Г.П. Коломоец

# ОРГАНИЗАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие

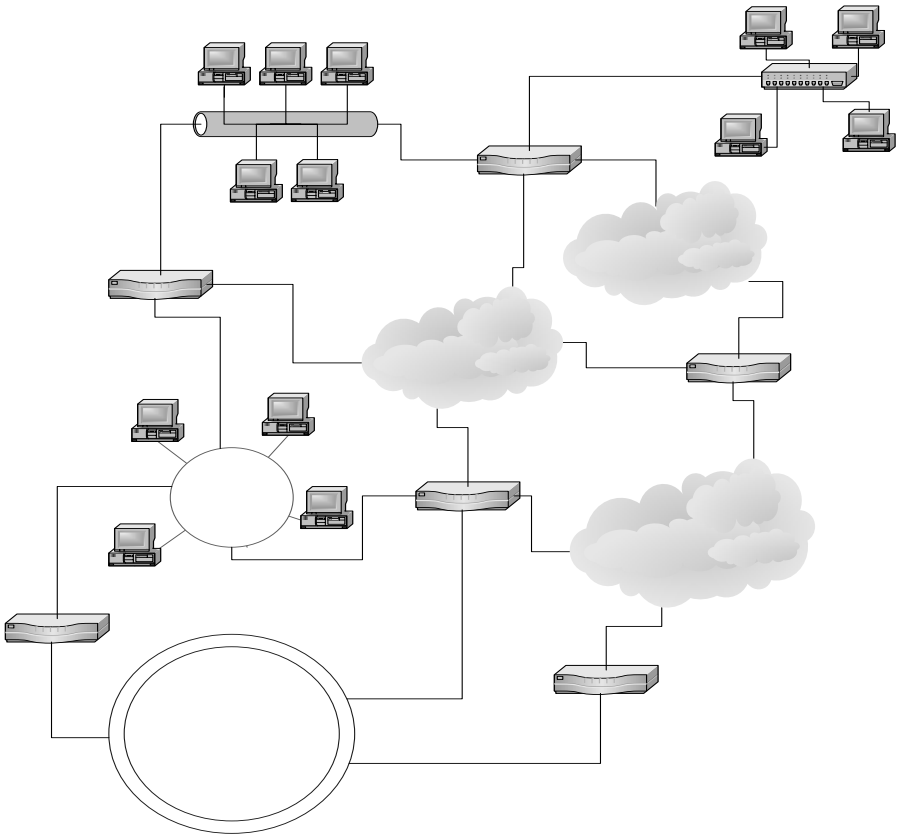
Запорожье
2012

КЛАССИЧЕСКИЙ ПРИВАТНЫЙ УНИВЕРСИТЕТ

**Г.П. Коломоец**

# ОРГАНИЗАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие



Запорожье
Классический приватный университет
2012

УДК 004.7
ББК 32.973.202
К 61

Утверждено к печати ученым советом
Классического приватного университета
протокол № 1 от 21 сентября 2011 г.

*Рецензенты:*
**Д.М. Пиза**, доктор технических наук, профессор,
директор Института информатики и радиоэлектроники,
Запорожский национальный технический университет;
**С.Ю. Борю**, кандидат технических наук, доцент,
зав. кафедрой информационных технологий,
Запорожский национальный университет.

**Коломоец Г.П.**
К 61 Организация компьютерных сетей : учебное пособие / Г.П. Коломоец. – Запорожье : КПУ, 2012. – 156 с.
ISBN 978-966-414-162-5

В учебном пособии изложены теоретические сведения и пошаговые практические рекомендации по организации локальных компьютерных сетей. Наряду с постановкой экспериментов в реальных сетях предлагается использование программного обеспечения, позволяющего моделировать структуру и изучать процессы в компьютерной сети. Практические вопросы конфигурирования сетевых интерфейсов и работы с утилитами рассмотрены с использованием кроссплатформенного подхода.

Предназначено для студентов и преподавателей, обучающихся и работающих по направлениям и специальностям отрасли знаний 0501 "Информатика и вычислительных техника".

**УДК 004.7**
**ББК 32.973.202**

**ISBN 978-966-414-162-5**

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ ..... 5
РАЗДЕЛ 1 ПОСТРОЕНИЕ И НАСТРОЙКА ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ ..... 7
1.1. Общая структура и оборудование локальной компьютерной сети 7
1.2. Конфигурирование сетевых средств операционных систем компьютеров локальной сети ..... 15
1.3. Моделирование и исследование работы локальной сети ..... 20
Задание для самостоятельной работы ..... 32
Вопросы для самоподготовки ..... 34
Тесты для контроля усвоения знаний ..... 35
Литература ..... 39
РАЗДЕЛ 2 ОРГАНИЗАЦИЯ СОВМЕСТНО ИСПОЛЬЗУЕМЫХ СЕТЕВЫХ РЕСУРСОВ ..... 40
2.1. Компоненты организации сетевого доступа и сетевые разрешения ..... 40
2.2. Организация сетевого доступа к каталогам (папкам) в Windows 46
2.3. Организация совместного использования по сети принтера в Windows ..... 50
2.4. Использование `net`-команд Windows ..... 55
2.5. Организация сетевого доступа к каталогам (папкам) в Linux ..... 58
2.6. Организация совместного использования по сети принтера в Linux ..... 61
Вопросы для самоподготовки ..... 63
Тесты для контроля усвоения знаний ..... 65
Литература ..... 66
РАЗДЕЛ 3 АНАЛИЗ КАДРОВ ETHERNET С ПОМОЩЬЮ АНАЛИЗАТОРА СЕТЕВЫХ ПРОТОКОЛОВ ..... 68
3.1. Сетевая технология Ethernet и форматы кадров данных ..... 68
3.2. Анализаторы сетевых протоколов ..... 74
3.3. Исследование протокола разрешения адреса ARP ..... 76
3.4. Изучение принципа работы коммутатора Ethernet ..... 78
Задание для самостоятельной работы ..... 79
Вопросы для самоподготовки ..... 88
Тесты для контроля усвоения знаний ..... 89
Литература ..... 91

РАЗДЕЛ 4 ИЗУЧЕНИЕ ПРОТОКОЛА IP И ТЕХНОЛОГИИ МАРШРУТИЗАЦИИ ..... 92
4.1. Адресация хостов, сетей и подсетей с использованием IP ..... 92
4.2. Маршрутизация IP-дейтаграмм ..... 102
4.3. Формат заголовка IP-пакета ..... 108
Задание для самостоятельной работы ..... 111
Вопросы для самоподготовки ..... 116
Тесты для контроля усвоения знаний ..... 117
Литература..... 119
РАЗДЕЛ 5 ИССЛЕДОВАНИЕ РАБОТЫ ПРОТОКОЛА УПРАВЛЯЮЩИХ СООБЩЕНИЙ ИНТЕРНЕТ ICMP И ПРОТОКОЛОВ ТРАНСПОРТНОГО УРОВНЯ UDP И TCP..... 120
5.1. Протокол управляющих сообщений Интернет ICMP ..... 120
5.2. Общая характеристика протоколов транспортного уровня стека TCP/IP ..... 122
5.3. Протокол пользовательских дейтаграмм UDP..... 126
5.4. Протокол управления транспортом TCP ..... 127
Задание для самостоятельной работы ..... 133
Вопросы для самоподготовки ..... 139
Тесты для контроля усвоения знаний ..... 140
Литература..... 141
СЛОВАРЬ ТЕРМИНОВ..... 143
РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА..... 150
ПРИЛОЖЕНИЕ А ..... 151

# ВВЕДЕНИЕ

Компьютерные сети сегодня являются привычным инструментом коммуникаций, информационного обмена и выполнения вычислений. Одновременно организация сетей, принципы их функционирования и правила конфигурирования не являются простыми и требуют от специалистов, выполняющих проектирование, построение и администрирование компьютерных сетей, определенных теоретических знаний и обязательного практического опыта.

При изучении дисциплин, связанных с организацией компьютерных сетей, перед студентами возникают несколько проблем. Во-первых, для выполнения большинства практических задач и экспериментов необходима сеть, объединяющая несколько компьютеров и сетевых устройств, которая не всегда доступна (например, в домашних условиях). Во-вторых, в университетских лабораториях студенты часто работают с ограниченными правами на выполнение действий в операционных системах, что не позволяет выполнять конфигурирование операционных систем и устройств. И в-третьих, очень часто лаборатории не оснащены (или не оснащены достаточно, чтобы с ними могли работать студенты) сетевыми устройствами, которые опять же можно конфигурировать только с административными полномочиями. Если к этому добавить очень малое время аудиторной работы и довольно большое время самостоятельной работы студентов, предусмотренное программами обучения в вузах Украины, то становится понятным, что использование программ моделирования структуры и процессов в компьютерных сетях является очень ценным и важным дополнением к практическому обучению в лабораториях.

Примерно десять лет назад автор познакомился с программным обеспечением *NetSim* разработки фирмы *Boson*, которое использовали для обучения слушателей в региональной сетевой академии *Cisco* в Тернопольском национальном техническом университете. С тех пор это программное обеспечение использовалось автором при преподавании дисциплин, связанных с компьютерными сетями. Недостатком программы была исключительная ориентация на Windows, а также коммерческий характер, что позволяло использовать только её ограниченные демо-версии. С недавних пор ведущая компания в области создания сетевых устройств *Cisco Systems* разработала для нужд своих академий программы *Cisco Packet Tracer*, которое превышает функциональность *Boson NetSim*, существуют его версии для Windows и Linux, и оно не является коммерческим. В данном пособии это программное обеспечение используется наряду с работой в реальных сетях и, по мнению автора, позволяет лучше понять принципы организации и функционирования компьютерных сетей.

Также важным, по мнению автора, является изучение компьютерных сетей с использованием программ-анализаторов протоколов, которые позволяют выполнять анализ структур данных, определяемых сетевыми протоколами разных уровней. В качестве такой программы в пособии предла-

гается свободно распространяемое кроссплатформенное программное обеспечение Wireshark.

Материал учебного пособия охватывает канальный, сетевой и транспортный уровни модели сетевого взаимодействия (ПРИЛОЖЕНИЕ А), поскольку именно эти уровни в основном отвечают за организацию компьютерных сетей.

Цель данного учебного пособия: содействовать подготовке специалистов, обладающих знаниями по общим принципам функционирования, стандартным протоколам и технологиям построения компьютерных сетей.

Основные компетенции пособия: дать студентам знания о принципах построения и функционирования компьютерных сетей, основных технологиях и оборудовании передачи данных, протоколах информационного обмена и сетевых возможностей операционных систем.

В результате изучения данного пособия студент должен

**получить теоретические знания в области:**

– основных стандартов и спецификаций компьютерных сетей;

– алгоритмов функционирования сетевых технологий, структуры локальных и глобальных компьютерных сетей;

– основных типов аппаратных компонентов компьютерных сетей;

– современных сетевых средств операционных систем и сетевого программного обеспечения;

**получить следующие практические навыки:**

– выполнять структурный анализ компьютерных сетей и анализировать кадры и пакеты, переносящие информацию в сетях;

– подбирать необходимые сетевые аппаратные компоненты и выполнять их настройки;

– конфигурировать стеки сетевых протоколов операционных систем и применять сетевое программное обеспечение для мониторинга и управления сетями.

# РАЗДЕЛ 1
# ПОСТРОЕНИЕ И НАСТРОЙКА ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ

## 1.1. Общая структура и оборудование локальной компьютерной сети

*Локальная компьютерная сеть* (*Local Area Network – LAN*) представляет собой набор компьютеров (часто называемых *рабочими станциями* (*Workstation*)), серверов, сетевых принтеров, коммутаторов (Switch), маршрутизаторов (Router), точек доступа (Access Point), другого оборудования, а также соединяющих их кабелей, обычно расположенных на относительно небольшой территории или в небольшой группе зданий (учебный класс, квартира, офис, университет, дом, фирма, предприятие) (рис. 1).

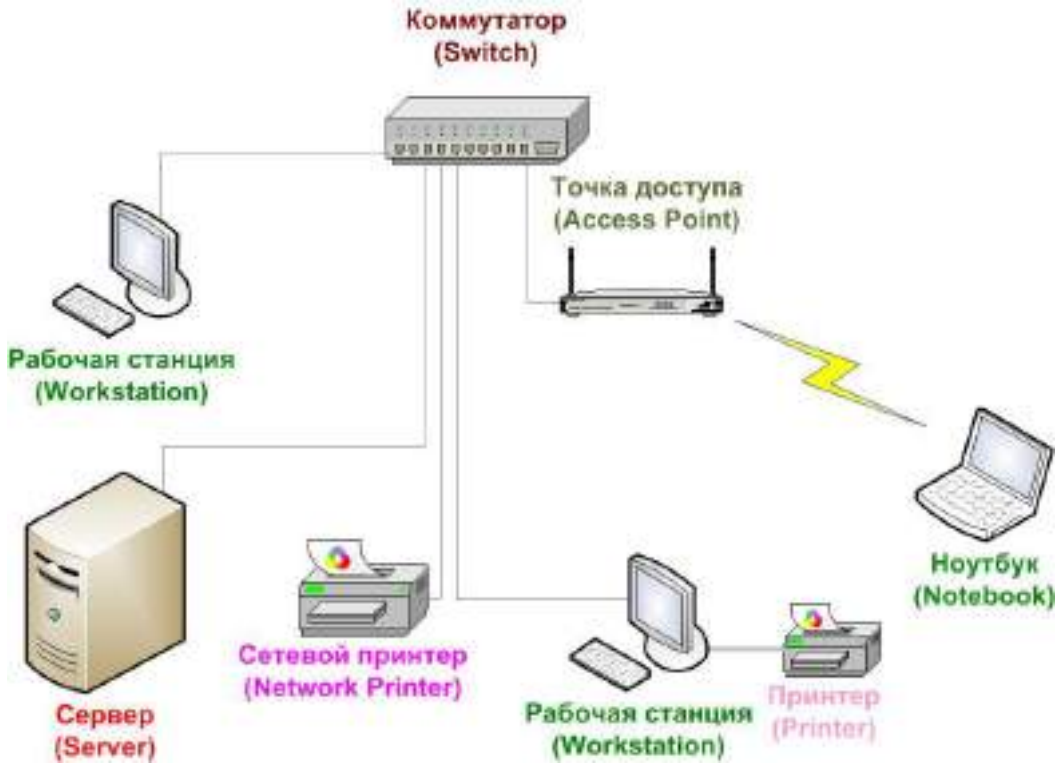



Рис. 1. Структура простейшей локальной компьютерной сети

В локальной сети можно выделить:

– оконечное оборудование пользователей, поставляющее данные в сеть и принимающее данные для обработки (рабочие станции, серверы, ноутбуки, сетевые принтеры и др.);

– активное сетевое оборудование, организующее каналы для передачи информации между оконечным оборудованием пользователей в структурах данных, называемых пакетами, кадрами, сообщениями (коммутаторы, маршрутизаторы, концентраторы, точки доступа, модемы и др.);

– пассивное сетевое оборудование, представляющее собой кабели, кабельные каналы (короба), разъёмы, розетки и другое соединительное оборудование, а также стойки и подставки для размещения активного сетевого оборудования.

Для организации работы локальной компьютерной сети необходимо:

а) выполнить физическое построение компьютерной сети:
   - установить в оконечное оборудование пользователей *сетевые интерфейсные адаптеры* (*Network Interface Card – NIC*) (рис. 2) (данный этап обычно пропускается, так как современные материнские платы оснащаются встроенными NIC);
   - подобрать и разместить активное сетевое оборудование;
   - выполнить соединение сетевых интерфейсных адаптеров в оконечном оборудовании пользователей и разъёмов активного сетевого оборудования с помощью кабелей и разъёмов (кабели и разъёмы не используются при организации беспроводного соединения).

б) настроить параметры набора (стека) сетевых протоколов на оконечном оборудовании пользователей: задать сетевые имена устройств и адреса, установить требуемые параметры сетевых протоколов;

в) выполнить работы по организации совместно используемых сетевых ресурсов и по предоставлению доступа к этим ресурсам пользователей сети.

г) установить необходимое сетевое программное обеспечение (дополнительное к входящему в состав операционных систем).


Рис. 2. Сетевой интерфейсный адаптер и его основные компоненты

Сетевые интерфейсные адаптеры предназначены для выполнения функций физического и канального уровня семиуровневой *модели взаимодействия открытых систем* (*Open System Interconnection – OSI*) (ПРИЛОЖЕНИЕ А) в устройствах локальной сети. Адаптеры имеют передающую и принимающую части, которые выполнены независимыми друг от друга с целью поддержки режима *полного дуплекса* (*Full Duplex*), при котором передача и приём данных происходят одновременно. Обычно

настройки драйверов сетевого адаптера позволяют выбирать и менее производительный режим *полудуплекса* (*Half Duplex*), при котором передача и приём данных происходят по очереди. Также существует возможность ручного выбора скорости передачи данных и других параметров NIC (по умолчанию для режима и скорости передачи устанавливается значение Автоопределение, активирующее схему *автоматического определения скорости и режима передачи* (*Autonegotiation*), наиболее производительных для данного подключения) (рис. 3). Ручное уменьшение скорости передачи данных и изменение режима передачи в полудуплексный может помочь при обнаружении проблем передачи, связанных с наличием интенсивных электромагнитных помех и/или необходимостью использования длин сетевых кабелей, превышающих установленные стандартами.

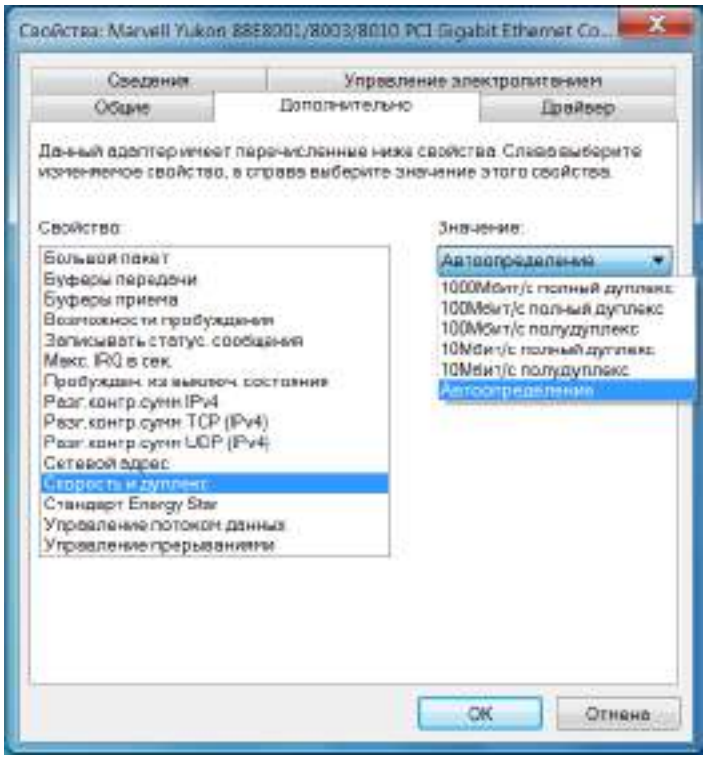



Рис. 3. Настройка параметров сетевого интерфейсного адаптера

В составе NIC можно выделить следующие основные компоненты (см. рис. 2):

– контроллер сетевого адаптера - микросхему, обеспечивающую подавляющее большинство функций адаптера;

– кварцевый резонатор тактового генератора;

– интерфейс (разъем) с системной шиной компьютера (обычно PCI или PCI-Express);

– разъёмы для подключения кабеля (наиболее популярным является 8-контактный RJ-45);

– светодиодные (Light Emission Diode – LED) индикаторы наличия связи (Link), приёма-передачи данных (Rx/Tx), скорости передачи (Speed);

– панелька для опциональной микросхемы BootROM, содержащей программное обеспечение, позволяющее выполнять загрузку с сервера в память компьютера образа операционной системы для бездисковых рабочих станций.

Сетевые интерфейсные адаптеры потребляют следующие системные ресурсы компьютера (рис. 4).

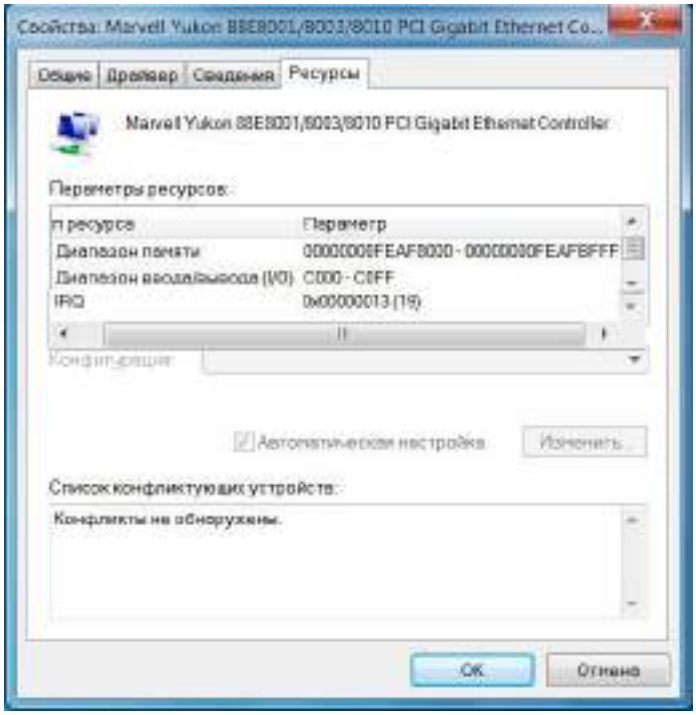



Рис. 4. Системные ресурсы, потребляемые сетевым адаптером

1. *Диапазон памяти адаптера* – буфер для передаваемых и принимаемых кадров. Буферы карт PCI или PCI-Express могут располагаться в любом месте адресного пространства, не занятого оперативной памятью компьютера и могут достигать нескольких мегабайт.

2. *Диапазон адресов ввода/вывода* – диапазон смежных адресов из области адресов портов ввода-вывода (Input-Output Ports – I/O Ports) $0000_H$ - $FFFF_H$. Используется для обращения к регистрам контроллера сетевого адаптера при инициализации, текущем управлении, опросе состояния, приёме и передаче данных.

3. *Запрос прерывания* (*Interrupt Request Query – IRQ*) - номер аппаратного прерывания, выделяемый сетевому адаптеру базовой системой ввода-вывода (Basic Input-Output System – BIOS) или операционной системой, прерывание выполняется при получении кадра, адресованного данному узлу, а также по окончании передачи кадра.

Под *конфигурированием адаптера* подразумевается настройка используемых системных ресурсов и выбор скорости, режима передачи иногда и других параметров. Конфигурирование осуществляется путём настройки драйвера (см. рис. 3), параметры конфигурирования хранятся в энергонезависимой памяти EEPROM, установленной на адаптере. Для со-

временных адаптеров характерно конфигурирование с использованием технологии *Plug And Play* – автоматическое распределение BIOS или операционной системой системных ресурсов между подключёнными устройствами с целью предотвращения конфликтов, происходящих при выделении одних и тех же ресурсов различным устройствам.

Наиболее популярным активным сетевым оборудованием современных локальных компьютерных сетей является *сетевой коммутатор* (*Switch*) (рис. 5), к портам которого с помощью кабелей подключается оконечное оборудование пользователей и/или другое активное сетевое оборудование. Коммутаторы осуществляют передачу структур данных, называемых *кадрами* (*Frame*), из порта, к которому подключено устройство-источник кадров (Source), в порт, к которому подключено устройство-приёмник кадров (Destination). Поиск выходного порта осуществляется коммутаторами на основании анализа адресной информации в заголовке кадра (подробнее структура кадров сетевой технологии Ethernet и работа коммутатора будет рассмотрена в разделе 3).


Рис. 5. Коммутатор локальной сети

Иногда для организации локальной сети в качестве активного сетевого оборудования используют *концентратор* (*Hub*), внешним видом очень похожий на коммутатор (рис. 6). Однако принцип работы концентратора отличается: если коммутатор анализирует адресную информацию в заголовках поступающих в его порты кадров и избирательно передаёт кадры с входного порта на выходной порт, к которому подсоединён получатель кадров, то концентратор просто копирует сигналы, соответствующие битам информации, со своего входного порта на все остальные порты. С практической точки зрения концентраторы имеют преимущество в скорости работы (точнее, в минимальной длительности задержки передаваемых кадров), поскольку они не выполняют буферизацию заголовков кадров и анализ адресной информации. Однако дублирование потоков кадров даже к тем устройствам, которые не являются адресатами (проверкой и отбрасыванием "не своих" кадров занимается сетевой интерфейсный адаптер устройства), приводит к снижению эффективности использования сети. Кроме того, существует возможность использования программ анализаторов протоколов, которые могут принимать и анализировать весь трафик, поступающий в адаптер (одна из таких программ будет использоваться в

последующих лабораторных работах). Очевидно, что в таком случае любой из компьютеров локальной сети сможет "видеть" трафик, передаваемый всеми остальными компьютеров, что является серьёзным недостатком с точки зрения безопасности передачи информации.


Рис. 6. Концентратор локальной сети

В настоящее время достаточно популярным способом организации локальной сети является построение *беспроводных локальных сетей* (*Wireless Local Area Network – WLAN*). Для их организации часто используют *точку доступа* (*Access Point*) (рис. 7 г), организующую радиоканалы между участниками сети, которые должны быть оснащены интерфейсными картами беспроводного доступа (Рис. 7 а, б, в) (следует отметить, что подавляющее большинство мобильных компьютеров и устройств оснащено встроенными контроллерами беспроводного доступа).

*а)* *б)* *в)* *г)*

Рис. 7. Адаптеры беспроводного доступа и точка доступа беспроводной сети

При необходимости подключения беспроводного сегмента локальной сети к её проводному сегменту на коммутаторе/концентраторе точка доступа подключается кабелем к одному из портов коммутатора/концентратора. В этом случае говорят, что беспроводная сеть работает в *режиме инфраструктуры* (*Infrastructure Mode*).

*Сетевые принтеры* представляют собой принтеры, оснащённые сетевыми адаптерами, что позволяет подключать их к сети непосредственно. Использование сетевого принтера является удобным, так как его работа не связана с необходимостью работы компьютера, к которому подключается

обычный принтер. Кроме того, сетевые принтеры обычно имеют повышенные производительность и ресурс картриджа. При отсутствии сетевого принтера совместный доступ к обычному принтеру, подключённому к компьютеру, может быть организован средствами операционной системы.

Наиболее популярными типами сетевых кабелей, использующихся в локальной сети, являются кабели *неэкранированной витой пары* (*Unshielded Twisted Pair – UTP*), представляющие собой свитые попарно четыре пары проводов (рис. 8). Свивка выполняется для компенсации электромагнитных полей, возникающих при прохождении тока по проводнику и наводящих паразитные электрические напряжения в соседних проводниках, оказавшихся в этом поле.

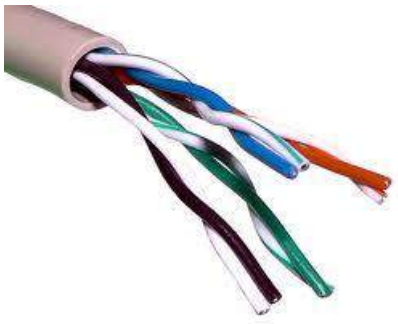
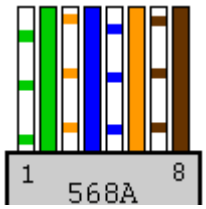


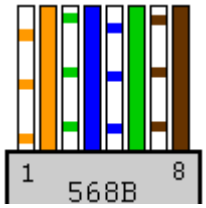
Рис. 8. Кабель неэкранированной витой пары (UTP)

С целью визуального различия кабельных пар выполняется их цветовая маркировка согласно стандарту TIA/EIA-568A и TIA/EIA-568B (рис. 9) (*TIA/EIA – Telecommunications Industry Association – Ассоциация телекоммуникационной промышленности США* – ассоциация изготовителей средств связи, разрабатывающая стандарты на кабельные системы, входит в состав Electronic Industries Alliance).

| **"прямая" (straight) заделка** | | | | | |
|---|---|---|---|---|---|
| **одна сторона** | **сигнал** | **цвет провода** | **другая сторона** | **сигнал** | |
| 1 | TX+ | бело-зеленый | 1 | TX+ | |
| 2 | TX- | зеленый | 2 | TX- | |
| 3 | RX+ | бело-оранжевый | 3 | RX+ | |
| 4 | | синий | 4 | | |
| 5 | | бело-синий | 5 | | |
| 6 | RX- | оранжевый | 6 | RX- | |
| 7 | | бело-коричневый | 7 | | |
| 8 | | коричневый | 8 | | |



| "перекрёстная" (crossover) заделка | | | | | |
|---|---|---|---|---|---|
| **одна сторона** | **сигнал** | **цвет провода** | **другая сторона** | **сигнал** | |
| 1 | TX+ | бело-оранжевый | 1 | TX+ | |
| 2 | TX- | оранжевый | 2 | TX- | |
| 3 | RX+ | бело-зеленый | 3 | RX+ | |
| 4 | | синий | 4 | | |
| 5 | | бело-синий | 5 | | |
| 6 | RX- | зеленый | 6 | RX- | |
| 7 | | бело-коричневый | 7 | | |
| 8 | | коричневый | 8 | | |




\+ передатчик сигнала, - приёмник сигнала

Рис. 9. Варианты заделки проводов типа "витая пара"
(стандарты TIA/EIA-568A и TIA/EIA-568B)

На рис. 10 поясняется необходимость использования кабелей с различными вариантами заделки проводов при соединениях компьютер – коммутатор/концентратор и соединении двух компьютеров непосредственно (последнее часто используется, например, для копирования большого объёма информации с одного компьютера пользователя на другой). В коммутаторе/концентраторе используются так называемые MDI/X порты, в которых приёмник и передатчик подсоединены к контактам, противоположным тем, к которым подсоединены приёмник и передатчик в сетевом адаптере (порт которого является MDI-портом – *MDI – Media Dependent Interface – интерфейс, зависящий от среды передачи*). В этом случае используют прямой кабель, с одинаковой разводкой проводов на его обоих концах. В то же время при непосредственном соединении двух компьютеров соединяются два MDI-порта сетевых адаптеров, в которых приёмник и передатчик расположены одинаковым образом. Поэтому приходится изготавливать или приобретать перекрёстный кабель, один конец которого подсоединён к разъёму RJ-45 согласно стандарту TIA/EIA-568A, а второй – согласно стандарту TIA/EIA-568B. Для монтажа разъёма RJ-45 на кабель UTP используется специальный обжимной инструмент, с помощью которого ножи контактов разъёма врезаются между тоненькими проводами *патч-кордового* (*patch cord*) UTP кабеля, которым подсоединяется компьютер к портам коммутатора/концентратора (рис. 11).

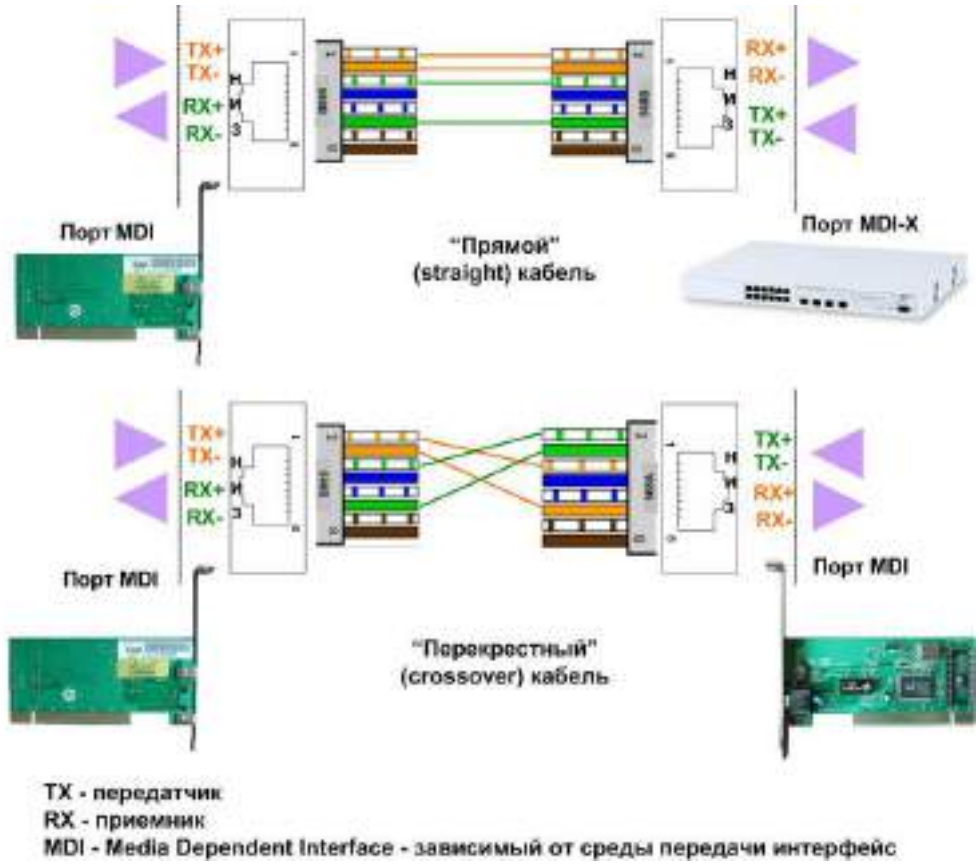



Рис. 10. Соединение прямым и перекрёстным кабелем

*а)* *б)* *в)*

Рис. 11. Способ монтажа разъёма на кабель UTP: а) разъем RJ-45
б) обжимной инструмент в) принцип монтажа разъёма на кабель

## 1.2. Конфигурирование сетевых средств операционных систем компьютеров локальной сети

Чтобы сетевые устройства могли узнать о присутствии других устройств, а также вести обмен данными между собой, на каждом из устройств должен быть установлен одинаковый стек (набор) сетевых протоколов. В настоящее время наиболее распространённым стеком сетевых протоколов является *TCP/IP – Transmission Control Protocol/Internet Protocol – протокол управления передачей/протокол Интернета*, его популярность связана с тем, что данный стек является необходимым услови-

ем для подключения компьютера к сети Интернет. Основной настройкой этого протокола является задание *IP-адреса*, который (для наиболее распространённой в настоящее время 4-й версии протокола IP) выглядит как четыре группы цифр, разделённых точками: `X.X.X.X`, где `X` – десятичное число в диапазоне от `0` до `255`. Старшие одна две или три цифры определяют номер сети, к которой принадлежат компьютеры, для возможности обмена информацией в локальной сети на коммутаторе/концентраторе они должны принадлежать одной IP-сети (более подробное рассмотрение IP-сетей и подсетей будет выполнено в последующих лабораторных работах). В простейшем случае можно использовать сеть с сетевой частью адреса `192.168.0`, при этом для компьютеров сети можно задавать адреса от `192.168.0.1` до `192.168.255.254` (адреса `192.168.0.0` и `192.168.0.255` являются служебными, их назначение также будет выяснено в последующих лабораторных работах). Другой важный параметр стека TCP/IP – *маска подсети* (*Subnet Mask*), представляющая собой 32-битное число, старшая часть которого содержит непрерывный ряд единиц, а младшая – непрерывный ряд нулей. Данный параметр позволяет "разреза́ть" IP-сети на подсети меньшего достаточно гибко задаваемого размера (с этой технологией мы также познакомимся позже). В нашем случае будем использовать маску `255.255.255.0`, задающую подсеть с адресом, определяемым первыми тремя числами IP-адреса – `192.168.0`, в которую можно включить 254 компьютера с адресами от `192.168.0.1` до `192.168.0.254`.

