

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

**Федеральное государственное образовательное бюджетное
учреждение высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»**

С. С. Владимиров

КОМПЬЮТЕРНЫЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ

**Лабораторный практикум
Работа в эмуляторе NetEmul**

СПб ГУТ)))

**Санкт-Петербург
2016**

УДК 004.738.5 (076)

ББК 00.00 x00

В 57

Рецензент
профессор кафедры СС и ПД,
доктор технических наук *О. С. Когновицкий*

Рекомендовано к печати редакционно-издательским советом СПбГУТ

Владимиров, С. С.

В 57 Компьютерные сети передачи данных : лабораторный практикум /
С. С. Владимиров ; СПбГУТ. — СПб, 2016. — 24 с.

Учебное пособие призвано ознакомить студентов старших курсов с моделированием компьютерных сетей передачи данных в эмуляторе NetEmul. Представленный материал служит справочным и методическим пособием при выполнении курса практических лабораторных работ по дисциплинам «Компьютерные сети передачи данных» и «Передача данных в локальных информационно-вычислительных сетях».

Предназначено для студентов, обучающихся по направлениям 11.03.02 (210700.62) «Инфокоммуникационные технологии и системы связи», 09.03.01 (230100.62) «Информатика и вычислительная техника» и 09.03.04 (231000.62) «Программная инженерия».

УДК 004.738.5 (076)

ББК 00.00 x00

- © Владимиров С. С., 2016
- © Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», 2016

Содержание

Лабораторная работа 1. Ознакомление с интерфейсом программы. Соединение ЭВМ в сеть	4
1.1. Цель работы	4
1.2. Теоретический материал	4
1.3. Порядок выполнения лабораторной работы	4
1.4. Форма представления и содержание отчета	8
1.5. Контрольные вопросы	8
Лабораторная работа 2. Использование маршрутизаторов. Статическая маршрутизация	9
2.1. Цель работы	9
2.2. Теоретический материал	9
2.3. Порядок выполнения лабораторной работы	9
2.4. Форма представления и содержание отчета	10
2.5. Контрольные вопросы	11
Лабораторная работа 3. Разрешение адресов по протоколу ARP. ARP-спуфинг	12
3.1. Цель работы	12
3.2. Теоретический материал	12
3.3. Порядок выполнения лабораторной работы	15
3.4. Форма представления и содержание отчета	17
3.5. Контрольные вопросы	18
Лабораторная работа 4. Динамическая маршрутизация по протоколу RIP. Получение сетевых настроек по DHCP	19
4.1. Цель работы	19
4.2. Теоретический материал	19
4.3. Порядок выполнения лабораторной работы	19
4.4. Форма представления и содержание отчета	21
4.5. Контрольные вопросы	21
Приложение. Правила оформления отчета	23

Лабораторная работа 1

Ознакомление с интерфейсом программы. Соединение ЭВМ в сеть

1.1. Цель работы

Ознакомиться с основами работы с программным эмулятором ЛВС NetEmul. Научиться строить простейшие модели ЛВС. Уяснить разницу в построении ЛВС на концентраторах и коммутаторах.

1.2. Теоретический материал

1.2.1. Запуск эмулятора NetEmul

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

1.3. Порядок выполнения лабораторной работы

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

1. Номер группы.
2. ФИО студентов, выполняющих работу.
3. Номер варианта согласно номеру студента (одного из студентов бригады) в журнале.

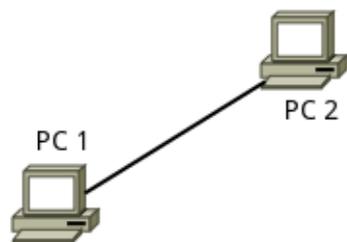
Таблица 1.1

Варианты задания (указаны согласно номеру студента в журнале)

