать (рис. 14.7). **Сделайте скриншот.**

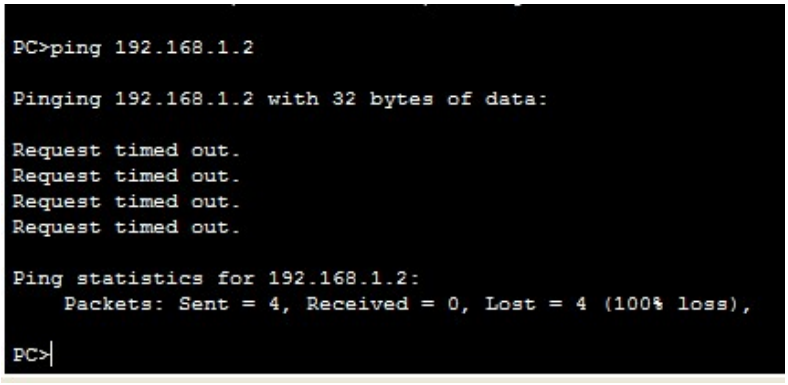


Рис. 14.7. Проверка связи с компьютером-«жертвой» после подмены MAC-адреса злоумышленником («жертва» не отвечает)

5. Просмотрите таблицу MAC-адресов на коммутаторе. Какие изменения в ней произошли?

Как видно на рисунке 14.8, в рассматриваемом примере запись, соответствующая компьютеру 2, была перезаписана новой записью, в которой указан интерфейс компьютера злоумышленника (Fa0/3). **Сделайте скриншот таблицы MAC-адресов.**

Таким образом, атака MAC-spoofing реализована. Компьютер-«жертва» стал не доступен в сети.

6. «Пропингуйте» с компьютера-«жертвы» (компьютер 2) оставшийся компьютер (компьютер 1). Потом попробуйте провести пинг в обратном направлении. Теперь компьютер-«жертва» опять доступен. Проверьте, что таблица MAC-адресов на коммутаторе приняла исходный вид.

```
Switch>sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.9711.69b3    DYNAMIC     Fa0/1
   1    00d0.ffdd.0060    DYNAMIC     Fa0/3
   1    00d0.ffdd.0062    DYNAMIC     Fa0/3
Switch>
```

Рис. 14.8. Перезапись MAC-адреса на коммутаторе

7. На компьютере злоумышленника откройте свойства, вкладку *Desktop*, *Traffic Generator*. Укажите в качестве типа трафика PING, *Destination IP Address* — IP-адрес оставшегося компьютера (компьютер 1), *Source IP Address* — IP-адрес компьютера злоумышленника. Введите произвольный номер в поле *Sequence Number*, установите переключатель в позицию *Periodic* и интервал в 1 с (рис. 14.9). Нажмите **Send**.

Теперь пинг с компьютера злоумышленника будет осуществляться постоянно (пока не будет остановлен в окне генерации трафика *Traffic Generator*).

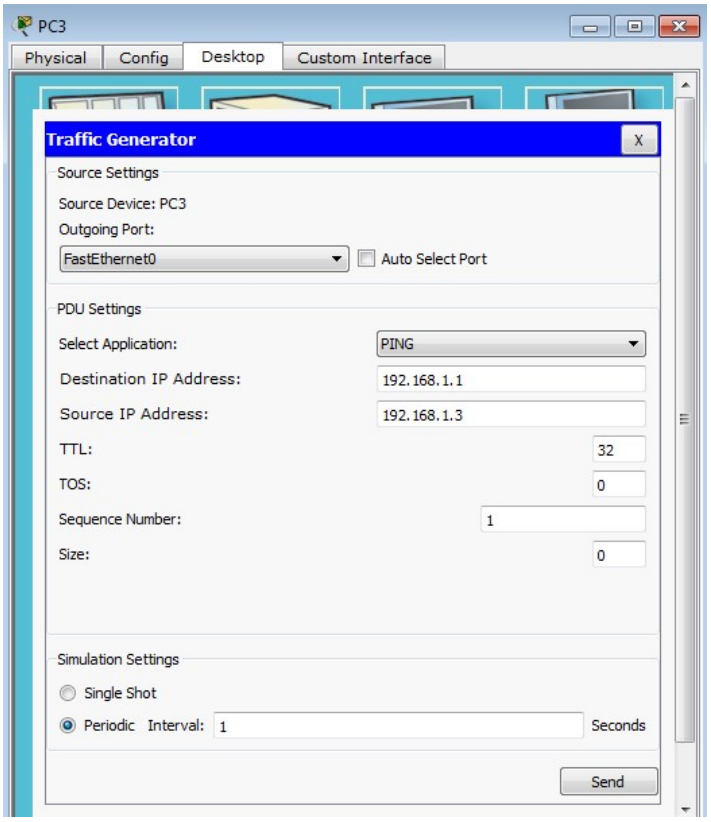


Рис. 14.9. Настройка генерации трафика

8. Проверьте, что теперь компьютер-«жертва» недоступен вне зависимости от того, посылает ли он пакеты оставшемуся компьютеру.

9. Остановите генерацию трафика компьютером злоумышленника, нажав **Stop** в окне *Traffic Generator*.

Задание 3. На коммутаторе настройте функцию port-security, обеспечивающую защиту от атак типа MAC-spoofing.

1. Откройте ранее сохраненный файл с «чистой» моделью сети (без подмены MAC-адресов).

2. Откройте интерфейс командной строки коммутатора. Войдите в режим редактирования, нажав Enter. Настройте «липкие адреса», привязав к каждому порту определенный MAC-адрес. Данные с других MAC-адресов будут портом блокироваться.

Перейдите в режим настройки коммутатора, набрав команду *ena*.

Приветствие коммутатора изменится с вида *Switch>* на *Switch#*.

Войдите в режим изменения конфигурации *conf t*.

Приветсвие коммутатора изменится на *Switch(config)#.*

Укажите, что будут настраиваться сразу все интерфейсы, — задайте диапазон интерфейсов (указав те номера интерфейсов, которые использованы в Вашей модели сети).

Пример: *interface range fastethernet0/1-3.*

Если номера интерфейсов идут не последовательно, интерфейсы указываются через запятую (например, *interface range fastethernet0/1, fastethernet0/11*).

Все последующие настройки будут применяться к каждому интерфейсу из заданного диапазона. Коммутатор показывает это, изменив подсказку на *Switch(config-if-range)#.*

Укажите для этих интерфейсов динамические (sticky) MAC-адреса, которые будут привязываться к порту *switchport port-security mac-address sticky*.

Укажите, что к порту может быть подключен максимум 1 MAC-адрес *switchport port-security maximum 1*.

Укажите режим работы port-security, позволяющий блокировать данные, поступающие с непривязанного MAC-адреса *switchport port-security violation protect*. Укажите режим, совместимый с *port-security switchport mode access* Включите сделанные настройки *switchport port-security*.

Сохраните сделанные настройки *do wr.*

3. Просмотрите сделанные настройки, выполнив команду *do sh run.*

Будет выдана конфигурация коммутатора, в которой должны быть записи, похожие на записи на рис. 14.10.

Для того чтобы не просматривать конфигурацию до конца, можно нажать Ctrl + X.

4. «Пропингуйте» все компьютеры между собой.

5. Повторно просмотрите конфигурацию коммутатора (do sh run) и убедитесь, что в конфигурацию добавились конкретные значения MAC-адресов (рис. 14.11). **Сделайте скриншот.**

6. Просмотрите таблицу MAC-адресов командой *do sh mac-address-table.*

7. Попробуйте повторить атаку MAC-spoofing, задав компьютеру злоумышленника MAC-адрес компьютера-«жертвы», а затем «пропинговав» с машины злоумышленника оставшийся компьютер.

Что произошло? **Сделайте скриншот.**

Злоумышленник не может осуществить сетевое взаимодействие. Это происходит потому, что поступающие фреймы, содержащие MAC-адрес, отличный от привязанного к порту «липкого» адреса, блокируются.

