Лабораторная работа № 1

Цель: *изучение и практическое освоение основ адресации, разрешения физических адресов и простейшей маршрутизации в IP-сетях.*

Теоретические сведения

1. СЕТЕВОЙ УРОВЕНЬ: IP-АДРЕСАЦИЯ

Сетевой уровень (межсетевой уровень) модели TCP/IP служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и обладать произвольной топологией. На этом уровне термин сеть означает совокупность компьютеров, соединенных между собой в соотвествии с некой топологией и использующих физический уровень модели TCP/IP для передачи данных. Единицей данных сетевого уровня является пакет. На этом уровне определяются два вида протоколов – сетевые протоколы и протоколы маршрутизации. Первые реализуют продвижение пакетов

через сеть. Это такие протоколы как IP, ICMP, ARP и другие. Вторые – предоставляют способы обмена информацией о маршрутах. Кроме того, сетевой уровень TCP/IP, с помощью средств IP-адресации, решает важную задачу идентификации узла-получателя пакета.

1.1. Типы сетевых адресов

Каждый компьютер в сети TCP/IP имеет адреса двух типов:

- локальный (физический) адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети – это MAC-адрес сетевого адаптера или порта маршрутизатора. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта – идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, физический адрес назначается администратором глобальной сети. Пример физического адреса: 44-BC-89-A2-FE-00;
- IP-адрес, состоящий из 4 байт. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети определяет конкретную физическую сеть. Номер узла определяет конкретную рабочую станцию, сервер и пр., включенную в сеть. *Подсеть* – это физический сегмент TCP/IP сети, в котором используется IP-адреса с общим номером сети. Пример IP-адреса: 172.168.10.15.

Номер узла в протоколе IP назначается независимо от физического адреса узла. Деление IP-адреса на поле номера сети и номера узла – гибкое, и граница между этими полями может устанавливаться произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом IP-адрес характеризует не отдельный компьютер или маршрутизатор, а один сетевой интерфейс (физический или виртуальный). IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:
10.10.1.4 – традиционная десятичная форма представления адреса,

00001010 00001010 00000001 00000100 – двоичная форма представления этого же адреса.

1.2. Структура IP-адреса

Какая часть IP-адреса относится к номеру сети, а какая к номеру узла, определяется двумя способами: с помощью классов (классовая адресация) или с помощью масок подсети (бесклассовая адресация).

В классовой адресации номер сети и номер узла определяются по принадлежности IP-адреса одному из классов адресов: A,B,C,D или E. Класс определяется значениями первых битов адреса:

- если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей);
- если первые два бита адреса равны 10, то сеть относится к классу B. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта;
- если адрес начинается с последовательности 110, то это сеть класса C. Под адрес сети отводится 24 бита, а под адрес узла – 8 битов;
- если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес;
- если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В бесклассовой адресации номер сети к которому принадлежит узел с заданным IP-адресом определяется другим способом: вместе с IP-адресом нам предоставляется *маска подсети*. В терминологии сетей TCP/IP маской подсети или маской сети называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая к адресу самого узла в этой сети. Например, узел с IP-адресом 192.168.0.1 и маской подсети 255.255.255.0 находится в сети 192.168.0.0. Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции. Например:

```
IP-адрес:00001110111000001000100000000000000000000000001000000000000000010000
Маскаподсети:11111111110000000000000000000(255000.0.0)
Адрессети:00000000000000000000000000(1.0.0.)
```

Для стандартных классов сетей маски имеют следующие значения:

- 255.0.0.0 – маска для сети класса A;
- 255.255.0.0 – маска для сети класса B;
- 255.255.255.0 – маска для сети класса C.