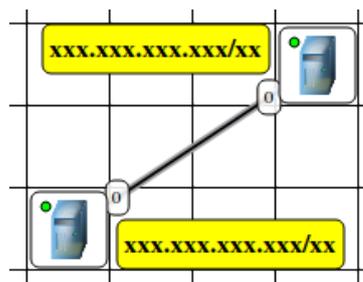
№	Адрес сети/маска	№	Адрес сети/маска	№	Адрес сети/маска
1	10.0.1.0/27	11	10.1.1.64/27	21	10.2.1.128/27
2	10.0.2.32/27	12	10.1.2.96/27	22	10.2.2.160/27
3	10.0.3.64/27	13	10.1.3.128/27	23	10.2.3.192/27
4	10.0.4.96/27	14	10.1.4.160/27	24	10.2.4.224/27
5	10.0.5.128/27	15	10.1.5.192/27	25	10.2.5.0/27
6	10.0.6.160/27	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

1.3.1. Соединение двух ЭВМ напрямую

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



(а). в общем виде



(б). в NetEmul

Рис. 1.1. Схема модели ЛВС при соединении двух ЭВМ напрямую

2. Добавить на рабочее поле эмулятора два компьютера (см. рис. 1.1), используя кнопку «Добавить компьютер» на панели инструментов.

3. Соединить добавленные компьютеры как показано на рис. 1.1. Для этого

- а) нажать кнопку «Создать соединение» на панели инструментов;
- б) навести указатель на один из компьютеров;
- в) зажав 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. 1.1.

5. Проверить работоспособность построенной модели 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 КВ;

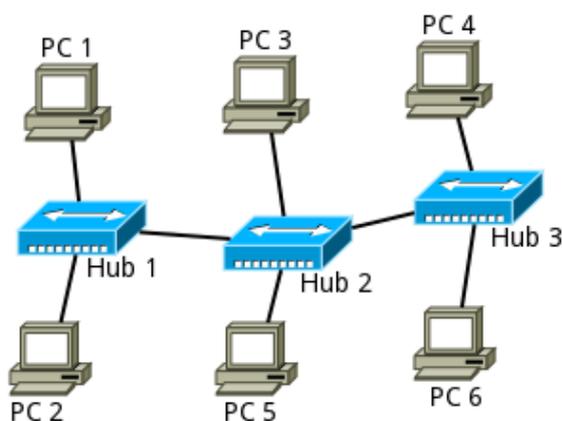
д) нажать «Далее» — окно пропадет, а кружок под курсором сменит цвет на зеленый;

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

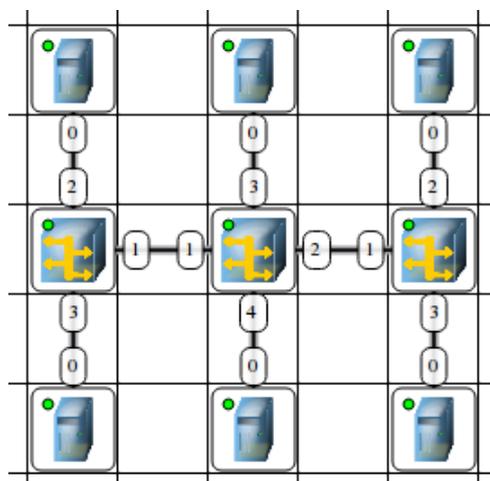
ж) в появившемся окне подтвердить интерфейс на принимающем компьютере eth0, нажав «Отправка»;

з) проследить за перемещением пакетов.

1.3.2. Построение ЛВС на концентраторах



(а). в общем виде



(б). в NetEmul

Рис. 1.2. Схема модели ЛВС на основе концентраторов

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. 1.2.