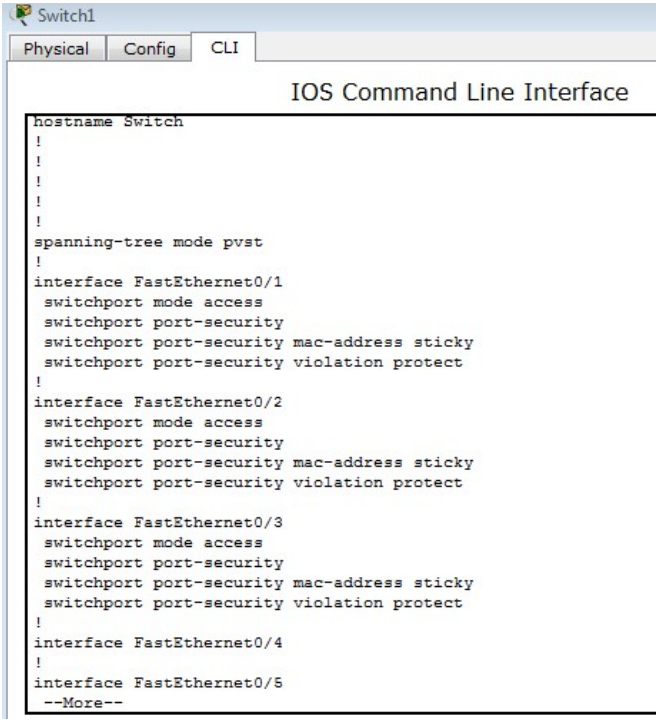


Рис. 14.10. Конфигурация коммутатора с включенной функцией port-security

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation protect
 switchport port-security mac-address sticky 00D0.9711.69B3
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation protect
 switchport port-security mac-address sticky 00D0.FFDD.0062
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation protect
 switchport port-security mac-address sticky 00D0.FFDD.0060
```

Рис. 14.11. «Липкие» адреса заданы

8. Просмотрите еще раз таблицу MAC-адресов на коммутаторе и убедитесь, что она не изменилась. **Сделайте скриншот окна команд коммутатора.**

9. Попробуйте изменить MAC-адрес компьютера злоумышленника на произвольное значение, отличное от заданного в таблице коммутатора. Убедитесь, что сетевое взаимодействие для этого компьютера по-прежнему не возможно.

Таким образом, функция port-security предотвращает как проведение атак на основе подмены MAC-адреса, так и подключение к сети неизвестных устройств.

10. Оформите отчет по выполнению практического задания согласно приложениям 1, 2.

Вопросы для самоконтроля:

1. Для чего нужна таблица MAC-адресов?
2. Как осуществляется настройка коммутатора?
3. Какая функция предотвращает проведение атак на основе подмены MAC-адреса и подключение к сети неизвестных устройств?

Тема 15. Протоколы и службы сети Microsoft

Практическое занятие: Атаки на протоколы DNS (DNS-Spoofing) и TLS (подмена сертификатов) и методы защиты от них

Цель работы: ознакомиться с проблемами безопасности веб-протоколов, которые могут возникнуть при реализации MITM-атаки («человек посередине»), а также возможными направлениями защиты.

Теоретический материал

Существует множество способов реализации MITM-атаки, в частности, в рамках локальной сети это может быть ARP Spoofing или DNS Spoofing. Однако в данной практической работе способы реализации MITM атаки не рассматриваются, а для простоты лишь эмулируется ситуация этой атаки, когда трафик проходит через атакующий узел. Это достигается путем использования атакующей машины (Kali Linux) в качестве шлюза для подключения к сети Интернет.

Указания по выполнению практической работы

Работа выполняется в виртуальной тестовой среде с использованием гипервизора Oracle Virtual Box.

Результаты выполнения практической работы оформляются в виде отчета, который должен содержать скриншоты основных этапов работы с необходимыми пояснениями и ответы на контрольные вопросы.

Материал предоставлен исключительно в учебных целях и не рекомендован к использованию в реальных системах. Помните, что действия по несанкционированному изменению компьютерной информации уголовно наказуемы (глава 28 УК РФ[16]).

Технология выполнения

Задание 1. Свяжите две виртуальные машины в локальную сеть так, чтобы одна из них (под управлением ОС Kali Linux) выполняла роль шлюза для выхода в Интернет.

1. Создайте две виртуальные машины под управлением ОС Windows и под управлением ОС Kali Linux. На Windows-машину дополнительно установите браузеры Mozilla FireFox и Chrome.

2. Свяжите созданные машины в локальную сеть.

В сетевых настройках виртуальной Windows-машины установите значение *Внутренняя сеть*. Запустите Windows-машину.

Посмотрите IP-адрес, назначенный Windows-машине по умолчанию командой *ipconfig.* Задайте статическую адресацию компьютера, например, из стандартной подсети 192.168.0.0 с маской 255.255.255.0.

Для этого откройте Центр управления сетями и общим доступом и перейдите по ссылке *Подключение по локальной сети*. В окне просмотра состояния

[16] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 09.03.2022). Нормативно-правовые акты приведены в соответствии с данными официального интернет-портала правовой информации Pravo.gov.ru (дата обращения: 12.01.2023).

подключения нажмите **Свойства**, затем выберите IPv4 и также откройте его **Свойства**.

Установите переключатель в позицию *Использовать следующий IP-адрес* и задайте IP-адрес машины (например, 192.168.0.1), маску подсети, в качестве шлюза укажите другой IP-адрес из этой подсети (например, 192.168.0.2). В качестве DNS сервера можно указать 8.8.8.8 (рис. 15.1).

Сохраните сделанные настройки, а потом проверьте назначенные параметры с помощью команды *ipconfig*.

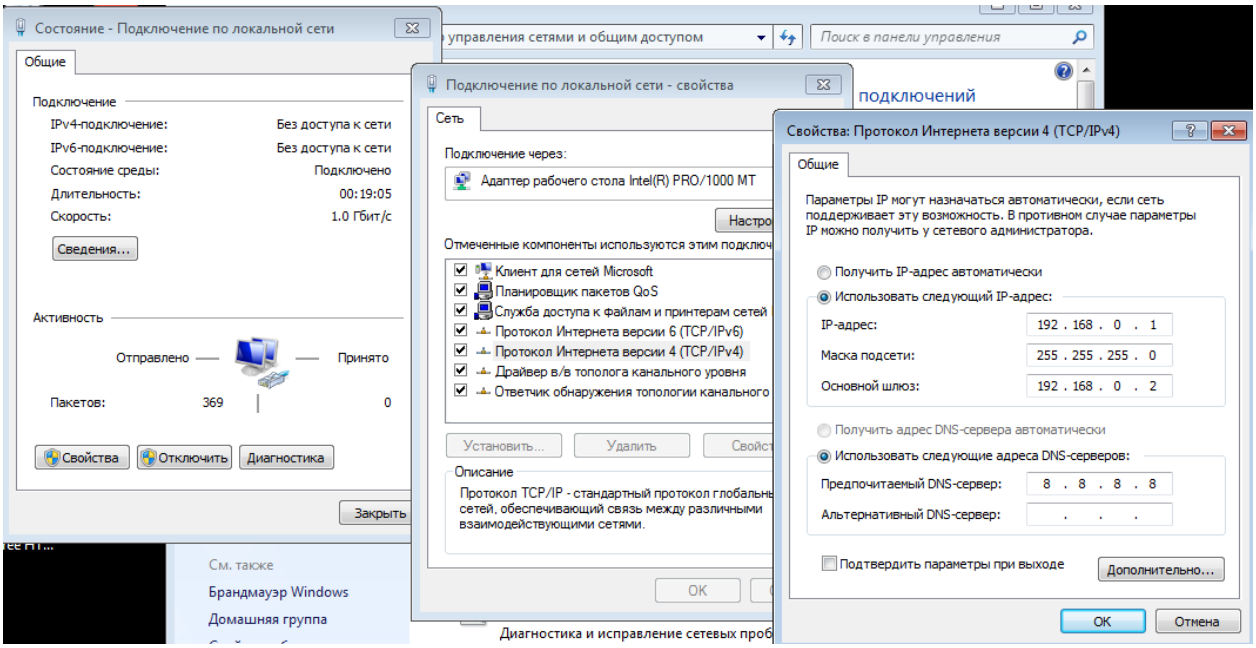


Рис. 15.1. Пример настройки IP-адресации в ОС Windows

В сетевых настройках виртуальной машины Kali Linux установите для первого адаптера значение *Сетевой мост*, включите второй адаптер и установите для него значение *Внутренняя сеть*. Запустите машину. В случае если сетевой интерфейс не включен, включите его.

