

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Локтионова Оксана Геннадьевна

Должность: проректор по учебной работе

Дата подписания: 19.09.2024 22:16:02

Уникальный программный ключ:

0b817ca911e6668abb13a5d426d39c51c11eab0f77e943dffa4851fda56d089

МИНОБРАЗОВАНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ

Проректор по учебной работе

О.Г. Локтионова

«23» 10

2023 г.



ПОСТРОЕНИЕ КАБЕЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ

Методические указания по выполнению лабораторных и практических работ для студентов по направлению подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи»

Курск 2023

УДК 004.7

Составители: И. Г. Бабанин, Е.Ю. Бабанина

Рецензент

Доктор технических наук, зав. кафедрой космического приборостроения
и систем связи *В.Г. Андронов*

Построение кабельных систем передачи данных: методические указания по выполнению лабораторных и практических работ/ Юго-Зап. гос. ун-т; сост.: И.Г. Бабанин, Е.Ю. Бабанина. – Курск, 2023. – 145 с.

Методические указания содержат сведения о технике безопасности на рабочем месте, порядке выполнения лабораторных, практических работ, рекомендации по подготовке, оформлению и защите лабораторных работ, а также критерии оценивания защиты отчета.

Методические указания соответствуют требованиям ФГОС ВО 3++ по направлению подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи».

Предназначены для студентов, осваивающих основную профессиональную образовательную программу по направлению подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи».

Текст печатается в авторской редакции

Подписано в печать «__» __.2023. Формат 60×84 1/16.
Усл. печ. л.8,43. Уч.- изд. л. 7,63. Тираж 100 экз. Заказ *1194*. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

СОДЕРЖАНИЕ

Инструкция по технике безопасности.....	4
Лабораторная работа №1 «Подключение к сетевым устройствам по протоколу защищенного удаленного доступа SSH».....	8
Лабораторная работа №2 «Блокировка резервных портов и агрегирование каналов».....	16
Лабораторная работа №3 «Виртуальные локальные сети VLAN».....	22
Лабораторная работа №4 «Статическая маршрутизация в сетях IPv4 и IPv6».....	34
Лабораторная работа №5 «Настройка локального сервера доменных имен (DNS)».....	50
Лабораторная работа №6 «Списки доступа ACL».....	64
Лабораторная работа №7 «Демилитаризованные зоны DMZ».....	72
Лабораторная работа №8 «Трансляция и туннелирование сетевых адресов».....	78
Лабораторная работа №9 «Настройка сервера динамического конфигурирования хостов DHCP в сети».....	96
Практическое занятие №1 «Анализ трафика локальной сети на примере ARP, DNS, HTTP».....	109
Практическое занятие №2 «Использование генератора трафика для создания нагрузки в сети».....	118
Практическое занятие №3 «Мониторинг в сетях связи: протокол ICMP, специализированные утилиты».....	126
Практическое занятие №4 «Виртуальная частная сеть VPN».....	136
Форма отчета обучающегося о выполняемой лабораторной работе....	142
Шкала оценивания и критерии оценивания выполненной лабораторной/практической работы.....	143
Заключение.....	144
Приложение А (обязательное) Форма титульного листа отчета обучающегося о выполненной лабораторной/ практической работе...	145

ИНСТРУКЦИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

Общие положения

Настоящая инструкция предназначена для студентов и работников, выполняющих работы на персональном компьютере и на сетевом оборудовании (коммутаторы, маршрутизаторы, межсетевые экраны и т.д.).

К выполнению работ допускаются лица:

- не моложе 16 лет;
- прошедшие медицинский осмотр;
- прошедшие вводный инструктаж по охране труда, а также инструктаж по охране труда на рабочем месте;
- прошедшие обучение безопасным приемам труда на рабочем месте по выполняемой работе.

Работник обязан:

- выполнять правила внутреннего трудового распорядка, установленные в положениях и инструкциях, утвержденных ректором ЮЗГУ, или его заместителями;
- выполнять требования настоящей инструкции;
- сообщать руководителю работ о неисправностях, при которых невозможно безопасное производство работ;
- не допускать присутствия на рабочем месте посторонних лиц;
- уметь оказывать первую помощь и при необходимости оказывать ее пострадавшим при несчастных случаях на производстве, по возможности сохранив обстановку на месте происшествия без изменения и сообщив о случившемся руководителю;
- выполнять требования противопожарной безопасности не разводите открытый огонь без специального на то разрешения руководителя работ;
- периодически проходить медицинский осмотр в сроки, предусмотренные для данной профессии.

Работник должен знать опасные и вредные производственные факторы, присутствующие на данном рабочем месте:

- возможность травмирования электрическим током при отсутствии или неисправности заземляющих устройств;
- вредное воздействие монитора компьютера при его неправильной установке или неисправности;

- возможность возникновения заболеваний при неправильном расположении монитора, клавиатуры, стула и стола;

- вредное воздействие паров, газов и аэрозолей выделяющихся при работе копировальной и печатающей оргтехники в непроветриваемых помещениях.

Работник при выполнении любой работы должен обладать здоровым чувством опасности и руководствоваться здравым смыслом. При отсутствии данных качеств он к самостоятельной работе не допускается.

Требования охраны труда перед началом работы

Перед началом работы работник обязан:

- получить от руководителя работ инструктаж о безопасных методах, приемах и последовательности выполнения производственного задания;

- привести в порядок одежду, застегнуть на все пуговицы, чтобы не было свисающих концов, уложить волосы, чтобы они не закрывали лицо и глаза;

- привести рабочее место в безопасное состояние;

- запрещается носить обувь на чрезмерно высоких каблуках;

Перед включением компьютера или сетевого оборудования убедиться в исправности электрических проводов, штепсельных вилок и розеток. Вилки и розетки должны соответствовать Евростандарту. Отличительной особенностью этих вилок и розеток является наличие третьего провода, обеспечивающего заземление компьютера или другого прибора. При отсутствии третьего заземляющего провода заземление должно быть выполнено обычным способом с применением заземляющего проводника и контура заземления;

Убедиться, что корпус включаемого оборудования не поврежден, что на нем не находятся предметы, бумага и т.п. Вентиляционные отверстия в корпусе включаемого оборудования не должны быть закрыты занавесками, завалены бумагой, заклеены липкой лентой или перекрыты каким-либо другим способом.

Требования охраны труда во время работы

Запрещается во время работы пить какие-либо напитки, принимать пищу;

Запрещается ставить на рабочий стол любые жидкости в любой таре (упаковке или в чашках);

Помещения для эксплуатации компьютеров, сетевого оборудования должны иметь естественное и искусственное освещение, естественную вентиляцию и соответствовать требованиям действующих норм и правил. Запрещается размещать рабочие места вблизи силовых электрических кабелей и вводов трансформаторов, технологического оборудования, создающего помехи в работе и отрицательно влияющие на здоровье операторов;

Окна в помещениях, где установлены компьютеры должны быть ориентированы на север и северо-восток. Оконные проемы оборудуются регулируемыми устройствами типа жалюзи или занавесками;

Площадь на одно рабочее место пользователей компьютера должна составлять не менее 6 м^2 при рядном и центральном расположении, при расположении по периметру помещения – 4 м^2 . При использовании компьютера без вспомогательных устройств (принтер, сканер и т.п.) с продолжительностью работы менее четырех часов в день допускается минимальная площадь на одно рабочее место 5 м^2 ;

Полимерные материалы, используемые для внутренней отделки интерьера помещений с ПК должны подвергаться санитарно-эпидемиологической экспертизе. Поверхность пола должна обладать антистатическими свойствами, быть ровной. В помещениях ежедневно проводится влажная уборка. Запрещается использование удлинителей, фильтров, тройников и т.п., не имеющих специальных заземляющих контактов;

Экран видеомонитора должен находиться от глаз оператора на расстоянии 600-700 мм, минимально допустимое расстояние 500 мм;

Продолжительность непрерывной работы с ПК должна быть не более 2 часов.

Требования охраны труда по окончании работы

По окончании работы работник обязан выполнить следующее:

- привести в порядок рабочее место;
- убрать инструмент и приспособления в специально отведенные для него места хранения;
- обо всех замеченных неисправностях и отклонениях от нормального состояния сообщить руководителю работ;

- привести рабочее место в соответствие с требованиями пожарной безопасности.

Действие при аварии, пожаре, травме

В случае возникновения аварии или ситуации, в которой возможно возникновение аварии немедленно прекратить работу, предпринять меры к собственной безопасности и безопасности других рабочих, сообщить о случившемся руководителю работ.

В случае возникновения пожара немедленно прекратить работу, сообщить в пожарную часть по телефону 01, своему руководителю работ и приступить к тушению огня имеющимися средствами.

В случае получения травмы обратиться в медпункт, сохранить по возможности место травмирования в том состоянии, в котором оно было на момент травмирования, доложить своему руководителю работ лично или через товарищей по работе.

Ответственность за нарушение инструкции

Каждый работник ЮЗГУ в зависимости от тяжести последствий несет дисциплинарную, административную или уголовную ответственность за несоблюдение настоящей инструкции, а также прочих положений и инструкций, утвержденных ректором ЮЗГУ или его заместителями.

Руководители подразделений, заведующий кафедрой, начальники отделов и служб несут ответственность за действия своих подчиненных, которые привели или могли привести к авариям и травмам согласно действующему в РФ законодательству в зависимости от тяжести последствий в дисциплинарном, административном или уголовном порядке.

Администрация ЮЗГУ вправе взыскать с виновных убытки, понесенные предприятием в результате ликвидации аварии, при возмещении ущерба работникам по временной или постоянной утрате трудоспособности в соответствии с действующим законодательством.

ЛАБОРАТОРНАЯ РАБОТА №1 «ПОДКЛЮЧЕНИЕ К СЕТЕВЫМ УСТРОЙСТВАМ ПО ПРОТОКОЛУ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА SSH»

Цель занятия: изучение способов подключения и первоначальных настроек сетевых устройств.

Задачи занятия:

- 1) Произвести подключение к сетевому оборудованию по консольному кабелю и выполнить первоначальную настройку;
- 2) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о стеках протоколов сетевого оборудования;
- формирование умений выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;
- формирование навыков управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях, использования шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях.

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционными системами Windows или Linux;
- 2) Сетевое устройство (или маршрутизатор, или управляемый коммутатор, или межсетевой экран);
- 3) Консольный кабель.

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Сетевые устройства, как правило, настраиваются в командной строке ОС. Подсоединение к ним осуществляется по протоколу Telnet, SSH на IP-адрес любого из его сетевых интерфейсов или с помощью любой терминальной программы через последовательный порт компьютера, связанный с консольным портом устройства (рисунок 1.1).

На рисунке 1.1 изображена схема подключения по консольному порту: на тыльной (лицевой) стороне сетевого устройства (1) расположены силовой разъем для подключения шнура питания (2) и консольный порт (3), обеспечивающий подключение к COM-порту компьютера администратора посредством кабеля RJ-45-to-DB-9.

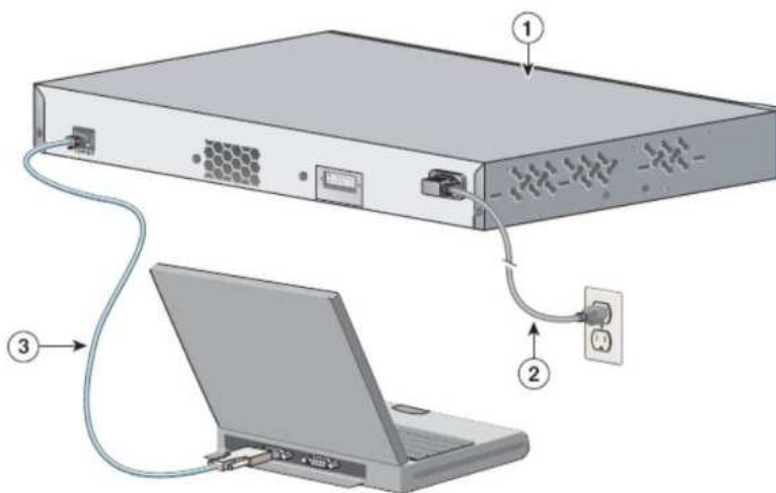


Рисунок 1.1 – Подключение по консольному кабелю

Последний способ предпочтительнее, потому что в процессе настройки оборудования могут измениться параметры физического порта или административного IP-интерфейса, что приведет к потере соединения, установленного по протоколу telnet или SSH.

COM-порт ПК (персонального компьютера) (консольный порт) сленговое название интерфейса стандарта RS-232, которым массово оснащались персональные компьютеры. Последовательным данный порт называется потому, что информация через него передаётся по одному биту, бит за битом (в отличие от параллельного порта). COM-порты в операционной системе Windows – это именованные каналы для передачи данных, называемые обычно COM1, COM2 и т. д. по порядку обнаружения драйверов соответствующих устройств. Максимально возможная скорость на интерфейсе 115 кбит/с.

На настоящий момент интерфейс считается устаревшим и отсутствует в большинстве ПК, тем не менее огромное количество сетевого оборудования (модемы, мультиплексоры, маршрутизаторы и т.д.) для первоначальной конфигурации имеют консольный порт, являющийся удаленным окончанием COM-порта.

Для работы с оборудованием посредством COM-порта с ПК, не имеющего такового применяется кабель-адаптер USB-COM, с помощью которого эмулируется работа консольного порта. Номер эмулируемого порта отображается в диспетчере устройств. Интерфейсы стандарта RS-232 бывают асинхронными и синхронными. COM-порт ПК является асинхронным интерфейсом.

Суть асинхронного принципа управления состоит вне зависимости (полностью или частично) работе (по времени) передатчика и приемника.

Наибольшее применение получили старт-стопные принципы синхронизации по битам и знакам. Суть стартстопного принципа управления состоит в том, что стартовый импульс в сообщении запускает местный синхрогенератор приемника, который работает на частоте передатчика, и линия стробируется в соответствии с частотой местного синхронизатора, а стоповый импульс в сообщении останавливает синхрогенератор.

Передача данных осуществляется порциями (кадрами). Начало и конец каждой порции информации отмечаются специальными метками.

Преимущества:

- устоявшаяся, несложная технология;
- недорогое оборудование (по сравнению с синхронным типом передачи), поскольку для взаимодействия приёмника и передатчика не требуется отдельных управляющих сигналов.

Недостатки:

- накладные расходы на передачу каждого символа составляют 20-30% (старт-стоповое обрамление и бит паритета);
- множественное искажение битов символа может сделать бесполезным применение паритетной схемы контроля ошибок;
- низкая скорость передачи (по сравнению с возможностями синхронной передачи).

Передача больших блоков данных более эффективно осуществляется методом синхронной передачи. Синхронная передача может выполняться как в бит-ориентированном режиме, так и в байт-ориентированном (символьном) режиме. Обычно данные буферизируются и передаются в виде сообщения (кадра) в отличие от асинхронного типа передачи, когда осуществляется транспортировка отдельно каждого символа. Поскольку сообщение передается в виде блока, на приёмной и передающей сторонах синхросчетчики должны поддерживаться в синхронном состоянии. Это достигается двумя способами:

- постоянной передачей отдельного синхронизирующего сигнала;
- применением самосинхронизирующего сигнала.

Как и в случае асинхронной передачи, синхронный метод передачи может осуществлять обнаружение ошибок. Для этого часто используется метод CRC (Cyclic-RedundancyCheck).

Преимущества:

- более эффективный;
- большие возможности организации передачи на высоких скоростях;
- улучшенный метод контроля ошибок.

Недостаток:

- требуется более сложное и дорогое оборудование.

COM-порты реализуются при помощи стандартных разъемов: 25-контактный (ISO 2110) и 9-контактный DB9 (рисунок 1.2).

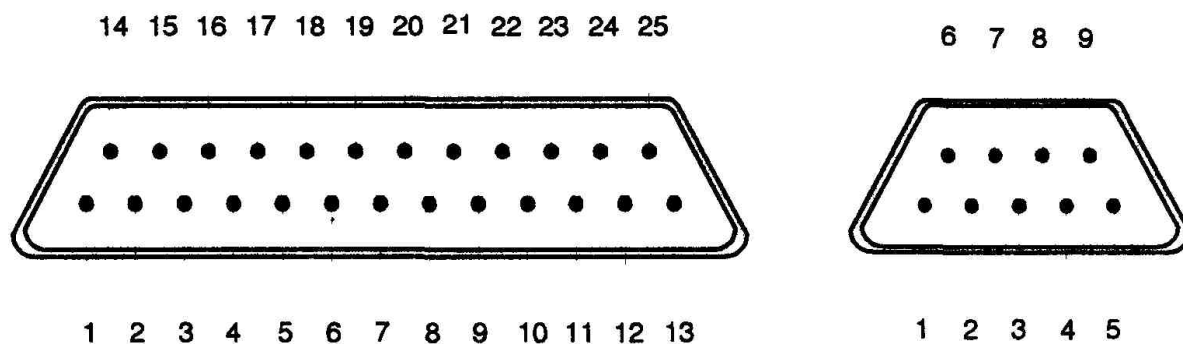


Рисунок 1.2 – Механические контактные разъемы RS-232

SSH (англ. Secure Shell — «безопасная оболочка») – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по зашифрованному каналу звуковой поток или видео. Также SSH может использовать сжатие передаваемых данных для последующего их шифрования, что удобно, например, для удалённого запуска клиентов на Windows.

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Какие существуют способы подключения к сетевому оборудованию для управления им?
- 2) Какую команду предпочтительней использовать при создании пароля на коммутаторах?
- 3) Опишите интерфейс V.24?

Алгоритм проведения эксперимента:

В случае использования персонального компьютера с операционной системой Windows.

1) С помощью консольного кабеля подключите СОМ-порт компьютера с программой PuTTY к консольному порту сетевого устройства. Выберите режим работы через СОМ-порт (рисунок 1.3). Номер СОМ-порта отображается в диспетчере устройств (рисунок 1.4).

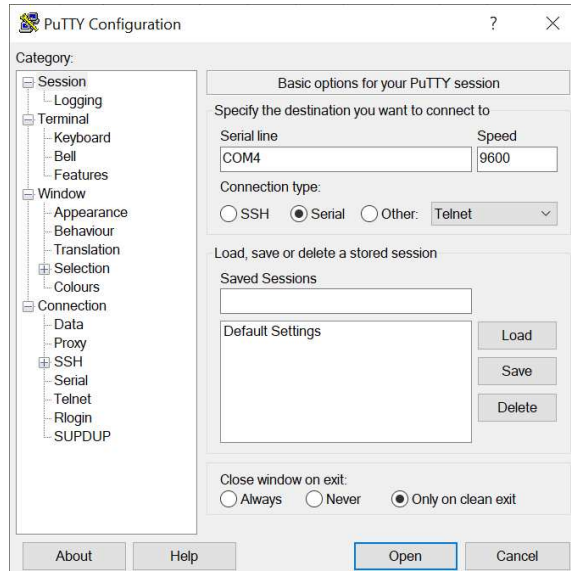


Рисунок 1.3 – Диалоговое окно с выбором СОМ-порта

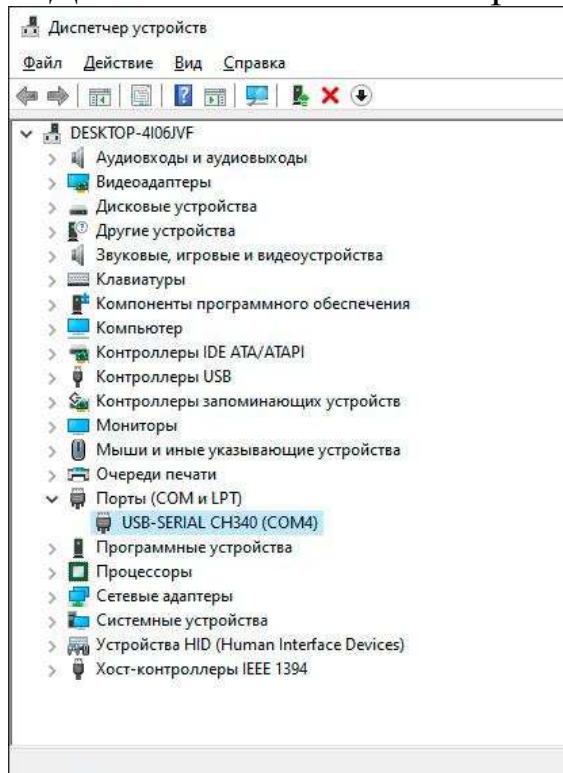


Рисунок 1.4 – Диалоговое окно диспетчера устройств

В случае использования оборудования от CiscoSystems.

2) Перейдите в привилегированный режим командой enable:

```
Router>enable
```

3) Перейдите в конфигурационный режим:

```
Router>#configureterminal
Enter configuration commands, one per line.
EndwithCNTL/Z.
```

4) Задайте имя сетевому устройству:

```
Router(config)#hostnameTELECOM1
```

5) Включите режим хранения паролей в файле конфигурации устройства в зашифрованном виде:

```
TELECOM1 (config) #servicepassword-encryption
```

6) Отключите управление сетевым устройством через HTTP, HTTPSиCDP:

```
TELECOM1 (config) #no ip http secure-server
TELECOM1 (config) #nocdprun
```

7) Задайте пароли на подключения через консольный порт:

```
TELECOM1 (config) #line console 0
TELECOM1 (config-line) #password cisco
TELECOM1 (config-line) #login
TELECOM1 (config-line) #exit
```

8) Задайте пароль на Enable-режим:

```
TELECOM1 (config) #enable secret cisco
TELECOM1 (config) #exit
TELECOM1#conf term
Enter configuration commands, one per line. End with
CNTL/Z.
```

9) ЗадайтеIP-адрес на интерфейсе gigabitEthernet 0/0:

```
TELECOM1 (config) #interface gigabitEthernet 0/0
TELECOM1 (config-if) #ip address 10.7.130.1 255.255.255.0
```

10) Включите интерфейс:

```
TELECOM1 (config-if) #no shutdown
TELECOM1 (config-if) #exit
```

11) Укажите имя домена и сгенерируйте RSA ключ:

```
TELECOM1(config)#ip domain name cisco.dom
TELECOM1(config)#crypto key generate rsa
The name for the keys will be: TELECOM1.cisco.dom
Choose the size of the key modulus in the range of 360
to 2048 for your
General Purpose Keys. Choosing a key modulus greater
than 512 may take a few minutes.
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-
exportable...[OK]
```

12) Создайте пользователя с именем user, паролем cisco1 и уровнем привилегий 15:

```
TELECOM1(config)#username user privilege 15 secret
cisco1
```

13) Активируйте протокол AAA и среду доступа через сеть по умолчанию SSH.

```
TELECOM1(config)#aaa new-model
TELECOM1(config)#line vty 0 4
TELECOM1(config-line)#transport input ssh
TELECOM1(config-line)#logging synchronous
TELECOM1(config-line)#exit
```

Алгоритм обработки полученных экспериментальных данных:

Представить скриншоты: выбора COM-порта, первоначальной настройки сетевого устройства из CLI.

ЛАБОРАТОРНАЯ РАБОТА №2 «БЛОКИРОВКА РЕЗЕРВНЫХ ПОРТОВ И АГРЕГИРОВАНИЕ КАНАЛОВ»

Цель занятия: изучение принципов блокировки резервных портов с использованием протоколов STP, PVST, RapidSTP и агрегирования каналов по протоколу LACP.

Задачи занятия:

- 1) Произвести построение сети с использованием протоколов STP и RapidSTP;
- 2) Создать сеть с агрегированием каналов по протоколу LACP;
- 3) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей, стеке протоколов сетевого оборудования;
- формирование умений выбора используемых программно-аппаратных средств защиты информации в компьютерных сетях и их режимов работы;
- формирование навыков контроля корректности функционирования и настройки программно-аппаратных средств защиты информации в компьютерных сетях.

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой Windows или Linux;
- 2) Коммутаторы (3 шт.).

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Протокол STP, основанный на стандарте мостового протокола IEEE 802.1D, обнаруживает и предотвращает формирование мостовых петель второго уровня. Параллельные маршруты в конфигурации сети могут существовать, но передача кадров допускается только по одному из них.

Коммутаторы сети запускают по одному экземпляру STP на каждую VLAN-сеть с помощью алгоритма PVST (Per-VLAN Spanning Tree – отдельные экземпляры распределенного связующего дерева для разных сетей VLAN). PVST-алгоритм требует использования между коммутаторами магистральных каналов.

Функционирование алгоритма STP и его конфигурирование на коммутаторах рассмотрим на примере упрощенной схемы сети и только для стандартной VLAN-сети с номером 1.

Так как поддержка протокола связующего дерева включена по умолчанию, то по истечении некоторого времени, необходимого для отработки алгоритма STP, на графе Вашей сети будет построено связующее дерево и, несмотря на присутствующие физические петли, между любыми узлами в сети будет существовать единственный маршрут.

Для вывода информации на оборудовании от Cisco Systems о состоянии STP используются следующие команды привилегированного режима:

- на активных интерфейсах:

```
Switch# show spanning-tree active
```

- на всех интерфейсах:

```
Switch#show spanning-tree detail
```

- на указанном интерфейсе:

```
Switch#show spanning-tree interface int-id
```

- в указанной VLAN-сети:

```
Switch#show spanning-tree vlan vlan-id
```

- вывод общей информации о состоянии STP:

```
Switch#show spanning-tree summary
```

Для конфигурирования протокола STP используются следующие команды режима глобального конфигурирования:

- включение функции поддержки протокола STP (с префиксом по – отключение):

```
Switch(config)#spanning-tree vlan vlan-id
```

- выбор режима функционирования протокола:

```
Switch(config)#spanning-treemode {pvst | rapid-pvst}
```

- выбор основного (primary) и дополнительного (secondary) корневого коммутатора:

```
Switch(config)#spanning-treevlanvlan-idroot {primary | secondary}
```

- установка приоритета коммутатора, допустимые значения параметра priority– 4096; 8192; 12288; 16384;20480; 24576; 28672; 32768; 36864; 40960; 45056; 49152; 53248;57344 и 61440 (по умолчанию – 32768):

```
Switch(config)#spanning-tree vlan vlan-id priority (priority – значение параметра)
```

Кроме приведенных есть и другие команды режимов глобального конфигурирования и конфигурирования интерфейсов, позволяющие более тонко настраивать функционирование протоколаSTP в сети.

Агрегирование каналов – технология, которая позволяет объединить несколько физических каналов в один логический.

Данное объединение позволяет увеличивать пропускную способность и надежность канала. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором, между коммутатором и хостом (рисунок 2.1).

Для агрегирования каналов существует и другое название: EtherChannel (в Cisco так называется агрегирование каналов, это может относиться как к настройке статических агрегированных каналов, так и с использованием протоколов LACP). Агрегирование каналов позволяет решить две задачи:

- повысить пропускную способность канала;
- обеспечить резерв на случай выхода из строя одного из каналов.

Большинство технологий по агрегированию позволяют объединять только параллельные каналы. То есть такие, которые начинаются на одном и том же устройстве и заканчиваются на другом.

Если рассматривать избыточные соединения между коммутаторами, то без использования специальных технологий для агрегирования каналов, передаваться данные будут только через один интерфейс, который не заблокирован STP. Такой вариант позволяет обеспечить резервирование каналов, но не дает возможности увеличить пропускную способность. Без использования STP такое избыточное соединение создаст петлю в сети.

Синтаксис команды `channel-group` на оборудовании от CiscoSystems:

- `active` – включить LACP; `passive` – включить LACP только если придет сообщение LACP; `on` – включить только Etherchannel:

```
sw(config-if) # channel-group<channel-group-
number>mode<<on> | <active | passive>>
```

Команды для просмотра информации:

```
sw# show etherchannel summary
sw1#show etherchannel port-channel
```

Перед настройкой агрегирования лучше выключить физические интерфейсы. Достаточно отключить их с одной стороны, затем настроить агрегирование с двух сторон и включить интерфейсы.

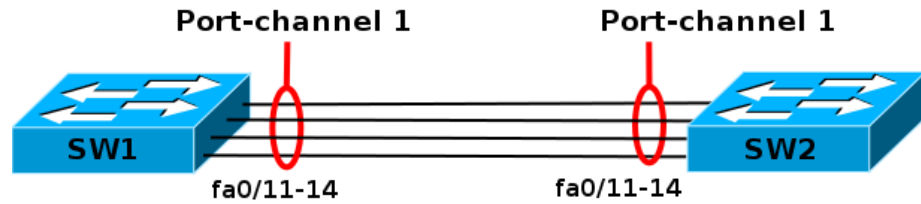


Рисунок 2.1 – Технология EtherChannel

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Для чего необходим протокол STP?
- 2) Может ли администратор каким-либо образом повлиять на расчет покрывающего дерева в сети?
- 3) Какой командой осуществляется выбор режима функционирования протокола?

Алгоритм проведения эксперимента:

- 1) Выполнить соединение 3 коммутатор по топологии «Кольцо», используя интерфейсы FastEthernet;
- 2) Определить активное связующее дерево STP;
- 3) Выбрать Switch3 дополнительным корневым коммутатором для расчета связующего дерева. Определить активное связующее дерево STP в сети.
- 4) Выбрать Switch1 основным корневым коммутатором для расчета связующего дерева. Определить активное связующее дерево STP в сети.
- 5) Установить приоритет для расчета связующего дерева на коммутаторе Switch2 – 20480. Определить активное связующее дерево STP в сети.
- 6) Удалить линию связи между коммутаторами Switch0 и Switch2. Определить приблизительное время расчета дерева по алгоритму PVST. Определить активное связующее дерево STP в сети.
- 7) Восстановить линию связи между коммутаторами Switch0 и Switch2. Установить на всех коммутаторах режим Rapid- PVST.

8) Удалить линию между коммутаторами Switch0 и Switch2. Определить приблизительное время расчета дерева по алгоритму Rapid-PVST.

9) С помощью протокола LACP настроить агрегирование с двух сторон на двух коммутаторах (рисунок 3.1).

Алгоритм обработки полученных экспериментальных данных:

1) Описать процесс прохождения пакетов в сети согласно установленному заданию;

2) Предоставить скриншоты выполнения каждого этапа работы.

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №3 «ВИРТУАЛЬНЫЕ ЛОКАЛЬНЫЕ СЕТИ VLAN»

Цель занятия: овладение основными навыками построения виртуальных локальных сетей на базе протокола IEEE 802.1Q.

Задачи занятия:

- 1) Построить локальную вычислительную сеть с использованием технологии VLAN;
- 2) Построить локальную вычислительную сеть с использованием технологий VLAN и Router-on-a-Stick;
- 3) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей, стеке протоколов сетевого оборудования;
- формирование умений выбора используемых программно-аппаратных средств защиты информации в компьютерных сетях и их режимов работы;
- формирование навыков синтеза шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях, настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации, управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях.

Материально-техническое оборудование и материалы:

- 1) Персональные компьютеры с операционной системой Windows или Linux (4-6 шт);
- 2) Коммутаторы 2 уровня (2 шт.);
- 3) Коммутатор 2 уровня с функциями 3 уровня (1 шт.);
- 4) Маршрутизатор (1 шт).

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на

лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

4) RFC3069 VLAN Aggregation for Efficient IP Address Allocation

5) IEEE's 802.1Q standard 2005 version

6) Cisco's Overview of Routing between Virtual LANs
<http://www.cisco.com>

7) RFC 3056 Connection of IPv6 Domains via IPv4 Clouds, February 2001.

8) RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers, August 2000.

9) RFC 3068 An Anycast Prefix for 6to4 Relay Routers, June 2001.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Виртуальной локальной сетью (VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети. Таким образом, становится невозможной передача кадров на основании адреса канального уровня между разными виртуальными сетями.

Основным назначением технологии VLAN является облегчение процесса создания изолированных сетей, впоследствии связываемых между собой с помощью маршрутизаторов (рисунок 3.1). Подобное построение сети позволяет избавиться от

распространения нежелательного трафика в различных её сегментах. Так, например, технология виртуальных сетей позволяет избежать периодического затопления всей сети широковещательными штормами.

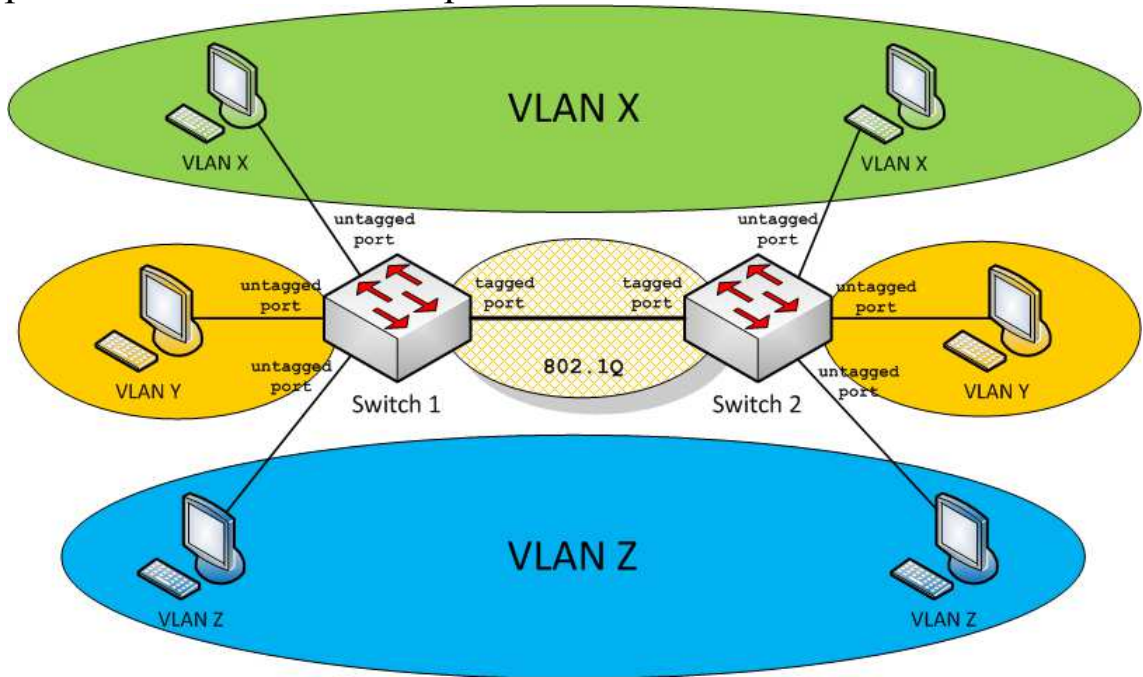


Рисунок 3.1 – Виртуальные локальные сети

Для передачи информации о принадлежности кадра к той или иной VLAN согласно стандарту IEEE 802.1Q в заголовок канального уровня добавляется дополнительный четырехбайтовый подзаголовок – тег. Кадр с инкапсулированным тегом принято называть тегированным. Пример тегированного кадра Ethernet приведен на рисунке 3.2.

6	6	4	2	42 - 1496	4								
Destination address	Source address	Tag 802.1Q	Длина/ Тип	Данные	Контр. сумма								
		<table border="1"> <tr> <td>2</td> <td>3 бита</td> <td>1 бит</td> <td>12 бит</td> </tr> <tr> <td>TPID (0x8100)</td> <td>PCP</td> <td>CFI</td> <td>VLAN ID</td> </tr> </table>				2	3 бита	1 бит	12 бит	TPID (0x8100)	PCP	CFI	VLAN ID
2	3 бита	1 бит	12 бит										
TPID (0x8100)	PCP	CFI	VLAN ID										

Рисунок 3.2 – Структура тегированного кадра Ethernet

Подзаголовок 802.1Q содержит, помимо идентификатора протокола VLAN – TPID (0x8100), индикатора канонического

формата CFI и трех бит приоритета кадра (к VLAN не относящихся), также 12 бит номера виртуальной сети, к которой принадлежит кадр. Соответственно, всего возможно создать до 4096 общих виртуальных сетей.

Коммутатор, поддерживающий работу с VLAN, оперирует таблицами коммутации, содержащими поле VLANID. Такой коммутатор, принимая кадр с заголовком 802.1Q, будет осуществлять в таблице поиск лишь среди тех портов, которые отмечены как участники указанного в теге VLAN.

Подробное описание технологии VLAN приводится в стандарте IEEE 802.1Q, определяющем базовые правила построения виртуальных локальных сетей.

Рекомендации по выполнению лабораторной работы для самостоятельного изучения:

Часть 1. Виртуальные локальные сети (VLAN)

В качестве примера рассмотрено создание трех виртуальных локальных сетей, как показано на рисунке 3.3.