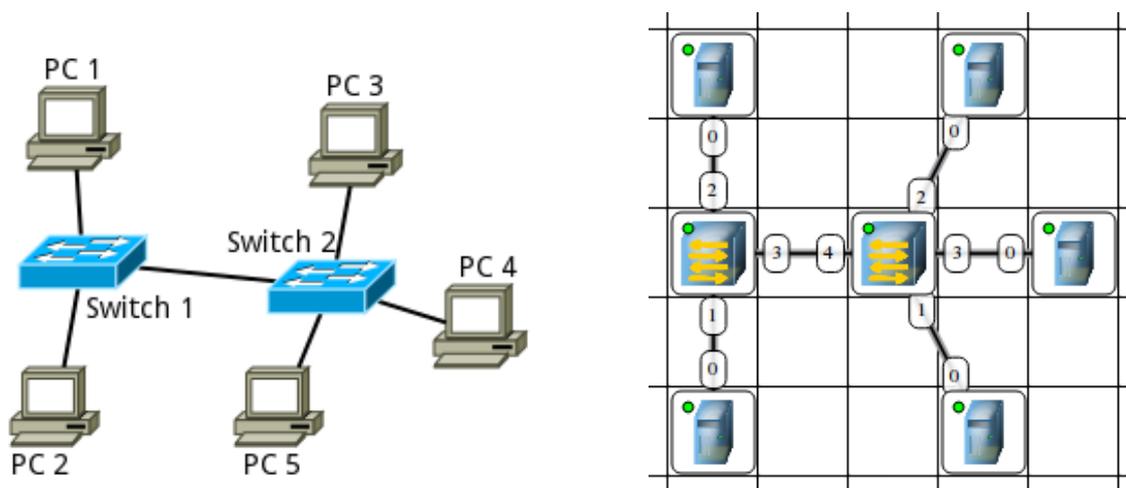
3. Соединить устройства как показано на рис. 1.2.

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 (ТСР, 5 КВ) от одного компьютера до другого. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе концентраторов.

1.3.3. Построение ЛВС на коммутаторах



(а). в общем виде

(б). в NetEmul

Рис. 1.3. Схема модели ЛВС на основе коммутаторов

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. 1.3.

3. Соединить устройства как показано на рис. 1.3.

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 (ТСР, 5 КВ) от одного компьютера до другого. Проследить за перемещением пакетов и сделать выводы об особенностях работы ЛВС на основе коммутаторов.

После выполнения работы продемонстрировать преподавателю работоспособность построенной модели.

Проект сохранить для отчета.

1.4. Форма представления и содержание отчета

Отчет в формате PDF отправляется на электронную почту преподавателя вместе с файлом проекта. Отчет выполняется один на бригаду.

Формат письма

- **Тема:** Номер группы, дисциплина, номер работы, ФИО первого студента в бригаде.
- **Тело:** Номер группы. Дисциплина. Номер работы. ФИО студентов.

Содержание отчета

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

1.5. Контрольные вопросы

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

Лабораторная работа 2

Использование маршрутизаторов. Статическая маршрутизация

2.1. Цель работы

Ознакомиться с работой маршрутизаторов. Научиться формировать статические маршруты и прописывать их в таблицы маршрутизации сетевых устройств.

2.2. Теоретический материал

2.2.1. Запуск эмулятора NetEmul

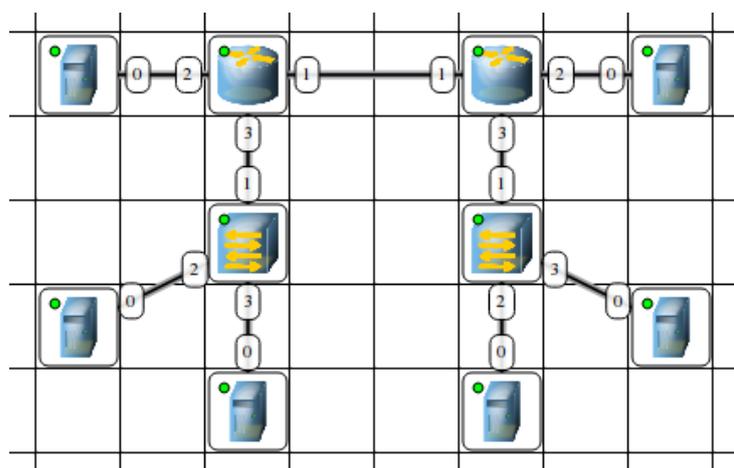
Для запуска эмулятора NetEmul необходимо либо воспользоваться соответствующим пунктом главного меню операционной системы, либо выполнить в терминале команду `netemul`.

