Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. Р. Е. АЛЕКСЕЕВА»

(НГТУ)

Институт ИРИТ, Институт радиоэлектроники и информационных технологий

сокращенное и полное наименование института

Кафедра ИРС, кафедра «Информационные радиосистемы»

сокращенное и полное наименование кафедры

Методические рекомендации по организации практических занятий по дисциплине *«СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИ И»*

наименование дисциплины

Направление подготовки

11.04.01 Радиотехника

код и полное наименование направления подготовки (специальности)

Программа академической магистратуры

Системы цифровой обработки сигналов в радиолокации, связи и управлении

наименование программы

Уровень высшего образования

Магистратура

Форма обучения

очная

Нижний Новгород

2015

Разработчик (и)/составитель(и) методических рекомендаций по организации практических занятий по дисциплине
«*СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ*»:

к.т.н., Смирнова Д.М.

ученое звание, степень, фамилия, инициалы

Кафедра «Информационные радиосистемы»

Дата, подпись 28.09.2015

Методические рекомендации по организации практических занятий по дисциплине «*СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ*» рассмотрены на заседании кафедры

«Информационные радиосистемы»

наименование кафедры

Протокол № 2 от «12» октября 2015 г.

Заведующий кафедрой _____ профессор, д.т.н. Рындык А.Г.

ученое звание, степень фамилия, имя, отчество

Дата, подпись 12.10.2015 г.

Методические рекомендации по организации практических занятий по дисциплине «*СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ*» согласованы с председателем координационного совета по направлению подготовки 11.04.01 Радиотехника

профессор, д.т.н. Рындык А.Г. 12.10.2015

ученое звание, степень, фамилия, инициалы дата, подпись

Методические рекомендации по организации практических занятий по дисциплине «*СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ*» утверждены Ученым советом образовательно-научного института «Институт радиоэлектроники и информационных технологий»

Протокол № 2 от «27» октября 2015г.

Методические рекомендации зарегистрированы в методическом отделе под учетным номером 294

Ведущий инженер Кулева Ж.А. 28.01.2016

ВВЕДЕНИЕ

Методические указания по организации практических занятий по дисциплине «Сетевые информационные технологии» предназначены для магистрантов второго курса, обучающихся по направлению 11.04.01 «Радиотехника», и содержат рекомендации для проведения практических занятий по курсу «Сетевые информационные технологии».

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории, направленное на углубление научно-теоретических знаний и овладение определенными методами самостоятельной работы, которое формирует практические умения (вычислений, расчетов, использования таблиц, справочников и др.). В процессе занятия студенты по заданию и под руководством преподавателя выполняют одну или несколько практических работ.

Цель методических указаний: помочь студентам при изучении учебной программы с использованием лекционных материалов и рекомендуемой учебно-методической литературы при формировании необходимых компетенций для исследования, проектирования коммуникационных сетей и последующего управления сетью.

Подготовка студентов к практическому занятию проводится в часы самостоятельной работы с использованием учебников, конспектов лекций и учебно-методических материалов.

В процессе выполнения практических заданий по дисциплине «Сетевые информационные технологии» студент должен:

– строго выполнять весь объем самостоятельной подготовки, указанный в описаниях соответствующих практических работ;

– знать, что выполнению каждой работы предшествует проверка готовности студента, которая проводится преподавателем;

– знать, что после выполнения работы студент должен представить отчет о проделанной работе с обсуждением полученных результатов и выводов.

В процессе выполнения практических работ по данной дисциплине студент формирует и демонстрирует следующие общепрофессиональные и профессиональные компетенции: ОПК-1, ОПК-2, ПК-2, ПК-3.

После выполнения практических заданий студент должен знать основные принципы и правила адресация сетевых устройств, правила конфигурирования протоколов TCP/IP, основные принципы маршрутизации, правила организации таблиц маршрутизации, способы тестирования отдельных протоколов, проводить анализ сетевого трафика, должен уметь проверять функционирование сети, организовать сетевое взаимодействие приложений, управлять сетью.

Практическое занятие № 1
Адресация и маршрутизация в IP-сетях

Цель: изучение основ адресации и маршрутизации.

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

IP адрес

IP-адрес – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. В сети Интернет требуется глобальная уникальность адреса; в случае работы в локальной сети требуется уникальность адреса в пределах сети. В версии протокола IPv4 IP-адрес имеет длину 4 байта.

IP-адрес состоит из двух частей: номера сети и номера узла. В случае изолированной сети её адрес может быть выбран администратором из специально зарезервированных для таких сетей блоков адресов (10.0.0.0/8, 172.16.0.0/12 или 192.168.0.0/16). Если же сеть должна работать как составная часть Интернета, то адрес сети выдаётся провайдером либо региональным интернет-регистратором (RegionalInternetRegistry, RIR). Согласно данным на сайте IANA,[1] существует пять RIR: ARIN, обслуживающий Северную Америку, а также Багамы, Пуэрто-Рико и Ямайку; APNIC, обслуживающий страны Южной, Восточной и Юго-Восточной Азии, а также Австралии и Океании; AfriNIC, обслуживающий страны Африки; LACNIC, обслуживающий страны Южной Америки и бассейна Карибского моря; и RIPENCC, обслуживающий Европу, Центральную Азию, Ближний Восток. Региональные регистраторы получают номера автономных систем и большие блоки адресов у IANA, а затем выдают номера автономных систем и блоки адресов меньшего размера локальным интернет-регистраторам (LocalInternetRegistries, LIR), обычно являющимся крупными провайдерами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

ARP протокол

ARP (протокол разрешения адресов) – протокол в компьютерных сетях, предназначенный для определения MAC-адреса по известному IP-адресу.

Рассмотрим суть функционирования ARP на простом примере. Компьютер А (IP-адрес 10.0.0.1) и компьютер Б (IP-адрес 10.22.22.2) соединены сетью Ethernet. Компьютер А желает переслать пакет данных на компьютер Б, IP-адрес компьютера Б ему известен. Однако сеть Ethernet, которой они соединены, не работает с IP-адресами. Поэтому компьютеру А для осуществления передачи через Ethernet требуется узнать адрес компьютера Б в сети Ethernet (MAC-адрес в терминах Ethernet). Для этой задачи и используется протокол ARP. По этому протоколу компьютер А отправляет широковещательный запрос, адресованный всем компьютерам в одном с ним широковещательном домене. Суть запроса: «компьютер с IP-адресом 10.22.22.2, сообщите свой MAC-адрес компьютеру с IP-адресом 10.0.0.1». Сеть Ethernet доставляет

этот запрос всем устройствам в том же сегменте Ethernet, в том числе и компьютеру Б. Компьютер Б отвечает компьютеру А на запрос и сообщает свой MAC-адрес (напр. 00:ea:d1:11:f1:11) Теперь, получив MAC-адрес компьютера Б, компьютер А может передавать ему любые данные через сеть Ethernet.

Наибольшее распространение ARP получил благодаря повсеместности сетей IP, построенных поверх Ethernet, поскольку практически в 100 % случаев при таком сочетании используется ARP. В семействе протоколов IPv6 ARP не существует, его функции возложены на ICMPv6.

Маршрутизация по умолчанию

Шлюз по умолчанию, шлюз последней надежды (англ. Lasthopegateway) – в маршрутизируемых протоколах это сетевой шлюз, на который отправляется трафик, для которого невозможно определить маршрут исходя из таблиц маршрутизации. Применяется в сетях с хорошо выраженными центральными маршрутизаторами, в малых сетях, в клиентских сегментах сетей. Шлюз по умолчанию задаётся записью в таблице маршрутизации вида «сеть 0.0.0.0 с маской сети 0.0.0.0».

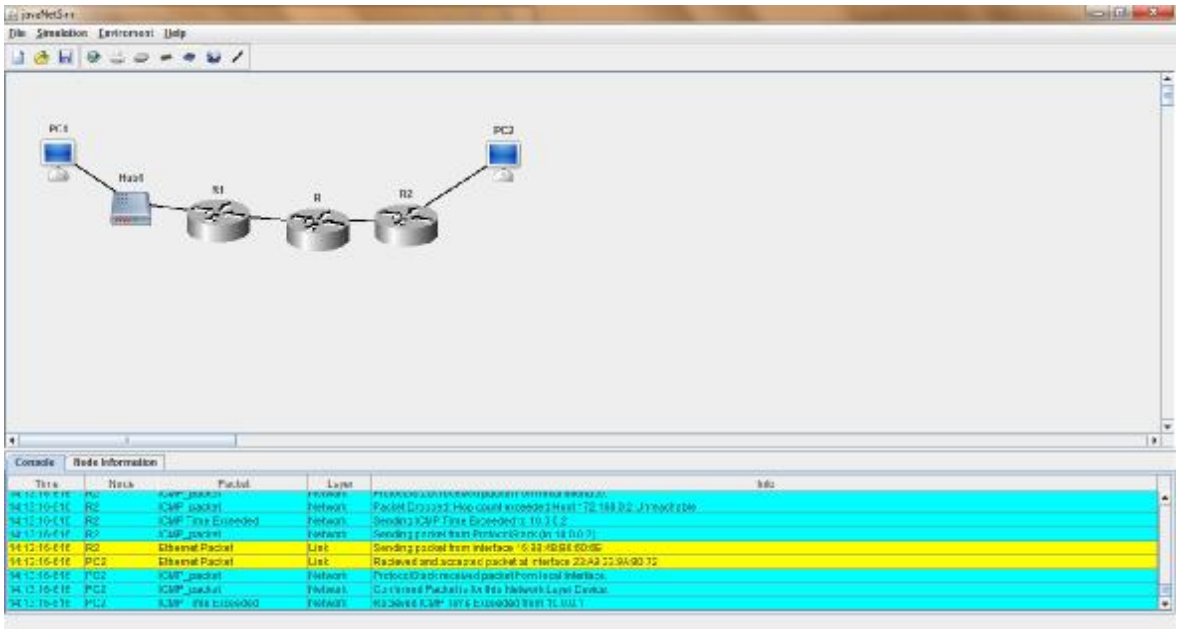
На компьютерах конечных пользователей за маршрутизацию пакетов отвечают совсем другие машины. Поэтому таблица маршрутизации у них крайне проста и, как правило, состоит из адреса 127.0.0.1 (Обратная петля), адреса локальной сети (или её сегмента, в котором рабочая станция находится) и шлюза по умолчанию, на который перенаправляется весь остальной трафик.

На маршрутизаторах шлюз по умолчанию позволяет упростить координацию трафика, направляя его на центральные маршрутизаторы. Если «центральных» маршрутизаторов несколько, шлюз по умолчанию может и не указываться. В этом случае при попытке отправить пакет в сеть, для которой нет маршрута, в консоль будет возвращаться сообщение noroutetohost, а отправителю - ICMP сообщение вида "узел недостижим".

ICMP протокол

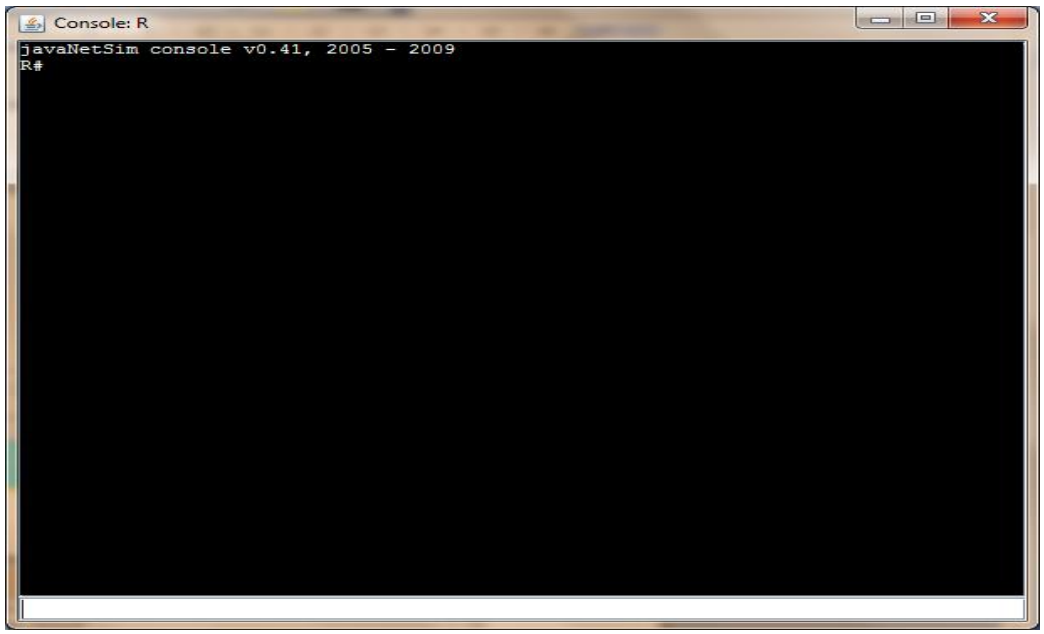
ICMP – сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