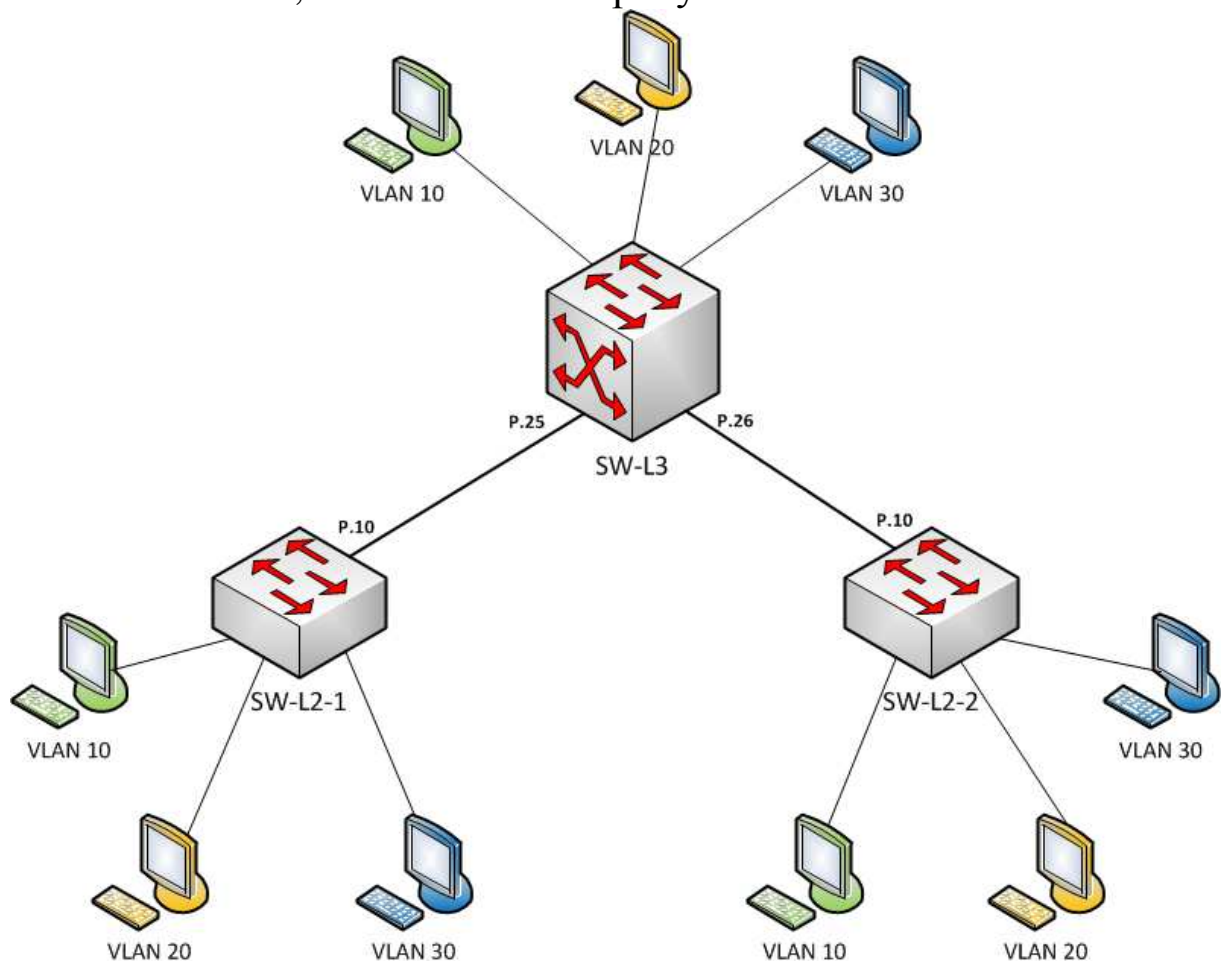


Рисунок 3.3 – Схема сети

Примечание: При недостаточном количестве рабочих машин в классе, создайте две виртуальные локальные сети вместо трех. Также уменьшить требуемое количество машин можно, создав сеть на двух коммутаторах.

Рассматриваемый в данной лабораторной работе способ организации виртуальных локальных сетей является наиболее распространенным и называется методом группировки портов.

Таблица 3.1 – Распределение VLAN

VLAN	Порты коммутаторов					
	SW-L2-1		SW-L2-2		SW-L3	
	Н	Т	Н	Т	Н	Т
10	1,2	10	1,2	10	1,2,3	25,26
20	3,4	10	3,4	10	4,5,6	25,26
30	5,6	10	5,6	10	7,8,9	25,26

Заметим, что на приведенной схеме компьютеры пользователей включаются непосредственно в порты коммутаторов, принадлежащие к определенным VLAN. Это значит, что трафик, которым обмениваются компьютер и порт коммутатора, не должен содержать инкапсулированного заголовка 802.1Q. Таким образом, порты коммутаторов можно разделить на две группы: нетегированные и тегированные. В широко распространенной терминологии они называются соответственно access- и trunk-порты.

Любой трафик, поступающий на нетегированный порт, принадлежащий определенному VLAN, будет передаваться дальше лишь в соответствии с таблицей коммутации для данного VLAN. Тегированный порт может передавать трафик нескольких VLAN, инкапсулируя в кадры Ethernet теги 802.1Q. В таблице 3.1 нетегированные порты помечены буквой Н, а тегированные – соответственно, буквой Т.

Для настройки коммутатора с помощью браузера необходимо зайти на его Web-интерфейс (таблица 3.2).

Таблица 3.2 – Web-интерфейсы коммутаторов

Коммутатор	Адрес Web-интерфейса
SW-L2-1	192.168.24.10

SW-L2-2	192.168.24.20
SW-L3	192.168.24.30

Примечание: Для удобства настройки коммутаторов необходимо подсоединиться к какому-либо порту коммутатора SW-L3, не задействованному в настраиваемой схеме VLAN (порты 10-24), и тогда из подсети 192.168.24.0/24 будут доступны все Web-интерфейсы коммутаторов.

Логин: admin

Пароль: admin

Настройка коммутаторов от D-Link (SW-L2-1 и SW-L2-2) производится следующим образом:

а) Выбирается пункт меню L2 Features → 802.1Q Static VLAN. На первой вкладке VLAN List отображаются настроенные на данном коммутаторе виртуальные локальные сети и входящие в них порты.

б) На вкладке Add/Edit VLAN в поле VID указывается номер создаваемого VLAN, а в поле VLAN Name – короткое (до 32 знаков) имя, после чего нажимается кнопка Apply (рисунок 3.4).

802.1Q Static VLAN

VLAN List | Add/Edit VLAN | Find VLAN | VLAN Batch Settings | Total Entries: 1

VID: 10 | VLAN Name: otdel-A (Name should be less than 32 characters) | Apply

Advertisement: Disabled

Port	Select	1	2	3	4	5	6	7	8	9	10
Tagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Tagged Ports

Untagged Ports

Forbidden Ports

Рисунок 3.4 – Создание VLAN

Подобным образом создаются все необходимые VLAN.

с) На вкладке VLAN List отображаются созданные пустые VLAN. Затем необходимо добавить в них соответствующие порты. Нажав кнопку Edit напротив нужного VLAN и, попав в окно редактирования, необходимо выставить радиокнопками требуемое

состояние (тегированный/нетегированный) портов входящих в VLAN (рисунок 3.5).

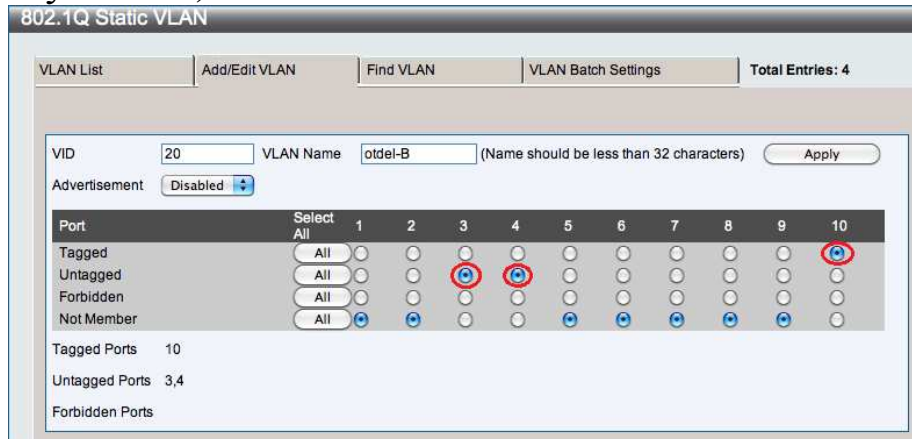


Рисунок 3.5 – Добавление портов в VLAN

Примечание: Положение радиокнопки NotMember означает, что данный порт не является участником настраиваемого VLAN.

Аналогично настраиваются все остальные VLAN.

Настройка коммутатора от D-Link (SW-L3) отличается от вышеописанной лишь тем, что производится в меню L2 Features→VLAN→802.1Q Static VLAN.

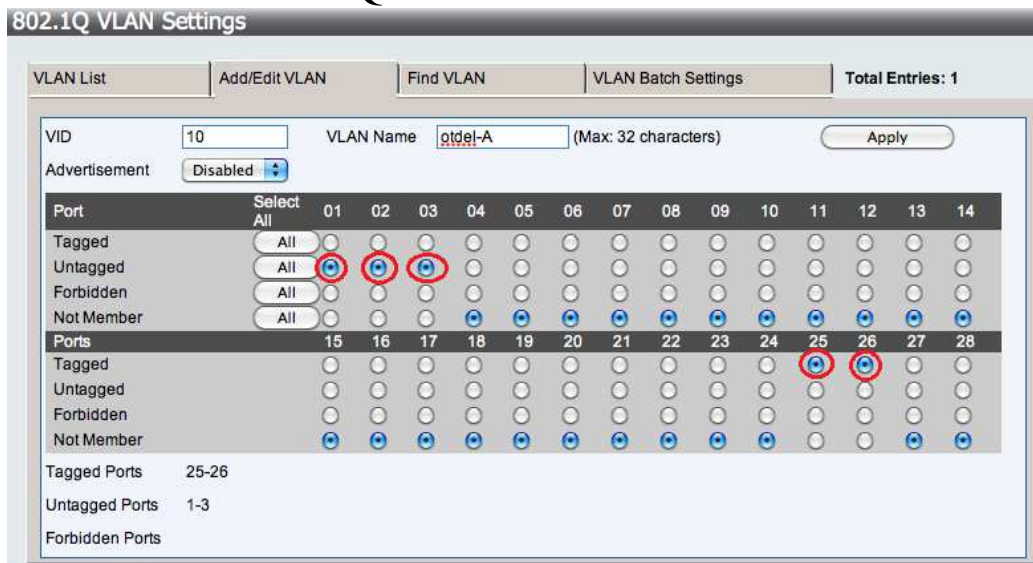


Рисунок 3.6 – Настройка портов VLAN в SW-L3

Запуская утилиту ping на разных компьютерах сети, можно убедиться в том, что друг другу доступны лишь участники одного и того же VLAN.

Часть 2. Маршрутизация между VLAN

Разделив локальную сеть на три изолированных подсети с помощью технологии VLAN, передача трафика между

ниминевозможна. Однако зачастую виртуальные локальные сети должны взаимодействовать, и такое взаимодействие может быть осуществлено на сетевом уровне с помощью маршрутизатора или коммутатора третьего уровня (рисунок 3.7).

Предположим, что локальная сеть состоит из трех подсетей, расположенных в трех различных VLAN (таблица 3.3). Для экономии портов маршрутизатора достаточно использовать один маршрутизирующий интерфейс – такая схема называется Router-on-a-Stick.

Таблица 3.3 – Распределение VLAN

VLAN	Подсети	Порты коммутаторов					
		SW-L2-1		SW-L2-2		SW-L3	
		Н	Т	Н	Т	Н	Т
10	192.168.10.0/24	1,2	10	1,2	10	1,2,3	25,26
20	192.168.20.0/24	3,4	10	3,4	10	4,5,6	25,26
30	192.168.30.0/24	5,6	10	5,6	10	7,8,9	25,26

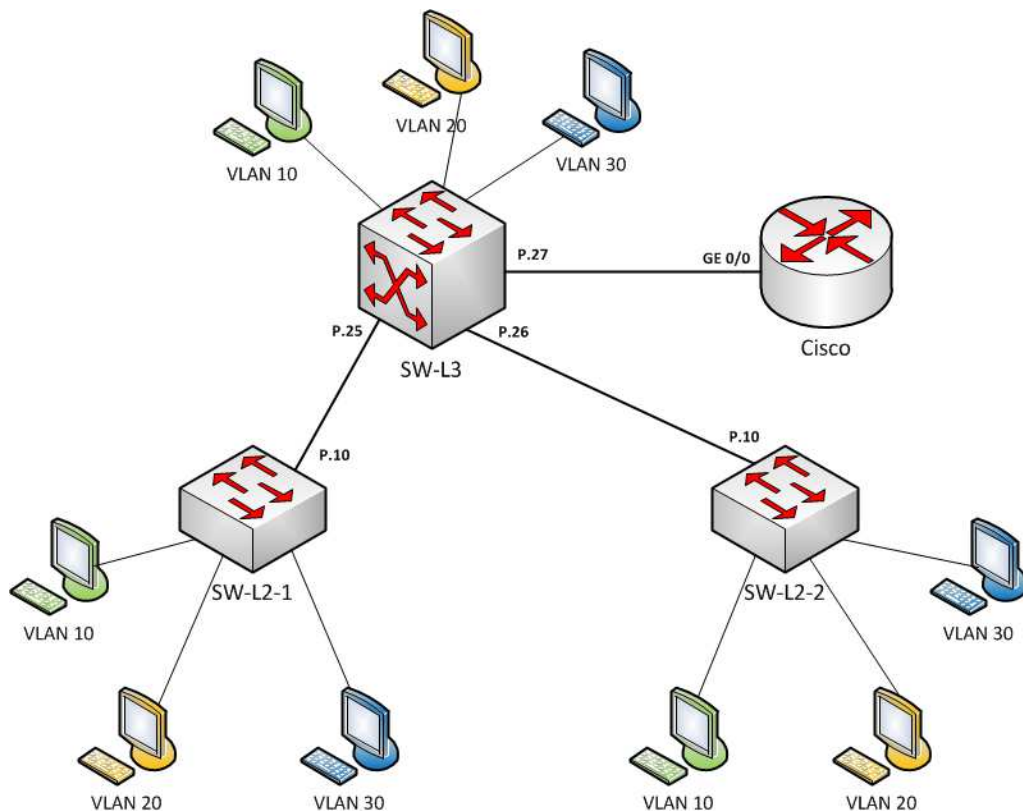


Рисунок 3.7 – Схема сети с подключением маршрутизатора

Настроив коммутаторы, аналогично тому, как было показано в первой части работы, необходимо добавить во все VLAN новый тегированный порт для связи с маршрутизатором.

Для использования одного порта маршрутизатора одновременно в трех различных подсетях необходимо создать так называемые субинтерфейсы. Субинтерфейсы представляют собой виртуальные интерфейсы, расположенные на одном физическом порту и позволяющие ему работать одновременно в нескольких подсетях.

Пример настройки маршрутизатора от CiscoSystems:

```
cisco-core>en
cisco-core# configure terminal
cisco-core(config)# interface gigabitEthernet 0/0
cisco-core(config-if)# no shutdown/включениеинтерфейса
cisco-core(config-if)# exit
cisco-core(config)# interface gigabitEthernet 0/0.10
/создание субинтерфейса 10 на физическом интерфейсе
gigabitEthernet 0/0
cisco-core(config-subif)# encapsulation dot1q 10
/указание,
что трафик на данном субинтерфейсе имеет инкапсулированный заголовок 802.1Q с VLAN ID=10
cisco-core(config-subif)# ip address 192.168.10.1
255.255.255.0 /задание IP-адреса на субинтерфейсе
cisco-core(config-subif)# exit /выход
cisco-core(config)# interface gigabitEthernet 0/0.20
cisco-core(config-subif)# encapsulation dot1q 20
cisco-core(config-subif)# ip address 192.168.20.1
255.255.255.0
cisco-core(config-subif)# exit
cisco-core(config)# interface gigabitEthernet 0/0.30
cisco-core(config-subif)# encapsulation dot1q 30
cisco-core(config-subif)# ip address 192.168.30.1
255.255.255.0
cisco-core(config)# ^Z
```

Просмотр интерфейсов осуществляется командой:

```
cisco-core#show ip interface brief
```

```
Interface IP-Address    OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES  NVRAM up up
GigabitEthernet0/0.10 192.168.10.1 YES manual up up
GigabitEthernet0/0.20 192.168.20.1 YES manual up up
GigabitEthernet0/0.30 192.168.30.1 YES manual up up
```

Примечание: Номера подсетей, субинтерфейсов и VLAN выбраны одинаковыми только для наглядности и во избежание путаницы. На практике они могут не совпадать.

Для проверки маршрутизации между разными VLAN необходимо утилитой ping проверить взаимную доступность всех узлов, находящихся в различных подсетях. Затем с помощью утилиты traceroute убедиться в том, что взаимодействие между узлами одного VLAN осуществляется свободно на канальном уровне, а между узлами, принадлежащими к разным VLAN – через соответствующий маршрутизирующий интерфейс (рисунок 3.8).

```
bash-3.2$ traceroute 192.168.10.91
traceroute to 192.168.10.91 (192.168.10.91), 64 hops max, 52 byte packets
 1 192.168.10.91 (192.168.10.91) 0.965 ms 0.232 ms 0.179 ms
bash-3.2$ traceroute 192.168.20.92
traceroute to 192.168.20.92 (192.168.20.92), 64 hops max, 52 byte packets
 1 192.168.10.1 (192.168.10.1) 1.328 ms 0.327 ms 0.444 ms
 2 192.168.20.92 (192.168.20.92) 1.302 ms 0.524 ms 0.512 ms
bash-3.2$ traceroute 192.168.30.93
traceroute to 192.168.30.93 (192.168.30.93), 64 hops max, 52 byte packets
 1 192.168.10.1 (192.168.10.1) 1.399 ms 0.833 ms 0.327 ms
 2 192.168.30.93 (192.168.30.93) 1.383 ms 0.394 ms 0.492 ms
bash-3.2$
```

Рисунок 3.8 – Результаты трассировки

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Какова область применения VLAN?
- 2) Какие существуют способы разделения сети на VLAN?
- 3) Какие знаете методы настройки VLAN ?
- 4) Как разделять сеть на VLAN, настраивать маршрутизацию между отдельными VLAN внутри одной сети.

Алгоритм проведения эксперимента:

- 1) Соберите сеть (рисунок 3.3).

2) Настройте коммутаторы сети согласно полученному заданию.

3) Убедитесь в доступности только участников одного и того же VLAN.

4) Добавьте маршрутизатор в схему сети (рисунок 3.7). Добавьте во все VLAN новый тегированный порт для связи с маршрутизатором.

5) Настройте маршрутизатор для использования одного порта одновременно в трех различных подсетях.

6) Проверьте маршрутизацию между разными VLAN.

Варианты заданий:

Таблица 3.4 – Задания к первой части лабораторной работы

Вариант	VLAN	Порты коммутаторов					
		SW-L2-1		SW-L2-2		SW-L3	
		Н	Т	Н	Т	Н	Т
1	5	5,6	8	5,6	9	3-5	14,15
	6	3,4	8	3,4	9	6-8	14,15
	7	1,2	8	1,2	9	9-11	14,15
2	31	3,4	1	3,4	2	13,14	5,6
	51	5,6	1	5,6	2	15,16	5,6
	71	7,8	1	7,8	2	17,18	5,6
3	90	1,3	10	1,3	9	2,4	23,24
	200	2,4	10	2,4	9	6,8	23,24
	500	5,7	10	5,7	9	10,12	23,24
4	100	1,2	9	1,2	10	1-4	22,24
	350	3,4	9	3,4	10	5-8	22,24
	700	5,6	9	5,6	10	9-12	22,24

Таблица 3.5 – Задания ко второй части лабораторной работы

Вариант	VLAN	Подсети	Порты коммутаторов					
			SW-L2-1		SW-L2-2		SW-L3	
			Н	Т	Н	Т	Н	Т
1	5	192.168.50.0/24	5,6	8	5,6	9	3-5	14,15
	6	192.168.60.0/24	3,4	8	3,4	9	6-8	14,15
	7	192.168.70.0/24	1,2	8	1,2	9	9-11	14,15
2	31	172.16.31.0/24	3,4	1	3,4	2	13,14	5,6
	51	172.16.51.0/24	5,6	1	5,6	2	15,16	5,6

	71	172.16.71.0/24	7,8	1	7,8	2	17,18	5,6
3	90	192.168.9.0/24	1,3	10	1,3	9	2,4	23,24
	200	192.168.20.0/24	2,4	10	2,4	9	6,8	23,24
	500	192.168.50.0/24	5,7	10	5,7	9	10,12	23,24
4	100	10.10.0.0/16	1,2	9	1,2	10	1-4	22,24
	350	10.35.0.0/16	3,4	9	3,4	10	5-8	22,24
	700	10.70.0.0/16	5,6	9	5,6	10	9-12	22,24

Алгоритм обработки полученных экспериментальных данных:

Представить схемы собранных сетей, результаты проверки доступности узлов, листинг настройки маршрутизатора.

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №4 «СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ В СЕТЯХ IPv4 И IPv6»

Цель занятия: получение навыков конфигурации локальной сети на основе протоколов IPv4 и IPv6 с использованием статической маршрутизации.

Задачи занятия:

- 1) Построить сеть на базе маршрутизаторов с использованием статической маршрутизации по протоколу IPv4;
- 2) Построить сеть на базе маршрутизаторов с использованием статической маршрутизации по протоколу IPv6;
- 3) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей, стеке протоколов сетевого оборудования, составе типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
- формирование навыков управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях.

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой (1 шт.);
- 2) Программный маршрутизатор (1 шт.);
- 3) Маршрутизаторы (2 шт.).

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

- 1) Соболев, Б. В. Сети и телекоммуникации [Текст]:

учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Базовое иерархическое построение сети предполагает наличие максимум трех уровней иерархии: ядро сети, уровень агрегации и уровень доступа (рисунок 4.1). В ядре как минимум находятся опорные маршрутизаторы, могут быть расположены граничные маршрутизаторы и серверы услуг.

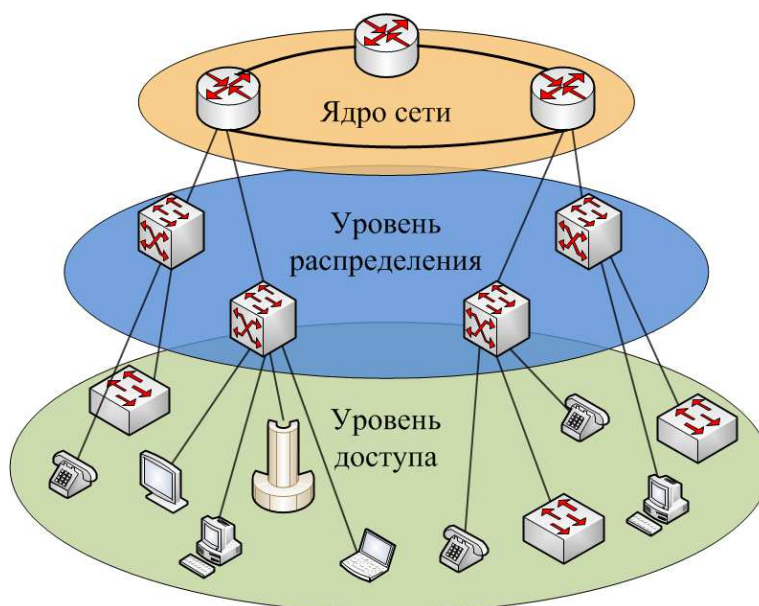


Рисунок 4.1 – Трехуровневая базовая модель построения сети

Уровень агрегации обеспечивает возможность агрегации и распределения трафика внутри сети оператора, может выполнять роль интегратора отдельных сегментов сети. Уровень доступа организует возможность физического доступа пользователя к сети оператора. Подобный подход не зависит от используемой

оператором технологии, но позволяет эффективно выстроить архитектуру, повысив устойчивость сети, и сделать процессы управления сетью прозрачными.

Отметим, что в небольших сетях может происходить вырождение иерархии до глубины в два уровня: доступ и ядро. Ядро небольшой сети представляет собой один маршрутизатор, выполняющий функции шлюза и, иногда, DNS-сервера. В этом случае чаще всего используется статическая маршрутизация, а управление потоками заключается в задании маршрутного правила.

В обобщенном виде запись маршрутного правила (далее маршрута) можно представить так:

```
Route network netmask gateway
```

Например, конкретная запись может быть представлена как:

```
Route 12.5.7.0 255.255.255.0 78.3.65.1,
```

где 12.5.7.0 – это адрес подсети (network), 255.255.255.0 – маска данной подсети (netmask), а 78.3.65.1 – адрес шлюза (gateway).

Шлюз представляет собой маршрутизатор, на который посылается весь трафик, удовлетворяющий данному маршруту, т.е. имеющий адрес получателя пакетов входящий в указанную подсеть.

Отметим, что существуют также многие другие способы маршрутизации пакетов, учитывающие различные параметры трафика (policyrouting), адаптирующиеся под изменяющуюся топологию сети и т.д., однако они используются в крупных сетях с динамической маршрутизацией и будут рассмотрены позднее.

Рекомендации по выполнению лабораторной работы для самостоятельного изучения:

Часть 1. Статическая маршрутизация на базе протокола IPv4

Ход выполнения работы проиллюстрирован на примере настройки маршрутизации в тестовой сети, приведенной на рисунке 4.2.

Для успешного выполнения лабораторной работы необходимо подготовить маршрутизаторы. На каждом программном маршрутизаторе следует запустить пакет маршрутизации Quagga. Применяемая в Quagga система команд очень близка к системе команд Cisco.

Включение программного маршрутизатора и подключение к нему, выполняется под суперпользователем:

```
login: root
passw: simulator
```

из запуска Quagga:

```
root@soft-core# service zebra start
```

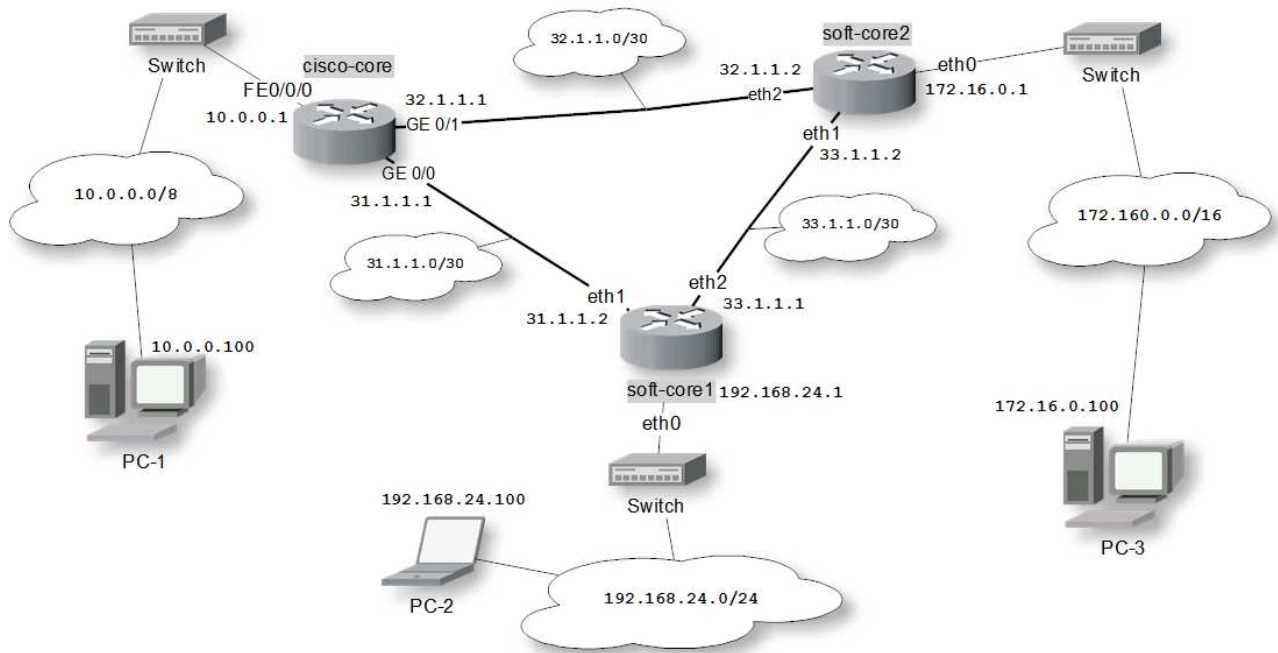


Рисунок 4.2 – Схема тестовой сети IPv4

Примечание: Обратите внимание, что при запуске пакета маршрутизации Quagga, он перехватывает управление сетевыми ресурсами и заменяет существующую сетевую конфигурацию своей, хранящейся в файле `/etc/quagga/zebra.conf`. По умолчанию в данной конфигурации на `soft-core1` (программном маршрутизаторе ядра 1) настроен интерфейс `eth0=192.168.24.1/24`. В случае использования в лабораторной работе двух программных маршрутизаторов, то на `soft-core2` (программном маршрутизаторе ядра 2) `eth0=172.16.0.1/16`.

На программные маршрутизаторы можно зайти посредством протокола SSH из тех локальных сетей, шлюзами которых они являются, т.е. на `soft-core1` через интерфейс `eth0` с адресом `192.168.24.1`, а на `soft-core2` – через `eth0` с адресом `172.16.0.1`.

Примечание: Для того, чтобы осуществить удаленное соединение по протоколу SSH, на машинах с ОС Linux необходимо запустить терминал и набрать команду:

```
ssh логин@IP-адрес_удаленного_хоста
```

после чего ввести запрашиваемый пароль. Логин и пароль на программном маршрутизаторе стенда по умолчанию:

```
login: admin
passw: admin
```

Важно: необходимо очистить таблицу правил фаервола на каждом программном маршрутизаторе. Это действие должно выполняться от суперпользователя:

```
pc2$ sshadmin@192.168.24.1
admin@192.168.24.1's password:
[admin@localhost ~]$ su
[root@localhost ~]$ iptables -F
[root@localhost ~]$ ip6tables -F
```

Для получения доступа к консоли управления Quagga, необходимо, установив удаленное подключение по SSH, набрать следующую команду:

```
telnetlocalhost 2601
```

Таким образом, подключаемся к процессу, ожидающему соединения на порту 2601 программного маршрутизатора (маршрутизирующий демон zebra).

Примечание: Пароль при подключении к консоли Quagga по умолчанию «softcore».

Процесс конфигурирования программного маршрутизатора выглядит следующим образом:

```
pc2$ sshadmin@192.168.24.1
admin@192.168.24.1's password:
[admin@localhost ~]$ telnet localhost 2601
soft-core1.lab> enable
soft-core1.lab# configure terminal
soft-core1.lab(config)# ip forwarding
/включениемаршрутизации IP
soft-core1.lab(config)# interface eth1
/настройкаинтерфейса eth1
```

```

soft-core1.lab(config-if)# ip address
31.1.1.2/30/присваиваниеадреса IPv4
soft-core1.lab(config-if)# description to
Cisco/добавлениеописания
soft-core1.lab(config-if)# no shutdown
    /включениеинтерфейса
soft-core1.lab(config-if)# exit/выход из режима
конфигурирования интерфейса
soft-core1.lab(config)# interface eth2
soft-core1.lab(config-if)# ip address 33.1.1.1/30
soft-core1.lab(config-if)# description to SC-2
soft-core1.lab(config-if)# no shutdown
soft-core1.lab(config-if)# exit
/Добавление статических маршрутов в формате
"dst_network/netmasknext-hop"
soft-core1.lab(config)# ip route 10.0.0.0/8 31.1.1.1
soft-core1.lab(config)# ip route 172.16.0.0/16 33.1.1.2
/Просмотртаблицымаршрутизации
soft-core1.lab# show ip route
Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF,I - ISIS, B - BGP, > - selected route, *
- FIB route
S>* 10.0.0.0/8 [1/0] via 31.1.1.1, eth1
C>* 31.1.1.0/30 is directly connected, eth1
C>* 33.1.1.0/30 is directly connected, eth2
C>* 127.0.0.0/8 is directly connected, lo
S>* 172.16.0.0/16 [1/0] via 33.1.1.2, eth2
C>* 192.168.24.0/24 is directly connected, eth0

```

Для контроля функционирования построенной сети запустите сеанс удаленного доступа по SSH и утилитами ping и traceroute проверьте доступность подключенного порта другого маршрутизатора и путь прохождения пакетов до него.

```

pc2$ ssh admin@192.168.24.1
admin@192.168.24.1's password:
Last login: Thu Jul 19 20:18:53 2012 from
192.168.24.100
[admin@localhost ~]$ ping 33.1.1.2
PING 33.1.1.2 (33.1.1.2) 56(84) bytes of data.
64 bytes from 33.1.1.2: icmp_seq=1 ttl=64 time=0.323 ms
64 bytes from 33.1.1.2: icmp_seq=2 ttl=64 time=0.095 ms
64 bytes from 33.1.1.2: icmp_seq=3 ttl=64 time=0.110 ms
--- 33.1.1.2 ping statistics ---

```

```

3 packets transmitted, 3 received, 0% packet loss, time
1999ms
rtt min/avg/max/mdev = 0.09/0.16/0.30/0.10 ms
[admin@localhost ~]$ traceroute 33.1.1.2
traceroute to 33.1.1.2 (33.1.1.2), 30 hops max, 60 byte
packets
1  33.1.1.2 (33.1.1.2)  0.262 ms  0.074 ms  0.058 ms

```

В случае использования маршрутизаторов от CiscoSystems. С компьютера управления вход на консольный порт осуществляется командой:

```
picocom /dev/ttyS0
```

и включением маршрутизатора. После загрузки на экране будет представлено приглашение. После производится следующая настройка:

```

cisco-core>enable          /переход в режим exec
cisco-core#configure terminal
cisco-core(config)#ip classless /включение CIDR
cisco-core(config)#ip routing /включение IP-
маршрутизации
/Настройка сетевых интерфейсов
cisco-core(config)#interface gigabitEthernet 0/0/выбор
интерфейса для настройки
cisco-core(config-if)#ip address 31.1.1.1
255.255.255.252 /присваивание интерфейсу IP-адреса и
маски подсети
cisco-core(config-if)#description to soft-core1
/добавление описания интерфейса (необязательно)
cisco-core(config-if)#no shutdown /включение интерфейса
cisco-core(config-if)#exit /выход из режима
конфигурирования данного интерфейса
cisco-core(config)#interface gigabitEthernet 0/1
cisco-core(config-if)#ip address 32.1.1.1
255.255.255.252
cisco-core(config-if)#description to soft-core2
cisco-core(config-if)#no shutdown
cisco-core(config-if)#end /выход из режима конфигурации
/Создание статических маршрутов
cisco-core#configureterminal
/В маршруте указывается в качестве шлюза next-hop
маршрутизатора
cisco-core(config)#ip route 192.168.24.0 255.255.255.0
31.1.1.2

```



```

cisco-core(config)#ip route 172.16.0.0 255.255.0.0
32.1.1.2
cisco-core(config)#exit
/Просмотр состояния интерфейсов и маршрутов
cisco-core#show ip interface brief
cisco-core#show ip route
/Проверка доступности LAN-интерфейсов шлюзов
cisco-core#ping 192.168.24.1
cisco-core#ping 172.16.0.1

```

Если интерфейсы доступны, значит маршрутизация настроена верно.