Настройку стека TCP/IP в операционной системе Microsoft Windows 7 можно выполнить, открыв свойства Протокола Интернета версии 4 (TCP/IPv4) в свойствах Сетевого подключения, которое находится: Панель управления – Центр управления сетями и общим доступом – Изменение параметров адаптера (для этого понадобятся права Администратора) (рис. 12). Понятие *основного шлюза* и *DNS-сервера* мы рассмотрим в разделе 4, в простейшей локальной сети эту информацию можно не задавать. Кроме адресной информации, каждому компьютеру должно быть задано *сетевое имя компьютера* и *имя рабочей группы*, в которую он входит. В операционной системе Microsoft Windows 7 имена можно задать (также обладая правами Администратора): Панель управления – Система – Дополнительные параметры – Имя компьютера (рис. 13).

После задания уникальных IP-адресов и сетевых имён устройствам локальной сети можно проверить наличие связи между ними. Проверку лучше начать с физического уровня модели взаимодействия открытых систем (ПРИЛОЖЕНИЕ А), на котором компьютеры обмениваются сигналами, кодирующими биты информации. Для этого достаточно убедиться, что на коммутаторе/концентраторе светится светодиод, соответствующий порту, к которому подключено проверяемое устройство компьютер (в случае, если коммутатор/концентратор находится в труднодоступном месте, можно проверить, светится ли светодиод сетевого адаптера устройства). Если светодиоды светятся, это свидетельствует о наличии соединения между

приёмниками и передатчиками сетевого адаптера и коммутатора/концентратора, если нет, то возможен либо обрыв провода, либо плохой контакт при монтаже разъёма, либо неправильная разводка пар в разъёмах, точнее это можно выяснить с помощью специальных тестеров кабельных сетей.

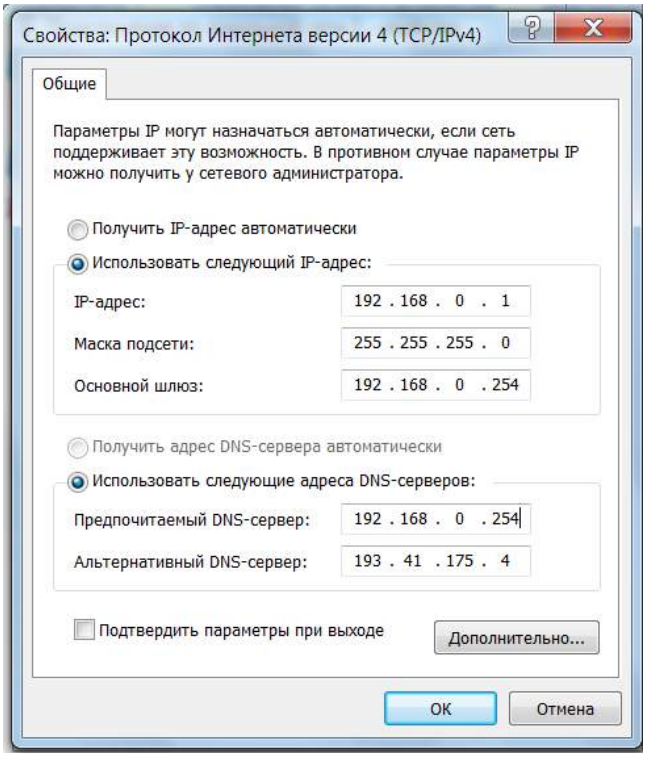



Рис. 12. Окно свойств сетевого подключения протокола Интернета версии 4 (TCP/IPv4) с адресной информацией

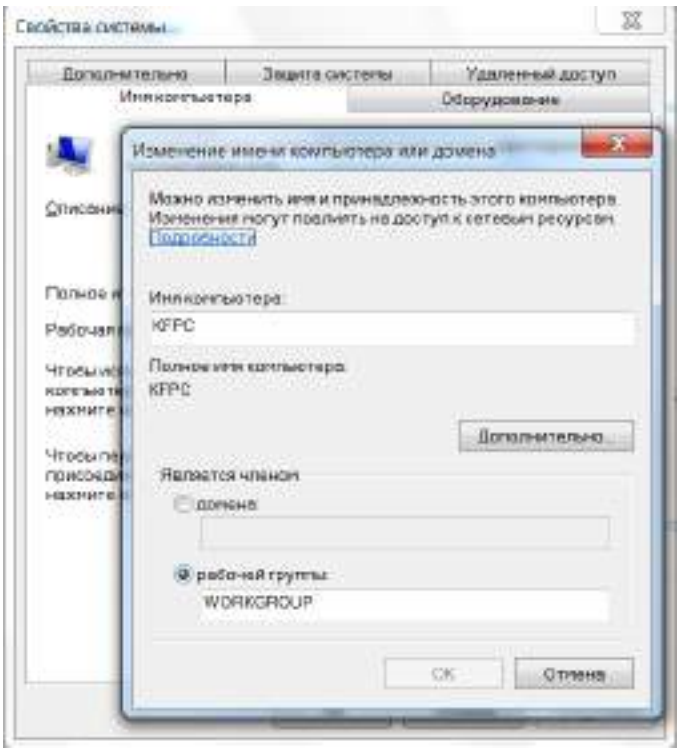



Рис. 13. Окно задания сетевого имени компьютера

При наличии связи на физическом уровне, можно попробовать проверить связь на сетевом уровне. Для этого необходимо открыть окно командной строки (Пуск-Выполнить-cmd) и запустить утилиту `ping`, в качестве аргумента которой указать IP-адрес удалённого компьютера, соединение к которому необходимо проверить.

На рис. 14 показан результат работы утилиты `ping`: 4 пакета размером `32` байта с временем жизни `TTL=128` (этот параметр IP-пакета будет рассмотрен в разделе 4) отправлены с компьютера с адресом `192.168.0.2` компьютеру с адресом `192.168.0.1` и возвращены последним обратно за время менее `1` миллисекунды. Можно сделать вывод, что связь существует, и компьютеры могут обмениваться информацией по сети. В то же время "пингование" компьютера с IP-адресом `192.168.0.254` показывает отрицательный результат, поэтому можно сделать вывод, что компьютера с таким адресом либо нет, либо он выключен, либо существуют проблемы с настройками стека сетевых протоколом на нем.

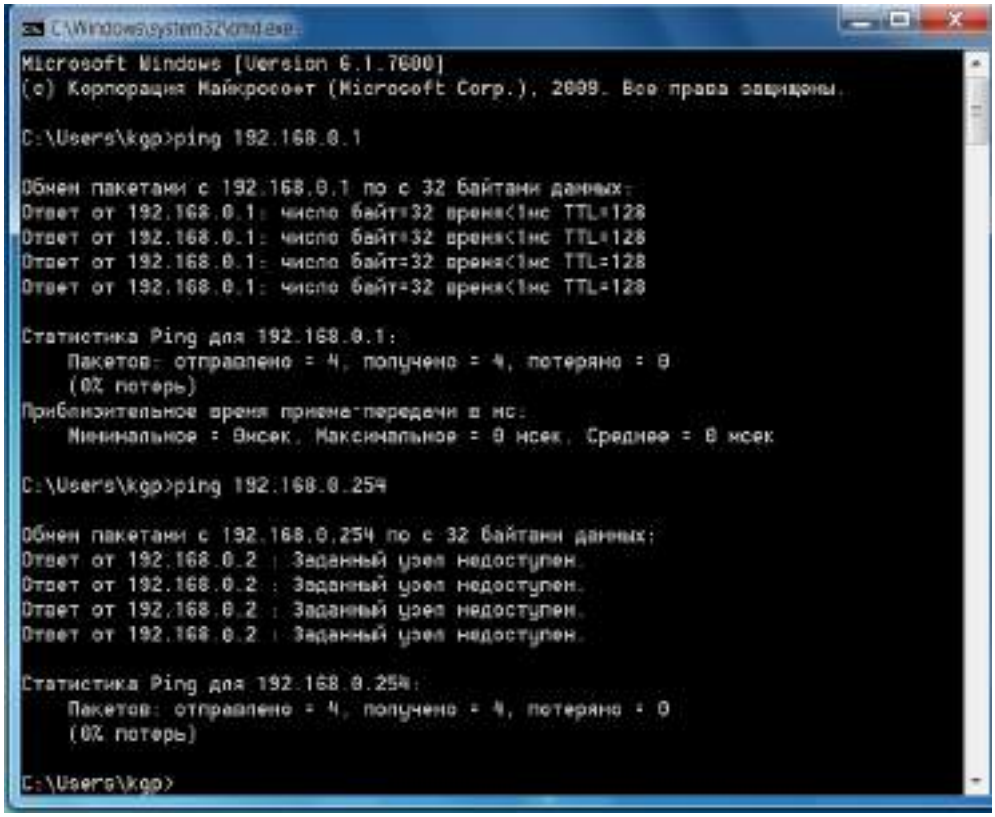



Рис. 14. Проверка связи с удалённым компьютером с помощью утилиты ping

Ещё одной полезной утилитой командной строки является утилита `ipconfig`, позволяющая вывести на экран адресные настройки сетевого стека компьютера (рис. 15). Утилита `ipconfig` с параметром `/all` позволяет вывести полную информацию о настройках сетевого стека, включая наименование сетевого адаптера, адрес канального уровня или MAC-адрес (в выводе `ipconfig` он значится как `Физический адрес`), адреса DNS-серверов (MAC-адрес и доменная систем имён DNS- будут рассмотрены в следующих разделах).

На компьютерах с операционной системой Linux настройка сетевых параметров проводится аналогичным образом. Так в операционной системе ASPLinux к настройкам параметров сети можно добраться: Система-Администрирование-Сеть (как и в Windows, понадобятся полномочия Администратора, который в Linux/Unix имеет пользовательское имя root) (рис. 16).

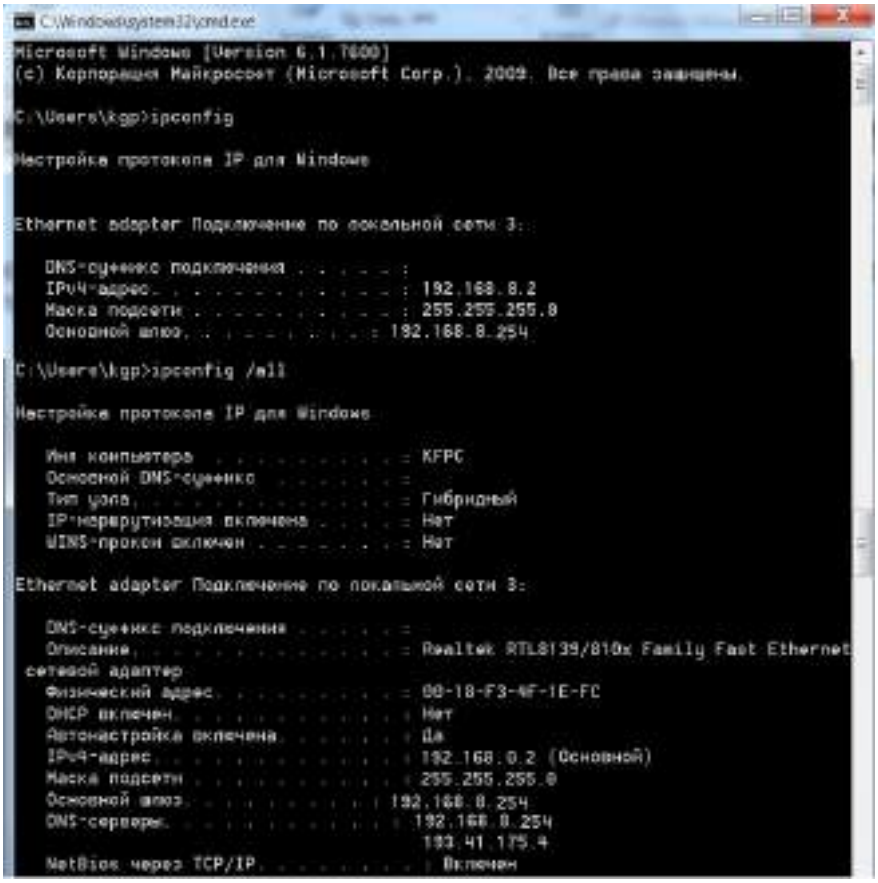



Рис. 15. Вывод конфигурационной информации стека сетевых протоколов компьютера утилитой ipconfig

Просмотр сетевых настроек может быть выполнен с помощью команды `/sbin/ifconfig`, которую можно запустить в окне Терминала (Приложения-Системные-Терминал) (рис. 17). Обратите внимание, что в Linux сетевому адаптеру задаётся системное имя `eth0` (адаптер работает по протоколу физического и канального уровня Ethernet, он будет рассмотрен в разделе 3). Кроме адресной информации, выводится состояние адаптера (`UP` означает, что он работает) и значения счётчиков, считающих переданные и принятые пакеты, а также пакеты с ошибками различного типа. В Linux/Unix также имеется утилита `ping`, работающая аналогично `ping` в Windows.

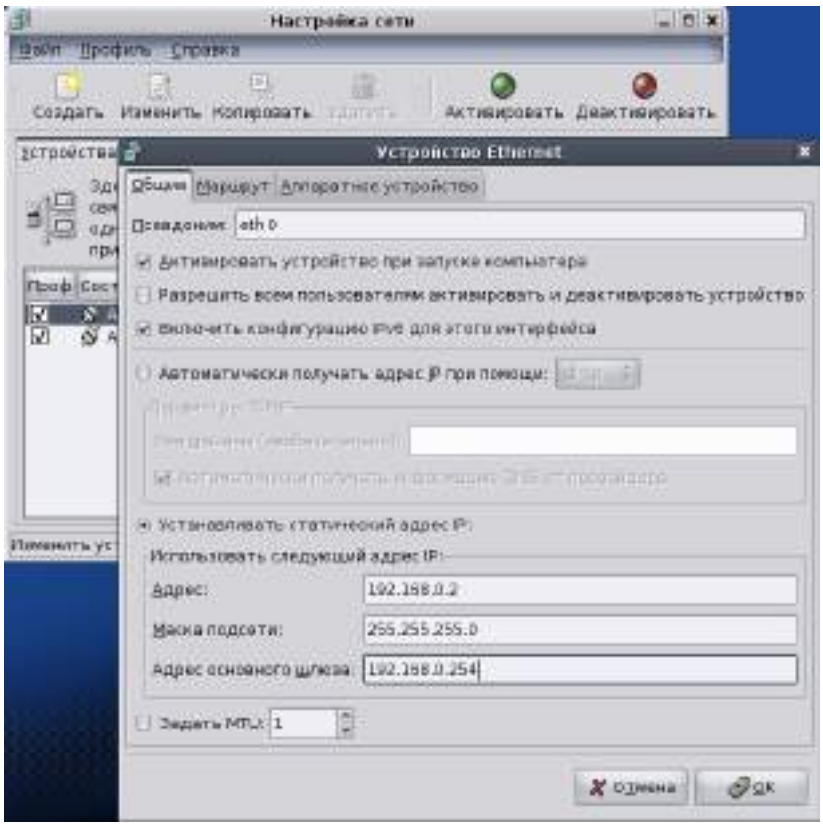



Рис. 16. Настройка сетевых параметров в операционной системе ASPLinux

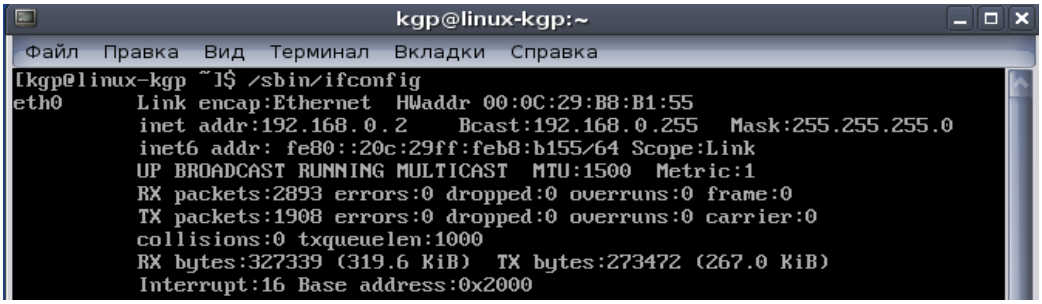



Рис. 17. Вывод адресной информации и значений счётчиков
в операционной системе ASPLinux

## 1.3. Моделирование и исследование работы локальной сети

Поскольку настройка сетевых параметров операционных систем требует прав Администратора, а это не всегда возможно в учебных классах, привлечём на помощь программное обеспечение Packet Tracer, разработанное одной из старейших и уважаемых компаний на рынке производства сетевого оборудования Cisco Systems. Данное программное обеспечение является бесплатным и кросс-платформенным (то есть существуют его версии для различных операционных систем), Cisco Systems активно использует его при обучении по сертификационным программам *Cisco Certified Network Associate (CCNA)* и *Cisco Certified Network Professional (CCNP)* в размещённых во многих странах подразделениях *сетевой академии Cisco* (*Cisco Networking Academy).* Cisco Packet Tracer позволяет создавать различные модели сети, настраивать различное пользовательское обо-

рудование, коммутаторы, маршрутизаторы, беспроводное оборудование и проверять наличие сетевых соединений между ними.

При запуске Packet Tracer открывает окно Рабочей области (Workspace) логического размещения (Logical) устройств сети (рис. 18).

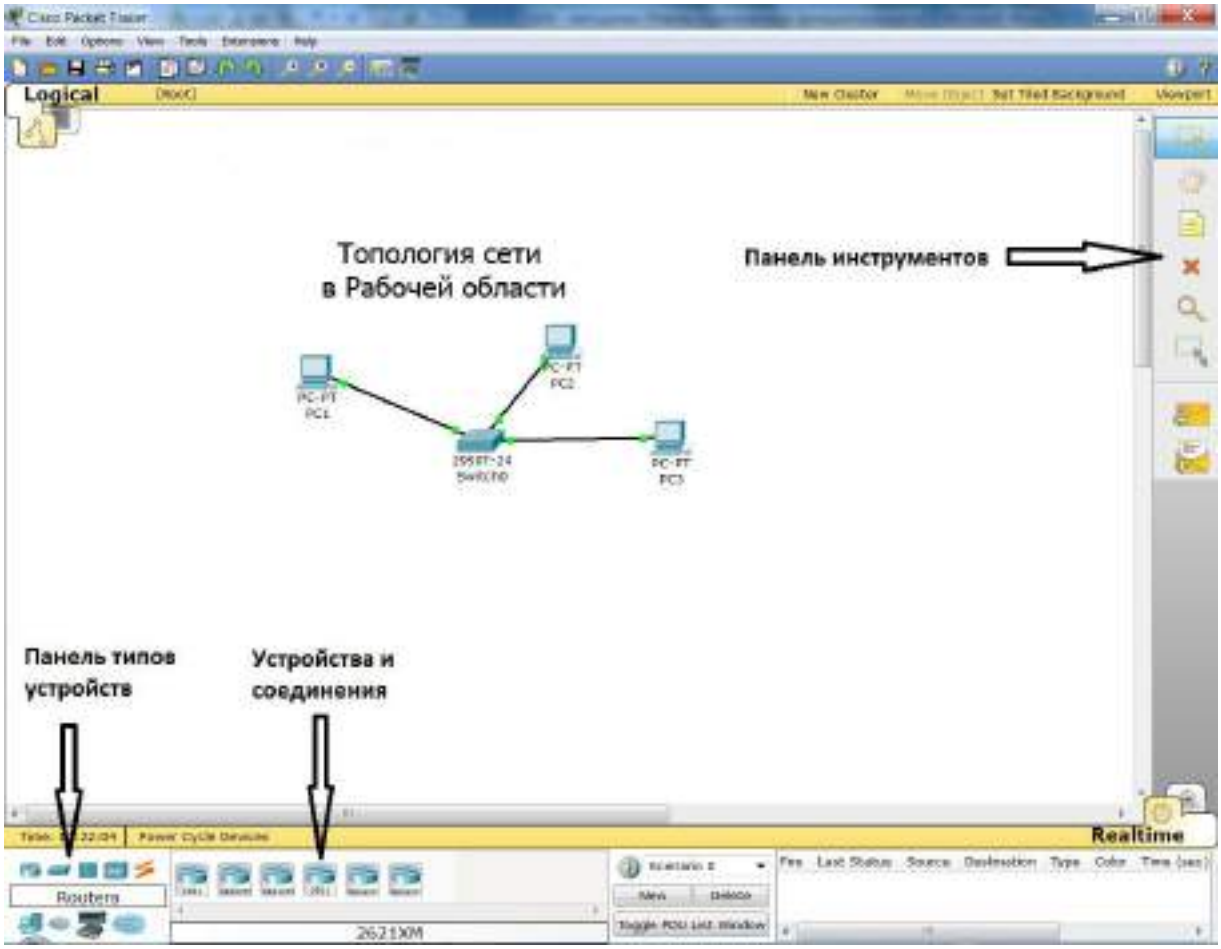



Рис. 18. Основные элементы управления Packet Tracer

Для создания сети необходимо на Рабочую область перетащить требуемые оконечные устройства пользователей - компьютеры, ноутбуки, серверы, принтеры и другие устройства. Именно в таком порядке оконечное оборудование пользователей представлено в Области отображения устройств и соединений после выбора в Панели типов устройств Оконечные устройства (End Devices) (рис. 19).


Рис. 19. Оконечное оборудование пользователей Packet Tracer

При выделении устройства внизу окна выбора устройств отображается его название. При необходимости добавления на Рабочую область нескольких устройств можно осуществить их выбор при нажатой клавише Ctrl и после этого выполнить щелчки на Рабочей области нужное количество

раз. Каждый щелчок приводит к созданию устройства и автоматическому заданию его имени, например PC0, PC1, PC2 и т.д. Имя устройства может быть изменено выделением имени устройства щелчком мыши на нём и вводом нового имени.

После размещения необходимого оборудования пользователей можно аналогичным образом разместить на Рабочей области сетевое оборудование, сгруппированное в следующих типах устройств: маршрутизаторы (Routers), коммутаторы (Switches), концентраторы (Hubs), беспроводные устройства (Wireless Devices) и др. При выборе типа устройств на Панели устройств и соединений отображается доступное в Packet Tracer сетевое оборудование данного типа (рис. 20).


Рис. 20. Выбор сетевого оборудования в Packet Tracer

Если поместить указатель мыши на устройство, всплывающее окно отобразит его конфигурацию (рис. 21).

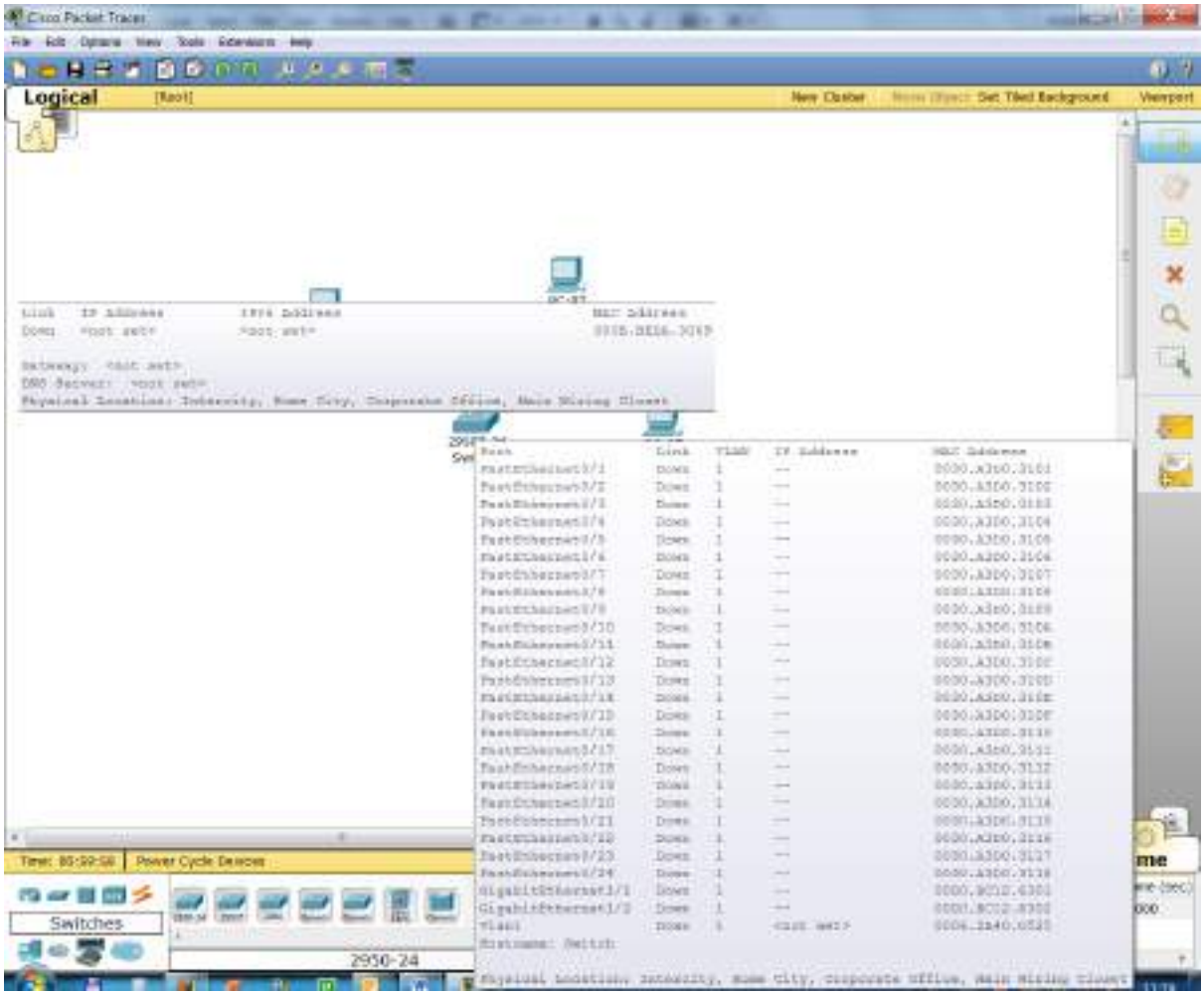



Рис. 21. Просмотр конфигурации устройств

Для соединения устройств пользователей и сетевого оборудования в Панели выбора типов устройств нужно выбрать Соединения (Connections), а в Области отображения устройств и соединений требуемое соединение (рис. 22).

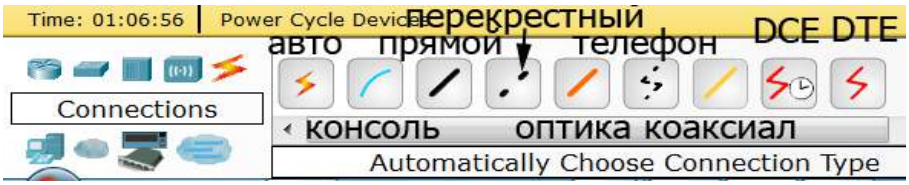



Рис. 22. Выбор типа соединения в Packet Tracer

Для соединения устройств необходимо выбрать тип соединения (прямой медный кабель – Copper Straight-Through для соединения компьютера и коммутатора), затем выполнить щелчок на первом устройстве, выбрать порт устройства из всплывающего меню и выполнить щелчок на втором устройстве, выбрав его порт (рис. 23). Подобным образом необходимо соединить все устройства. Обратите внимание, что при создании нового соединения занятые порты устройства не отображаются во всплывающем окне.

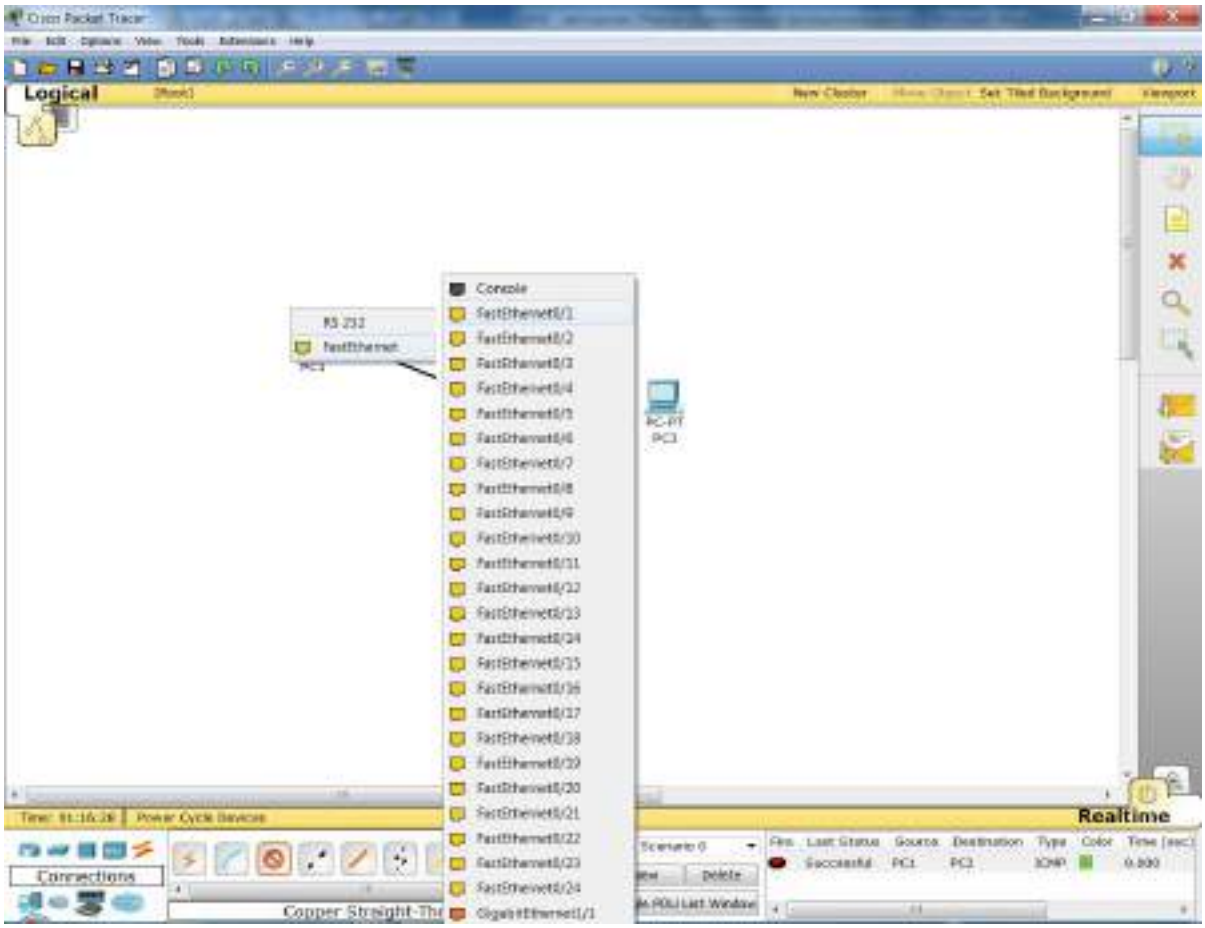



Рис. 23. Соединение устройств в Packet Tracer

Если создавать соединение с автоматическим выбором типа (Automatically Choose Connection Type), то всплывающие окна появляться не будут, а Packet Tracer сам определит тип соединения и используемые порты (с методиче-

ской точки зрения эту возможность использовать не рекомендуется, поскольку нужно представлять, какие порты и как соединяются).

После завершения соединения устройств сети Packet Tracer сигнализирует о наличии соединений на физическом и канальном уровнях двумя зелёными периодически мигающими квадратиками на концах каждого соединения (мигание означает активность линии). При отсутствии соединения квадратики становятся красными (рис. 24). Это можно проверить, выключив питание одного из компьютеров. Для этого выполните щелчок левой кнопкой мыши на одном из компьютеров и перейдите в открывшемся окне на вкладку Физическая конфигурация (Physical). Выполните щелчок мышью по кнопке питания на изображении компьютера, обратите внимание, что находящийся над ней индикатор погас. После включения устройства квадратик на линии связи возле устройства не сразу изменяет цвет на зелёный. Это обусловлено необходимостью некоторого времени на распознавание устройства коммутатором.