Ошибка при выполнении команды ping 172.168.0.2 с компьютера 10.0.0.2

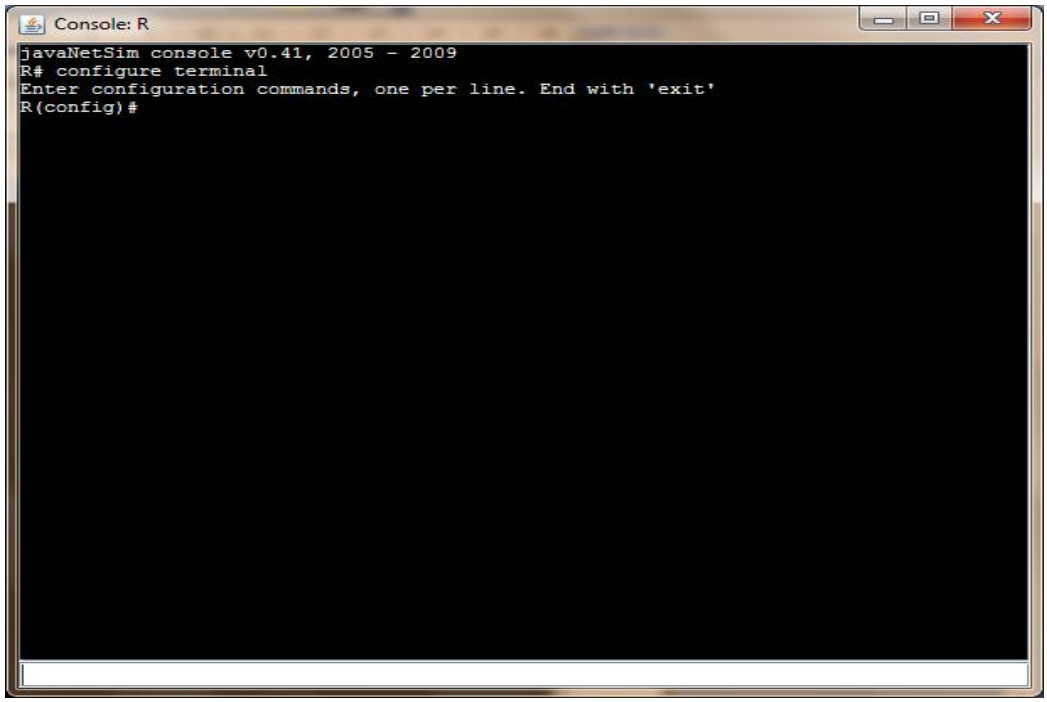


Настройка маршрутизатора R

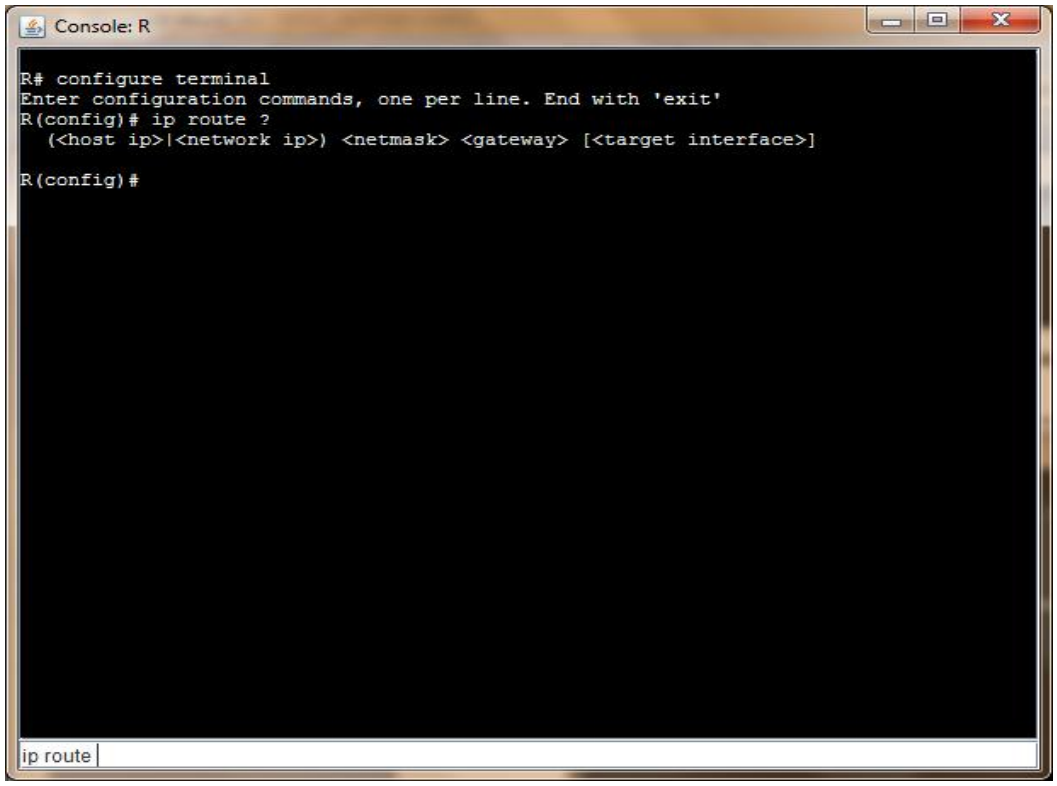
Кликнув правой кнопкой мыши по изображению маршрутизатора, выбрать пункт меню «Console», после чего откроется диалоговое окно:



В нижней строке необходимо набрать команду «configure terminal», в результате чего будет запущен режим конфигурирования роутера:

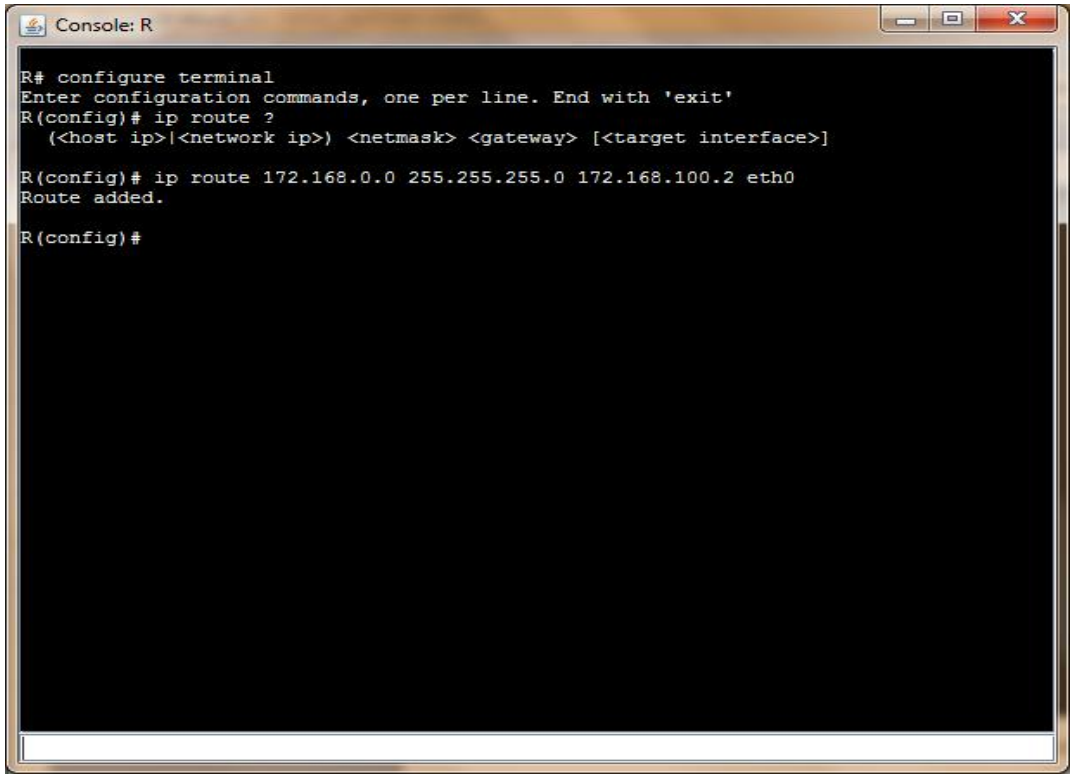


Добавление маршрута путем указания в строке «ip route»:

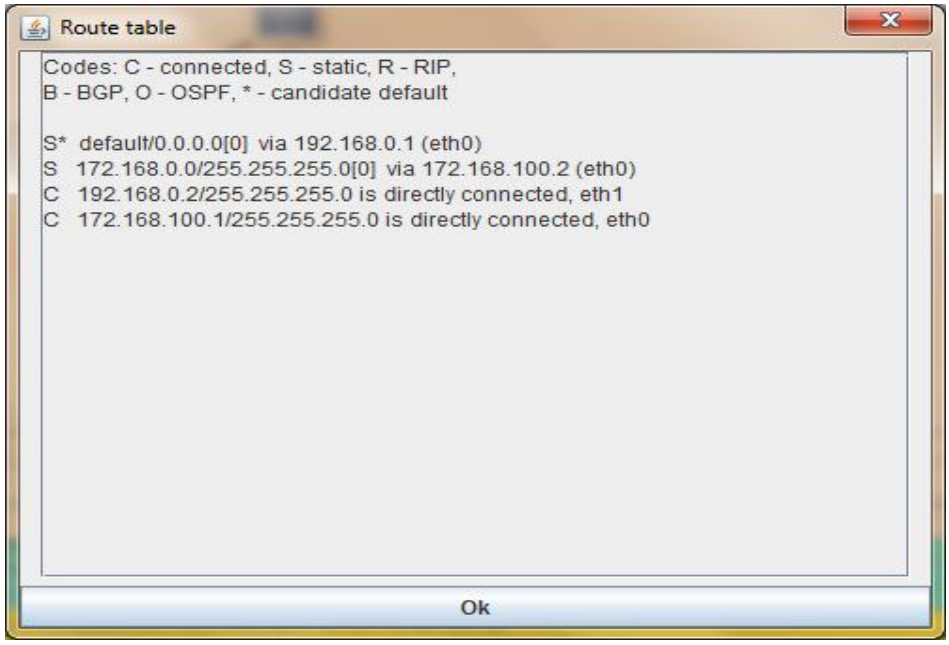


Добавление маршрута:

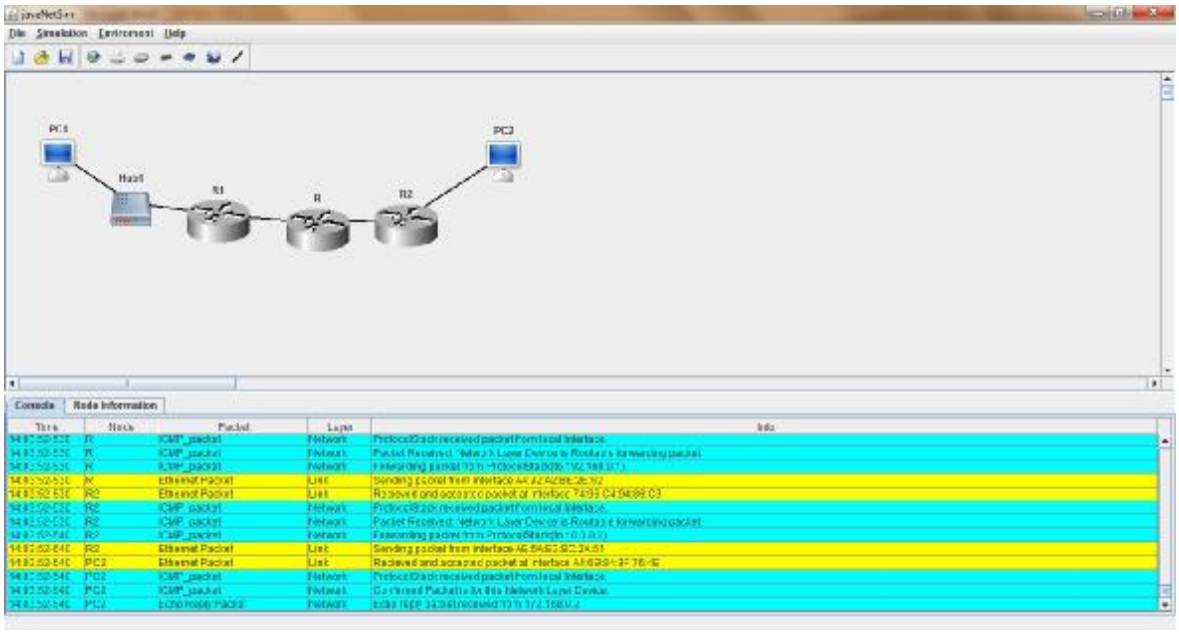
172.168.0.0 255.255.255.0 172.168.100.2 eth0