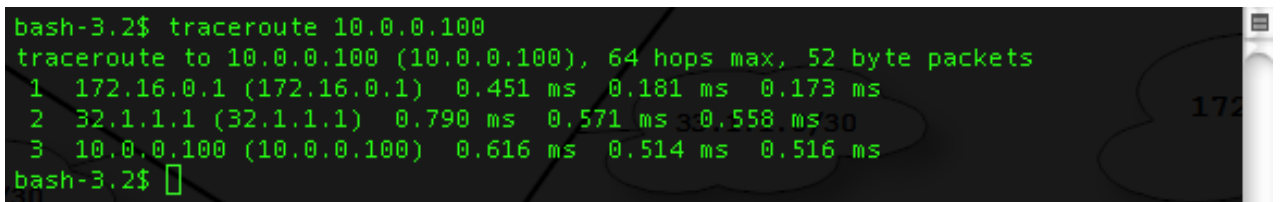
После настройки маршрутизаторов ядра нужно проверить взаимную доступность локальных подсетей. Для этого с различных машин, находящихся в разных подсетях производится несколько проверок доступности подсетей.

```

pc1#ping 192.168.24.100
pc1#ping 172.16.0.100
pc2#ping 10.0.0.100
pc2#ping 172.16.0.100
pc3#ping 192.168.24.100
pc3#ping 10.10.0.100

```

Если ping проходит успешно, отслеживание пути продвижения пакетов по сети производится утилитой traceroute (рисунок 4.3).



```

bash-3.2$ traceroute 10.0.0.100
traceroute to 10.0.0.100 (10.0.0.100), 64 hops max, 52 byte packets
 1 172.16.0.1 (172.16.0.1)  0.451 ms  0.181 ms  0.173 ms
 2 32.1.1.1 (32.1.1.1)    0.790 ms  0.571 ms  0.558 ms
 3 10.0.0.100 (10.0.0.100) 0.616 ms  0.514 ms  0.516 ms
bash-3.2$

```

Рисунок 4.3 – Прохождение пакетов через сеть.

Снятие ARP-таблицы с маршрутизаторов сети. Для того чтобы посмотреть ARP-таблицу программного маршрутизатора, необходимо подключиться к нему по SSH и ввести команду ipneighbor (рисунок 4.4).

```
[admin@localhost ~]$ ip neighbor
33.1.1.2 dev eth2 lladdr 00:1b:21:cc:0f:4e DELAY
31.1.1.1 dev eth1 lladdr 64:00:f1:19:6a:60 STALE
[admin@localhost ~]$ ping -c1 33.1.1.2
PING 33.1.1.2 (33.1.1.2) 56(84) bytes of data.
64 bytes from 33.1.1.2: icmp_seq=1 ttl=64 time=0.093 ms

--- 33.1.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.093/0.093/0.093/0.000 ms
[admin@localhost ~]$ ip neighbor
33.1.1.2 dev eth2 lladdr 00:1b:21:cc:0f:4e REACHABLE
31.1.1.1 dev eth1 lladdr 64:00:f1:19:6a:60 STALE
[admin@localhost ~]$
```

Рисунок 4.4 – ARP-таблица программного маршрутизатора

Обратите внимание на то, как изменяется статус записи об узле 33.1.1.2 после проверки связи с ним. Просмотр ARP-таблицы в маршрутизаторе Cisco осуществляется командой `show arp` (рисунок 4.5).

```
cisco-core#show arp
Protocol Address      Age (min) Hardware Addr  Type  Interface
Internet 10.0.0.1        -        6400.f119.6a60  ARPA  Vlan2
Internet 10.0.0.100     6        001d.0fc0.bcb3  ARPA  Vlan2
Internet 31.1.1.1       -        6400.f119.6a60  ARPA  GigabitEthernet0/0
Internet 31.1.1.2      15       001b.21cc.10fb  ARPA  GigabitEthernet0/0
Internet 32.1.1.1       -        6400.f119.6a61  ARPA  GigabitEthernet0/1
Internet 32.1.1.2       0        001b.21cc.10d9  ARPA  GigabitEthernet0/1
cisco-core#
```

Рисунок 4.5 – ARP-таблица маршрутизатора Cisco

Часть 2. Статическая маршрутизация на базе протокола IPv6

Эта часть лабораторной работы аналогична рассмотренной в первой части, за исключением сетевого протокола: в данном случае сеть построена на IPv6. Схема тестовой сети приведена на рисунке 4.6.

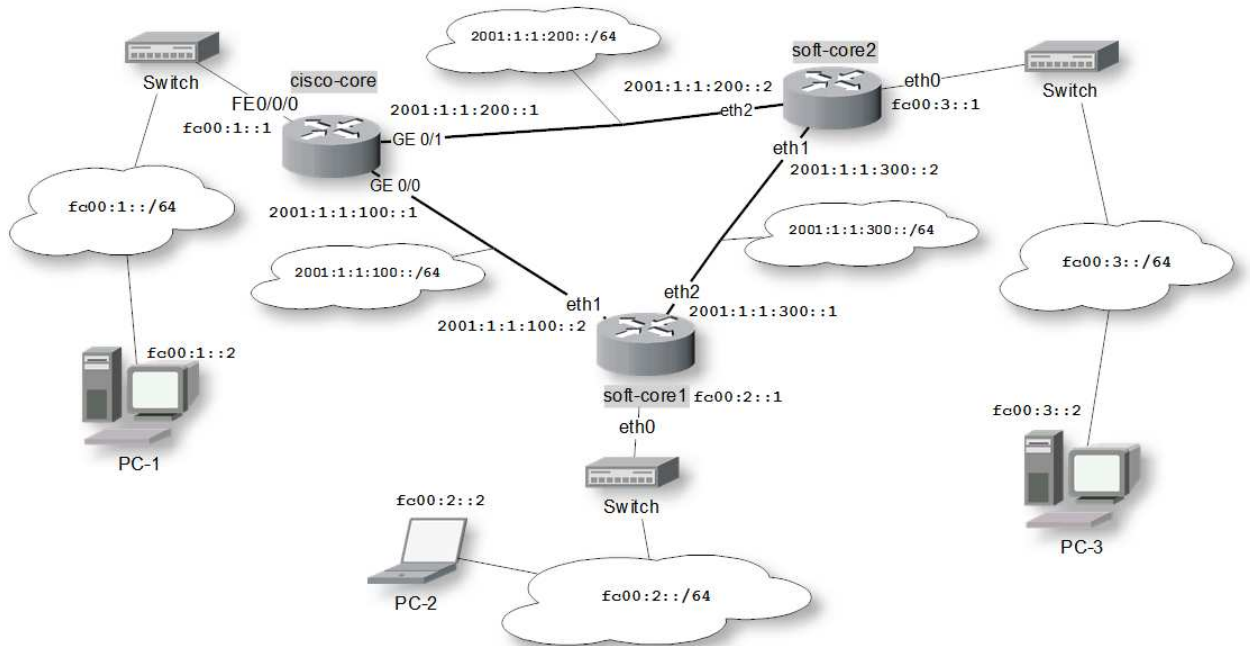


Рисунок 4.6 – Схема тестовой сети IPv6

Настройка программного маршрутизатора для работы в сети с IPv6-адресацией осуществляется аналогично проведенной для сетей IPv4:

- 1) Осуществляются необходимые подключения.
- 2) Конфигурируется программный маршрутизатор. Обратите внимание на то, что интерфейсам eth0 по умолчанию присвоены только IPv4-адреса!

```
pc2$ ssh admin@192.168.24.1
admin@192.168.24.1's password:
[admin@localhost ~]$ telnet localhost 2601
soft-core1.lab> enable
soft-core1.lab# configure terminal
soft-core1.lab(config)# ipv6 forwarding
soft-core1.lab(config)# interface eth0
soft-core1.lab(config-if)# ipv6 address fc00:2::1/64
soft-core1.lab(config-if)# exit
soft-core1.lab(config)# interface eth1
soft-core1.lab(config-if)# ipv6 address
2001:1:1:100::2/64
soft-core1.lab(config-if)# exit
soft-core1.lab(config)# interface eth2
soft-core1.lab(config-if)# ipv6 address
2001:1:1:300::1/64
soft-core1.lab(config-if)# exit
```

```
soft-core1.lab(config)# ipv6 route fc00:1::/64
2001:1:1:100::1
soft-core1.lab(config)# ipv6 route fc00:3::/64
2001:1:1:300::2
soft-core1.lab(config)# exit
```

Данная настройка производится в соответствии с заданием.

3) Проверяется доступность программного маршрутизатора (рисунок 4.7).

```
TonyMac:~ tony$ ssh admin@fc00:2::1
admin@fc00:2::1's password:
Last login: Thu Jul 26 18:55:49 2012 from fc00:2::2
[admin@localhost ~]$ ping6 -c2 2001:1:1:300::2
PING 2001:1:1:300::2(2001:1:1:300::2) 56 data bytes
64 bytes from 2001:1:1:300::2: icmp_seq=1 ttl=64 time=0.174 ms
64 bytes from 2001:1:1:300::2: icmp_seq=2 ttl=64 time=0.117 ms

--- 2001:1:1:300::2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.117/0.145/0.174/0.030 ms
[admin@localhost ~]$ traceroute6 2001:1:1:300::2
traceroute to 2001:1:1:300::2 (2001:1:1:300::2), 30 hops max, 80 byte packets
 1 2001:1:1:300::2 (2001:1:1:300::2) 0.165 ms 0.121 ms 0.096 ms
[admin@localhost ~]$
```

```
TonyMac:~ tony$ ssh admin@fc00:3::1
admin@fc00:3::1's password:
Last login: Thu Jul 26 18:58:21 2012 from fc00:2::2
[admin@localhost ~]$ ping6 -c2 2001:1:1:300::1
PING 2001:1:1:300::1(2001:1:1:300::1) 56 data bytes
64 bytes from 2001:1:1:300::1: icmp_seq=1 ttl=64 time=0.162 ms
64 bytes from 2001:1:1:300::1: icmp_seq=2 ttl=64 time=0.089 ms

--- 2001:1:1:300::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.089/0.125/0.162/0.038 ms
[admin@localhost ~]$ traceroute6 2001:1:1:300::1
traceroute to 2001:1:1:300::1 (2001:1:1:300::1), 30 hops max, 80 byte packets
 1 2001:1:1:300::1 (2001:1:1:300::1) 0.099 ms 0.065 ms 0.045 ms
[admin@localhost ~]$
```

Рисунок 4.7 – Проверка взаимной доступности

В случае использования оборудования от CiscoSystems после загрузки маршрутизатора на экране появится приглашение. Затем производится настройка:

```
cisco-core>enable /переходв режимехес
cisco-core#configureterminal /конфигурирование из терминала
cisco-core(config)#ipv6 unicast-routing
/включениемаршрутизации IPv6
cisco-core(config)#ipv6 cef /включениеподдержки Cisco Express Forwarding для протокола IPv6
/Настройка сетевых интерфейсов
cisco-core(config)#interface vlan 2
```

```

cisco-core(config-if)#ipv6 address fc00:1::1/64
/Задание IPv6 адресатипа Unique Local интерфейсу LAN
cisco-core(config-if)#no shutdown /включениеинтерфейса
cisco-core(config-if)#exit
cisco-core(config)#interface gigabitEthernet 0/0
/настройкаинтерфейса GE0/0
cisco-core(config-if)#ipv6 address 2001:1:1:100::1/64
/Задание IPv6 адресатипа Global Unicast интерфейсу
GE0/0
cisco-core(config-if)#no shutdown
cisco-core(config-if)#exit
cisco-core(config)#interface gigabitEthernet 0/1
cisco-core(config-if)#ipv6 address 2001:1:1:200::1/64
cisco-core(config-if)#no shutdown
cisco-core(config-if)#^Z
/Посмотрсостоянияинтерфейсов
cisco-core#sh ipv6 interface brief
/Проверкадоступностимаршрутизаторов
cisco-core#pingipv6 2001:1:1:100::2
    /Пингинтерфейсаeth1 маршрутизатора1
cisco-core#pingipv6 2001:1:1:200::2
    /Пингинтерфейсаeth2 маршрутизатора2
/Созданиестатическогомаршрута
cisco-core(config)#ipv6 routefc00:2::/64
2001:1:1:100::2 /Маршрутвлोकальнуюсеть,
находящуюсязамаршрутизатором 1
cisco-core(config)#ipv6 routefc00:3::/64
2001:1:1:200::2 /Маршрут в локальную сеть, находящуюся
за маршрутизатором 2
/Просмотр таблицы маршрутизации для IPv6
cisco-core#showipv6 route

```

После настройки маршрутизации в ядре сети проверяется взаимная доступность локальных подсетей. Для этого производится запуск проверки утилитой `ping6` с различных машин, находящихся в разных подсетях.

```

pc1#ping6 fc00:2::2
pc1#ping6 fc00:3::2
pc2#ping6 fc00:1::2
pc2#ping6 fc00:3::2
pc3#ping6 fc00:1::2
pc3#ping6 fc00:2::2

```

Если ping6 проходит успешно, утилитой traceroute6 отслеживается путь продвижения пакетов по сети (рисунок 4.8).

```
bash-3.2$ ping6 -c2 fc00:1::2
PING6(56=40+8+8 bytes) fc00:2::2 --> fc00:1::2
16 bytes from fc00:1::2, icmp_seq=0 hlim=62 time=0.632 ms
16 bytes from fc00:1::2, icmp_seq=1 hlim=62 time=0.687 ms

--- fc00:1::2 ping6 statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.632/0.659/0.687/0.028 ms
bash-3.2$ traceroute6 fc00:1::2
traceroute6 to fc00:1::2 (fc00:1::2) from fc00:2::2, 64 hops max, 12 byte packets
 1 fc00:2::1  0.833 ms  0.206 ms  0.159 ms
 2 2001:1:1:100::1  0.582 ms  0.534 ms  0.552 ms
 3 fc00:1::2  0.629 ms  0.533 ms  0.564 ms
bash-3.2$
```

Рисунок 4.8 – Путь прохождения пакета

В случае использования протокола IPv6 снимается таблица не ARP, а ND-протокола (NeighbourDiscovery). Это связано с особенностями протокола IPv6.

На Cisco данная таблица выводится командой show ipv6 neighbors(рисунок 4.9).

```
cisco-core#show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
FC00:1::2                                  12 000c.42eb.030d STALE V12
2001:1:1:200::2                             144 001b.21cc.10d9 STALE Gi0/1
2001:1:1:100::2                             12 001b.21cc.10fb STALE Gi0/0
FE80::21B:21FF:FECC:10FB                    12 001b.21cc.10fb STALE Gi0/0
FE80::21B:21FF:FECC:10D9                    144 001b.21cc.10d9 STALE Gi0/1
FE80::20C:42FF:FEEB:30D                     12 000c.42eb.030d STALE V12

cisco-core#
```

Рисунок 4.9 – Кэш протокола ND в Cisco

На программном маршрутизаторе просмотр общей таблицы осуществляется той же командой, что и в первой части работы (рисунок 4.10).

```
[admin@localhost ~]$ ip neighbour
2001:1:1:100::1 dev eth1 lladdr 64:00:f1:19:6a:60 router STALE
2001:1:1:300::2 dev eth2 lladdr 00:1b:21:cc:0f:4e router STALE
192.168.24.99 dev eth0 lladdr 00:22:41:26:34:cc REACHABLE
[admin@localhost ~]$
```

Рисунок 4.10 – Кэш протоколов канального уровня в Linux

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Какие особенности адресации в сетях IPv4 и IPv6?
- 2) Какие функции коммутаторов и маршрутизаторов?
- 3) Как произвести конфигурирование маршрутизаторов для организации статической маршрутизации в сетях IPv4/IPv6?

Алгоритм проведения эксперимента:

Часть 1

- 1) Соберите тестовую схему сети согласно рисунку 4.2.
- 2) Подготовьте программные маршрутизаторы, войдите под суперпользователем и установите соединение по SSH.
- 3) Сконфигурируйте программные маршрутизаторы согласно заданию (таблица 4.1).
- 4) Сконфигурируйте маршрутизатор Cisco. Проверьте взаимную доступность подсетей.
- 5) Снимите ARP-таблицы маршрутизаторов.

Часть 2

- 1) Соберите тестовую схему сети согласно рисунку 4.6.
- 2) Выполните действия согласно п. 2-4 части 1, но только для IPv6.
- 3) Снимите таблицу канального уровня ND-протокола.

Варианты заданий

Таблица 4.1 – Статическая маршрутизация в сетях IPv4

№ вар.	Cisco-core			Soft-core1			Soft-core2		
	FE 0/0/0	GE 0/0	GE 0/1	eth0	eth1	eth2	eth0	eth1	eth2
1	192.168.5.0/24	50.0.0.1/30	60.0.0.2/30	172.16.0.0/16	50.0.0.2/30	70.0.0.1/30	10.0.0.0/8	70.0.0.2/30	60.0.0.1/30
2	172.16.0.0/16	42.1.15.5/25	42.1.16.10/25	10.0.0.0/8	42.1.15.15/25	42.1.17.1/29	192.168.4.0/24	42.1.17.3/29	24.1.16.20/25
3	192.168.75.0/24	24.1.1.2/30	25.2.2.4/28	10.0.0.0/8	24.1.1.1/30	26.3.3.3/29	172.16.0.0/16	26.3.3.2/29	25.2.2.1/28
4	192.168.50.0/24	65.1.0.1/30	65.2.0.7/28	192.168.70.0/24	65.1.0.2/30	65.3.0.4/29	10.0.0.0/8	65.3.0.3/29	65.2.0.8/28

Таблица 4.2 – Статическая маршрутизация в сетях IPv6

№ вар.	Cisco-core			Soft-core1			Soft-core2		
	FE 0/0/0	GE 0/0	GE 0/1	eth0	eth1	eth2	eth0	eth1	eth2
1	fc00:ab:30::/64	2001:a::11aa/64	2001:b::12aa/64	fc00:ab:10::/64	2001:a::11bb/64	2001:c::13aa/64	fc00:ab:20::/64	2001:c::13bb/64	2001:b::12bb/64
2	fc00:1:3:1::/64	2001:1:aa::1/64	2001:22:aa::45/64	fc00:1:2:1::/64	2001:11:aa::2/64	2001:33:aa::950/64	fc00:1:1:1::/64	2001:33:aa::750/64	2001:22:aa::de/64
3	fc00:b::/64	2001:a3::120/64	2001:b4::110/64	fc00:a::/64	2001:a3::220/64	2001:d5::200/64	fc00:c::/64	2001:d5::100/64	2001:b4::210/64
4	fc00:74:52:300::/64	2001:1:2:a::64bf/64	2001:1:2:b::123/64	fc00:74:52:200::/64	2001:1:2:a::12cd/64	2001:1:2:c::f5/64	fc00:74:52:100::/64	2001:1:2:c::f4/64	2001:1:2:b::246/64

Алгоритм обработки полученных экспериментальных данных:

Представить листинги производимых действий по настройке оборудования, результаты проверки работоспособности сконфигурированных сетей (таблицы маршрутизации, результаты проверки доступности узлов и подсетей).

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №5 «НАСТРОЙКА ЛОКАЛЬНОГО СЕРВЕРА ДОМЕННЫХ ИМЕН (DNS)»

Цель занятия: изучение методов организации работы с символьными адресами.

Задачи занятия:

- 1) Настроить сервер с плоской адресацией;
- 2) Настройка системы доменных имен;
- 2) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей, стеке протоколов сетевого оборудования, составе типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
- формирование умений о выборе режимов работы программно-аппаратных средств защиты информации в компьютерных сетях;
- формирование навыков настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации.

Материально-техническое оборудование и материалы:

- 1) Персональные компьютеры с операционной системой Windows или Linux (2-4 шт.);
- 2) Маршрутизатор (1 шт.);
- 3) Коммутатор 2 уровня (1 шт).

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

1) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

2) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

3) Ли К., Альбитц П. DNS и BIND, 5-е издание. - Пер. с англ. - СПб.: Символ-Плюс, 2008.

4) Рекомендации RFC-1101, RFC-1032, RFC-1033, RFC-1034, RFC-1035, RFC-1183, RFC-1535, RFC-1536, RFC-1712, RFC-1713, RFC-1886, RFC-2052.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Существует два вида методов организации пространства символьных имен в IP-сетях. Первый, называемый «плоской адресацией», позволяет присваивать имена хостам в небольших локальных сетях, используя широковещательную рассылку. Данный метод подходит только для небольших локальных сетей, так как требует настройки вручную всех хостов сети и в настоящее время используется редко.

В крупных сетях используется второй способ: применение централизованной службы, поддерживающей соответствие между различными типами адресов всех компьютеров сети. Такой службой является DNS (Domain Name System – система доменных имен), основанная на распределенной базе соответствий доменных имен IP-адресам.

Служба DNS использует в своей работе принцип «клиент-сервер». DNS-серверы поддерживают распределенную базу соответствий, а DNS-клиенты обращаются к серверам с запросами о разрешении доменных имен в IP-адреса. В качестве базы соответствий используются текстовые файлы вида «доменное имя –

IP-адрес», подготавливаемые администратором, и использует в основе иерархию доменов. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и субдоменов имен и добавлением в службу DNS новых серверов.

На рисунке 5.1 представлена логическая структура службы DNS. Все домены верхнего (первого) уровня разделяются на три типа: территориальная принадлежность или домены государств (двухбуквенные), принадлежность к сообществам – профессиональным и т.п. (трехбуквенные), информационные домены (четырёхбуквенные). Среди информационных доменов отдельно отмечается домен .arpa, зарезервированный за службой DNS.

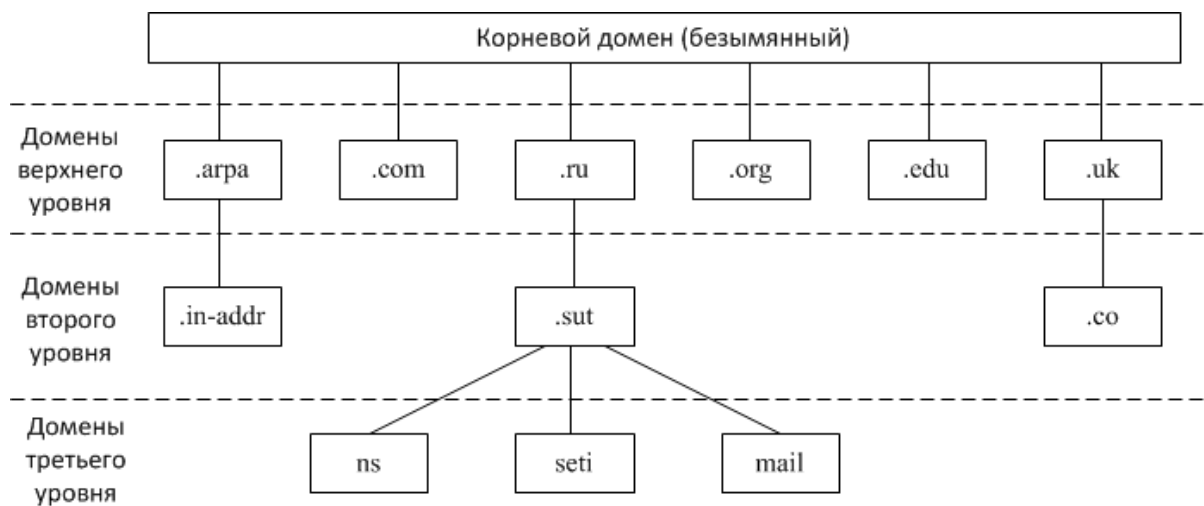


Рисунок 5.1 – Логическая структура доменных имен с примерами

Для каждого домена имен создается свой DNS-сервер. Имеется два вида распределения имен на серверах. В первом случае сервер может хранить отображения для всего домена, включая его субдомены. Однако такое решение оказывается плохо масштабируемым, так как при добавлении новых субдоменов нагрузка на этот сервер может превысить его возможности. Чаще используется другой подход, когда сервер доменов хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети.

Каждый DNS-сервер помимо таблицы соответствий имен содержит ссылки на DNS-серверы своих субдоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными.

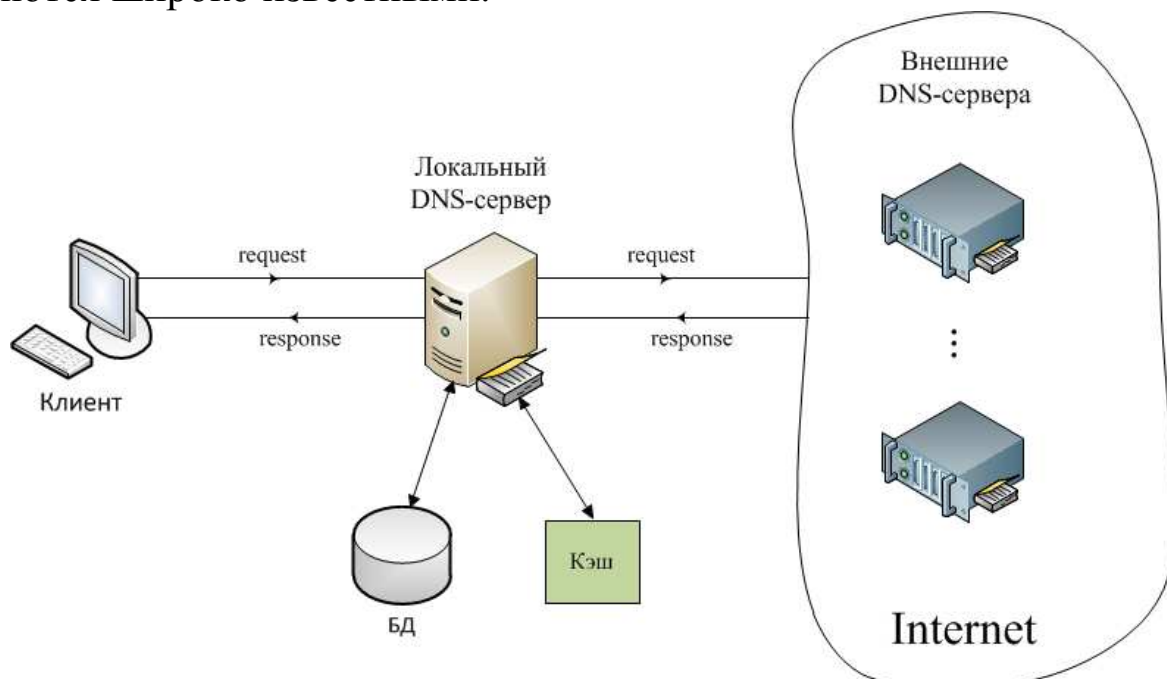


Рисунок 5.2 – Схема взаимодействия с серверами имен

Для определения IP-адреса по доменному имени необходимо просмотреть все DNS-серверы, обслуживающие цепочку субдоменов, входящих в имя хоста, начиная с корневого домена. При этом предварительно проверяются кэш и текущий каталог.

Рассмотрим основные схемы разрешения DNS-имен. В первом варианте работу по поиску IP-адреса координирует DNS-клиент.

1) DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени.

2) DNS-сервер отвечает клиенту, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в следующей старшей части запрошенного имени.

3) DNS-клиент делает запрос следующего DNS-сервера, который отправляет его к DNS-серверу нужного субдомена и т.д., пока не будет найден DNS-сервер, в котором хранится соответствие

запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Такая процедура разрешения имени называется нерекурсивной, когда клиент сам итеративно выполняет последовательность запросов к разным серверам имен. Эта схема загружает клиента достаточно сложными задачами и применяется редко.

Во втором варианте реализуется рекурсивная процедура.

1) DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, обслуживающий субдомен, которому принадлежит имя клиента.

2) Далее возможны два варианта действий:

а) Если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту (это может произойти, когда запрошенное имя входит в тот же субдомен, что и имя клиента, или когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше);

б) Если локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т.д. точно так же, как это делал клиент в предыдущем варианте, а получив ответ, передает его клиенту, который все это время просто ждет его от своего локального DNS-сервера.

В этой схеме клиент перепоручает работу своему серверу, поэтому схема называется косвенной, или рекурсивной. Для ускорения поиска IP-адресов DNS-серверы широко применяют кэширование проходящих через них ответов. Чтобы служба DNS могла оперативно отрабатывать изменения, происходящие в сети, ответы кэшируются на относительно короткое время - обычно от нескольких часов до нескольких дней.

Служба DNS предназначена не только для нахождения IP-адреса по имени хоста, но и для решения обратной задачи - нахождению DNS-имени по известному IP-адресу. Обратная запись не всегда существует даже для тех адресов, для которых есть прямые записи. Данная задача решается путем организации так называемых обратных зон. Обратная зона - это система таблиц, которая хранит соответствие между IP-адресами и DNS-именами хостов некоторой сети. Для организации распределенной службы и использования для поиска имен того же программного обеспечения, что и для поиска адресов, применяется оригинальный подход, связанный с представлением IP-адреса в виде DNS-имени.

Например, для адреса 192.31.106.0 имя обратной зоны будет выглядеть так:

106.31.192.in-addr.arpa

Для записей в серверах, поддерживающих старшие в иерархии обратные зоны, создана специальная зона in-addr.arpa.

Серверы для обратных зон используют файлы баз данных, не зависящие от файлов основных зон, в которых имеются записи о прямом соответствии тех же имен и адресов.

Рекомендации по выполнению лабораторной работы для самостоятельного изучения:

Часть 1. Плоская адресация

Во времена зарождения компьютерных сетей всю информацию об узлах, необходимую для преобразования имен в адреса, хранил один единственный файл hosts, копия которого располагалась на каждом отдельном узле сети. Этот файл присутствует и в современных операционных системах.

При использовании плоской адресации пространство символьных имен никак не структурировано. Такой подход может быть оправдан при администрировании небольшой изолированной локальной сети, внутри которой требуется символьная адресация хостов, а изменения в сети происходят крайне редко.

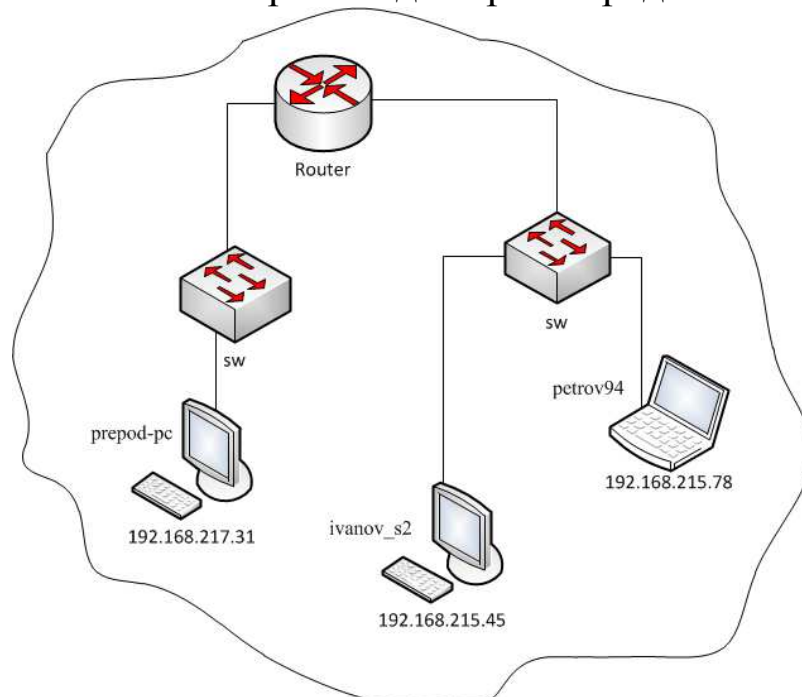


Рисунок 5.3 – Распределение плоских символьных имен

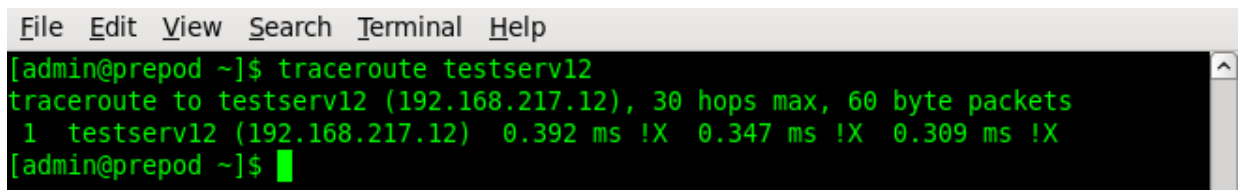
Для реализации данного подхода в Unix-подобных операционных системах существует специальная таблица разрешения имен, хранящаяся в файле /etc/hosts (в Windows этот файл расположен по адресу %SystemRoot%\system32\drivers\etc\hosts). Таблица имеет следующий вид:

```
#IP-адрес          Имя хоста
127.0.0.1         localhost
192.168.215.45    ivanov_s2
192.168.215.78    petrov94
192.168.217.31    prepod-pc
ит. п....
```

Данная таблица имеет значение только для компьютера, на котором она размещена. Таким образом, для поддержания рабочей адресации в подобной сети, необходимо следить за своевременностью обновления таблиц hosts на всех хостах.

Файл hosts является текстовым и создается вручную.

Для проверки работоспособности получившейся адресной таблицы необходимо воспользоваться утилитой traceroute, в качестве аргумента указывая ей символьные адреса хостов (рисунок5.4).



```
File Edit View Search Terminal Help
[admin@prepod ~]$ traceroute testserv12
traceroute to testserv12 (192.168.217.12), 30 hops max, 60 byte packets
 1 testserv12 (192.168.217.12)  0.392 ms !X  0.347 ms !X  0.309 ms !X
[admin@prepod ~]$
```

Рисунок5.4 – Проверка плоской адресации

Часть 2. Система доменных имен

На данный момент стандартом де-факто для UNIX-систем является DNS-сервер BIND (BerkleyInternetNameDomain). В данной работе используется версия BIND 9.7.3, что определяет специфику формата приведенных конфигурационных файлов.

Настройка сервера доменных имен производится путем редактирования рабочих конфигурационных файлов. Основным файлом настроек является /etc/named.conf – здесь хранится общая конфигурация сервера и указатели на описания зон, за которые

отвечает данный сервер. В каталоге `/var/named/` по умолчанию содержатся файлы, описывающие зоны доменных имен данного сервера. Установленный пакет BIND уже содержит вспомогательные описания типовых зон, таких как корневая зона, `localhost` и т.д. Таким образом, для запуска DNS-сервера достаточно создать и настроить описания для протоколов IPv4 и IPv6 прямых и обратных зон, ответственность за которые несет данный сервер.

Рассмотрим пример настройки DNS-сервера, обслуживающего домен `lab.org`, схематично изображенный на рисунке 5.5.

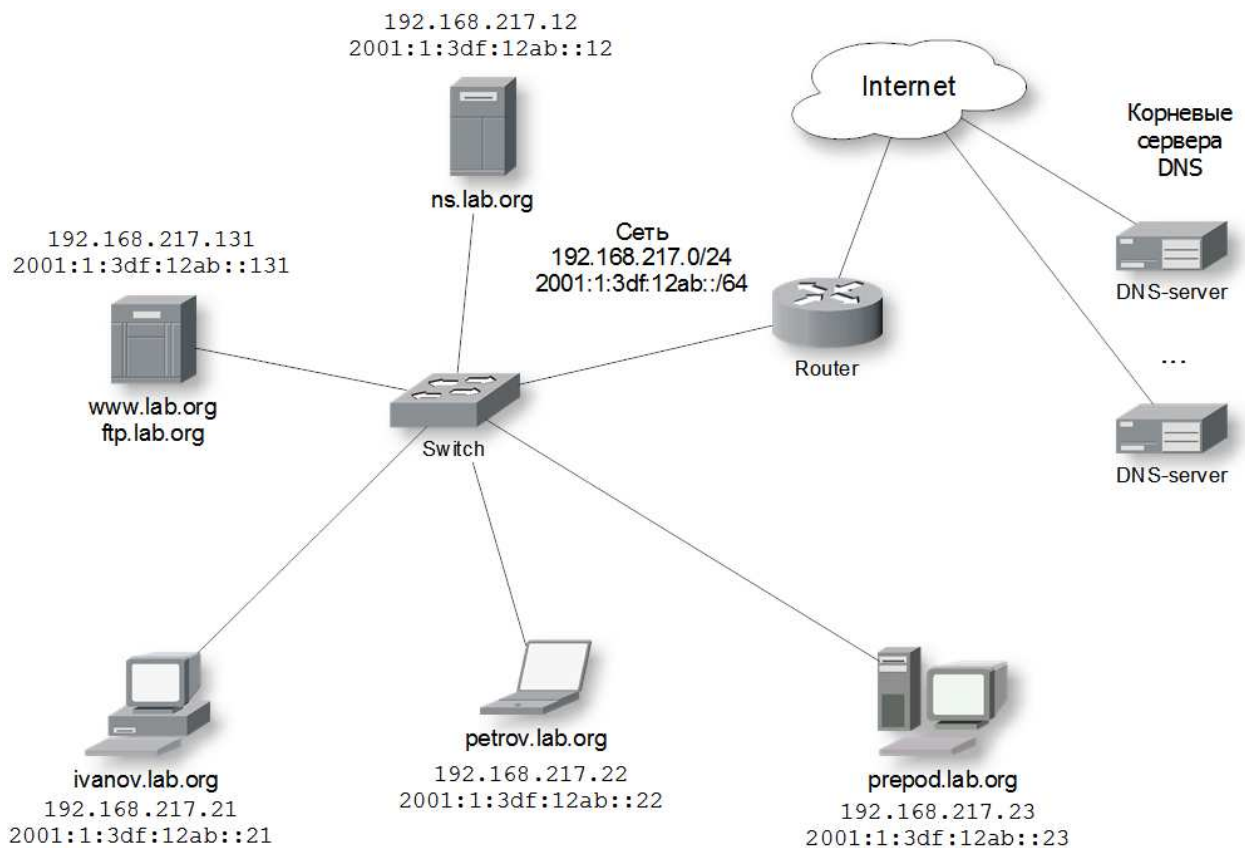


Рисунок 5.5 – Структура домена `lab.org`

Из рисунка, зона `lab.org` располагается в подсети `192.168.217.0/24` (`2001:1:3df:12ab::/64` при адресации посредством IPv6) и содержит шесть доменных имен.