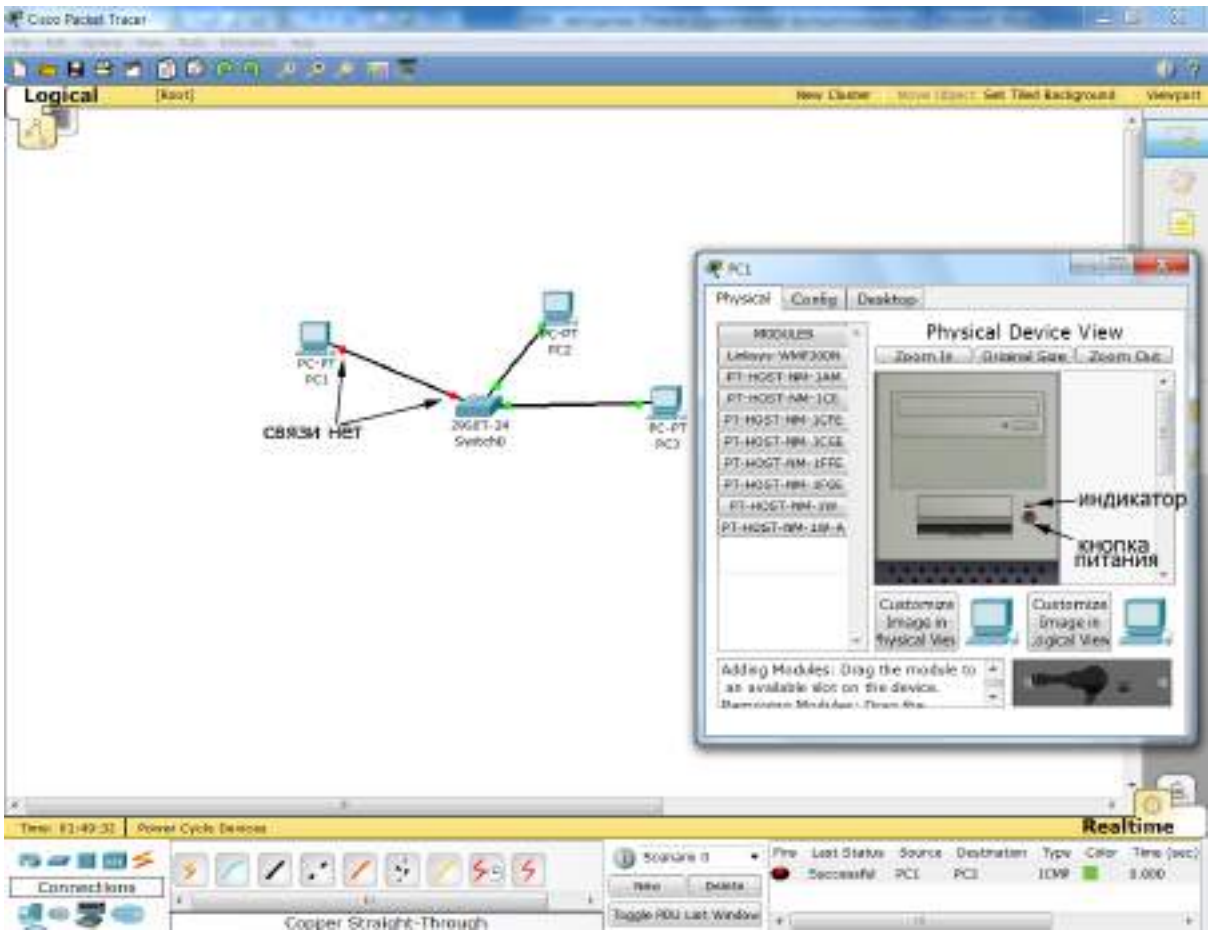



Рис. 24. Отключение устройства и неактивность линии связи

В случае ошибочно созданных на Рабочей области устройств и связей их можно удалить, используя инструмент Удаление (Delete) на Панели инструментов (см. рис. 18). Инструмент Выделение (Select) позволяет выделить необходимое одно или несколько устройств, инструмент Изменение

размеров (Resize)  позволяет при необходимости изменить их размер. Созданная сетевая топология может быть сохранена/считана из файла с расширением `.pkt` стандартным способом.

Следующим шагом может быть создание беспроводного сегмента сети и подключение его к проводной сети (то есть создание беспроводной сети, работающей в *режиме инфраструктуры – Infrastructure Mode*). Для этого необходимо добавить на Рабочую область Точку доступа (Access Point-PT), предварительно выбрав в Панели типов устройств Беспроводные устройства (Wireless Devices) (рис. 25), добавьте также из группы Оконечные устройств (End Devices) Ноутбук (Laptop-PT).

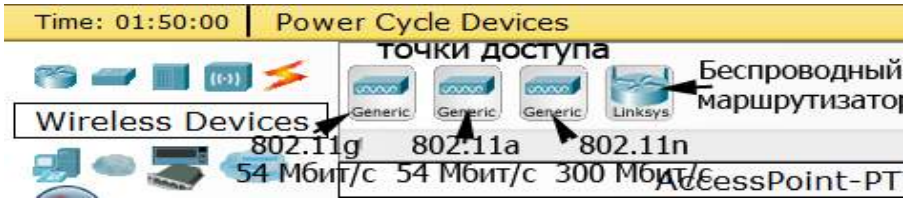



Рис. 25. Выбор типа беспроводных устройств в Packet Tracer

Поскольку ноутбук по -умолчанию оснащён проводным интерфейсом, необходимо заменить его на беспроводный. Для этого выполните щелчок левой кнопкой мыши на ноутбуке и перейдите на вкладку Физическая конфигурация (Physical). Прокрутите линейку прокрутки вниз так, чтобы увидеть изображение ноутбука (рис. 26).

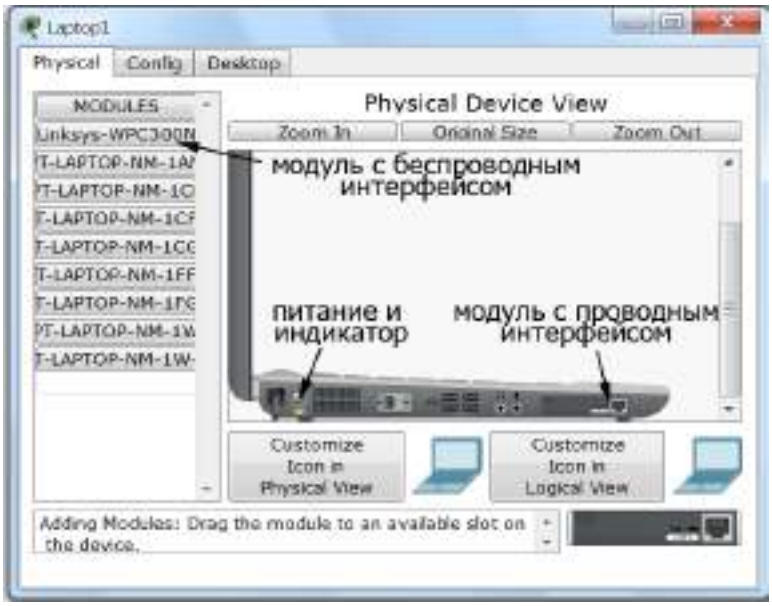



Рис. 26. Замена интерфейсного модуля в ноутбуке на беспроводный

Отключите питание ноутбука, выполнив щелчок левой кнопкой мыши на кнопке питания, при этом погаснет индикатор питания. Перетащите мышью модуль с проводным интерфейсом в Список модулей (MODULES) слева от изображения ноутбука. После этого перетащите верхний модуль с беспроводным интерфейсом Linksys-WPC300N из Списка модулей (MODULES)

в разъем ноутбука, в котором был установлен модуль с проводным интерфейсом. Включите питание ноутбука и закройте окно конфигурирования ноутбука. Вы должны увидеть, что ноутбук связался с точкой доступа с помощью радиоволн (рис. 27).

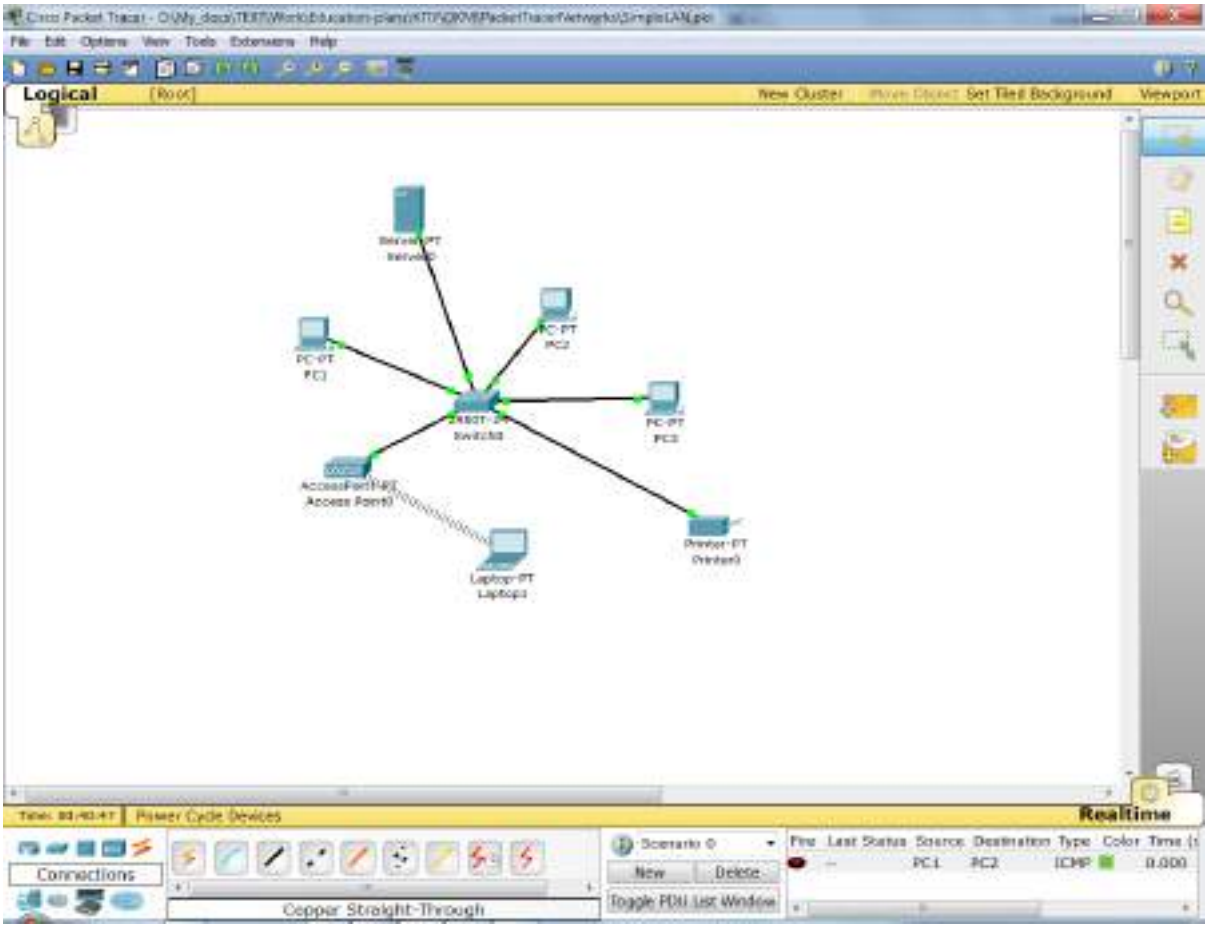



Рис. 27. Завершённая топология локальной компьютерной сети

Добавьте к сети из группы Оконечные устройств (End Devices) на Панели типов устройств Сервер (Server-PT) и Принтер (Printer-PT). Оба устройства по-умолчанию оснащены проводными интерфейсами Fast Ethernet, работающими со скоростью 100 Мбит/с. Подсоедините принтер к порту коммутатора аналогично соединению с ПК. Замените сетевой интерфейс сервера его на интерфейс Gigabit Ethernet, работающий со скоростью 1000 Мбит/с. Для этого выполните щелчок на изображении сервера и на вкладке Физическая конфигурация (Physical) после выключения питания сервера замените так, как Вы это выполняли для ноутбука, сетевой интерфейс сервера на модуль PC-HOST-NM-1CGE (рис. 28).

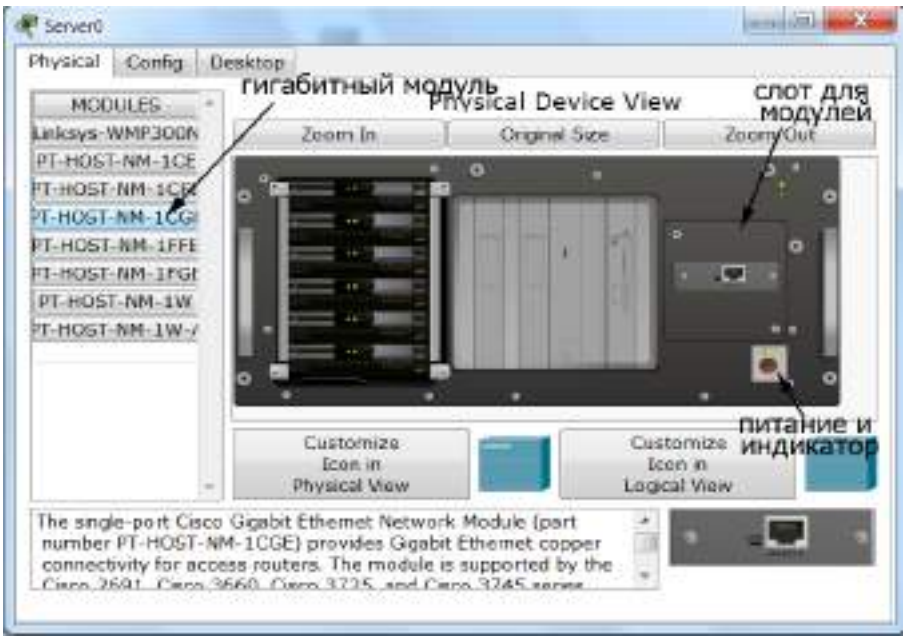


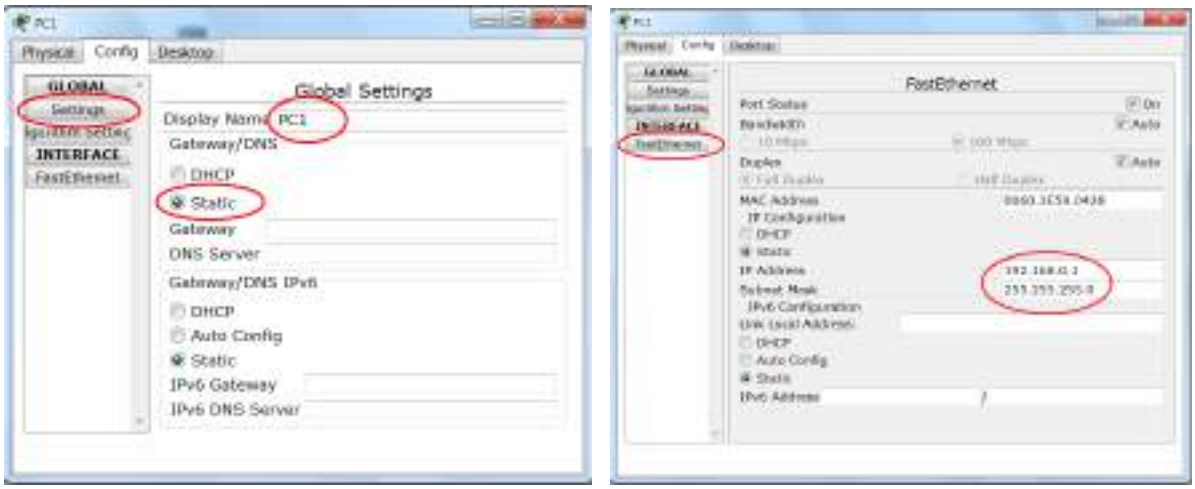

Рис. 28. Замена интерфейсного модуля сервера на Gigabit Ethernet

Обратите внимание, что при подсоединении сервера к коммутатору необходимо выбрать на коммутаторе гигабитный порт, например Gigabit Ethernet 1/1. В этом случае пакеты между коммутатором и сервером будут проходить на скорости в 10 раз большей скорости между коммутатором и остальными устройствами сети, что является оправданным, так как сервер обычно используется несколькими устройствами.

После создания сети следующим шагом является конфигурирование устройств. Сетевые имена устройств задаются автоматически при создании, их можно изменять прямо в Рабочей области или в окне конфигурирования устройств. Устройства Packet Tracer поддерживают стек сетевых протоколов TCP/IP, причём поддерживается и IP 4 версии (в настоящее время наиболее распространённой), и IP версии 6 (переход к которой уже начался). В данной работе мы будем задавать устройствам адреса протокола IP 4 версии.

Назначение имён и IP-адресов ПК, принтера и сервера происходит одинаковым образом, поэтому приведём последовательность действий по конфигурированию этих параметров на примере ПК. Выполните щелчок по изображению устройства левой кнопкой мыши, при этом откроется окно конфигурирования устройств, выберите его вкладку Конфигурация (Config) (рис. 29).

Из списка слева выберите команду Настройки (Settings) для перехода к окну (рис. 29а), в котором можно ввести/изменить сетевое имя устройства. Здесь также можно указать IP-адреса шлюза (Gateway) сети, в которую входит данное устройство, и DNS-сервера, на котором находятся соответствия имён пользовательских устройств сети и их IP-адресов, и указать будет ли назначаться им адрес автоматически (с использованием сервера, работающего по протоколу Dynamic Host Configuration Protocol - DHCP-сервера) или вручную (Static).




а) б)

Рис. 29. Задание: а) сетевого имени, б) IP-адреса и маски подсети устройствам

Сетевой шлюз (Gateway) представляет собой сетевой интерфейс, через который сетевые пакеты от устройств данной сети уходят в другие сети и пакеты от устройств других сетей входят в данную сеть. Поскольку в данной лабораторной работе моделируется только одна сеть, адрес шлюза задавать не нужно. Рассмотрение работы Доменной системы имён (Domain Name System – DNS) и конфигурирование DNS-сервера будет рассмотрено в последующих разделах. Без конфигурирования такого сервера мы сможем посылать пакеты с помощью утилиты `ping`, используя в качестве её аргумента только IP-адрес удалённого компьютера. После конфигурирования DNS-сервера появляется дополнительная возможность связи с ним по его сетевому имени.

Из списка слева выберите тип сетевого интерфейса устройства (Fast Ethernet на рис. 29б) для открытия окна задания адресной информации. В поле IP-адрес (IP Address) для компьютера с сетевым именем PC1 введите адрес `192.168.0.1`, далее выполните щелчок в поле Маска подсети (Subnet Mask), программа автоматически введёт маску `255.255.255.0`, оставьте её без изменений. Обратите внимание, что на этой вкладке автоматически задаётся MAC-адрес, а также скорость и режим передачи данных (100 Мбит/с и полный дуплекс на рис. 29б).

Выполните аналогичным способом конфигурирование остальных пользовательских устройств созданной локальной сети, задав им IP-адреса и маски, приведенные в табл. 1. Обратите внимание, что сетевой интерфейс сервера имеет тип Gigabit Ethernet и работает на скорости 1000 Мбит/с.

Табл. 1

**Адресная информация для конфигурирования пользовательских устройств локальной компьютерной сети на рис. 27**

| Устройство | Сетевое имя | IP-адрес | Маска подсети |
|---|---|---|---|
| ПК-1 | PC1 | 192.168.0.1 | 255.255.255.0 |
| ПК-2 | PC2 | 192.168.0.2 | 255.255.255.0 |
| ПК-3 | PC3 | 192.168.0.3 | 255.255.255.0 |
| Ноутбук | Laptop1 | 192.168.0.4 | 255.255.255.0 |
| Сетевой принтер | Printer0 | 192.168.0.5 | 255.255.255.0 |
| Сервер | Server0 | 192.168.0.6 | 255.255.255.0 |

Конфигурирование адресов для ноутбука имеет особенности, поскольку мы оснастили его беспроводным интерфейсом. По умолчанию окно конфигурирования интерфейса открывается с установленной настройкой автоматического задания IP-адреса и маски подсети устройствам (DHCP). Но поскольку в данной сети отсутствует DHCP-сервер, следует переключить установку в режим ручного задания адресов (Static) и задать IP-адрес и маску подсети описанным выше способом. Обратите внимание на наличие настроек аутентификации (Authentication) устройств при беспроводном подключении к точке доступа – передачу точке доступа пароля, по которому она будет подключать устройство, и настроек шифрования передаваемых по беспроводной сети данных (Encryption). Учитывая простоту несанкционированного подключения к беспроводной сети, на практике эти возможности являются часто используемыми. Пока оставьте их отключёнными (Disabled) (рис. 30). Обратите внимание на скорость передачи данных, в соответствии с протоколом IEEE 802.11g, используемом точкой доступа и беспроводным адаптером, она составляет 54 Мбит/с.

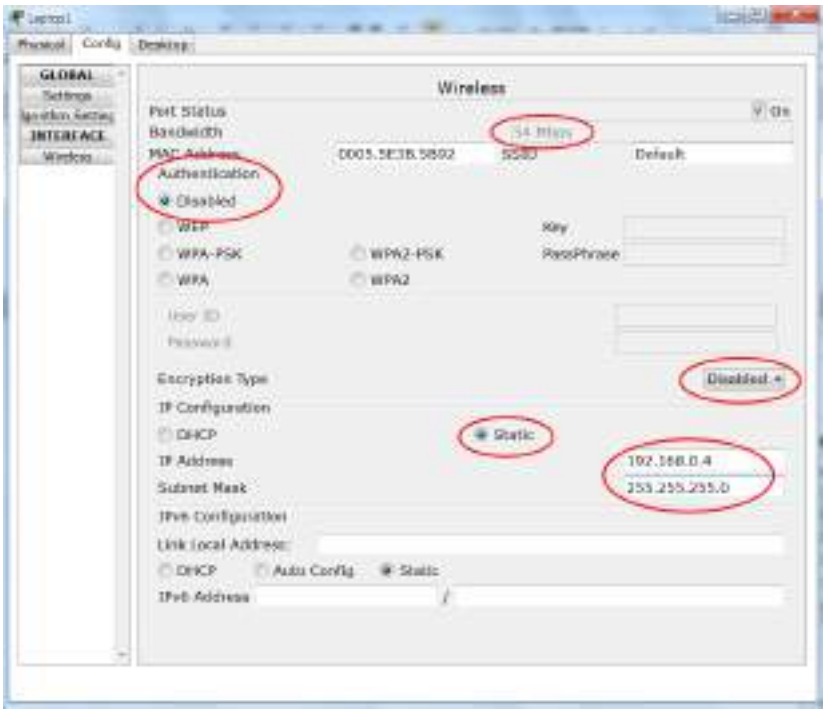



Рис. 30. Конфигурирование беспроводного интерфейсного адаптера

Конфигурирование сетевого оборудования моделируемой локальной сети выполняется автоматически, однако просмотр возможных параметров конфигурации представляет интерес. На рис. 31 приведено окно конфигурации беспроводной точки доступа. В списке её интерфейсов слева присутствуют два интерфейса – Port 0 – проводной интерфейс Fast Ethernet, связывающий точку доступа с коммутатором, и беспроводный интерфейс Port 1. Здесь так же, как и для беспроводного адаптера есть поля для настройки аутентификации и шифрования, включая указание ключевой/парольной фразы, которую должен передать беспроводный адаптер для подключения к точке доступа.

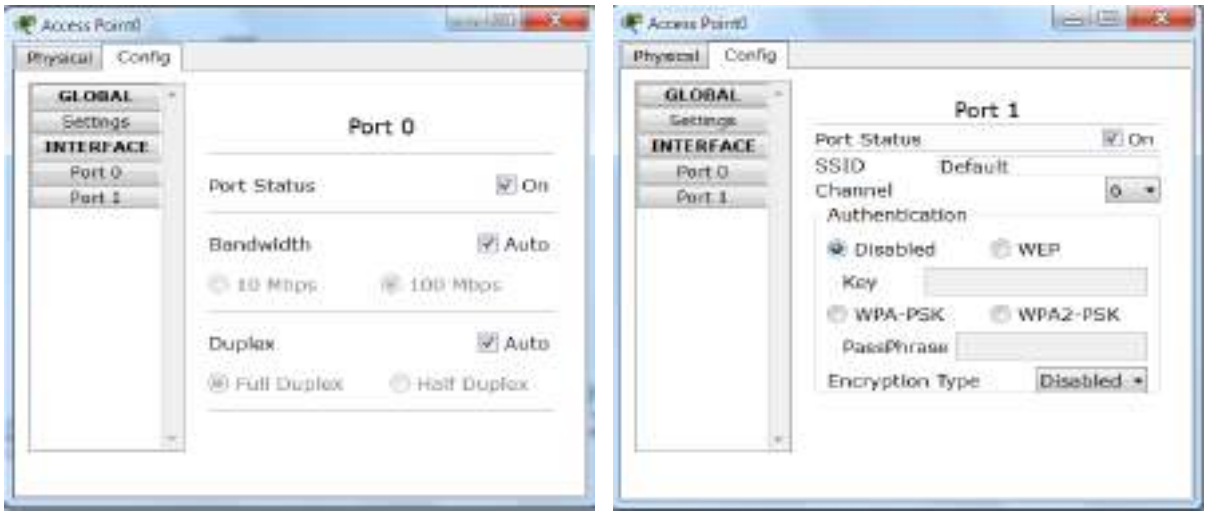
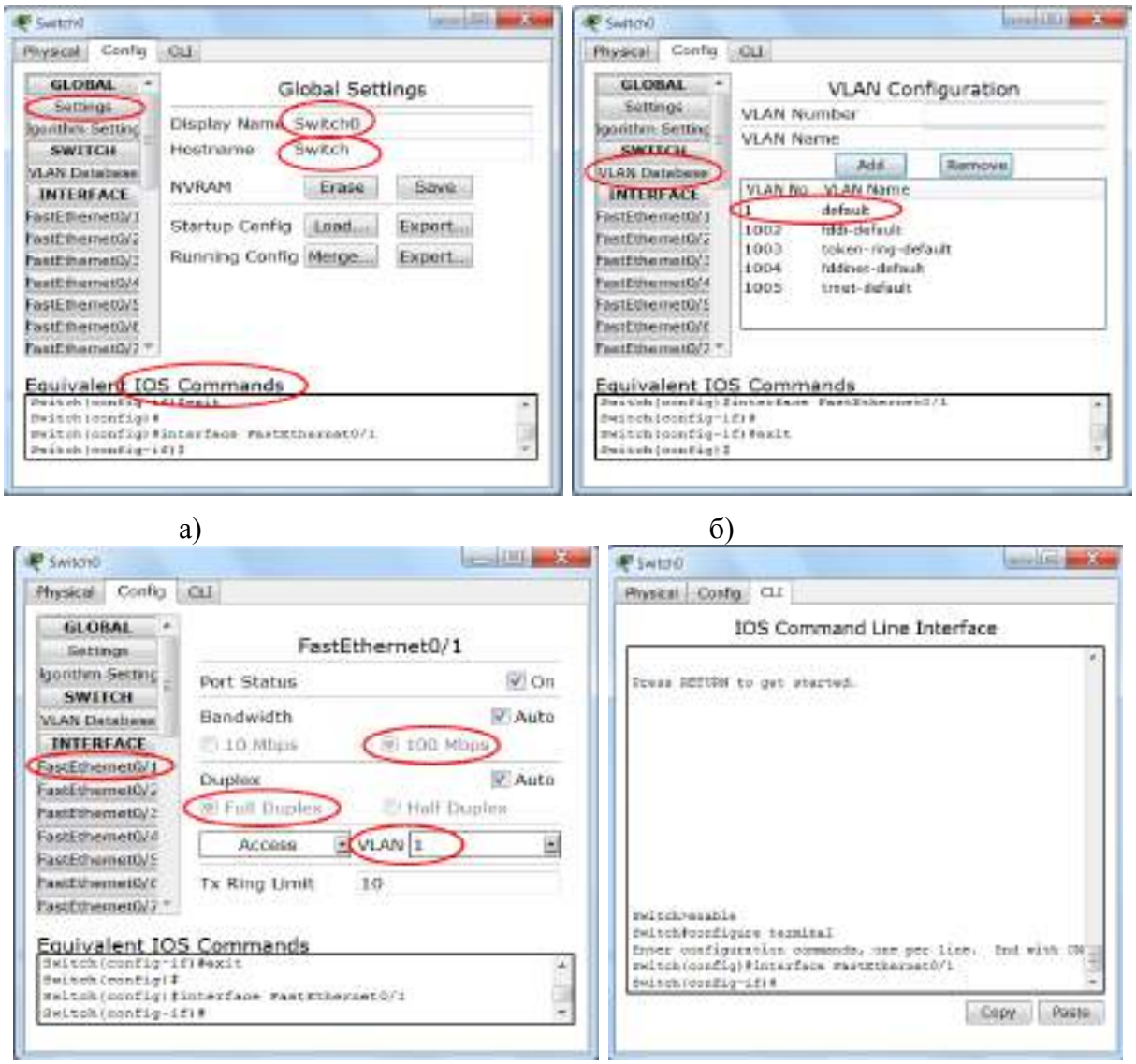



Рис. 31. Конфигурационные параметры беспроводной точки доступа

На рис. 32а приведены конфигурационные параметры коммутатора в окне глобальных настроек (Global Settings), включающие имя коммутатора, отображаемое на схеме сети (Display Name) и хост-имя (Hostname), по которому коммутатор идентифицируется командами *межсетевой операционной системы* Cisco (*Internetwork Operating System – IOS*) – программного обеспечения, зашитого в постоянную память большинства сетевых устройств производства Cisco Systems. Все выполняемые настройки сопровождаются соответствующими им командами IOS в окне Equivalent IOS Command.

При выборе команды База данных VLAN (VLAN Database) из списка команд слева отображается окно со списком *виртуальных локальных сетей* (*Virtual LAN – VLAN*) – технологии, позволяющей приписывать порты сетевых устройств к различным VLAN, тем самым разделяя эти порты на отдельные сети на канальном уровне (рис. 32б). VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. В нашей сети все порты приписаны к VLAN с именем `default` (по -умолчанию) и идентификатором `1`.




а) б)

в) г)

Рис. 32. Конфигурационные параметры коммутатора

При выборе из списка слева названия сетевого интерфейса (порта) коммутатора (`Fast Ethernet 0/1` в примере на рис. 32в) открывается окно задания параметров интерфейса. Здесь возможно приписать порт к той либо иной VLAN, а также при необходимости изменить автоматически выбираемые скорость и режим работы порта.

На вкладке интерфейса командной строки (Command Line Interface – CLI) все настройки конфигурации могут выполняться вручную с помощью команд IOS (рис. 32г).

Для проверки связи между устройствами смоделированной локальной сети можно использовать утилиту `ping`. Для этого выполните щелчок левой кнопкой мыши, например, на ПК и перейдите на вкладку Рабочий стол (Desktop). На нем будут доступны дополнительные инструменты для настройки данного устройства (их доступность зависит от физического конфигурирования устройства – наличия тех либо иных модулей или устройств). Нам понадобится инструмент Окно командной строки (Command

Prompt), в котором можно запустить утилиту `ping` с IP-адресом устройства сети, связь с которым проверяется в качестве её аргумента (рис. 33).

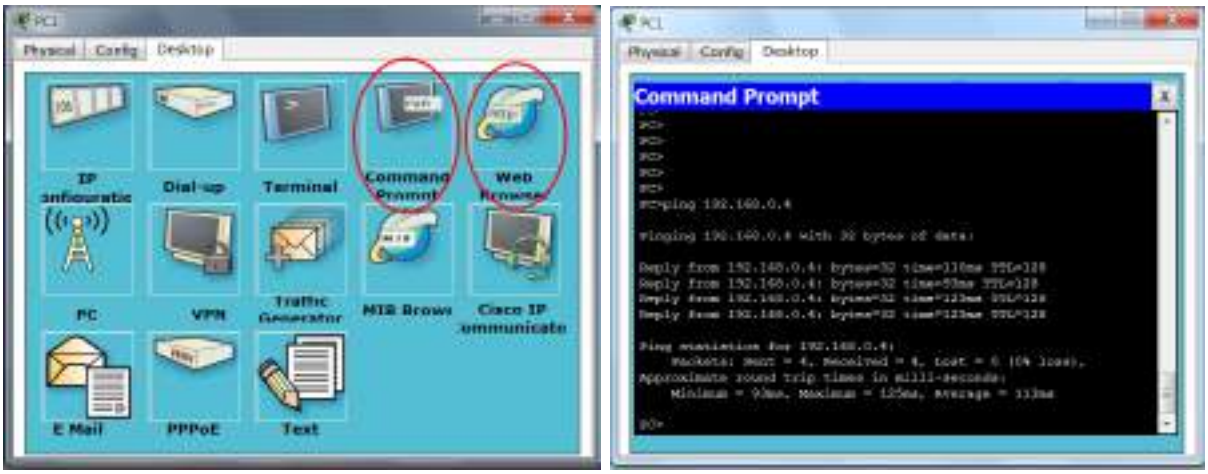



Рис. 33. Проверка связи с помощью утилиты ping

Также существует возможность проверить связь с сервером, открыв на нем Web-страницу с помощью Web-браузера, которым оснащён ПК (рис. 33). Это возможно, поскольку на сервере по -умолчанию устанавливается целый ряд серверных приложений, в том числе и HTTP-сервер с несколькими простыми HTML-страницами (рис. 34).

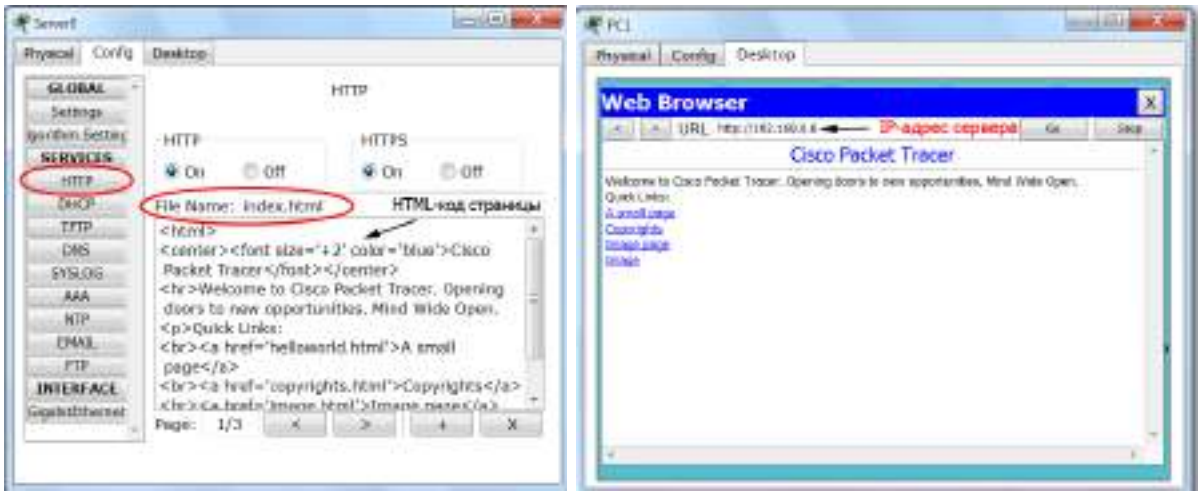



Рис. 34. Открытие Web-страницы HTTP-сервера в браузере ПК

## Задание для самостоятельной работы

1. Выведите конфигурацию сетевого интерфейса Вашего компьютера на экран и приведите скриншот в отчёт.
2. Выполните проверку связи Вашего компьютера с любым другим работающим и неработающим компьютером на физическом и сетевом уровнях. Приведите в отчёт описание и скриншот с результатами проверки.
3. Постройте с помощью программы Packet Tracer модель локальной компьютерной сети на одном коммутаторе и одной беспроводной точке доступа с оконечными устройствами пользователей, количества ко-

торых перечислены в табл. 2для Вашего варианта V, вычисляемого по порядковому номеру N, под которым числится Ваша фамилия в журнале академической группы: V = mod(N) / 20 + 1. Ноутбуки должны быть оснащены беспроводными интерфейсами, а серверы – интерфейсами Gigabit Ethernet.