1.3. Отображение физических адресов на логические

Отображение физических адресов на IP-адреса происходит с помощью протокола *ARP*. Функционирование ARP происходит различным образом, в зависимости от того, какой протокол канального уровня работает в данной сети. В локальных сетях протокол ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и осуществляет его широковещательную рассылку по сети. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свои IP-и локальный- адреса. ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети. Для того, чтобы не перегружать сеть запросами, ARP использует таблицу отображения (так называемый ARP-кэш). Эта таблица содержит три поля – IP-адрес, соответствующий ему MAC-адрес и тип. Тип может быть статическим или динамическим. Запись в таблице имеет динамический тип, если она внесена в таблицу путем широковещательного запроса ARP. Такие записи имеют время устаревания (обычно 180 или 360 секунд), после истечения которого они удаляются из таблицы. Запись в таблице будет иметь статический тип, если она добавлена вручную (например, с помощью команды arp в ОС Windows или Unix). Статическая запись имеет неограниченное время устаревания.

1.4. Маршрутизация по умолчанию

Для объединения подсетей в единую сеть в простейшем случае используется маршрутизация по умолчанию. Она организуется посредством шлюзов. Шлюзом будем называть узел внутри подсети, который предоставляет доступ в другую подсеть. Чаще всего в виде шлюза выступает маршрутизатор. Схема такой маршрутизации выглядит следующим образом: задан адрес *шлюза по умолчанию*. При

попытке отправки пакета в сеть, узел проверяет совпадение подсети назначения пакета с подсетью узла. Если подсети разные, то пакет отправляется на шлюз. В простейшем случае, шлюз сравнивает сеть IP-адреса назначения с номерами сетей на своих интерфейсах и в случае совпадения, направляет пакет узлу назначения через этот сетевой интерфейс. В противном случае он отправляет пакет узлу, указанному в качестве шлюза по умолчанию на самом шлюзе. Если такового нет, то пакет теряется.

1.5. Протокол ICMP

Для проверки соединений и корректного функционирования сети обычно используется *протокол ICMP* . ICMP – Internet Control Message Protocol, протокол управляющих сообщений интернета. ICMP – протокол сетевого уровня и работает поверх протокола IP. Он предназначен для обмена информацией об ошибках между маршрутизаторами (шлюзами) сети и узлом-источником пакета.С помощью специальных пакетов этот протокол сообщает о невозмодности доставки пакета, превышении времени жизни, аномальных значениях параметров, изменении маршрта пересылки, состоянии системы и т. п. В простейшем случае, для проверки работоспособности сети используются два сообщения ICMP: эхо-запрос (Echo request) и эхо-ответ (Echo reply). Когда на узел приходит сообщение ICMP типа эхо-запрос, он отправляет сообщение эхо-ответ на тот узел, с которого пришел запрос. Пример реализации такого обмена представлен в утилите ping, входящей в состав почти любой сетевой ОС.

Порядок выполнения работы

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. Объяснить результат.
5. Выполнить эхо-запрос на IP-адрес 200.100.0.1 с K1. Объяснить вывод программы.
6. Выполнить эхо запросы с K1 и K2 на все узлы сети. Убедиться, что эхо-ответы приходят.

В отчет необходимо включить схему сети, настройки протокола TCP/IP для все узлов сети и результаты вывода программы полученные при выполнении при эхо-запросов.

Варианты заданий

Вариант 1. Файл со схемой сети: lab1_var1.jfst. Сеть между маршрутизаторами R1,R2 и Boss_R: 117.168.0.0. Компьютер Boss имеет IP-адрес 64.2.0.1. Компьютер Hacker имеет IP-адрес 117.168.0.5.
Обозначения в задании: K1 – Boss, K2 – Hacker, K3 – OFFICE2 pc1.

Вариант 2. Файл со схемой сети: lab1_var2.jfst. Сеть между маршрутизаторами OFF_R и R2: 136.15.0.0. Компьютер BIG BOSS имеет IP-адрес 136.15.32.1. Компьютер M_CH_S имеет IP-адрес 10.10.0.2. Сеть между маршрутизаторами R2 и M_CH_S_Router: 192.178.0.0.
Обозначения в задании: K1 – BIG BOSS, K2 – M_CH_S, K3 – OFFICE1_pc4.