Убедитесь, что с Kali-машины имеется доступ в Интернет, открыв какой-нибудь сайт в браузере или «пропинговав» его из командной строки, например, *ping ya.ru*.

Посмотрите назначенные по умолчанию IP-адреса командой *ip a*.

Для машины должны быть определены два сетевых интерфейса (eth0 и eth1), причем для первого из них задан IP-адрес — это внешний интерфейс для выхода в Интернет, а для второго IP-адрес не определен (рис. 15.2).

Для второго интерфейса задайте статическую IP-адресацию, назначив IP-адрес, который ранее был указан в качестве адреса шлюза для Windows-машины. Это можно сделать в графическом режиме — из меню Kali выберите пункт **Settings**, а затем **Advanced Network Configuration**.

В окне настроек добавьте новый интерфейс, щелкнув на значке «+», выберите тип подключения *Ethernet* и нажмите **Create…**

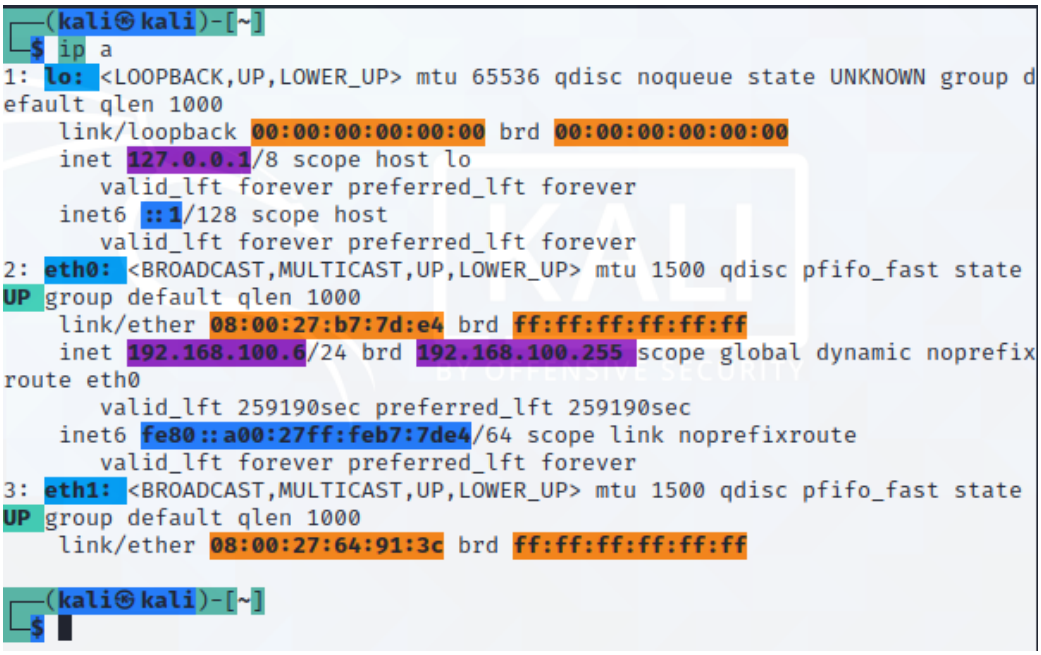


Рис. 15.2. Просмотр IP-адресов в ОС Kali Linux

В открывшемся окне настроек задайте название соединения (например, *Ethernet connection*), перейдите на вкладку *IPv4Settings* (рис. 15.3):

– выберите метод *Manual*;

– нажмите **Add** и задайте IP-адрес (например, 192.168.0.2) и маску подсети (например, 24).

Сохраните сделанные настройки, нажав **Save.**

Проверьте сделанные настройки, выполнив в команде команду *ip a.*

«Пропингуйте» обе машины (Kali с Windows и наоборот) по их IP-адресу и убедитесь, что осуществляется сетевое взаимодействие между ними.

Настройте на машине Kali Linux маршрутизацию пакетов (forwarding) для того, чтобы Windows-машина могла выходить через нее в Интернет.

В ОС Kali Linux отредактируйте содержимое файла /etc/sysctl.conf, для этого можно использовать простой редактор nano:

nano /etc/sysctl.conf.

В этом файле надо найти и раскомментировать строку (рис. 15.4)

net.ipv4.ip_forward=1.

Затем следует нажать Crtl + O для сохранения изменений и Ctrl + X для выхода из редактора (подсказка по командам выводится внизу окна редактора).

Если разрешения на модификацию файла отсутствуют (в новых версиях Kali), надо до начала редактирования файла поднять права до root, выполнив команду *sudo su* (или *sudo -i*).

Чтобы изменения в файле sysctl.conf вступили в силу, выполните команду *sysctl -p /etc/sysctl.conf.*

Проверьте, что перенаправление пакетов включено, убедившись, что системный параметр */proc/sys/net/ipv4/ip_forward* имеет значение 1. Если значение параметра не было выдано на экран после выполнения предыдущей команды, его можно посмотреть следующим образом:

cat /proc/sys/net/ipv4/ip_forward.

Рис. 15.3. Задание сетевых настроек в Kali Linux

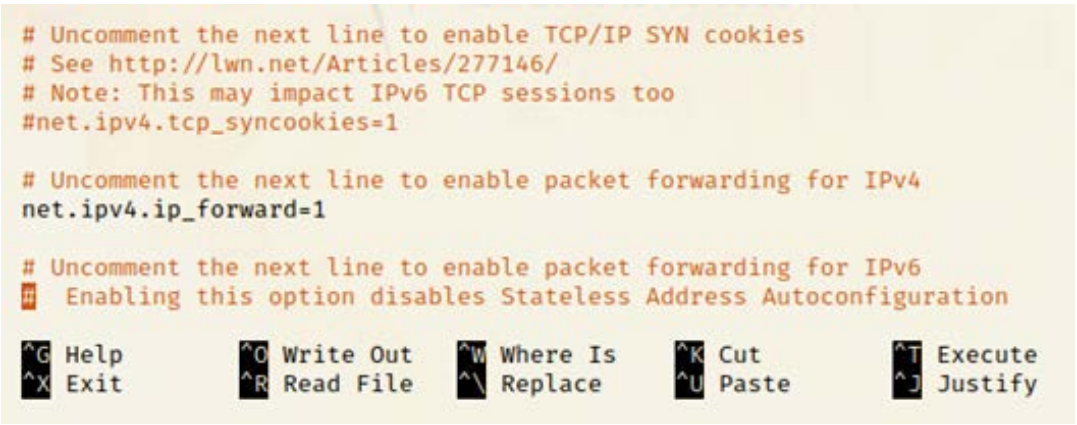


Рис. 15.4. Настройка перенаправления пакетов

Установите для сетевой карты внутренней сети неразборчивый режим — в сетевых настройках виртуальной машины Kali Linux для адаптера, имеющего тип подключения *Внутренняя сеть*, раскройте список *Дополнительно* и в строке *Неразборчивый режим* выберите значение *Разрешить все*.

Настройте на машине Kali Linux NAT для трансляции внутренних адресов локальной сети во внешний адрес. Это можно сделать с помощью встроенного межсетевого экрана *iptables* (требуются root-права):

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE.

Проверьте, что указанные правила были добавлены, выполнив

iptables -t nat –L.

Сохраните настройки iptables, чтобы созданное правило действовало после перезагрузки. Для этого сохраните правила в файл (например, в файл /etc/iptables.rules):

iptables-save > /etc/iptables.rules.

Просмотреть содержимое созданного файла можно с помощью команды *cat /etc/iptables.rules.*

Кроме того, в конец файла /etc/network/interfaces следует дописать строку

post-up iptables-restore < /etc/iptables.rules.

Проверьте, что с Windows-машины имеется выход в Интернет.

Если все настройки сделаны правильно, Windows-машина получит доступ в Интернет через шлюз, в роли которого выступает машина Kali Linux. То есть весь Интернет трафик для Windows-машины идет через шлюз.

Задание 2. Реализуйте атаку подмены DNS-трафика и изучите действие механизма защиты HSTS.

Установите на Kali Linux утилиту dns2proxy (требуются root-права):

Определите версию языка python, которая установлена в вашей версии ОС:

python –V.

Найдите на сайте pkgs.org пакет dnspython, выберите версию ОС (для версии Kali Linux 2020.4 с python 2.7 можно выбрать, например, Debian 10) и подходящую версию пакета, скачайте deb-пакет.