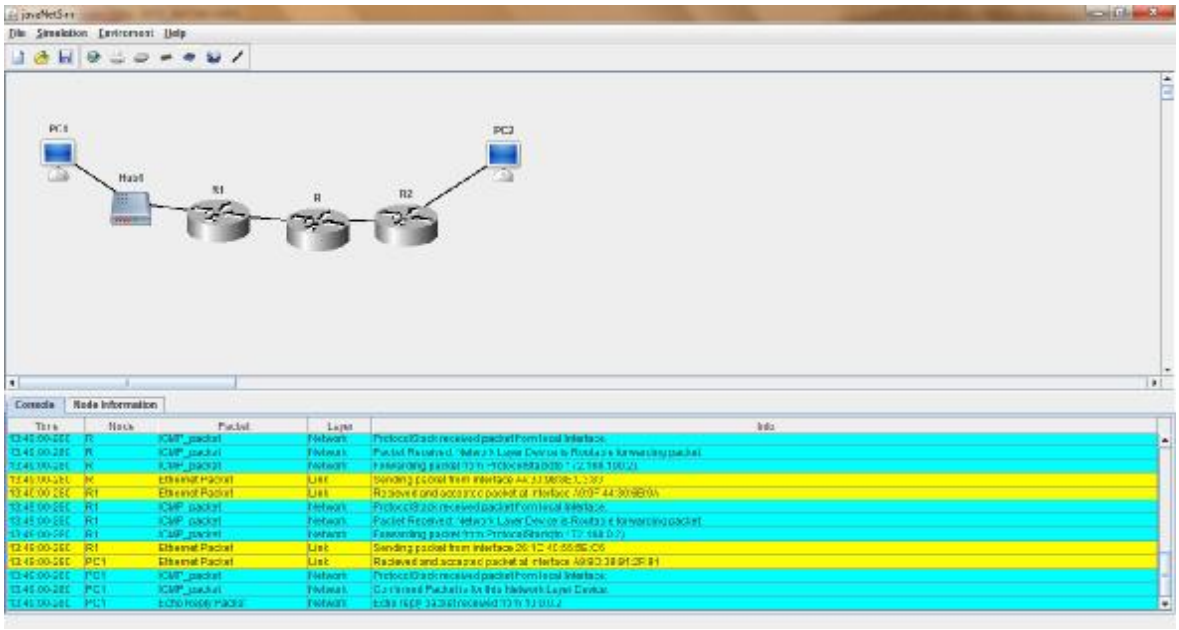
Вид таблицы маршрутизации после добавления нового маршрута:



Результат выполнения утилиты «Ping» с адресом 172.168.0.2



Результат выполнения утилиты «Ping» с адресом 10.0.0.2



ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В соответствии со своим вариантом задания научиться проверять работоспособность сети, управлять её конфигурацией.

Подготовка к работе

Изучите теоретическую часть по данной теме. Ознакомьтесь с заданием на лабораторную работу, определяемым преподавателем.

Выполнение работы

Используя программу JavaNetSim (http://sourceforge.net/projects/javanetsim/), выполните следующие задания:

1. Исправить структуру сети (если это необходимо), обеспечив корректную доставку кадров на физическом уровне.

2. Задать ip-адреса, маски подсети и шлюзы по умолчанию для всех узлов сети, чтобы обеспечить корректную доставку эхо-запроса от K1 к K2 и эхо-ответа обратно. Обосновать свои установки.

3. Выполнить эхо-запрос с K1 на K2. Посмотреть вывод программы.

4. Добавить статическую запись ARP для K3 на K1. Подождать устаревания ARP-таблиц и выполнить эхо-запрос с K1 на K2. Пояснить результат.

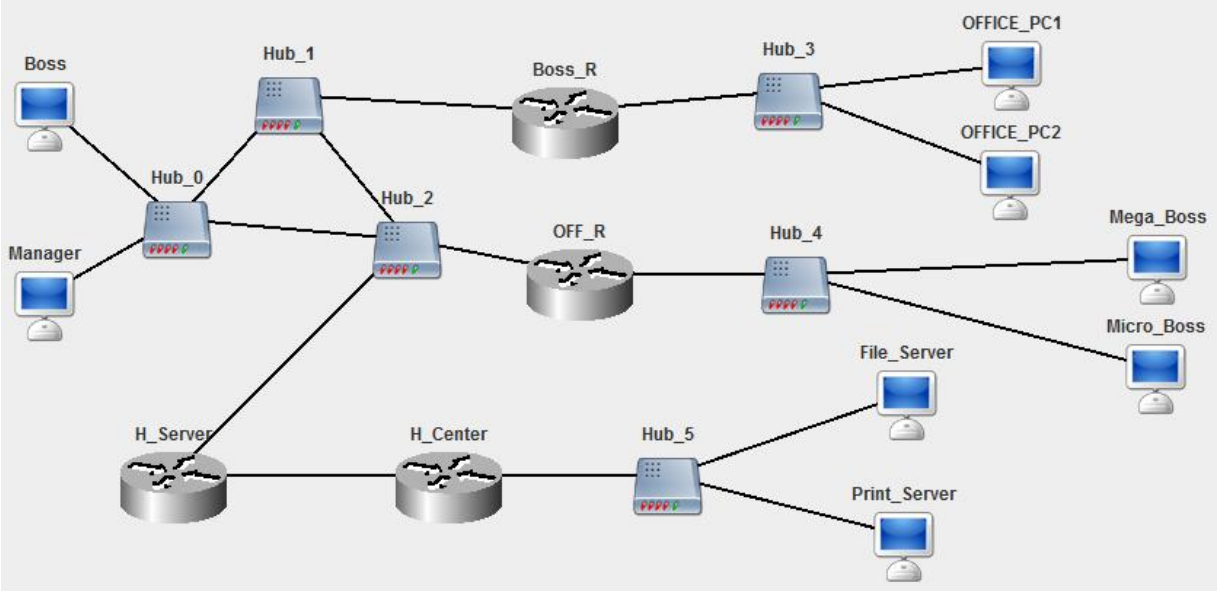
5. Выполнить эхо-запрос на IP-адрес 200.100.0.1 с K1. Пояснить результат работы программы.

6. Выполнить эхо-запросы с K1 и K2 на все узлы сети. Убедиться, что эхо-ответы приходят.

Продемонстрировать результат преподавателю и ответить на контрольные вопросы.

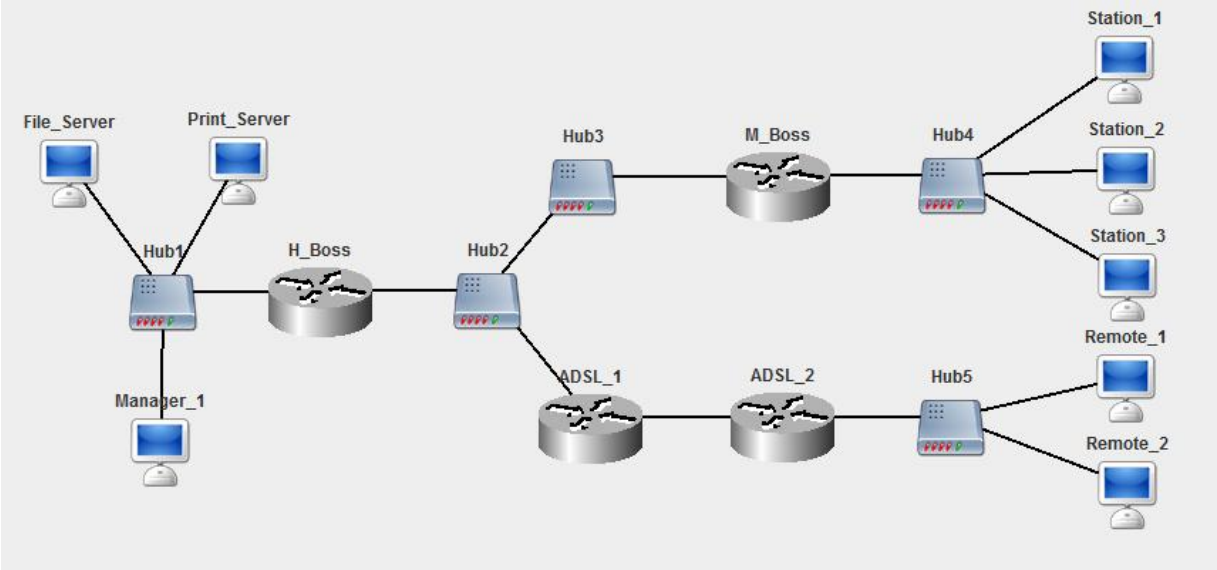
ВАРИАНТЫ ЗАДАНИЙ

Вариант № 1



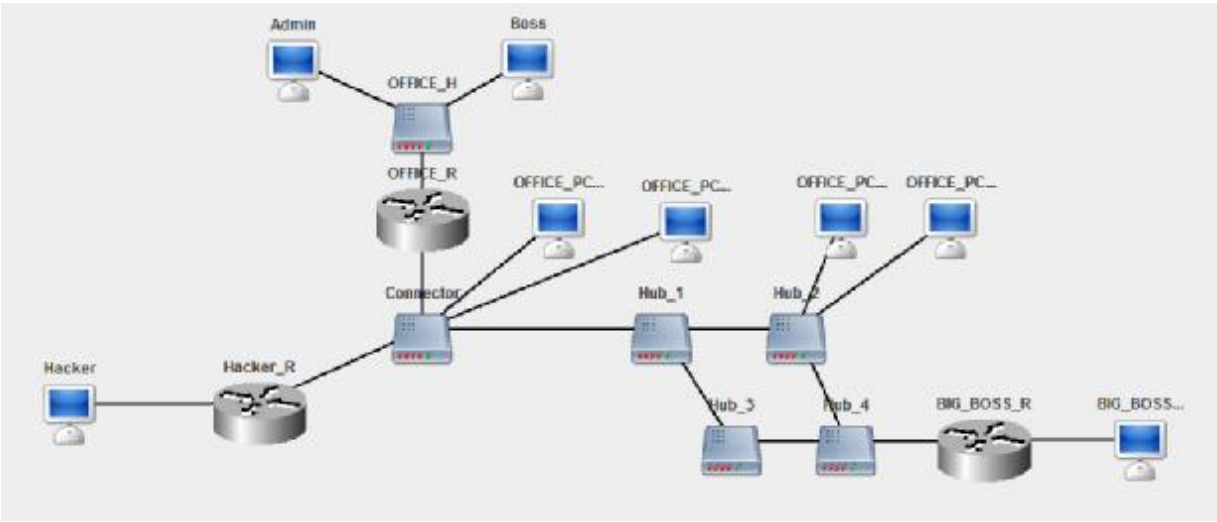
Сеть 1 между маршрутизаторами Boss_R, OFF_R и H_Server: 217.241.26.0
Сеть 2 между маршрутизаторами H_Server и H_Center: 117.168.0.0
Компьютер OFFICE_PC1 имеет IP-адрес: 164.157.125.1
Компьютер Mega_Boss имеет IP-адрес: 125.148.25.1
Компьютер File_Server имеет IP-адрес: 165.125.148.1
Обозначения в задании: K1-Boss, K2-Manager, K3-Print_Server

Вариант № 2



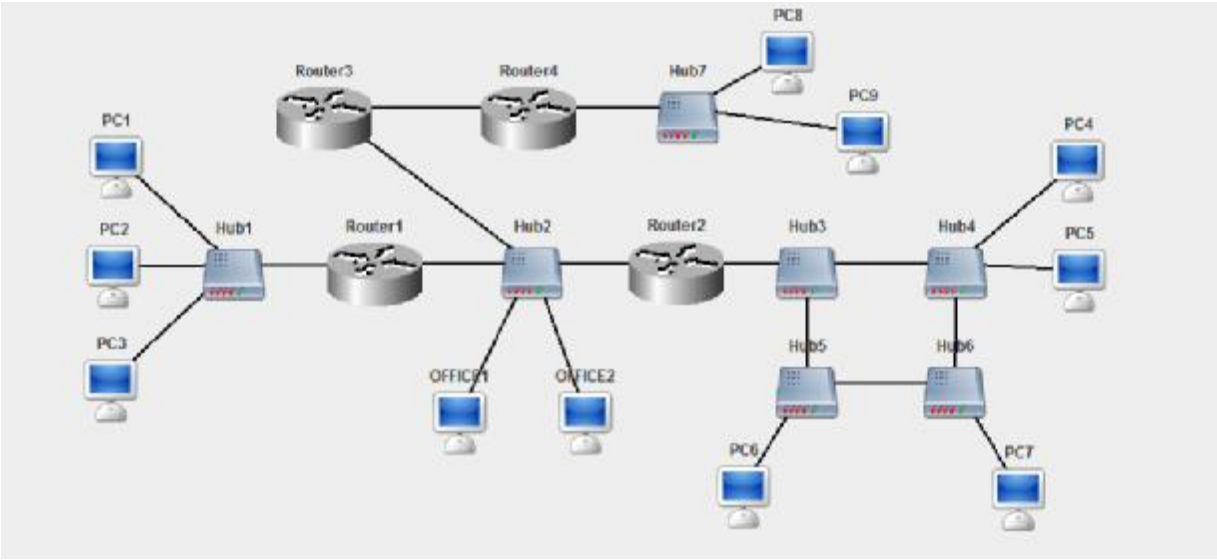
Сеть 1 между маршрутизаторами H_Boss, M_Boss, ADSL_1: 10.125.168.0
Сеть 2 между маршрутизаторами ADSL_1 и ADSL_2: 172.198.0.0
Компьютер File_Server имеет IP-адрес: 192.168.102.1
Компьютер Station_1 имеет IP-адрес: 172.145.85.1
Компьютер Remote_1 имеет IP-адрес: 10.124.125.1
Обозначения в задании: K1-File_Server, K2-MANAGER_1, K3-Station_1