Вариант 3. Файл со схемой сети: lab1_var3.jfst. Сеть между маршрутизаторами R1,R2 и Boss_R: 172.198.0.0. Компьютер Boss имеет IP-адрес 10.2.0.1. Компьютер Hacker имеет IP-адрес 172.198.99.252.
Обозначения в задании: K1 – Boss, K2 – Hacker, K3 – OFFICE2_pc1.

Вариант 4. Файл со схемой сети: lab1_var4.jfst. Сеть между маршрутизаторами OFF_R и R2: 204.188.0.0. Компьютер BIG BOSS имеет IP-адрес 204.188.0.1. Компьютер M_CH_S имеет IP-адрес 10.0.0.2. Сеть между маршрутизаторами R2 и M_CH_S_Router: 192.178.0.0.
Обозначения в задании: K1 – BIG BOSS, K2 – M_CH_S, K3 – OFFICE1_pc4.

Вариант 5. Файл со схемой сети: lab1_var5.jfst. Сеть между маршрутизаторами RServers, RManagers и RBosses: 10.0.0.0. Компьютер MegaBoss имеет IP-адрес 172.16.0.5. Компьютер Manager2 имеет IP-адрес 172.16.1.12. Компьютер FileServer имеет IP-адрес 172.16.10.10.
Обозначения в задании: K1 – MegaBoss, K2 – Manager2, K3 – File-Server.

Вариант 6. Файл со схемой сети: lab1_var6.jfst. Сеть между маршрутизаторами RServers, RManagers и RBosses: 192.168.0.0. Компьютер MicroBoss имеет IP-адрес 10.0.1.5. Компьютер Manager3

имеет IP-адрес 10.0.2.5. Компьютер PrintServer имеет IP-адрес 10.0.64.1.
Обозначения в задании: K1 – Manager3, K2 – PrintServer, K3 – Micro-Boss.

Вариант 7. Файл со схемой сети: lab1_var7.jfst. Сеть между маршрутизаторами R1 и ADSL: 172.168.0.0. Компьютер Station1 имеет IP-адрес 172.168.1.2. Компьютер Remote1 имеет IP-адрес 10.0.0.110. Сеть между маршрутизаторами ADSL и ADSL2: 192.168.0.0.
Обозначения в задании: K1 – Station1, K2 – Remote1, K3 – Station2.

Вариант 8. Файл со схемой сети: lab1_var8.jfst. Сеть между маршрутизаторами R1 и ADSL: 192.168.0.0. Компьютер Station1 имеет IP-адрес 192.168.1.2. Компьютер Remote1 имеет IP-адрес 99.11.0.11. Сеть между маршрутизаторами ADSL и ADSL2: 172.168.0.0.
Обозначения в задании: K1 – Station1, K2 – Remote1, K3 – Station2.

Вариант 9. Файл со схемой сети: lab1_var9.jfst. Сеть между маршрутизаторами R1 и R2: 192.168.100.0. Компьютер PC1 имеет IP-адрес 129.64.128.1. Компьютер PC2 имеет IP-адрес 129.64.127.254. Компьютер PC4 имеет IP-адрес: 10.0.0.2. Длина маски подсети (количество значащих единиц) на PC1, PC2, PC3 должно быть минимально возможным (обеспечивая при этом корректную работу).
Обозначения в задании: K1 – PC1, K2 – PC2, K3 – PC3.

Вариант 10. Файл со схемой сети: lab1_var10.jfst. Сеть между маршрутизаторами R1 и R2: 192.168.0.0. Компьютер PC1 имеет IP-адрес 172.168.0.1. Компьютер PC2 имеет IP-адрес 172.168.0.2. Компьютер PC4 имеет IP-адрес: 1.0.0.2.
Обозначения в задании: K1 – PC1, K2 – PC2, K3 – PC3.

Вариант 11. Файл со схемой сети: lab1_var11.jfst. Сеть между маршрутизаторами R-C-M и R-S-C: 10.1.0.0. Сеть между маршрутизаторами R-C-M и R-M-S: 10.0.32.0. Сеть между маршрутизаторами R-M-S и R-S-C: 10.0.0.128. Компьютер Chief имеет IP-адрес 10.1.0.3. Компьютер Manager1 имеет IP-адрес 10.0.32.11. Компьютер Service имеет IP-адрес: 10.0.0.135.
Обозначения в задании: K1 – Chief, K2 – Manager1, K3 – Service.