В сети находятся следующие хосты:

- `ns.lab.org` – DNS-сервер сети.
- `ivanov.lab.org` – клиентская машина.
- `petrov.lab.org` – клиентская машина.
- `prepod.lab.org` – клиентская машина.

- www.lab.org, ftp.lab.org – сервер с запущенными на нем службами Web и FTP.

Примеры конфигурационных файлов для рассмотренной сети с необходимыми пояснениями приведены в Приложении А.

В соответствии с вариантом нужно создать конфигурационный файл named.conf и файлы с описаниями прямой и обратной зон на сервере с запущенным BIND, после чего проверить работоспособность полученной конфигурации.

После изменения конфигурационных файлов необходимо перезапустить сервер от имени суперпользователя:

```
servicenamedrestart
```

Для проверки работоспособности конфигурации необходимо воспользоваться специализированной утилитой host(рисунок 5.6, 5.7, 5.8).

```
File Edit View Search Terminal Help
[admin@localhost ~]$ host petrov.lab.org
petrov.lab.org has address 192.168.217.22
petrov.lab.org has IPv6 address 2001:1:3df:12ab::22
[admin@localhost ~]$
```

Рисунок 5.6 – Прямой запрос

```
File Edit View Search Terminal Help
[admin@localhost ~]$ host 192.168.217.131
131.217.168.192.in-addr.arpa domain name pointer www.lab.org.
131.217.168.192.in-addr.arpa domain name pointer ftp.lab.org.
[admin@localhost ~]$
```

Рисунок 5.7 – Обратный запрос IPv4

```
File Edit View Search Terminal Help
[admin@localhost ~]$ host 2001:1:3df:12ab::23
3.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.a.2.1.f.d.3.0.1.0.0.0.1.0.0.2.ip6.arpa
domain name pointer prepod.lab.org.
[admin@localhost ~]$
```

Рисунок 5.8 – Обратный запрос IPv6

Для получения более полной информации необходимо использовать утилиту dig (рисунок 5.9), для обратных запросов она применяется с опцией -x.

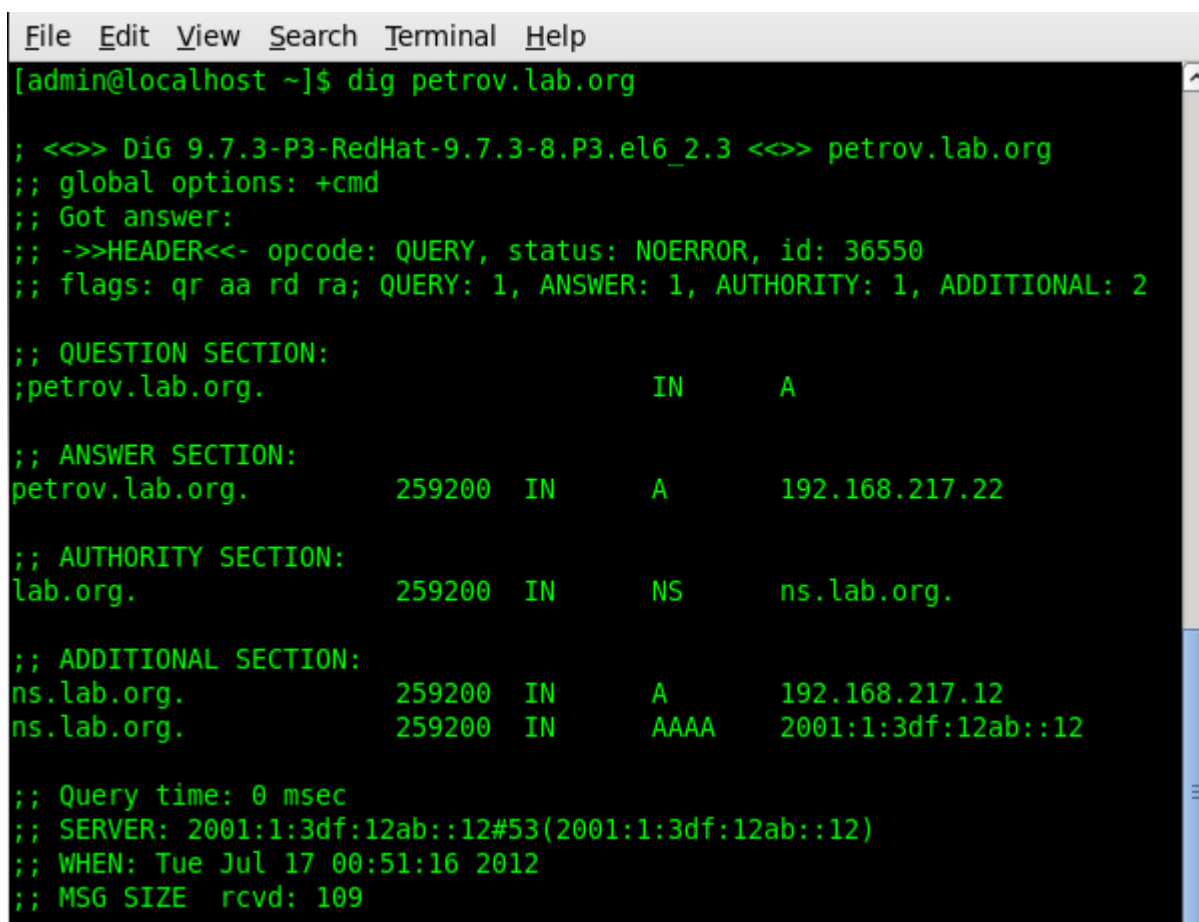
Примечание: При проверке на клиентских машинах необходимость выставить IP-адрес компьютера управления с запущенным на нем BIND в качестве DNS-сервера. Узнать текущий используемый DNS-сервер на клиентской машине можно командой:

```
cat /etc/resolv.conf
```

Аналогичным образом проверяются IPv6-записи.

Для этого необходимо запустить на управляющем компьютере анализатор трафика Wireshark и снять трэйс, в то время как на клиентской машине будет произведен запрос какого-либо доменного имени из глобальной сети, например:

```
host yahoo.com
```



```
File Edit View Search Terminal Help
[admin@localhost ~]$ dig petrov.lab.org

; <<> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.3 <<> petrov.lab.org
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 36550
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;petrov.lab.org.                IN      A

;; ANSWER SECTION:
petrov.lab.org.                259200  IN      A      192.168.217.22

;; AUTHORITY SECTION:
lab.org.                       259200  IN      NS     ns.lab.org.

;; ADDITIONAL SECTION:
ns.lab.org.                    259200  IN      A      192.168.217.12
ns.lab.org.                    259200  IN      AAAA   2001:1:3df:12ab::12

;; Query time: 0 msec
;; SERVER: 2001:1:3df:12ab::12#53(2001:1:3df:12ab::12)
;; WHEN: Tue Jul 17 00:51:16 2012
;; MSG SIZE rcvd: 109
```

Рисунок 5.9 – Утилита dig

После получения ответа завершается съём трафика, включается фильтр протокола dns и инструментом Statistics -

>FlowGraphстроится диаграмма рекурсивного разрешения адреса (рисунок 5.10).

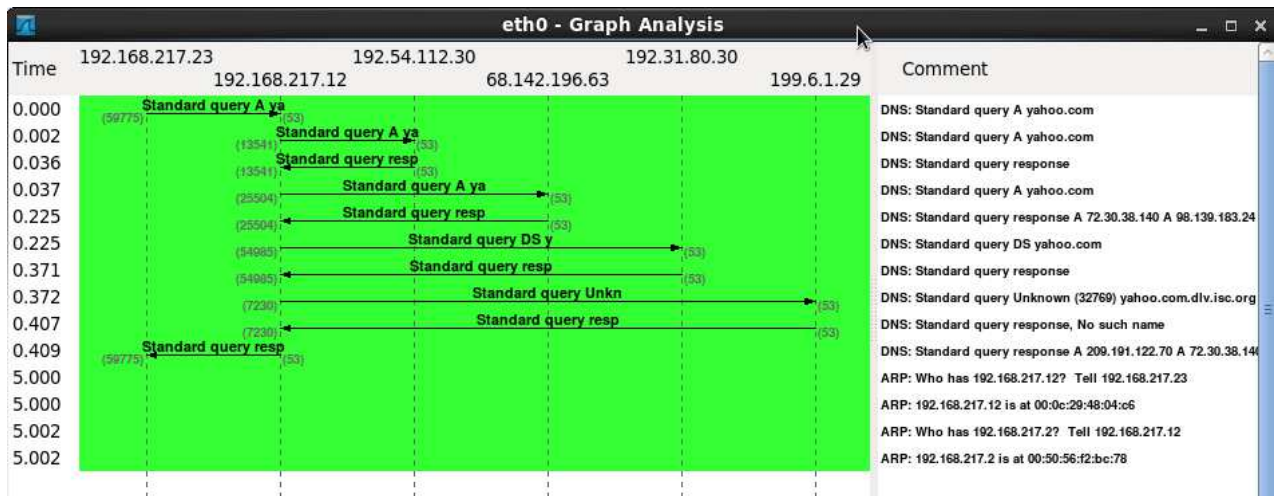


Рисунок 5.10 – Разрешение адреса в глобальной сети

Утилита `dig` прослеживает процесс разрешения адреса в глобальной сети:

```
dig доменное_имя +trace
```

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Какие Вы имеете представления о структуре службы DNS и обработке DNS-запросов?
- 2) Как работают утилиты `host` и `dig`?
- 3) Какой формат пакета DNS-запроса и DNS-ответа, номер DNS-порта?
- 4) Как анализировать пакет DNS-службы, полученный с помощью анализатора трафика?

Алгоритм проведения эксперимента:

1) Согласно варианту создать файл `hosts`, описывающий хосты лабораторной сети.

2) Провести проверку работоспособности получившейся адресной таблицы, в качестве аргумента укажите символьные адреса хостов.

3) Провести настройку сервера доменных имен путем редактирования рабочих конфигурационных файлов: named.conf и с описаниями прямой и обратной зон на сервере с запущенным BIND

4) Проверить работоспособность полученной конфигурации для IPv4 и IPv6.

5) Проверить взаимодействие локального DNS-сервера с общей инфраструктурой DNS, построить диаграмму рекурсивного разрешения адреса.

Варианты заданий:

Таблица 5.1 – Задание к части 1

Вариант	Адресация подсети	Адреса хостов	Символьные имена
1	192.168.215.0/24	192.168.215.45 192.168.215.52 192.168.215.53 192.168.215.54 192.168.215.78 192.168.215.31	ivanov_s2 sidorov1 sidorov2012 sidorov_vasya petrov94 prepod-pc
2	192.168.17.0/24	192.168.17.22 192.168.17.25 192.168.17.29 192.168.17.34 192.168.17.143 192.168.17.144 192.168.17.145 192.168.17.221	Masha_C1 np_C1 zakupki support cat128 vi_galkin am_semionov ad_min
3	172.16.0.0/16	172.16.23.12 172.16.2.58 172.16.8.23 172.16.7.32 172.16.240.3 172.16.1.1 172.16.98.112	host12 ivan2 guest_house32 ftp1 mohamed administrator alla_fin
4	10.0.0.0/8	10.0.1.2 10.2.88.3 10.78.2.2 10.233.1.2 10.55.0.8 10.9.77.6 10.63.5.4	admin gw3-11 maria_f 23-adv loc3serv gw4-56 testbed

Таблица 5.2 – Задание к части 2 согласно схеме рисунка 5.5

Вариант	Имя зоны	Адресация	Хосты			
			IPv4-адрес	IPv6-адрес	Имя	Назначение
1	gazt.org	172.16.0.0/16 2001:33:a::/64	172.16.0.12	2001:33:a::12/64	ns.gazt.org	DNS-сервер сети
			172.16.88.2	2001:33:a::8802/64	techsupp.gazt.org	клиентская машина
			172.16.31.88	2001:33:a::3188/64	mess3.gazt.org	клиентская машина
			172.16.1.1	2001:33:a::101/64	billing.gazt.org	клиентская машина
			172.16.76.45	2001:33:a::7645/64	www.gazt.org, ftp.gazt.org	сервер Web и FTP
2	ss.stu.edu	10.0.0.0/8 2001:6::/64	10.2.3.4	2001:6::2:304/64	ns.ss.stu.edu	DNS-сервер сети
			10.88.75.2	2001:6::88:7502/64	guest.ss.stu.edu	клиентская машина
			10.9.22.1	2001:6::9:2201/64	maria.ss.stu.edu	клиентская машина
			10.60.70.2	2001:6::60:7002/64	testbed.ss.stu.edu	клиентская машина
			10.1.1.1	2001:6::1:101/64	www.ss.stu.edu, ftp.ss.stu.edu	сервер Web и FTP
3	comp.net	192.168.217.0/24 2001:c17::/64	192.168.217.12	2001:c17::12/64	ns.comp.net	DNS-сервер сети
			192.168.217.21	2001:c17::21/64	ivan.comp.net	клиентская машина
			192.168.217.22	2001:c17::22/64	trade.comp.net	клиентская машина
			192.168.217.23	2001:c17::23/64	buh22.comp.net	клиентская машина
			192.168.217.131	2001:c17::131/64	www.comp.net, ftp.comp.net	сервер Web и FTP
4	rus.ztel.com	192.168.11.0/24 2001:d:e2::/64	192.168.11.1	2001:d:e2::1/64	ns.rus.ztel.com	DNS-сервер сети
			192.168.11.24	2001:d:e2::24/64	gw12.rus.ztel.com	клиентская машина
			192.168.11.77	2001:d:e2::77/64	gw33.rus.ztel.com	клиентская машина
			192.168.11.87	2001:d:e2::87/64	support.rus.ztel.com	клиентская машина
			192.168.11.245	2001:d:e2::245/64	www.rus.ztel.com, ftp.rus.ztel.com	сервер Web и FTP

Алгоритм обработки полученных экспериментальных данных:

По части 1: представить полученную конфигурацию файла hosts, результат работы утилиты traceroute;

По части 2: представить конфигурационный файл named.conf, файлы с описаниями прямой и обратной зон на сервере с запущенным BIND, результаты работы утилит host и dig, скриншот FlowGraph.

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №6 «СПИСКИ ДОСТУПА ACL»

Цель занятия: изучение работы со стандартными и расширенными списками доступа.

Задачи занятия:

- 1) Настроить межсетевой экран со стандартным списком доступа;
- 2) Настроить межсетевой экран с расширенным списком доступа;
- 3) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей; стеке протоколов сетевого оборудования; составе типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; программно-аппаратных средствах, методы защиты информации в компьютерных сетях; видах политик управления доступом и информационными потоками в компьютерных сетях; методах измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;
- формирование умений о выборе режимов работы программно-аппаратных средств защиты информации в компьютерных сетях; Настройки правил фильтрации пакетов в компьютерных сетях;
- формирование навыков настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации; управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях, управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой Windows или Linux (1 шт.);
- 2) Межсетевой экран (1 шт.).

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

4) Андрончик, А.Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие; под общ. ред. Синадского Н.И. / А.Н.Андрончик, А.С.Коллеров, А.С.Синадский, М.Ю.Щербаков. – Екатеринбург: Урал. ун-т, 2014. – 180 с.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Списки доступа (access lists) представляют собой общекритерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах.

Списки доступа, производящие отбор по IP-адресам, создаются командами access-list в режиме глобальной конфигурации, каждый список определяется номером – числом в диапазоне 0 ÷ 99.

Каждая такая команда на оборудовании CiscoSystems добавляет новый критерий отбора в список:

```
router(config)# access-
list<номер_списка><{deny|permit}><IP-адрес>
[маска_шаблона].
```

IP-адрес и маска шаблона записываются в десятично-точечной нотации, при этом в маске шаблона устанавливаются биты, значение которых в адресе следует игнорировать, остальные биты сбрасываются. При этом сетевая маска (netmask) и маска шаблона(wildcard) – это разные вещи. Например, чтобы строка списка сработала для всех узлов с адресами 1.16.124.xxx, адрес должен быть 1.16.124.0, а маска – 0.0.0.255, поскольку значения первых 24 бит жестко заданы, а значения последних 8 бит могут быть любыми.

Как видно в этом случае маска шаблона является инверсией соответствующей сетевой маски. Однако маска шаблона в общем случае не связана с сетевой маской и даже может быть разрывной (содержать чередования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Соответствующая комбинация адреса и маски шаблона: 1.2.3.10.0.0.254.

Комбинация «адрес – маска шаблона» вида 0.0.0.0 255.255.255.255(то есть соответствующая всем возможным адресам) может быть записана в виде одного ключевого слова any. Если маска отсутствует, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют, соответственно, положительное (принять, пропустить, отправить, отобразить) или отрицательное (отбросить, отказать, игнорировать) будет принято решение при срабатывании данного критерия отбора. Например, если список используется при фильтрации дейтаграмм по адресу источника, то эти операторы определяют, пропустить или отбросить дейтаграмму, адрес источника которой удовлетворяет комбинации «адрес – маска шаблона». Если же список применяется для идентификации какой-либо категории трафика, то оператор allow отбирает трафик в эту категорию, а deny – нет.

Список доступа представляет собой последовательность из одного и более критериев отбора, имеющих одинаковый номер списка. Последовательность критериев имеет значение:

маршрутизатор просматривает их по порядку; срабатывает первый критерий, в котором обнаружено соответствие образцу; оставшаяся часть списка игнорируется. Любые новые критерии добавляются только в конец списка. Удалить критерий нельзя, можно удалить только весь список. В конце списка неявно подразумевается критерий «отказать в любом случае» (deny any) – он срабатывает, если ни одного соответствия обнаружено не было.

Для аннулирования списка доступа на оборудовании CiscoSystems следует ввести команду:

```
router(config)#no access-list <номер_списка>.
```

Чтобы применить список доступа для фильтрации пакетов, проходящих через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду:

```
router(config-if)#ip                                     access-group
<номер_списка><{in|out}>.
```

Ключевое слово in или out определяет, будет ли список применяться к входящим или исходящим пакетам соответственно.

Входящими считаются пакеты, поступающие к интерфейсу из сети.

Исходящие пакеты движутся в обратном направлении.

Только один список доступа может быть применен на конкретном интерфейсе для фильтрации входящих пакетов, и один – для исходящих. Соответственно, все необходимые критерии фильтрации должны быть сформулированы администратором внутриодного списка.

В стандартных списках доступа отбор пакетов производится по IP-адресу источника пакета.

Кроме стандартных (standard) списков доступа существуют также расширенные (extended), имеющие большее количество параметров и предлагающие более богатые возможности для формирования критериев отбора.

Расширенные списки доступа на оборудовании CiscoSystems создаются также с помощью команды access-list в режиме глобальной конфигурации, но номера этих списков лежат в диапазоне 100–199. Пример синтаксиса команды создания строки расширенного списка для контроля TCP-соединений:

```
router(config)#          access-list<номер_списка><{deny|
permit}>tcp<IP-
адрес_источника><маска_шаблона>[операторпорт[порт]]
<IP-адрес_получателя><маска_шаблона>
[операторпорт[порт]] [established]
```

Маски шаблона для адреса источника и узла назначения определяются так же, как и в стандартных списках.

Оператор при значении порта должен иметь одно из следующих значений: lt (меньше), gt (больше), eq (равно), neq (не равно), range (диапазон включительно). После оператора следует номер порта (или два номера порта в случае оператора range), к которому этот оператор применяется.

Комбинация оператор-порт, следующая сразу же за адресом источника, относится к портам источника. Соответственно, комбинация оператор-порт, которая следует сразу же за адресом получателя, относится к портам узла-получателя. Применение этих комбинаций позволяет отбирать пакеты не только по адресам мест отправки и назначения, но и по номерам TCP- или UDP-портов.

Кроме того, ключевое слово established определяет сегменты TCP, передаваемые в состоянии установленного соединения. Это значит, что строке, в которую включен параметр established, будут соответствовать только сегменты с установленным флагом ACK (или RST).

Пример: «запретить установление соединений с помощью протокола Telnet со всеми узлами сети 22.22.22.0 netmask 255.255.255.0 со стороны всех узлов Интернета, причем в обратном направлении все соединения должны устанавливаться; остальные TCP-соединения разрешены». Фильтр устанавливается для входящих сегментов со стороны Интернета (предположим, к Интернету маршрутизатор подключен через интерфейс FastEthernet 1/0).

```
router(config)#access-list 101 permit tcp any22.22.22.0
0.0.0.255 eq 23 established
router(config)#access-list 101 deny tcp any22.22.22.0
0.0.0.255 eq 23
router(config)#access-list 101 permit ip any any
router(config)#interface FastEthernet 1/0
router(config-if)#ip access-group 101 in.
```

Указание `ip` вместо `tcp` в команде `access-list` означает «все протоколы». Отметим, что в конце каждого списка доступа подразумевается `denyipanyany`, поэтому в предыдущем примере мы указали `permitipanyany` для разрешения произвольных пакетов, не попавших под предшествующие критерии.

Расширенный список с протоколом `ip` позволяет также производить отбор произвольных пакетов по адресу отправителя и по адресу получателя (в стандартных списках отбор производится только по адресу отправителя).

Критерии для отбора UDP-сообщений составляются аналогично TCP, при этом вместо `tcp` следует указать `udp`, а параметр `established`, конечно, не применим.

Контроль за ICMP-сообщениями может осуществляться с помощью критериев отбора типа:

```
router(config)#access-  
list<номер_списка><{deny|permit}>icmp<IP-  
адрес_источника><маска_шаблона><IP-  
адрес_назначения><маска_шаблона>[icmp-тип [icmp-код]].
```

Здесь `icmp-тип` и, если требуется уточнение, `icmp-код` определяют ICMP-сообщение.

Вообще, в расширенных списках можно работать с пакетами любого IP-протокола. Для этого после оператора `deny/permit` надо указать название протокола (`ahp`, `esp`, `igrp`, `gre`, `icmp`, `igmp`, `igrp`, `ipinip`, `ospf`, `tcp`, `udp`) или его номер, которым он кодируется в поле Protocol заголовка пакета. Далее указываются адреса источника и узла назначения с масками и, возможно, дополнительные параметры, специфичные для данного протокола.

В конце команды `access-list` (расширенный) можно указать параметр `log`, тогда все случаи срабатывания данного критерия (то есть обнаружения пакета, соответствующего критерию), будут протоколироваться на консоль или как указано командой `logging`. После того, как протоколируется первый случай срабатывания, дальше сообщения посылаются каждые 5 минут с указанием числа срабатываний за отчетный период.

Просмотр имеющихся списков доступа на оборудовании CiscoSystems (с указыванием числа срабатываний каждого критерия):

```
router#showaccess-lists
```

Более подробную статистику работы списков доступа можно получить, включив режим `ip accounting`. Режим включается в контексте конфигурирования интерфейса. Следующая команда включает режим учета случаев нарушения (то есть, пакетов, которые не были пропущены списком доступа на данном интерфейсе):

```
router(config-if)# ip accounting access-violations
```

Просмотр накопленной статистики (с указанием адресов отправителей и получателей пакетов):

```
router#show ip accounting access-violations
```

При конфигурировании запрещающих фильтров (в конце которых подразумевается `denyall`) администратор должен не забыть оставить «дверь» для сообщений протоколов маршрутизации, если они используются на конфигурируемом интерфейсе.

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Что представляют собой списки доступа (`accesslists`)?
- 2) Какие существуют списки доступа и чем они отличаются друг от друга?
- 3) Какие действие будет производить команда `log` в конце `access lists` (расширенный)?

Алгоритм проведения эксперимента:

- 1) Создать стандартный список доступа, разрешающий прохождения сетевых пакетов только для сетей `192.168.20.1/24` и `10.0.0.1/24`.
- 2) Применить созданный стандартный список доступа на вход одного из интерфейсов межсетевого экрана.
- 3) С помощью команды `ping` проверить доступность компьютеров из сетей `192.168.20.1/24` и `10.0.0.1/24`.
- 4) Аннулировать созданный стандартный список доступа.
- 5) Создать расширенный список доступа, запрещающий установление соединений с помощью протокола

HTTP со всеми узлами сети 192.168.20.0 netmask 255.255.255.0 со стороны всех узлов сети «Интернет», но разрешающий установление всех соединений в обратном направлении.

6) Применить созданный расширенный список доступа на вход одного из интерфейсов межсетевого экрана.

7) Проверить работоспособность созданного расширенного списка, подключив к межсетевому экрану две сети с Web-серверами и осуществив к ним поочередно запросы.

8) Просмотреть число срабатываний каждого критерия из созданного списка доступа.

9) Включить учет случаев нарушения списка доступа.

10) Выполнить несколько запросов к Web-серверам.

11) Просмотреть результаты работы команды ping.

12) Вывести на консоль накопленную статистику по учету случаев нарушений.

13) Аннулировать созданный расширенный список доступа.

Алгоритм обработки полученных экспериментальных данных:

Каждую итерацию задания подтвердить скриншотом (-ами).

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №7 «ДЕМИЛИТАРИЗОВАННЫЕ ЗОНЫ DMZ»

Цель занятия: изучение способом построения демилитаризованных зон (DMZ).

Задачи занятия:

- 1) Настроить демилитаризованную зону на одном межсетевом экране;
- 2) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей; стеке протоколов сетевого оборудования; составе типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; программно-аппаратных средствах, методы защиты информации в компьютерных сетях; видах политик управления доступом и информационными потоками в компьютерных сетях; методах измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;
- формирование умений о выборе режимов работы программно-аппаратных средств защиты информации в компьютерных сетях; Настройки правил фильтрации пакетов в компьютерных сетях;
- формирование навыков настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации; управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях, управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой Windows или Linux (1 шт.);

2) Межсетевой экран (1 шт.).

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

5) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

6) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

7) Андрончик, А.Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие; под общ. ред. Синадского Н.И. / А.Н.Андрончик, А.С.Коллеров, А.С.Синадский, М.Ю.Щербаков. – Екатеринбург: Урал. ун-т, 2014. – 180 с.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Начиная с версии IOS 12.4, в маршрутизаторах появилась функция Zone-Based Policy Firewall, позволяющая производить настройку правил меж сетевого экрана. Эта функция позволяет назначить интерфейсам маршрутизатора зоны безопасности и установить правила взаимодействия между ними.

Конфигурирование Zone-Based Policy Firewall заключается в выполнении следующих шагов:

- назначить зоны меж сетевого экрана;
- определить возможность прохождения сетевого трафика между зонами;

- включить существующие сетевые интерфейсы в созданные зоны;
- определить классы, к которым будут применяться политики для пересечения пары зон;
- определить политики для пар зон, регламентирующие производимые действия над проходящим сетевым трафиком;
- применить политики для выбранных пар зон.

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Зачем необходимо построение демилитаризованных зон (DMZ)?
- 2) В выполнении каких шагов заключается конфигурирование Zone-Based Policy Firewall?
- 3) Какие существуют схемы построения сетей с использованием демилитаризованных зон?

Алгоритм проведения эксперимента:

- 1) Собрать на лабораторном макете топологию сети, представленную на рисунке 7.1.

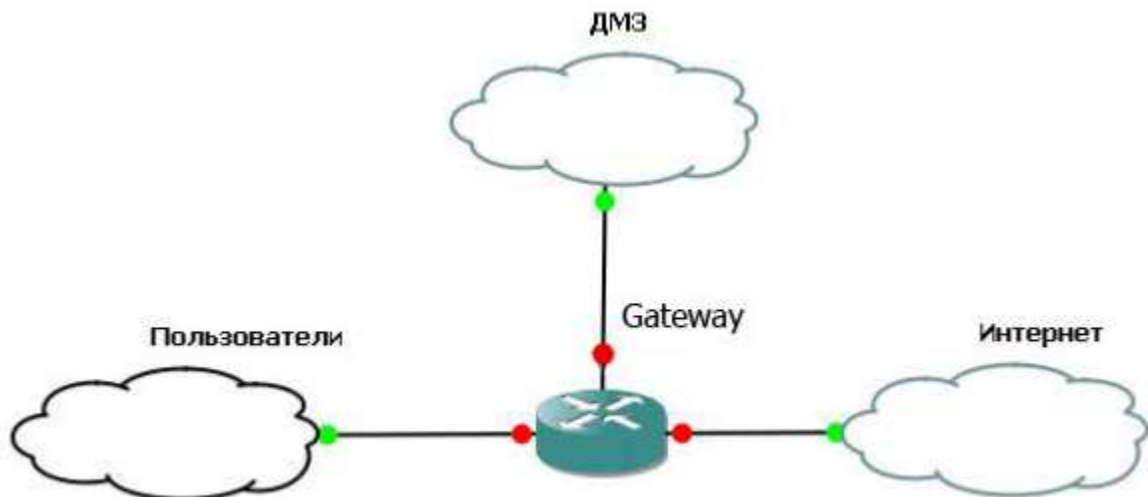


Рисунок 7.1 – Топология сети

- 2) В режиме глобального конфигурирования определить зоны безопасности. Для пользователей задать зону с именем `inside`, для

Интернета – outside, для ДМЗ – DMZ. В случае использования оборудования от Cisco Systems:

```
Gateway(config)#zone security outside
Gateway(config-sec-zone)#description internet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security inside
Gateway(config-sec-zone)#description intranet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security dmz
Gateway(config-sec-zone)#description DMZ
Gateway(config-sec-zone)#exit.
```

3) Назначить интерфейсы в зоны. По умолчанию прохождения трафика между зонами запрещено. В случае использования оборудования от Cisco Systems:

Для зоны outside:

```
Gateway(config)#interface FastEthernet0/0
Gateway(config-if)#ip address 10.0.0.2 255.0.0.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security outside
Gateway(config-if)#description outside
Gateway(config-if)#exit.
```

Для зоны inside:

```
Gateway(config)#interface FastEthernet0/1
Gateway(config-if)#ip address 192.168.20.2
255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security inside
Gateway(config-if)#description inside
Gateway(config-if)#exit.
```

Для зоны DMZ:

```
Gateway(config)#interface FastEthernet1/0
Gateway(config-if)#ip address 172.16.0.2 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security dmz
Gateway(config-if)#description DMZ
Gateway(config-if)#exit.
```

4) Определить протоколы, по которым пользователям разрешено выходить в Интернет (http, ftp, smtp, pop3, dns, icmp). В случае использования оборудования от Cisco Systems:

```

Gateway(config)#class-map    type    inspect    match-any
cm_http-ftp-dns-smtp-pop3-icmp
Gateway(config-cmap)#match protocol http
Gateway(config-cmap)#match protocol ftp
Gateway(config-cmap)#match protocol pop3
Gateway(config-cmap)#match protocol smtp
Gateway(config-cmap)#match protocol dns
Gateway(config-cmap)#match protocol icmp
Gateway(config-cmap)#exit.

```

5) Определить политики. В случае использования оборудования от CiscoSystems:

```

Gateway(config)#policy-map type inspect in-out
Gateway(config-pmap)#class type inspect cm_http-ftp-
dns-smtp-pop3-icmp
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#exit.

```

6) Создать цепочку из пары зон inside → outside. В случае использования оборудования от Cisco Systems:

```

Gateway(config)#zone-pair    security    inside-outside
source inside destination outside
Gateway(config-sec-zone-pair)#service-policy    type
inspect in-out
Gateway(config-sec-zone-pair)#exit.

```

7) Создать списки доступа для публичных серверов:

```

Gateway(config)#access-list 101 remark web-server
Gateway(config)#access-list 101 permit ip any host
172.16.0.4
Gateway(config)#access-list 102 remark mail-server
Gateway(config)#access-list 102 permit ip anyhost
172.16.0.5
Gateway(config)#access-list 103 remark ftp-server
Gateway(config)#access-list 103 permit ip anyhost
172.16.0.6.

```

8) Определить протоколы для доступа к серверам из внешней сети. В случае использования оборудования от Cisco Systems:

```

Gateway(config)#class-map type inspect match-allweb

```

```

Gateway(config-cmap)#match access-group 101
Gateway(config-cmap)#match protocol http
Gateway(config-cmap)#exit
Gateway(config)#class-map type inspect match-allmail
Gateway(config-cmap)#match access-group 102
Gateway(config-cmap)#match protocol smtp
Gateway(config-cmap)#match protocol pop3
Gateway(config-cmap)#exit
Gateway(config)#class-map type inspect match-allftp
Gateway(config-cmap)#match access-group 103
Gateway(config-cmap)#match protocol ftp
Gateway(config-cmap)#exit.

```

9)Задать политики для ДМЗ:

```

Gateway(config)#policy-map type inspect web-mail-ftp-
dmz
Gateway(config-pmap)#class type inspect web
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect mail
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect ftp
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#exit.

```

10)Создать цепочку из пары зон outside → dmz. В случае использования оборудования от CiscoSystems:

```

Gateway(config)#zone-pair security out-dmzsource
outside destination dmz
Gateway(config-sec-zone-pair)#service-policytype
inspect web-mail-ftp-dmz
Gateway(config-sec-zone-pair)#exit.

```

11) Проверить работоспособность созданной конфигурации.

Алгоритм обработки полученных экспериментальных данных:

Каждую итерацию задания подтвердить скриншотом (-ами).

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №8 «ТРАНСЛЯЦИЯ И ТУННЕЛИРОВАНИЕ СЕТЕВЫХ АДРЕСОВ»

Цель занятия: получение навыков настройки механизмов NAT.

Задачи занятия:

- 1) Выполнить настройку «классического» NAT в IPv4 сетях.
- 2) Выполнить туннелирование подсетей с адресацией IPv6 через сеть с адресацией IPv4;
- 3) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей, стеках протоколов сетевого оборудования, принципах работы и правил эксплуатации эксплуатируемых программно-аппаратных средств защиты информации;
- формирование умений о выборе используемых программно-аппаратных средств защиты информации в компьютерных сетях и их режимах работы, оценке оптимальности выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
- формирование навыков синтеза шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях, настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации, управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях.

Материально-техническое оборудование и материалы:

- 1) Персональные компьютеры с операционной системой Windows или Linux (3 шт.);
- 2) Программные маршрутизаторы (2 шт.);
- 3) Коммутаторы 2 уровня (2 шт.);
- 4) Коммутатор 2 уровня с функциями 2 уровня (1 шт.)

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

4) Официальная документация Netfilter: <http://netfilter.org/documentation/>

5) RFC 2893. Transition Mechanisms for IPv6 Hosts and Routers. August 2000.

6) RFC 3056. Connection of IPv6 Domains via IPv4 Clouds. February 2001.

7) IP Command Reference: <http://linux-ip.net/gl/ip-cref/>

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

Трансляция сетевых адресов является универсальным способом расширения адресного пространства. Появление системы трансляции сетевых адресов, или NAT (NetworkAddressTranslation) обусловлено бурным ростом небольших сетей, в то время относящихся к классу С, и, как следствие, сокращение IP-адресов данного класса. Тогда одним из способов расширения адресного пространства наравне с введением бесклассовой адресации стало использование не уникальных IP-адресов, иногда называемых маскардными. Традиционно это адреса вида 192.168.0.0 и 10.0.0.0, но в последнее время могут использоваться некоторые другие.

Такие адреса уникальны только в пределах закрытой сети (например, корпоративной или сети провайдера). Для выхода в общедоступную сеть необходим уникальный адрес, который присвоен шлюзу. Система NAT позволяет осуществлять подмену адресов на шлюзе.

Рассмотрим такие виды трансляции сетевых адресов, как SourceNAT (SNAT) и DestinationNAT (DNAT). Как следует из названий, данные виды NAT подменяют адреса отправителя и получателя пакета соответственно. Маскарадингом (Masquerade) называется разновидность SNAT, в которой подменяемый адрес отправителя может изменяться динамически в соответствии с текущим адресом шлюзового интерфейса.

