Лабораторная работа № 4

Изучение маршрутизации IP

**Цель работы:** Изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети

**Оборудование:** персональный компьютер, включенный в сеть IP, Microsoft Windows

# Основные понятия

[Сетевой уровень](file:///%5C%5CAsubru%5CWebAsu%5C%D0%A3%D1%87%D0%B5%D0%B1%D0%BD%D0%BE-%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5%20%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%B0%D0%BB%D1%8B%5C%D0%94%D0%B8%D1%81%D1%86%D0%B8%D0%BF%D0%BB%D0%B8%D0%BD%D1%8B%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D1%8B%5C%D0%A3%D0%9C%D0%9A_2018_%D0%A0%D0%91%5C_%D0%A1%D0%B5%D1%82%D0%B8%20%D0%AD%D0%92%D0%9C%20%D0%B8%20%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B9%5CAPOS-2006-11-%D0%9B%D0%B0%D0%B1%D0%A0%D0%B0%D0%B1%5Ccontent%5Clab3.htm#z01) отвечает за возможность доставки пакетов по сети передачи данных – совокупности сегментов сети, объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов TCP/IP» означает «набор протоколов, связанных с IP и TCP(протоколом транспортного уровня)».

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи.

Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети. Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами.

Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий шлюз (шлюз подключен к подсети также как обычный узел). Шлюз (gateway)– любое сетевое оборудование с несколькими сетевыми интерфейсами и осуществляющее продвижение пакетов между сетями на уровне протоколов сетевого уровня.

Из шлюза пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель; там пакет направляется к получателю.

Таким образом, шлюз выполняет маршрутизацию – процедуру нахождения в структуре сети пути достижения получателя (построение пути доставки пакетов).

Если хост подключен к нескольким сетям, он должен иметь несколько сетевых адресов, как минимум столько, сколько каналов к нему подключено.

Даже если хост не является шлюзом между подсетями, все равно в нем присутствует таблица маршрутизации, ведь любой хост должен отправлять пакеты напрямую членам своей подсети, через какой-то шлюз другим подсетям и не передавать в сеть пакеты, предназначенные самому себе (заворачивать их по внутренней петле 127.0.0.1).

# Правила маршрутизации

Правила маршрутизации определяют куда и как должны посылаться пакеты для разных сетей.

Каждое правило состоит из следующих компонентов:

1. Начальный адрес подсети, порядок достижения которой описывает правило.
2. [Маска](file:///%5C%5CAsubru%5CWebAsu%5C%D0%A3%D1%87%D0%B5%D0%B1%D0%BD%D0%BE-%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5%20%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%B0%D0%BB%D1%8B%5C%D0%94%D0%B8%D1%81%D1%86%D0%B8%D0%BF%D0%BB%D0%B8%D0%BD%D1%8B%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D1%8B%5C%D0%A3%D0%9C%D0%9A_2018_%D0%A0%D0%91%5C_%D0%A1%D0%B5%D1%82%D0%B8%20%D0%AD%D0%92%D0%9C%20%D0%B8%20%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B9%5CAPOS-2006-11-%D0%9B%D0%B0%D0%B1%D0%A0%D0%B0%D0%B1%5Ccontent%5Clab3.htm#z03) подсети, которую описывает правило.
3. Шлюз показывает, на какой адрес будут посланы пакеты, идущие в сеть назначения. Если пакеты будут идти напрямую, то указывается собственный адрес (точнее тот адрес того канала, через который будут передаваться пакеты).
4. Интерфейс показывает через какой сетевой адаптер (его номер или IP адрес) должен посылаться пакет в заданную сеть;
5. Метрика показывает время за которое пакет может достигнуть сети получателя (величина условная и может быть изменена при маршрутизации). Если имеется несколько правил достижения одной сети, пакеты посылаются по правилу с наименьшей метрикой.

Применение правила заключается в определении, принадлежит ли хост назначения сети, указанной в правиле, и если принадлежит, то пакет отправляется на адрес шлюза через интерфейс.

Правила маршрутизации сведены в таблицу маршрутизации (где расположены по степени уменьшения маски), которую можно посмотреть с помощью команды ROUTE PRINT.

Правила применяются в порядке уменьшения масок.

Правила с равными масками применяются в порядке увеличения метрики.