Табл. 2

**Устройства для индивидуального моделируемых локальных сетей**

| Вариант | ПК | серверов | принтеров | ноутбуков | Вариант | ПК | серверов | принтеров | ноутбуков |
|---|---|---|---|---|---|---|---|---|---|
| **1** | 5 | 1 | 2 | 2 | **11** | 20 | 1 | 2 | 3 |
| **2** | 7 | 2 | 1 | 3 | **12** | 18 | 2 | 1 | 4 |
| **3** | 9 | 1 | 2 | 4 | **13** | 16 | 1 | 2 | 2 |
| **4** | 11 | 2 | 1 | 2 | **14** | 14 | 2 | 1 | 3 |
| **5** | 13 | 1 | 2 | 3 | **15** | 12 | 1 | 2 | 4 |
| **6** | 15 | 2 | 1 | 4 | **16** | 10 | 2 | 1 | 2 |
| **7** | 17 | 1 | 2 | 2 | **17** | 8 | 1 | 2 | 3 |
| **8** | 19 | 2 | 1 | 3 | **18** | 6 | 2 | 1 | 4 |
| **9** | 21 | 1 | 2 | 4 | **19** | 13 | 1 | 2 | 2 |
| **10** | 22 | 2 | 1 | 2 | **20** | 16 | 2 | 1 | 3 |

4. Задайте сетевые имена для компьютеров ПК1 – ПКМ (М – количество ПК из табл. 2), Сервер1 – Сервер2, Принтер1 – Принтер2, Ноутбук1 – НоутбукL (L – количество ноутбуков из табл. 2). Приведите в отчёт скриншот с топологией локальной сети.
5. Задайте IP-адреса пользовательским устройством, выбрав их из диапазона адресов IP-сети `192.168.1.0 - 192.168.1.255`, имеющей маску подсети `255.255.255.0`. Вначале диапазона IP-адресов разместите серверы, затем принтеры, затем ПК, затем ноутбуки. Приведите в отчёт таблицу с сетевыми именами, IP-адресами и масками подсети, заданными устройствам, а также названиями сетевых интерфейсов коммутатора, к которым эти устройства подключены.
6. Выполните проверку связи между одним из ноутбуков и любым ПК, любым сервером, любым принтером. Приведите в отчёт скриншоты с результатами проверки.
7. Настройте параметры беспроводного подключения, позволяющие выполнять аутентификацию и шифрование по протоколам WEP и WPA. Выполните поиск в Интернет и приведите в отчёт краткое сравнение этих протоколов.
8. Измените IP-адреса первой половины Ваших ПК на адреса из диапазона адресов IP-сети `192.168.2.0 - 192.168.2.255`, имеющей маску подсети `255.255.255.0`. Проверьте связь на сетевом уровне между ПК1 и ПКМ (М – количество ПК из табл. 2). Проверьте связь между ПК1 и ПК2. Приведите результаты исследования в отчёт.
9. Создайте в коммутаторе VLAN с номером `2` и именем `test`. Для IP-сети, в которой находится три и более ПК, назначьте портам коммутатора, к которым подсоединены первый и третий ПК этой подсети,

идентификатор VLAN 2. Выполните проверку связи между вторым компьютером рассматриваемой IP-подсети и первым, а затем третьим компьютером. Выполните проверку связи между первым и третьим компьютером рассматриваемой IP-подсети.

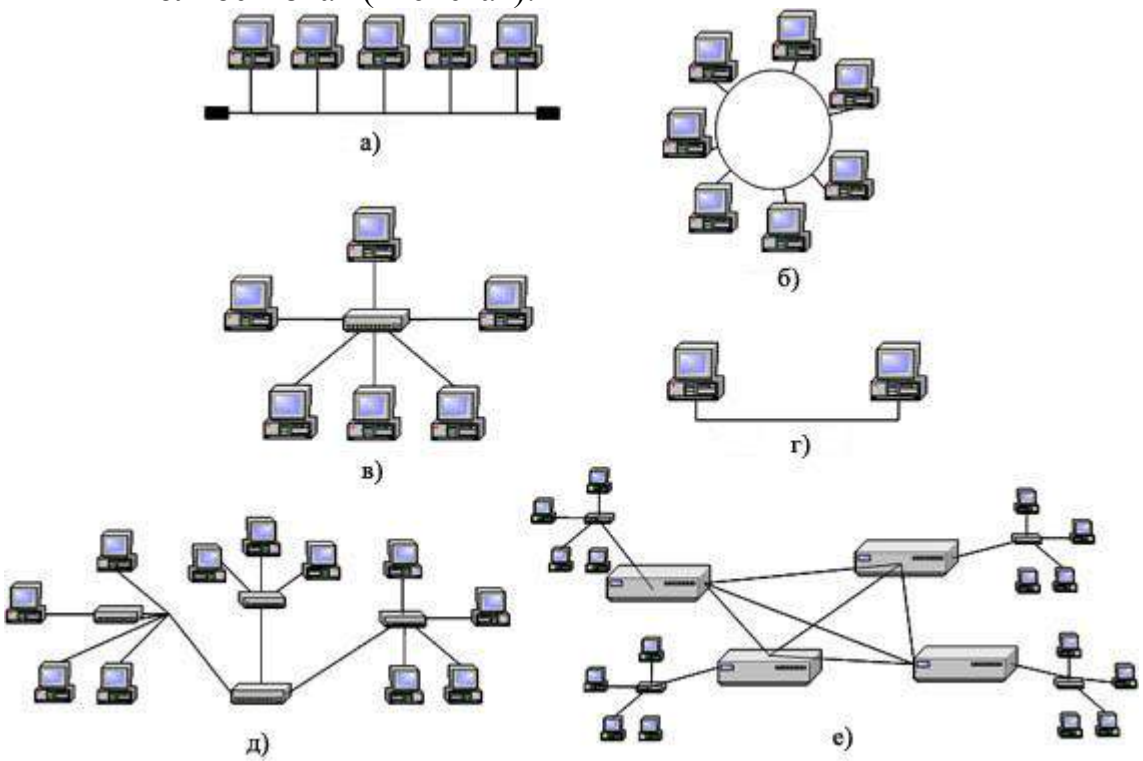
10. Приведите в отчёт описание возможных способов объединения сетевых устройств в группы с изолированным друг от друга трафиком. Укажите, на каких уровнях модели OSI (ПРИЛОЖЕНИЕ А) работают эти технологии.

## Вопросы для самоподготовки

1. Перечислите действия, необходимые для организации локальной компьютерной сети.
2. Назовите основные компоненты, входящие в состав сетевого адаптера.
3. Назовите известные Вам скорости и режимы передачи данных, используемые в сетевых адаптерах, поддерживающих тот либо иной вариант технологии Ethernet.
4. Перечислите системные ресурсы, потребляемые сетевыми адаптерами.
5. Опишите отличия работы сетевого коммутатора и сетевого маршрутизатора.
6. Охарактеризуйте режим инфраструктуры беспроводной локальной сети.
7. Назовите порядок раскладки проводов в разъёме RJ-45 согласно стандарту *TIA/EIA-568B*.
8. Поясните, в каких случаях и почему применяются прямой и перекрёстный кабели UTP.
9. Назовите параметры стек сетевых протоколов TCP/IP, конфигурируемые для компьютеров сети.
10. Опишите формат IP-адреса 4-й версии протокола IP. Почему максимальное значение любого из чисел IP-адреса ограничено `255`?
11. Опишите формат вывода работы утилиты `ping`.
12. Что называют шлюзом сети?
13. Какие дополнительные возможности при связи компьютеров даёт организация в сети DNS-сервера?
14. Какие дополнительные возможности даёт организация в сети DHCP-сервера?
15. Чем сетевой принтер отличается от обычного принтера, подключённого к компьютеру, входящему в локальную сеть?
16. Что такое Cisco IOS?
17. Опишите возможности технологии VLAN и способы организации VLAN в сетевых устройствах.

## Тесты для контроля усвоения знаний

1. Выберите соответствие рисунков, указав букву подписи, и названий сетевых топологий:
   - шина;
   - звезда;
   - кольцо;
   - точка – точка;
   - древовидная;
   - полносвязная (ячеистая).




2. Выберите правильные определения сетевых устройств из приведенного перечня:
   а) сетевой интерфейсный адаптер;
   б) концентратор;
   в) коммутатор;
   г) маршрутизатор.

Сетевое устройство, принимающее поток битов, поступающих из сети, на один из своих портов и передающее этот поток на все остальные порты – это …

Электронная плата, устанавливаемая в разъем системной платы компьютера и обеспечивающая подключение и прием-передачу данных по линиям компьютерной сети – это …

Устройство, получающее сетевые пакеты на один из своих портов и передающее их на другой соответствующий порт, определяемый в зависимости от значения адреса сетевого уровня в заголовке пакета, – это …

Устройство, принимающее кадры из сети на один из своих портов и передающее эти кадры на соответствующий другой порт, определяемый по MAC-адресу получателя в заголовке кадра, – это …

3. Выберите соответствие названий типов сетей устройств из приведенного перечня в зависимости от их масштаба:
   а) муниципальная вычислительная сеть (Munitipal Area Network – MAN);
   б) территориальная вычислительная сеть (Wide Area Network – WAN);
   в) локальная вычислительная сеть – ЛВС (Local Area Network – LAN);
   г) кампусная вычислительная сеть (Campus Area Network – CAN);
   д) персональная вычислительная сеть (Personal Area Network – PAN).

Сеть, обеспечивающая передачу данных в пределах страны или континента, – это …

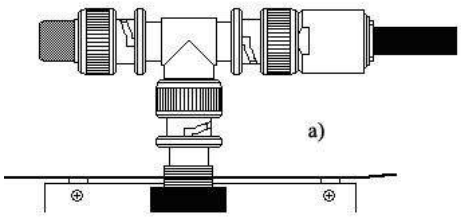
Сеть, объединяющая провайдеров услуг Интернет в одном городе, – это …

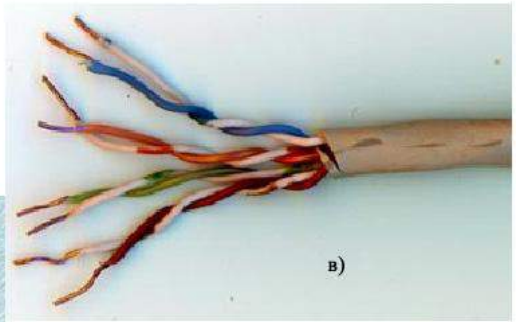
Сеть, объединяющая компьютеры компьютерного класса, – это …

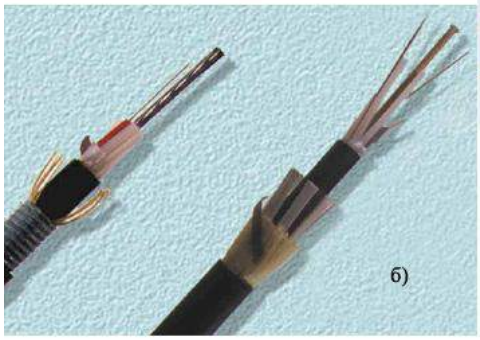
Сеть, объединяющая коммуникационные устройства одного человека, – это …

Сеть, объединяющая университетские компьютеры и компьютеры, находящиеся в общежитиях и других зданиях студенческого городка, – это …

4. Определите тип кабелей на рисунках, указав букву подписи:




- медный коаксиальный кабель;
- медный кабель типа "неэкранированная витая пара" (Unshielded Twisted Pair – UTP);
- оптоволоконный кабель.

5. Установите соответствие между указанными в списке названиями и определениями режимов передачи данных:
   а) полнодуплексный (Full Duplex);
   б) полудуплексный (Half Duplex);
   в) симплексный (Simplex).

Режим, при котором передача и прием данных происходят одновременно, – это …

Режим, при котором передача и прием данных происходят по очереди, – это …

Режим, при котором происходит только передача или только прием данных, – это …

6. Расположите в правильном порядке уровни модели ISO взаимодействия открытых систем (Open System Interconnect), пронумеровав уровни от нижнего до верхнего – от 1 до 7:
   - транспортный =
   - физический =
   - канальный =
   - сетевой =
   - представления данных =
   - прикладной =
   - сеансовый =

7. Выберите соответствие между названиями и определениями уровней модели OSI:
   а) транспортный;
   б) физический;
   в) канальный;
   г) сетевой;
   д) представления данных;
   е) прикладной;
   ж) сеансовый.

Уровень, обеспечивающий проверку доступности передающей среды, адресацию интерфейсов сетевых устройств, реализацию механизмов определения и коррекции ошибок передачи, – это …

Уровень, обеспечивающий адресацию сетей, подсетей и рабочих станций, а также передачу пакетов данных из сети в сеть с выбором оптимального маршрута к получателю, – это …

Уровень, обеспечивающий передачу битов данных по передающей среде, – это …

Уровень, обеспечивающий возможность одновременной передачи отправителем нескольких потоков данных, а также обеспечивающий гарантированную передачу данных, – это …

Уровень, обеспечивающий преобразование формата данных, представляемых вышележащим уровнем, в некоторый общий формат представления данных, а также шифрование и дешифрование данных, – это …

Уровень, обеспечивающий определение активной стороны при передаче данных, а также синхронизацию соединения с возможностью установки контрольных точек, – это …

Уровень, предоставляющий пользовательским приложениям сетевые протоколы и службы для обеспечения передачи данных по сети, – это …

8. Укажите название утилиты, пересылающей набор тестовых пакетов на удаленный компьютер и получающей от него в случае его нормальной работы ответные пакеты
   а) gong;
   б) ping;
   в) ring;
   г) gang.
9. Выберите компоненты, входящие в состав сетевого адаптера:
   а) постоянное запоминающее устройство с BIOS;
   б) разъем для подключения кабеля;
   в) контроллер аппаратных прерываний IRQ;
   г) кварцевый элемент тактового генератора;
   д) СБИС контроллера сетевого адаптера;
   е) панелька для BootROM;
   ж) южный мост (Input-Output Controller Hub).
10. Выберите минимальное количество настроек, необходимых для организации работы компьютера настройки в сети с сетевым протоколом TCP/IP:
    а) установить IP-адрес компьютера;
    б) установить основной шлюз подсети данного компьютера;
    в) установить маску подсети, в которую входит компьютер;
    г) установить IP-адрес DNS-сервера локальной сети компьютера;
    д) установить IP-адрес почтового сервера домена;
    е) установить IP-адрес прокси-сервера.
11. Выберите вариант, в котором правильно расположены в порядке возрастания значений полосы пропускания следующие среды передачи данных – коаксиальный медный кабель, кабель на основе медной витой пары, оптоволоконный кабель:
    а) коаксиальный медный кабель, кабель на основе медной "витой пары", оптоволоконный кабель;
    б) оптоволоконный кабель, коаксиальный медный кабель, кабель на основе медной "витой пары";
    в) кабель на основе медной "витой пары", коаксиальный медный кабель, оптоволоконный кабель.
12. Выберите ресурсы, выделяемые операционной системой сетевому адаптеру:
    а) MAC-адрес адаптера;
    б) порт ввода-вывода (I/O port);
    в) полоса пропускания канала;
    г) запрос прерывания IRQ;

д) диапазон адресов памяти адаптера.

13. Укажите вводимую в окне командной строки команду, отображающую IP-адрес компьютера, работающего под операционной системой Windows:
    а) `cmd`;
    б) `net`;
    в) `ipconfig`;
    г) `netstat`.
14. Укажите преимущества использования компьютерных сетей:
    а) возможность оперативной коммуникации между участниками сети и оперативного доступа к информации;
    б) возможность совместного использования аппаратных ресурсов;
    в) возможность практически безграничного увеличения вычислительной производительности систем;
    г) возможность организации совместной работы путем разделения прикладных программ и файлов;
    д) упрощение конфигурирования и пользования операционными системами и пользовательскими программами;
    е) возможность централизованного управления данными и программами.

## Литература


1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с.: ил.
2. Новиков Ю.В. Основы локальных сетей: курс лекций : учеб. пособие: для студентов вузов, обучающихся по специальностям в обл. информ. технологий Ю.В. Новиков, С.В. Кондратенко. – М.: Интернет-ун-т информ. технологий, 2005. – 360 с.
3. Официальный сайт Cisco Systems. Программа Cisco Packet Tracer [электронный ресурс]. – Режим доступа: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html.

# РАЗДЕЛ 2
# ОРГАНИЗАЦИЯ СОВМЕСТНО ИСПОЛЬЗУЕМЫХ СЕТЕВЫХ РЕСУРСОВ

## 2.1. Компоненты организации сетевого доступа и сетевые разрешения

Операционные системы Microsoft Windows (здесь и далее под Windows подразумеваются операционные системы Windows 9x/NT/2000//XP/Vista/7) для доступа к сети используют Сетевые подключения через сетевые интерфейсные адаптеры, модемы и другие интерфейсные устройства (их можно увидеть в окне, открываемом последовательностью команд Панель управления – Центр управления сетями и общим доступом – Изменение параметров адаптера (рис. 35)).

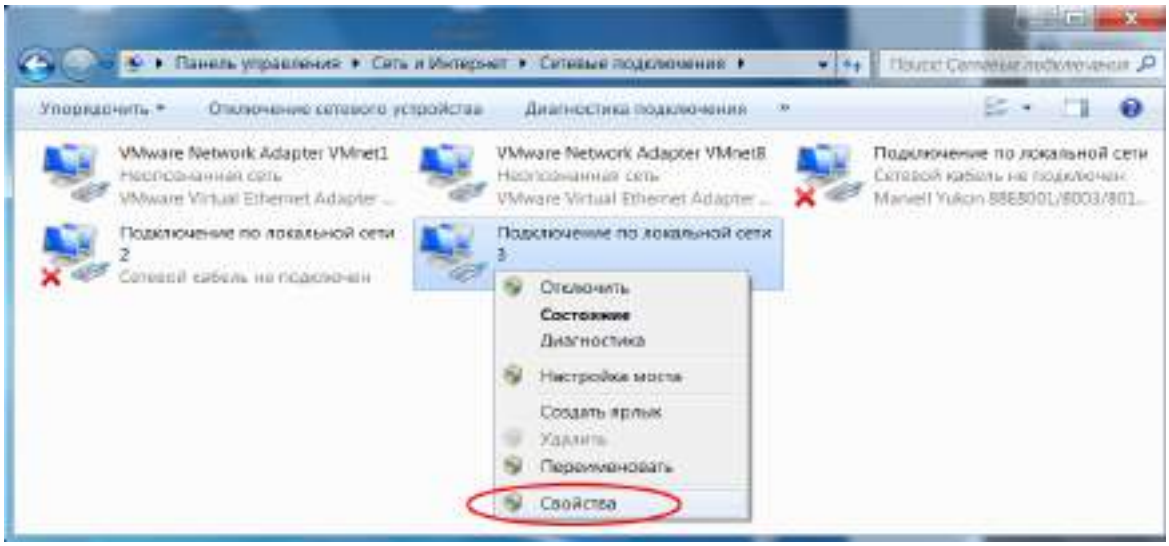



Рис. 35. Сетевые подключения в операционной системе Windows

Выбрав в контекстном меню сетевого подключения команду Свойства можно увидеть используемые этим подключением сетевые компоненты, основными из которых являются (рис. 36):

- драйвер сетевого адаптера;
- протоколы;
- клиент;
- службы.

*Драйвер сетевого адаптера* – программное обеспечение, обеспечивающее взаимодействие операционной системы с адаптером, через который выполняется подключение. Драйвер может быть создан как производителем операционной системы, так и производителем самого адаптера, настройки сетевого адаптера, выполняемые через драйвер, приведены на Рис. 3.

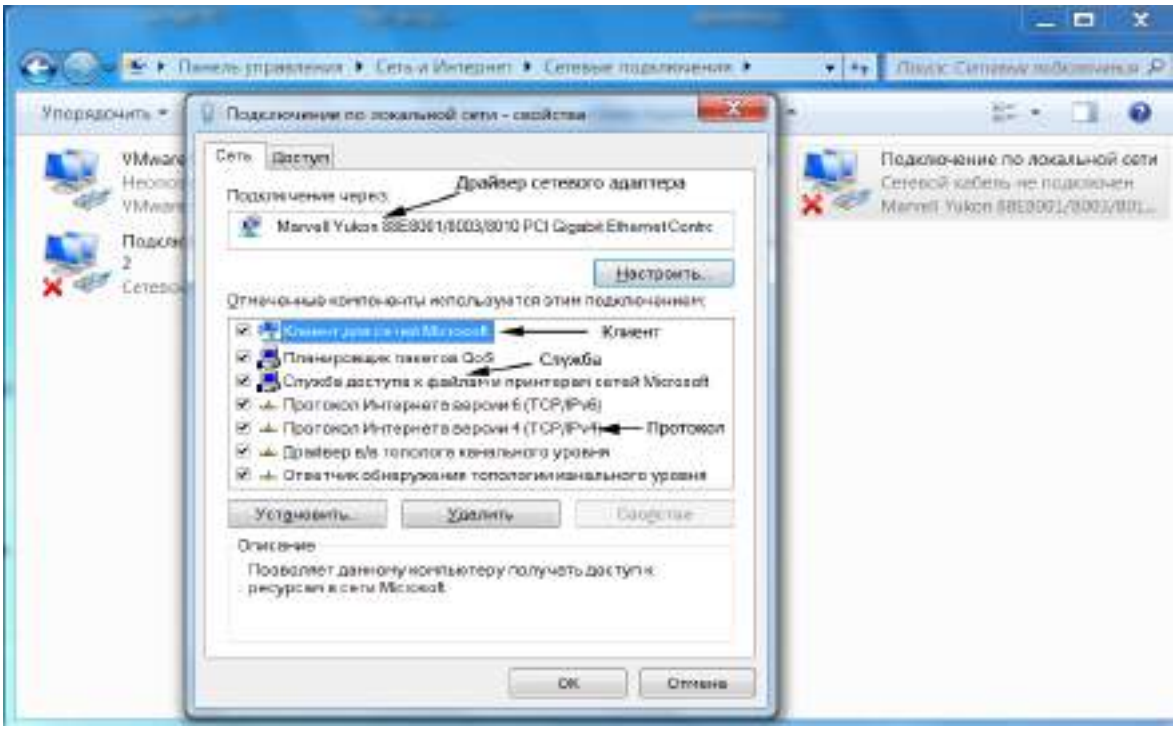



Рис. 36. Сетевые компоненты, используемые подключением

*Сетевой протокол* – программное обеспечение, реализующее набор правил, позволяющих осуществлять соединение и обмен данными между двумя и более подключёнными к сети устройствами. Основными задачами протоколов являются разбиение потока информации на пакеты, формирование заголовков пакетов с адресной и другой информацией, позволяющей реализовывать различные механизмы протоколов по надёжной доставке данных, обеспечению целостности данных, безопасности передачи и др. Обязательным условием работы сети является наличие одинаковых стеков сетевых протоколов на компьютерах – участниках сети. Необходимо отметить, что существуют и совместимые сетевые протоколы, например, IP версий 4 и 6. Наиболее распространённым стеком сетевых протоколов в настоящее время является стек TCP/IP с IP 4-й версии, однако уже осуществляется переход к новой 6-й версии IP и современные операционные системы по умолчанию устанавливают стеки с обеими версиями (рис. 36). Задание сетевых адресов интерфейса подключения (IP-адресов) для протокола IP версии 4 показано на рис. 12.

*Клиент* – программное обеспечение, позволяющее компьютеру обращаться к сетевым ресурсам серверов компьютерных сетей: файловым ресурсам, принтерам, каналам доступа к Интернету. Клиент, в частности, передаёт идентификатор пользователя, по которому сервер проверяет, разрешён ли ему доступ к запрашиваемому ресурсу и с какими правами. В Windows автоматически устанавливается Клиент для сетей Microsoft, позволяющий подключаться к сетевым ресурсам рабочих станций под управлением Windows, входящих в сетевые рабочие группы (Workgroups), и сетевым ресурсам доменов (Domains) компьютерных сетей под управлением операционных систем Microsoft Windows Server (имеются в виду системы

Windows Server NT/2000/2003/2008/2011). Параметры Клиента для сетей Microsoft конфигурируются автоматически, без участия пользователя.

*Сетевая служба* – программное обеспечение, работающее на сервере и обеспечивающее обслуживание клиентских запросов к сетевым ресурсам этого сервера. В Windows автоматически устанавливается Служба доступа к файлам и принтерам сетей Microsoft. Параметры этой службы конфигурируются автоматически, без участия пользователя.

В состав сетевых компонентов, устанавливаемых по умолчанию, также включён ряд других дополнительных протоколов и служб, которые используются для реализации дополнительных возможностей компьютерных сетей. По умолчанию в Windows 7 устанавливаются также:

- Планировщик пакетов QoS – служба, реализующая поддержку «качества обслуживания» (*Quality of Service – QoS*) – набора технологий, обеспечивающих приоритетное использование канала связи некоторыми видами трафика или программами по сравнению с методом «равных возможностей»;
- Протокол Интернета (стек TCP/IP) 6 версии – стек с новой реализацией IP, для которой характерно большее пространство адресов (используются 128-битные адреса), автоматическое конфигурирование интерфейсов, оптимизированная маршрутизация пакетов, передача трафика мультимедиа с минимальными задержками и др.;
- Драйвер ввода-вывода топологии канального уровня – это компонент сетевой инфраструктуры Windows, благодаря которому компьютеры и другие устройства могут быть нанесены на карту сети. Увидеть её можно в Центре управления сетями и общим доступом по ссылке Просмотр полной карты. На карту наносятся все обнаруженные в сети компьютеры и сетевые устройства (рис. 37);
- Ответчик обнаружения топологии канального уровня – также отвечает за заполнение сетевой карты.

Если на компьютере не установлена служба доступа к файлам и принтерам, то он может обращаться к другим компьютерам сети, но другие компьютеры не могут обращаться к нему. Серверные функции обеспечивает служба доступа к файлам и принтерам. Она позволяет выделять в совместное использование для пользователей сети такие ресурсы компьютера, как диски, папки и принтеры. Если в сети все компьютеры сконфигурированы с наличием и клиентского, и серверного компонентов, такая сеть называется *одноранговой* или *пиринговой* (*Peer-To-Peer*).

Следует отметить реализованную в современных операционных системах возможность организации для компьютеров локальной сети *общего канала доступа к Интернету*. При использовании этой технологии на подключённом к Интернету компьютере, который через другой интерфейс подключён к локальной сети, можно обеспечить подключение к Интернету остальных компьютеров локальной сети (рис. 38).

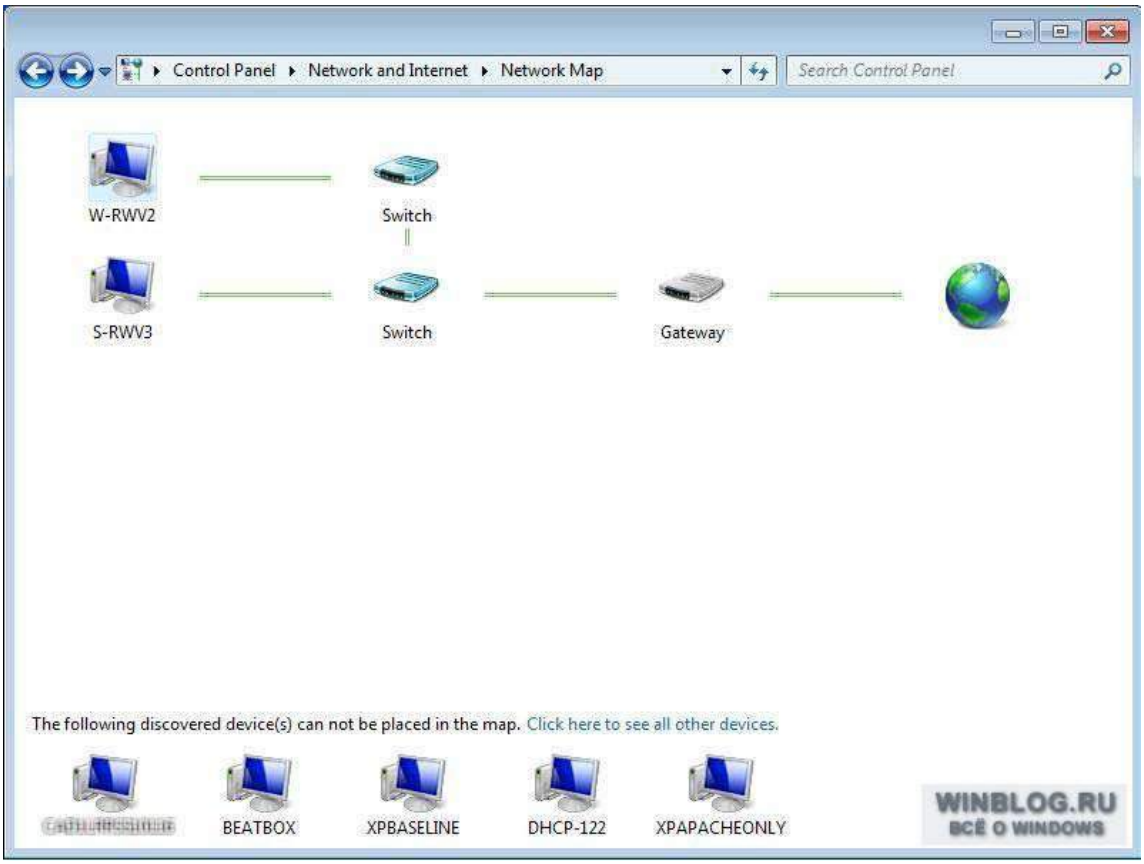



Рис. 37. Карта сети в Windows 7

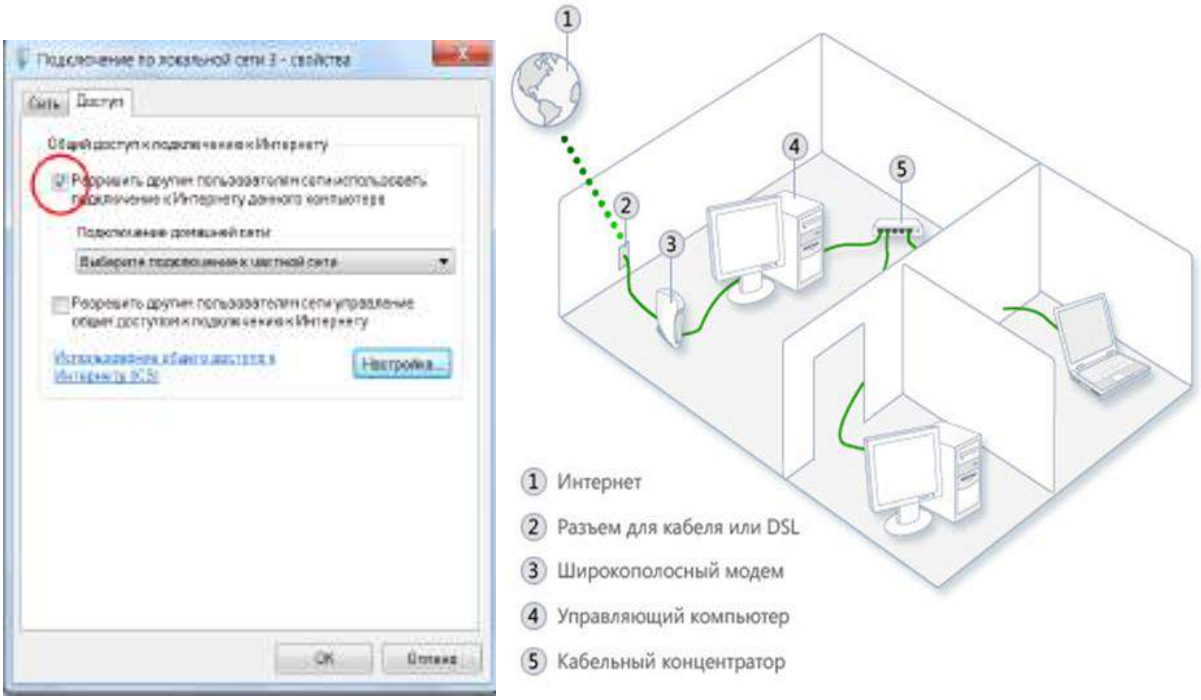



Рис. 38. Настройка общего доступа к подключению Интернета в Windows 7

Для компьютеров, подключённых к сети, приходиться решать круг задач, связанных с обеспечением информационной безопасности. Если необходимо предоставить другим пользователям доступ к тому или иному сетевому ресурсу компьютера, необходимо установить разрешения на до-

ступ к этому ресурсу для *пользователей* или *групп пользователей*. Установка разрешений группам зачастую является более удобной, поскольку группе один раз назначаются все необходимые разрешения, а затем необходимые пользователи добавляются или удаляются из группы. Добавление/удаление пользователей в/из группы требует выполнения администратором меньшего числа операций, чем выделение каждому из пользователей необходимых сетевых ресурсов.

Организация совместного доступа к файловому ресурсу данного компьютера по сети выполняется в Проводнике выбором команды Свойства из контекстного меню папки/диска, для которых должен быть организован общий доступ по сети (рис. 39).