Вариант № 3



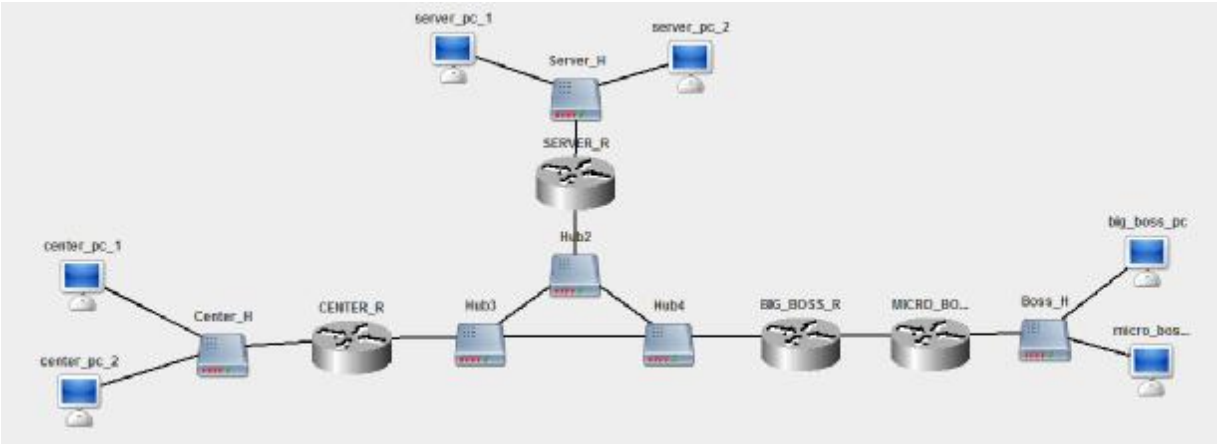
Сеть между маршрутизаторами Hacker_R, OFFICE_R, BIG_BOSS_R: 10.136.89.0
Компьютер Hacker имеет IP-адрес: 172.168.25.1
Компьютер Admin имеет IP-адрес: 168.147.86.1
Компьютер BIG_BOSS_PC имеет IP-адрес: 204.198.178.1
Обозначения в задании: K1-Admin, K2-Boss, K3-BIG_BOSS

Вариант № 4



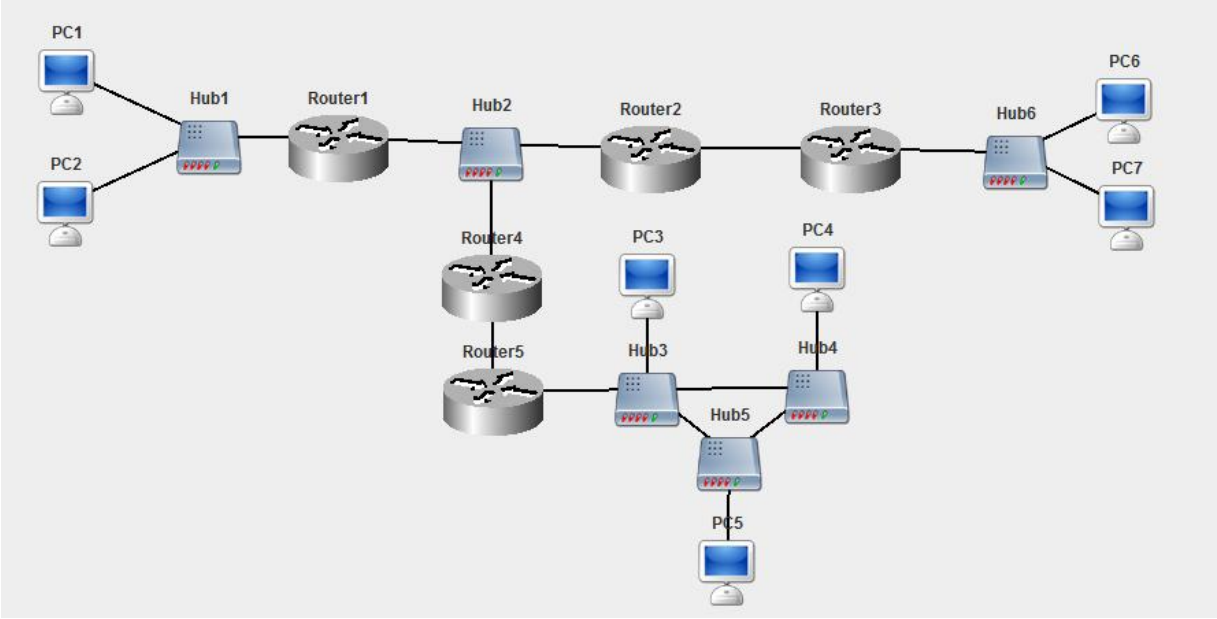
Сеть 1 между маршрутизаторами Router1, Router2 и Router3: 168.125.145.0
Сеть 2 между маршрутизаторами Router3 и Router4: 204.108.0.0
Компьютер PC1 имеет IP-адрес: 204.198.125.1
Компьютер PC8 имеет IP-адрес: 162.23.159.1
Компьютер PC4 имеет IP-адрес: 214.149.130.1
Обозначения в задании: K1-PC1, K2-PC2, K3-PC6

Вариант № 5



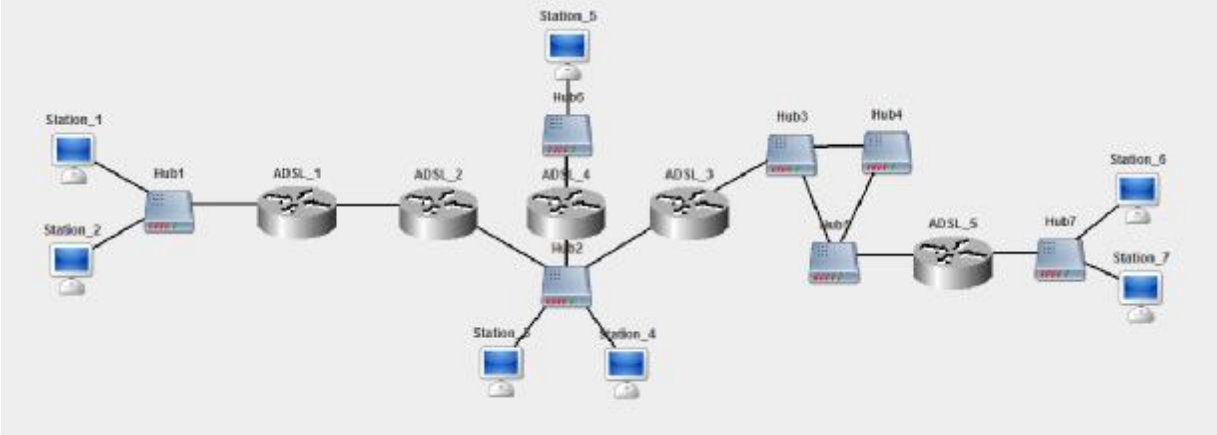
Сеть 1 между маршрутизаторами CENTER_R, SERVER_R и BIG_BOSS_R: 172.168.156.0
Сеть 2 между маршрутизаторами BIG_BOSS_R и MICRO_BOSS_R: 10.0.0.0
Компьютер center_pc_1 имеет IP-адрес: 204.198.175.1
Компьютер server_pc_1 имеет IP-адрес: 198.145.102.1
Компьютер big_boss_pc имеет IP-адрес: 214.148.25.1
Обозначения в задании: K1-center_pc_1, K2-center_pc_2, K3-big_boss_pc

Вариант № 6



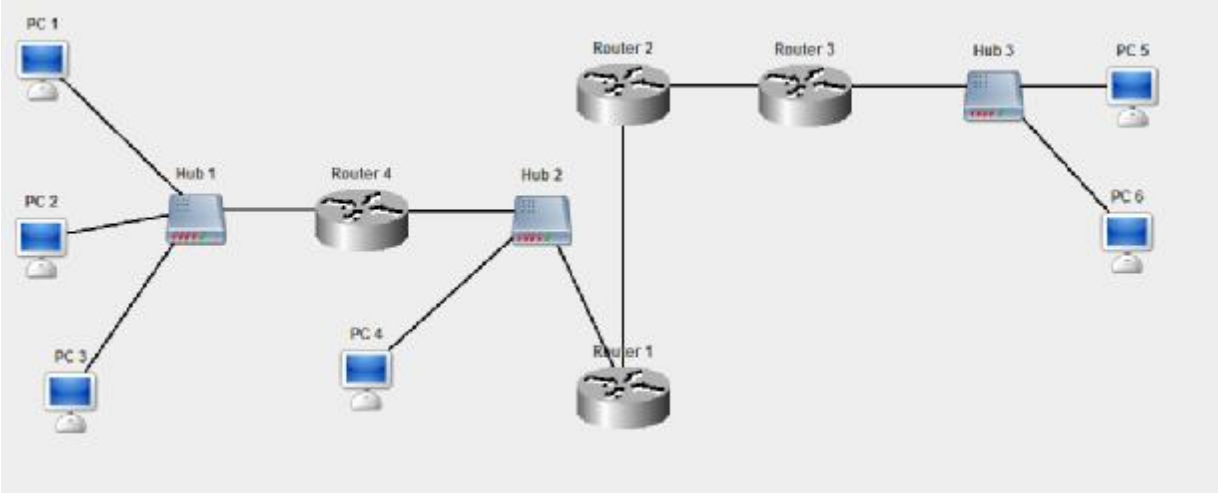
Сеть 1 между маршрутизаторами Router1, Router2 и Router4: 10.0.0.0
Сеть 2 между маршрутизаторами Router2 и Router3: 192.168.0.0
Сеть между маршрутизаторами Router4 и Router 5: 204.108.0.0
Компьютер PC1 имеет IP-адрес: 192.139.36.1
Компьютер PC6 имеет IP-адрес: 216.125.47.1
Компьютер PC3 имеет IP-адрес: 10.125.148.1
Обозначения в задании: К1- PC1, К2-PC2, К3-PC5

Вариант № 7



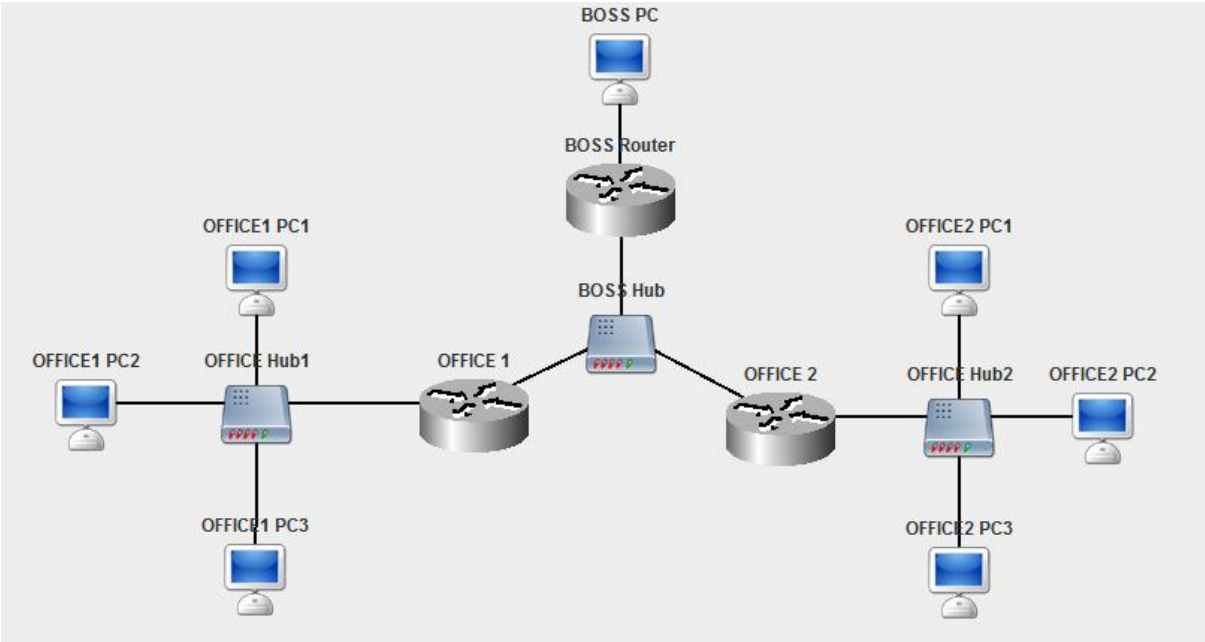
Сеть 1 между маршрутизаторами ADSL_1 и ADSL_2: 172.168.0.0
Сеть 2 между маршрутизаторами ADSL_2, ADSL_4 и ADSL_3: 10.147.126.0
Сеть между маршрутизаторами ADSL_3 и ADSL_5: 192.168.0.0
Компьютер Station_1 имеет IP-адрес: 214.102.32.1
Компьютер Station_5 имеет IP-адрес: 214.36.128.1
Компьютер Station_6 имеет IP-адрес: 198.168.128.1
Обозначения в задании: К1-Station_1, К2-Station_2, К3-Station_5