# Пример таблицы маршрутизации

Рассмотрим таблицу маршрутизации, имеющую следующий вид:

| Сетевой адрес | Маска сети | Адрес шлюза | Интерфейс | Метрика |
| --- | --- | --- | --- | --- |
| 0.0.0.0 | 0.0.0.0 | 192.168.200.1 | 192.168.200.47 | 30 |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 192.168.192.0 | 255.255.240.0 | 192.168.200.47 | 192.168.200.47 | 30 |
| 192.168.200.47 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 30 |
| 192.168.200.255 | 255.255.255.255 | 192.168.200.47 | 192.168.200.47 | 30 |
| 224.0.0.0 | 240.0.0.0 | 192.168.200.47 | 192.168.200.47 | 30 |
| 255.255.255.255 | 255.255.255.255 | 192.168.200.47 | 192.168.200.47 | 1 |

Проанализируем вышеприведенную таблицу маршрутизации, пересортировав правила:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Сетевой адрес | Маска сети | Адрес шлюза | Интерфейс | Метрика |
| 255.255.255.255 | 255.255.255.255 | 192.168.200.47 | 192.168.200.47 | 1 |
| 192.168.200.47 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 30 |
| 192.168.200.255 | 255.255.255.255 | 192.168.200.47 | 192.168.200.47 | 30 |
| 192.168.192.0 | 255.255.240.0 | 192.168.200.47 | 192.168.200.47 | 30 |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 224.0.0.0 | 240.0.0.0 | 192.168.200.47 | 192.168.200.47 | 30 |
| 0.0.0.0 | 0.0.0.0 | 192.168.200.1 | 192.168.200.47 | 30 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 255.255.255.255 | 255.255.255.255 | 192.168.200.47 | 192.168.200.47 | 1 |

Обратите внимание на маску сети в первом правиле. Она описывает подсеть размером в 1 хост с адресом 255.255.255.255 – это широковещательный адрес. Пакеты будут посылаться на адрес 192.168.200.47 через интерфейс 192.168.200.47. Это наш адрес, т.е. пакеты будут отправляться напрямую.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 192.168.200.255 | 255.255.255.255 | 192.168.200.47 | 192.168.200.47 | 30 |

Опять широковещательный адрес. Смотри предыдущий комментарий.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 192.168.200.47 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 30 |

Опять такая же маска, но адрес нашего хоста. Отправлять будем через внутреннюю петлю.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 192.168.192.0 | 255.255.240.0 | 192.168.200.47 | 192.168.200.47 | 30 |

А вот и наша подсеть. Отправляем напрямую.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |

Все, что начинается со 127, отправляем через внутреннюю петлю.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 224.0.0.0 | 240.0.0.0 | 192.168.200.47 | 192.168.200.47 | 30 |

Класс D – отправляем напрямую.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0.0.0.0 | 0.0.0.0 | 192.168.200.1 | 192.168.200.47 | 30 |

Самое интересное правило. Маска покрывает ВСЕ возможные адреса! Пакеты отправляются через наш интерфейс на адрес 192.168.200.1. Правило применяется последним, поэтому его можно озвучить так: по всем адресам, которые не подошли по предыдущим правилам, пакеты отправляем на адрес 192.168.200.1. Такой адрес обычно имеется в любой сети и называется шлюзом по умолчанию (default gateway). Этот адрес скрывает от хостов и пользователей структуру сети и позволяет упростить таблицы маршрутизации и снять нагрузку с хостов, перенеся маршрутизацию на специально выделенные шлюзы – маршрутизаторы.

Нетрудно догадаться, что все адреса в колонке Адрес шлюза должны достигаться напрямую, т.е. входить в нашу подсеть.

# Разбиение сети на подсети

Одной из основных задач, стоящих при проектировании сетей, является распределение по подсетям сетевых адресов из заданного диапазона, т.е. разделение сети на подсети.

При разделении сети на подсети следует учитывать следующие правила:

1. Размер подсетей должен быть степенью двойки.
2. Имеются запрещенные адреса.
3. Начальный адрес подсети должен быть кратен ее размеру.

В качестве шлюза по умолчанию можно использовать любой узел, но, исходя из увеличения пропускной способности сети и уменьшения времени передачи пакетов, следует в качестве шлюза по умолчанию использовать либо ближайший узел, либо узел, соединенный с максимальным количеством сетей, т.е. следует учитывать топологию сети.