Вариант 12. Файл со схемой сети: lab1_var12.jfst. Сеть между маршрутизаторами R-C-M и R-S-C: 172.168.128.0. Сеть между маршрутизаторами R-C-M и R-M-S: 172.168.1.0. Сеть между маршрутизаторами R-M-S и R-S-C: 172.168.0.64. Компьютер Chief имеет IP-адрес 172.168.128.5. Компьютер Manager3 имеет IP-адрес 172.168.1.13. Компьютер Service имеет IP-адрес: 172.168.0.76.
Обозначения в задании: K1 – Manager3, K2 – Service, K3 – Chief.

Вариант 13. Файл со схемой сети: lab1_var13.jfst. Сеть между

маршрутизаторами R120, R230 и R232: 172.31.128.0. Сеть между маршрутизаторами R232 и R233: 10.10.0.0. Компьютер Remote1 имеет IP-адрес 172.31.127.0. Компьютер Remote2 имеет IP-адрес 172.31.200.1. Компьютер Remote3 имеет IP-адрес: 10.0.39.0.
Обозначения в задании: K1 – Remote1, K2 – Remote2, K3 – Remote3.
Вариант 14. Файл со схемой сети: lab1_var14.jfst. Сеть между маршрутизаторами R120, R230 и R232: 63.12.95.0. Сеть между маршрутизаторами R232 и R233: 63.12.225.0. Компьютер Remote1 имеет IP-адрес 168.20.88.0. Компьютер Remote2 имеет IP-адрес 63.12.95.1. Компьютер Remote3 имеет IP-адрес: 168.20.120.0.
Обозначения в задании: K1 – Remote2, K2 – Remote3, K3 – Remote1.

Пример выполнения лабораторной работы

Рассмотрим конфигурацию сети, приведенную на рисунке 1.1. Файл со схемой сети: lab1_sample.jfst. Сеть между маршрутизаторами R1 и R2: 172.168.100.0. Компьютер PC1 имеет IP-адрес 172.168.0.2. Компьютер PC2 имеет IP-адрес 10.0.0.2.

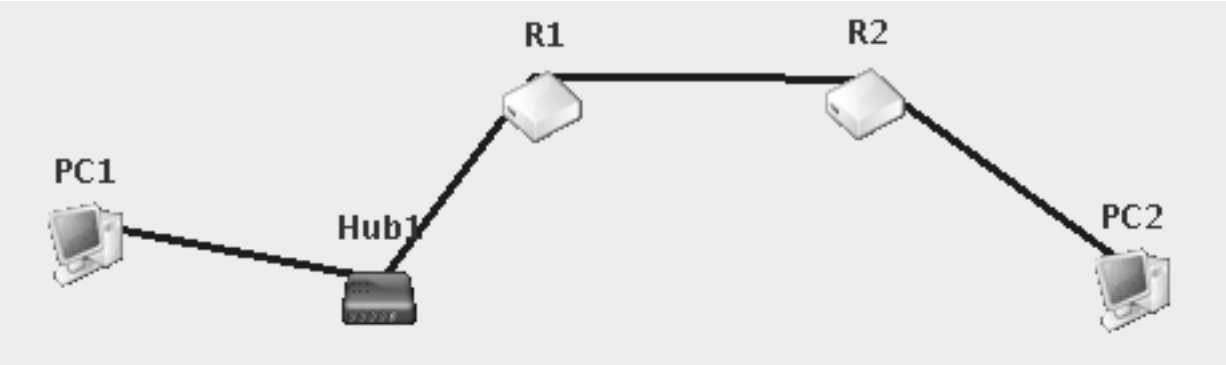

Рис. 1.1 Схема сети

Задание:

1. Задать маски подсети и шлюзы по умолчанию для PC1 и PC2, а также IP-адреса из заданного диапазона вместе с масками и шлюзами для R1 и R2 так, чтобы обеспечить корректную доставку эхо-запроса от PC1 к PC2 и эхо-ответа обратно. Обосновать свои установки.
2. Выполнить эхо-запрос с PC1 на PC2. Проанализировать вывод программы.
3. Выполнить эхо-запрос на IP-адрес 192.168.0.1 с PC1. Объяснить вывод программы.