В операционной системе Linux за трансляцию сетевых адресов отвечает утилита iptables (или ip6tables для IPv6). Вообще, iptables является одним из командных интерфейсов межсетевого экрана Netfilter и используется для настройки разнообразных правил фильтрации сетевого трафика.

Рассмотрим некоторые ключевые понятия iptables:

- Правило – состоит из критерия, действия и счетчика. Если пакет соответствует критерию, к нему применяется действие, и он учитывается счетчиком. Критерия может и не быть – тогда неявно предполагается критерий «все пакеты».

- Критерий – логическое выражение, анализирующее свойства пакета и/или соединения и определяющее, подпадает ли данный конкретный пакет под действие текущего правила.

- Действие – описание действия, которое нужно проделать с пакетом и/или соединением в том случае, если они подпадают под действие этого правила.

- Цепочка – упорядоченная последовательность правил. Цепочки можно разделить на пользовательские и базовые.

- Базовая цепочка – цепочка, создаваемая по умолчанию при инициализации таблицы. Каждый пакет, в зависимости от того, предназначен ли он самому хосту, сгенерирован им или является транзитным, должен пройти положенный ему набор базовых цепочек различных таблиц. Имена базовых цепочек всегда записываются в верхнем регистре (PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING).

- Пользовательская цепочка – цепочка, созданная пользователем. Может использоваться только в пределах своей таблицы.

- Таблица – совокупность базовых и пользовательских цепочек, объединенных общим функциональным назначением. Имена таблиц записываются в нижнем регистре, так как в принципе не могут конфликтовать с именами пользовательских цепочек. При вызове команды iptables таблица указывается в формате -t имя_таблицы. При отсутствии явного указания, используется таблица filter.

Все пакеты пропускаются через определенные для них последовательности цепочек. При прохождении пакетом цепочки, к нему последовательно применяются все правила этой цепочки в порядке их следования. Таким образом, во-первых, пакет проверяется на соответствие критерию, а во-вторых, если он соответствует данному критерию, то к нему применяется указанное действие. Под действием может подразумеваться как элементарная операция (например, ACCEPT, REJECT), так и переход в одну из пользовательских цепочек. Действия ACCEPT, REJECT и DROP являются терминальными, т.е. прекращающими обработку пакета в рамках данной базовой цепочки.

В обобщенном виде добавление правила iptables можно представить так:

```
iptables -t<имя_таблицы> -A<цепочка><критерий> -j<действие>
```

Здесь -A обозначает, что данное правило будет дописано в конец заданной цепочки заданной таблицы. Просмотр правил в цепочке происходит последовательно сверху вниз.

Таблица NAT содержит три базовые цепочки: PREROUTING, OUTPUT и POSTROUTING. В цепочку PREROUTING попадают все входящие пакеты, адресованные данному хосту или транзитные, до принятия хостом решения о маршрутизации пакета. Пакеты, отсылаемые данным хостом, будут проходить цепочку OUTPUT, а транзитные пакеты на выходе из узла попадут в цепочку POSTROUTING. Таким образом, можно заметить, что для организации SNAT/Masquerade на транзитном шлюзе нужно применять правила цепочки POSTROUTING, в то время как

цепочка PREROUTING будет использоваться при организации DNAT.

В операциях NAT, производимых с помощью iptables, отслеживание состояний используется автоматически. Достаточно указать критерии, под которые подпадет лишь первый пакет в соединении – и трансляция адресов будет применена ко всем пакетам в этом соединении, а также в связанных с ним соединениях.

С появлением сетей IPv6 возникла необходимость совместной работы сегментов сетей с разной адресацией. Скорее всего, еще довольно долгое время доминирующим протоколом останется IPv4. В таких условиях особую актуальность приобретают методы конвергенции и взаимодействия сетей различных типов. На данный момент разработано множество решений этой проблемы, из наиболее распространенных можно назвать 6to4, 6rd, Teredo, NAT64 и др.

Рассмотрим универсальный способ передачи трафика IPv6 через сети IPv4, основанный на использовании протокола 6to4 (рисунок 8.1).

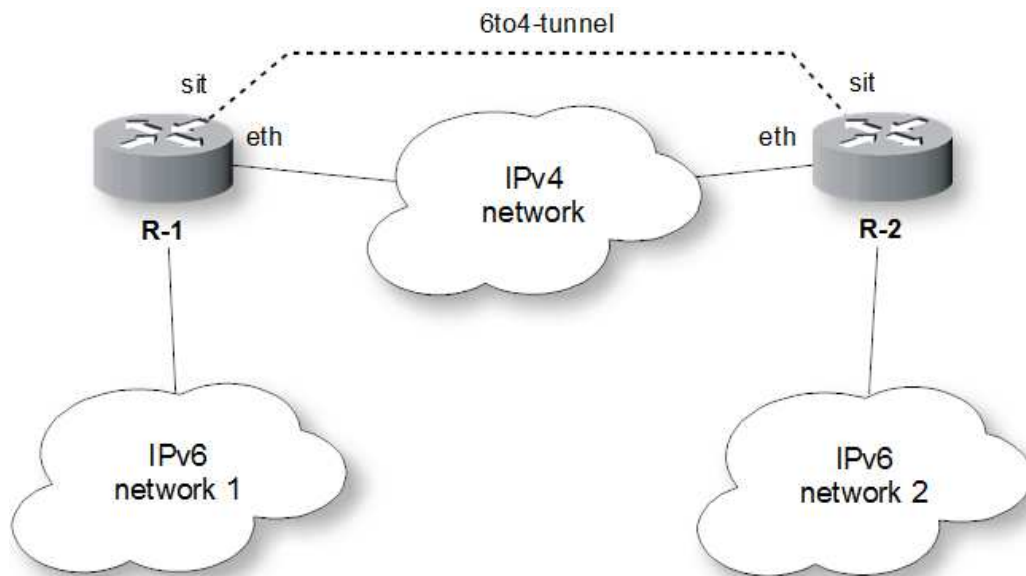


Рисунок 8.1 – Туннель 6to4

Протокол 6to4 предназначен для связи двух подсетей IPv6 через IPv4 и инкапсулирует пакеты версии 6 в тело обыкновенных IPv4-пакетов. Подробное описание работы протокола 6to4 в RFC3056.

Рекомендации по выполнению лабораторной работы для самостоятельного изучения:

Часть 1. «Классический» NAT в сетях IPv4

Рассмотрим организацию трансляции адресов в соответствии с приведенной на рисунке 8.2 схемой.

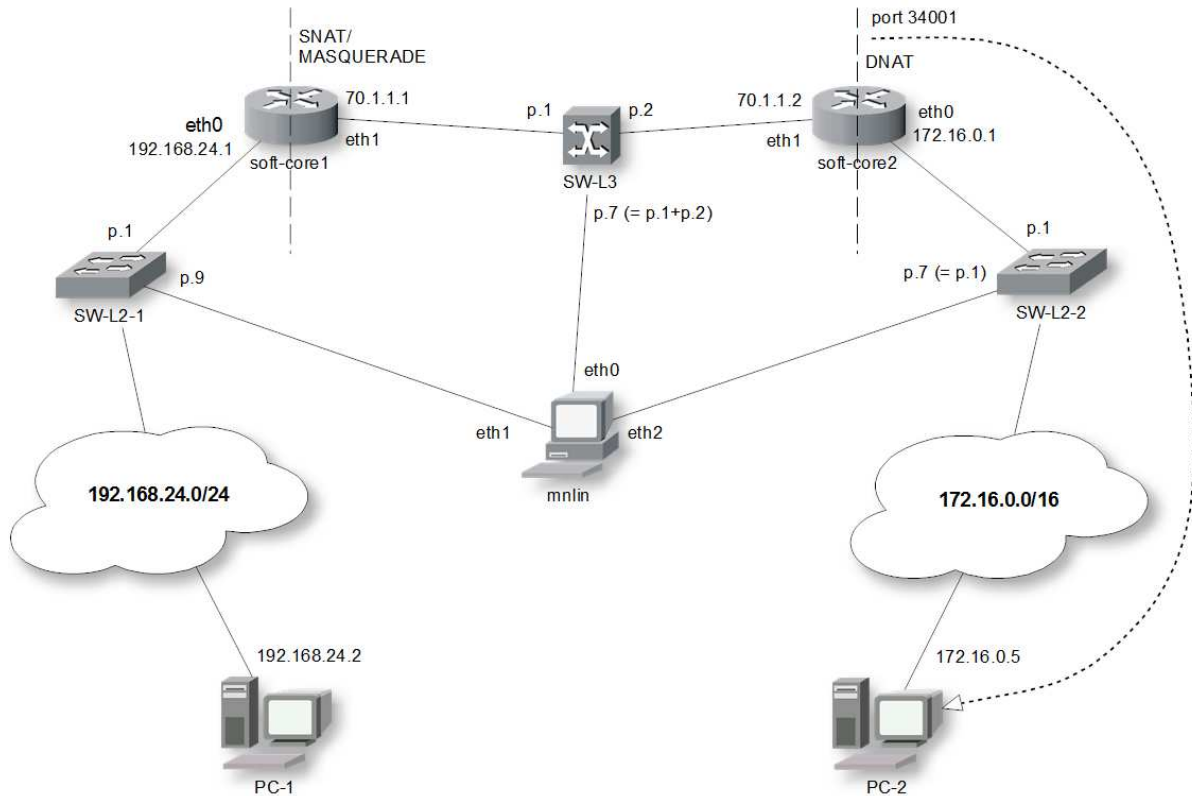


Рисунок 8.2 – Схема сети для организации NAT

Таблица 8.1

Интерфейс	Адрес
mnlm – eth0	не выставляется
mnlm – eth1	192.168.24.33/24
mnlm – eth2	не выставляется
soft-core1 – eth0	192.168.24.1/24
soft-core1 – eth1	70.1.1.1/30
soft-core2 – eth0	172.16.0.1/16
soft-core2 – eth1	70.1.1.2/30
PC-1	192.168.24.2/24
PC-2	172.16.0.5/16

Удобным инструментом, объединяющим различные сетевые программные средства, является созданная нашим соотечественником утилита `ip`. Синтаксис этой утилиты довольно обширен, отметим необходимые команды. Для задания IP-адреса сетевому интерфейсу сначала необходимо удалить старый адрес, а затем присвоить новый.

```
root@sc-1#
ipaddrdel<старый_адрес/префикс>dev<интерфейс>
root@sc-1# ip -4/-6
addradd<новый_адрес/префикс>dev<интерфейс>
```

В данном случае опции `-4` и `-6` обозначают тип адреса: IPv4 или IPv6 соответственно. Например, смена адреса `eth0`:

```
root@sc-1# ipaddrdel 192.168.24.1/24 dev eth0
root@sc-1# ip -4 addr add 10.0.0.1/8 dev eth0
```

Просмотр информации о сетевых интерфейсах осуществляется вводом команды `ifconfig` (все интерфейсы) или `ifconfig<интерфейс>` (для просмотра конкретного интерфейса).

При сборке сети необходимо настроить зеркалирование указанных портов коммутаторов. На схеме запись вида «`p.7 (= p.1)`» обозначает, что на порту 7 настроено зеркалирование всего трафика с порта 1.

Таблица 8.2

Коммутатор	Адрес Web-интерфейса
SW-L2-1	192.168.24.10
SW-L2-2	192.168.24.20
SW-L3	192.168.24.30

Для настройки зеркалирования в коммутаторах от D-Link (SW-L2-1 и SW-L2-2) необходимо зайти в веб-интерфейс нужного коммутатора (login: admin, passw: admin), перейти на вкладку L2 Features → Port Mirror и выставить зеркалирование, как показано на рисунке 8.3.

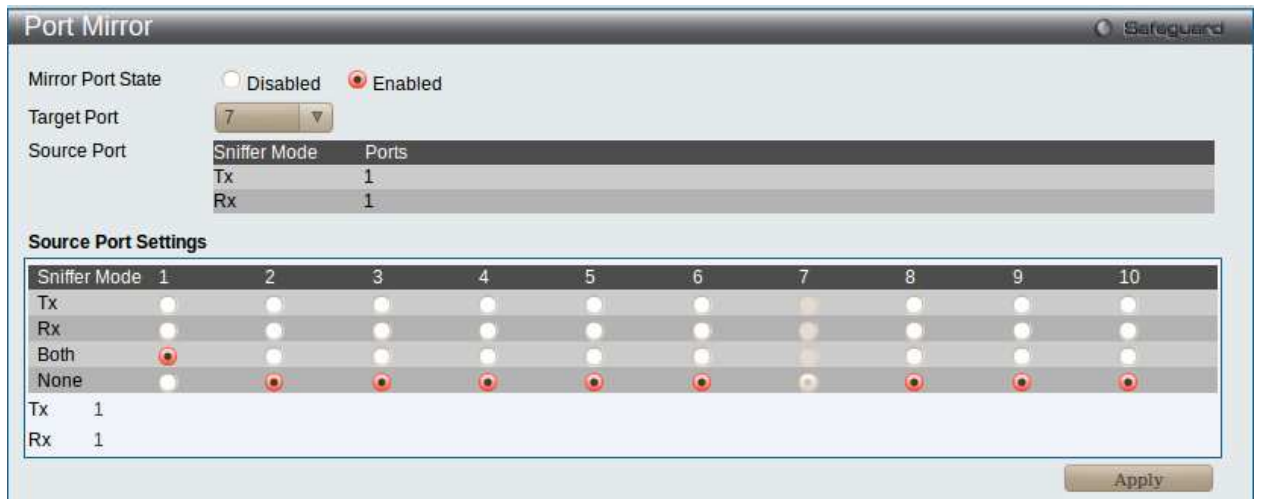


Рисунок 8.3 – Настройка зеркалирования портов на коммутаторах от D-Link (SW-L2-1/ SW-L2-2)

Процедура настройки зеркалирования портов коммутатора от D-Link (SW-L3) напоминает выше описанную, с той лишь разницей, что она производится на вкладке Monitoring → Mirror → PortMirrorSettings (рисунок 8.4).

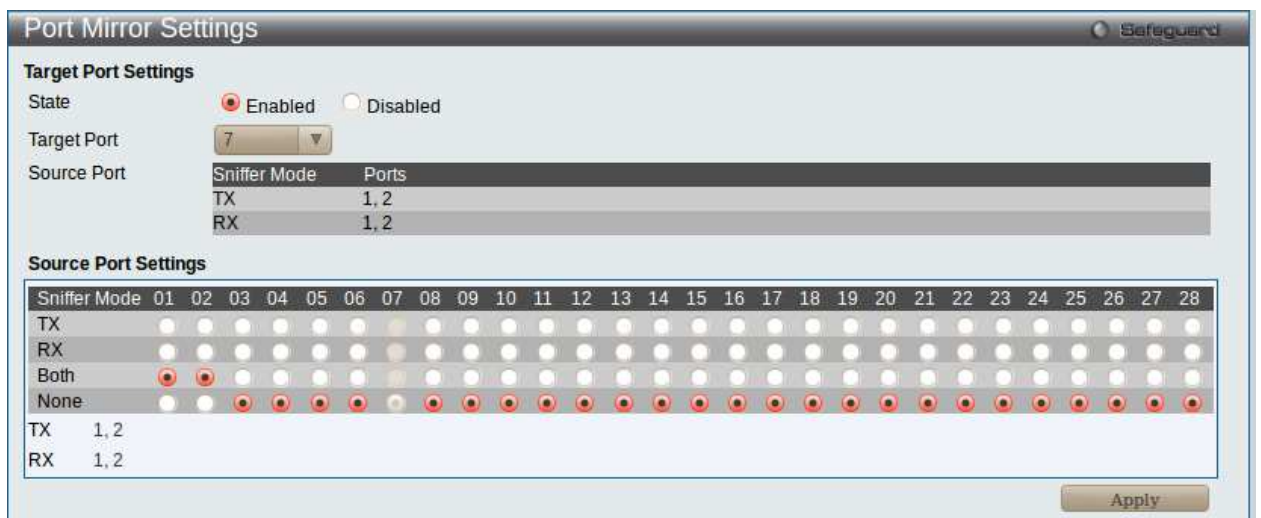


Рисунок 8.4 – Настройка зеркалирования портов в SW-L3

В поле TargetPort указывается тот порт, на который будет осуществляться зеркалирование трафика.

Для настройки маскардинга на soft-core1 согласно приведенной схеме необходимо выполнить подключение к программному маршрутизатору и выполнить следующие действия:

```
student@pc# sshadmin@192.168.24.1 /подключение к SC-1
admin@sc-1# su/получение прав суперпользователя
```

```

root@sc-1# sysctl net.ipv4.ip_forward=1    /включение
IP-forwarding
root@sc-1# iptables -F/очиститаблицыfilter
root@sc-1# iptables -t nat -F/очиститаблицы nat
/правилатрансляции:
root@sc-1# iptables -t nat -A POSTROUTING -o eth1 -j
MASQUERADE    /добавлениеправила,
осуществляющегомаскарадингвсехпакетов,
выходящихизинтерфейса eth1 данногохоста (т.е. SC-1)

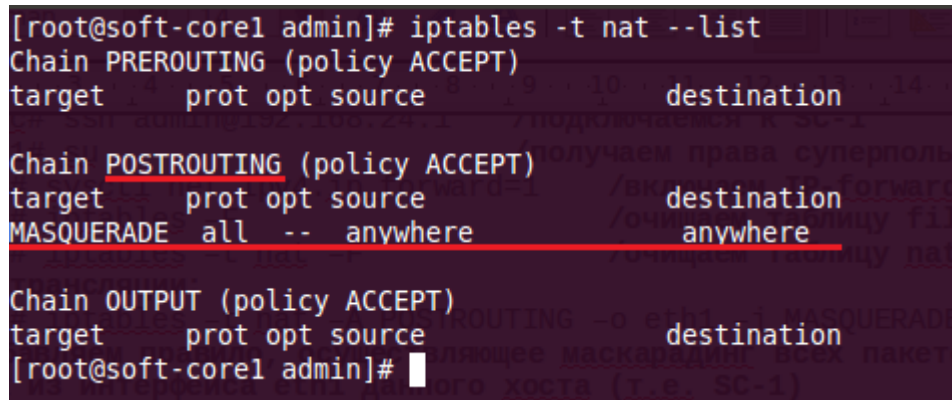
```

Другое правило для настройки SNAT:

```

root@sc-1# iptables -tnat -APOSTROUTING -oeth1 -jSNAT -
-to-source 70.1.1.1    /подменаIP-адреса отправителя всех
пакетов выходящих из интерфейса eth1 на 70.1.1.1
/Просмотр имеющихся в таблице nat правил
root@sc-1# iptables -t nat --list

```



```

[root@soft-core1 admin]# iptables -t nat --list
Chain PREROUTING (policy ACCEPT)
target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target      prot opt source                destination
MASQUERADE all -- anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
[root@soft-core1 admin]#

```

Рисунок 8.5 — Просмотр правил трансляции сетевых адресов

Маскарадинг может адаптироваться к изменяющемуся динамическому внешнему адресу шлюза, а SNAT использует меньше системных ресурсов маршрутизатора, т.к. не проверяет адрес шлюза для каждого исходящего пакета.

Подключитесь к компьютеру управления mnlin и запустите генератор трафика Ostinato. На порту eth0 mnlin произведите запуск Wireshark, а для порта eth1 создайте поток UDP-пакетов с произвольными портами (1024-65535), фиксированным IPv4-адресом отправителя из подсети 192.168.24.0/24 и адресом назначения 70.1.1.2.

Примечание: Для успешной передачи потока в поле Destination Address протокола Media Access Protocol необходимо выставить

реальное значение MAC-адреса интерфейса eth0 маршрутизатора soft-core1 (рисунок 8.6). Узнать MAC-адреса можно командой:

```
root@soft-core1# ifconfig eth0
```

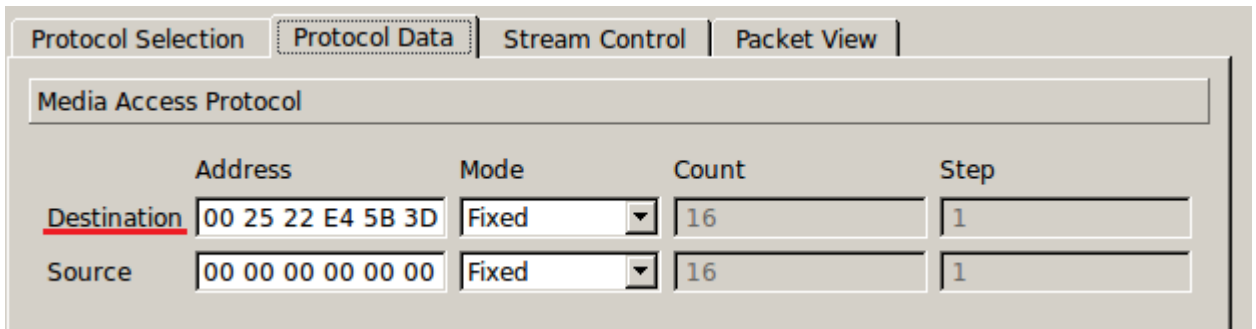


Рисунок 8.6 – Настройка генератора трафика

Отследить в анализаторе трафика поток по адресу назначения можно, запустив генерацию. В поле IP-адреса отправителя у всех пакетов должно быть значение 70.1.1.1, т.е. адрес шлюзового интерфейса.

Настройка DNAT на маршрутизаторе soft-core2 производится следующим образом:

```
student@pc# sshadmin@172.16.0.1 /подключение к SC-2
admin@sc-2# su /получение прав суперпользователя
root@sc-2# sysctl net.ipv4.ip_forward=1 /включение
IP-forwarding
root@sc-2# iptables -F /очищениетаблицы filter
root@sc-2# iptables -t nat -F /очищениетаблицы nat
/правилатрансляции:
root@sc-2# iptables -tnat -APREROUTING -d 70.1.1.2 -
pUDP --dport 34001 -jDNAT --to-destination 172.16.0.5
/подмена у всех пакетов UDP пришедших на порт 34001
адреса назначения на 172.16.0.5 (порт назначения
остаётся прежним - 34001)
root@sc-2# iptables -t nat -A PREROUTING -d 70.1.1.2 -p
TCP --dport 34001 -j DNAT --to-destination
172.16.0.5/тожедля TCP
```

Запустив на компьютере управления прослушивание порта eth2 с помощью Wireshark, а в Ostinato для порта eth1 изменив созданный ранее UDP-поток таким образом, чтобы портом назначения был 34001, можно начать передачу трафика для снятия трэйса с порта eth2. Результатом правильной настройки работы механизма трансляции адресов всей сети должен стать исходный

поток UDP-пакетов с адресом отправителя 70.1.1.1 и адресом назначения 172.16.0.5.

Проверка правильности выполненных настроек производится с помощью netcat. Netcat представляет собой утилиту для чтения и пересылки данных посредством протоколов TCP и UDP. Для установления TCP-соединения на узле 172.16.0.5 необходимо запустить netcat в режиме сервера, прослушивая (listen), например, порт 34001 (или любой другой незанятый порт):

```
root@pc-2# nc -l -p 34001
```

а на узле 192.168.24.2 – в режиме клиента, подключающегося к серверу по адресу 70.1.1.2 на тот же порт 34001:

```
root@pc-1# nc 70.1.1.2 34001
```

В случае успешного установления соединения, станет возможным обмен текстовыми сообщениями между двумя экземплярами netcat, образовав некоторое подобие текстового чата.

Последовательно снимая трафик с портов eth0 и eth2 компьютера управления во время передачи данных с помощью netcat, можно убедиться в том, что трансляция адресов на разных участках сети работает должным образом.

Часть 2. Преобразование Ipv4/IPv6

Рассмотрим создание автономного туннеля (без выхода в глобальную сеть), проходящий через сеть IPv4 и связывающий между собой две подсети IPv6. Во второй части рассматриваться вариант построения сети, приведенный на рисунке 8.7.

В начале необходимо выполнить настройку зеркалирования портов коммутаторов. В случае выполнения первой части работы заново настраивать зеркалирование не требуется.

Для осуществления функционирования сети необходимо подключиться (по SSH) к программным маршрутизаторам и на каждом из них выполнить описанные ниже действия.

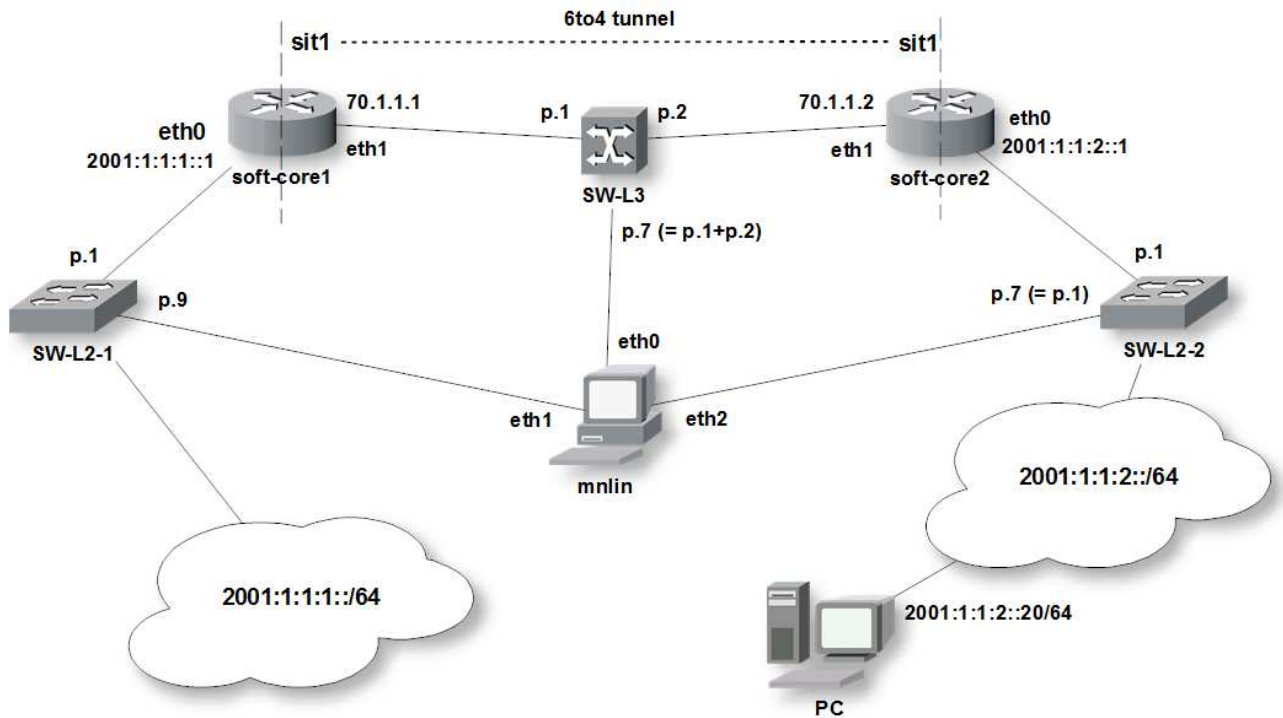


Рисунок 8.7 – Схема сети для настройки 6to4

Таблица 8.3

Интерфейс	Адрес
mnlm – eth0	не выставляется
mnlm – eth1	2001:1:1:1::33/64
mnlm – eth2	не выставляется
soft-core1 – eth0	2001:1:1:1::1/64
soft-core1 – eth1	70.1.1.1/30
soft-core2 – eth0	2001:1:1:2::1/64
soft-core2 – eth1	70.1.1.2/30
PC	2001:1:1:2::20/64

Сначала необходимо удалить существующие правила файрвола и включить транзит трафика IPv6:

```
root@sc-1# sysctl net.ipv6.conf.all.forwarding=1
/включение IPv6 Forwarding
root@sc-1# iptables -F/очиститетаблицы filter
root@sc-1# iptables -t nat -F /очиститетаблицы nat
root@sc-1# ip6tables -F/очиститетаблицы filter для IPv6
```

Очистить таблицы нужно на обоих маршрутизаторах!

Далее необходимо задать IPv6-адреса интерфейсам eth0 маршрутизаторов. В общем виде команда выглядит так:

```
ip -6 addradd<ipv6-адрес>/<префикс>dev<интерфейс>
```

Например, для задания IPv6-адреса интерфейсу eth0 маршрутизатора soft-core1 команда примет следующий вид:

```
root@sc-1# ip -6 addr add 2001:1:1:1::1/64 dev eth0
```

а для soft-core2:

```
root@sc-2# ip -6 addr add 2001:1:1:2::1/64 dev eth0
```

Просмотреть текущие настройки сетевых интерфейсов можно запустив от суперпользователя команду `ifconfig` (все интерфейсы) или `ifconfig <имя_интерфейса>` (выбранный интерфейс, например eth0).

Для настройки туннеля `6to4` необходимо настроить виртуальный туннельный адаптер, включить его и прописать статический маршрут в сеть на противоположном конце туннеля. В обобщенном виде создание туннельного адаптера будет выглядеть так:

```
Iptunnel add <имя_адаптера> mode sit ttl
<время_жизни_пакета> remote
<ipv4_адрес_удаленного_конца_туннеля> local
<локальный_адрес_ipv4>
```

Имена адаптеров принято давать по типу адаптера (здесь sit) + порядковый номер, начиная с единицы.

Весь процесс настройки на стороне soft-core1:

```
root@sc-1# ip tunnel add sit1 mode sit ttl 64 remote
70.1.1.2 local 70.1.1.1
root@sc-1# ip link set dev sit1 up
root@sc-1# ip -6 route add 2001:1:1:2::/64 dev sit1
metric 1
```

Для создания простого статического маршрута используются стандартные средства Linux – утилита `ip`. В общем виде для создания маршрута применяется следующая команда:

```
ip routeadd<удаленная_сеть/префикс>dev<адаптер>metric<значение_метрики>
```

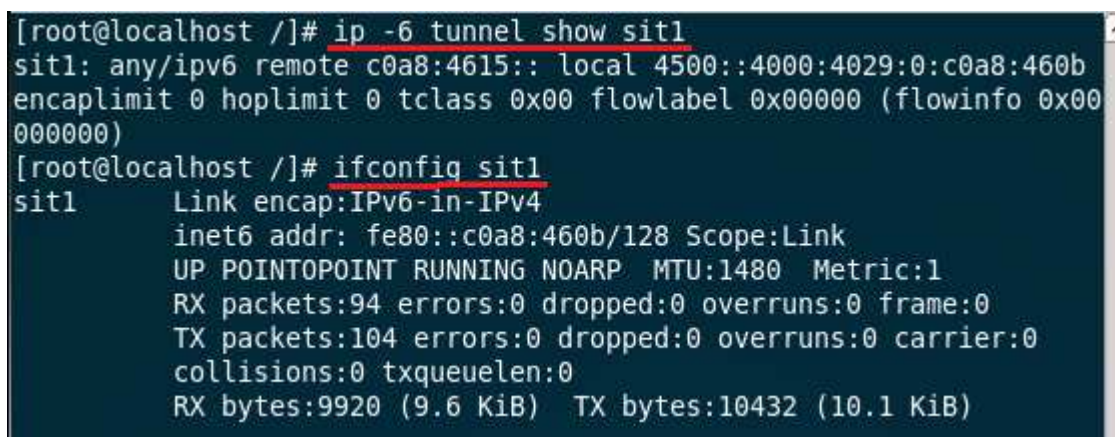
Здесь опция «-6» указывает на то, что используется адресация IPv6, имя адаптера указывает исходящий интерфейс, а значение метрики определяет приоритет маршрута: 1 – высший приоритет.

Аналогичным образом будет выглядеть процесс настройки на другой стороне туннеля (soft-core2):

```
root@sc-2# ip tunnel add sit1 mode sit ttl 64 remote
70.1.1.1 local 70.1.1.2
root@sc-2# ip link set dev sit1 up
root@sc-2# ip -6 route add 2001:1:1:1::/64 dev sit1
metric 1
```

Просмотреть существующий 6to4 туннель можно командами (рисунок 8.8):

```
ip -6 tunnel show sit1
ifconfig sit1
```



```
[root@localhost ~]# ip -6 tunnel show sit1
sit1: any/ipv6 remote c0a8:4615:: local 4500::4000:4029:0:c0a8:460b
encaplimit 0 hoplimit 0 tclass 0x00 flowlabel 0x000000 (flowinfo 0x00
000000)
[root@localhost ~]# ifconfig sit1
sit1      Link encap:IPv6-in-IPv4
          inet6 addr: fe80::c0a8:460b/128 Scope:Link
          UP POINTOPOINT RUNNING NOARP MTU:1480 Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9920 (9.6 KiB)  TX bytes:10432 (10.1 KiB)
```

Рисунок 8.8 – Информация о туннеле

Для проверки работоспособности туннеля необходимо запустить генератор трафика Ostinato на управляющем компьютере и создать новый UDP/IPv6-поток для интерфейса eth1.

Для этого соберите пакеты для потока как показано на рисунке 8.9.

Рисунок 8.9 – Проверочный поток. Конструирование пакета

При создании потока необходимо не забыть указать верный адрес назначения в поле MediaAccessProtocol (MAC-адрес порта eth0 маршрутизатора soft-core1), а также выставить верные значения в полях заголовка сетевого уровня IPv6 (рисунок 8.10).

	Address	Mode	Count	Prefix
Source	2001:1:1:1:0:0:33	Fixed	16	/64
Destination	2001:1:1:2:0:0:20	Fixed	16	/64

Рисунок 8.10 – Проверочный поток. Сетевой уровень

Убедиться в том, что в трейсе находятся инкапсулированные в IPv4 пакеты IPv6 необходимо запустить генерацию трафика, анализатором Wireshark снять трафик с порта eth0. Затем снять трафик с порта eth2. В случае успешной работы 6to4-туннеля увидите чистые IPv6-пакеты с адресом отправителя из сети 2001:1:1:1::/64.

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

- 1) Какие знаете методы расширения адресного пространства в сетях IPv4 и создания туннелей в сетях IPv4/IPv6?
- 2) Опишите Ваши представления о туннелировании в сетях?
- 3) Как настраивается NAT для организации расширенного адресного пространства в сетях IPv4?
- 4) Как настраивается туннель 6to4?
- 5) Как использовать специализированные утилиты для проверки состояния туннеля?

Алгоритм проведения эксперимента:

Часть 1:

1) Соберите сеть для выполнения первой части лабораторной работы согласно полученному заданию (рисунок 8.2, таблица 8.4).

2) Настройте SNAT/маскарадинг на soft-core1 согласно приведенной схеме подключившись к программному маршрутизатору.

3) Подключитесь к компьютеру управления и запустите генератор трафика Ostinato. Создайте для порта eth1 поток UDP-пакетов с произвольными портами (1024-65535), фиксированным IPv4-адресом отправителя (из указанных в задании подсети) и адресом назначения.

4) Настройте DNAT на маршрутизаторе soft-core2. Измените созданный ранее UDP-поток таким образом, чтобы портом назначения был 34001.

5) Проведите проверку правильности конфигурации NAT.

Часть 2:

6) Соберите сеть для выполнения второй части лабораторной работы согласно полученному заданию (рисунок 8.7, таблица 8.5).

7) Подключитесь к программным маршрутизаторам и создайте туннель согласно методике выполнения лабораторной работы.

8) Проверьте работу созданного туннеля.

Варианты заданий:

Таблица 8.4 – Задания к части 1

Вариант	Подсеть 1 (за SC-1)	Подсеть 2 (за SC-2)	soft-core1 eth1	soft-core2 eth1	PC-2 IP-адрес и порт DNAT	Тип NAT
1	192.168.17.0/24	192.168.78.0/24	51.1.1.2/27	51.1.1.18/27	.12:35468	MASQ
2	10.0.0.0/8	172.16.0.0/16	78.2.5.6/28	78.2.5.3/28	.98:47362	SNAT
3	192.168.82.0/24	10.0.0.0/8	122.98.2.1/26	122.98.2.3/26	.44:55612	SNAT
4	172.16.0.0/16	192.168.67.0/24	65.4.15.2/29	65.4.15.1/29	.75:29867	MASQ

Таблица 8.5 – Задания к части 2

Вариант	Подсеть 1 (за soft-core1)	Подсеть 2 (за soft-core2)	soft-core1 eth1	soft-core2 eth1
1	2001:8fa:ba4:23:: /64	2001:8fa:ba4:45:: /64	15.79.54.16/2 4	15.79.54.122/ 24
2	2001:9487:26ac:: 64	2001:9487:ac4:: 64	78.2.5.6/28	78.2.5.3/28
3	2001:b64:84:: /64	2001:b64:68d:: 64	203.78.9.1/29	203.78.9.3/29
4	2001:29:a1:330:: 64	2001:29:a1:320:: 64	51.1.1.2/27	51.1.1.18/27

Алгоритм обработки полученных экспериментальных данных:

Представить листинги проведенных действий, трейсы анализатора трафика, доказывающие правильность настройки NAT и туннеля bto4.