2.3. Порядок выполнения лабораторной работы

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

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

2.3.1. Построение модели сети



(a). в NetEmul

Рис. 2.1. Связь сетей посредством маршрутизаторов

1. Выбрать исходные данные для выполнения работы согласно своему варианту. Варианты заданий взять из лаб. работы 4 методических указаний Небаева И.А. "Учебное пособие к лабораторным работам по курсу КСПД для среды исполнения Computer Network Simulator 2013.

2. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 2.1. 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 возле каждого компьютера и интерфейса роутера надписи с их IP-адресом и маской подсети.

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

2.3.2. 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 (ТСР, 5 КВ) между удалёнными 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.

2.4. Форма представления и содержание отчета

Отчет в формате PDF отправляется на электронную почту преподавателя вместе с файлом проекта. Отчет выполняется один на бригаду.

Формат письма

- **Тема:** Номер группы, дисциплина, номер работы, ФИО первого студента в бригаде.
- **Тело:** Номер группы. Дисциплина. Номер работы. ФИО студентов.

Содержание отчета

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

2.5. Контрольные вопросы

1. Что такое IP-адрес?
2. Что такое маска подсети?
3. Как работает маршрутизатор?
4. Принципы статической маршрутизации?

Лабораторная работа 3

Разрешение адресов по протоколу ARP. ARP-спуфинг

3.1. 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.

3.2. Теоретический материал

3.2.1. Запуск эмулятора NetEmul

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

3.2.2. 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 повсеместности 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 ширококестельно (в поле MAC-адрес назначения заголовка Ethernet указывается ширококестельный 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 А) указывает свой локальный адрес.

Схема работы показана на рис. 3.1.

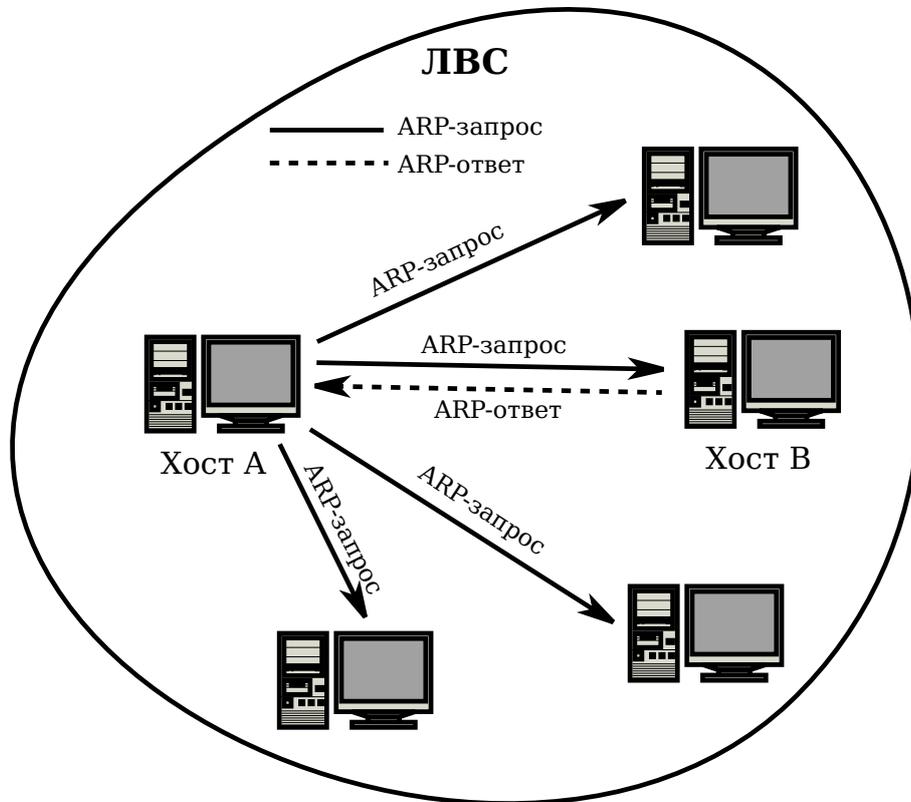


Рис. 3.1. Схема работы протокола ARP

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

Структура кадра ARP с учетом заголовка Ethernet показана на рис. 3.2.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Destination MAC						Source MAC						ETH TYPE	HTYPE		
PTYPE		HLEN	PLEN	OP CODE	Sender MAC						Sender IP				
Target MAC						Target IP									

Рис. 3.2. Кадр протокола ARP

Значения полей заголовка кадра ARP приведены в табл. 3.1.