В графическом интерфейсе Kali Linux откройте расположение пакета, щелкните на пакете правой кнопкой мыши и выберите **Copy Location**. Перейдите в терминал и выполните команду

apt install <путь/пакет>,

вставив скопированный путь к пакету.

Найдите на сайте pkgs.org пакет pcapy, выберите версию ОС и подходящую версию пакета, скачайте и установите deb-пакет.

Установите утилиту dns2proxy, выполнив

git clone https://github.com/singe/dns2proxy.git.

Задайте необходимое для работы утилиты правило iptables:

iptables -t nat -A PREROUTING -p udp --destination-port 53 -j REDIRECT --to-port 53.

Трафик, поступающий на порт 53, будет перенаправляться обратно на этот же порт 53. DNS теперь работать не будет.

Проверьте, что с Windows-машины теперь невозможно выйти в Интернет.

После установки dns2proxy перейдите в каталог утилиты

cd dns2proxy/.

Запустите утилиту dns2proxy из текущего каталога

python ./dns2proxy.

Проверьте, что с Windows-машины можно выйти в Интернет, а на Kali-машине отображаются DNS-запросы на посещение сайтов и соответствующие им DNS ответы с IP-адресами.

Откройте разные сайты и посмотрите, какая информация выводится dns2proxy. Обратите внимание, что, кроме запросов браузера на посещение открываемых ресурсов, DNS-запросы может посылать и другое ПО, например, в ходе обновления.

Осуществите атаку подмены DNS. Например, можно подменить какой-либо сайт на страницу, сообщающую о блокировке сайта.

Откройте в браузере сайт, который вы будете подменять, чтобы точно определить используемое на нем доменное имя (например, unecon.ru).

Откройте в браузере сайт, который будет отображаться вместо первого (например, noumei.ru). «Пропингуйте» это доменное имя, чтобы определить соответствующий IP-адрес (например, 77.222.61.44).

Как вариант, для подмены можно использовать незащищенную страницу сообщения о блокировке ресурса (например, warning.rt.ru с IP-адресом 95.167.13.51 или 185.37.129.10).

В браузере Chrome отключите защиту: в меню браузера выберите **Настройки/ Конфиденциальность и безопасность/ Безопасность**, в группе *Дополнительные* выключите опцию *Использовать безопасный DNS-сервер* (рис. 15.5). При необходимости дополнительно можно отключить защиту в группе *Безопасный просмотр*.

Остановите утилиту dns2proxy. Измените конфигурационный файл domains.cfg утилиты dns2proxy (файл находится в каталоге dns2proxy). В этом файле следует указать имя домена, для которого будет осуществляться подмена DNS и IP-адрес ресурса, который будет выдаваться вместо исходного сайта (рис. 15.6).

Сделайте замены для 2–3 сайтов.

Сохраните изменения в файле domains.cfg и запустите dns2proxy.

Закройте сайт, который будет подменяться в браузере Windows-машины, если он был открыт.

Очистите кеш браузера:

– в Chrome очищается при очистке истории;

– в FireFox достаточно перезапустить браузер, если в настройках браузера на вкладке *Приватность и защита* стоит флажок *Удалять куки и данные сайтов при закрытии FireFox*, в противном случае там же в настройках надо нажать **Удалить данные**.

Протестируйте открытие подменяемого сайта в разных браузерах, включая устаревший (Internet Explorer) (рис. 15.7).

Таким образом, злоумышленник может перенаправить соединение на фишинговый сайт. Кроме того, он может, например, заблокировать сервер обновлений, чтобы предотвратить обновление ПО с целью эксплуатации известных уязвимостей.

Методы защиты. В ряде случаев (при использовании для подмены сайта, требующего подключения по HTTPS) будут выдаваться сообщения об ошибке (рис. 15.8).

Это действует защитный механизм, называемый HSTS (HTTP Strict Transport Security), который позволяет сайтам уведомить браузер о том, что доступ к ним должен осуществляться только по протоколу HTTPS. HSTS нацелен на предотвращения атак с перехватом соединения и понижением степени защиты с HTTPS до открытого протокола HTTP. Кроме того, большинство современных браузеров использует список сайтов (HSTS preload list), требующих подключения по протоколу HTTPS.

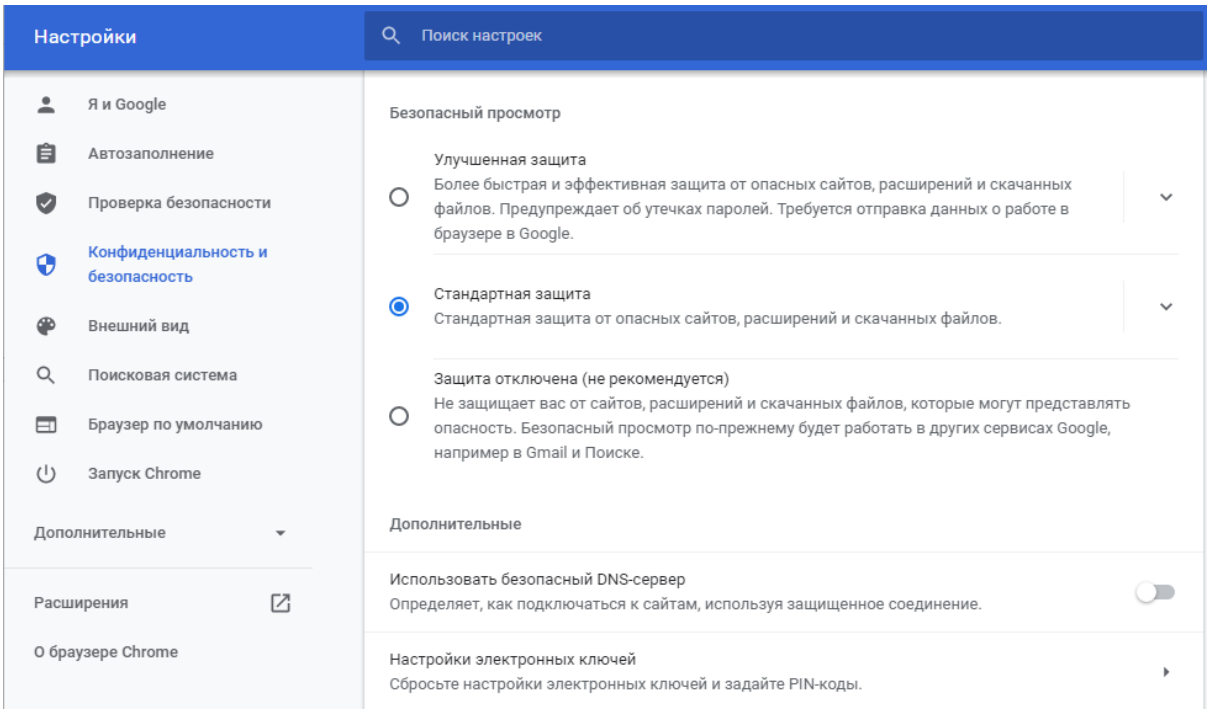


Рис. 15.5. Отключение сервиса безопасности DNS

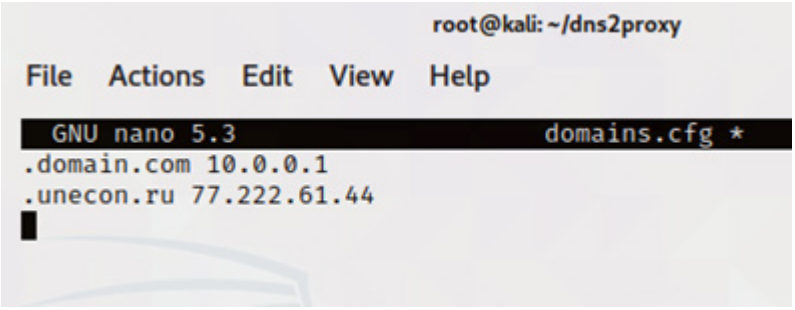


Рис. 15.6. Пример конфигурирование dns2proxy для подмены DNS

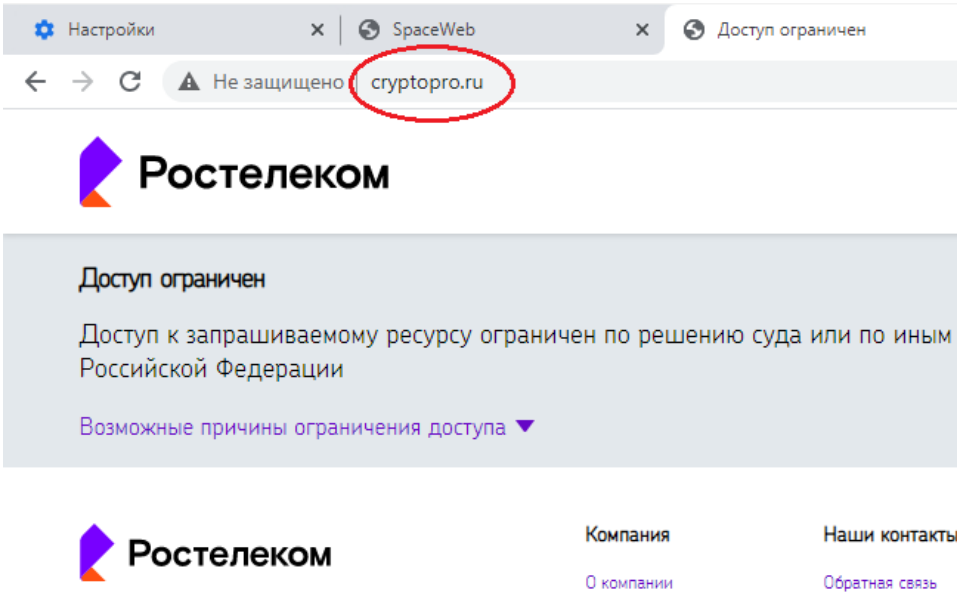


Рис. 15.7. Пример подмены DNS

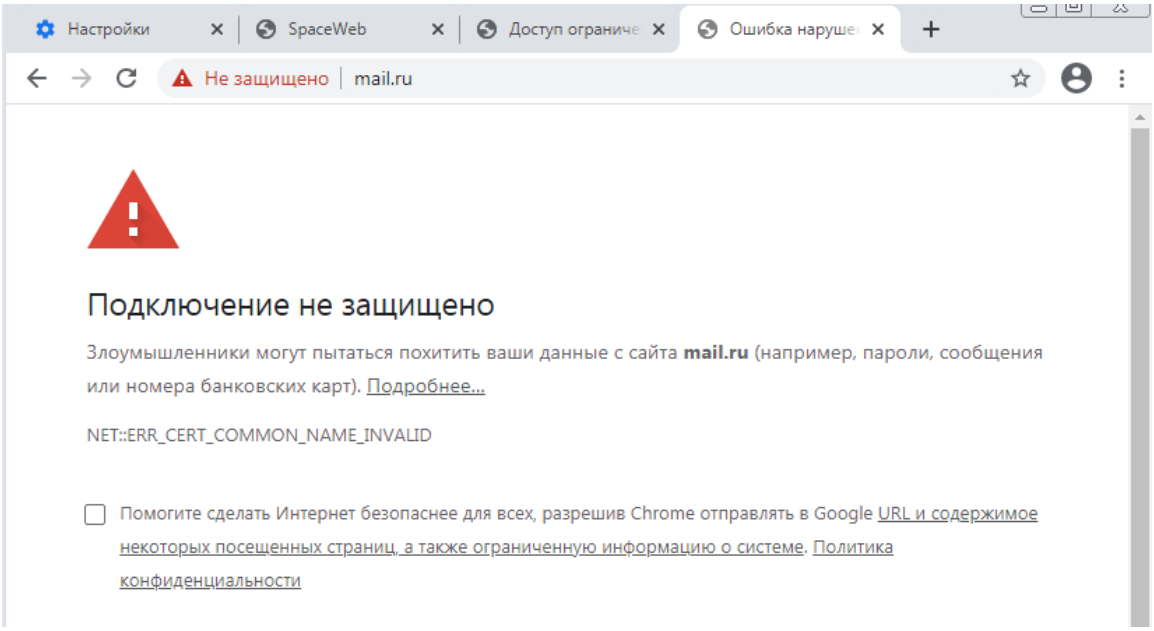


Рис. 15.8. Пример ошибки Chrome

Проверьте действие механизма HSTS при попытке обратиться к сайту, поддерживающему HTTPS, по протоколу HTTP (например, введите в строке браузера http://rea.ru).

Протокол HTTP в запросе будет автоматически заменяться на HTTPS.