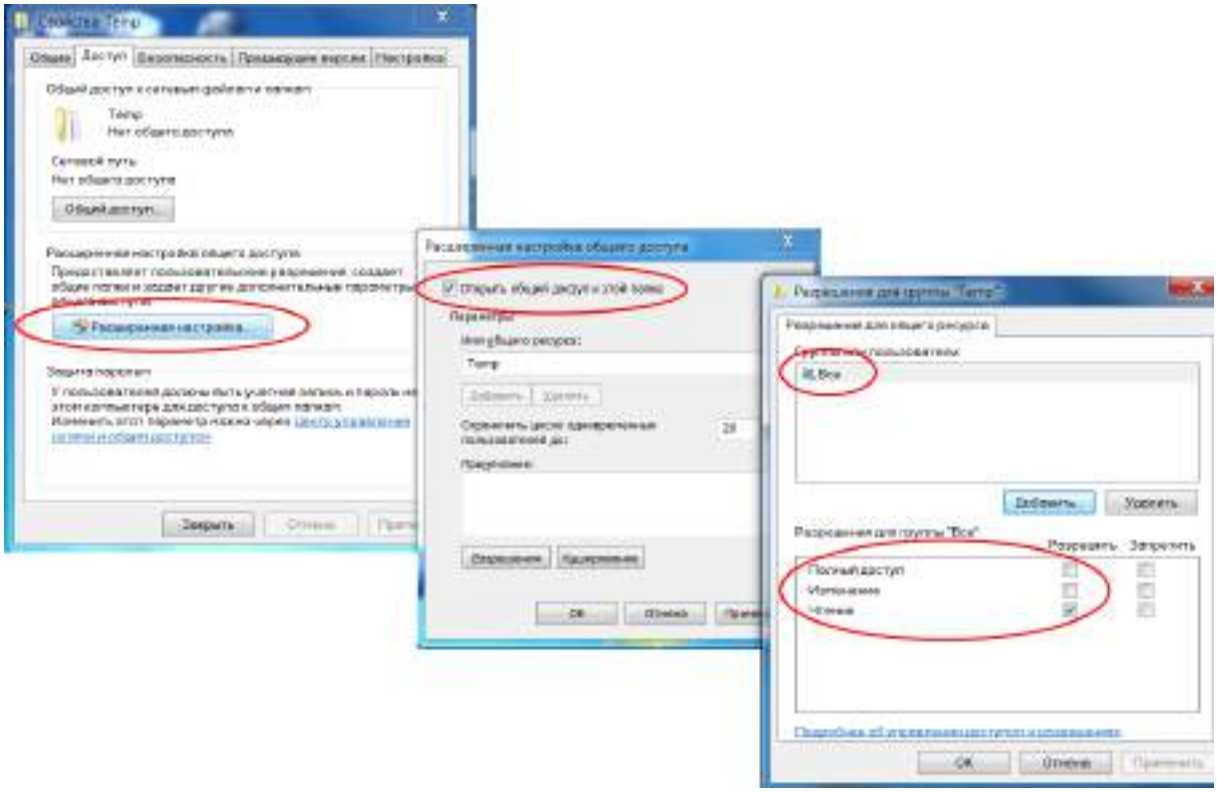


Рис. 39. Организация общего доступа по сети к папке Temp

В Windows существует три типа разрешений для сетевого доступа к файловым ресурсам: Только чтение, Изменение и Полный доступ. Разрешение Чтение используется по умолчанию для всех новых общих ресурсов и назначается группе пользователей Все (при этом под Все понимаются все пользователи, зарегистрированные в операционной системе данного компьютера или, если данный компьютер входит в домен Windows, зарегистрированные как пользователи домена в серверной операционной системе контроллера домена).

Разрешение Чтение позволяет:

- просматривать имена файлов и подкаталогов;
- просматривать подпапки;
- просматривать данные в файлах;
- выполнять программные файлы.

Разрешение Изменение включает разрешение Чтение, а также позволяет:

- добавлять файлы и подпапки;
- изменять данные в файлах;
- удалять подпапки и файлы.

Разрешение Полный доступ включает разрешения Изменение, а также позволяет:

- изменять разрешения безопасности (только для файлов и папок *NTFS – New Technology File System* – файловая система, использующая механизмы управления доступом к файловым ресурсам по идентификаторам пользователей/групп и спискам разрешений на операции с этими ресурсами);
- стать владельцем ресурса (только для файлов и каталогов NTFS).

В качестве сетевых файловых ресурсов могут выступать папка (каталог) и диск. При этом разрешения, назначенные для папки, распространяются на все находящиеся в ней файлы (для подкаталогов могут быть установлены другие разрешения). Аналогично, если в совместное использование выделяется диск, то это означает, что выделяются все находящиеся на нем папки (хотя существует возможность изменять разрешения доступа для каждой из них). Следует также отметить, что пользователь с правами Администратора компьютера одноранговой локальной сети сможет подключиться по сети к дискам этого компьютера, даже если они не выделены в совместное использование (указав в строке команды Выполнить `\\Имя_компьютера\Имя_диска$`, например, `\\PC1\C$`). Администраторы домена могут выполнять аналогичные действия для любых компьютеров, входящих в домен.

В Windows существует возможность подключения к выделенному для совместного использования по сети ресурсу сервера путём организации так называемого сетевого диска на своём компьютере с присвоением ему в качестве идентификатора незанятой другими дисками буквы латинского алфавита. При этом дальнейший доступ и использование такого ресурса с точки зрения пользователя ничем не будет отличаться от использования локальных дисков.

Для средних и крупных компьютерных сетей фирма Microsoft предлагает технологию использования доменов сетей. Характерной особенностью домена является наличие в нем сервера (Windows Server NT/2000/2003/2008/2011) – так называемого *контроллера домена* – с централизованной базой данных пользователей, выполняющего аутентификацию пользователей в начале их работы и хранящего разрешения на использование сетевых ресурсов на различных рабочих станциях домена. Это позволяет пользователям входить в домен с любого компьютера и пользоваться выделенными для них ресурсами на различных компьютерах. Необходимо отметить, что для того, чтобы реализовать подобную работу в одноранговой сети без построения домена, необходимо на каждом компьютере завести одинаковый перечень пользователей (и групп) с одинаковыми

паролями пользователей, что, в общем случае, сложно для большого количества компьютеров и пользователей.

Следует обратить внимание на принципиальное различие настроек, доступных на вкладках Доступ и Безопасность свойств папки и диска. Вкладка Доступ служит для организации общего доступа по сети и позволяет задавать пользователям и группам описанные выше разрешения Полного доступа, Изменения и Чтения (рис. 39). Вкладка Безопасность регулирует доступ к файловым ресурсам на основе разрешений файловой системы NTFS, характерной для современных версий Windows (рис. 40). Эта система для каждого файлового ресурса поддерживает так называемый *список разрешений доступа* (*Access Control List – ACL*), содержащий перечень идентификаторов пользователей и групп, которым разрешено использование этого ресурса, и их разрешений. Отметим большее количество типов разрешений в этом случае и тот факт, что эти разрешения работают при интерактивном входе пользователя на компьютер (то есть при его регистрации на данном компьютере при помощи клавиатуры).

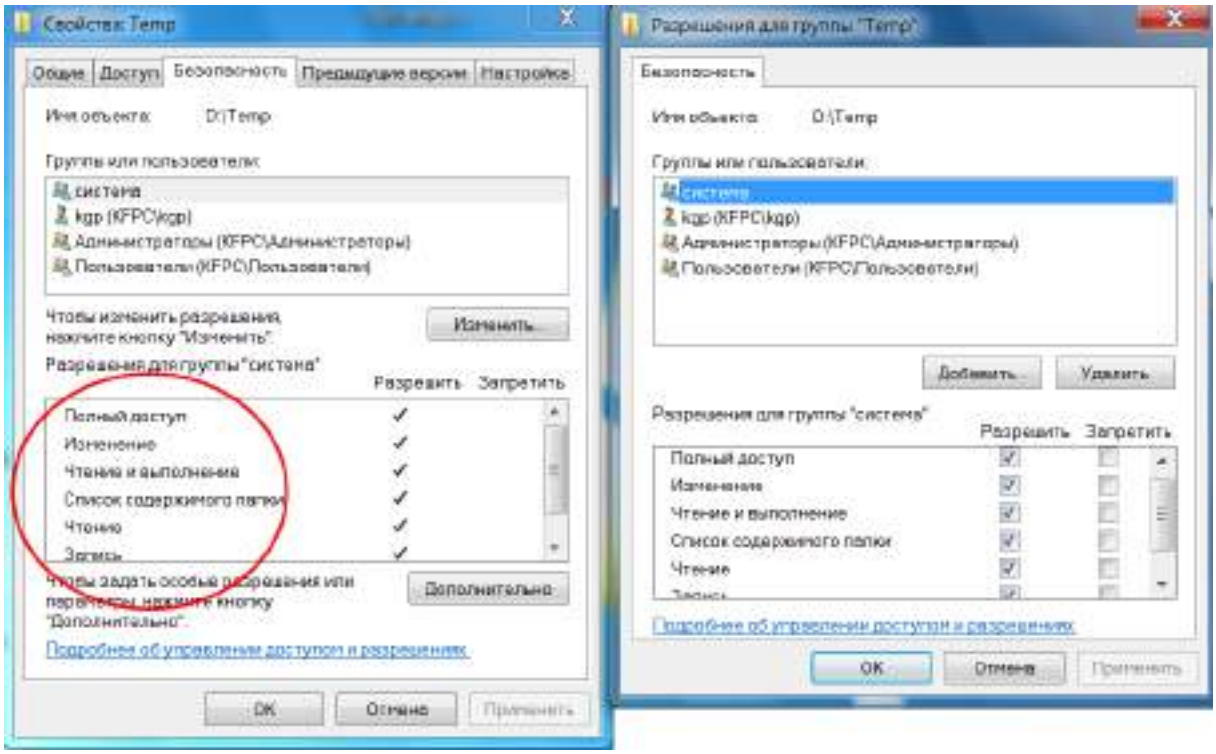



Рис. 40. Разрешения NTFS папки Temp

## 2.2. Организация сетевого доступа к каталогам (папкам) в Windows

- Запустите программу Проводник.
- Выделите в Проводнике папку, к которой необходимо организовать совместный сетевой доступ, и откройте её контекстное меню. В контекстном меню выберите команду Свойства.
- В открывшемся окне свойств папки выберите вкладку Доступ и выполните щелчок по кнопке Расширенная настройка…(рис. 39). Воз-

можно, понадобится ввести пароль Администратора, поскольку организация общего доступа является одной из его задач.

- В открывшемся окне установите отметку возле команды Открыть общий доступ к этой папке, при необходимости замените имя сетевого ресурса (по умолчанию оно совпадает с именем папки) (рис. 39).
- Выполните щелчок на кнопке Разрешения, откроется окно разрешений для соответствующей папки (рис. 41). В нем перечислены пользователи и группы пользователей, которым разрешён доступ к данной папке по сети, а также указываются права доступа для каждого пользователя или группы. Права можно изменять с помощью чекбоксов напротив типов прав в этом окне.

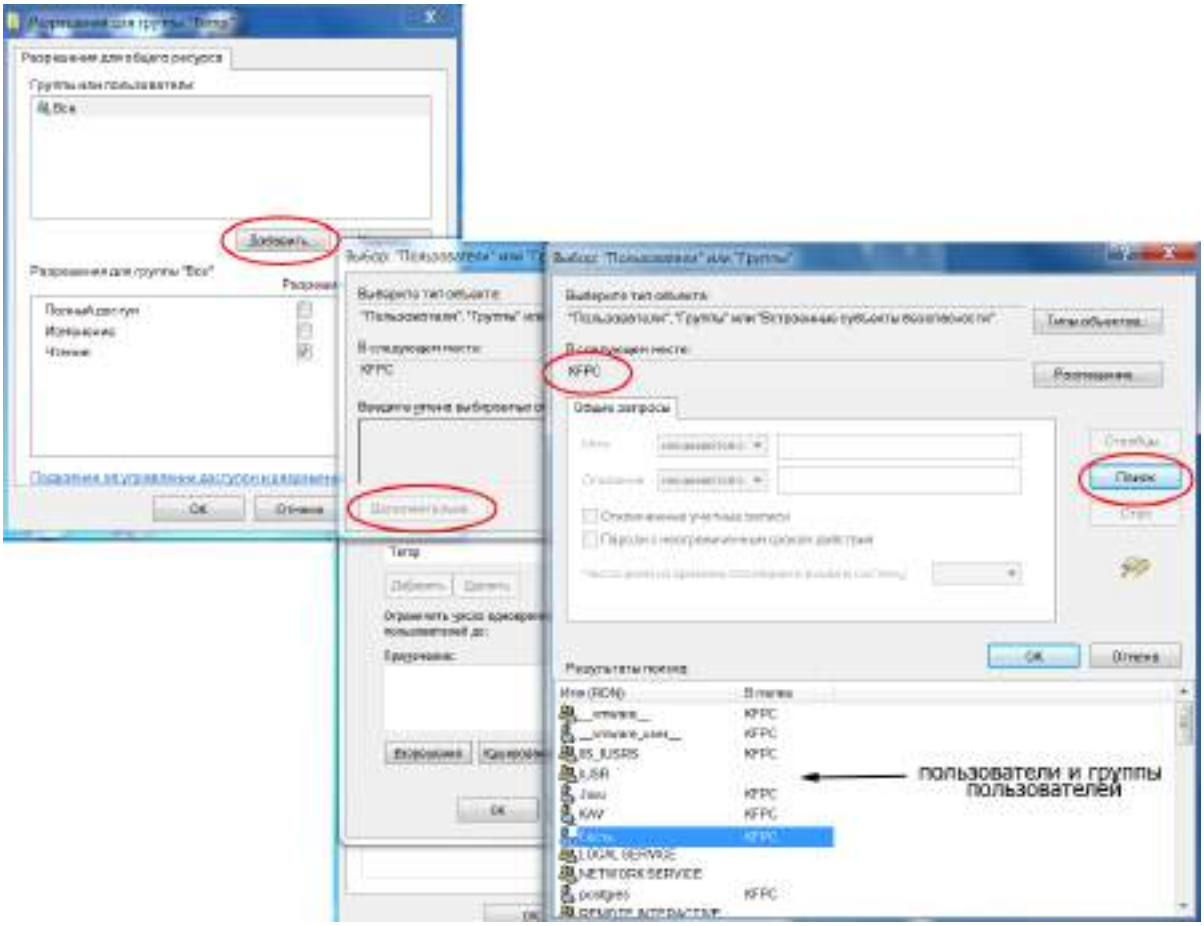



Рис. 41. Добавление пользователя при организации общего доступа к папке

- Для добавления пользователя, которому будет разрешён доступ по сети к данной папке, необходимо выполнить щелчок на кнопке Добавить и в открывшемся окне Выбор: Пользователи или Группы выполнить щелчок на кнопке Дополнительно (рис. 41).
- Окно Выбор: Пользователи или Группы развернётся и после щелчка на кнопке Поиск в правой нижней части окна, появится список пользователей и групп данного компьютера (рис. 41). Одним из пользователей, зарегистрированных в системе по умолчанию, является пользователь Гость, учётная запись которого используется для ор-

ганизации сетевого доступа к ресурсам для незарегистрированных на данном компьютере пользователей.

- Выберите в списке пользователя Гость и щёлкните на кнопке ОК. Ещё раз щёлкните на ОК в свернувшемся окне Выбор: Пользователи или Группы. По умолчанию Гостю назначается разрешение Чтение, оставьте его без изменений (рис. 42).

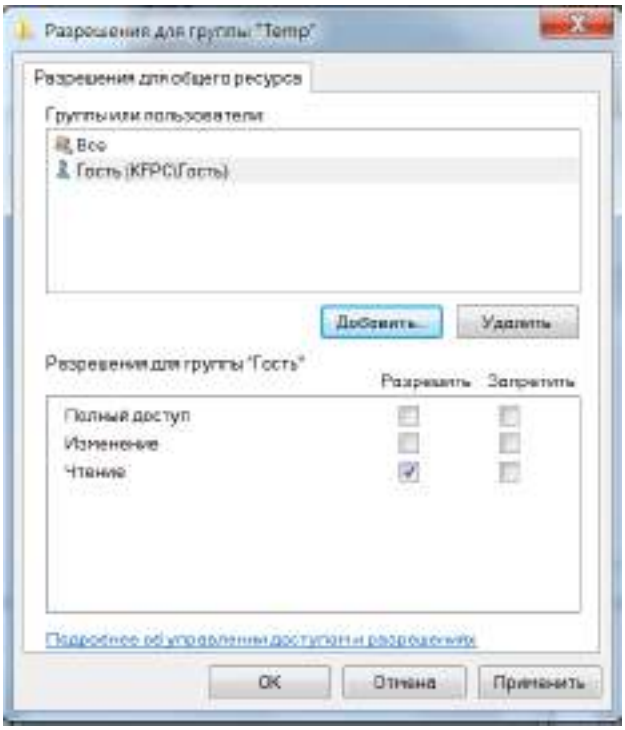



Рис. 42. Добавление пользователя Гость для папки Temp

- Повторите описанные выше действия для добавления к списку разрешённых пользователей пользователя student (или любого другого, под которым Вы сможете зарегистрироваться) с разрешением Изменение (при этом автоматически отмечается и разрешение Чтение).
- Удалите из списка разрешённых пользователей группу Все. Закройте все окна.
- Зарегистрируйтесь на соседнем компьютере локальной сети под именем student (или другим, которому организован доступ к сетевой папке) и откройте окно Сеть, выполнив щелчок мышью на соответствующей пиктограмме Рабочего стола. Вы должны увидеть список компьютеров Вашей локальной сети.
- Откройте компьютер, на котором находится выделенная для совместного использования по сети папка. Вы должны увидеть изображение папки, к которой организован доступ (рис. 43). Убедитесь, что Вы можете изменять содержимое документов и этой папки (добавьте в неё подпапку).
- Зарегистрируйтесь на своём компьютере под любым именем, которого нет в списке разрешённых пользователей для папки с об-

щим доступом. Убедитесь, что теперь Вам недоступны действия по созданию новых подпапок и файлов, а также сохранению изменённых файлов.

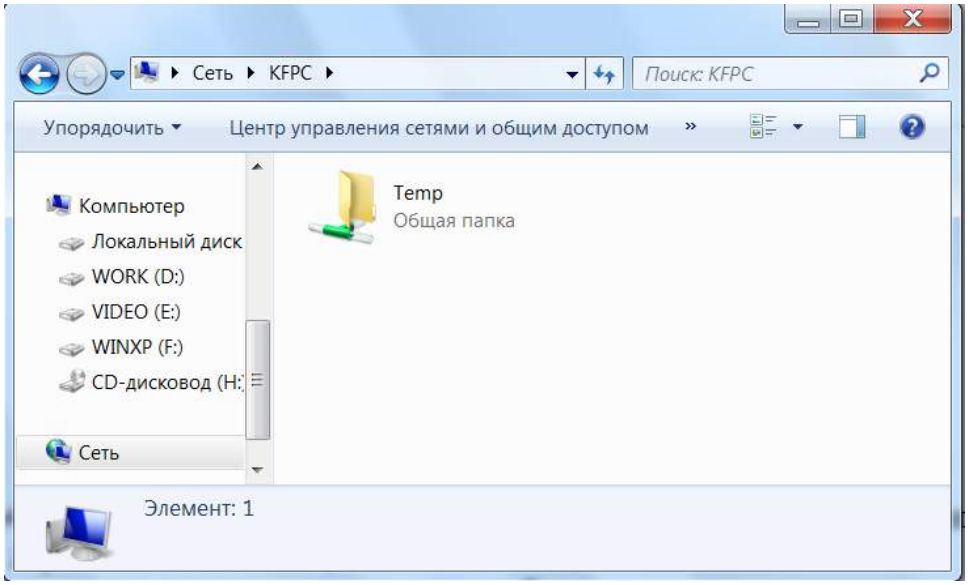



Рис. 43. Общая папка в окне Сеть

- Выполните подключение выделенной для совместного использования по сети папки сервера как сетевого диска Вашего компьютера. Для этого выполните щелчок правой кнопкой мыши по пиктограмме Сеть на Рабочем столе и выберите команду Подключить сетевой диск... В открывшемся окне выберите букву, которой будет идентифицирован сетевой ресурс в Вашей системе, и, выполнив щелчок по кнопке Обзор..., выберите необходимый сетевой ресурс на удалённом компьютере сети. Обратите внимание на запись, указывающую местонахождения ресурса: `\\Имя_компьютера\Имя_ресурса` (рис. 44).

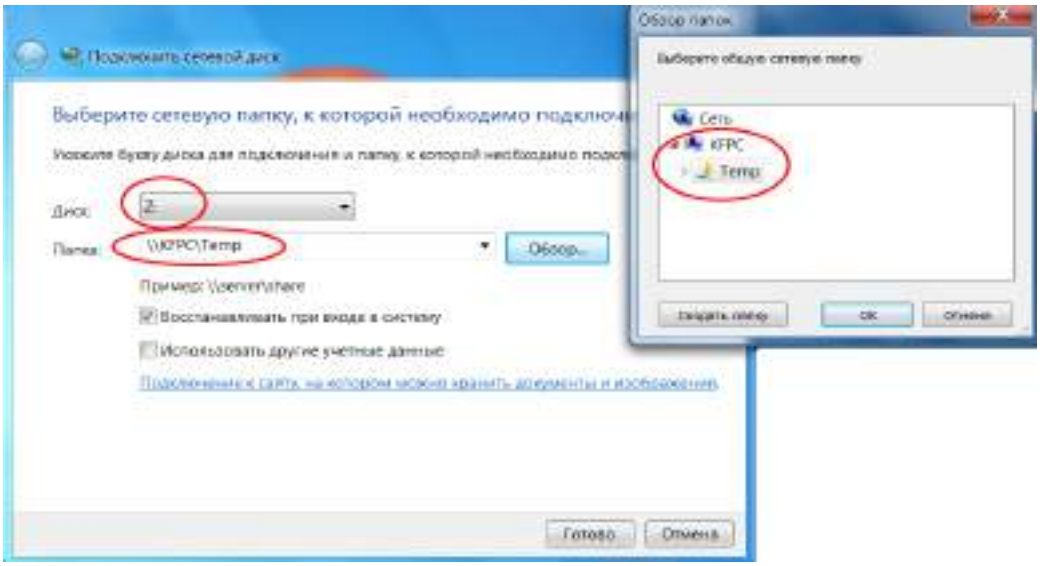



Рис. 44. Подключение выделенной в совместное использование по сети папки как сетевого диска

Существует возможность организовать подключение сетевого диска от имени другого пользователя – Использовать другие учётные данные (естественно, для этого необходимо знать его пароль). Отметка возле опции Восстанавливать при входе в систему позволяет сохранить выполненные настройки для последующих сеансов работы текущего пользователя.

Необходимо отметить, что работа одного человека под несколькими учётными записями является очень полезной. Так, если обычно выполняемая работа не требует прав Администратора системы, то настоятельно рекомендуется завести себе учётную запись с правами пользователя и работать под этой учётной записью. Только при необходимости выполнения системных работ (установка/удаление программ, настройка оборудования и т.д.) следует кратковременно использовать учётную запись Администратора. Такой подход позволит обеспечить длительную адекватную работу операционной системы, поскольку вирусные программы и другое вредоносное программное обеспечение, запущенное обычным пользователем, не может выполнять изменение системных файлов. На рис. 45 показан подключённый сетевой диск в окне Компьютера.

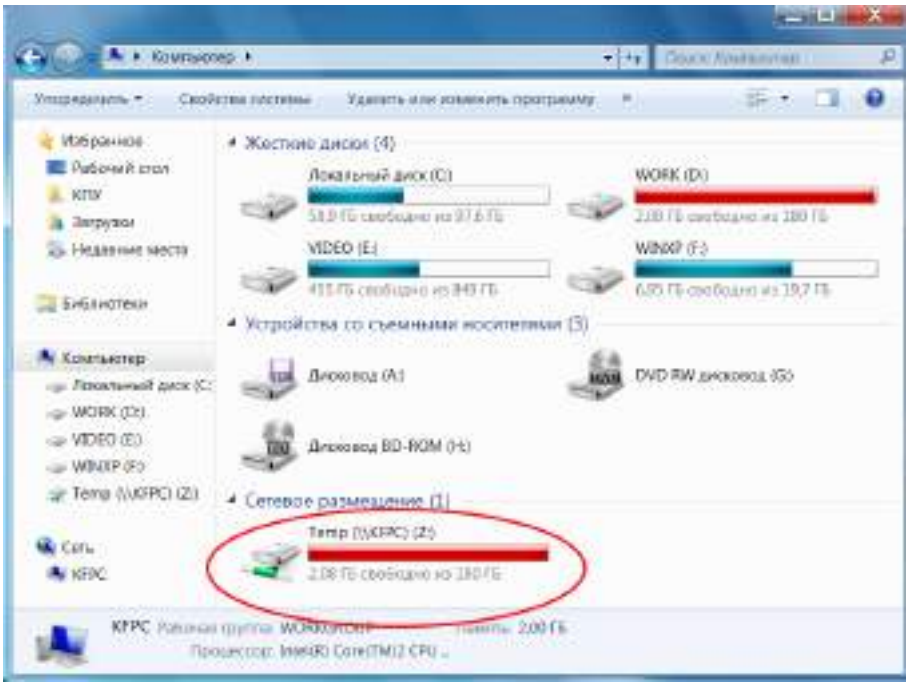



Рис. 45. Подключение выделенной в совместное использование по сети папки как сетевого диска

Для отключения сетевого диска необходимо выполнить щелчок на его пиктограмме правой кнопкой мыши и выбрать команду Отключить из контекстного меню.

## 2.3. Организация совместного использования по сети принтера в Windows

- Откройте окно Устройства и принтеры на компьютере, к которому подключён планирующийся в совместное использование по сети

принтер, выполнив щелчок по соответствующей пиктограмме в Панели управления Windows, а затем вызовите щелчком правой кнопки на пиктограмме принтера его контекстное меню (рис. 46). В этом меню выберите команду Свойства принтера.

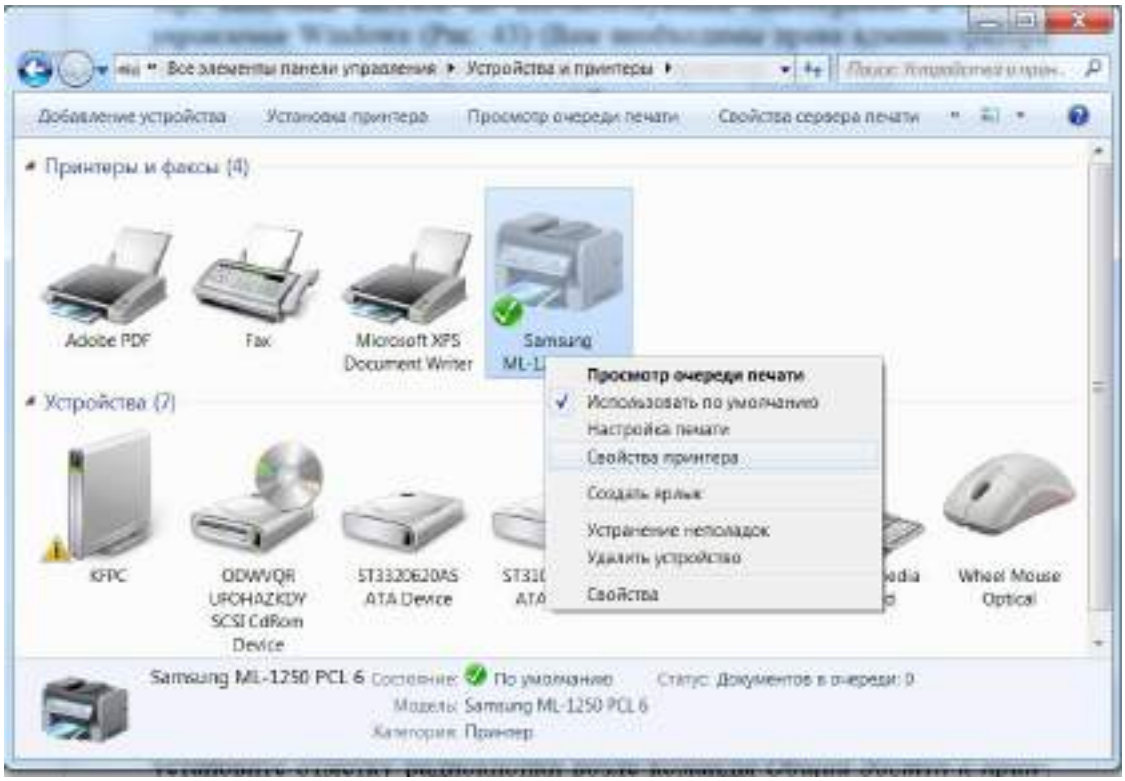



Рис. 46. Окно Устройства и принтеры с контекстным меню принтера, планирующегося к использованию по сети

- В открывшемся окне свойств принтера выполните щелчок на вкладке Доступ и установите отметку возле команды Общий доступ к данному принтеру. В текстовом поле Сетевое имя можно задать имя, под которым принтер будет виден в сети (по умолчанию оно совпадает с названием модели принтера) (рис. 47).
- На вкладке Безопасность указывается список пользователей и их прав относительно выполнения сетевой печати (добавление пользователей и прав производится аналогично действиям, описанным для конфигурирования сетевой папки). По умолчанию для всех зарегистрированных в системе пользователей разрешается только Печать, для Администраторов дополнительно Управление принтерами и Управление документами, для пользователя СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ – только Управление документами (рис. 48). Разрешение Управление принтерами обеспечивает полный административный контроль над принтером: пользователь может приостанавливать и возобновлять работу принтера, изменять параметры очереди печати, предоставлять принтер в совместное использование, корректировать разрешения для принтера и изменять свойства принтера. Разрешение Управление документами обеспечивает возможность приостановки,

возобновления, перезапуска, отмены и изменения очереди печати документов, отправленных другими пользователями.

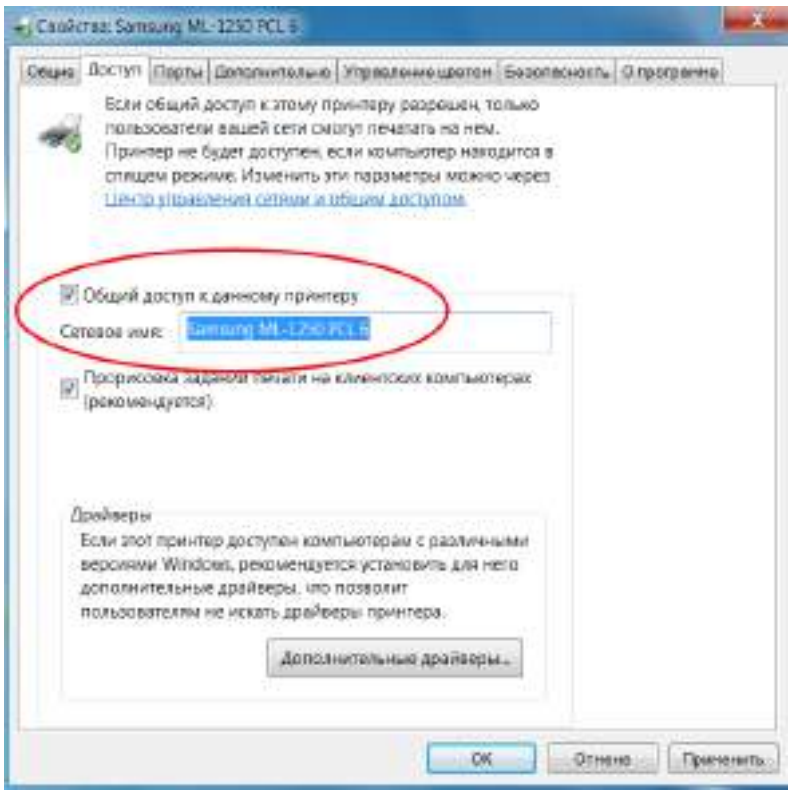



Рис. 47. Вкладка установки общего доступа к принтеру

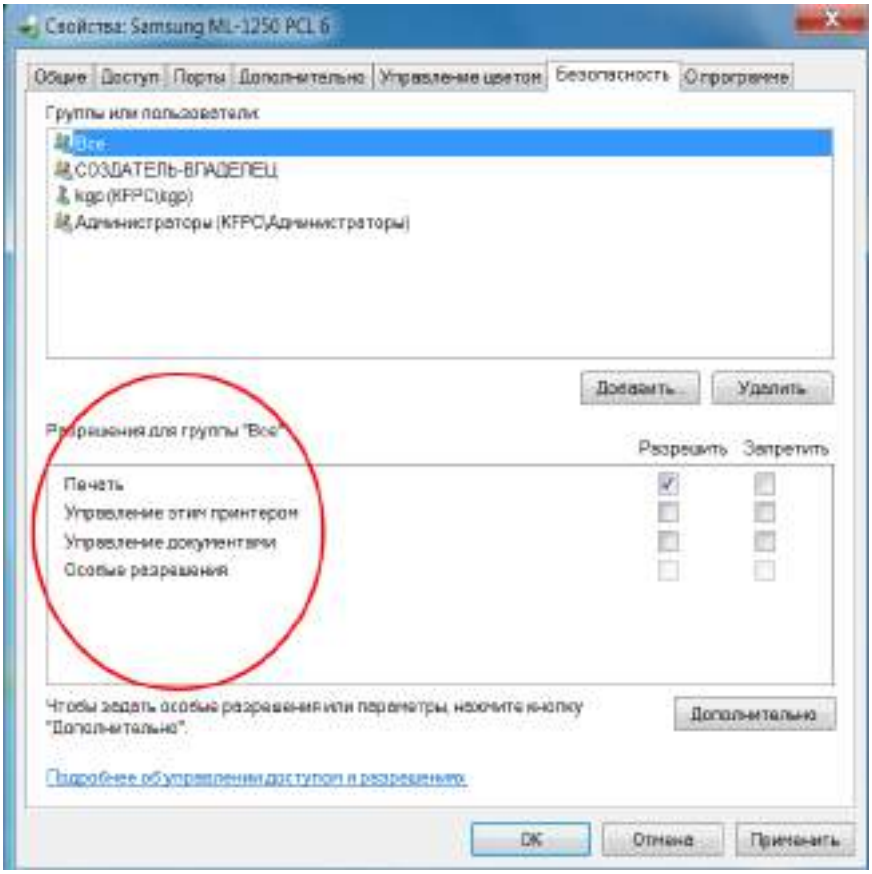



Рис. 48. Вкладка разрешений для сетевого принтера

- Откройте с соседнего компьютера локальной сети окно Сеть, выполнив щелчок мышью на одноименной пиктограмме Рабочего стола. Вы должны увидеть список компьютеров Вашей локальной сети. Откройте компьютер, на котором находится сетевой принтер. Вы должны увидеть изображение принтера, к которому организован доступ (рис. 49).