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №9 «НАСТРОЙКА СЕРВЕРА ДИНАМИЧЕСКОГО КОНФИГУРИРОВАНИЯ ХОСТОВ DNS В СЕТИ»

Цель занятия: получение навыков по организации адресного пространства в локальной и корпоративной сети.

Задачи занятия:

- 1) Настроить сервер динамического конфигурирования хостов;
- 2) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей, стеке протоколов сетевого оборудования, составе типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
- формирование умений о выборе режимов работы программно-аппаратных средств защиты информации в компьютерных сетях;
- формирование навыков настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации.

Материально-техническое оборудование и материалы:

- 1) Персональные компьютеры с операционной системой Windows или Linux (1 шт.);
- 2) Маршрутизатор (1 шт.);
- 3) Управляемый коммутаторы 2 уровня (1 шт).

План проведения лабораторного занятия

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к лабораторному занятию:

1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

4) RFC 2131: Dynamic Host Configuration Protocol, R. Droms, Bucknell University, March 1997. <http://tools.ietf.org/html/rfc2131>

5) RFC 3046: DHCP Relay Agent Information Option M. Patrick, Motorola BCS, January 2001. <http://tools.ietf.org/html/rfc3046>

6) Семенов Ю.А. Протокол динамического конфигурирования ЭВМ DHCP (и NAT/PAT). <http://book.itep.ru/4/4/dhcp.htm>.

Краткая теоретическая справка для самостоятельной подготовки к лабораторному занятию:

IP-адреса в сети могут назначаться стационарно (вручную) или динамически, для чего используется специализированный протокол DHCP. Dynamic Host Configuration Protocol – протокол динамической конфигурации узла – это сетевой протокол, позволяющий компьютерам автоматически получать как IP-адрес, так и адреса DNS-серверов и другие параметры, необходимые для работы в сети TCP/IP.

Во взаимодействии по протоколу DHCP могут принимать участие следующие стороны:

- DHCP-клиент – устройство, запрашивающее параметры настройки TCP/IP;
- DHCP-сервер – устройство, выдающее параметры настройки TCP/IP;
- DHCP-ретранслятор (relay agent) – вспомогательный участник, который может играть роль посредника между клиентом и сервером. DHCP-ретранслятор обрабатывает стандартный

широковещательный DHCP-запрос и перенаправляет его на DHCP-сервер в виде целенаправленного (unicast) пакета, а полученный от DHCP-сервера ответ, в свою очередь, перенаправляет DHCP-клиенту. Является не обязательным.

Стандартная процедура получения конфигурации от DHCP-сервера показана на рисунке 9.1.

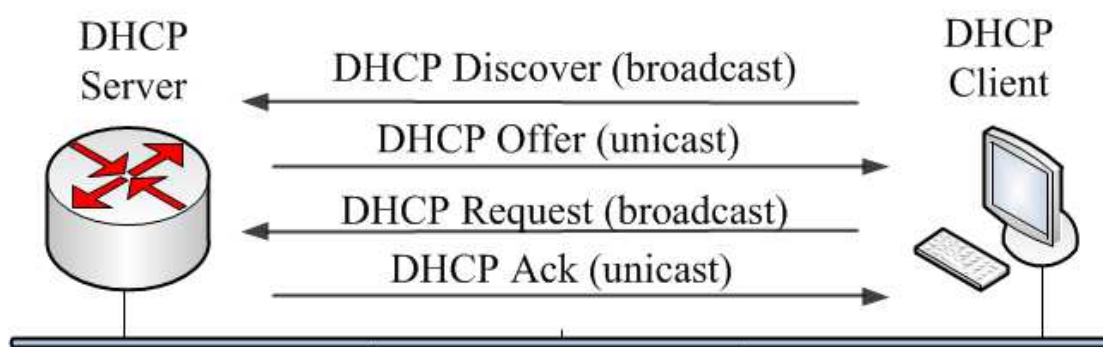


Рисунок 9.1 – Диаграмма процедура получения сетевой конфигурации от DHCP-сервера

Коммутатор может быть сконфигурирован как агент DHCP Relay. В этом случае он только перенаправляет DHCP-запрос от клиента локальной подсети на удалённый DHCP-сервер. Специализированная опция (Option 82) используется для передачи дополнительной информации в DHCP-запросе, которую добавляет непосредственно коммутатор. Опция 82 состоит из двух подопций:

1) *Agent Circuit ID* – содержит информацию о том, с какого порта пришел запрос на DHCP-ретранслятор.

2) *Agent Remote ID* – идентификатор самого DHCP-ретранслятора (который задается при настройке, можно, например, использовать MAC-адрес коммутатора или его описание, любое удобное значение).

Опция 82 в запросе DHCP приведена на рисунке 9.2.

Рекомендации по выполнению лабораторной работы для самостоятельного изучения:

Перед выполнением лабораторной работы необходимо привести макет в исходное состояние, загрузить в сетевое оборудование, которое будет использоваться в данной лабораторной работе, соответствующие конфигурационные файлы, убедиться в работоспособности файлового сервера.

```

Option: (t=82,l=12) Agent Information Option
Option: (82) Agent Information Option
Length: 12
Value: 010200030206001560792800
Agent Circuit ID: 0003
Agent Remote ID: 001560792800
End Option

```

Рисунок 9.2 – Вид опции 82 в запросе DHCP

1) Подключить терминальными кабелями маршрутизатор и управляемый коммутатор SW-L2-1 к компьютеру управления, включить сетевое оборудование, настроить статические сетевые интерфейсы на компьютере управления согласно схеме сети (рисунок 9.3), проверить доступность FTP-сервера.

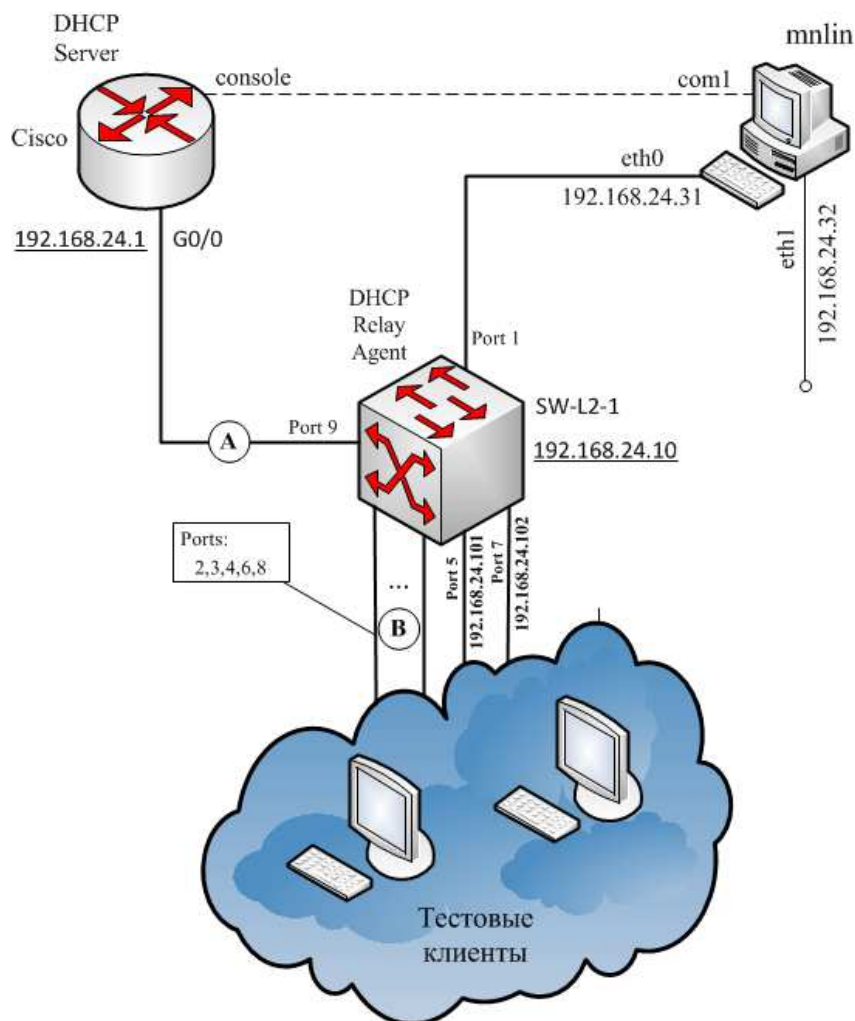


Рисунок 9.3 – Схема лабораторной сети

2) Включить в коммутаторе поддержку DHCP Relay Agent. Для этого с компьютера управления необходимо зайти на web-интерфейс коммутатора, который находится по адресу 192.168.24.10. В случае использования коммутатора от D-Link зайти во вкладку Configuration→DHCP Relay→DHCP Relay Global Settings и выставить значения полей DHCP Relay State и DHCP Relay Agent Information Option 82 в состояние Enable (рисунок 9.4).

Примечание: При необходимости здесь же можно изменить MAC-адрес коммутатора, передающийся DHCP- серверу в опции 82, выставив его в поле DHCP Relay Agent Information Option 82 Remote-ID.

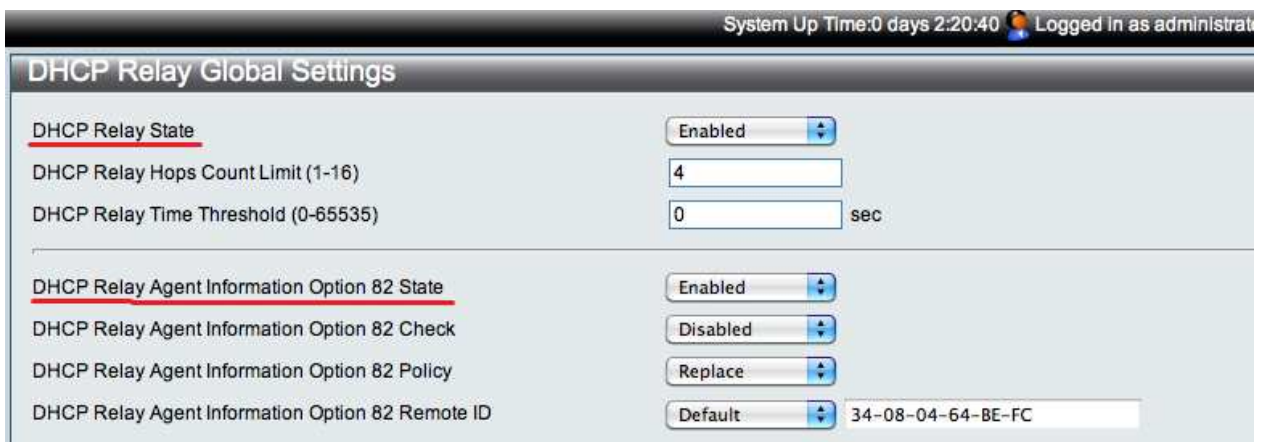


Рисунок 9.4 – Вкладка DHCP Relay Global Settings

После необходимо указать адрес используемого DHCP-сервера на вкладке Configuration→DHCP Relay→DHCP Interface Settings (рисунок 9.5). Для этого нужно добавить IP-адрес будущего сервера: 192.168.24.1, и принять сделанные изменения.



Рисунок 9.5 – Вкладка DHCP Interface Settings

3) Для того чтобы сервер мог распознать запросы, содержащие опцию 82, нужно выяснить вид данной опции в конкретном случае. Как описано выше, существует стандартная форма опции 82, однако у разных производителей оборудования эта реализация

может отличаться. Поэтому надежным вариантом будет определение её вида на конкретном оборудовании:

а) Собрать вспомогательную схему сети, представленную на рисунке 9.6, для определения вида опции 82.

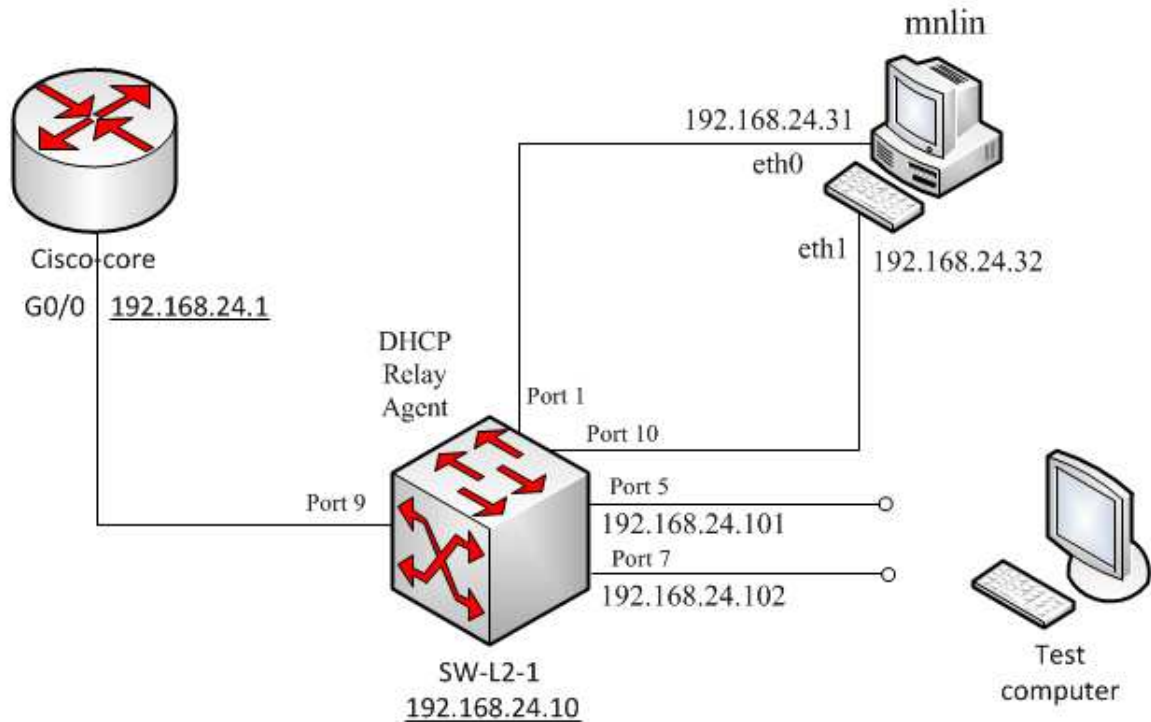


Рисунок 9.6 – Схема вспомогательной сети

б) Настроить полное зеркалирование трафика с порта 9 на порт 10. Это позволит отслеживать запросы DHCP Discover с добавленной опцией 82, посылаемые коммутатором в сторону ранее указанного нами DHCP-сервера (192.168.24.1). Находясь в web-интерфейсе коммутатора, необходимо перейти на вкладку L2 Features→Port Mirror и выставить зеркалирование всего трафика с порта 9 на порт 10 как показано на рисунке 9.7.

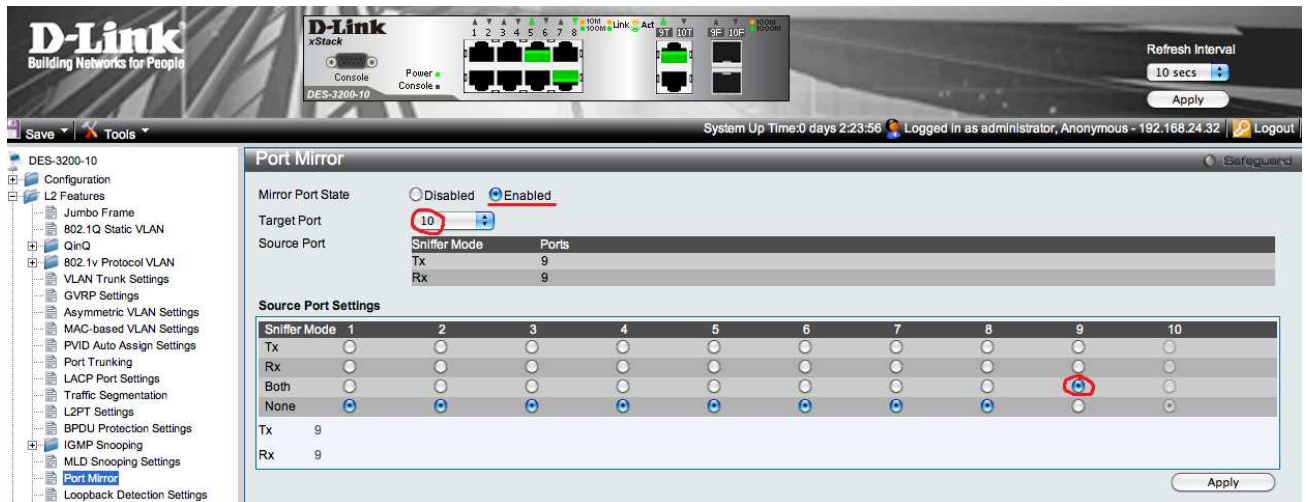


Рисунок 9.7 – Настройка зеркалирования портов

с) Запустить анализатор трафика на интерфейсе eth1 компьютера управления, соединенном с портом 10 коммутатора. Для уменьшения количества пакетов в трейсе необходимо нажать Start в тот момент, когда будете готовы выполнить следующий пункт или подключить фильтр трафика.

д) Подключить тестовую машину с сетевым интерфейсом настроенным на получение конфигурации по протоколу DHCP к порту 5 коммутатора.

е) Определить вид поля Option 82 в запросе DHCP Discover. После подключения тестовой машины достаточно снимать трэйс в течение приблизительно 10 секунд. Для облегчения поиска в полученном трэйсе используйте фильтрующее выражение «bootp». В трэйсе необходимо найти первое по времени сообщение протокола DHCP, направленное на адрес 192.168.24.1 (это и будет сообщение Discover), и в заголовке верхнего уровня найти поле Option (82): Agent information option. Значение value и будет интересующей опцией 82. Данное значение необходимо записать для последующего использования.

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_19:6a:60	Cisco_19:6a:60	LOOP	60	Reply
2	0.466752	192.168.24.2	192.168.24.1	DHCP	384	DHCP Discover - Transaction ID 0xe4c15elf
3	0.467083	192.168.24.1	192.168.24.2	ICMP	70	Destination unreachable (Port unreachable)
4	2.340338	192.168.24.32	224.0.0.251	MDNS	269	Standard query PTR _apple-mobdev._tcp.local, *QM* question PTR_a
5	2.340398	fe80::222:41ff:fe26:34cc	ff02::fb	MDNS	289	Standard query PTR _apple-mobdev._tcp.local, *QM* question PTR_a
6	2.340424	192.168.24.32	224.0.0.251	MDNS	269	Standard query PTR _apple-mobdev._tcp.local, *QM* question PTR_a
7	2.340428	fe80::222:41ff:fe26:34cc	ff02::fb	MDNS	289	Standard query PTR _apple-mobdev._tcp.local, *QM* question PTR_a
8	3.825561	192.168.24.32	255.255.255.255	DB-LSP-DI	150	Dropbox LAN sync Discovery Protocol
9	3.825626	192.168.24.32	255.255.255.255	DB-LSP-DI	150	Dropbox LAN sync Discovery Protocol
10	3.826729	192.168.24.32	192.168.24.255	DB-LSP-DI	150	Dropbox LAN sync Discovery Protocol
11	3.826800	192.168.24.32	192.168.24.255	DB-LSP-DI	150	Dropbox LAN sync Discovery Protocol
12	3.855857	192.168.24.2	192.168.24.1	DHCP	384	DHCP Discover - Transaction ID 0xe4c15elf
13	3.856109	192.168.24.1	192.168.24.2	ICMP	70	Destination unreachable (Port unreachable)


```

Boot file name not given
Magic cookie: DHCP
Option: (t=53,l=1) DHCP Message Type = DHCP Discover
Option: (t=57,l=2) Maximum DHCP Message Size = 1500
Option: (t=60,l=46) Vendor class identifier = "dhcpcd-5.2.11:Linux-2.6.37.4:i686:AuthenticAMD"
Option: (t=12,l=7) Host Name = "zenwalk"
Option: (t=55,l=15) Parameter Request List
Option: (t=82,l=18) Agent Information Option
  Option: (82) Agent Information Option
  Length: 18
  Value: 01060004000100070208000634080464befc
  Agent Circuit ID: 000400010007
  Agent Remote ID: 000634080464befc
End Option

```



```

0140 69 36 38 36 3a 41 75 74 68 65 6e 74 69 63 41 4d i686:Aut henticAM
0150 44 0c 07 7a 65 6e 77 61 6c 6b 37 0f 01 79 21 03 D..zenwa lk7..y!
0160 06 0c 0f 1a 1c 2a 33 36 3a 3b 77 52 12 01 06 00 .....*36 ;;wR...
0170 04 00 01 00 07 02 08 00 05 34 08 04 64 be fc ff .....4..d..

```

Рисунок 9.8 – Получение значения опции 82

- f) Выполнить аналогичную процедуру для порта 7.
- 4) Собрать сеть согласно схеме, приведенной на рисунке 3.
- 5) Сконфигурировать DHCP-сервер. С компьютера управления необходимо подключиться к консольному порту маршрутизатора и сконфигурировать на нем DHCP-сервер. Для этого можно использовать терминальную утилиту `picosom`:

```
root@mnlm# picosom /dev/ttyS0
```

где `ttyS0` – символьное устройство порта `com1`, `ttyS1` – соответственно, `com2` и т.д. Для выхода из утилиты `picosom` нажмите одновременно клавиши `Ctrl+A+Q`.

Ниже приведен пример конфигурации DHCP-сервера на маршрутизаторе от CiscoSystems с необходимыми пояснениями:

```

cisco-core>
cisco-core>enable/Вход в привилегированный режим
cisco-core#configure terminal /режимконфигурирования
cisco-core(config)#interface gigabitethernet 0/0
/выборинтерфейса
cisco-core(config-if)#ip address 192.168.24.1
255.255.255.0 /задание ip-адресаинтерфейсаимаскиподсети
cisco-core(config-if)#no shutdown /включениеинтерфейса
cisco-core(config-if)#end /выходизрежимаконфигурации
cisco-core#configureterminal

```

```
cisco-  
core(config)#ipdhcpdatabaseftp://admin:пароль@192.168.2  
4.31/dhcp-db /указание DHCP-серверу адреса для хранения  
базы данных подключающихся клиентов (FTP-сервер  
управляющем компьютере)  
cisco-core(config)#service dhcp/включение службы DHCP  
cisco-core(config)#ipdhcpuseclass /включение  
использования классов  
cisco-core(config)#ipdhcpexcluded-address 192.168.24.1  
192.168.24.59 /задание диапазона, адреса из которого  
не будут выдаваться клиентам  
cisco-core(config)#ip dhcp class port5/создание класса  
port5  
cisco-core(config-dhcp-  
class)#relayagentinformation/указывание, что  
сопоставление запроса данному классу будет  
производиться путем сравнения поля option 82 запроса с  
заданным значением  
cisco-core(config-dhcp-class-relayinfo)#relay-  
informationhex 01060004000100050208000634080464befc  
/указание строки сопоставления запроса данному классу;  
здесь нужно использовать полученное ранее значение  
опции 82  
cisco-core(config-dhcp-class-relayinfo)#end /выход из  
режима конфигурации  
cisco-core#  
cisco-core#configure terminal  
cisco-core(config)#ip dhcp class port7  
cisco-core(config-dhcp-class)#relay agent information  
cisco-core(config-dhcp-class-relayinfo)#relay-  
information hex 01060004000100070208000634080464befc  
cisco-core(config-dhcp-class-relayinfo)#end  
cisco-core#  
cisco-core#configure terminal  
cisco-core(config)#ipdhcpclasscommon-net /создание  
общего класса для всех запросов не соответствующих  
классам port5 и port7  
cisco-core(config-dhcp-class)#relay agent information  
cisco-core(config-dhcp-class-relayinfo)#end  
cisco-core#  
cisco-core#configure terminal  
cisco-core(config)#ipdhcppoolLAN1 /создание пула  
адресов LAN1 и указание сведений, которые DHCP-сервер  
будет выдавать клиентам
```



```

cisco-core(dhcp-config)#network 192.168.24.0
255.255.255.0 /подсеть, в которой DHCP-сервером
будут выдаваться адреса
cisco-core(dhcp-config)#domain-name lan1.maket /доменное
имя
cisco-core(dhcp-config)#dns-server 192.168.24.1 /DNS-
сервер
cisco-core(dhcp-config)#default-router
192.168.24.1/шлюз по умолчанию
cisco-core(dhcp-config)#classport5 /специфические
настройки для клиентов, чей запрос соответствует классу
port5
cisco-core(config-dhcp-pool-class)#addressrange
192.168.24.101 192.168.24.101 /диапазон выдаваемых
адресов (в нашем случае, по заданию, состоит из одного
адреса)
cisco-core(config-dhcp-pool-class)#end
cisco-core#configure terminal
cisco-core(config)#ip dhcp pool LAN1 / настройка пула
LAN1
cisco-core(dhcp-config)#class port7
cisco-core(config-dhcp-pool-class)#address range
192.168.24.102 192.168.24.102
cisco-core(config-dhcp-pool-class)#end
cisco-core#
cisco-core#configure terminal
cisco-core(config)#ip dhcp pool LAN1
cisco-core(dhcp-config)#class common-net
cisco-core(config-dhcp-pool-class)#end
cisco-core#
cisco-core#showrunning-config
/проверкаполученнойконфигурации

```

Включение вывода сообщений DHCP-сервера относящихся к процедуре сопоставления входящих запросов имеющимся классам:

```

cisco-core#debug ip dhcp server class
DHCP server class debugging is on.

```

На основе приведенной процедуры конфигурации необходимо настроить DHCP-сервер в соответствии с заданием к лабораторной работе.

б) Проверка работоспособности конфигурации производится путем подключения тестовых машин к разным портам коммутатора и определения на них назначенных IP-адресов.

Посмотреть статистику работы DHCP-сервера по базе данных можно в терминале Cisco следующими командами:

```
cisco-core#show ip dhcp bindings
cisco-core#show ip dhcp conflicts
cisco-core#show ip dhcp database
cisco-core#show ip dhcp statistics
```

После просмотра статистику можно очистить:

```
cisco-core#clear ip dhcp binding *
cisco-core#clear ip dhcp conflict *
cisco-core#clear ip dhcp server statistics
```

7) Используя анализатор трафика и возможности зеркалирования портов коммутатора, необходимо зарисовать диаграмму процедуры получения хостами конфигурации от DHCP-сервера в точках А и В (рисунок 9.3) и сравнить ее со стандартной процедурой.

Дополнительно: на основе полученных значений опции 82 определить содержащиеся в ней поля и предсказать значение опции 82 для любых портов и MAC-адресов применяемого коммутатора.

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной лабораторной работе:

5) Какие принципы работы протокола DHCP?

2) Опишите Ваши представления о методах зеркалирования трафика.

3) Как использовать анализатор трафика для оценки полученного результата?

Алгоритм проведения эксперимента:

Организовать локальную сеть, в которой подключаемые клиенты будут получать конфигурацию сетевых интерфейсов динамически от DHCP-сервера на базе маршрутизатора. Раздаваемые адреса должны находиться в подсети 192.168.24.0/24, причем адреса в диапазоне 192.168.24.1 – 192.168.24.59

зарезервированы (не должны выдаваться клиентам). Клиенты, подключенные к портам 5 и 7 коммутатора, должны всегда получать адреса 192.168.24.101 и 192.168.24.102 соответственно.

Алгоритм обработки полученных экспериментальных данных:

Представить схему сети (аналогично рисунку 9.3), трейс анализатора трафика, диаграмму процедуры получения конфигурации хостами от DHCP-сервера в точках А и В.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №1 «АНАЛИЗ ТРАФИКА ЛОКАЛЬНОЙ СЕТИ НА ПРИМЕРЕ ARP, DNS, HTTP»

Цель занятия: исследование основных типов трафика в реальной локальной сети на примере наиболее распространенных протоколов стека TCP/IP.

Задачи занятия:

- 1) Произвести анализ сетевого трафика с использованием программного продукта Wireshark;
- 2) Произвести анализ структуры сети с использованием программного продукта Zenmap;
- 3) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование умений настраивать правила фильтрации пакетов в компьютерных сетях;
- проведение мониторинга функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
- формирование знаний о методах измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой Windows или Linux, подключенный в сеть Интернет;
- 2) Анализатор трафика Wireshark;
- 3) Сетевой сканер Zenmap.

План проведения практического занятия

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к практическому занятию:

1) Wireshark User Guide, U.Lamping, R.Sharpe, E.Warnicke. http://www.wireshark.org/docs/wsug_html_chunked.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

Краткая теоретическая справка для самостоятельной подготовки к практическому занятию:

В лабораторной работе исследуется два типа трафика: broadcast (широковещательный, на примере протокола ARP) и unicast (на примере протокола HTTP). Предполагается, что к моменту выполнения лабораторной работы из курса лекций известна структура и основные принципы работы протоколов ARP, DNS и HTTP, а также структура кадра Ethernet. Лабораторная работа проводится с использованием свободно распространяемого (лицензия GNU GPL) анализатора трафика Wireshark.

В настоящее время существует достаточно большой выбор анализаторов трафика – специальных программ, позволяющих получить информацию о пакетах, передающихся по исследуемой сети. Все они, несмотря на различных разработчиков, объединены одной идеей: предоставить возможность не только определить тип пакета, но и его структуру. Информация о структуре пакета в ПО Wireshark выводится в виде таблиц анализа (рисунок 10.1).

Таблица анализа представляет собой три поля, которые заполняются динамически по мере поступления пакетов. В основной части представлена информация о соединении: MAC-адреса источника и получателя, IP-адреса источника и получателя, протокол, порт отправителя и порт получателя. Обратите внимание – зарезервированные порты часто обозначаются именем протокола: например, порты 80 и 8080 могут обозначаться как HTTP. Одна строка в этой таблице относится к одному пакету. При выделении строки в двух других окнах появляется информация о структуре пакета.

Поле со структурой пакета позволяет определить, как заполнены поля протоколов в соответствии со стандартом. Это позволяет определить адреса отправителя и получателя, номер порта, корректность контрольной суммы и т.п.

Поле с представлением пакета в ASCII кодах и 16-ричной системе дает представление о реальном виде пакета при передаче по сети. В большинстве анализаторов предусмотрена возможность

выделения пункта в поле со структурой пакета и одновременное выделение соответствующих знаков в поле с представлением пакета в 16-ричной системе.

The screenshot shows the Wireshark interface with the following details:

- Packet List:**

No.	Time	Source	Destination	Protocol	Info
25	2.285390	81.26.181.191	192.168.1.100	UDP	Source port: 53071 Destination port: 53530
26	2.285442	192.168.1.100	81.26.181.191	ICMP	Destination unreachable (Port unreachable)
27	2.285764	81.26.181.191	192.168.1.100	TCP	52892 > 35836 [SYN] Seq=0 Win=8192 Len=0 MSS=1416 WS=2
28	2.285772	192.168.1.100	81.26.181.191	TCP	35836 > 52892 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	2.376521	192.168.1.100	213.180.193.119	HTTP	GET /clmap/4308403?rn=220421&page-url=http%3A%2F%2Fflenta.ru%2Fpointe
30	2.379107	192.168.1.100	213.180.193.119	TCP	33998 > http [FIN, ACK] Seq=764 Ack=1 Win=1002 Len=0 TSV=560158 TSER=
31	2.379472	192.168.1.100	81.19.85.92	TCP	60295 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=560158 TSER=0 WS
32	2.390681	213.180.193.119	192.168.1.100	HTTP	HTTP/1.1 200 OK (GIF89a)
33	2.390726	192.168.1.100	213.180.193.119	TCP	33998 > http [RST] Seq=764 Win=0 Len=0
34	2.392232	188.32.134.146	192.168.1.100	UDP	Source port: 35691 Destination port: 35836
35	2.392256	192.168.1.100	188.32.134.146	ICMP	Destination unreachable (Port unreachable)
36	2.392507	213.180.193.119	192.168.1.100	TCP	http > 33998 [FIN, ACK] Seq=385 Ack=765 Win=1881 Len=0 TSV=561707318
37	2.392516	192.168.1.100	213.180.193.119	TCP	33998 > http [RST] Seq=765 Win=0 Len=0
38	2.392708	188.32.134.146	192.168.1.100	TCP	npsd > 35836 [SYN] Seq=0 Win=65535 Len=0 MSS=1440
39	2.392716	192.168.1.100	188.32.134.146	TCP	35836 > npsd [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
- Packet 29 Details:**
 - Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst: 213.180.193.119 (213.180.193.119)
 - Transmission Control Protocol, Src Port: 33998 (33998), Dst Port: http (80), Seq: 1, Ack: 1, Len: 763
 - Hypertext Transfer Protocol
 - GET /clmap/4308403?rn=220421&page-url=http%3A%2F%2Fflenta.ru%2Fpointer-click=x:16294;y:12822;t:473;p:1%3B%5Db%5C%5B%5D1b%5C%5B2 HTTP/1.1\r\n
 - Host: mc.yandex.ru\r\n
 - User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:11.0) Gecko/20100101 Firefox/11.0\r\n
 - Accept: image/png,image/*;q=0.8,*/*;q=0.5\r\n
 - Accept-Language: ru-ru,ru;q=0.8,en-us;q=0.5,en;q=0.3\r\n
 - Accept-Encoding: gzip, deflate\r\n
- Packet Bytes:**

```

00c0 32 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 2 HTTP/1.1..Host
00d0 3a 20 6d 63 2e 79 61 6e 64 65 78 2e 72 75 0d 0a : mc.yan dex.ru..
00e0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
00f0 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 55 62 lla/5.0 (X11; Ub
0100 75 6e 74 75 3b 20 4c 69 6e 75 78 20 69 36 38 36 untu; Li nux i686
0110 3b 20 72 76 3a 31 31 2e 30 29 20 47 65 63 6b 6f ; rv:11.0) Gecko
0120 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f /20100101 Firefo
0130 78 2f 31 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 x/11.0.. Accept:
0140 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f image/pn g,image/
0150 2a 3b 71 3d 30 2e 38 2c 2a 2f 2a 3b 71 3d 30 2e /*;q=0.8, */;q=0.
0160 35 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 5..Accep t-Langua
0170 67 65 3a 20 72 75 2d 72 75 2c 72 75 3b 71 3d 30 ge: ru-r u,ru;q=0
0180 2e 38 2c 65 6e 2d 75 73 3b 71 3d 30 2e 35 2c 65 .8,en-us;q=0.5,e
0190 6e 3b 71 3d 30 2e 33 0d 0a 41 63 63 65 70 74 2d n;q=0.3..Accep t-
01a0 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 Encoding: gzip,
01b0 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 deflate. .Connect
01c0 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: kee n-alive

```

Рисунок 10.1 – Пример таблицы анализа: пакет HTTP, запрос к серверу

Также анализатор трафика позволяет собрать статистику о пакетах, проходящих по сети на различных уровнях модели TCP/IP. В качестве примера на рисунке 10.2 представлена статистика по размерам пакетов (Statistics→PacketLengths), а на рисунке 10.3 – по типам протоколов и видам данных, встречающихся в захваченном трафике (Statistics→ProtocolHierarchy).

При необходимости можно визуально оценить на общем графике интенсивность интересующих видов трафика по протоколам (до пяти протоколов одновременно), настроив соответствующим образом фильтры в окне IOGraphs (как показано на рисунке 10.4). Данный инструмент находится в меню Statistics→IOGraphs.