Вариант № 8



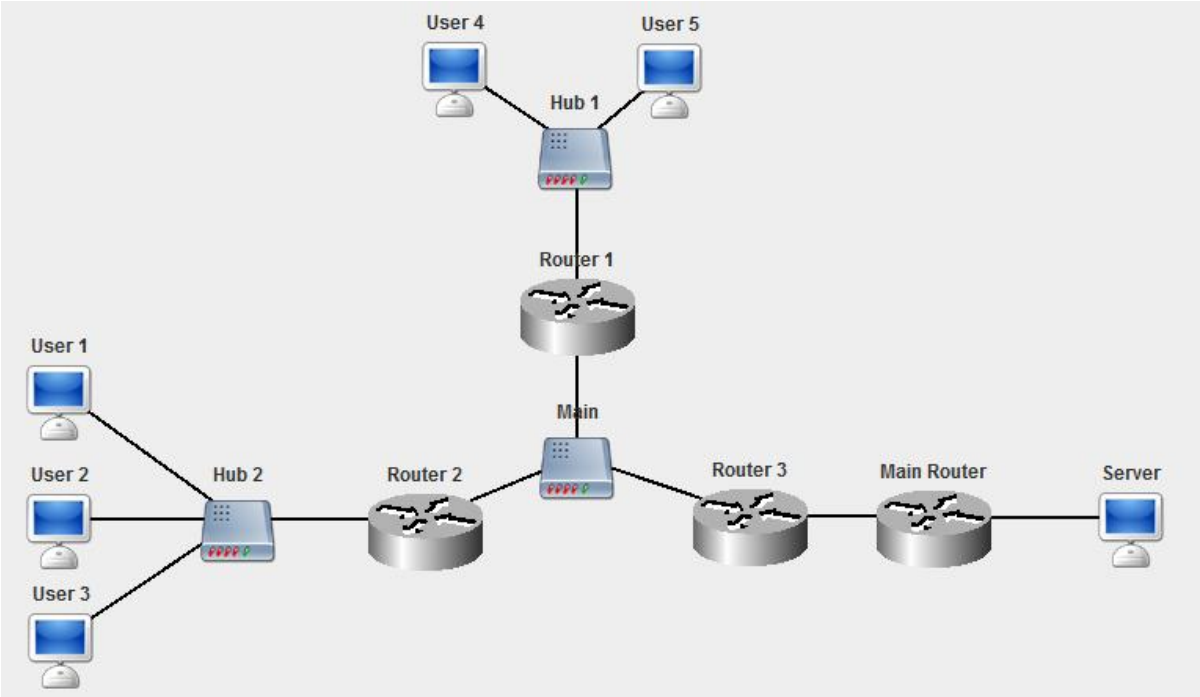
Сеть между маршрутизаторами Router 2 и Router 3: 192.168.0.0
Компьютер PC1 имеет IP-адрес: 10.0.0.1
Компьютер PC6 имеет IP-адрес: 172.168.100.2
Сеть между маршрутизаторами Router 4 и Router 1: 126.168.80.0
Обозначения в задании: K1-PC 1, K2-PC 4, K3-PC 6

Вариант № 9



Компьютер BOSSPC имеет IP-адрес: 10.0.0.1
Компьютер OFFICE1 PC1 имеет IP-адрес: 172.168.26.1
Компьютер OFFICE2 PC1 имеет IP-адрес: 192.100.10.1
Обозначения в задании: K1-BOSS, K2-OFFICE1 PC3, K3-OFFICE2 PC2

Вариант № 10



Компьютер Server имеет IP-адрес: 10.0.0.1
Компьютер User 1 имеет IP-адрес: 172.168.10.56
Компьютер User 4 имеет IP-адрес: 100.56.99.4
Сеть между маршрутизаторами Router 3 и MainRouter: 126.168.80.0
Обозначения в задании: K1-Server, K2-User 2, K3-User 5

Контрольные вопросы

1. Назначение и принцип работы протокола ICMP;
2. Назначение и принцип работы протокола ARP;
3. Типы и виды адресации. Выделенные адреса сети.
4. Опишите структуру MAC-адреса.
5. Опишите структуру IP-адреса.
6. Назначение и использование маски сети;
5. Принцип работы маршрутизатора.

Практическое занятие № 2
Статическая маршрутизация в IP-сетях

Цель: изучение таблиц маршрутизации.

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Таблица маршрутизации – электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора. Является простейшей формой правил маршрутизации.

Таблица маршрутизации обычно содержит:

- адрес сети или узла назначения, либо указание, что маршрут является маршрутом по умолчанию;
- маску сети назначения (для IPv4-сетей маска /32 (255.255.255.255) позволяет указать единичный узел сети);
- шлюз, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения;
- интерфейс (в зависимости от системы, это может быть порядковый номер, GUID или символьное имя устройства);
- метрику – числовой показатель, задающий предпочтительность маршрута.Чем меньше это число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).

Типы записей в таблице маршрутизации:

- маршрут до сети;
- маршрут до компьютера;
- маршрут по умолчанию.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В соответствии со своим вариантом задания научиться управлять таблицами маршрутизации.

Подготовка к работе

Изучите теоретическую часть по данной теме. Ознакомьтесь с заданием на лабораторную работу, определяемым преподавателем.

Выполнение работы:

1. Для всех узлов сети установить IP-адреса, маски подсетей и шлюзы по умолчанию, чтобы добиться успешного выполнения эхо-запроса ближайших соседей (находящихся в одной подсети).

2. Настроить таблицы маршрутизации на маршрутизаторах, чтобы добиться доставки пакетов от узла К1 к узлу К2 и обратно, от узла К2 к К3 и обратно, от узла К3 к К1 и обратно. Пакеты должны доходить до узлов кратчайшим путем.

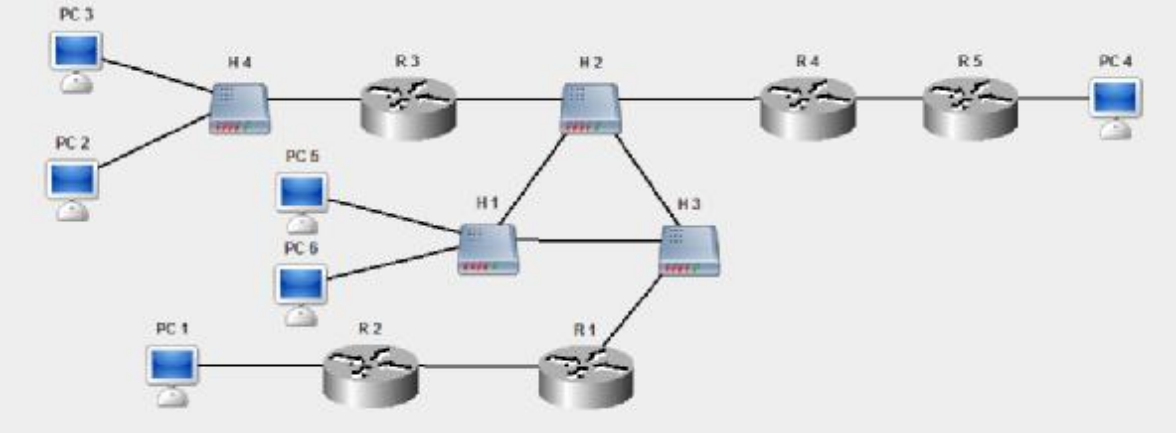
3. Настроить таблицы маршрутизации на узлах K1, K2 и K3, чтобы обеспечить кратчайшую доставку пакетов между этими узлами, если это невозможно было обеспечить в пункте 2.

Продемонстрировать результат преподавателю, оформить отчёт по работе, содержащий название работы, задание и результаты выполнения и ответить на контрольные вопросы.

В отчете привести конфигурацию стека TCP/IP для каждого из узлов, таблицы маршрутизации, результаты эхо-запросов между узлами K1, K2 и K3, а также обоснование правильности и оптимальности выбранных маршрутов.

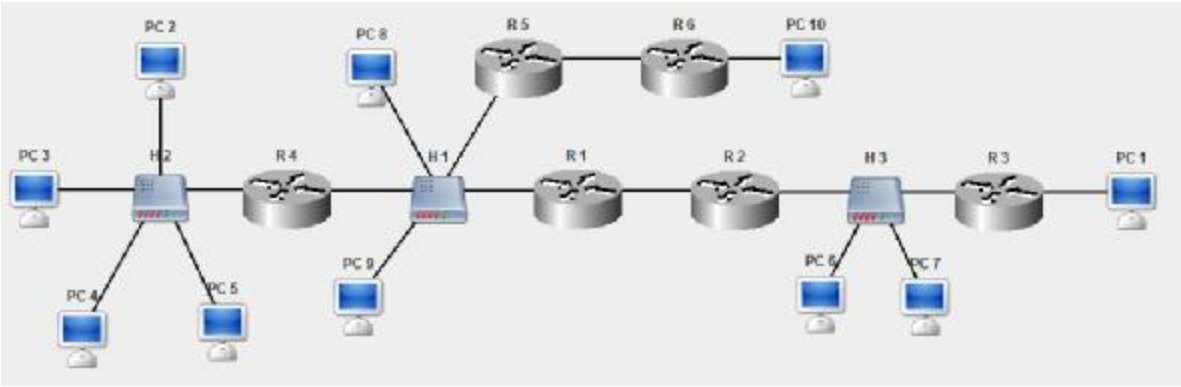
ВАРИАНТЫ ЗАДАНИЙ:

Вариант 1



Сеть 1 между маршрутизаторами R4 и R5: 126.168.80.0
Сеть 2 между маршрутизаторами R2 и R1: 192.168.0.0
Сеть между маршрутизаторами R 3, R 4 и R 1: 200.100.0.0
Компьютер PC 4 имеет IP-адрес: 135.120.15.1
Компьютер PC 3 имеет IP-адрес: 192.168.1.1
Компьютер PC 1 имеет IP-адрес: 10.0.0.1
Обозначения в задании: K1-PC 1, K2-PC 2, K3-PC 4

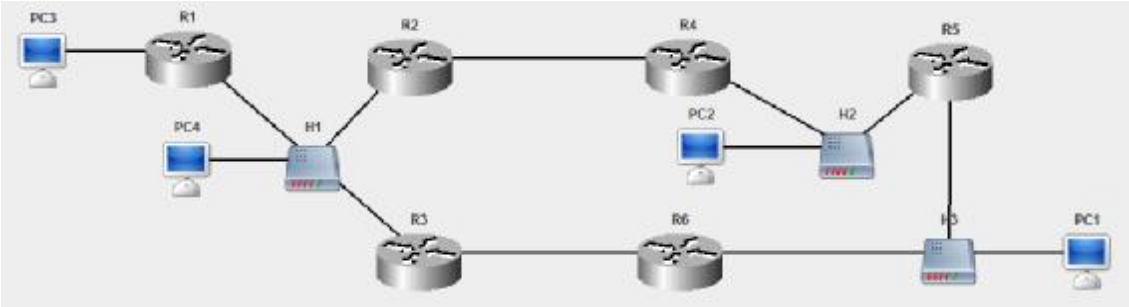
Вариант 2



Сеть 1 между маршрутизаторами R1, R4 и R5: 204.188.45.128
Сеть 2 между маршрутизаторами R2 и R3: 204.188.45.192