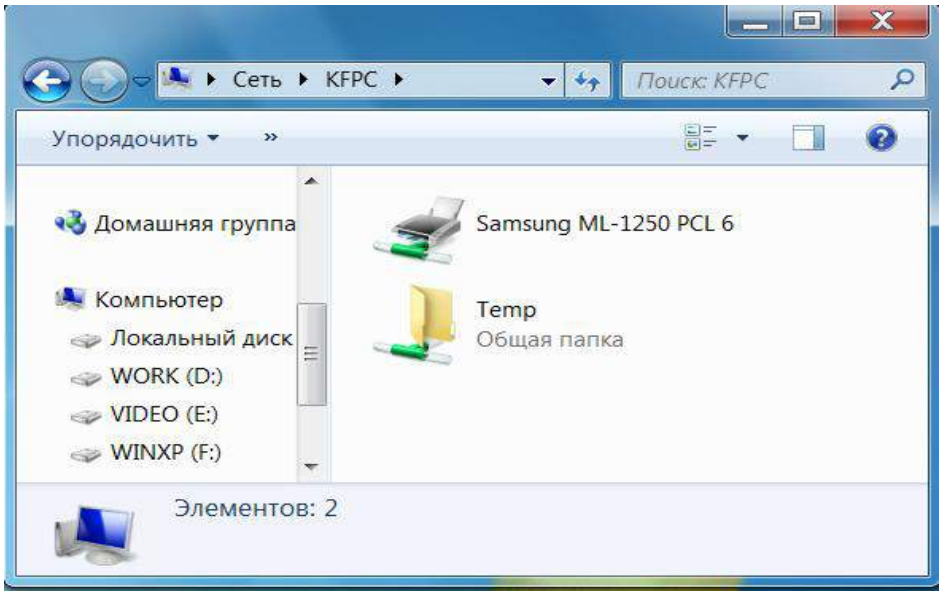



Рис. 49. Окно сетевых ресурсов удалённого компьютера

- Выполните установку на Вашем компьютере (компьютере локальной сети, к которому не подсоединён принтер) сетевого принтера. Для этого откройте окно Устройства и принтеры и выполните команду Установка принтера в строке меню команд (или выполните щелчок на свободном месте окна правой кнопкой и выберите команду Добавить принтер). Запустится Мастер установки принтеров.
- В окне Мастера выберите опцию Добавить сетевой, беспроводный или Bluetooth-принтер и выполните щелчок на кнопке Далее (рис. 50).
- Мастер выполнит поиск доступных сетевых принтеров и предоставит их в списке (рис. 51). Выберите необходимый и нажмите Далее. Если список будет пуст или в нем будет отсутствовать необходимый сетевой принтер, существует возможность указать его вручную выбором команды Нужный принтер отсутствует в списке.
- В открывшемся окне будет выведена информация об установленном на Вашем компьютере сетевом принтере и после нажатия на кнопку Далее откроется последнее окно Мастера с предложением выполнить Печать пробной страницы на установленном сетевом принтере.
- В окне Устройства и принтеры компьютера, на котором сконфигурирован сетевой принтер, должна появиться его пиктограмма.
- Откройте любое приложение Windows, например Microsoft Word, наберите несколько слов документа и выполните команду Файл-

Печать. Откроется окно печати, в котором будет указан сетевой принтер. Распечатайте документ на сетевом принтере.

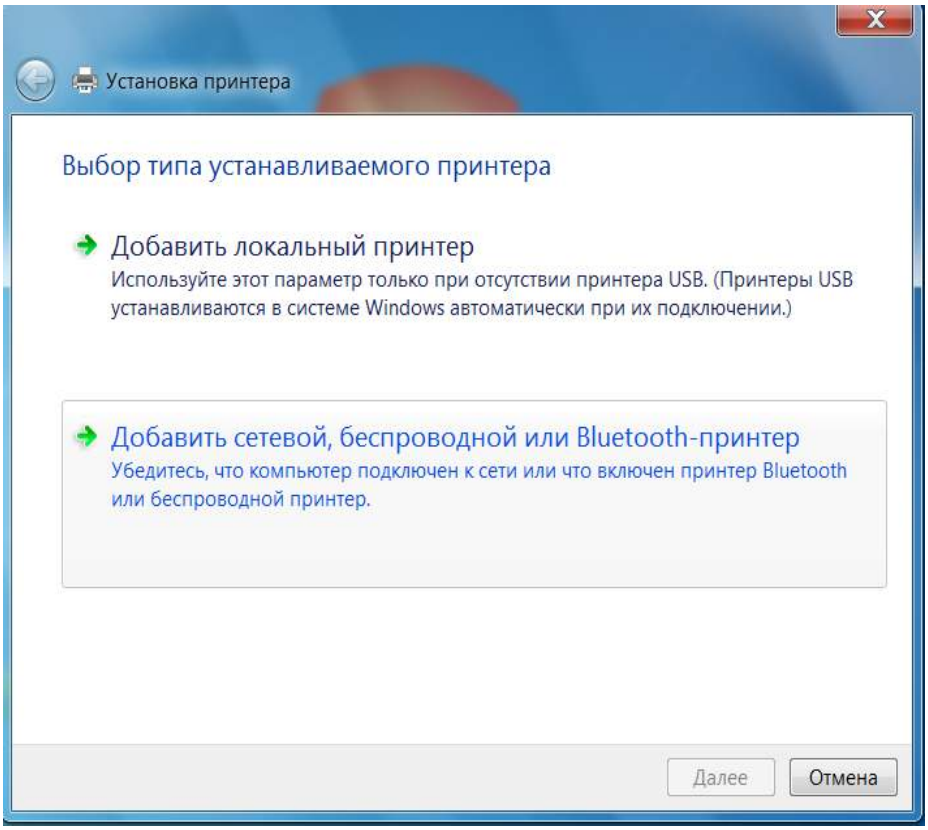



Рис. 50. Окно Мастера установки принтера с указанием в качестве подключаемого сетевого принтера

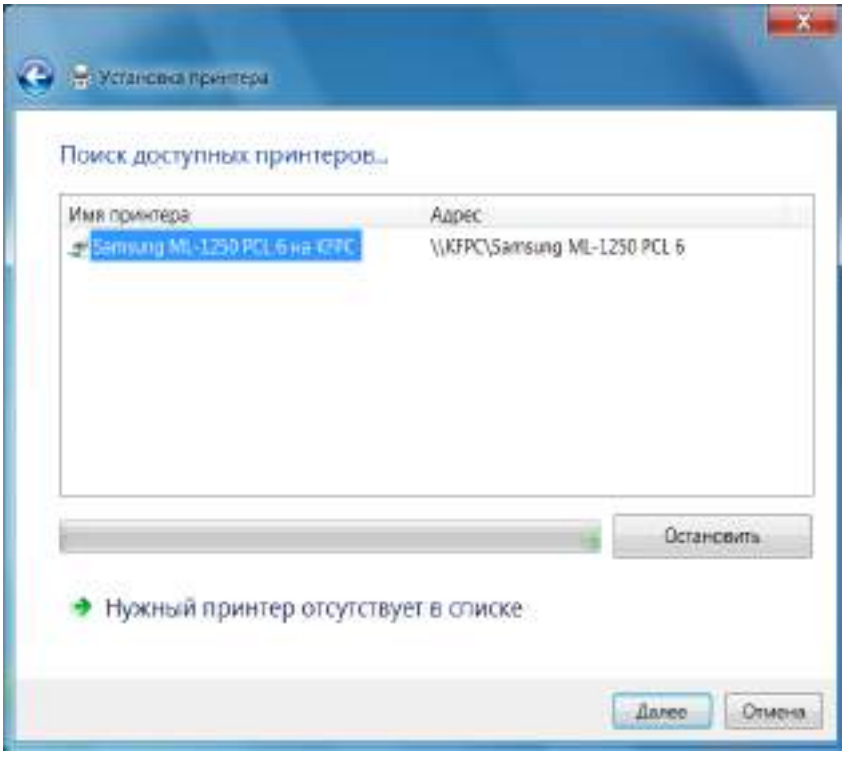



Рис. 51. Окно Мастера установки принтера со списком обнаруженных сетевых принтеров

## 2.4. Использование net-команд Windows

Выделение и использование сетевых ресурсов может быть организовано так называемыми net-командами Windows. Для знакомства с ними запустите окно командной строки (Пуск – Выполнить cmd). Для просмотра поддерживаемых сетевых команд в окне командной строки необходимо набрать `net help` (рис. 52).

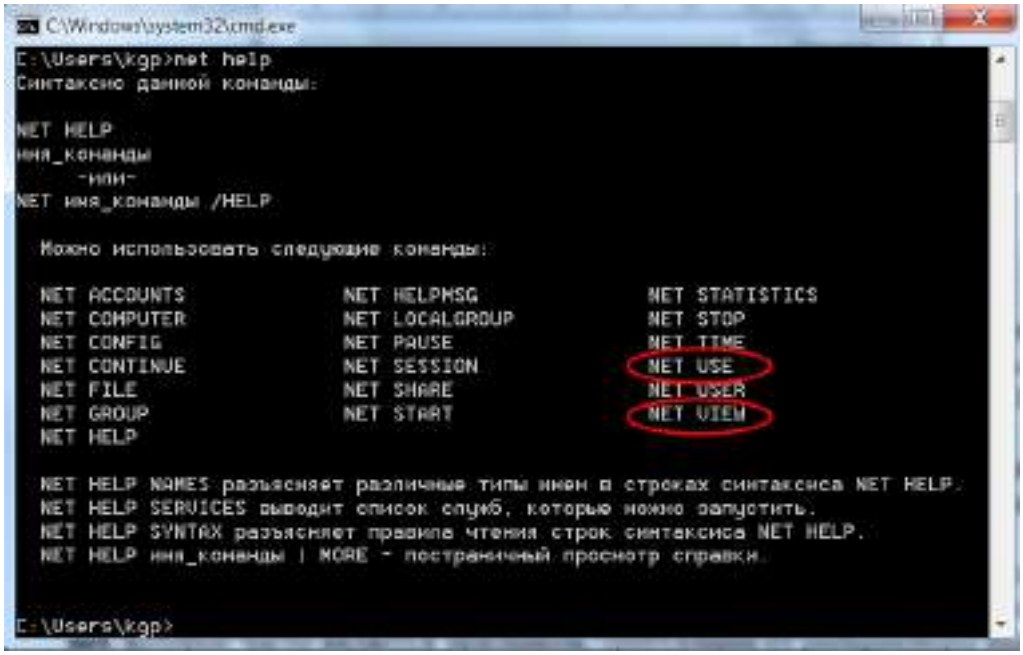



Рис. 52. Список сетевых команд Windows и правила просмотра их синтаксиса и параметров

Команда `net view` выводит список компьютеров сети или сетевых ресурсов на указанном в качестве параметра компьютере (рис. 53).

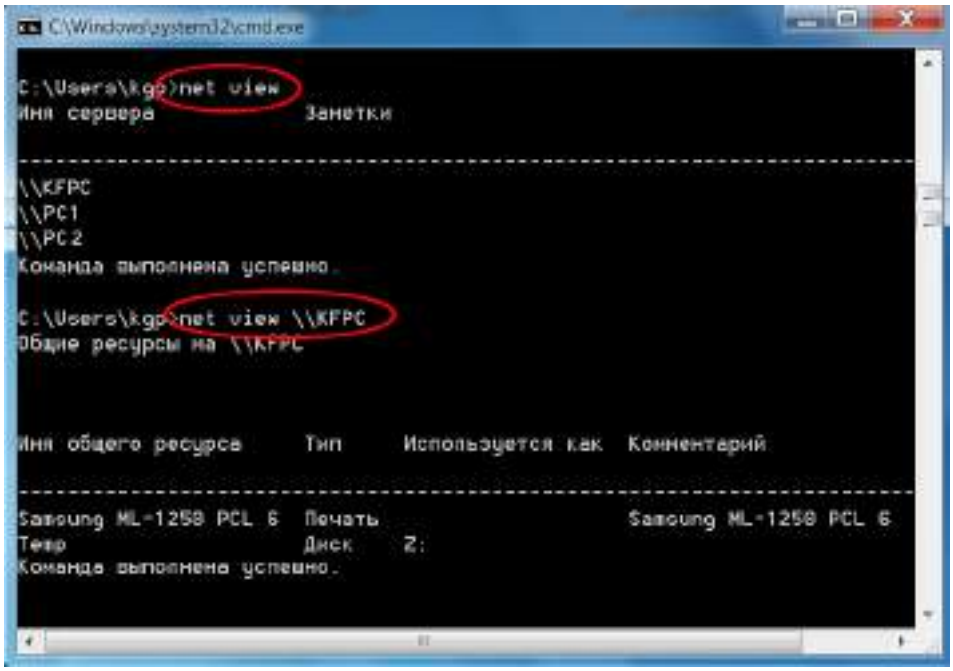



Рис. 53. Просмотр компьютеров сети и сетевых ресурсов командой net vew

Вызванная без параметров команда net view выводит список компьютеров локальной сети. Список общих ресурсов компьютера может быть получен с помощью команды net view \\Имя_компьютера.

Команда net share обеспечивает управление общими ресурсами. При вызове команды net share без параметров выводятся сведения обо всех общих ресурсах локального компьютера. Для выделения пользователю папки в совместное использование по сети следует задать команду net share [Сетевое_имя=] диск: путь_к_папке [/GRANT: имя_пользователя, [READ | CHANGE | FULL]]. Для отмены общего доступа к папке используется команда net share сетевое_имя|диск: путь_к_папке /delete. В квадратных скобках указаны необязательные параметры, а вертикальная черта обозначает задание или параметра перед ней, или параметра после неё. Если не указывать сетевое имя папки, то оно будет совпадать с именем папки на локальном диске, если не задавать разрешения конкретным пользователям опцией /GRANT, будет выдано разрешение Чтение для группы Все данного компьютера или домена. В качестве примера на рис. 54 показано выделение папки D:\News в совместное использование по сети с сетевым именем Новости для пользователя Гость с разрешением Чтение. Обратите внимание, командой net share на экран выводятся и системные ресурсы с сетевыми именами, заканчивающимися символом $ (они доступны пользователям с правами Администратора).

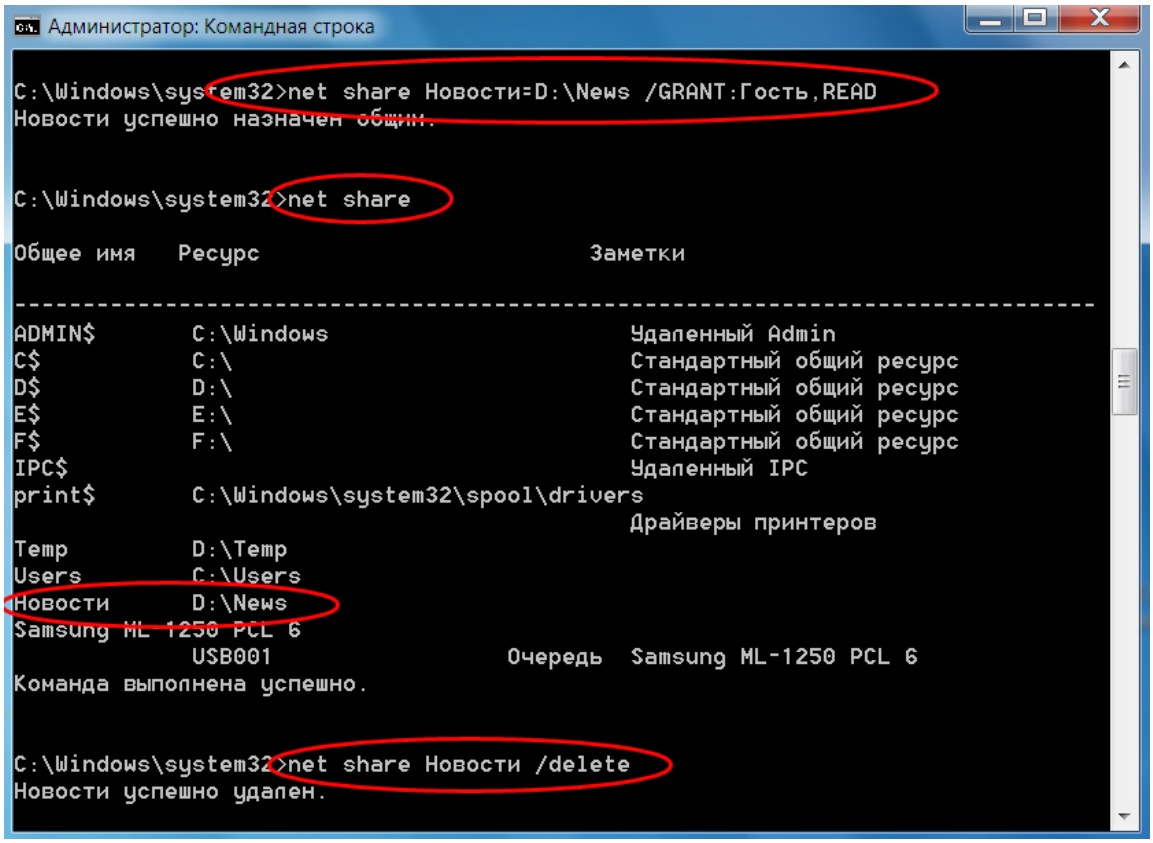



Рис. 54. Организация сетевой папки командой net share

Команда `net use` обеспечивает подключение к общим сетевым ресурсам на удалённом компьютере или вывод информации о сетевых подключениях текущего компьютера. Вызванная без параметров команда `net use` извлекает список сетевых подключений данного компьютера (рис. 55). Для подключения выделенной для совместного использования по сети папки на компьютере-сервере необходимо задать команду `net use [буква_диска:] \\имя_компьютера\имя_сетевой_ папки`. Если не указывать букву диска, папка будет подключена, но доступ к ней будет возможен только по ссылке в виде `\\имя_компьютера\имя_сетевой_папки`. Естественно, Вы должны обладать полномочиями, разрешающими Вам использовать указанную сетевую папку. Для отключения сетевой папки на удалённом компьютере необходимо задать команду `net use буква_диска: | \\имя_компьютера\имя_сетевой_папки /delete.` Вертикальная черта обозначает задание или буквы диска, или имени удалённого компьютера-сервера и сетевой папки.

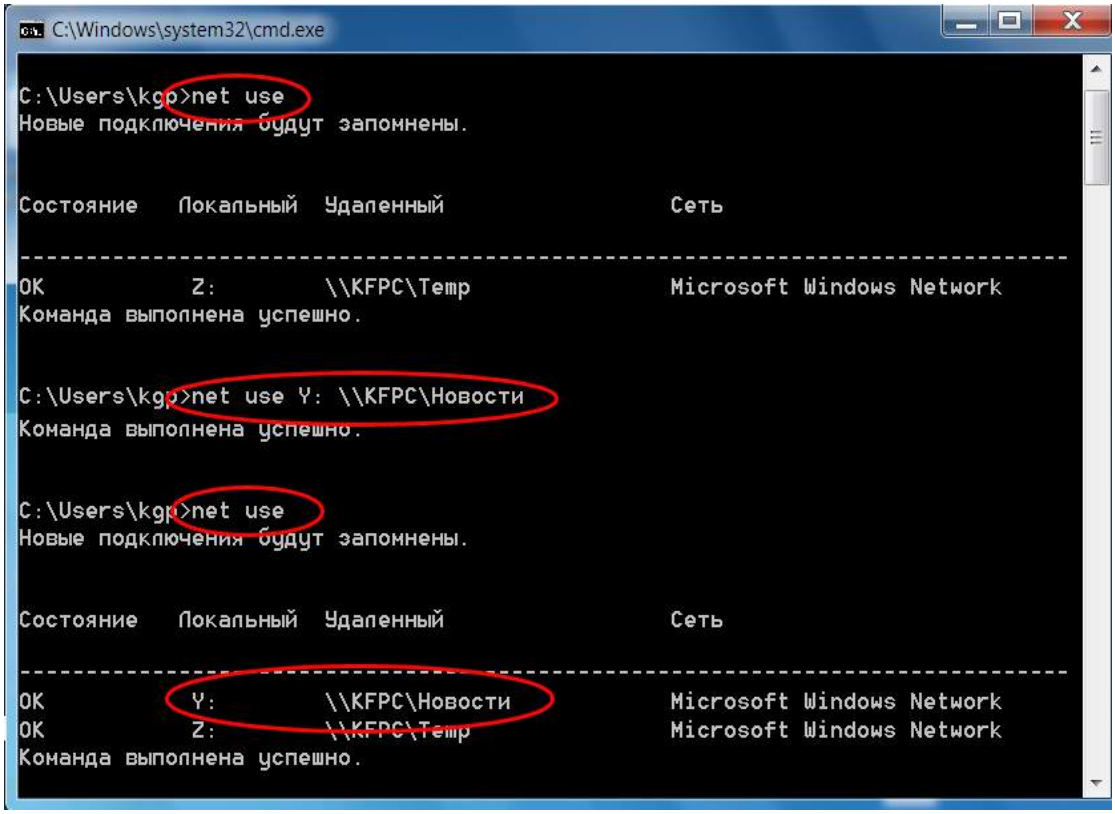



Рис. 55. Подключение сетевой папки командой net use

Следует отметить, что если `имя_компьютера` или `имя_сетевой_папки` содержат пробелы, их следует заключать в кавычки.

Рассмотренные сетевые команды могут быть полезными при составлении конфигурационных (командных) файлов, загружаемых, например, при старте системы и подключающих большое число сетевых ресурсов для многих пользователей.

- Выполните с помощью `net`-команды просмотр ресурсов файлового сервера Вашей сети (например, `\\FS_STUD`).

- Выполните с помощью net-команды подключение сетевой папки на сервере (например, `\\FS_STUD\User\tmp`) как диска с буквой `M:`.
- Просмотрите с помощью `net`-команды подключённые сетевые ресурсы на Вашем компьютере. Убедитесь, что они также отображаются в окне Компьютер.
- Отключите подключённый сетевой ресурс с помощью `net`-команды.

## 2.5. Организация сетевого доступа к каталогам (папкам) в Linux

В операционных системах Linux/Unix организация доступа к сетевым ресурсам может быть выполнена несколькими способами, в том числе и с использованием прикладного протокола *общей файловой системы Интернета/блоков сообщения сервера (Common Internet File System/Server Message Blocks – CIFS/SMB)*, который использует операционная система Windows при выполнении вышеописанных операций. Реализация этого протокола в Linux/Unix обычно выполняется программным обеспечением *Samba*, часто встраиваемым в дистрибутивы операционных систем.

Организация совместного доступа к файловому ресурсу данного компьютера по сети выполняется в окне Настройка сервера Samba, которое в ASPLinux можно открыть командой Система-Администрирование-Samba (для этого придётся ввести пароль пользователя с административными правами root) (рис. 56). При нажатии кнопки Добавить ресурс на панели инструментов откроется окно, в котором на вкладке Основной можно указать путь к каталогу (папке), к которой организуется доступ, опциональные имя сетевого ресурса и его описание, а также право на запись в этом ресурсе (поддерживаются только права Только чтение и Запись) и опцию, определяющую будет ли виден ресурс в окне Обозревателя файлов. Перейдя на вкладку Доступ, появится возможность выбрать пользователей, для которых организуется данный ресурс.

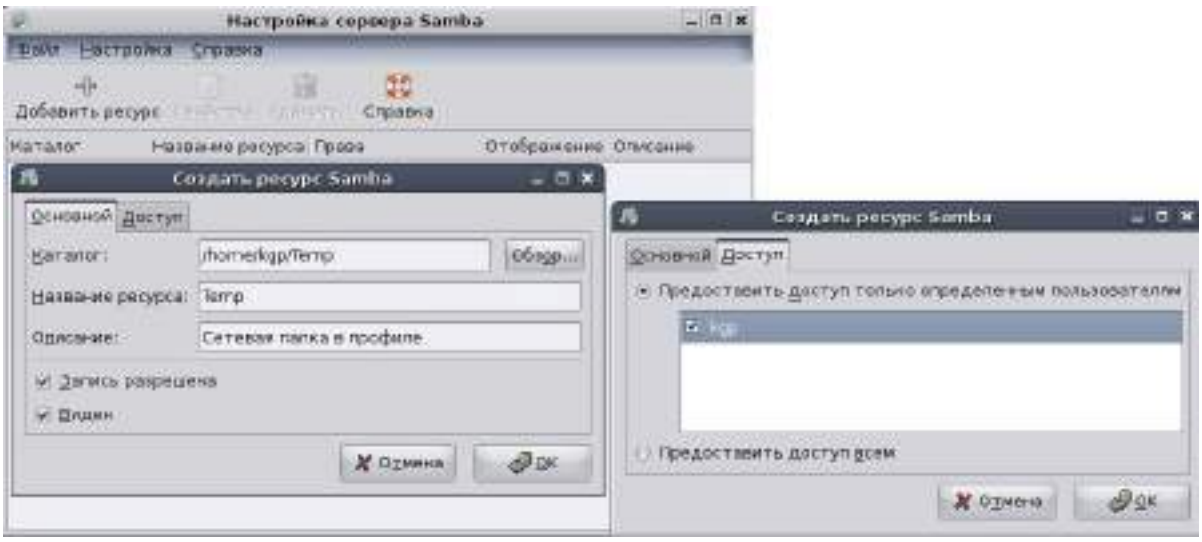



Рис. 56. Добавление ресурса Samba в ASPLinux

Следует отметить, что серверу Samba необходимо указать его пользователей, это можно сделать в окне добавления пользователя Samba, которое открывается командой Настройка-Пользователи Samba. Пользователи выбираются из зарегистрированных пользователей операционной системы (рис. 57).

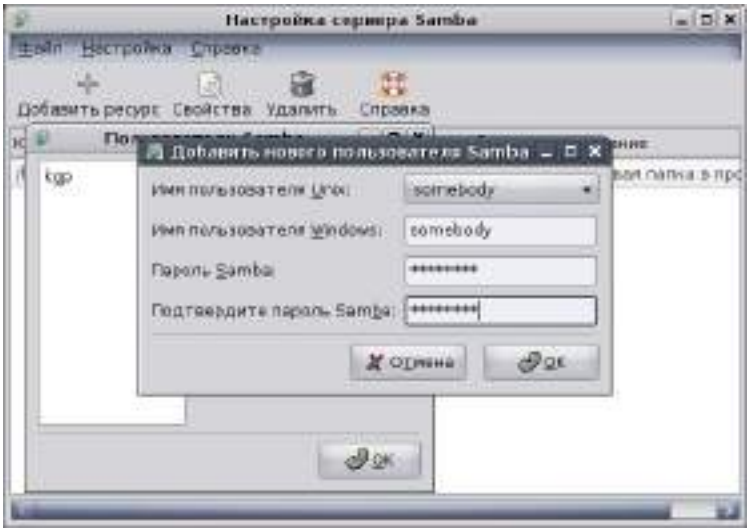



Рис. 57. Добавление пользователя сервера Samba в ASPLinux

На рис. 58 приведен пример настройки того же ресурса с правом Только чтение для добавленного на рис. 57 пользователя.

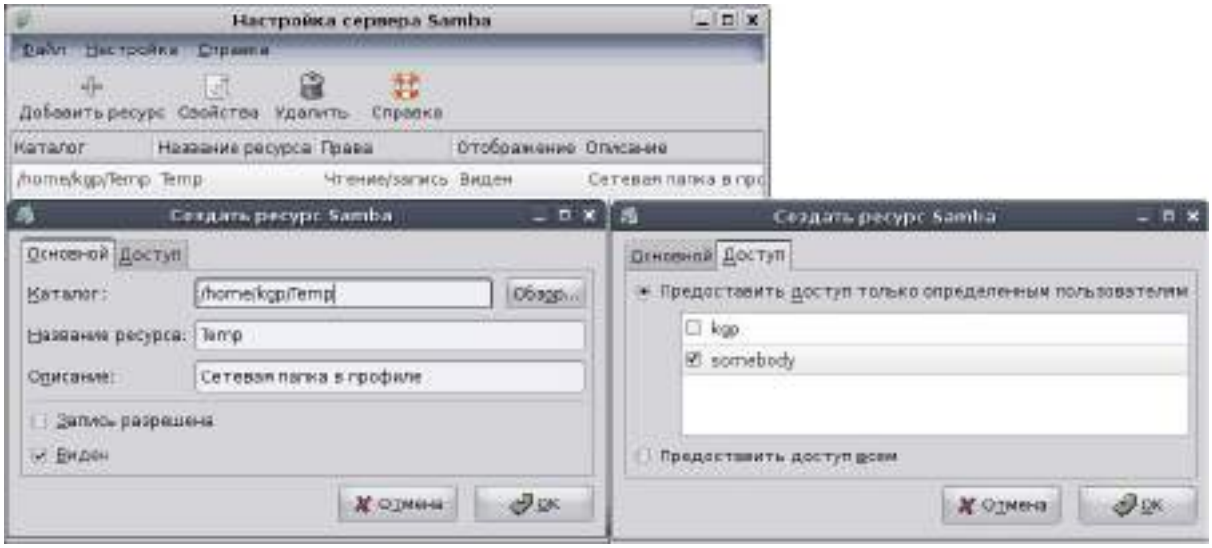



Рис. 58. Добавление ресурса Samba для другого пользователя

Подключение к сетевому ресурсу может быть осуществлено через Обозреватель файлов путём выполнения команды Переход-Сеть. После её подачи в открывшемся окне Сеть можно увидеть значки компьютеров сети, открыв которые можно увидеть сетевой ресурс (рис. 59). Поскольку в Windows для организации доступа к файловым сетевым также ресурсам используется протокол CIFS/SMB, сетевую папку на компьютере с операционной системой Linux можно использовать с компьютера, работающего под Windows и наоборот (рис. 60). Напомним, что для успешного доступа

в обеих системах нужно зарегистрировать пользователя с одинаковыми именем и паролем.

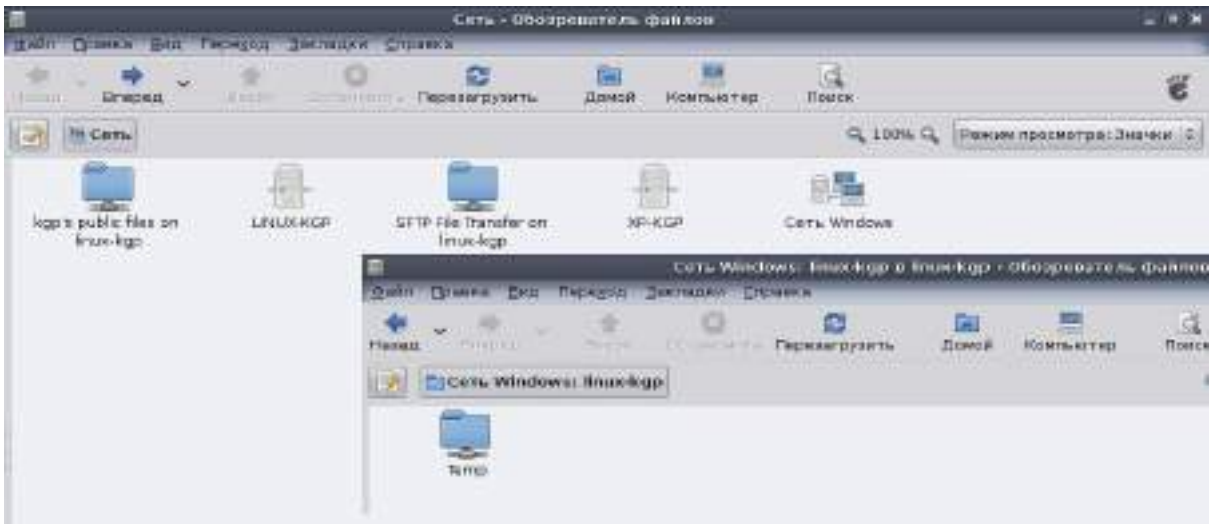



Рис. 59. Доступ к сетевому ресурсу через Обозреватель файлов


Рис. 60. Доступ к сетевому ресурсу Linux из Windows

## 2.6. Организация совместного использования по сети принтера в Linux

Для выделения принтера подключённого к компьютеру, работающему под управлением операционной системы Linux (ASPLinux в данном примере), необходимо выполнить команду Система-Администрирование-Печать. После ввода в диалоговое окно пароля пользователя с административными правами `root` появится окно Настройка принтера (рис. 61), в левой части которого перечисленные подключённые к компьютеру принтеры, а также имеется опция (включена на рис. 61) Общий доступ, разрешающая использовать принтер по сети.