Чтобы избежать ошибки, изображенной на рис. 15.8, можно в качестве подменного сайта использовать изначально незащищенную страницу (например, страницу сообщения о блокировке).

Задание 3. Реализуйте атаку подмены сертификатов веб-сайтов (https://blog.heckel.io/2013/08/04/use-sslsplit-to-transparently-sniff-tls-ssl-connections/).

Утилита sslsplit должна быть предустановлена на Kali Linux. Для того, чтобы проверить это, выполните

apt-get install sslsplit.

Для работы утилита нуждается в сертификате закрытого ключа центра сертификации (CA). При этом можно использовать имеющийся валидный сертификат или цепь сертификации либо сгенерировать сертификат самостоятельно с помощью пакета OpenSSL. Однако в последнем случае нарушителю придется решать проблему доверия к сертификату.

Создайте папку (например, sslcert), перейдите в нее и запустите команды генерации закрытого RSA ключа (файл ca.key) и сертификата корневого центра сертификации (файл ca.crt)

openssl genrsa -out ca.key 4096

openssl req -new -x509 -days 1826 -key ca.key -out ca.crt.

При создании сертификата введите требуемую информацию (произвольным образом; см. рис. 15.9).

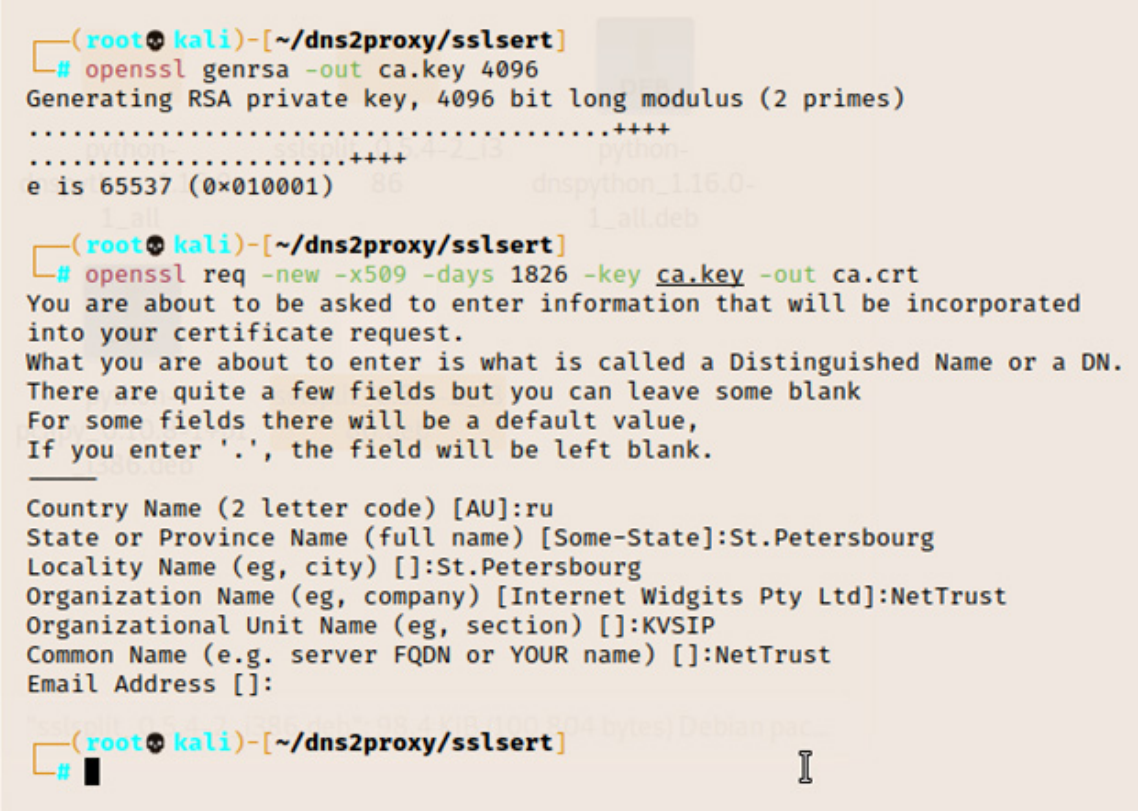


Рис. 15.9. Пример генерации корневого сертификата

Просмотрите содержимое папки и содержимое файлов в ней, чтобы убедиться, что сертификат имеется.

Передайте файл сертификата на Windows-машину (например, через почту). При необходимости предварительно скопируйте файл сертификата в другое место с помощью команды *ср*.

Чтобы решить проблему доверия к сертификатам, выданным поддельным центром сертификации, установите на Windows-машине сгенерированный сертификат в хранилище *Доверенные корневые центры сертификации* (запуск установки сертификата осуществляется двойным щелчком мыши на иконке файла сертификата, **Установить сертификат**).

Удостоверьтесь, что сертификат был включен в список доверенных корневых центров сертификации. Это можно посмотреть в меню браузера Internet Explorer (**Сервис/ Свойства обозревателя/ Содержание/ Сертификаты/ Доверенные корневые центры сертификации**) либо в настройках браузера Chrome (**Настройки/ Конфиденциальность и безопасность/ Безопасность/ Настроить сертификаты/ Доверенные корневые центры сертификации**).

3. На машине Kali Linux настройте правила для работы iptables (потребуются root-права):

iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080
iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8443
iptables -t nat -A PREROUTING -p tcp --dport 587 -j REDIRECT --to-ports 8443
iptables -t nat -A PREROUTING -p tcp --dport 465 -j REDIRECT --to-ports 8443
iptables -t nat -A PREROUTING -p tcp --dport 993 -j REDIRECT --to-ports 8443
iptables -t nat -A PREROUTING -p tcp --dport 5222 -j REDIRECT --to-ports 8080.

Запустите утилиту dns2proxy, если она не была запущена.

Перейдите в папку sslcert. Создайте в ней две подпапки: tmp и logdir.

Запустите из текущей папки утилиту sslsplit

sslsplit -D -l connections.log -j ./tmp -S ./logdir -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080.

Утилита должна стартовать и вывести на экран служебную информацию.

На Windows-машине откройте сайты, подключение к которым должно осуществляться через HTTPS, убедитесь, что они открываются без проблем, браузер показывает наличие защищенного соединения, но при этом используется поддельный сертификат (рис. 15.10), который был создан для sslsplit.

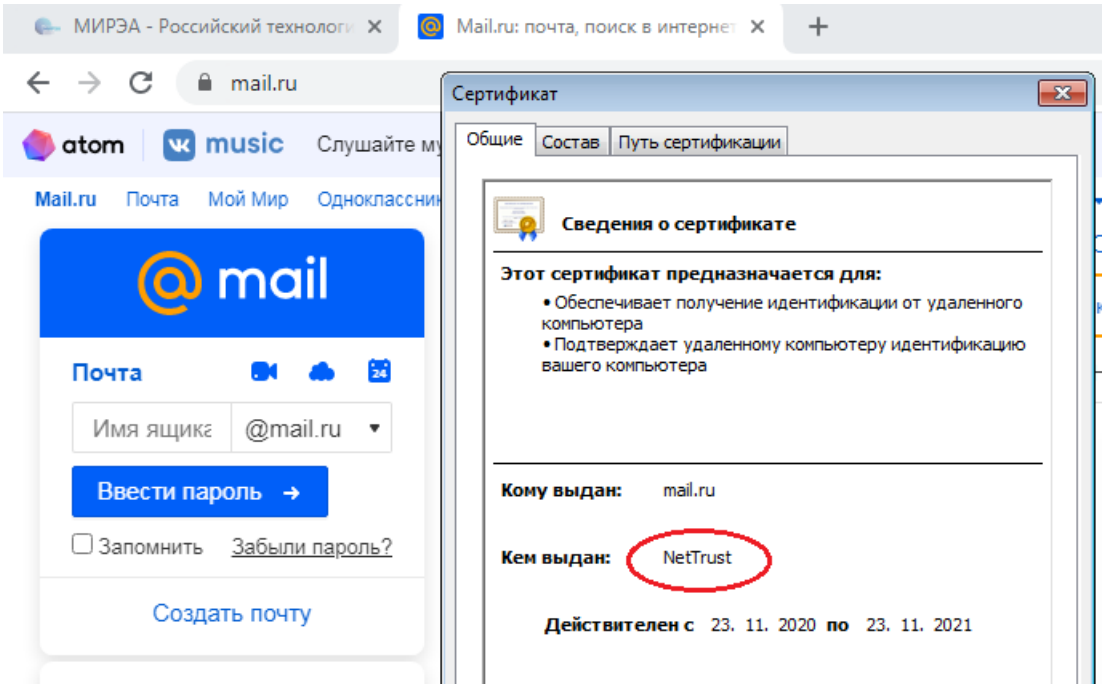


Рис. 15.10. Использование поддельного сертификата сайта для HTTPS, Google Chrome

Обратите внимание, что, хотя Mozilla FireFox и не выдает никаких предупреждений о проблемах с сертификатом, при просмотре самого сертификата выдается сообщение, что FireFox не может его проверить. Это происходит потому, что Mozilla FireFox имеет свой встроенный список доверенных корневых центров сертификации. Однако и в этот список при желании можно включить самоподписанный сертификат.

Методы защиты. В настройках браузеров включите технологию DOH (DNS-over-HTTPS) и проанализируйте ее действие.

При использовании этой технологии браузер создает HTTPS-туннель с доверенным сервером DNS, и все DNS-запросы передаются по этому туннелю.

Включите DOH, одновременно наблюдая перехватываемую прокси-сервером dns2proxy информацию.

В браузере Chrome в меню браузера выберите **Настройки/ Конфиденциальность и безопасность/ Безопасность**, в группе *Дополнительные* включите опцию *Использовать безопасный DNS-сервер*, можно оставить сервер по умолчанию (*Использовать текущего поставщика услуг*), а можно выбрать другой, например, OpenDNS.