# Программа ROUTE

Для работы с таблицами маршрутизации в составе ОС имеется программа route (упоминалась ранее). Выводит на экран и изменяет записи в локальной таблице IP-маршрутизации.

route [-f] [-p] [команда [конечная\_точка] [mask маска\_сети] [шлюз] [metric метрика]] [if интерфейс]]

Параметры:

-f – Очищает таблицу маршрутизации от всех записей, которые не являются узловыми маршрутами (маршруты с маской подсети 255.255.255.255), сетевым маршрутом замыкания на себя (маршруты с конечной точкой 127.0.0.0 и маской подсети 255.0.0.0) или маршрутом многоадресной рассылки (маршруты с конечной точкой 224.0.0.0 и маской подсети 240.0.0.0). При использовании данного параметра совместно с одной из команд (таких, как add, change или delete) таблица очищается перед выполнением команды.

-p – При использовании данного параметра с командой add указанный маршрут добавляется в реестр и используется для инициализации таблицы IP-маршрутизации каждый раз при запуске протокола TCP/IP. При использовании параметра с командой print выводит на экран список постоянных маршрутов. Все другие команды игнорируют этот параметр.

команда – Указывает команду, которая будет запущена на удаленной системе. В следующей таблице представлен список допустимых параметров.

|  |  |
| --- | --- |
| Команда | Назначение      |
| Add | Добавление маршрута |
| change | Изменение существующего маршрута |
| Delete | Удаление маршрута или маршрутов |
| Print | Печать маршрута или маршрутов |

конечная\_точка – Определяет конечную точку маршрута. Конечной точкой может быть сетевой IP-адрес (где разряды узла в сетевом адресе имеют значение 0), IP-адрес маршрута к узлу, или значение 0.0.0.0 для маршрута по умолчанию.

mask маска\_сети – Указывает маску сети в соответствии с точкой назначения. Маска сети может быть маской подсети соответствующей сетевому

шлюз – Указывает IP-адрес пересылки или следующего перехода, по которому доступен набор адресов, определенный конечной точкой и маской подсети

metric метрика – Задает целочисленную метрику стоимости маршрута (в пределах от 1 до 9999) для маршрута, которая используется при выборе в таблице маршрутизации одного из нескольких маршрутов, наиболее близко соответствующего адресу назначения пересылаемого пакета.

if интерфейс – Указывает индекс интерфейса, через который доступна точка назначения. В случае, когда параметр if пропущен, интерфейс определяется из адреса шлюза.

/? – Отображает справку в командной строке.

# Задания для выполнения

* 1. С помощью программы route print посмотрите таблицу маршрутизации Вашего компьютера. Объясните все правила.
	2. Посмотрите таблицу маршрутизации хоста, имеющего несколько каналов. Объясните все правила.
	3. Посмотрите таблицу маршрутизации маршрутизатора. Объясните все правила.
	4. Добавьте новое правило в таблицу маршрутизации для сети 192.168.0.0/24 через шлюз в вашей сети с последним байтом в адресе 125 и метрикой 12.
	5. Удалите это правило.
	6. В соответствии с таблицей и схемами выполните задание на распределение адресов по подсетям (согласно варианта). Постройте таблицы маршрутизации для всех шлюзов и для одного хоста для каждого сегмента.

|  |  |  |
| --- | --- | --- |
| №Варианта | Количество хостов в подсети | Диапазон адресов |
| A | B | C | D | E | от | до |
| 1 | 5 | 10 | 20 | 15 | 50 | 10.0.20.0 | 10.0.20.255 |
| 2 | 20 | 15 | 6 | 70 | 25 | 192.168.0.0 | 192.168.0.255 |
| 3 | 15 | 25 | 5 | 40 | 5 | 112.38.25.128 | 112.38.25.255 |
| 4 | 24 | 32 | 8 | 10 | 2 | 196.13.49.0 | 196.13.49.128 |
| 5 | 50 | 16 | 64 | 20 | 15 | 68.76.115.0 | 68.76.115.255 |
| 6 | 40 | 6 | 10 | 12 | 5 | 211.3.45.0 | 211.3.45.128 |



* 1. Разделите сеть, состоящую из трех сегментов, имеющую диапазон адресов 192.168.0.32 – 192.168.0.159 на подсети, содержащие 64, 20 и 44 хостов (включая шлюзы).

# Контрольные вопросы

1. Сколько адресов может иметь хост?
2. Может ли у хоста быть прописано несколько шлюзов и почему?
3. Может ли у хоста быть прописано несколько шлюзов по умолчанию и почему?
4. Чем отличаются таблицы у разных классов сетевых устройств и почему?
5. Почему начальный адрес подсети должен быть кратен ее размеру?
6. Чем Вы руководствовались при выборе шлюзов по умолчанию?
7. Может ли физический сегмент сети содержать несколько сетевых подсетей?