Порядок выполнения будет следующим:

1. Зададим IP-адреса и маски подсети для маршрутизаторов R1 и

R2. Как видно, сети 172.168.100.0 и 172.168.0.0 (если использовать стандартную маску подсети для класса B) эквивалентны. Будем использовать маску подсети, отличную от стандартной. Зададим для маршрутизатора R1 на интерфейсе eth0 адрес 172.168.0.1 и маску подсети 255.255.255.0. На интерфейсе eth1 установим адрес 172.168.100.1 и маску 255.255.255.0. Теперь необходимо сконфигурировать маршрутизатор R2. На его интерфейсе eth0 зададим IP 172.168.100.2 и маску 255.255.255.0. Установим шлюз по умолчанию в 172.168.100.1. На интерфейсе eth1 для R2 установим любой IP-адрес из диапазона сети PC2, например 10.0.0.1 и соответствующую ему маску: 255.0.0.0. Для корректной маршрутизации осталось задать только шлюз по умолчанию для R1. Он будет адресом маршрутизатора R2.

2. Теперь настроим конечные узлы. На PC1 зададим маску подсети соответствующую новому адресному пространству – 255.255.255.0. Так как пакеты от узла PC1 в другие сети должны проходить через маршрутизатор R1, зададим шлюз по умолчанию 172.168.0.1 (адрес R1). Аналогичные операции проведем на PC2 – установим маску подсети в 255.0.0.0, а шлюз по умолчанию в 10.0.0.1. Стоит заметить, что приведенная конфигурация не является единственно верной.
3. После отправки эхо-запроса с PC1 на PC2 в консоли будет выведен результат прохождения запроса и ответа на него по сети:

```
PPPCCC111CCCrrreeeaaattteeedddEchoRequestpacketttto10.0.0.2
          ARPdiscoverypacketosourceMACaddress.
     forIP172.168.0.1
PC1Sendingbroadcastpacketfromprotocolstack.
...
PPPCCC111ProtocolStaaacccckkkreceivedpackeeetttfromlocalInterface.
   ConfirmedPeeetttisforthisN
workLayerDevice.PC1Echoreplypack
receivedfrom10.0.0.2
```

   Как видно, PC1 успешно получил эхо-ответ на свой запрос к PC2.
4. Выполним эхо-запрос для несуществующего узла с IP-адресом 192.168.0.1. Для этого выполним на PC1 последовательность действий, аналогичную предыдущему пункту, вместо адреса 10.0.0.2 используя адрес 192.168.0.2:

```
PPPCCC111CreatedEchoRequestpacketto192.168.0.1
   SendingpacketfromProtocolStack(to172.168.0.1).
...
R1ProtocolStackreceivedpacketfromlocalInterface.
```

```
R1PacketReceived:NetworkLayerDeviceis
     Routableforwardingpacket.
R1ForwardingpacketfromProtocolStack
     (to172.168.100.1).
      rotocolStackreceivedpacketfromlocalInterface.
RRR222PPPacketDropped:Hopcountexceeded.
Host192.168.0.2Unreachable
```

Как видно, пакет попал в "петлю" между двумя маршрутизаторами и находился там, пока у него не закончилось время жизни (TTL).

Контрольные вопросы

1. Что такое кэш ARP? Какие типы записей могут содержаться в кэше ARP?
2. Какому классу IP-адресов принадлежат адреса 10.11.0.1, 127.1.1.1?
3. Разделите адресное пространство 192.168.1.0 на 4 подсети при помощи масок.
4. Что такое концентратор? Объясните принцип работы концентратора. Чем концентратор отличается от повторителя?
5. Что такое шлюз?
6. Для чего предназначен протокол ICMP?