В браузере Mozilla FireFox в меню браузера выберите **Настройки**, а потом нажмите **Настроить** в группе *Параметры сети*. В настройках соединения включите флажок *Включить DNS через HTTPS* (рис. 15.11), сохраните настройки, нажав OK.

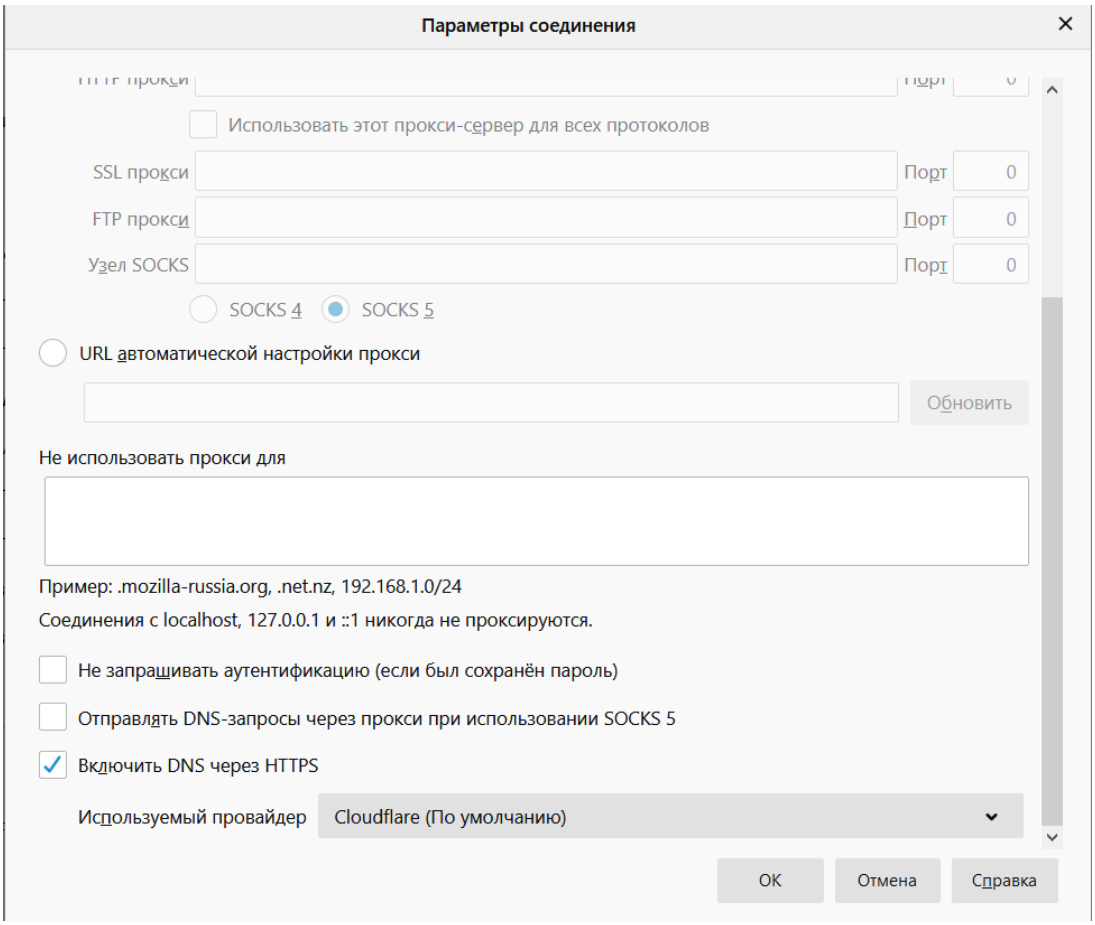


Рис. 15.11. Настройка DOH в браузере Mozilla FireFox

Откройте в браузерах несколько сайтов, в том числе и те, для которых ранее была сделана подмена. Отслеживайте изменения в выводе dns2proxy. Что произошло?

Dns2proxy ничего не выводит, так как DNS-запросы идут через HTTPS-туннель и неотличимы от обычного HTTPS-трафика. Сайты выводятся без изменений, подмена DNS не работает.

Проверьте, сказалось ли включение DOH на подмене сертификатов сайтов? Сертификаты по-прежнему подменяются, значит, MITM атака осуществляется, и можно перехватить передающийся трафик.

Сам по себе HTTPS-трафик не представляет большого интереса, так как все сообщения зашифрованы. Однако утилита sslsplit, реализуя MITM, фактически создает две сессии (рис. 15.12), в каждой из которых согласовывает сессионные ключи. Имея доступ к сессионному ключу, можно расшифровать передаваемый трафик.

Рис. 15.12. Схема MITM атаки с подменой сертификата

Задание 4. Расшифруйте перехватываемый HTTPS трафик.

Для того чтобы получить доступ к сессионным ключам, для утилиты sslsplit нужно указать параметр *-M ssl_key_logfile* для сохранения ключей во внешнем файле.

Убедитесь, что dns2proxy работает. Перезапустите утилиту sslsplit с параметром *-M ssl_key_logfile:*

sslsplit -D -l connections.log -j ./tmp -S ./logdir -M ssl_key_logfile -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080.

Откройте на Windows-машине какой-либо сайт, требующий подключения по протоколу HTTPS.

Убедитесь, что в папке, созданной для логов sslsplit (sslcert), создан файл ssl_key_logfile, просмотрите его содержимое командой *cat* и убедитесь, что он содержит ключи.

Осуществите перехват и расшифровку HTTPS-трафика в Wareshark.

На машине Kali Linux запустите Wireshark на интерфейсе eth1. Просмотрите захватываемый трафик, он зашифрован.

Примените в Wareshark фильтр по протоколу http и убедитесь, что результат захвата пуст (если не просматривали незащищенные страницы). Примените новый фильтр tls и убедитесь, что идет шифрованный трафик.

Откройте на Windows-машине какой-либо сайт, требующий ввода учетных данных пользователя (например, mail.ru, yandex.ru или online.sberbank.ru).

Укажите Wareshark-файл с сессионными ключами — откройте настройки Wareshark (**Edit/ Preferences**), раскройте список *Protocols* и выберите *TLS*. В настройках протокола в строке *(Pre)-Master-Secret log filename* укажите путь к файлу ssl_key_logfile, нажмите ОК.

Просмотрите захваченный TLS-трафик и убедитесь, что часть его расшифрована и доступна в виде HTTP.

Примените фильтр по протоколу http — в явном виде видны DOH запросы и передаваемый контент.

Осуществите поиск по имени открываемого сайта (щелкните на значке лупы, выберите тип значения *String*, в строке поиска введите, например, sber). Будут найдены соответствующие DOH-запросы и ответы. Раскройте в найденных DOH-пакетах верхний уровень — Domain Name System, в записях ответа найдите доменное имя просматриваемого сайта и его IP (рис. 15.13).

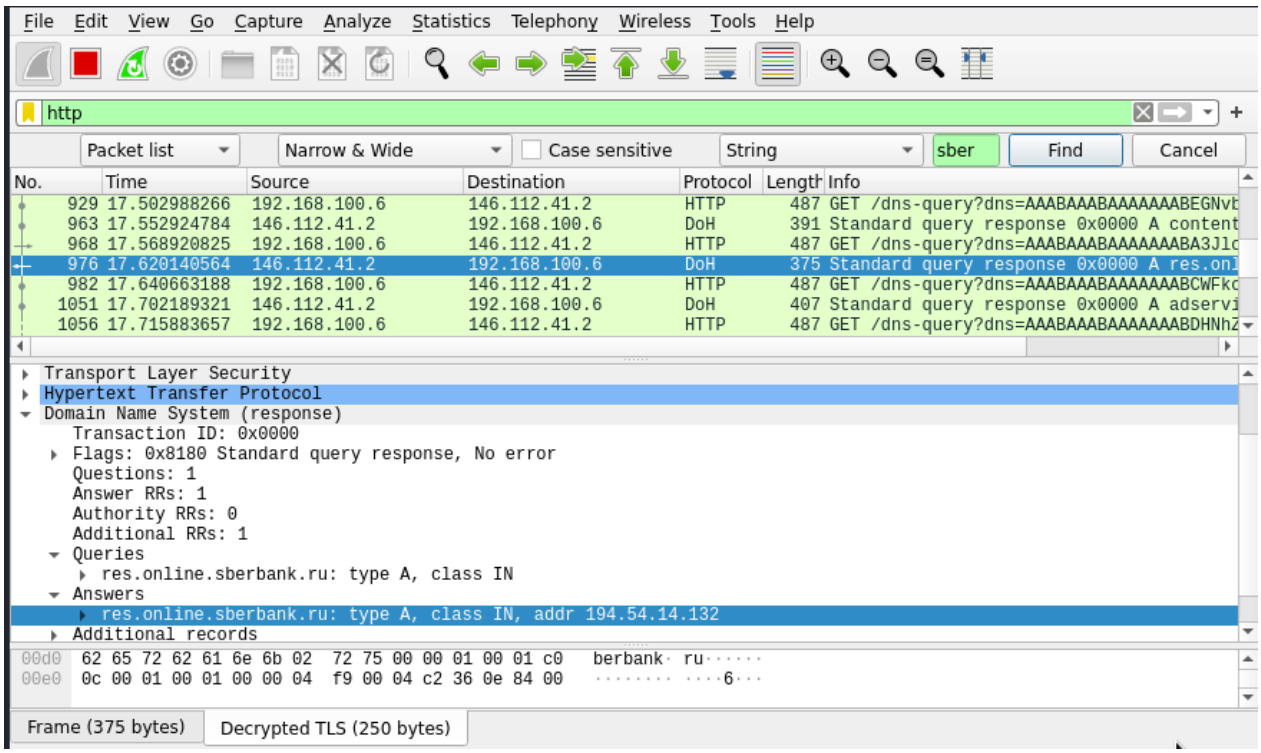


Рис. 15.13. Просмотр DNS-ответа DOH-пакета

На Windows-машине в браузере введите в форму входа сайта тестовые значения, например, логин: test, пароль: test1, и нажмите Войти.

В Wareshark примените фильтр вида http.host == <доменное имя>[17], например, *online.sberbank.ru.*

Выделите пакет, содержащий информацию об отсылке данных методом POST (значение в поле Info начинается со слова POST, идет передача данных в формате JSON). Выполните команду **Analyze/ Follow/ HTTP Stream**. Найдите в HTTP-потоке слово password или test (рис. 15.14).

Таким образом, удалось перехватить учетные данные пользователя.

Методы защиты. Основной метод защиты от подобных атак строится на доверии к сертификатам открытого ключа.

Атака была успешно осуществлена, поскольку поддельный сертификат был установлен в качестве доверенного. Поэтому подобные атаки могут быть реализованы, прежде всего, в корпоративной среде, где используются корпоративные CA (центры сертификации) с самоподписанными сертификатами, которые включаются в список корневых доверенных центров сертификации.

Кроме того, основным условием осуществления рассмотренных атак является реализация MITM-атаки. Поэтому следует исключить потенциальные возможности реализации MITM (защита от ARP-Spoofing, DHCP-Spoofing в локальной сети, защита узлов транспортировки и инфраструктуры провайдера от внешних атак).