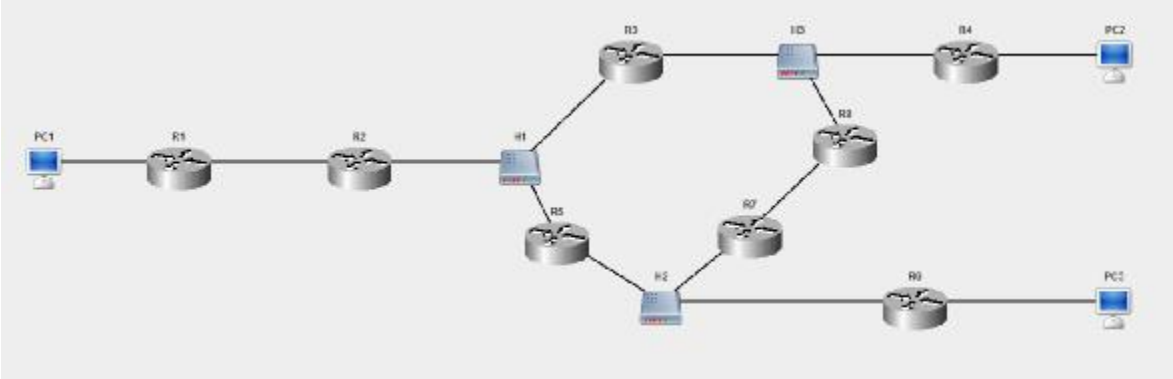
Сеть между маршрутизаторами R5 и R6: 192.168.20.0
Сеть между маршрутизаторами R1 и R2: 172.100.58.0
Компьютер PC1 имеет IP-адрес: 204.188.45.1
Компьютер PC3 имеет IP-адрес: 204.188.45.65
Компьютер PC8 имеет IP-адрес: 204.188.45.129
Компьютер PC7 имеет IP-адрес: 204.188.45.196
Обозначения в задании: K1-PC 1, K2-PC 5, K3-PC 10

Вариант 3



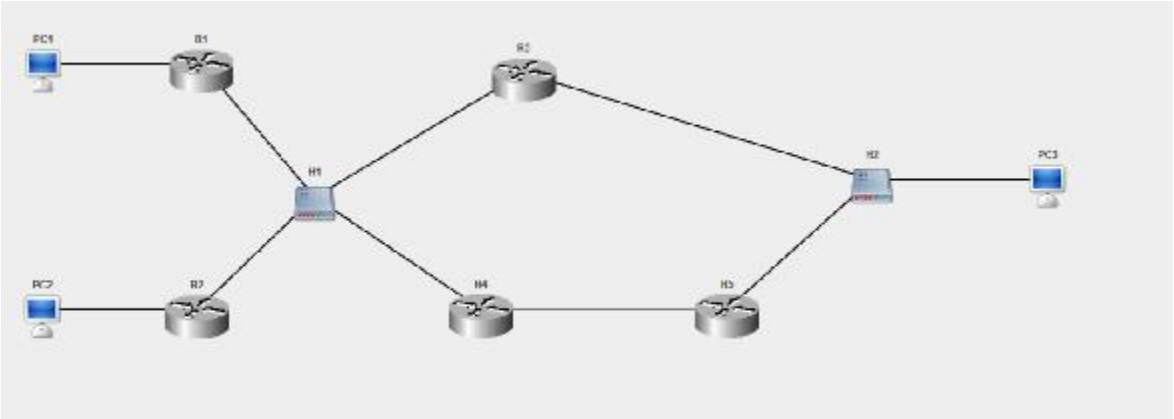
Сеть 1 между маршрутизаторами R1, R2 и R3: 192.168.3.0
Сеть 2 между маршрутизаторами R3 и R6: 204.188.45.0
Сеть 3 между маршрутизаторами R2 и R4: 172.168.100.0
Сеть 4 между маршрутизаторами R 5 и R6: 204.188.45.12
Компьютер PC3 имеет IP-адрес: 10.15.45.1
Компьютер PC2 имеет IP-адрес: 135.187.20.5
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Вариант 4



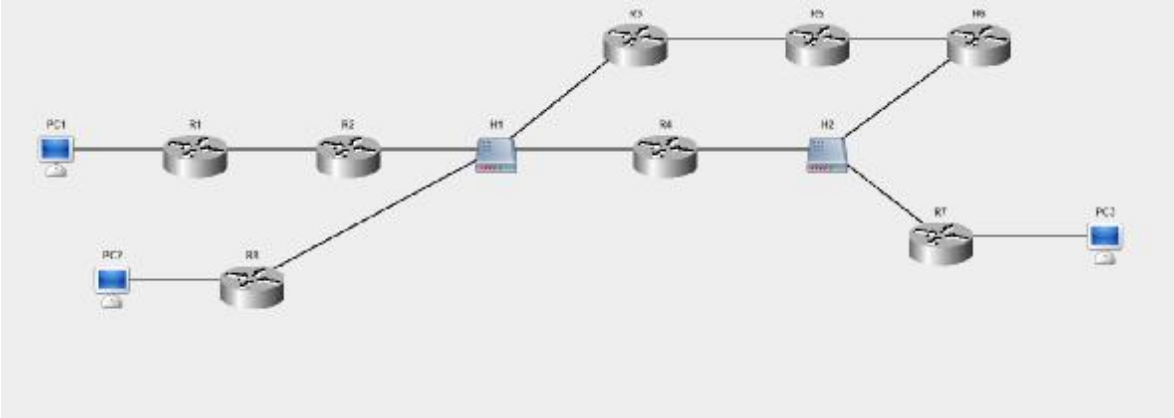
Компьютер PC1 имеет IP-адрес: 192.168.1.5
Компьютер PC1 имеет IP-адрес: 180.167.2.1
Компьютер PC1 имеет IP-адрес: 178.168.3.12
Маршрутизатор R4 имеет адрес 10.200.1.3 на первом интерфейсе
Маршрутизатор R6 имеет адрес 15.12.0.3 на первом интерфейсе
Сеть 1 между маршрутизаторами R1, R2: 10.1.1.0
Сеть 2 между маршрутизаторами R7, R8: 11.2.2.0
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Вариант 5



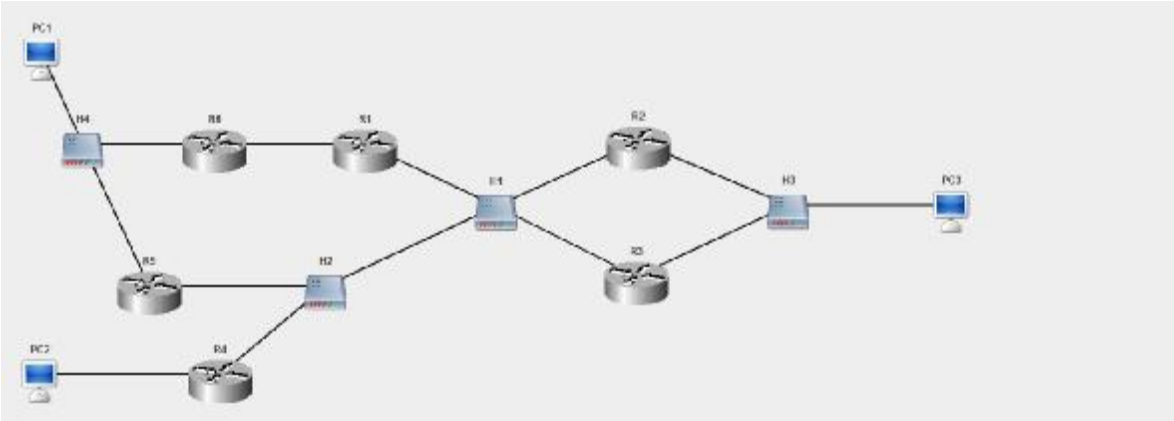
Компьютер PC1 имеет IP-адрес: 201.158.3.1
Компьютер PC1 имеет IP-адрес: 200.140.20.1
Компьютер PC1 имеет IP-адрес: 150.130.1.3
Сеть 1 между маршрутизаторами R1, R2, R3, R4: 12.0.0.0
Сеть 2 между маршрутизаторами R4, R5: 192.100.13.0
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Вариант 6



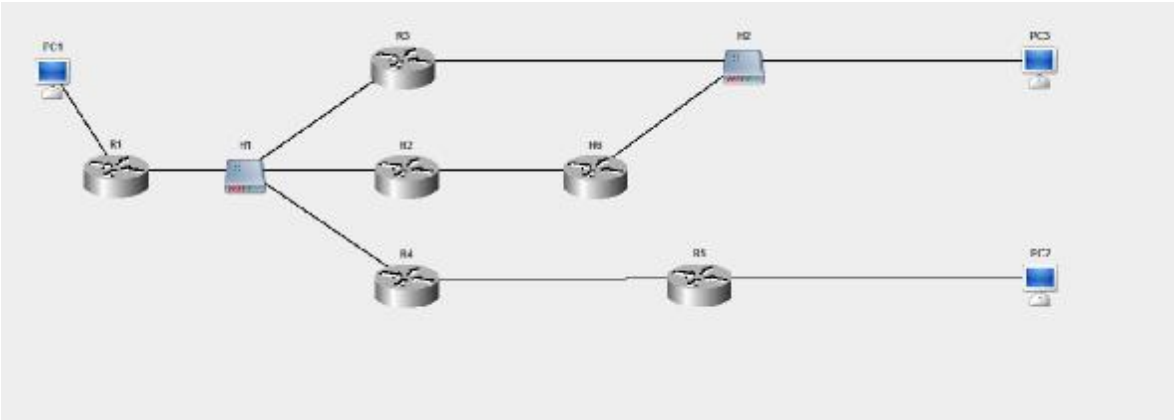
Компьютер PC1 имеет IP-адрес: 190.118.26.1
Компьютер PC1 имеет IP-адрес: 100.11.15.13
Компьютер PC1 имеет IP-адрес: 126.17.26.3
Маршрутизатор R5 имеет адрес 10.0.1.2 на первом интерфейсе и адрес 15.7.2.1 на втором интерфейсе
Сеть 1 между маршрутизаторами R2, R3, R4, R8: 110.90.70.0
Сеть 2 между маршрутизаторами R4, R6, R7: 120.15.27.0
Сеть 3 между маршрутизаторами R1 и R2: 178.36.98.0
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Вариант 7



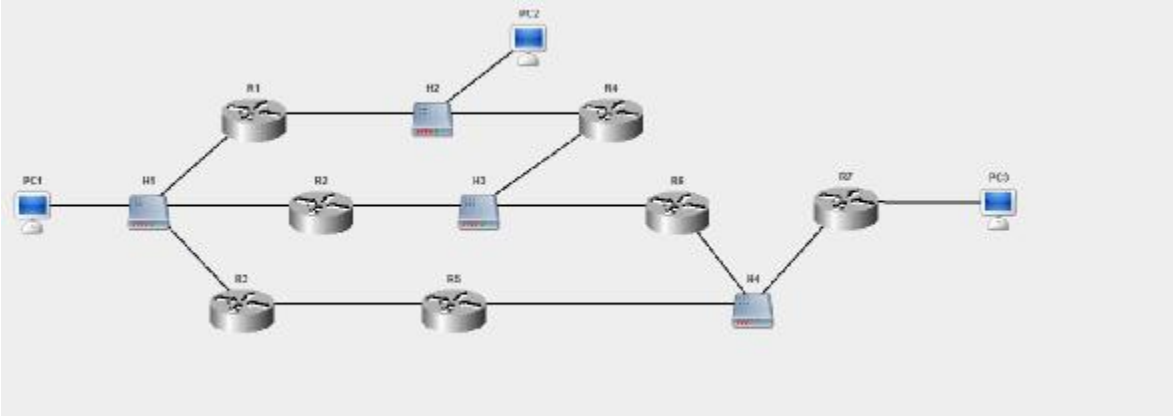
Компьютер PC1 имеет IP-адрес: 150.151.20.1
Компьютер PC1 имеет IP-адрес: 130.10.11.2
Компьютер PC1 имеет IP-адрес: 178.16.76.3
Сеть 1 между маршрутизаторами R1, R2, R3, R4, R5: 200.17.56.0
Сеть 2 между маршрутизаторами R1, R6: 140.120.33.0
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Вариант 8