Topic / Item	Count	Rate	Percent
Packet Lengths	441	0,064235	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	294	0,042823	66,67%
80-159	32	0,004661	7,26%
160-319	17	0,002476	3,85%
320-639	24	0,003496	5,44%
640-1279	19	0,002767	4,31%
1280-2559	55	0,008011	12,47%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Рисунок 10.2 – Пример статистики по размерам пакетов

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	441	137628	0,160	0	0	0,000
Ethernet	100,00 %	441	137628	0,160	0	0	0,000
Internet Protocol	100,00 %	441	137628	0,160	0	0	0,000
Transmission Control Protocol	85,03 %	375	129157	0,151	327	99389	0,116
Hypertext Transfer Protocol	10,88 %	48	29768	0,035	26	17906	0,021
Compuserve GIF	1,59 %	7	3753	0,004	7	3753	0,004
Line-based text data	2,95 %	13	5905	0,007	13	5905	0,007
JPEG File Interchange Format	0,23 %	1	1494	0,002	1	1494	0,002
Media Type	0,23 %	1	710	0,001	1	710	0,001
User Datagram Protocol	9,98 %	44	5628	0,007	0	0	0,000
Data	4,76 %	21	2139	0,002	21	2139	0,002
Teredo IPv6 over UDP tunneling	0,23 %	1	88	0,000	0	0	0,000
Internet Protocol Version 6	0,23 %	1	88	0,000	1	88	0,000
Domain Name Service	4,99 %	22	3401	0,004	22	3401	0,004
Internet Control Message Protocol	4,99 %	22	2843	0,003	22	2843	0,003

Рисунок 10.3 – Пример статистики по типам протоколов

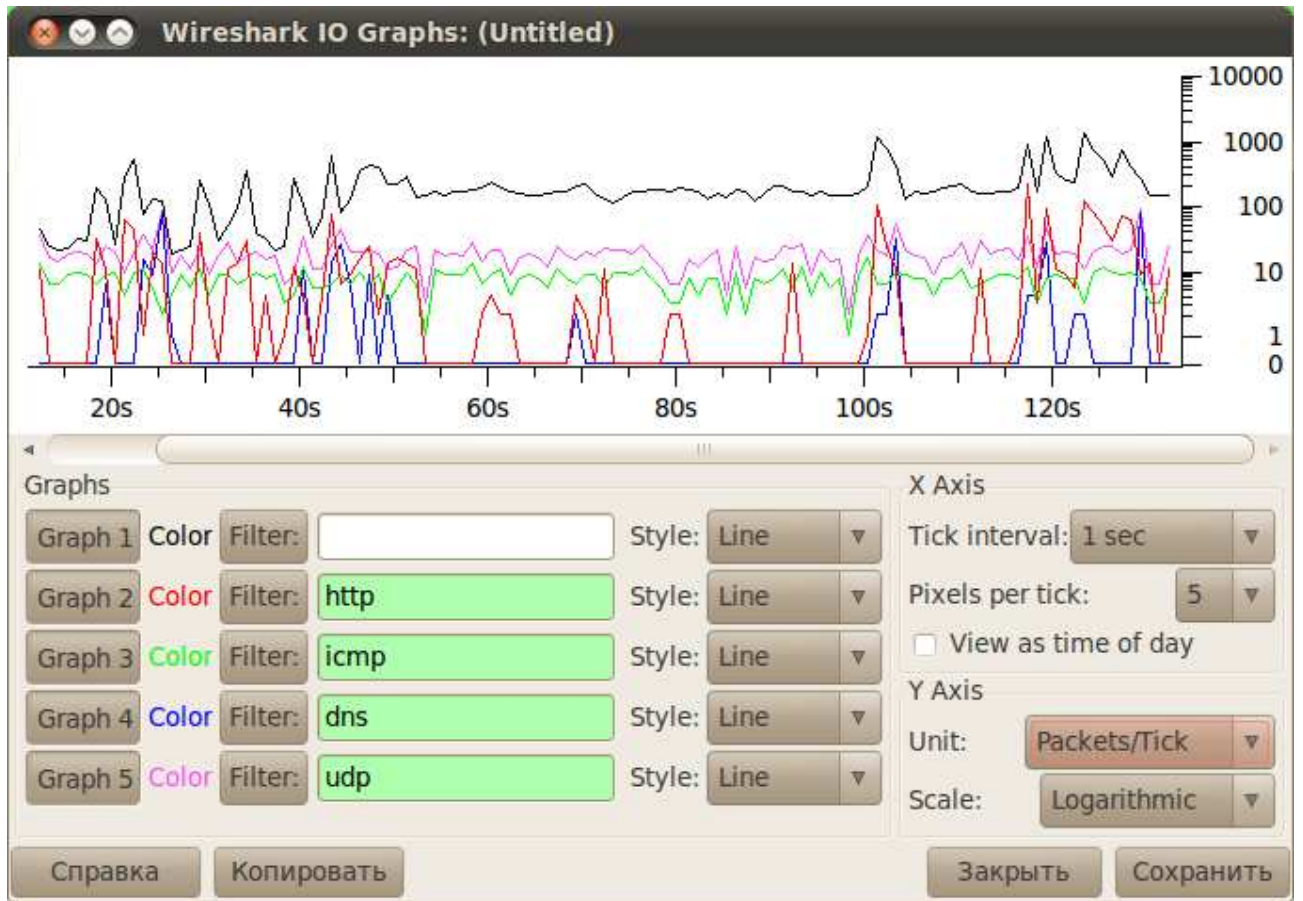


Рисунок 10.4 – Графики интенсивности захваченного трафика

Кроме того, в большинстве анализаторов можно увидеть статистику по хостам. На сетевом уровне такая статистика (Statistics→IPDestinations) позволяет оценить долю трафика соответствующую конкретным IP-адресам и используемым ими протоколам (рисунок 10.5).

Инструмент GraphAnalysis из меню Statistics, окно которого показано на рисунке 10.6, позволяет в графическом виде представлять процедуры обмена данными на основании захваченного трафика.

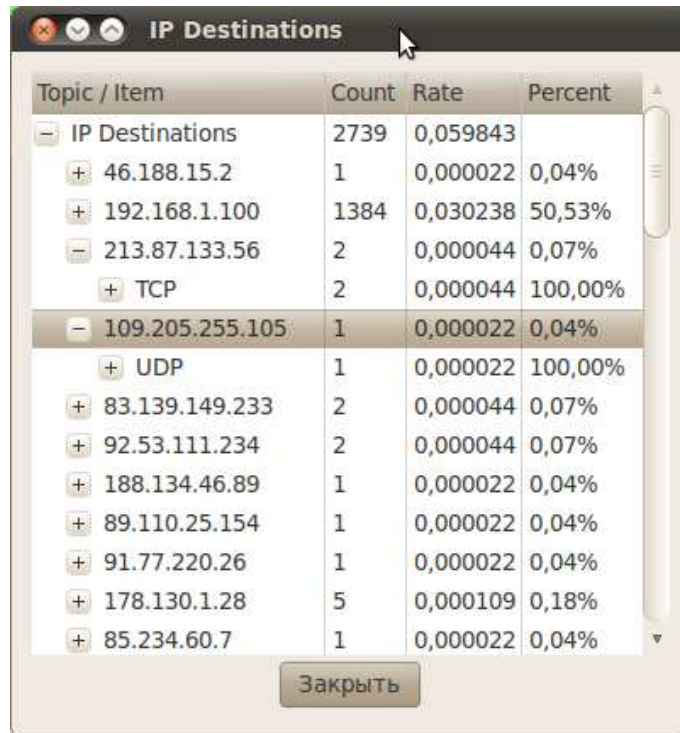


Рисунок 10.5 – Статистика IP-адресов в захваченном трафике

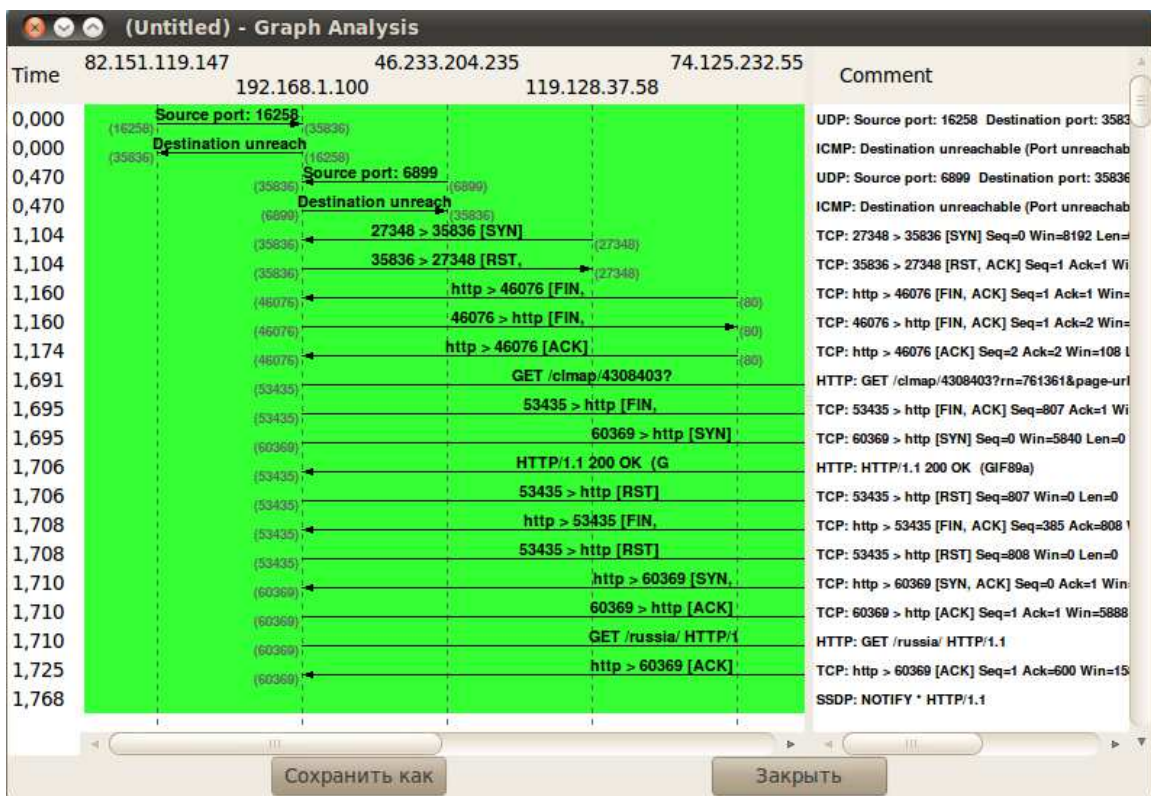


Рисунок 10.6 – Диаграммы соединений

Качество подготовки к практическому занятию преподаватель оценивает по результатам собеседования, защиты отчета по практической работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной практической работе:

- 1) Какие знаете принципы формирования пакетов в локальных сетях (технологии IP и Ethernet)?
- 2) Опишите представление о функциях и процессе формирования пакетов протоколов ARP и HTTP, запросов/ответов DNS.
- 3) Каковы особенности широковещательного трафика?

Алгоритм проведения практического задания:

1) Запустить анализатор трафика Wireshark. После выбора требуемого сетевого интерфейса кнопкой Start начать сбор трафика (рисунок 10.7).

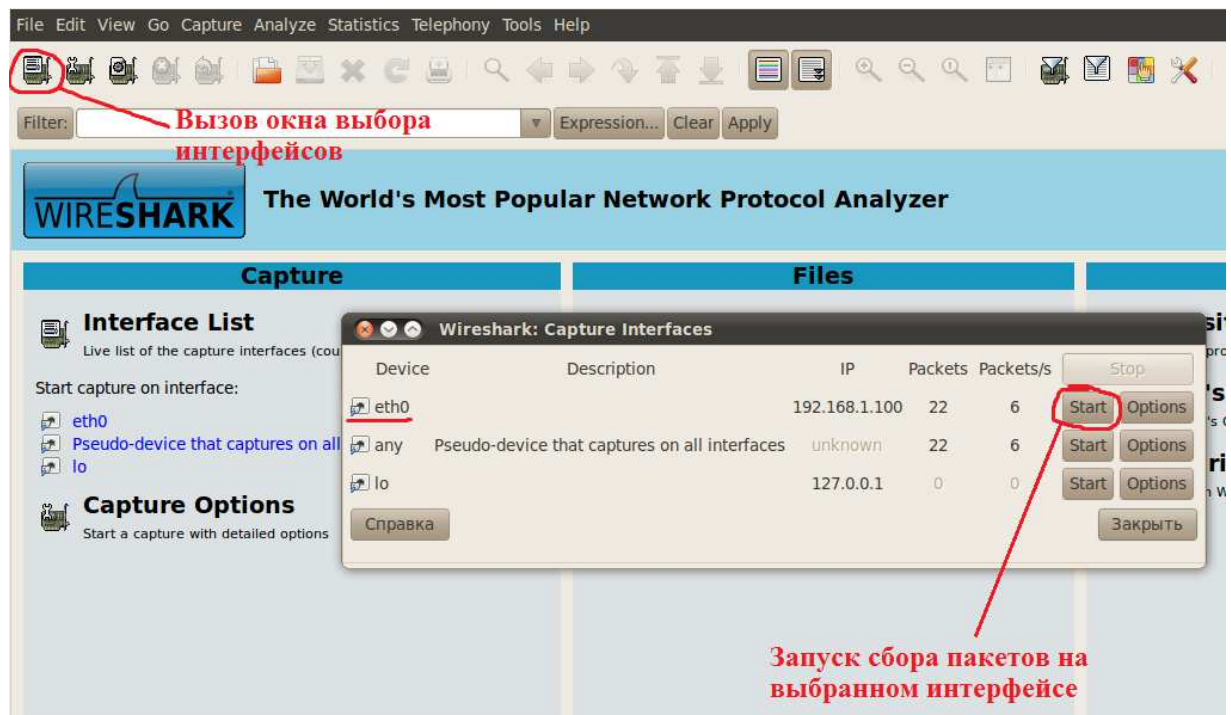


Рисунок 10.7 – Запуск процедуры сбора пакетов

2) Настроить фильтр на широковещательный трафик (рисунок 10.8): нажатием на кнопку Filter в панели инструментов Wireshark запустить окно выбора/создания фильтра, ввести любое имя для нового фильтра в поле FilterName, а в качестве фильтрующего выражения (FilterString) выставить название протокола ARP. Для применения фильтра нажмите кнопку Apply на панели инструментов.

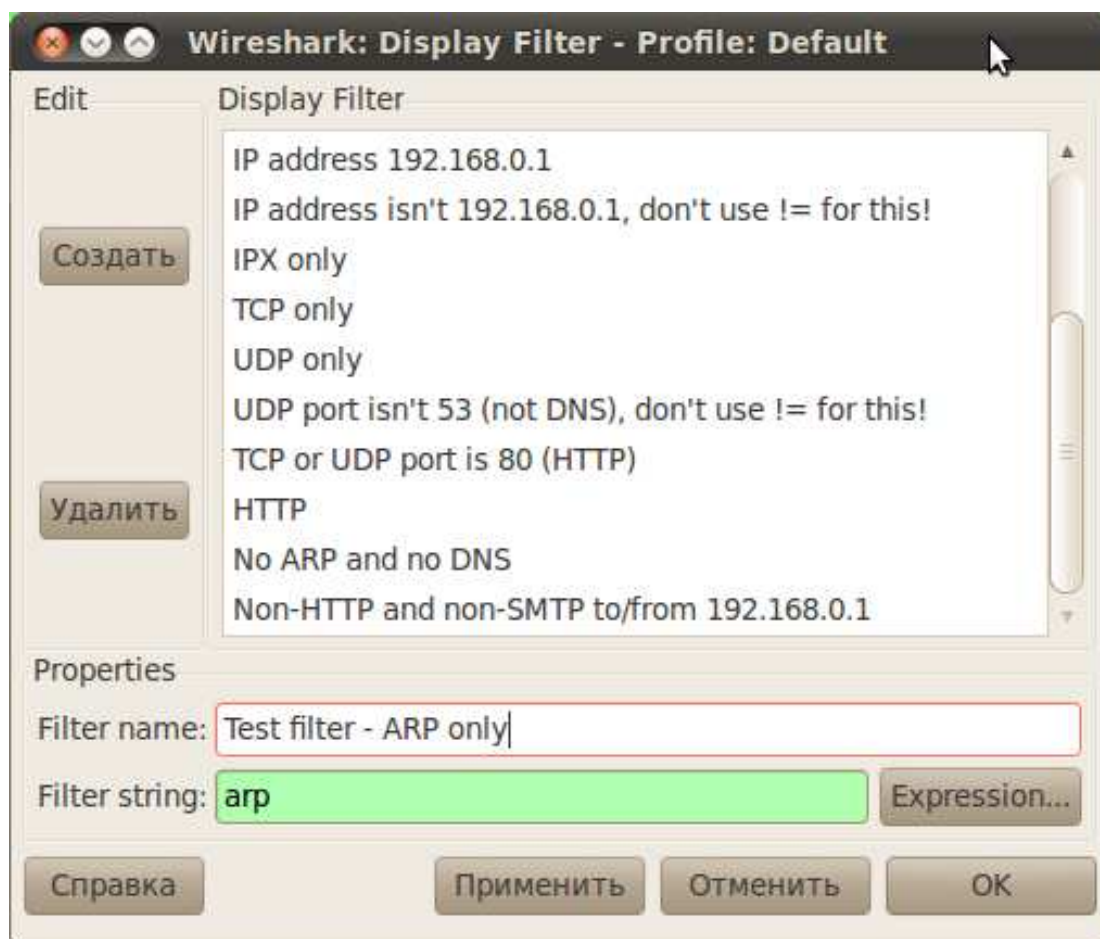


Рисунок 10.8 – Настройка фильтра для анализа ARP-пакетов

3) Разобрать пакет ARP: запрос и ответ. Снять скриншоты экранов с таблицами анализа протокола ARP.

4) Убрать настройку фильтров. Запустить браузер, набрать URL какого-либо веб-ресурса (по желанию слушателя или заданию преподавателя). Отследить и разобрать пакеты DNS (запрос и ответ).

5) Разобрать пакеты HTTP двух типов: запрос (GET) и ответ сервера. Снять скриншоты экранов: таблицы анализа, график интенсивности трафика HTTP в общем трафике, диаграмму соединений.

6) На основании данных об IP-адресах, полученных в программе Zenmap, построить карту сети (рисунок 10.9), указав с помощью соединительных линий логические связи (т.е. наличие соединений) между хостами.

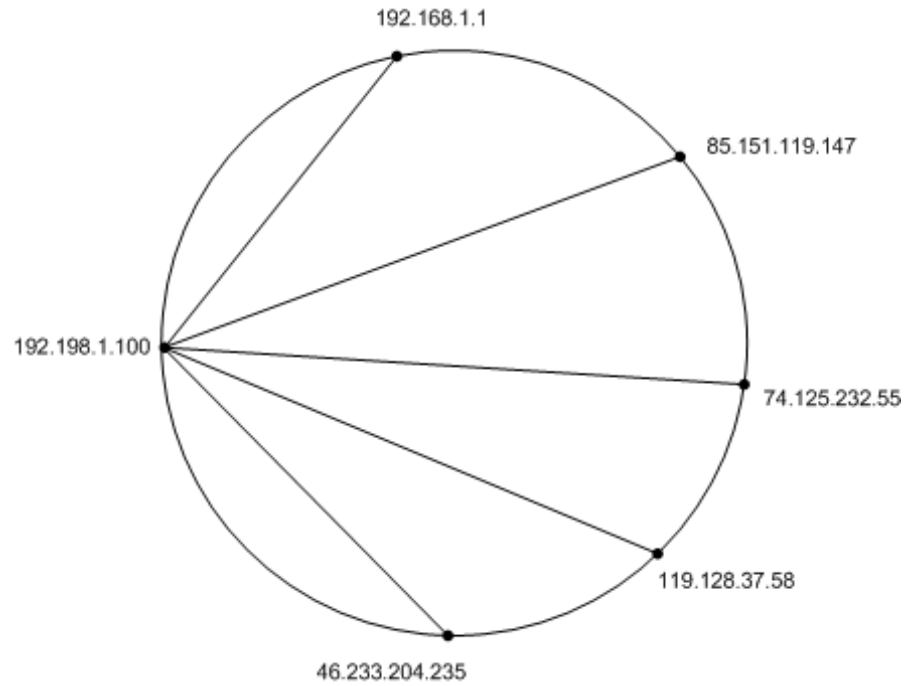


Рисунок 10.9 – Пример карты сети

Алгоритм обработки полученных данных:

Представить скриншоты для всех исследуемых протоколов:
таблицы с анализом трафика, графики, диаграммы.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №2 «ИСПОЛЬЗОВАНИЕ ГЕНЕРАТОРА ТРАФИКА ДЛЯ СОЗДАНИЯ НАГРУЗКИ В СЕТИ»

Цель занятия: изучение принципов генерации трафика с помощью программы Ostinato на примере наиболее распространенных протоколов стека TCP/IP.

Задачи занятия:

- 1) Произвести нагрузку локальной сети с использованием программного продукта «Ostinato»;
- 2) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о стеке протоколов сетевого оборудования, принципах работы и правилах эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, видах политик управления доступом и информационными потоками в компьютерных сетях, методах измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;
- формирование умений выбора режимов работы программно-аппаратных средств защиты информации в компьютерных сетях;
- формирование навыков о контроле корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой, подключенный в сеть Интернет;
- 2) Генератор трафика «Ostinato».

План проведения практического занятия

Практическому занятию предшествует самостоятельная работа

студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к практическому занятию:

1) Ostinato: Packet/Traffic Generator and Analyzer.
<https://code.google.com/p/ostinato/>

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

Краткая теоретическая справка для самостоятельной подготовки к практическому занятию:

Генераторы трафика являются необходимыми инструментами для проверки работоспособности сетей как на этапе тестовых испытаний, так и при разработке новых услуг и технологий. Генераторы трафика бывают как программно-аппаратными, так и программными. Программно-аппаратные генераторы трафика обычно крайне дороги, являются закрытыми решениями, но при этом обладают специальным функционалом, ориентированным на тип сети. Что касается программных генераторов, то среди них есть достаточно большое количество предложений с открытым кодом, но позволяющих конструировать только пакетный трафик (в этом случае их иногда называют генераторами пакетов). Для ознакомления с принципами генерации трафика в лабораторной работе предлагается использовать одно из таких решений Ostinato.

Ostinato представляет собой кроссплатформенный open-source генератор пакетного трафика с графическим пользовательским интерфейсом, построенный на базе клиент-серверной архитектуры. Данный генератор позволяет передавать данные несколькими потоками и имеет широкие возможности для настройки поведения трафика и различных опций используемых сетевых протоколов. Генератор трафика Ostinato предустановлен на компьютере. Для начала работы с генератором запустите Ostinato из терминала с правами суперпользователя:

```
root@mnlin# ostinato&
```

Повышенные привилегии необходимы для получения доступа к сетевым устройствам компьютера.

Основной интерфейс программы разделен на три окна (рисунок 11.1): порты (portslist), потоки (streamlist) и статистика (statistics).

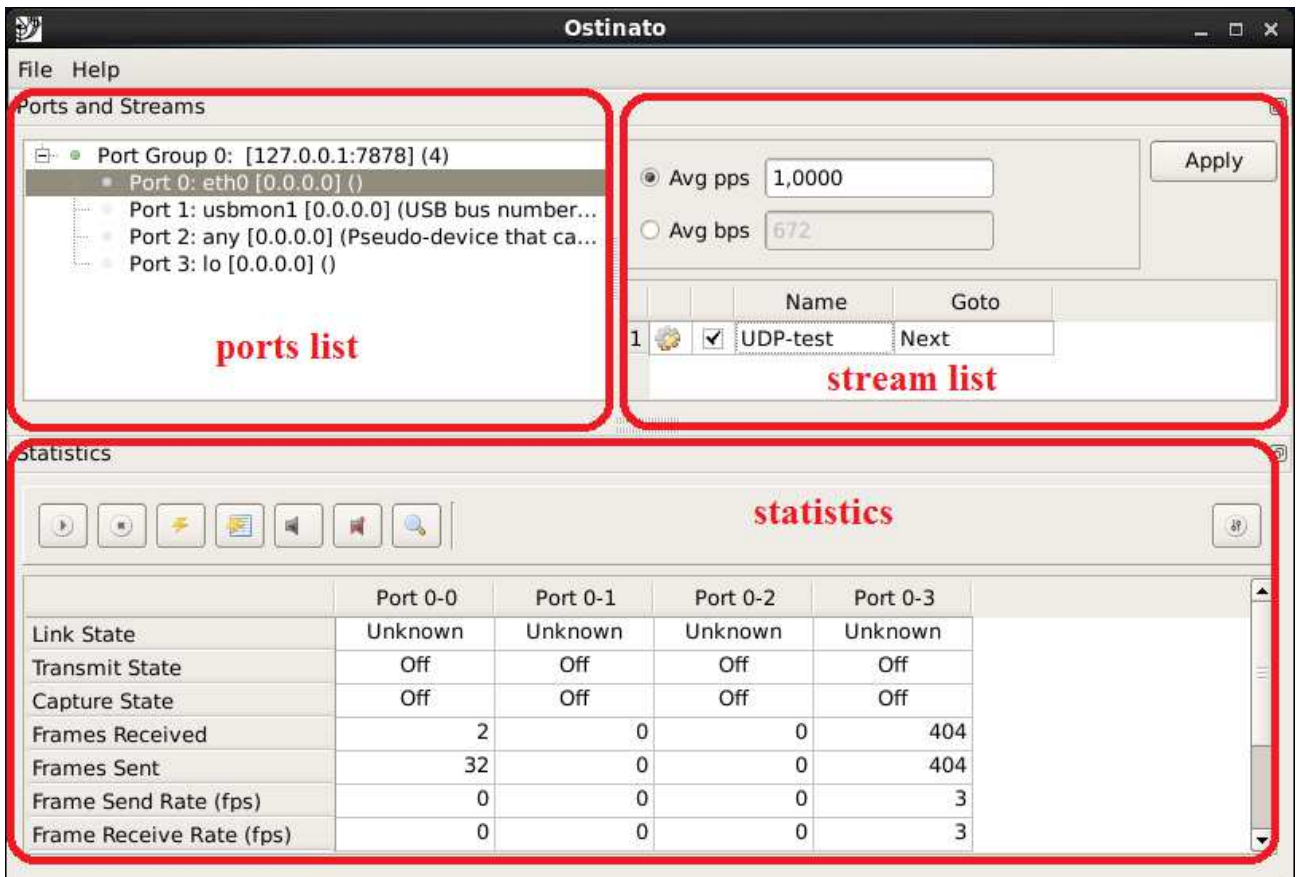


Рисунок 11.1 – Интерфейс Ostinato

В окне портов представлена группа портов [127.0.0.1] и зеленый индикатор напротив нее, что обозначает доступность группы портов. Ostinato является клиентским приложением и может работать с несколькими различными серверами (Drone). В данном случае клиент и сервер расположены на одном компьютере и обмениваются данными через сокет 127.0.0.1:7878.

Открыв группу портов (нажав на +) можно увидеть все доступные на данной машине порты. Выберите порт, с которого будет производиться отправка пакетов в сеть. Нажатием правой кнопки мыши в окне потоков откройте меню и создайте новый поток (newstream). Дважды кликнув на значке созданного потока, вы получите доступ к конфигуратору потока.

На первой вкладке Protocol Selection (рисунок 11.2) конструируйте будущий пакет в соответствии с моделью OSI. На рисунке 11.2 необходимые пункты помечены красным.

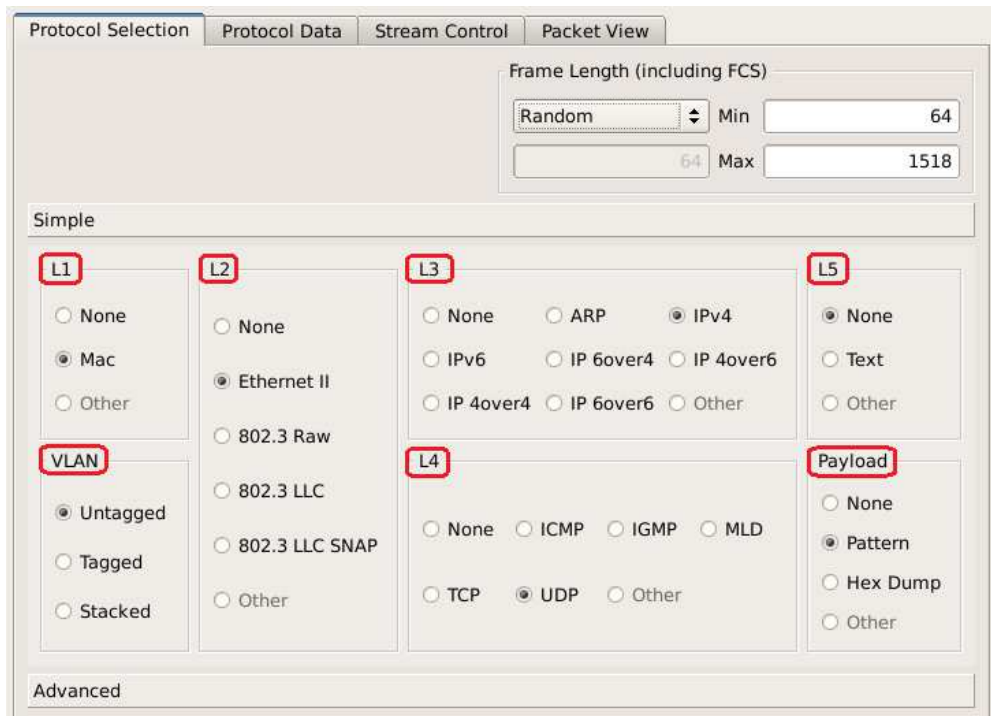


Рисунок 11.2 – Вкладка ProtocolSelection

Вкладка Protocol Data (рисунок 11.3) позволяет настроить некоторые специфичные поля выбранных протоколов, такие как, например, адреса источника и получателя в протоколе IP, порты в UDP и т.п.

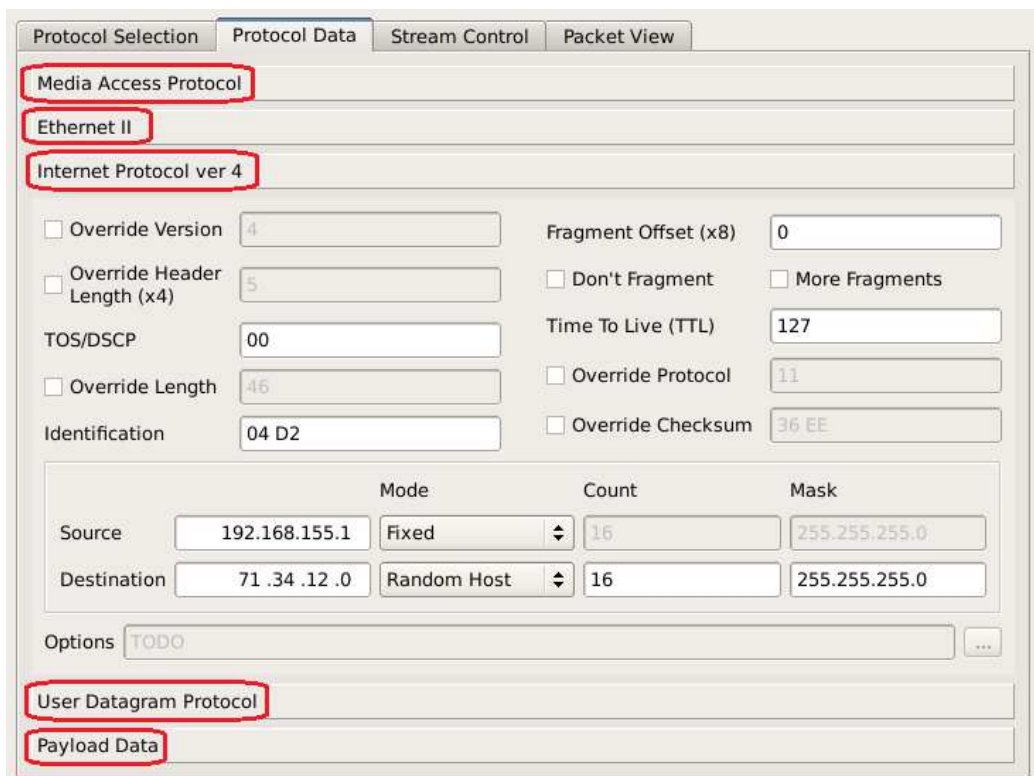


Рисунок 11.3 – Вкладка ProtocolData

Примечание: при конструировании пакета в реальной сети задавайте реальный MAC-адрес назначения в поле Media Access Protocol!

На вкладке Stream Control (рисунок 11.4) выставляются опции потока. Например, можно настроить генерацию трафика пачками или отдельными пакетами, количество пакетов в секунду/битовую скорость потока, поведение потока и т.д.

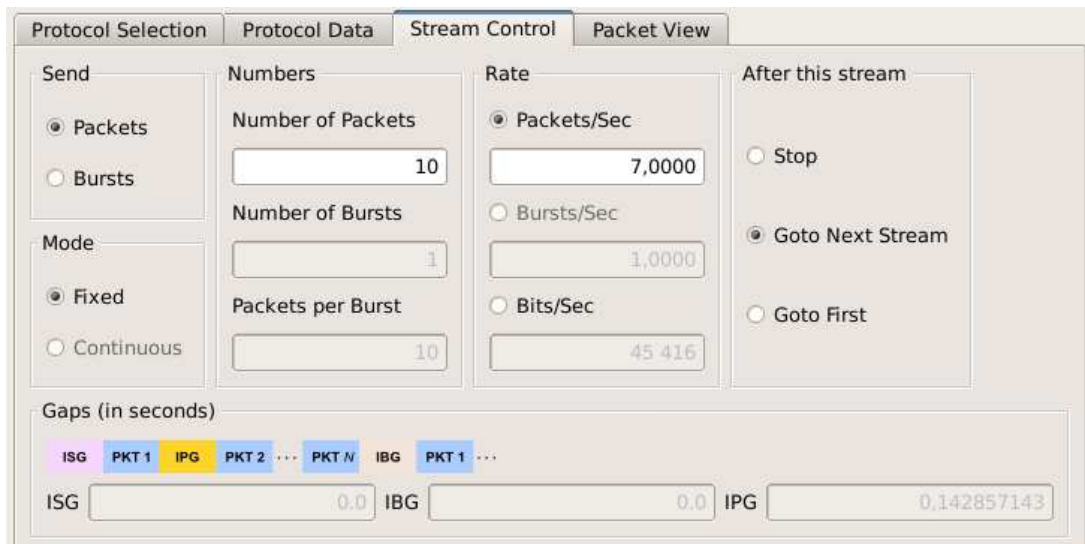


Рисунок 11.4 – Вкладка StreamControl

Создав несколько различных потоков для данного порта и выставив для каждого из них опцию GotoNextStream в поле Afterthisstream, можно организовать последовательную передачу этих потоков в сеть.

Также возможно организовать одновременную смешанную передачу. Для этого необходимо в окне портов выбрать требуемый, правой кнопкой мыши открыть контекстное меню и в пункте PortConfiguration изменить режим работы передачи порта на InterleavedStreams (смешанные потоки). Теперь все созданные для данного порта потоки будут передаваться на сетевой интерфейс одновременно (рисунок 11.5).



Рисунок 11.5 – Перевод порта в смешанный режим передачи

Примечание: В смешанном режиме вместо количества передаваемых пакетов указывается скорость передачи пакетов/пачек или битовая скорость потока. Соответственно, передача трафика будет продолжаться до тех пор, пока не будет остановлена нажатием кнопки StopTx.

Вкладка PacketView позволяет просмотреть получившийся пакет в «собранном» виде (рисунок 11.6).

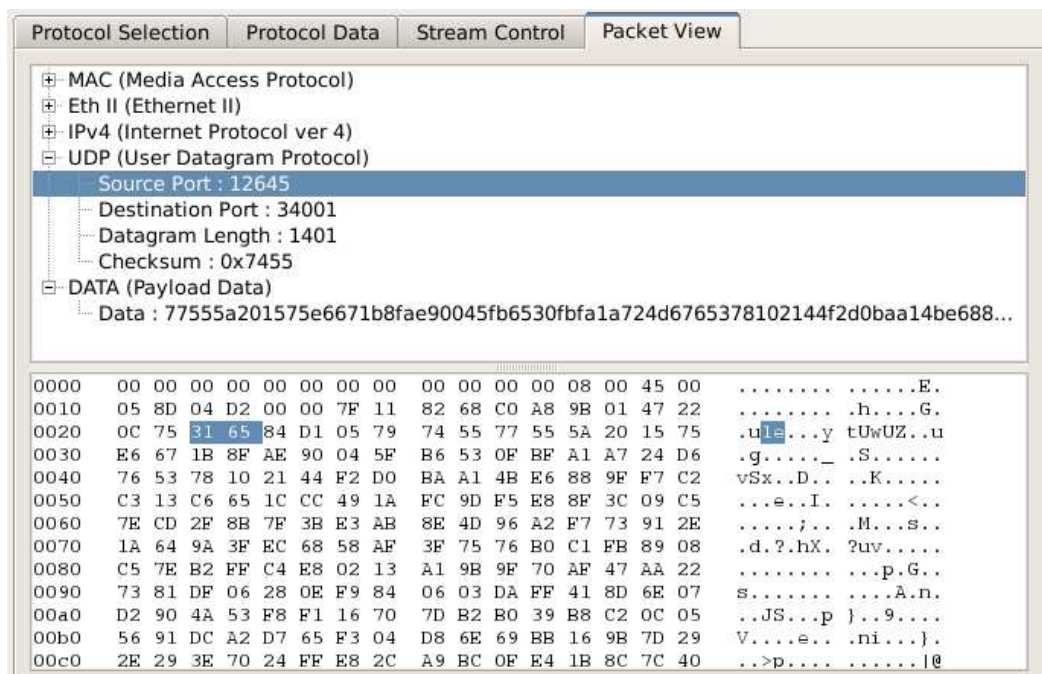


Рисунок 11.6 – Вкладка PacketView

После окончания настройки потока нажмите Ok и передайте изменения на сервер кнопкой Apply. Если этого не сделать,

генерирующий демон Drone не получит информацию о произошедших изменениях.