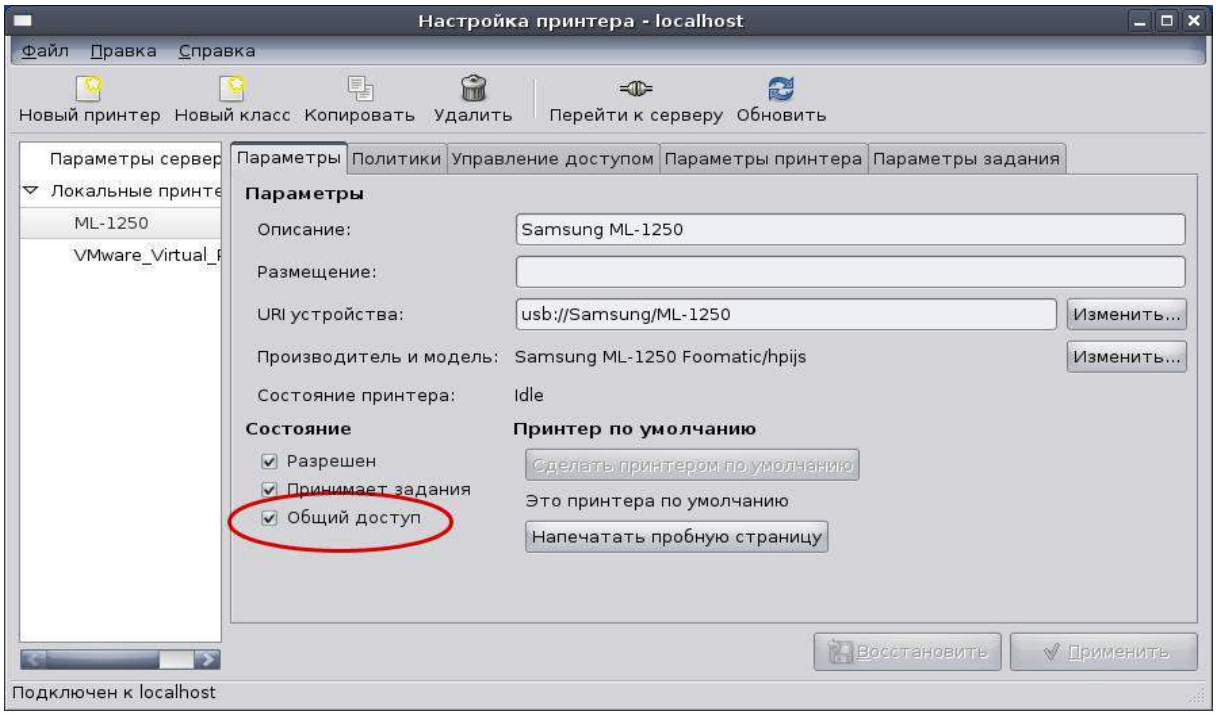



Рис. 61. Окно Настройка принтера ASPLinux с включённым общим доступом по сети

Открыв вкладку Управление доступом этого окна можно указать пользователей, которым разрешено (или запрещено) использование принтера по сети (рис. 62).

Подключение к сетевому принтеру другого компьютера можно осуществить также в окне Настройка принтера (рис. 61). Для этого необходимо выполнить щелчок по кнопке Новый принтер на панели инструментов и в открывшемся окне в списке слева выбрать опцию Windows Printer via SAMBA (принтер Windows через SAMBA)(рис. 63). После чего в дереве ресурсов этого окна необходимо выбрать последовательно группу, имя компьютера и сетевое имя принтера этого компьютера.

В верхней части окна автоматически отобразится универсальный указатель ресурса (*Uniform Resource Identifier – URI*) для данного принтера, а в нижней необходимо ввести имя и пароль пользователя, которому разрешено использование принтера.

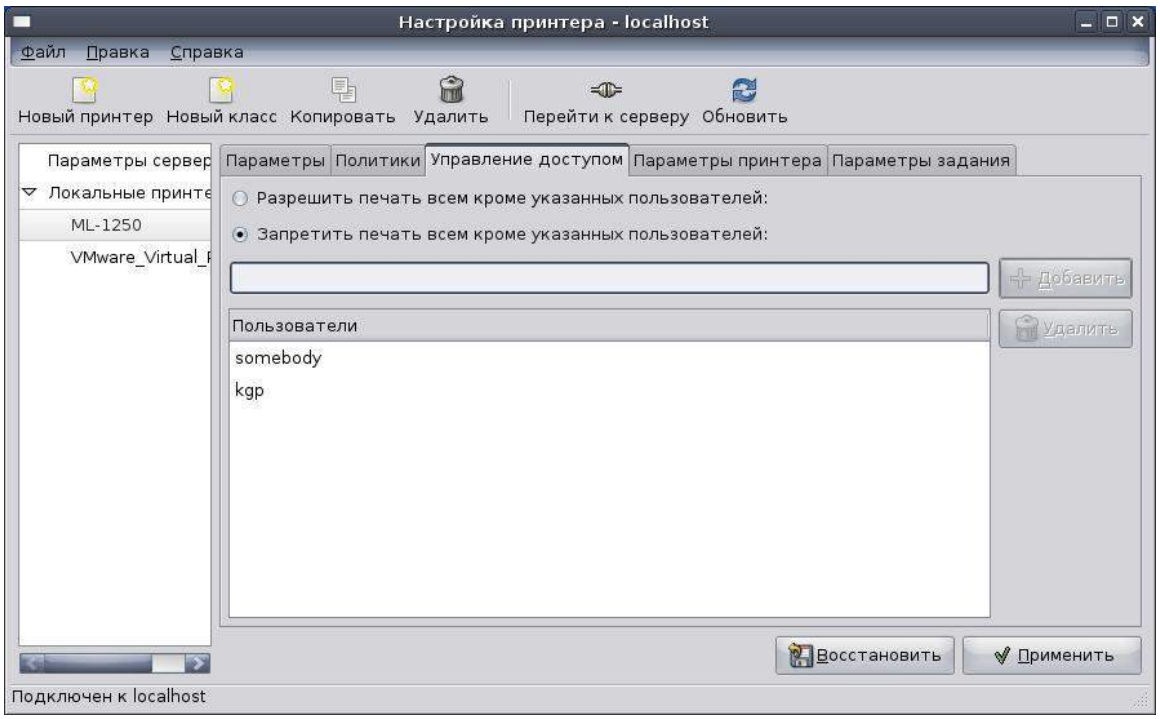



Рис. 62. Окно Настройка принтера ASPLinux с добавленными пользователями

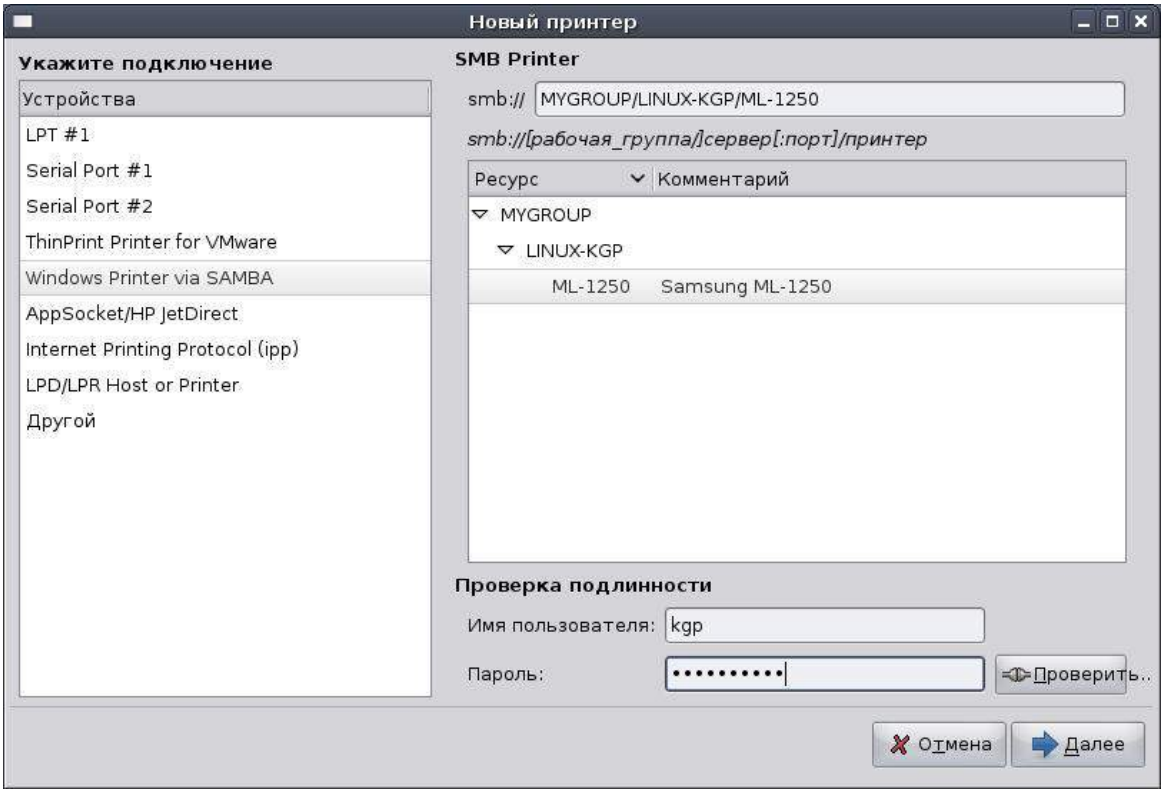



Рис. 63. Окно Добавления принтера ASPLinux

На следующих шагах Мастера добавления принтера необходимо выбрать производителя и модель принтера (для установки соответствующих драйверов), а также ввести опциональные описание принтера и его размещение. После установки сетевого принтера, он добавляется в список уста-

новленных на компьютере принтеров (рис. 64) и может быть использован из приложений.

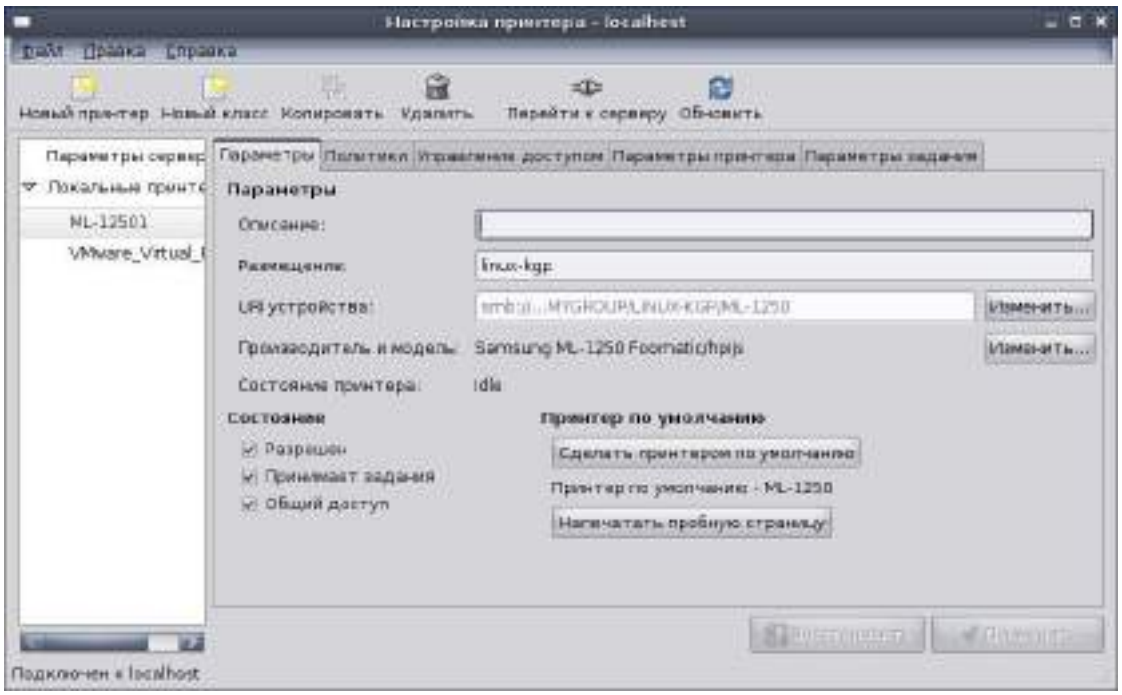



Рис. 64. Окно Настройка принтера ASPLinux с добавленным сетевым принтером

Сетевой принтер, подключённый к компьютеру с операционной системой Linux, может быть использован и Windows-клиентами, для этого необходимо на клиентах выполнить установку принтера так же, как было описано в разделе 2.3.

## Вопросы для самоподготовки

1. Назовите основные сетевые компоненты, обеспечивающие работу сетевого подключения в операционных системах семейства Windows.
2. Что называют драйвером устройства, каковы его основные функции?
3. Что называют сетевым протоколом и стеком сетевых протоколов? Назовите основные задачи протокола сетевого уровня.
4. Назовите задачи клиентского и серверного компонентов сетевого подключения. Поясните, что собой представляет одноранговая сеть.
5. Опишите способ организации общего доступа компьютеров локальной сети к Интернет, доступный в современных версиях Windows.
6. Объясните, для чего пользователи операционной системы объединяются в группы. Как в операционной системе Windows добавить пользователя в ту или иную группу?
7. Какие типы ресурсов могут быть выделены в совместное использование по сети?
8. Охарактеризуйте типы разрешений сетевого доступа к файловым ресурсам. Чем разрешение Полный доступ отличается от разрешения Изменение?

9. Назовите известные Вам имена пользователей и групп, зарегистрированные в Windows по умолчанию. Для чего существует учётная запись Гость? Какие пользователи входят в группу Все?
10. Сможет ли пользователь с правами Администратора на удалённом компьютере подключиться к папке, специально не выделенной в совместное использование по сети? Если сможет, то как?
11. Что собой представляет технология доменов фирмы Microsoft, какова роль контроллера домена? Можно ли для определённого перечня пользователей выделить сетевые ресурсы на разных компьютерах сети с возможностью использования этих ресурсов этими пользователями, зарегистрировавшимися на любом из компьютеров?
12. В чем различие назначения разрешений на вкладках Доступ и Безопасность окна Свойства папки/диска?
13. В чем состоит опасность постоянной работы с учётной записью с правами Администратора?
14. Назовите последовательность действий при выделении в общее пользование по сети папки в операционной системе Windows.
15. Назовите последовательность действий, выполняемых при подключении к сетевой папке на удалённом компьютере.
16. Охарактеризуйте разрешения, выбираемые при выделении принтера в совместное использование по сети.
17. Назовите последовательность действий при выделении в общее пользование по сети принтера в операционной системе Windows.
18. Назовите последовательность действий, выполняемых при подключении на своём компьютере сетевого принтера.
19. Приведите `net`-команду, позволяющую просмотреть перечень имён компьютеров Вашей локальной сети.
20. Приведите `net`-команду, позволяющую просмотреть перечень сетевых ресурсов на конкретном удалённом компьютере.
21. Приведите `net`-команду, позволяющую подключить на своём компьютере удалённый файловый ресурс как локальный диск.
22. Приведите `net`-команду, позволяющую просмотреть сконфигурированные сетевые ресурсы на Вашем компьютере, и команду, позволяющую отключить указанный сетевой файловый ресурс?
23. Назовите протокол прикладного уровня, используемый в операционных системах Windows и Linux/Unix для организации сетевого доступа к файловым ресурсам и принтерам и программное обеспечение, обычно реализующее его в Linux/Unix.
24. Выделите каталог (папку) в качестве сетевого ресурса на компьютере, работающем под управлением Linux, и подключитесь к нему с компьютера, работающего под управлением Windows.
25. Настройте сетевой принтер на компьютере, работающем под управлением Linux, и подключитесь к нему с компьютера, работающего под управлением Windows.

26. Повторите задания предыдущих двух пунктов, выбрав в качестве сервера компьютер, работающий под управлением Windows.

## Тесты для контроля усвоения знаний

1. Выберите соответствие названий и определений сетевых компонентов Windows, приведенных в списке:
   а) клиент;
   б) протокол;
   в) служба;
   г) адаптер.

   Драйвер сетевой платы, непосредственно взаимодействующий с сетевой платой, установленной в компьютере, – это…

   Компонент, регламентирующий правила разбиения потока информации на пакеты и правила адресации компьютеров-участников сети, – это…

   Компонент, позволяющий подключаться к серверам сети, – это…

   Компонент, позволяющий выделять сетевые ресурсы на компьютере, на котором он установлен, – это…
2. Выберите типы доступа для сетевых дисков и папок, определяемых в операционной системе Windows:
   а) чтение;
   б) чтение и выполнение;
   в) изменение;
   г) запись;
   д) полный доступ;
   е) просмотр;
   ж) список содержимого папки.
3. Какой из сетевых компонентов Windows обеспечивает возможность предоставления ним сетевых ресурсов?
   а) адаптер;
   б) сетевой протокол;
   в) клиент;
   г) служба.
4. Какой из сетевых компонентов Windows отвечает за адресацию узлов сети на сетевом уровне?
   а) адаптер;
   б) сетевой протокол;
   в) клиент;
   г) служба.
5. Выберите правильную команду выделения на Вашем компьютере папки `C:\Data` в общее пользование по сети с сетевым именем `AllData`:
   а) `net share AllData =c:\data;`
   б) `net share c:\data AllData;`
   в) `net use AllData = c:\data;`
   г) `net use c:\data AllData;`

д) `net view AllData =c:\data;`
е) `net view c:\data AllData.`

6. Выберите команду подключения сетевого ресурса `\\FS_stud\user` и отображения его как сетевого диска `Z`:
   а) `net share Z: \\Fs_stud\user;`
   б) `net share \\Fs_stud\user Z: ;`
   в) `net use Z: \\Fs_stud\user;`
   г) `net use \\Fs_stud\user Z:`
   д) `net view Z: \\Fs_stud\user`
   е) `net view \\Fs_stud\user Z:`
7. Выберите команду, позволяющую вывести список сетевых имен работающих в данный момент компьютеров Вашей сети:
   а) `net computer`
   б) `net view`
   в) `net config`
   г) `net name`
   д) `net group`
8. Определите, правильно ли следующее утверждение: в одноранговой сети под управлением Windows на каждом компьютере сети установлены и клиент для сетей Microsoft, и служба доступа к файлам и принтерам.
9. Укажите, кто входит в группу пользователей Все в операционной системе Windows:
   а) все пользователи локальной сети;
   б) все пользователи сети предприятия;
   в) все зарегистрированные в операционной системе пользователи.
10. Выберите права, которые отличают разрешение Изменение от разрешения Полный доступ:
    а) добавлять файлы и подпапки;
    б) изменять владельца сетевого ресурса;
    в) изменять данные в файлах;
    г) изменять разрешения безопасности;
    д) удалять подпапки и файлы.
11. Выберите название протокола прикладного уровня, позволяющего одновременно организовывать сетевой доступ к файловым ресурсам и принтерам в Windows и Linux:
    а) HTTP
    б) FTP
    в) CIFS/SMB.

## Литература

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с.: ил.

2. Мак-Федрис П. Microsoft Windows 7. Полное руководство / П.Мак-Федрис. – М. : Вильямс, 2010. – 800 с.

3. Официальный сайт Windows 7. Раздел Помощь - Интернет, электронная почта и локальная сеть [электронный ресурс]. – режим доступа: http://windows.microsoft.com/ru-RU/windows7/help/ networking-e-mail-getting-online.

4. Официальный сайт ASPLinux [электронный ресурс]. – режим доступа: http://www.asplinux.ru/.

# РАЗДЕЛ 3
# АНАЛИЗ КАДРОВ ETHERNET С ПОМОЩЬЮ АНАЛИЗАТОРА СЕТЕВЫХ ПРОТОКОЛОВ

## 3.1. Сетевая технология Ethernet и форматы кадров данных

*Ethernet* представляет собой пакетную технологию передачи данных, работающую на физическом и канальном уровнях модели OSI (ПРИЛОЖЕНИЕ А) в основном в локальных компьютерных сетях. Стандарты Ethernet разрабатываются комитетом 802.3 Международного профессионального сообщества – *Институтом инженеров электротехники и электроники* (*Institute of Electrical and Electronics Engineers – IEEE*). В настоящее время наиболее распространёнными версиями технологии являются *Fast Ethernet* со скоростью передачи данных 100 Мбит/с (стандарт IEEE 802.3u (оптика/витая пара) и *Gigabit Ethernet* со скоростью передачи данных 1 Гбит/с (стандарт IEEE 802.3z – по оптике/802.3ab – по витой паре). В то же время все большая часть сетевых устройств и серверов уже выпускается с поддержкой технологии *10Gigabit Ethernet* (или *10GbE*) со скоростью передачи данных 10 Гбит/с (стандарты 802.3ae – по оптике/802.3an – по витой паре). В июне 2010 г. окончательно утверждён стандарт 802.3ba (только оптика) для следующих поколений Ethernet – *40 Gigabit Ethernet* (или *40 GbE*) и *100 Gigabit Ethernet* (или *100 GbE*) со скоростью передачи данных 40 и 100 Гбит/с, соответственно. Следующим рубежом Ethernet должна стать разработка технологии *Terabit Ethernet*, позволяющей передавать данные со скоростью 1Тбит/с. Наиболее распространёнными средами передачи технологии Ethernet являются витая пара (рис. 8) и оптоволоконный кабель. Учитывая гораздо большую полосу пропускания оптоволокна, чем медной витой пары, реализация версий технологий Ethernet для оптики является более простой. В настоящее время оптоволоконные каналы Ethernet в основном применяются в магистралях сетей и при подключении серверов, а более дешёвые каналы на медной витой паре, а также каналы беспроводной связи, построенные с использованием протоколов, разработанных комитетом IEEE 802.11, известными также как протоколы технологии *Wi-Fi*.

Информация, передаваемая технологией Ethernet, размещается в структурах данных, называемых *кадрами* (*frame*) Ethernet. Эти структуры имеют *заголовок* (*Header*) со служебной информацией, поле данных (*Data*) и концевик с *контрольной суммой* (*Frame Check Sequence – FCS*) (рис. 65). Размер кадров может варьироваться в пределах 64–1518 байт, не считая синхронизирующей преамбулы (8 байт) и не учитывая опциональную возможность увеличения минимального размера кадра до 512 байт в полудуплексном режиме работы технологии Gigabit Ethernet и возможность передачи гигантских кадров (Jambo Frame) технологией Gigabit Ethernet и более поздними.

Первыми двумя полями заголовка кадра являются 6-байтовые поля *Адрес получателя* (*Destination Address – DA*) и *Адрес отправителя* (*Source Address – SA*). Остальные поля могут варьироваться в разных типах кадров и будут рассмотрены далее. Концевик кадра содержит четырёхбайтовое значение *контрольной суммы* (*Frame Check Sequence – FCS*), вычисленной с использованием алгоритма CRC-32 (*Cyclic Redundancy Code – циклический избыточный код*).

| 14-22 байт | 46-1500 байт | 4 байта |
|---|---|---|
| **Заголовок** | **Поле данных** | **FCS** |

Рис. 65. Обобщённый формат кадра Ethernet

*Контрольная сумма* представляет собой некоторое значение, рассчитанное по определённому алгоритму из последовательности передаваемых данных отправителем и помещённое в поле кадра. Это значение используется получателем для проверки правильности передачи данных путём расчёта из последовательности полученных данных по тому же алгоритму и последующему сравнению результата расчёта со значением контрольной суммы, переданной в кадре. Алгоритм CRC-32 характеризуется очень высокой вероятностью изменения значения контрольной суммы при изменении значения хотя бы одного бита в поле данных кадра Ethernet. Следует отметить, что технология Ethernet в общем случае не выполняет запрос на повторную передачу кадра при несовпадении значений контрольной суммы, а просто отбрасывает кадр. Повторная передача кадра организуется протоколами более высоких уровней модели OSI (ПРИЛОЖЕНИЕ А).

В качестве адресов технология Ethernet использует 6-байтовые MAC-адреса, определяемые для подуровня *доступа к среде передаче* (*Media Access Control – MAC*) канального уровня производителями сетевых интерфейсов. Эти адреса считаются жёстко привязанными к конкретному интерфейсу, хотя и существует возможность их переопределить в дополнительных настройках драйвера сетевого адаптера (рис. 3). Напомним, что MAC-адрес сетевого адаптера Вашего компьютера можно увидеть командой `ipconfig /all` (рис. 15) для Windows или `ifconfig` для Linux/Unix (рис. 17). На рис. 66 приведен формат 48-битового MAC-адреса.

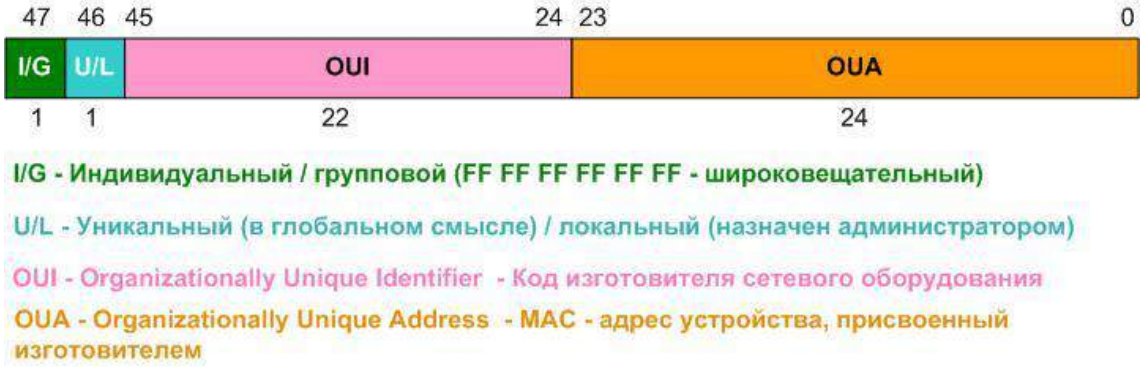



Рис. 66. Формат MAC-адреса

Старшие 3 байта MAC-адреса представляют собой так называемый *организационно уникальный идентификатор* (*Organizationally Unique Identifier – OUI*) – IEEE выделяет такие уникальные идентификаторы для производителей сетевого оборудования. На сайте IEEE по адресу http://standards.ieee.org/regauth/oui/index.shtml организована возможность поиска информации о производителе по значению OUI (рис. 67). Младшие 3 байта представляют собой *организационно уникальный адрес* (*Organizationally Unique Address – OUA*), который назначается производителем каждому выпущенному ним контроллеру сетевого интерфейса. Таким образом, уникальность MAC-адреса обеспечивается, с одной стороны, IEEE – не существует двух одинаковых значений OUI, выделенных разным производителям. С другой стороны производитель задаёт уникальные значения OUA производимым ним контроллерам сетевых интерфейсов. В результате можно гарантировать уникальность значения любого MAC-адреса, записанного в конфигурационную информацию контроллера сетевого интерфейса.

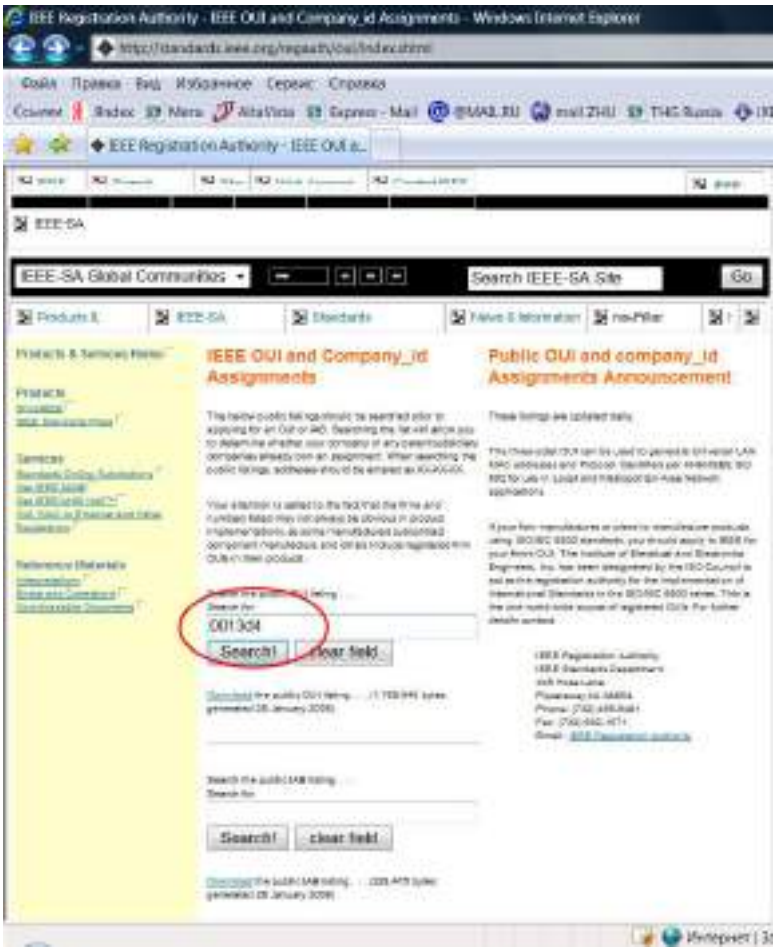



Рис. 67. Форма поиска производителя сетевого интерфейса
по значению OUI на сайте IEEE

Существуют три типа MAC-адресов: *индивидуальные* или *однопунктовые* (*Unicast*), *групповые* (*Multicast*) и *широковещательные* (*Broadcast*). *Индивидуальный (однопунктовый)* адрес определяет одну конкретную ра-

бочую станцию сети, это наиболее часто встречаемый адрес в кадрах Ethernet. Иногда необходимо разослать информацию всем компьютерам локальной сети. Например, при включении рабочей станции она высылает всем участниками сети своё сетевое имя и адресную информацию (после чего её имя отображается, например, в окне Сеть). MAC-адрес, указывающийся в этом случае в поле адреса получателя, является *широковещательным*. Широковещательный адрес представляет собой 48 единичных битов, которые в шестнадцатеричной системе выглядят как $FF\text{-}FF\text{-}FF\text{-}FF\text{-}FF\text{-}FF_{H}$. В случае, когда получателей кадра должно быть более одного, но менее, чем все компьютеры локальной сети, используют *групповые* MAC-адреса. Такие адреса используются, например, при потоковой передаче аудио и видео тем компьютерам, пользователи которых подписались на эти передачи. Признаком индивидуального (однопунктового) адреса является установленный в ноль старший бит (47-й) MAC-адреса (I/G). Соответственно, если старший бит установлен в единицу, адрес является групповым (рис. 66). Следует отметить, что адрес отправителя может быть только индивидуальным (однопунктовым). А 46-й бит MAC-адреса (U/L) указывает, является ли этот адрес уникальным в глобальном смысле (бит равен 0) или в пределах локальной сети в случае, если он переопределён администратором (бит равен 1). С учётом характерного для Ethernet порядка передачи битов: первыми передаются младшие биты байта, значения старшего байта группового адреса могут равняться либо $01_{H}$ (для уникального в глобальном смысле адреса), либо $03_{H}$ (для уникального в пределах локальной сети адреса).

В сетях Ethernet на канальном уровне могут использоваться заголовки четырёх типов (рис. 68). Их существование связано с длительной (по меркам информационных технологий) историей развития технологии Ethernet. Практически всё сетевое оборудование умеет работать со всеми форматами кадров технологии Ethernet.

Исторически первым типом кадра является так называемый кадр *Ethernet II или Ethernet DIX* (где DIX – первые буквы названий фирм DEC, Intel и Xerox, разработавших этот формат). Формат этого кадра определяет следующие поля:

- *Адрес получателя* (*DA*) – шестибайтовый MAC-адрес получателя.
- *Адрес отправителя* (*SA*) – шестибайтовый MAC-адрес отправителя.
- *Тип протокола* (*Type -T*) – двухбайтовое поле предназначено для указания идентификатора протокола, вложившего свой пакет в поле данных кадра Ethernet. Идентификаторы протоколов, использующих кадры Ethernet в качестве транспорта, определены IEEE, они представляют собой двухбайтовые значения, превышающие значение максимальной длины поля данных кадра, равное 1500 байт ($05DC_{H}$ в шестнадцатеричной системе), например $0800_{H}$ – для протокола IP, $0806_{H}$ – для протокола ARP и т.д.

- *Поле данных* (*Data*) – может содержать от 46 до 1500 байт, если длина поля меньше 46 байт, то используется заполнение нулевыми байтами ($00_H$), чтобы дополнить кадр до минимально допустимой длины.
- *Поле контрольной суммы* (*FCS*) – 4 байта, содержащие значение, которое вычисляется по алгоритму CRC-32.

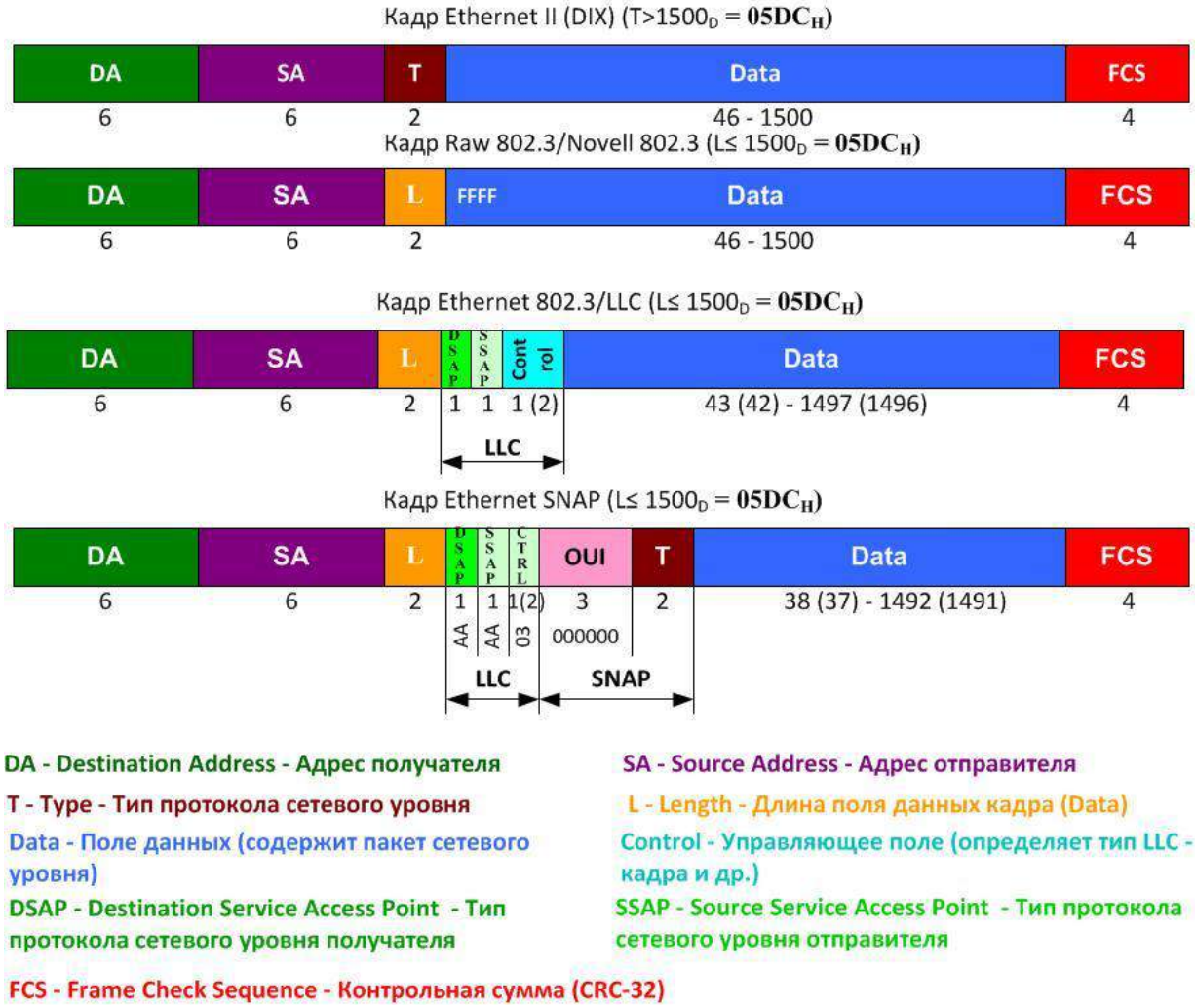



Рис. 68. Форматы кадров Ethernet

Описанный тип кадра появился во время появления и развития Интернет, очевидно, поэтому и в настоящее время он используется для переноса в локальных сетях пакетов протокола IP и других протоколов стека TCP/IP.