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 (*gratuitous ARP*) — такое поведение ARP, когда ARP-ответ присылается, когда 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*.

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.

3.2.3. 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. 3.3.

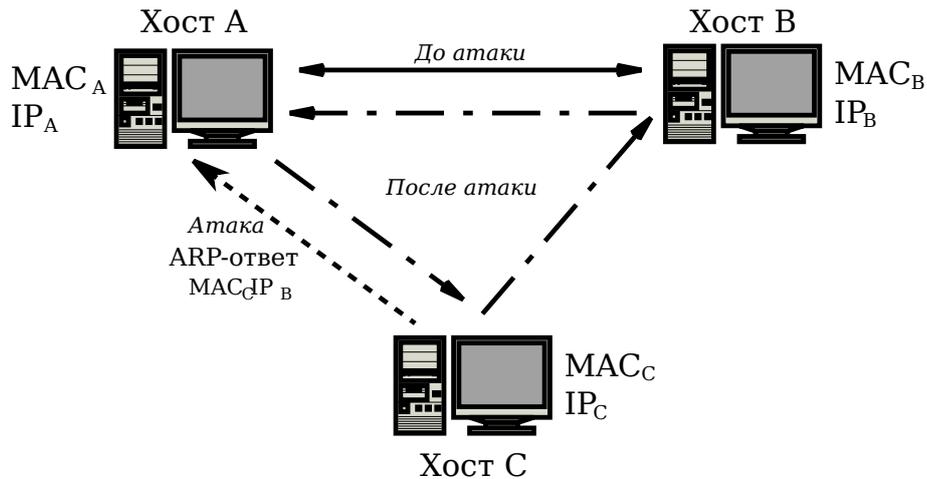


Рис. 3.3. Схема сетевой атаки ARP-спуфинг

3.3. Порядок выполнения лабораторной работы

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

1. Номер группы.
2. ФИО студентов, выполняющих работу.
3. Номер варианта согласно номеру студента (одного из студентов бригады) в журнале.

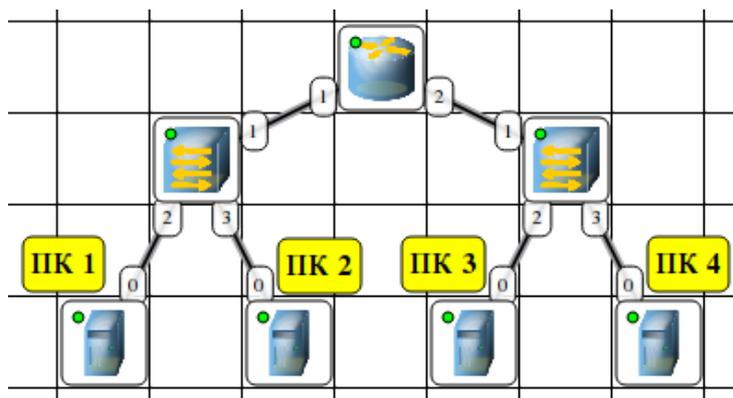
Таблица 3.2

Варианты задания (указаны согласно номеру студента 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

3.3.1. 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.



(а). в NetEmul

Рис. 3.4. Сеть для изучения протокола ARP

2. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 3.4. В свойствах маршрутизатора необходимо указать количество интерфейсов, равное 2.

3. Настроить интерфейсы компьютеров и маршрутизаторов, задав каждому IP-адрес и маску подсети (слева — первая подсеть в заданной сети, справа — вторая подсеть). Добавить возле каждого компьютера и интерфейса 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».

3.3.2. 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 широкоэвещательно (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.

3.3.3. 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 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.

3.4. Форма представления и содержание отчета

Отчет в формате PDF отправляется на электронную почту преподавателя вместе с файлом проекта. Отчет выполняется один на бригаду.