[17] Надо вводить FQDN той страницы, на которой происходит ввод данных для аутентификации, например, не yandex.ru, а passport.yandex.ru.

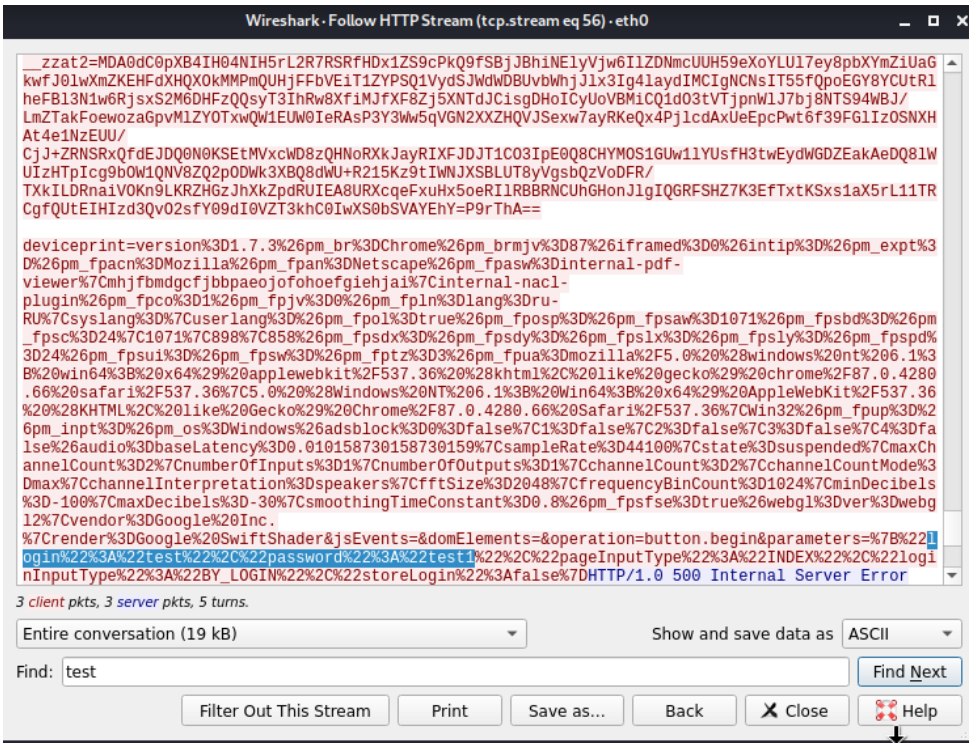


Рис. 15.14. Введенные пользователем учетные данные

Задание для самостоятельной работы. Анализ методов защиты от атак на протоколы DNS и TLS.

Найдите и запишите краткое описание следующих механизмов защиты:

– DNSSec;
– DOH;
– HSTS;
– доверенные центры сертификации.

Для каждого из этих механизмов укажите, от какого типа атак он защищает.

Вопросы для самоконтроля:

1. Назовите существующие способы реализации MITM-атак.
2. Для чего нужна программа Wireshark?
3. В чём особенности протокола https?

Тема 16. Прикладные сервисы Интернета

Семинар: Принципы функционирования систем электронной почты. Маршрутизация почтовых сообщений

Семинар посвящён изучению принципов функционирования систем электронной почты и вопросов осуществления маршрутизации почтовых сообщений. Занятие проводится в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области прикладных сервисов сети «Интернет».
2. Расширение научных представлений обучающихся о прикладных сервисах сети «Интернет».

3. Развитие мышления и творческой активности обучающихся.

4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.

5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Почтовая служба.
2. Непосредственное взаимодействие клиента и сервера.
3. Схема с выделенным почтовым сервером.
4. Схема с двумя почтовыми серверами-посредниками.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания о прикладных сервисах Интернета.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь принципов функционирования систем электронной почты и вопросов осуществления маршрутизации почтовых сообщений с общими принципами передачи данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 25 «Служба управления сетью» учебного пособия[18].

2. Изучить принципы функционирования систем электронной почты и вопросы осуществления маршрутизации почтовых сообщений.

3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Практический материал для занятия

Задание 1. Заполните таблицу, описывающую свойства протоколов IMAP, POP3 и SMTP (табл. 16.1).

[18] Компьютерные сети. Принципы, технологии, протоколы.

Таблица 16.1

Свойства протоколов IMAP, POP3 и SMTP

Свойства протокола	Протоколы
Используется почтовым клиентом для передачи письма за сервер	
Используется почтовым клиентом для получения письма с сервера	
При получении почты письмо перемещается с сервера на клиента	
При получении почты письмо копируется с сервера на клиента	

Задание 2. Браузер находит информацию по адресам специального формата, например: http://www.brauser.tv.ru/mobile/web/versions.shml. Заполните таблицу, описывающую соответствующий путь к файлу (табл. 16.2).

Таблица 16.2

Путь к файлу

Путь к объекту	
DNS-имя сервера	
URL-имя	
Тип протокола доступа	

Вопросы для самоконтроля:

1. Дайте определение понятий «почтовая служба», «почтовый клиент», «почтовый сервер».
2. Как происходит непосредственное взаимодействие клиента и сервера при организации почтовой службы?
3. В чём особенности схемы с выделенным почтовым сервером при организации почтовой службы?
4. Раскройте особенности схемы с двумя почтовыми серверами-посредниками при организации почтовой службы.

Тема 17. Передача мультимедийных данных

Семинар: Практическое применение систем передачи мультимедийной информации в компьютерных сетях

Семинар посвящён изучению принципов применения систем передачи мультимедийной информации в компьютерных сетях. Занятия проводятся в интерактивной форме учебной дискуссии.

Цели занятия:

1. Закрепление знаний обучающихся в области передачи мультимедийных данных.
2. Расширение научных представлений обучающихся о практическом применении систем передачи мультимедийной информации в компьютерных сетях.
3. Развитие мышления и творческой активности обучающихся.
4. Формирование умений и навыков самостоятельной работы с учебной и научной литературой, ведения дискуссии и публичного выступления.

5. Осуществление контроля процесса изучения и освоения учебного материала.

Учебные вопросы:

1. Мобильный IP. Проблема сохранения адреса.
2. Мобильный IPv4.
3. Мобильный IPv6.
4. Прокси-мобильный IPv6.

Порядок работы:

Этап 1. Информационный. На данном этапе обучающимся объявляются тема, цели и учебные вопросы семинара, разъясняются порядок проведения занятия, регламент выступлений и процедуры их обсуждения. Осуществляется проверка выполнения заданий для самостоятельной работы. Педагогический работник актуализирует теоретические знания о прикладных сервисах Интернета.

Этап 2. Практический. Заслушивание сообщений обучающихся. К своему выступлению каждый докладчик готовит демонстрационные материалы и мультимедиапрезентации. Активное участие каждого обучающегося обеспечивается обязательным конспектированием и групповой дискуссией по материалам выступления, ответами на контрольные вопросы.

Руководящая роль педагогического работника заключается в организации выступлений обучающихся, в дополнении и уточнении излагаемого материала, оценке их работы, в обобщении результатов.

Этап 3. Заключительный. Подведение итогов занятия: формулировка выводов по теме занятия; постановка задач по самостоятельному изучению наиболее сложных вопросов темы. Педагогический работник, подводя итоги занятия, подчеркивает взаимосвязь применения систем передачи мультимедийной информации в компьютерных сетях с общими принципами передачи мультимедийных данных.

Методические рекомендации обучающимся для подготовки к занятию:

1. Проработать материал главы 23 «Мобильные телекоммуникационные сети» учебного пособия[19].
2. Изучить принципы передачи аудио- и видеоданных по мобильным телекоммуникационным сетям.
3. Уяснить смысл и содержание основных терминов и определений и уметь ответить на контрольные вопросы.

Вопросы для самоконтроля:

1. Может ли проводная связь быть мобильной?
2. Раскройте понятие мобильного IP.
3. Как происходит обмен трафиком через туннель между домашним и внешним агентами?

[19] Компьютерные сети. Принципы, технологии, протоколы.

ЗАКЛЮЧЕНИЕ

Учебная дисциплина «Системы и сети передачи информации» очень широка и многогранна, а быстрый рост числа компьютерных сетей и их развитие сопровождаются сменой или совершенствованием сетевых технологий.

Знание современных тенденций их развития раскрывает для обучающихся возможности проявления профессиональных навыков в учебной и профессиональной деятельности.

Выполнение предложенных в учебно-методическом пособии заданий является необходимым условием для практического освоения дисциплины «Системы и сети передачи информации». Читатели, заинтересовавшиеся более подробным изучением рассмотренной тематики, могут воспользоваться рекомендуемыми источниками.

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

1. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие / В. Олифер, Н. Олифер. — Санкт-Петербург; Москва; Екатеринбург: Питер, 2021. — 1005 с.

2. Компьютерные сети : учебное пособие / Н. П. Табачук; [науч. ред. В. А. Казинец]. — Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2019. — 234 с.

3. Компьютерные сети передачи данных : лабораторный практикум / С. С. Владимиров. — Санкт-Петербург: СПбГУТ, 2016. — 24 с.

4. Национальный Открытый Университет «ИНТУИТ». Официальный сайт. URL: https://intuit.ru/studies/courses/3688/930/lecture/20109.

5. NetEmul. Сайт программы для визуализации возникающих в сети процессов, связанных с передачей служебной и пользовательской информации. URL: http://netemul.sourceforge.net/ruindex.html.

Приложение 1

Правила оформления отчета по практическим занятиям

1. Структура отчета должна соответствовать требованиям, представленным в соответствующем пункте лабораторной работы.
2. Размер основного шрифта отчета: Times New Roman, 14.
3. Отчёт должен включать титульную страницу и непосредственно сам ход выполнения.

Приложение 2

Образец оформления титульного листа

Федеральное государственное казенное образовательное
учреждение высшего образования
«Санкт-Петербургский университет Министерства внутренних дел
Российской Федерации»

Факультет подготовки сотрудников для оперативных подразделений
Кафедра специальных информационных технологий

Отчёт по практическому занятию № 2.2

Тема: «Коммутация каналов и пакетов»

Выполнил:
курсант 3 курса,
335 учебного взвода
младший сержант полиции Иванов И. И.

Санкт-Петербург
2023

Учебное издание

Локнов Алексей Игоревич,
кандидат технических наук;
Васильева Ирина Николаевна,
кандидат физико-математических наук, доцент

СИСТЕМЫ И СЕТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Учебно-методическое пособие

Редактор *Корчуганова И. А.*
Компьютерная вёрстка *Фролова А. В.*
Дизайн обложки *Шеряй А. Н.*

ISBN 978-5-91837-674-4

Подписано в печать 06.02.2023. Формат 60×84 $^{1}/_{16}$
Печать цифровая. Объём 4,5 п. л. Тираж 100 экз. Заказ № 3/23

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1