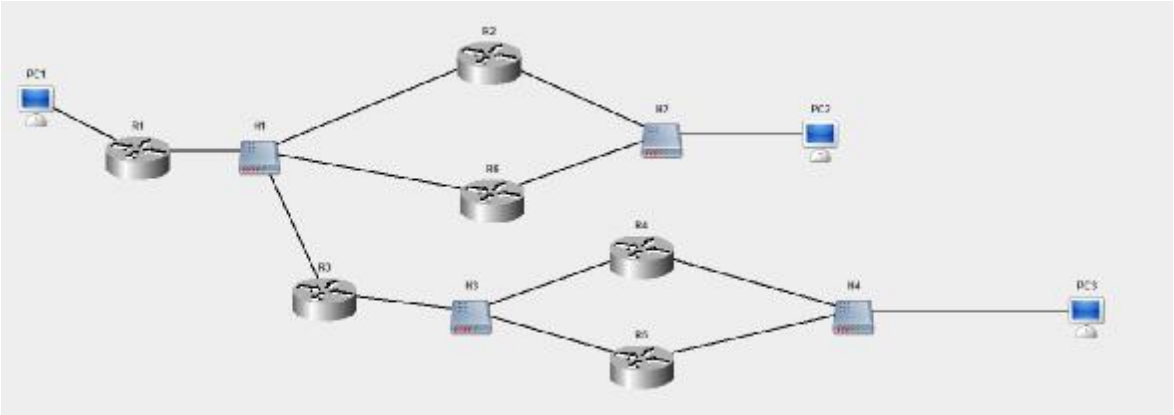
Компьютер PC1 имеет IP-адрес: 188.44.15.1
Компьютер PC1 имеет IP-адрес: 160.159.11.2
Компьютер PC1 имеет IP-адрес: 133.26.17.3
Маршрутизатор R5 имеет адрес 178.36.15.1 на первом интерфейсе
Сеть 1 между маршрутизаторами R1, R2, R3, R4: 122.250.11.0
Сеть 2 между маршрутизаторами R2, R6: 150.11.23.0
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Вариант 9



Компьютер PC1 имеет IP-адрес: 222.33.44.1
Компьютер PC1 имеет IP-адрес: 234.56.78.2
Компьютер PC1 имеет IP-адрес: 210.100.5.12
Сеть 1 между маршрутизаторами R2, R3, R5, R6: 148.82.28.0
Сеть 2 между маршрутизаторами R5, R6, R7: 132.2.50.0
Сеть 3 между маршрутизаторами R3 и R5: 228.100.101.0
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Вариант 10



Компьютер PC1 имеет IP-адрес: 122.34.56.1
Компьютер PC1 имеет IP-адрес: 134.27.44.1
Компьютер PC1 имеет IP-адрес: 12.1.13.2
Сеть 1ммежду маршрутизаторами R1, R2, R3, R6: 15.0.1.0
Сеть 2 между маршрутизаторами R3, R4, R5: 125.124.13.0
Обозначения в задании: K1-PC1, K2-PC2, K3-PC3

Контрольные вопросы

1. Опишите структуру таблицы маршрутизации;
2. Опишите возможные типы маршрутов;
3. Опишите назначение поля "Адрес сети" таблицы маршрутизации;

4. Опишите назначение поля "Шлюз" таблицы маршрутизации;
5. Опишите назначение поля "Интерфейс" таблицы маршрутизации.

Практическое занятие № 3
Управление сетью. Протокол SNMP

Цель: изучение протокола SNMP.

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

SNMP (англ. SimpleNetworkManagementProtocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определен Инженерным советом интернета (IETF) как компонент TCP/IP. Он состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.

Средства протокола SNMP позволяют организовать управление путем задания значений переменных, которые описывают конфигурацию управляемой системы. Эти переменные могут быть запрошены (а иногда и заданы) управляющими приложениями.

При использовании SNMP один или более административных компьютеров (где функционируют программные средства, называемые менеджерами) выполняют отслеживание или управление группой хостов или устройств в компьютерной сети. На каждой управляемой системе есть постоянно запущенная программа, называемая агент, которая через SNMP передаёт информацию менеджеру.

Менеджеры SNMP обрабатывают данные о конфигурации и функционировании управляемых систем и преобразуют их во внутренний формат, удобный для поддержания протокола SNMP. Протокол также разрешает активные задачи управления, например, изменение и применение новой конфигурации через удаленное изменение этих переменных. Доступные через SNMP переменные организованы в иерархии. Эти иерархии, как и другие метаданные (например, тип и описание переменной), описываются базами управляющей информации (базы MIB, от англ. Management information base).

Управляемые протоколом SNMP сети состоят из трех ключевых компонентов:

1) Управляемое устройство;

2) Агент — программное обеспечение, запускаемое на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства;

3) Система сетевого управления (Network Management System, NMS) — программное обеспечение, взаимодействующее с менеджерами для поддержки комплексной структуры данных, отражающей состояние сети[1].

Управляемое устройство — это элемент сети (оборудование или программное средство), реализующий интерфейс управления (не обязательно SNMP), который раз-

решает однонаправленный (только для чтения) или двунаправленный доступ к конкретной информации об элементе. Управляемые устройства обмениваются этой информацией с менеджером. Управляемые устройства могут относиться к любому виду устройств: маршрутизаторы, серверы доступа, коммутаторы, мосты, концентраторы, IP-телефоны, IP-видеокамеры, компьютеры-хосты, принтеры и т.п.

Агентом называется программный модуль сетевого управления, располагающийся на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства. Агент обладает локальным знанием управляющей информации и переводит эту информацию в специфичную для SNMP форму или из неё (медиация данных).

В состав системы сетевого управления (NMS) входит приложение, отслеживающее и контролирующее управляемые устройства. NMS обеспечивают основную часть обработки данных, необходимых для сетевого управления. В любой управляемой сети может быть одна и более NMS.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В соответствии со своим вариантом задания научиться управлять сетью средствами протокола SNMP.

Подготовка к работе

Изучите теоретическую часть по данной теме. Ознакомьтесь с заданием на лабораторную работу, определяемым преподавателем.

Выполнение работы:

1. На компьютере К1 запустить SNMP агента. Порт и имя группы доступа выбираются студентом.

2. С компьютера К2 отправить запрос(ы) get, и получить переменные П1, П2, П3. Сравнить полученные значения с действительными значениями.

3. С компьютера К2 отправить запрос(ы) getnext для переменных П1, П2, П3. Пояснить полученные результаты;

4. На компьютере К1 с помощью диалога "Set TCP/IP Properties" изменить IP адрес, маску подсети и шлюз по умолчанию. С компьютера К2 с помощью запросов set вернуть К1 в исходное состояние. Проверить результаты посредством SNMP;

Продемонстрировать результат преподавателю и ответить на контрольные вопросы.

ВАРИАНТЫ ЗАДАНИЙ:

Вариант 1

- Обозначения в задании: Компьютеры К1 – OFFICE2 pc1; К2 – Boss; К3 – Hacker.
- SNMP переменные П1 – Counter.InputIP; П2 – IP.AllInterfaces; П3 – IP.Address_Eth0.

Вариант 2

- Обозначения в задании: Компьютеры К1 – OFFICE1 pc4; К2 – BIGBOSS; К3 – M_CH_S.
- SNMP переменные П1 – Counter.OutputIP; П2 – IP.ARPTable; П3 – IP.SubnetMask_Eth0.

Вариант 3

- Обозначения в задании: Компьютеры К1 – OFFICE2 pc2; К2 – Hacker; К3 – Boss.
- SNMP переменные П1 – Counter.ARP; П2 – IP.DefaultGateway; П3 – SNMP.CommunityName.

Вариант 4

- Обозначения в задании: Компьютеры К1 – BIG BOSS; К2 – OFFICE1 pc1; К3 – OFFICE1 pc3.
- SNMP переменные П1 – Counter.InputTCP; П2 – IP.Address_Eth0; П3 – SNMP.revision.

Вариант 5

- Обозначения в задании: Компьютеры К1 – FileServer; К2 – Manager1; К3 – MegaBoss.
- SNMP переменные П1 – Counter.OutputTCP; П2 – IP.SubnetMask_Eth0; П3 – IP.DefaultGateway.

Вариант 6

- Обозначения в задании: Компьютеры К1 – PrintServer; К2 – Manager3; К3 – MicroBoss.
- SNMPпеременныеП1 – Counter.ReceiveDuplicatedTCP; П2 – SNMP.CommunityName; П3 – IP.ARPTable.

Вариант 7

- Обозначения в задании: Компьютеры К1 – Station1; К2 – Station4; К3 – Remote1.
- SNMP переменныеП1 – Counter.SendDuplicatedTCP; П2 – SNMP.revision; П3 – IP.AllInterfaces.

Вариант 8

- Обозначения в задании: Компьютеры К1 – Station3; К2 – Remote1; К3 – Station2.
- SNMP переменные П1 – Counter.SendAckTCP; П2 – Counter.InputIP; П3 – Device.MACaddress_Eth0.

Вариант 9

- Обозначения в задании: Компьютеры К1 – PC1; К2 – PC2; К3 – PC4.
- SNMP переменные П1 – Counter.InputUDP; П2 – Counter.OutputIP; П3 – Device.AvailableInterfaces.

Вариант 10

- Обозначения в задании: Компьютеры К1 – РС2; К2 – РС3; К3 – РС4.
- SNMP переменные П1 – Counter.OutputUDP; П2 – Counter.ARP; П3 – Device.AllInterfaces.

Контрольные вопросы

1. Опишите состав и назначение SNMP-протокола;
2. Опишите менеджера в протоколе SNMP;
3. Опишите структуру базы управляющей информации;
4. Опишите запросы протокола SNMP;
5. Расскажите о вопросах безопасности протокола SNMP.

Библиографический список

1.Исследование уровней организации IPсетей. Лабораторный практикум // Алекперов И.А. Большев А.К. Карпов К.Э. Кринкин К.В. Яновский В.В. СПб.: Изд-во СПбГЭТУ "ЛЭТИ", 2006. 80 с.

Лабораторная работа № 4
Анализатор протокола. Возможности и практика использования

Цель: освоить методику анализа сетевого трафика с помощью специализированного программного обеспечения.

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Анализатор трафика, или сниффер (от англ. tosniff — нюхать) — сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Сниффер может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию. Использование коммутаторов (switch, switch-hub) и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы. Коммутация пакетов — форма передачи, при которой данные, разбитые на отдельные пакеты, могут пересылаться из исходного пункта в пункт назначения разными маршрутами. Так что если кто-то в другом сегменте посылает внутри него какие-либо пакеты, то в ваш сегмент коммутатор эти данные не отправит.

Перехват трафика может осуществляться:

-обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);

- подключением сниффера в разрыв канала;

- ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер (Networktap);

- через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;

- через атаку на канальном (2) (MAC-spoofing) или сетевом (3) уровне (IP-spoofing), приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

В начале 1990-х гг перехват траффика широко применялся хакерами для захвата пользовательских логинов и паролей, которые в ряде сетевых протоколов передаются в незашифрованном или слабозашифрованном виде. Широкое распространение хабов позволяло захватывать трафик без больших усилий в больших сегментах сети практически без риска быть обнаруженным.

Снифферы применяются как в благих, так и в деструктивных целях. Анализ прошедшего через сниффер трафика позволяет:

1) Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (снифферы здесь малоэффективны; как правило, для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием и её последующий анализ).

2) Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных снифферов — мониторов сетевой активности).

3) Перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации.

4) Локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами)

5) Поскольку в «классическом» снифферe анализ трафика происходит вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), то он подходит для анализа лишь небольших его объёмов.

Снизить угрозу сниффинга пакетов можно с помощью таких средств, как:

- аутентификация

- криптография

- антиснифферы

- коммутируемая инфраструктура

Работа с анализатором протоколов WinDump

Обычно вы будете запускать WinDump с некоторыми установленными опциями или фильтрами, чтобы уменьшить и сфокусировать вывод. Общий вид инструкции запуска WinDump таков:

WinDump: опции выражения

Замените опции и выражения одной или несколькими допустимыми переменными.