Формат письма

- **Тема:** Номер группы, дисциплина, номер работы, ФИО первого студента в бригаде.
- **Тело:** Номер группы. Дисциплина. Номер работы. ФИО студентов.

Содержание отчета

1. Заголовок согласно приложению.
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 лабораторной должны быть приведены выводы по работе.

3.5. Контрольные вопросы

1. Протокол ARP.
2. Формат пакета ARP.
3. Самопроизвольный ARP.
4. IP-адрес.
5. MAC-адрес.
6. ARP-спуфинг.

Лабораторная работа 4

Динамическая маршрутизация по протоколу RIP.

Получение сетевых настроек по DHCP

4.1. Цель работы

Ознакомиться с механизмом динамической маршрутизации по протоколу RIP. Научиться настраивать компьютеры и серверы для автоматизации получения компьютерами сетевых настроек.

4.2. Теоретический материал

4.2.1. Запуск эмулятора NetEmul

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

4.3. Порядок выполнения лабораторной работы

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

1. Номер группы.
2. ФИО студентов, выполняющих работу.
3. Номер варианта согласно номеру студента (одного из студентов бригады) в журнале.

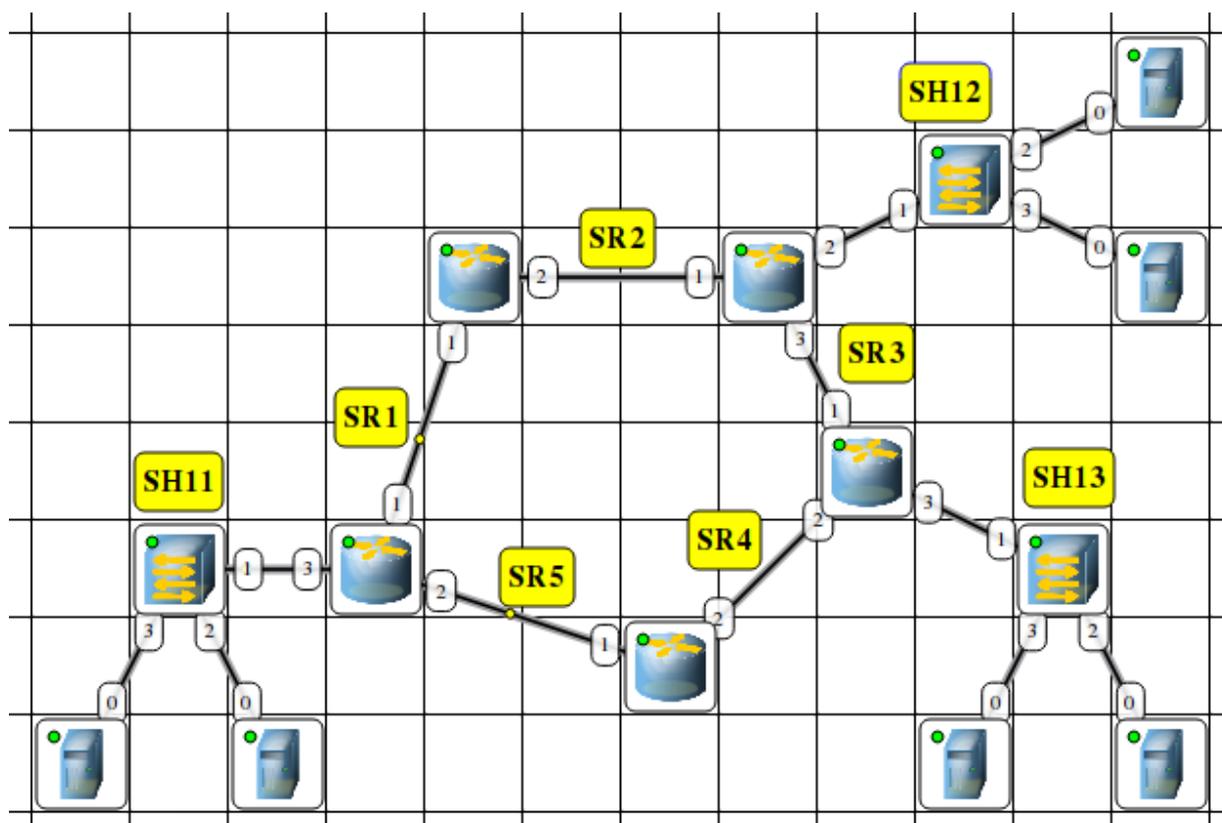
Таблица 4.1

Варианты задания (указаны согласно номеру студента 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

4.3.1. 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.