Для проверки работы генератора, предварительно запустите анализатор трафика Wireshark, настроив его на прослушивание того порта, на который вы передаете сгенерированный трафик. Теперь можно начинать генерацию (рисунок 11.7).

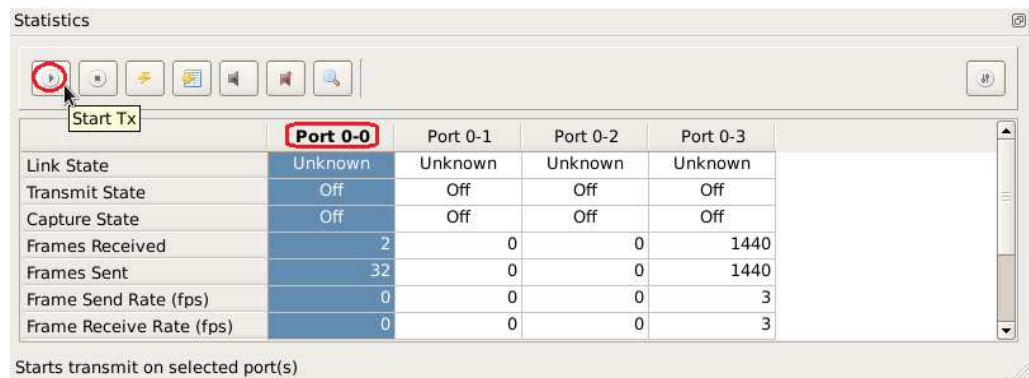


Рисунок 11.7 – Запуск генератора

В окне статистики выберите тот же порт, для которого вы конструировали поток (например, нажмите Port 0-0, если вы настроили PortGroup 0 и в ней Port 0) и кнопкой StartTx запустите генерацию трафика.

Качество подготовки к практическому занятию преподаватель оценивает по результатам собеседования, защиты отчета по практической работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной практической работе:

1) Какие основные принципы конструирования пакетов согласно модели TCP/IP, характеристики трафика пакетных сетей, процессы формирования потоков, принципы инкапсуляции?

2) Как использовать генератор трафика для создания потоков с различными характеристиками?

Алгоритм проведения практической работы:

1) Создайте 3 произвольных потока данных, состоящих из пакетов различных протоколов, заданных общим количеством пакетов и пакетной скоростью потока.

2) Создайте 3 произвольных потока данных, состоящих из пакетов различных протоколов, заданных числом пачек (bursts).

3) Запустите анализатор трафика Wireshark и начните захват на том порту, на котором предполагается генерировать трафик с помощью Ostinato.

4) Организуйте последовательную передачу сконструированных потоков в произвольном порядке. Сохраните полученный трэйс-файл.

5) Организуйте смешанную передачу (interleaved) сконструированных потоков трафика. Сохраните полученный трэйс-файл.

6) Изучив содержимое полученных трэйс-файлов, убедитесь в корректной работе генератора трафика. Используйте инструменты из меню Statistics:

- IOGraph;
- PacketLengths;
- ProtocolHierarchy.

Алгоритм обработки полученных данных:

1) Описать характеристики сконструированных потоков трафика согласно п. 1 и 2 задания, примеры полученных пакетов (см. на рисунке 11.6);

2) Зафиксировать трэйс-файлы, статистику работы согласно меню Statistics.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3 «МОНИТОРИНГ В СЕТЯХ СВЯЗИ: ПРОТОКОЛ ICMP, СПЕЦИАЛИЗИРОВАННЫЕ УТИЛИТЫ»

Цель занятия: овладение основными инструментами мониторинга сетей.

Задачи занятия:

- 1) Произвести анализ доступности удаленных узлов с использованием специализированных утилит;
- 2) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о стеках протоколов сетевого оборудования, методах измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации, видах политик управления доступом и информационными потоками в компьютерных сетях;
- формирование умений выбора режимов работы программно-аппаратных средств защиты информации в компьютерных сетях, проведения мониторинга функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
- формирование навыков определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях.

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой, подключенный в сеть Интернет.

План проведения практического занятия

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к практическому занятию:

1) RFC 792 Internet control message protocol. September, 1981.

2) RFC 950 Internet Standard Subnetting Procedure. August 1985

3) RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. March, 2006

4) RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations. September, 2000.

5) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

Краткая теоретическая справка для самостоятельной подготовки к практическому занятию:

Протокол ICMP (Internet Control Message Protocol) является протоколом сообщений об ошибках. Несмотря на то, что ICMP считается протоколом сетевого уровня, его сообщения инкапсулируются в IP. Сообщения ICMP довольно разнообразны, но имеют единый формат (рисунок 12.1). На этом протоколе базируются средства мониторинга сетей связи, а также сообщения о недоступности узла в некоторых протоколах прикладного уровня, например, ошибка 404 в HTTP.

Тип сообщения	Код сообщения	Контрольная сумма
Параметры		
Данные		

Тип сообщения – согласно классификации

Код сообщения – дополнительные сведения об ошибке

Параметры – например, IP-адрес узла

Данные – например, IP-заголовок и первые 64 бита пакета, переадресованного на другой узел.

Рисунок 12.1 – Формат сообщений ICMP

Протокол ICMP для IPv4 и его сообщения описаны в RFC 792, работа с масками сетей – в RFC 950. Протокол ICMP для IPv6 описан в RFC 4443.

Инструменты мониторинга утилиты ping и traceroute описаны в RFC 2529.

Утилита ping (Packet Internet Groper – одно из возможных прочтений) является одним из главных средств, используемых для отладки сетей, и служит для принудительного вызова ответа конкретной машины. Она позволяет проверять работу приложений ТСП/IP (по портам) на удаленных машинах, адреса устройств в локальной сети, адрес удаленного сетевого устройства. В выполнении команды ping участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы. Это утилита низкого уровня, которая не требует наличия серверных процессов на зондируемой машине, поэтому успешный результат при прохождении запроса вовсе не означает, что выполняются какие-либо сервисные программы высокого уровня, а говорит о том, что сеть находится в рабочем состоянии, питание зондируемой машины включено, и машина не отказала. Утилита ping входит во все реализации ТСП/IP независимо от операционной системы.

Получив эхо-запрос ping, программное обеспечение, реализующее протокол IP у адресата, посылает эхо-ответ. Эхо-запросы посылаются заданное количество раз (ключ -n) или по умолчанию до тех пор, пока пользователь не введет команду прерывания (Ctrl+C или Del), после чего выводятся статистические данные. В некоторых реализациях количество посылок эхо-запросов ограничено, например, в Windows их 4. В некоторых случаях можно в целях обеспечения безопасности (защита от DDOS-атак) выставить запрет на эхо-ответы. Список ключей и формат команды можно посмотреть самостоятельно, набрав в командной строке ping.

На практике большинство опций в формате команды можно опустить, тогда в командной строке может быть: ping имя_узла или ping IP-адрес.

Пример:

```
C:\Users\admin>ping yandex.ru
Обмен пакетами с yandex.ru [77.88.21.11] с 32 байтами данных:
Ответ от 77.88.21.11: число байт=32 время=1651мс TTL=57
Ответ от 77.88.21.11: число байт=32 время=154мс TTL=57
Ответ от 77.88.21.11: число байт=32 время=79мсTTL=57
Ответ от 77.88.21.11: число байт=32 время=77мс TTL=57
Статистика Ping для 77.88.21.11:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
```


(0% потерь)

Приблизительное время приема-передачи в мс:

Минимальное = 77мсек, Максимальное = 1651 мсек, Среднее = 490 мсек

Утилита `tracert` (в реализациях Windows используется название `tracert`) позволяет выявлять последовательность шлюзов, через которые проходит IP-пакет на пути к пункту своего назначения. У этой команды есть много опций, большинство из которых применяются крайне редко. Традиционно используется формат `tracert имя_узла`, которое может быть задано в символической или числовой форме. Выходная информация представляет собой список машин, начиная с первого шлюза и кончая пунктом назначения.

Принцип работы `tracert` основан на установке поля времени жизни (TTL) исходящего пакета таким образом, чтобы это время истекло до достижения пакетом пункта назначения. При получении пакета с обнуленным полем TTL текущий шлюз отправит сообщение об ошибке на машину-источник. Каждое приращение поля времени жизни позволяет пакету пройти на один шлюз дальше.

Утилита `tracert` посылает для каждого значения поля TTL три пакета. Если промежуточный шлюз распределяет трафик по нескольким маршрутам, то эти пакеты могут возвращаться разными машинами. Некоторые системы не посылают уведомлений о пакетах, время жизни которых истекло, а некоторые посылают уведомления, которые поступают обратно с задержкой, превышающей время ожидания на машине-источнике. Эти шлюзы обозначаются рядом звездочек. Если конкретный шлюз определить нельзя, все равно с помощью `tracert` можно увидеть следующие за ним узлы маршрута. Заметим, что в связи с использованием на сетях динамической маршрутизации, в разные моменты времени можно получить различные маршруты прохождения пакетов. Это также относится к зеркалированным узлам.

Пример:

```
admin@ddd:~$ traceroutelenta.ru
```

```
tracert to lenta.ru (81.19.85.92), 30 hops max, 60 byte packets
```

```
 1 172.24.255.254          (172.24.255.254)    13.218 ms 14.129 ms 14.019 ms
 2 84.204.14.254           (84.204.14.254)    13.848 ms 15.145 ms 15.040 ms
 3 46.47.255.33            (46.47.255.33)     13.910 ms 13.815 ms 14.594 ms
 4 mx960-spb.peterstar.net (82.196.95.169)    15.117 ms 25.568 ms 26.261 ms
```

```

5 ix-j-mx240.m9.ramtel.ru (193.232.244.118) 39.993 ms 39.870 ms 39.750 ms
6 s193-mx240.vr.rambler.ru (81.19.64.93) 39.672 ms 17.704 ms 19.828 ms
7 81.19.94.132 (81.19.94.132) 19.772 ms 19.708 ms 19.590 ms
8 81.19.85.92 (81.19.85.92) 19.529 ms 19.424 ms 28.634 ms

```

Пример:

```

C:\Users\admin>tracert yandex.ru
Трассировка маршрута к yandex.ru [87.250.251.11]с максимальным числом прыжков 30:
 1 100 ms104 ms 106 msHS2-1-16.xG.SPb.SkyLink.RU [89.253.1.16]
 2 119 ms 99 ms106 msHS2-0-1.xG.SPb.SkyLink.RU [89.253.0.1]
 3 107 ms 106 ms 106 ms 212.129.96.227
 4 112 ms 104 ms 106 ms aurora-spb-ix.yandex.net [194.226.100.90]
 5 128 ms198 ms 110 ms213.180.213.134
 6 * * * Превышен интервал ожидания для запроса.
 7 124 ms 108 ms 105 ms s650-eto2c1.yandex.net [213.180.213.65]
 8 121 ms 132 ms 133 ms l3-s550-s650.yandex.net [213.180.213.28]
 9 116 ms 106 ms 133 ms yandex.ru [87.250.251.11]
Трассировка завершена.

```

Существует комбинированная диагностическая утилита `mtr` (MyTraceroute), сочетающая в себе функциональность рассмотренных выше `tracert` и `ping`. Данная утилита основана на библиотеке `libncurses` (консольная версия) или на базе `GTK+` (оконная версия), позволяет в реальном времени отслеживать маршрут до заданного узла и изменяющееся время ответа каждого из промежуточных узлов, а также процент потерянных пакетов. Консольный вывод утилиты `mtr` представлен на рисунке 12.2. На данный момент `mtr` включена практически во все дистрибутивы Linux.

```

Файл Правка Вид Терминал Справка
My traceroute [v0.75]
happybook (0.0.0.0) Mon May 21 14:38:30 2012
Keys: Help Display mode Restart statistics Order of fields quit
          Packets
Host      Loss%  Snt   Last   Avg    Best  Wrst  StDev
1. 172.24.255.254 4.8%   63    1.7   16.4   1.7  185.0  35.9
2. 84.204.14.254 0.0%   63    3.3   13.6   2.7  147.5  25.9
3. 46.47.255.33 0.0%   63    4.5   11.9   2.5  142.6  23.0
4. mx960-1-298-spb-ru.xe-1-0-0-0.pe 3.2%   63    3.7   11.4   3.0  105.4  17.2
5. ix-j-mx240.m9.ramtel.ru 1.6%   63   19.7   26.5  15.8  179.2  24.8
6. s193-mx240-xe-1-3-0-811.vr.rambl 1.6%   63   19.7   29.3  15.8  155.1  28.4
7. 81.19.94.132 0.0%   63   19.6   29.0  16.3  193.2  28.4
8. 81.19.85.89 0.0%   63   17.9   31.5  15.8  311.6  41.7

```

Рисунок 12.2 – Пример работы утилиты `mtr` в консольном режиме

Утилита netstat выводит информацию о локальной сети и средствах ТСР/Р. Она реализована непосредственно в операционной системе и занимается сбором статистики об ошибках, текущих соединениях, состоянии портов и соединений. Содержание и форма выходной информации зависят от операционной системы, но обычно выводятся следующие данные: список соединений, статистика сетевых интерфейсов, статистика по буферам данных, содержание таблицы маршрутизации, статистика работы протоколов. Характер выводимой информации можно выбирать с помощью опций командной строки. Рассмотрим основные возможности мониторинга с помощью утилиты netstat.

Утилита netstat обладает набором ключей для отображения портов, находящихся в активном и/или пассивном состоянии. Таким образом, можно получить список всех серверных приложений, работающих на данном компьютере. Отметим, что формат списка соединений для сервера с системой NAT и для клиентской машины будет разным.

Информация выводится столбцами. В первом из них указан протокол, затем размеры очередей приема и передачи для установленного соединения на данной машине (на другом конце соединения размеры очередей могут быть другими), локальный и удаленный адреса и текущее состояние соединения.

Пример:

```
admin@ddd:~$ netstat -ta
```

Активные соединения с интернетом (servers and established)

```
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 *:29011 *: * LISTEN
tcp 0 0 localhost:ipp *: * LISTEN
tcp 0 0 172.24.0.157:35608 213.199.179.141:40041 ESTABLISHED
tcp 0 0 172.24.0.157:37760 163-247.static.quie:www TIME_WAIT
tcp 0 0 172.24.0.157:36441 95-28-49-237.broa:26647 ESTABLISHED
tcp 0 0 172.24.0.157:38541 172.24.0.170:55554 TIME_WAIT
tcp 0 0 172.24.0.157:54369 bos-w031b-rdr1.bl:https ESTABLISHED
tcp 0 0 172.24.0.157:38543 172.24.0.170:55554 TIME_WAIT
tcp 0 0 172.24.0.157:55651 broadband-95-84-1:17654 ESTABLISHED
tcp 0 0 172.24.0.157:43546 178.204.199.167:26639 ESTABLISHED
tcp 0 0 172.24.0.157:44763 agama.yande:xmpp-client ESTABLISHED
tcp 0 0 172.24.0.157:43715 chat-p01c-rdr1.bl:https ESTABLISHED
tcp 0 0 172.24.0.157:53870 broadband-109-173:20143 ESTABLISHED
tcp 0 0 172.24.0.157:43067 h178-129-218-223.d:8740 ESTABLISHED
tcp 0 0 172.24.0.157:53809 89.189.134.198.dy:22113 ESTABLISHED
tcp 0 0 172.24.0.157:44762 agama.yande:xmpp-client ESTABLISHED
tcp 0 0 172.24.0.157:53246 212.8.166.36:https ESTABLISHED
```

```

tcp 0 0 172.24.0.157:55257 bart-w04b.blue.ic:https ESTABLISHED
tcp 0 0 172.24.0.157:33021 dialin.customers.:26770 ESTABLISHED
tcp 0 0 172.24.0.157:58275 140.222.81.95.chtt:4078 ESTABLISHED
tcp 0 0 172.24.0.157:46402 91.190.216.24:12350 ESTABLISHED
tcp6 0 0 localhost:ipp      [::]:* LISTEN

```

Состояние соединения имеет значение только для протокола ТСР. Протокол UDP факта установления соединения не проверяет.

Каждое соединение машины с сетью называется сетевым интерфейсом. Машина, имеющая более одного интерфейса, может принимать данные по одному интерфейсу и передавать их по другому, осуществляя пересылку данных между сетями. Эта функция называется маршрутизацией, а машина, выполняющая ее – шлюзом.

Данные маршрутизации хранятся в так называемых таблицах маршрутизации, которые могут быть статическими и динамическими в зависимости от уровня сети и протокола маршрутизации. Для направления пакета по конкретному адресу подбирается наилучший маршрут согласно метрике. Если такой маршрут отсутствует, и нет маршрута по умолчанию, то отправителю возвращается сообщение об ошибке.

Утилита `netstat` -г позволяет отображать таблицу маршрутизации.

Пункты назначения и шлюзы могут показываться в виде имен машин или в виде их IP-адресов. Флаги даются для оценки маршрута.

Пример:

```

admin@ddd:~ > netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags           Ifac
ddd.sut.ru       *                255.255.255.255 UH              eth1
195.19.219.120   *                255.255.255.248 U                eth0
195.19.219.128   *                255.255.255.192 U                eth1
192.168.1.0      *                255.255.255.0   U                eth0
195.19.221.0     lgw.ccs.sut.ru   255.255.255.0   UG              eth1
193.125.0.0      lgw.ccs.sut.ru   255.255.0.0     UG              eth1
loopback         *                255.0.0.0       U                lo
default          lgw.ccs.sut.ru   0.0.0.0         UG              eth1

```

При использовании ключа `-e` на экран будут выведены статистические данные всех используемых Ethernet-интерфейсов. Исходя из них, можно выяснить, исправно ли соединение с сетью.

Пример:

```
admin@ddd:~ > netstat -e
Kernel Interface table
Iface MTU Met RX-OKRX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0 1000 0 844904 0 17 0 1454454 5 0 0 BRU
eth1 1500 0 590844 0 7 0 434438 59 0 0 BRU
lo 3924 0 45754 0 0 0 45754 0 0 0 LRU
```

Ошибки являются следствием проблем в кабельной системе или следствием неисправности платы сетевого адаптера. В нормально работающей сети количество конфликтов (RX-OVR, TX-OVR) не должно превышать 3% от числа пакетов, а другие ошибки не должны составлять более 0,5% от общего числа пакетов.

Использование netstat -спозволяет вывести содержимое счетчиков сетевых программ. В выходной информации есть разделы, относящиеся к различным протоколам: IP, ICMP, TCP, UDP. С ее помощью можно определить место появления ошибки в принятом пакете.

Пример:

```
admin@ddd:~$ netstat -s
```

Ip:

```
  всего пакетов принято 17058
    2 с неверными адресами
    0 перенаправлено
    0 входящих пакетов отклонено
  входящих пакетов доставлено: 4364
  запросов отправлено: 3936
```

Icmp:

```
  ICMP сообщений получено: 306
    неудачных входящих ICMP сообщений: 0
  Гистограмма входа ICMP
    пункт назначения недоступен: 8
    потери при прохождении: 263
    эхо-ответы: 35
      послано сообщений ICMP: 280
      неудачные сообщения ICMP: 0
  Гистограмма выхода ICMP
    пункт назначения недоступен: 8
    эхо-запросов: 14
```

IcmpMsg:

```
  InType0: 35
    InType3: 8
    InType11: 263
    OutType3: 8
    OutType8: 14
  OutType69: 258
```

Tcp:

открытия активных соединений: 148
 открытия пассивных соединений: 0
 неудачные попытки соединения: 4
 получено сбросов соединений: 2
 соединений установлено: 0
 сегментов получено: 3386
 отправлено сегментов: 2895
 повторно передано сегментов: 39
 плохих сегментов получено: 0
 сбросов послано: 8

Udp:

пакетов принято: 661
 принято пакетов на неизвестный порт: 8
 ошибок приема пакетов: 0
 пакетов послано: 723

UdpLite:

TcpExt:

пакеты, вырезанные из очереди приема по причине переполнения буфера сокета: 1
 67 TCP sockets finished time wait in fast timer
 задержанных подтверждений послано: 119
 Режим быстрого подтверждения приема был активирован 69 раз
 11 packets directly queued to recvmsg prequeue.
 3635 bytes directly received in process context from prequeue
 ожидаемых заголовков пакетов: 1745
 ожидаемых заголовков пакетов, непосредственно стоявших в очереди к пользователю: 5
 311 acknowledgments not containing data payload received
 ожидаемые подтверждения: 299
 9 congestion windows recovered without slow start after partial ack
 1 timeouts in loss state
 19 retransmits in slow start
 других TCP тайм-аутов: 19
 22 packets collapsed in receive queue due to low socket buffer
 получено DSACKs: 9
 1 соединения сброшены из-за неожиданных данных
 2 connections reset due to early user close
 TCPDSACKIgnoredNoUndo: 3
 TCPSackShiftFallback: 9

IpExt:

InMcastPkts: 15
 OutMcastPkts: 19
 InOctets: 4353792
 OutOctets: 405434
 InMcastOctets: 2714
 OutMcastOctets: 2990

Изучаемые в процессе выполнения лабораторной работы средства мониторинга относятся к универсальным в сетях IP. Они являются встроенными во все операционные системы с поддержкой

IP, работают как с IPv4, так и с IPv6. Для своей работы утилита netstat использует статистику, собранную при помощи ICMP. Так как ICMP для IPv4 и IPv6 имеет отличия, связанные непосредственно с изменением формата заголовка, то и результат для этих протоколов будет отличаться. Современные операционные системы поддерживают обе версии ICMP.

Качество подготовки к практическому занятию преподаватель оценивает по результатам собеседования, защиты отчета по практической работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной практической работе:

- 1) Какие основные принципы мониторинга сетей, характеристики сетей (TTL, время приема-передачи и т.п.)?
- 2) Какие принципы работы средств мониторинга (всех используемых в лабораторной работе утилит)?
- 3) Как использовать средства мониторинга IP-сетей?

Алгоритм проведения практической работы:

1) Провести трассировку трех узлов по заданию преподавателя. По результатам построить графики зависимости времени прохождения пакета от номера узла. Указать шлюзы перехода из одной сети в другую. Листинги трассировки привести в отчете.

2) Провести оценку работоспособности узлов: узлов в подсети лаборатории, шлюза подсети, 5 узлов из ранее сделанных трассировок. Оценить TTL для каждого из них.

3) Запустить несколько сетевых приложений на клиентской машине (например, несколько сайтов, интернет-мессенджер и т.п.). Снять с клиентской машины при помощи утилиты netstat таблицу маршрутизации, список соединений, статистику передачи данных, состояние интерфейса Ethernet. На основании списка соединений построить карту сети (смотри практическую работу №1). На основе таблицы маршрутизации зарисовать архитектуру сети.

Алгоритм обработки полученных данных:

Представить листинг работоспособности узлов, результаты трассировки, графики зависимости времени прохождения пакета от номера узла, статистику работы сети согласно netstat, карту сети, архитектуру сети на основе таблицы маршрутизации.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4 «ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ VPN»

Цель занятия: изучение технологии настройки и установки VPN- сервера для защиты информации.

Задачи занятия:

- 1) Настроить виртуальную частную сеть с использованием ПО SoftEtherVPN;
- 2) Составить отчет о выполненной работе, зафиксировав в нем производимые вами действия.

Планируемые результаты обучения:

- формирование знаний о принципах построения компьютерных сетей, стеке протоколов сетевого оборудования, составе типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
- формирование умений о выборе режимов работы программно-аппаратных средств защиты информации в компьютерных сетях;
- формирование навыков настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации.

Материально-техническое оборудование и материалы:

- 1) Персональный компьютер с операционной системой Windows или Linux (2 шт.).

План проведения практического занятия

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Рекомендуемая литература для подготовки к практическому занятию:

- 1) Соболев, Б. В. Сети и телекоммуникации [Текст]: учебное

пособие / Б. В. Соболев, М. С. Герасименко, А. А. Манин. – Москва: Феникс, 2015. – 191 с.

2) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2019. – 922 с.

3) Самуйлов, К. Е. Сети и телекоммуникации [Текст]: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – Москва: Юрайт, 2019. – 363 с.

Краткая теоретическая справка для самостоятельной подготовки к практическому занятию:

VPN (англ. Virtual Private Network – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений). В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть. SoftEther VPN Server позволяет легко и быстро развернуть VPN сервер на Windows. Это позволяет объединить различные устройства, сервера и компьютеры в одну сеть (виртуальную). При этом все эти устройства могут физически находиться где угодно в мире. В данной лабораторной работе рассмотрена установка и настройка SoftEther VPN Server на Windows. SoftEther VPN Server является freeware продуктом. Обычно VPN сервер используют для организации удалённого доступа в сеть предприятия из дома или других удалённых сетей (офисов) организации. Так же в эту сеть могут подключаться любые другие устройства которым разрешен доступ, например мобильный телефон. Т.е. можно с мобильного телефона войти на рабочий стол своего рабочего компьютера. Поэтому, часто, VPN сервер – это центральный узел, к которому

подключаются клиенты, чтобы получить доступ во внутреннюю сеть предприятия.

Качество подготовки к лабораторному занятию преподаватель оценивает по результатам собеседования, защиты отчета по лабораторной работе.

Примерные вопросы к собеседованию, к защите отчета по выполненной практической работе:

- 1) Что такое VPN? Для чего он используется?
- 2) Какие виды VPN соединений существуют? Для чего они применяются?
- 3) Какие порты использует SoftEtherServer для входящих подключений?

Алгоритм проведения практической работы:

Конфигурирование шлюза:

- 1) Переименуйте одну виртуальную машину в GATE или в Шлюз.
- 2) Переименуйте вторую виртуальную машину в Client или Клиент.
- 3) В виртуальной машине Шлюз установите две сетевые карты. Первой сетевой карте установите режим Внутренняя сеть и имя сети intnet2. Второй сетевой карте установите режим NAT.
- 4) Запустите виртуальную машину Шлюз.
- 5) Зайдите в настройки IP-адреса «Подключение по локальной сети» и установите IP-адрес 192.168.10.1 маска 255.255.255.0.
- 6) Зайдите в настройки IP-адреса «Подключение по локальной сети 2» и установите IP-адрес «получать IP-адрес автоматически» и «получить адрес DNS-сервера автоматически».
- 7) Отключите все профили брандмауэра, в случае использования ОС Windows.
- 8) С помощью команды ping проверьте доступность узлов 8.8.8.8 и ya.ru. Они должны быть доступны.

Конфигурирование клиента:

- 9) Проверьте, что на клиентской машине включен ОДИН сетевой адаптер и установлен режим «Внутренняя сеть».
- 10) Запустите ОС на клиентской машине.

11) Зайдите в настройки IP-адреса «Подключение по локальной сети» и установите IP-адрес 192.168.10.1 маска 255.255.255.0.

12) Отключите брандмауэр аналогично настройке шлюза

13) Проверьте связь со шлюзом (ping 192.168.10.1).

Установка VPN-Server:

14) Перейдите на виртуальную машину Шлюз.

15) Загрузите установочный дистрибутив SoftEther.

16) Запустите скачанный дистрибутив. На всех шагах установки нажимайте Далее и Да. На одном из шагов выберите SoftEther VPN Server.

17) После окончания установки запустится SoftEther VPNServer Manager – программа для конфигурирования VPN-серверов SoftEther. Если этого не произошло, запустите данную программу ярлыком на рабочем столе.

18) Выберите в списке localhost и нажмите Connect.

Базовая конфигурация VPN-сервера:

19) Если все выполнено верно, то сервер при первом соединении система предложит сменить пароль администратора. Введите 123 в оба поля и нажмите ОК.

20) Запустится мастер простой конфигурации VPN-сервера. На данном шаге предлагается выбрать режим работы VPN. Отметьте «RemoteAccessVPNServer» и нажмите ОК.

21) Нажмите ОК в окне подтверждения выбора настроек.

22) SoftEther объединяет настройки, относящиеся к одной конфигурации VPN. В диалоговом окне укажите название концентратора «VPN» и нажмите ОК.

23) Следующее окно – конфигурация IPSec. Нажмите ОК.

24) Следующее окно - Настройка VPN Azure Cloud, отметьте «DisableVPNAzure» и нажмите ОК.

25) Откроется новое окно. На данном этапе необходимо выбрать с какой внешней сетью будет коммутироваться соединение по VPN. Для этого в разделе «Step 3. SetLocalBridge» выберите «Подключение по локальной сети 2» (Сетевая карта в режиме NAT).

26) Нажмите CreateUsers для добавления пользователя. Укажите имя пользователя user1, выберите способ аутентификации PasswordAuthentication и задайте пароль 123. Нажмите кнопку ОК для сохранения.

27) Откроется окно управления пользователями. Поскольку пользователь добавлен, то нажмите Exit, чтобы закрыть окно.

28) В результате, увидите главное окно программы. Если все выполнено верно, в списке VirtualHubName должна быть одна строка VPN со статусом Online.

Настройка NAT и DHCP:

29) В главном окне программы, выделите VPN в списке Virtual Hub Name и нажмите Manage Virtual Hub (Управление виртуальным хабом)

30) Откроется окно Management of Virtual Hub. В этом окне можно отредактировать настройки текущего VPN сервера. Поэкспериментируйте с различными пунктами настроек. После нажмите кнопку «Virtual NAT and Virtual DHCP Server». В главном окне программы, выделите VPN в списке Virtual Hub Name и нажмите ManageVirtualHub (Управление виртуальным концентратором).

31) Откроется окно Management of Virtual Hub. В этом окне отредактируйте настройки текущего VPN сервера. Поэкспериментируйте с различными пунктами настроек. Нажмите кнопку «VirtualNATandVirtualDHCPSTerver» откроется окно.

32) В данном окне Включается, отключается и конфигурируется NAT и встроенный DHCP-сервер. Нажмите кнопку SecureNATConfiguration для просмотра настроек NAT и DHCP.

33) В открывшемся окне, определите: какие заданы параметры виртуального хоста (ip-адрес, маска), какие параметры заданы для DHCP сервера (диапазон адресов, маска, срок аренды). Закройте окно кнопкой ОК.

34) Вернитесь к предыдущему окну нажмите EnableSecureNAT для включения NAT и DHCP-сервера. При этом может появиться окно с подтверждением действия. Нажмите ОК.

Установка VPN- клиента:

35) Перейдите на виртуальную машину Клиент.

36) Загрузите установочный дистрибутив.

37) Запустите скачанный дистрибутив. На всех шагах установки нажимайте Далее и Да. На одном из шагов выберите SoftEther VPN Client.

38) После установки запустится SoftEther VPN Client Manager. Это система управления VPN-соединениями. Если приложение не запустилось, запустите его ярлыком в рабочего стола.

39) Далее необходимо добавить новый виртуальный VPN-адаптер. Это виртуальная сетевая карта, через которую устанавливается VPN-соединение. Для этого нажмите правой кнопкой мыши в нижней части окна и выберите «NewVirtualNetwork Adapter».

40) Укажите название нового адаптера «VPN».

41) В нижней части главного окна Client Manager должен появиться новый адаптер.

42) Теперь необходимо создать VPN подключение. Для этого нажмите правой кнопкой мыши на Add VPNConnection и выберите «NewVPNConnection».

43) Откроется окно конфигурации VPN-соединения. Задайте IP-адрес VPN-сервера (192.168.10.1) порт 443. Так же укажите имя пользователя user1 пароль 123 и способ аутентификации StandartPasswordAuthentification. Нажмите ОК для закрытия окна.

44) В главном окне программы нажмите правой кнопкой на созданное подключение и кликните на пункт Connect. Надпись в столбце статус должна поменяться на Connected.

45) Запустите на Клиенте браузер и перейдите по адресу <https://yandex.ru> если все сделано правильно, сайт откроется.

Алгоритм обработки полученных данных:

Каждую итерацию задания подтвердить скриншотом (-ами).

ФОРМА ОТЧЕТА ОБУЧАЮЩЕГОСЯ О ВЫПОЛНЕННОЙ ЛАБОРАТОРНОЙ/ПРАКТИЧЕСКОЙ РАБОТЕ

Отчёт должен быть оформлен с помощью редактора MS Word, версии 97 и выше или LibreOffice(.doc, .rtf).

Параметры страницы:

- верхнее поле – 2 см;
- нижнее поле – 2 см;
- левое поле – 2 см;
- правое поле – 1 см;
- переплет – 0 см;
- размер бумаги – А4;
- различать колонтитулы первой страницы.

Шрифт текста Times New Roman, 14 пунктов, через 1,5 интервала, выравнивание по ширине, первая строка с отступом 1,5 см. Номер страницы внизу, по центру, 14 пунктов.

Несложные формулы должны быть набраны с клавиатуры и с использованием команды «Вставка→Символ». Сложные формулы должны быть набраны в редакторе «MathType 6.0 Equation».

Отчёт обучающегося о выполненной лабораторной/практической работе должен содержать:

- название дисциплины, номер и название лабораторной работы;
- фамилию и инициалы автора, номер группы;
- фамилию и инициалы преподавателя;
- дату выполнения и личную подпись;
- цель занятия;
- материально-техническое оборудование и материалы;
- последовательность действий проведения исследований;
- вывод о проделанной работе.

Форма титульного листа отчета представлена в приложении А.

Результаты различных измерений необходимо представить в виде нескольких самостоятельных таблиц и графиков. Каждая таблица и каждый график должны иметь свой заголовок и исходные данные эксперимента.

При выполнении численных расчетов надо записать формулу определяемой величины, сделать соответствующую численную подстановку и произвести вычисления.

ШКАЛА ОЦЕНИВАНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ВЫПОЛНЕННОЙ ЛАБОРАТОРНОЙ/ПРАКТИЧЕСКОЙ РАБОТЫ

Оценка «отлично» выставляется слушателю, если лабораторная/практическая работа выполнена правильно, в установленное преподавателем время или с опережением времени, при этом слушателем выбран наиболее эффективный способ выполнения задания.

Оценка «хорошо» выставляется слушателю, если лабораторная/практическая работа выполнена правильно, в установленное преподавателем время, типовым способом и допущено наличие несущественных недочетов.

Оценка «удовлетворительно» выставляется слушателю, если при выполнении лабораторной/практической работы допущены ошибки некритического характера и (или) превышено установленное преподавателем время.

Оценка «неудовлетворительно» выставляется слушателю, если лабораторная/практическая работа не выполнена или при его выполнении допущены грубые ошибки.

ЗАКЛЮЧЕНИЕ

По результатам выполнения лабораторных/практических работ студент формирует следующие компетенции:

ПК-2 Способен проектировать и разрабатывать интерфейсные модули сетевых узлов, создавать структурированные кабельные системы, в том числе для малых космических аппаратов, в части:

ПК-2.1 Контролирует соблюдение утвержденных проектных решений при подготовке исполнительной документации;

ПК-2.2 Уточняет проектную документацию и вносит изменения при изменении технических решений;

ПК-2.3 Разрабатывает исполнительную документацию в составе группы соисполнителей-смежников.

ПРИЛОЖЕНИЕ А

(обязательное)

**Форма титульного листа отчета обучающегося о выполненной
лабораторной/ практической работе****МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Юго-Западный государственный университет»

Кафедра космического приборостроения и систем связи

ОТЧЕТо выполненной лабораторной/практической работе
по дисциплине «Проектирование кабельных систем передачи»
на тему «_____»

Выполнил

(подпись)

/Фамилия, инициалы/

Проверил

(подпись)

/Фамилия, инициалы/

Курск 20__