Опции WinDump перечислены в таблице ниже:

Опция	Описание
-a	Пытается преобразовать адреса в имена. Это создает дополнительную нагрузку на систему и может привести к потере пакетов
-c	Число. Останавливает WinDump после обработки заданного числа пакетов
-C	Размер_файла. Ограничивает размер выходных файлов заданным числом байт
-d	Выдает процедуру сопоставления пакетов с образцом в удобочитаемом виде и затем останавливается
-dd	Выдает процедуру сопоставления пакетов с образцом в виде фрагмента программы на языке Си
-ddd	Выдает процедуру сопоставления пакетов с образцом в виде десятичных чисел
-e	В каждой строке выдачи печатает заголовок канального уровня (в сетях Ethernet это MAC-адрес)
-E	Алгоритм «секрет». Использует встроенную в WinDump возможность расшифровывать на лету пакеты, зашифрованные по протоколу IPsecESP. Разумеется, чтобы использовать эту опцию, нужно располагать разделяемым секретным ключом. В число возможных значений параметра "алгоритм" входят des-cbc, 3des-cdc, blowfish-cbc, r3c-cbc, приведенный 128-cbc. Кроме того, оно может быть пустым. По умолчанию используется des-cbc. Значением параметра "секрет" должен служить секретный ключ ESP в текстовом виде
-F	Файл. Использует файл (а не сеть) для ввода данных. Это удобно для анализа событий "постфактум".
-i	Интерфейс. Читает из заданного интерфейса, когда на анализирующей машине имеется несколько сетевых интерфейсов. По умолчанию WinDump использует действующий интерфейс с наименьшим номером. В системах Linux можно использовать также параметр any для перехвата пакетов из всех сетевых интерфейсов
-n	Не преобразовывает адреса в имена
-N	Не печатает в именах хостов имя домена вышележащего уровня. Это полезно, если вам необходимо представить обезличенную версию вывода и вы не хотите раскрывать, чья это сеть

-p	Не переводит интерфейс в режим прослушивания. Используется только при исследовании трафика, направленного в анализирующий компьютер
-q	Печатает быстрый вывод. Печатается меньше протокольной информации, поэтому строки оказываются короче
-T	Тип. Заставляет интерпретировать пакеты, выбранные заданным в выражении фильтром, в соответствии с указанным типом
-t	Не печатает метку времени в каждой строке
-tt	Печатает неформатированную метку времени в каждой строке
-ttt	Печатает интервал времени между пакетами
-tttt	Печатает в каждой строке дату, а затем метку времени в подразумеваемом формате
-v	Использует чуть более подробный вывод, включающий время жизни, идентификатор, общую длину и поля опций каждого пакета
-vv	Предоставляет более детальный вывод. Пакеты NFS и SMB полностью декодируются
-vvv	Предоставляет еще более подробный вывод. Это может существенно замедлить работу анализатора
-w	Имя_файла. Записывает пакеты в указанный файл вместо вывода их на экран. Таким образом результаты "вынюхивания" без участия человека можно сохранить и проанализировать их позже. Например, если в вашей сети происходят какие-то странные вещи, вы можете запустить WinDump на ночь, чтобы перехватить весь необычный трафик. Не забудьте написать хороший фильтр, иначе полученный наутро файл может оказаться слишком большим
-x	Выводит каждый пакет (без заголовка канального уровня) в шестнадцатеричном виде.
-X	Выводит содержимое пакетов и в шестнадцатеричном, и в текстовом видах

Выражения WinDump

Выражения WinDump определяют выбор отображаемых сетевых пакетов. Именно здесь происходит реальная работа WinDump. Выдаются только те объекты, которые соответствуют выражению; если выражения не заданы, отображаться будут все пакеты. Выражение WinDump состоит из одной или нескольких директив, называемых примитивами, которые, в свою очередь, состоят из идентификатора и следующего за ним квалификатора.

Существуют также более сложные выражения, которые можно строить с помощью булевых операций, таких как И, ИЛИ, НЕ, и операций сравнения (больше, меньше и т.п.). Обратитесь к оперативной справке WinDump, чтобы детальнее ознакомиться с примерами и методами применения выражений.

В таблицах ниже перечислены три различных вида квалификаторов, и доступные комбинации примитивов.

Квалификаторы WinDump

- тип: Определяет, к чему относится идентификатор, заданный как имя или номер. Возможными типами служат host, net и port. Например, hostfoo, net 128.3 или port 20

- направление: Определяет направление трафика от определенного идентификатора. Возможными направлениями служат src; dst; srcordst и srcanddst (src обозначает исходный адрес, dst - целевой)

- протокол: Позволяет определить протокол для фильтрации. Возможными протоколами являются ether, fddi, tr, ip, ipv6, arp, rarp, decnet, tcp и udp. Если протокол не задан, то допустимы все протоколы, совместимые с остальной частью выражения. При помощи фильтров с этим квалификатором можно определить, какая машина делает чрезмерное количество arp-запросов, или для отбрасывания на фильтре udp-запросов, которых немало во многих сетях, так как DNS использует udp

Допустимые комбинации примитивов

1) dsthost хост: Показывает только трафик, адресованный хосту, который может быть задан IP-адресом или именем;

2) srchost хост: Показывает только трафик, исходящий из хоста;

3) host хост: Показывает как исходящий, так и входящий трафик хоста;

4) etherdstEthernet-хост: Показывает трафик, предназначенный для указанногоEthernet-хоста, который может быть задан либо именем, либо MAC-адресом;

5) ethersrcEthernet-хост: Показывает трафик, исходящий из Ethernet-хоста

6) etherhostEthernet-хост: Показывает как исходящий, так и входящий трафик Ethernet-хоста;

7) gateway хост: Показывает любой трафик, использующий хост в качестве шлюза. Иными словами, трафик, переправляемый с хоста. Так происходит, когда IP-адрес отправителя или получателя не соответствует Ethernet-адресу хоста. Данную возможность целесообразно использовать, когда необходимо отследить весь трафик, проходящий через Интернет-шлюз или некоторый конкретный маршрутизатор;

8) dstnet сеть: Фильтрует трафик, предназначенный для конкретной сети, заданной в нотации 0.0.0.0. Аналогично etherdstEthernet-хост за исключением того, что это может быть значительно больше, чем один хост;

9) srcnet сеть: Фильтрует сеть отправителя;

10) net сеть: То же, что и две предыдущие инструкции, но трафик разрешен как в заданную сеть, так и из нее;

11) net сеть maskмаска_сети: Сопоставляется с трафиком в заданную сеть или из нее, с указанной маской сети. Применяется для задания точного размера сети с шагом меньше, чем класс C. В этой комбинации допускается использование примитивов src и dst для указания направления потоков данных;

12) net сеть/длина_маски: Сопоставляется с трафиком с сетевыми адресами из указанной сети и заданным числом бит в маске сети. Аналогична предыдущей комбинации;

13) dstport порт: Фильтрует трафик TCP и UDP с заданным целевым портом. Здесь можно также специфицировать тип перехватываемого трафика, TCP или UDP. По умолчанию отображается трафик обоих типов;

14) srcport порт: То же, что и предыдущая комбинация, только перехватывается трафик с заданным исходным портом;

15) less длина: Отображает пакеты с длиной, меньшей или равной заданной. Допустима также комбинация len<= длина;

16) greater длина: То же, что и предыдущая комбинация, только перехватывается трафик с длиной пакетов больше или равной указанной;

17) ipproto протокол: Перехватывает трафик заданного протокола. Допустимыми протоколами служат icmp, icmpv6, igmp, igrp, pim, ah, esp, vrrp, udp и tcp. Имена tcp, udp и icmp должны помещаться между двумя обратными косыми чертами, чтобы они не читались как ключевые слова. Пример: ipproto \tcp\;

18) ip6 proto протокол: Аналогично предыдущей комбинация, но для пакетов и типов IPv6;

19) ip6 protochain протокол: Ищет пакеты IPv6, имеющие заголовок указанного протокола;

20) ipprotochain протокол: То же, что и выше, но для пакетов IPv4;

21) ipbroadcastЖ Идентифицирует только широковещательный трафик, то есть трафик, имеющий все нули или все единицы в поле целевого адреса;

22) ethermulticastЖ Регистрирует вещательные пакеты Ethernet;

23) ipmulticast: Регистрирует вещательные пакеты IP;

24) ip6 multicast: Регистрирует вещательные пакеты IPv6;

25) etherproto протокол: Отображает трафик, который имеет указанный тип протокола Ethernet. Допустимыми именами протоколов служат ip, ipv6, arp, rarp, atalk, aarp, decnet, sca, lat, mopdl, moprc, iso, stp, ipx и netbeui. Эти имена являются также идентификаторами, поэтому они должны быть экранированы с помощью обратных косых черт;

26) decnetsrc хост: Перехватывает трафик DECnet с исходным адресом хоста;

27) decnetdst хост: Аналогична предыдущей комбинация, но фильтрует целевой адрес хоста;

28) decnet хост: Фильтрует трафик DECnet с исходным или целевым адресом хоста;

29) ip: Сокращенный вариант описанной выше комбинации etherprotoip. Перехватывает трафик, соответствующий Ethernet-протоколу ip;

30) ip6: Сокращенный вариант описанной выше комбинации etherprotoip6. Перехватывает трафик, соответствующий Ethernet-протоколу ip6;

31) arp: Сокращенный вариант описанной выше комбинации etherprotoarp. Перехватывает трафик, соответствующий Ethernet-протоколу arp;

32) rarp: Сокращенный вариант описанной выше комбинации etherprotorarp. Перехватывает трафик, соответствующий Ethernet-протоколу rarp;

33) atalk: Сокращенный вариант описанной выше комбинации etherprotoatalk. Перехватывает трафик, соответствующий Ethernet-протоколу atalk;

34) aarp: Сокращенный вариант описанной выше комбинации etherprotoaarp. Перехватывает трафик, соответствующий Ethernet-протоколу aarp;

35) decnet: Сокращенный вариант описанной выше комбинации etherprotodecnet. Перехватывает трафик, соответствующий Ethernet-протоколу decnet

36) iso: Сокращенный вариант описанной выше комбинации etherprotoiso. Перехватывает трафик, соответствующий Ethernet-протоколу iso;

37) stp: Сокращенный вариант описанной выше комбинации etherprotostp. Перехватывает трафик, соответствующий Ethernet-протоколу stp;

38) ipx: Сокращенный вариант описанной выше комбинации etherprotoipx. Перехватывает трафик, соответствующий Ethernet-протоколу ipx;

39) netbeui: Сокращенный вариант описанной выше комбинации etherprotonetbeui. Перехватывает трафик, соответствующий Ethernet-протоколу netbeui;

40) vlan:идентификатор_ВЛВС Перехватывает пакеты на основе стандарта 802.1QVLAN. Идентификатор виртуальной локальной сети можно опускать;

41) tcp: Сокращенная форма комбинации ipprototcp;

42) udp: Сокращенная форма комбинации ipprotoudp;

43) icmp: Сокращенная форма комбинации ipprotoicmp;

44) isoproto: протокол Перехватывает пакеты ВОС с заданным типом протокола - clnp, esis или isis;

45) clnp: Сокращенная форма описанной выше комбинации с clnp в качестве протокола;

46) esis: Сокращенная форма комбинации isoproto протокол с esis в качестве протокола;

47) isis: Сокращенная форма комбинации isoproto протокол с isis в качестве протокола.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В соответствии с заданием научиться анализировать и исследовать сетевой трафик.

Подготовка к работе

Изучите теоретическую часть по данной теме. Ознакомьтесь с заданием на лабораторную работу, определяемым преподавателем.

Выполнение работы:

1. Запустить windump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

2. Запустить windump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

3. Запустить windump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

4. Запустить windump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

5. Прочесть программой windump созданный в предыдущем пункте файл.

6. Выполните наблюдение за входящим и исходящим трафиком 23 порта;

7. Выполните просмотр входящего и исходящего трафика определенного хоста, за исключением некоторых видов трафика (трафик 23 порта).

Продемонстрировать результат преподавателю и ответить на контрольные вопросы.

Контрольные вопросы:

1. Назначение анализатора пакетов;
2. Доступные опции программы windump;
3. Фильтрация пакетов в windump;
4. Примитивы фильтрации пакетов в windump;
5. Логические выражения в windump.

Рекомендуемая литература:

№ п/п	Автор(ы)	Заглавие	Издательство, год издания	Назначение, вид издания, гриф	Кол-во экз. в библиотеке
1.	В.Г. Олифер, Н.А. Олифер	Компьютерные сети. Принципы, технологии, протоколы	СПб.: Питер, 2010	Изложены принципы построения компьютерных сетей, вопросы создания крупных составных сетей и управления такими сетями; учебник для Вузов; Рекомендовано Министерством образования и науки Российской Фе-	8

				дерации	
2	Битнер В.И.	Принципы и протоколы взаимодействия телекоммуникационных сетей	М.: Горячая линии – Телеком, 2008	Изучаются специальные разделы курса; учебное пособие	15
3	Ю. Л. Муромцев [и др.].	Информационные технологии проектирования радиоэлектронных средств	М.: Академия, 2010	Приведены основные положения, классификация и характеристики информационных технологий (ИТ) и систем; с позиций системного подхода рассматриваются архитектура, принципы и тенденции развития ИТ; изложена методология автоматизированного проектирования радиоэлектронных средств (РЭС); учебное пособие	3
4	Пятибратов А.П., Гудыно Л.П., Кириченко А.А.; Под ред. А.П. Пятибратова	Вычислительные системы, сети и телекоммуникации	М. : КНОРУС, 2013	Изучаются специальные разделы курса; учебное пособие	5
5	Алекперов И.А. Большев А.К. Карпов К.Э. Кринкин К.В. Яновский В.В.	Исследование уровней организации IP-сетей	СПб.: Изд-во СПбГЭТУ "ЛЭТИ ", 2006	Лабораторный практикум	каф.ИРС