(а). в NetEmul

Рис. 4.1. Модель сети для изучения работы протоколов RIP и DHCP

2. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 4.1.
3. Распределить полученные ранее адреса сетей между сетями SR1–SR5 и SH11–SH13. Добавить возле каждой сети надпись с ее IP-адресом.
4. Настроить интерфейсы маршрутизаторов, задав каждому IP-адрес и маску подсети в соответствии с выбранным распределением.

4.3.2. Настройка динамической маршрутизации по протоколу RIP

1. На каждом маршрутизаторе добавить и запустить программу RIP. Пункт контекстного меню «Программы». Кнопка «Добавить». Не забудьте 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.

4.3.3. 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. Не забудьте поставить флаг для активации программы.

4. В настройках каждого DHCP-клиента укажите 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 не 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.

4.4. Форма представления и содержание отчета

Отчет в формате PDF отправляется на электронную почту преподавателя вместе с файлом проекта. Отчет выполняется один на бригаду.

Формат письма

- **Тема:** Номер группы, дисциплина, номер работы, ФИО первого студента в бригаде.
- **Тело:** Номер группы. Дисциплина. Номер работы. ФИО студентов.

Содержание отчета

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

4.5. Контрольные вопросы

1. Протокол RIP.

2. Протокол ДНСР.

Приложение

Правила оформления отчета к лабораторным работам

1. Структура отчета должна соответствовать требованиям представленным в соответствующем пункте лабораторной работы.
2. Размер основного шрифта отчета: 11–12 pt.
3. Заголовок отчета должен иметь вид:

**Отчет к лабораторной работе №1
Изучение принципов работы утилит
для исследования и мониторинга состояния сети**

Группа: ГР-00

Студент: Пупкин В. И.

Цель работы: ...

4. Результаты работы консольных программ (листинги), сами запускаемые команды и диаграммы, отображаемые в текстовом виде, должны быть оформлены моноширинным шрифтом (Courier New, Lusida Console, FreeMono и т. п.). Они должны вмещаться в ширину страницы (шрифт можно уменьшать до 9 pt). Если ширины вертикально расположенного листа А4 не хватает, то можно разместить диаграмму на нескольких горизонтально расположенных листах А4.

Например:

```
student@comp:~\ $ ping -c 4 www.ya.ru
PING ya.ru (87.250.250.3) 56(84) bytes of data.
64 bytes from www.yandex.ru (87.250.250.3): icmp_seq=1 ttl=52 time=16.8 ms
64 bytes from www.yandex.ru (87.250.250.3): icmp_seq=2 ttl=52 time=16.8 ms
64 bytes from www.yandex.ru (87.250.250.3): icmp_seq=3 ttl=52 time=18.7 ms
64 bytes from www.yandex.ru (87.250.250.3): icmp_seq=4 ttl=52 time=13.5 ms

--- ya.ru ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 13.542/16.484/18.759/1.874 ms
```

5. Текст на диаграммах и графиках должен быть свободно читаем.
6. На графиках должны быть подписаны оси и единицы измерения.

Владимиров Сергей Сергеевич

КОМПЬЮТЕРНЫЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Лабораторный практикум

Редактор *Х. Х. Хxxxxxxxxx*
Компьютерная верстка *Х. Х. Хxxxxxxxxx*

План изданий 20XX г., п. XX

Подписано к печати XX.XX.20XX
Объем X,XX усл.-печ. л. Тираж XX экз. Заказ XXX

Редакционно-издательский центр СПбГУТ
191186 СПб., наб. р. Мойки, 61
Отпечатано в СПбГУТ