Формат Ethernet II (DIX) имеет один недостаток: если передача кадра внезапно прервалась, то получатель такого незавершённого кадра будет принимать его как целый и обнаружит ошибку только после полного его приёма и расчёта контрольной суммы. Очевидно, что в этом случае достаточно много компьютерного времени будет потрачено впустую. Инженеры фирмы Novell, являющейся первой фирмой, разработавшей системное программное обеспечение для работы в локальных компьютерных сетях Netware, предложили формат кадра, называемый *Novell 802.3* или *Raw*

*802.3* (англ. – сырой, необработанный), в котором вместо типа протокола отправителем помещалась *длина поля данных* (*Length – L*). Получатель устанавливал счётчик байтов в это значение и декрементировал его с получением каждого байта поля данных. Очевидно, что обнуление счётчика свидетельствовало об окончании поля данных. Если данные заканчивались до обнуления счётчика, то данный кадр являлся незавершённым и его можно отбросить без необходимости расчёта контрольной суммы. Мотивацией для замены типа протокола счётчиком длины являлся тот факт, что в начале 1980-х гг. для локальных сетей, где работает технология Ethernet, кроме стека протоколов IPX/SPX операционной системы Novell Netware, альтернатив не было, а значит, отсутствовала необходимость идентификации протоколов, использующих Ethernet.

Естественно, что такая позиция легко подвергается критике, и такое решение не могло быть долговечным. Поэтому IEEE разработал третий формат кадра *Ethernet 802.3/LLC*, в котором добавил так называемый подзаголовок LLC с идентификаторами протоколов вышележащих уровней на стороне получателя и на стороне отправителя. Эти идентификаторы, также определённые IEEE, размещаются в поле *точки доступа к услугам получателя* (*Destination Service Access Point – DSAP*) – и в поле *точки доступа к услугам отправителя* (*Source Service Access Point – SSAP*). Обычно эти поля имеют одинаковые значения, например, для протокола IPX они равны $E0_H$, для протокола NetBIOS – $F0_H$, для протокола STP BPDU – $42_H$. *Поле управления* (*Control*) подзаголовка LLC используется для обозначения типа кадра данных – информационный, управляющий или ненумерованный (обычно в Ethernet используются ненумерованные кадры, в этом случае значение поля равно $03_H$). Так как кадр LLC имеет заголовок длиной 3(4) байта, то максимальный размер поля данных уменьшается до 1497(1496) байт. Кадры данного формата используются в качестве транспорта при установке в операционной системе стеков сетевых протоколов IPX/SPX и NetBIOS.

Появление четвёртого типа кадра *Ethernet SNAP* (*SNAP – SubNetwork Access Protocol – протокол доступа к подсетям*), скорее всего, обязано просчёту разработчиков IEEE, выделивших для идентификации протоколов вышележащих уровней однобайтовые поля DSAP и SSAP, в которые можно записать не более 256 уникальных идентификаторов. Как только количество протоколов стало приближаться к этой цифре, возникла необходимость разработки нового формата кадра. Кадр Ethernet SNAP определён в стандарте 802.2H и представляет собой расширение кадра 802.3/LLC путём введения дополнительного подзаголовка SNAP, в котором размещено поле типа протокола (*Type – T*), имеющее размер два байта. При этом двухбайтовые идентификаторы протоколов совпадают с идентификаторами протоколов для формата Ethernet II (DIX). Кроме типа протокола, в подзаголовке SNAP указывается идентификатор организации (OUI), которая определяет идентификаторы протоколов, указывающиеся в поле типа

протокола. Примерами использующихся в SNAP кодов OUI являются: код IEEE = 00 00 $00_н$, код Cisco Systems = 00 00 $0C_н$. В поля DSAP и SSAP при использовании заголовка SNAP помещаются значения $AA_н$, которые указывают, что в поле данных кадра LLC вложен заголовок SNAP. Поскольку подзаголовок SNAP "забирает" ещё пять байт у поля данных, последнее уменьшается до размеров 38(37) – 1491(1492) байт.

Современное оборудование Ethernet поддерживает все четыре формата кадров. Для распознания формата кадра, полученного получателем, получатель выполняет следующие проверки:

- проверяется двухбайтовое значение в 13 и 14 байтах, если оно превышает 1500 ($05DC_н$), то оно не может быть длиной и данный кадр имеет формат Ethernet II (DIX);
- если значение в 13 и 14 байтах меньше либо равно 1500 ($05DC_н$), то это длина поля данных и проверяется двухбайтовое значение в 15 и 16 байтах;
- если проверяется двухбайтовое значение в 15 и 16 байтах равно $FFFF_н$, то это начало пакета IPX и данный кадр имеет формат Raw/Novell;
- в противном случае проверяется, равно ли двухбайтовое значение в 15 и 16 байтах $AAAA_н$, если да, то это кадр формата Ethernet SNAP;
- в оставшемся случае кадр имеет формат 802.3/LLC.

Алгоритм определения типа кадра приведен на рис. 69.

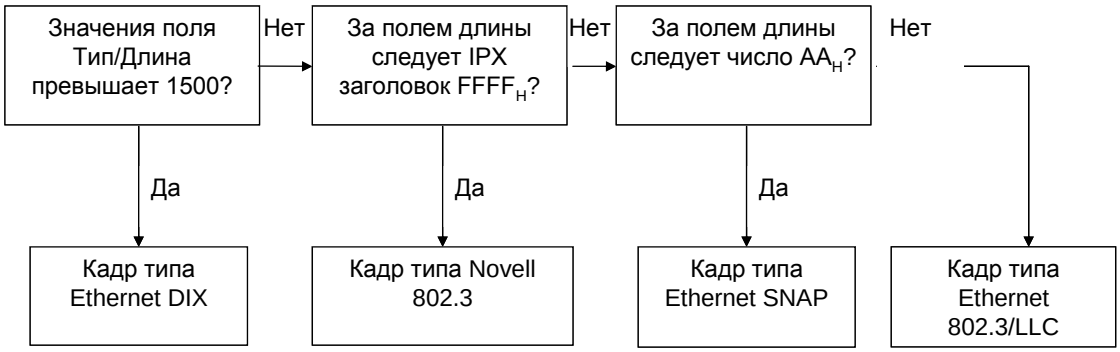



Рис. 69. Алгоритм определения типа кадра Ethernet

## 3.2. Анализаторы сетевых протоколов

Программное обеспечение, способное выполнять анализ проходящих через сетевой интерфейс кадров и переносимых в них пакетов сетевых протоколов, называется *анализаторами сетевых протоколов* и представляет собой один из часто используемых инструментов администратора компьютерной сети. Работа анализаторов основывается на использовании так называемого "*неразборчивого*" (*promiscuous*) режима работы сетевого интерфейсного адаптера, который позволяет захватывать и анализировать сетевые кадры и пакеты, отсылаемые и получаемые не только станцией, на которой работает программа, но и другими станциями сети. Примерами такого рода программ могут быть *tcpdump* фирмы Network Research Group,

*Sniffer Pro* фирмы Network Associated Inc., *Сетевой Монитор* фирмы Microsoft, входящий в состав её серверных операционных систем, и ряд других. Мы рассмотрим работу анализаторов сетевых протоколов на примере бесплатного кроссплатформенного программного обеспечения *Wireshark*, разработанного группой программистов и доступного для загрузки по адресу http://www.wireshark.org.

На рис. 70 приведен интерфейс программы с несколькими захваченными пакетами, высылаемыми утилитой `ping`. В верхней части окна перечислены захваченные пакеты с указанием их основных свойств: порядкового номера в захваченной последовательности, относительного времени захвата, сетевых адресов отправителя и получателя, типа протокола и общей информации о пакете. В средней части отображаются структуры данных сетевых протоколов различных уровней модели OSI (ПРИЛОЖЕНИЕ А), которые переносят свои данные в выделенном в верхнем окне пакете. Развернув уровни, можно увидеть детальное описание полей заголовка сетевого протокола, работающего на этом уровне. В нижней части выводится дамп пакета в виде байтовых значений в шестнадцатеричной системе исчисления и соответствующих этим значениям US-ASCII-кодов в правой части области дампа. Поэтому, если в пакете передаётся пользовательский текст на английском языке, то он будет здесь отображаться, символы второй половины таблиц ASCII (куда входят и русские буквы) отображаются точками.

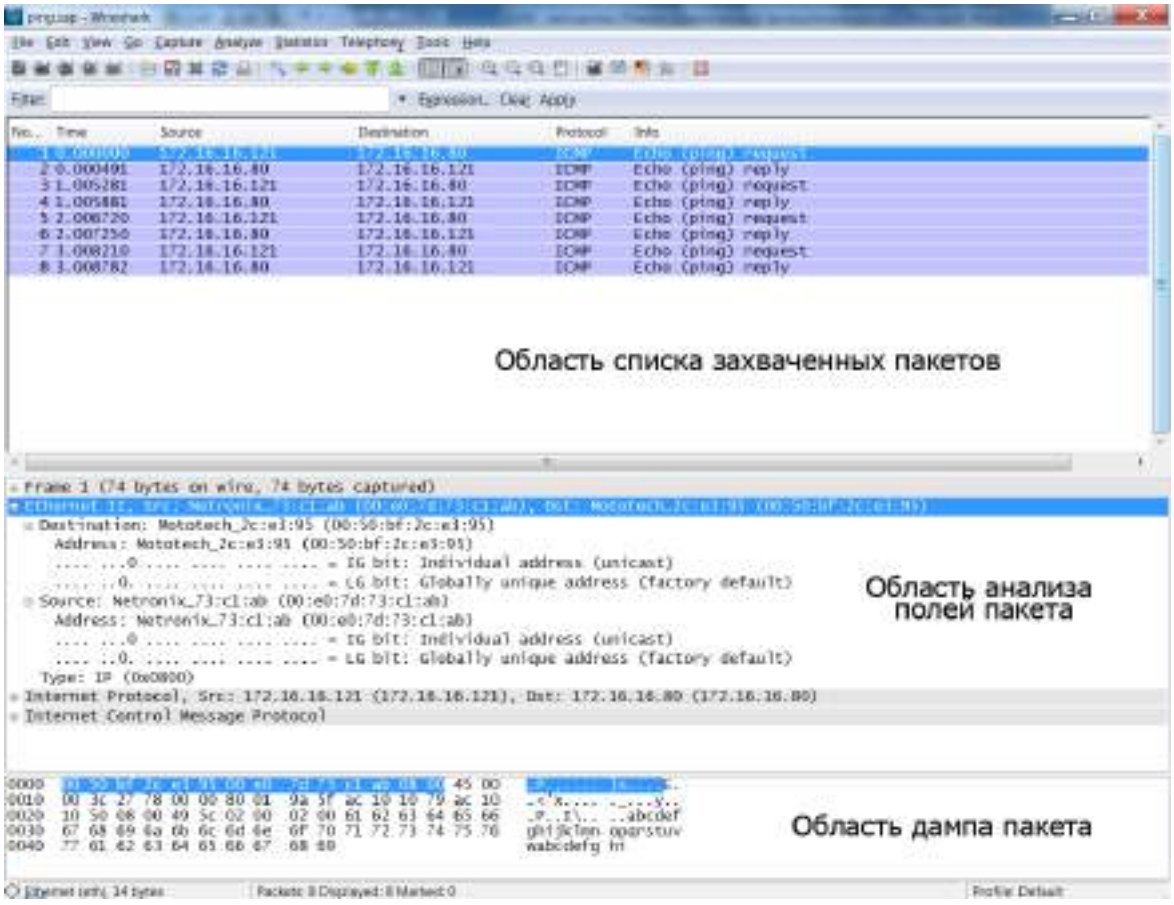



Рис. 70. Интерфейс анализатора сетевых протоколов Wireshark

При выделении в области анализа полей пакета какого-либо заголовка или поля в области дампа выделяются соответствующие ему данные. Так на рис. 70 выделен заголовок кадра канального уровня Ethernet, анализатор распознал формат этого кадра (Ethernet II) и выполнил подробный анализ полей заголовка этого кадра. В области дампа при этом выделены 14 байт, соответствующие структуре заголовка Ethernet II (DIX) (рис. 68). Следует отметить, что первая строка области анализа полей пакета (`Frame 1 (74 bytes on wire, 74 bytes captured)` на рис. 70) не отображает какой-либо уровень стека протоколов, а содержит общую информацию о пакете: длину, время захвата, относительные времена и т.д. Захват кадров осуществляется командой Capture-Start и Capture-Stop (или соответствующими кнопками на Панели инструментов).

## 3.3. Исследование протокола разрешения адреса ARP

Изучение типов MAC-адресов в заголовках кадров Ethernet может быть выполнено путём захвата кадров, переносящих данные *протокола разрешения адреса* (*Address Resolution Protocol – ARP*), выполняющего отображение IP-адреса сетевого интерфейса на его адрес MAC-адрес. Проблема заключается в том, что когда высылается пакет по указанному в качестве параметра IP-адресу получателя (например, командой `ping 192.168.2.1`), отправителю (например, с IP-адресом (SA IP) `192.168.2.2` и MAC-адресом (SA MAC) `00-A0-C9-83-16-16`) необходимо сформировать кадр Ethernet с заполнением адресных полей заголовков канального и сетевого уровней. IP и MAC-адрес отправителя могут быть заполнены, поскольку они известны сетевому интерфейсу отправителя, IP-адрес получателя заполняется значением параметра команды `ping`. А вот MAC-адрес получателя в общем случае для отправителя является неизвестным (рис. 71).

| DA MAC<br>**???** | SA MAC<br>`00-A0-C9-83-16-16` | SA IP<br>`192.168.2.2` | DA IP<br>`192.168.2.1` | Данные пакета |
|---|---|---|---|---|

Рис. 71. Адресная информация в заголовках канального и сетевого уровня при отправке пакета по указанному IP-адресу

Выяснением MAC-адреса получателя занимается протокол ARP, устанавливаемый автоматически вместе со стеком TCP/IP. Он формирует и высылает в сеть ARP-запрос в поле данных широковещательного кадра Ethernet (то есть кадра с широковещательным MAC-адресом получателя $FF\text{-}FF\text{-}FF\text{-}FF\text{-}FF\text{-}FF_{H}$). В запросе указывается IP-адрес интерфейса, чей MAC-адрес выясняется. Широковещательный кадр получают все компьютеры локальной сети, однако ARP-ответ высылается в кадре с индивидуальным (однопунктовым) адресом получателя только компьютером, распознавшим свой IP-адрес в запросе (рис. 72). После получения ответа отпра-

витель заполняет поле MAC-адрес получателя в кадре с пакетом утилиты `ping` (рис. 71) и высылает его в сеть.

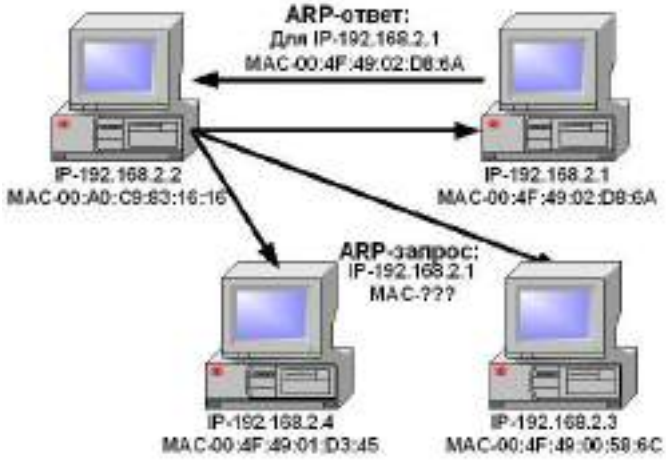



Рис. 72. Модель работы ARP

Соответствие "IP-адрес – MAC-адрес" сохраняется в памяти компьютера-отправителя пакета в так называемой *ARP-таблице* (или *ARP-кэше*). При необходимости повторной высылки пакета по имеющемуся в таблице адресу широковещательный запрос не рассылается. Командой `arp –a` можно просмотреть содержимое этой таблицы (рис. 73).

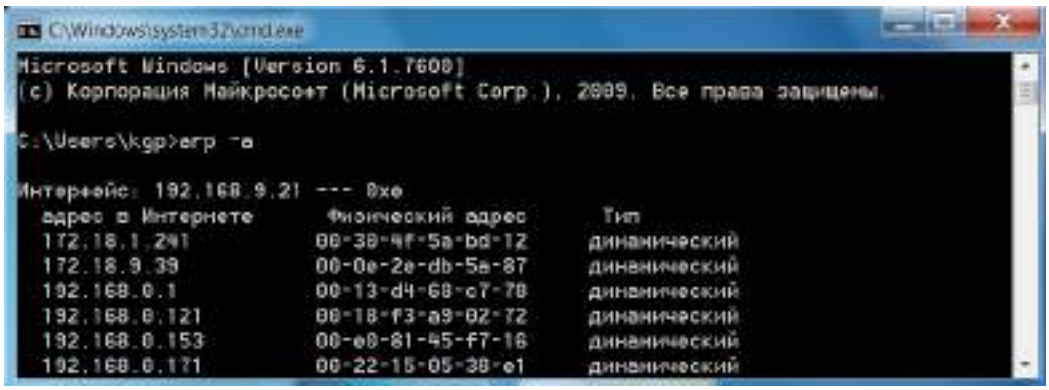



Рис. 73. Пример ARP-таблицы

На рис. 74 приведена структура кадра Ethernet с запросом/ответом ARP. Следует отметить, что рассылка широковещательных сообщений обычно производится только в пределах локальной сети (точнее сегмента сети с компьютерами с одинаковой частью сетевых адресов). Это важно, поскольку широковещательный трафик при большом количестве компьютеров сети может занимать значительную часть полосы пропускания сети. Динамические записи создаются модулем ARP с использованием широковещательных рассылок, статические – вручную администратором командой `arp -s IP-адрес MAC-адрес`. Динамические записи в таблице периодически удаляются (обычно через пять минут), поскольку существует вероятность изменения IP-адресов сетевых интерфейсов, статические остаются неизменными в течение сеанса работы системы. Существует также

протокол *реверсивный протокол разрешения адреса* (*Reverse Address Resolution Protocol – RARP*), решающий задачу нахождения IP-адреса по известному адресу канального уровня. Он используется при старте бездисковых рабочих станций, не знающих в этот момент своего IP-адреса, но знающих MAC-адрес.

| DA | SA | T | MT | PT | MAL | PAL | OC | SMA | SPA | TMA | GPA | Pad | FCS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 6 | 2 | 2 | 2 | 1 | 1 | 2 | 6 | 4 | 6 | 4 | 18 | 4 |

| ARP-запрос | | | ARP-ответ | | |
|---|---|---|---|---|---|
| **Поле** | **Расшифровка** | **Значение (hex)** | **Примеч.** | **Значение (hex)** | **Примеч.** |
| DA | Destination Address | FF:FF:FF:FF:FF:FF | широковещательный | 00:A0:C9:83:16:16 | MAC источника ARP-запроса |
| SA | Source Address | 00:A0:C9:83:16:16 | MAC отправителя | 00:4F:49:02:D8:6A | MAC отправителя |
| T | Type | 0806 | ARP | 0806 | ARP |
| MT | Media Type | 0001 | Ethernet | 0001 | Ethernet |
| PT | Protocol Type | 0800 | IP | 0800 | IP |
| MAL | Media Address Length | 06 | байт (MAC) | 06 | байт (MAC) |
| PAL | Protocol Address Length | 04 | байта (IP) | 04 | байта (IP) |
| OC | Operation Code | 0001 | ARP-запрос | 0001 | ARP-ответ |
| SMA | Sender Media Address | 00:A0:C9:83:16:16 | MAC отправителя | 00:4F:49:02:D8:6A | MAC отправителя |
| SPA | Sender Protocol Address | 192.168.2.2 | IP отправителя | 192.168.2.1 | IP отправителя |
| TMA | Target Media Address | 00:00:00:00:00:00 | текущая подсеть | 00:A0:C9:83:16:16 | MAC получателя |
| GPA | Get Protocol Address | 192.168.2.1 | IP получателя | 192.168.2.2 | IP получателя |
| Pad | Padding | 00 - 18 байт | дополнение кадра до 64 байт | 00 - 18 байт | дополнение кадра до 64 байт |
| FCS | Frame Check Sequence | | Контрольная сумма | | Контрольная сумма |

Рис. 74. Структура кадров ARP запроса и ответа

## 3.4. Изучение принципа работы коммутатора Ethernet

Рассмотрим принцип работы коммутатора Ethernet на примере локальной сети, приведенной на рис. 75. Коммутатор постоянно изучает заголовки поступающих в его порты кадров и заносит в так называемую *таблицу MAC-адресов* значения MAC-адресов из поля адреса отправителя входящих в коммутатор кадров, приписывая их идентификатору порта, в который эти кадры поступают извне (`Fa0/номер_порта` на рис. 75).

Таблица MAC-адресов используется для нахождения номера порта, на который необходимо передать кадр, по MAC-адресу, извлекаемому из поля адреса получателя кадра. Таким образом, коммутатор передаёт кадр со своего входящего порта на исходящий порт, ведущий к получателю кадра

(с порта 3 на порт 6 на рис. 75). Широковещательные кадры коммутатор передаёт на все свои порты, кроме порта, в который поступает кадр извне. Аналогичным образом происходит и коммутирование кадров с неизвестным для коммутатора MAC-адресом (который ещё не занесен в его таблицу MAC-адресов). Отметим, что заполнение таблицы обычно происходит быстро, т.к. при включении рабочих станций каждая из них стразу же высылает в широковещательном кадре своё сетевое имя.

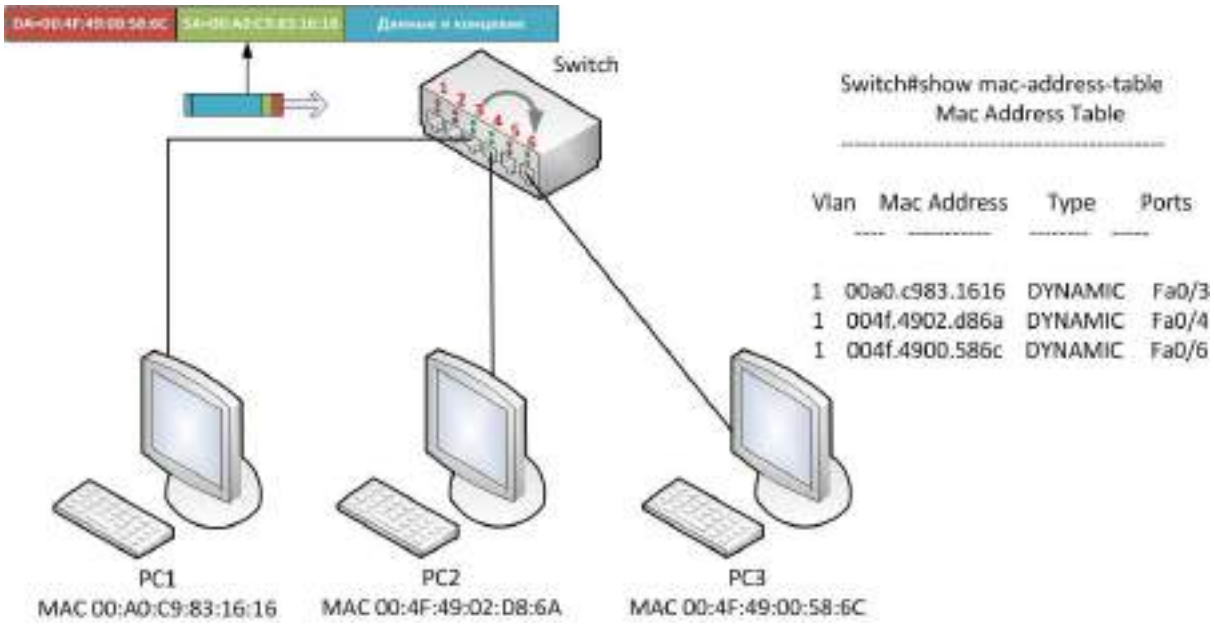



Рис. 75. Принцип работы коммутатора Ethernet

## Задание для самостоятельной работы

Запустите анализатор протоколов Wireshark. Выполните захват пакетов утилиты `ping`, с помощью которой они посылаются на соседний компьютер. Для этого в Wireshark выполните щелчки по пунктам меню Capture (Захват) – Option…(Опции…). Откроется окно настроек параметров захвата (рис. 76), в котором необходимо выбрать интерфейс, который будет захватывать пакеты (на компьютере с одним сетевым интерфейсом он выбирается автоматически). Название интерфейса и его IP-адрес будут совпадать со значениями, выводимыми командой `ipconfig /all (ifconfig)`. Обратите внимание, что по умолчанию сетевой интерфейс захватывает пакеты в *неразборчивом режиме* (*promiscuous mode*), то есть не только пакеты, предназначаемые для него, а все, которые он видит в сети.

В строке определения фильтра захвата целесообразно указывать фильтр с целью захвата только пакетов с интересующей нас информацией. На рис. 76 указано, что захватывать необходимо только пакеты, переносящие данные *протокола контрольных сообщений Интернета* (*Internet Control Message Protocol – ICMP*), поскольку утилита `ping` переносит данные именно этого протокола. Достаточно часто необходимо захватывать пакеты, только отправляемые и получаемые одной рабочей станцией. В этом случае фильтр будет выглядеть `host ip_адрес_станции`. *Wireshark*

обладает очень гибкой системой фильтрации, с примерами фильтров можно ознакомиться, открыв окно щелчком по кнопке Capture Filter. Выделив название фильтра в списке предопределённых фильтров в нижней части окна можно увидеть название этого фильтра и команду, которая задаёт правила фильтрации. Можно изменять их, подставляя необходимые параметры. Также существует возможность создания и удаления пользовательских фильтров. Нужно отметить, что применяемые фильтры сохраняются в строке-списке фильтров захвата окна Capture Options (рис. 76).

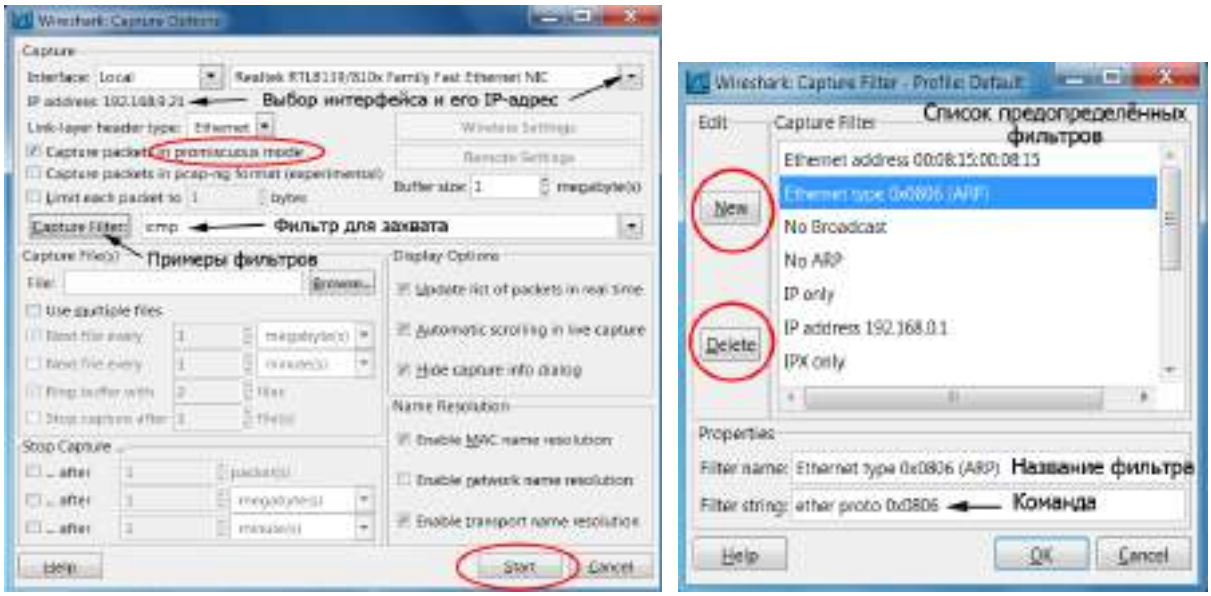



Рис. 76. Настройка параметров захвата в Wireshark

После настройки захвата только ICMP-пакетов выполните щелчок на кнопке Start в окне Capture Options, после чего откройте окно командной строки (Пуск-Выполнить-cmd) и запустите в нём команду `ping` с указанием IP-адреса соседнего компьютера в качестве параметра. Wireshark выполнит захват пакетов в окне, приведенном на рис. 70. Для завершения захвата пакетов выполните щелчок на кнопке Остановить текущий захват (Stop the running live capture) (рис. 77).

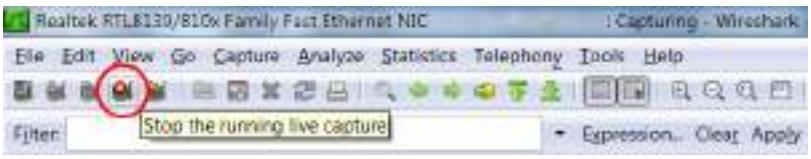



Рис. 77. Остановка захвата пакетов в Wireshark

Выделите первый из захваченных пакетов (отправленный Вашим компьютером), в области анализа полей пакета выделите заголовок Ethernet. Приведите в отчёт шестнадцатеричный дамп этого заголовка, выделенный в нижней части окна. Выполните расшифровку полей заголовка.

Выделите второй из захваченных пакетов (полученный Вашим компьютером) и повторите предыдущее задание.

Выполните в отчёте расшифровку MAC-адресов отправителя и получателя, указав тип адреса (индивидуальный, групповой, широковещательный), значения *OUI* и *OUA*, является ли адрес локально уникальным или глобально уникальным. Выполните запросы к базе данных IEEE и определите по значениям *OUI* информацию о производителе контроллеров сетевых интерфейсов отправителя и получателя. Приведите полученную информацию в отчёт.

С помощью команды `arp –a` просмотрите текущее состояние ARP-таблицы Вашего компьютера и приведите её в отчёт. Настройте Wireshark на захват всех пакетов, получаемых и отправляемых компьютером локальной сети, адреса которого не содержатся в ARP-таблице. Запустите захват и в командной строке с помощью утилиты `ping` пошлите пакеты компьютеру, адрес которого указан в фильтре захвата. ICMP-пакетами утилиты `ping` должны быть захвачены два пакета: с ARP-запросом и ARP-ответом. Выделите в окне анализа полей пакета заголовок Ethernet пакета с ARP-запросом. Выполните его сравнение с ICMP-пакетом, отправленным Вашим компьютером в предыдущем задании. Опишите в отчёте различия полей заголовка Ethernet этих кадров. Укажите, какой формат кадров Ethernet используется для транспортировки этих пакетов. Выполните анализ полей ARP-запроса и ARP-ответа и приведите его в отчёт.

Для изучения работы коммутатора Ethernet создайте с помощью Packet Tracer модель локальной сети, состоящей из четырёх рабочих станций с именами `PC1`, `PC2`, `PC3`, `PC4`, подсоединённых, соответственно, к портам `FastEthernet0/1`, `0/2`, `0/3` и `0/4`, коммутатора 2950-24 с именем `Switch0`. Задайте станциям IP-адреса `192.168.1.1`, `192.168.1.2`, `192.168.1.3` и `192.168.1.4`, соответственно, с маской подсети `255.255.255.0`. Выполните щелчок на инструменте Inspect (Инспектировать)  , а затем на коммутаторе, из открывшегося окна выберите команду MAC Table (Таблица MAC-адресов). Должно открыться пустое окно MAC Table for Switch0, поскольку `Switch0` пока не получал кадров ни от одного компьютера.

Детальное изучение процессов, происходящих в сети, удобно выполнять в режиме Simulation (Симуляция) Packet Tracer (под симуляцией понимается моделирование программой событий, происходящих в реальной сети). Для перехода в этот режим выполните щелчок по переключателю в правом нижнем углу окна из Realtime (Режима реального времени) в режим Simulation (Симуляция). Откроется окно Event List (Список событий) в правой части окна Рабочей области. (рис. 78). На Панели инструментов выберите Add simple PDU (Добавить простой PDU)  . Термином *Протокольная единица данных – Protocol Data Unit, PDU* обозначается структура данных протокола любого уровня модели взаимодействия открытых систем (ПРИЛОЖЕНИЕ А), в Packet Tracer инструмент Add simple PDU (Добавить простой PDU) добавляет пакет ICMP, высылаемый с помощью утилиты `ping`. После выбора этого инструмента выполните щелчок вначале по станции-отправителю (например,

PC1), а затем по станции-получателю (например, PC2) пакета. Вы должны увидеть обозначающий ICMP-пакет конвертик с перемещающимися прямоугольниками возле станции-отправителя, а также первое событие в списке – наличие отправляемого пакета ICMP у станции PC1. Кроме того, поскольку станции-отправителю PC1 не известен MAC-адрес станции-получателя PC2, возле неё также будет находиться конвертик другого цвета, обозначающий запрос ARP, соответствующее событие также будет находиться в списке событий (рис. 78).

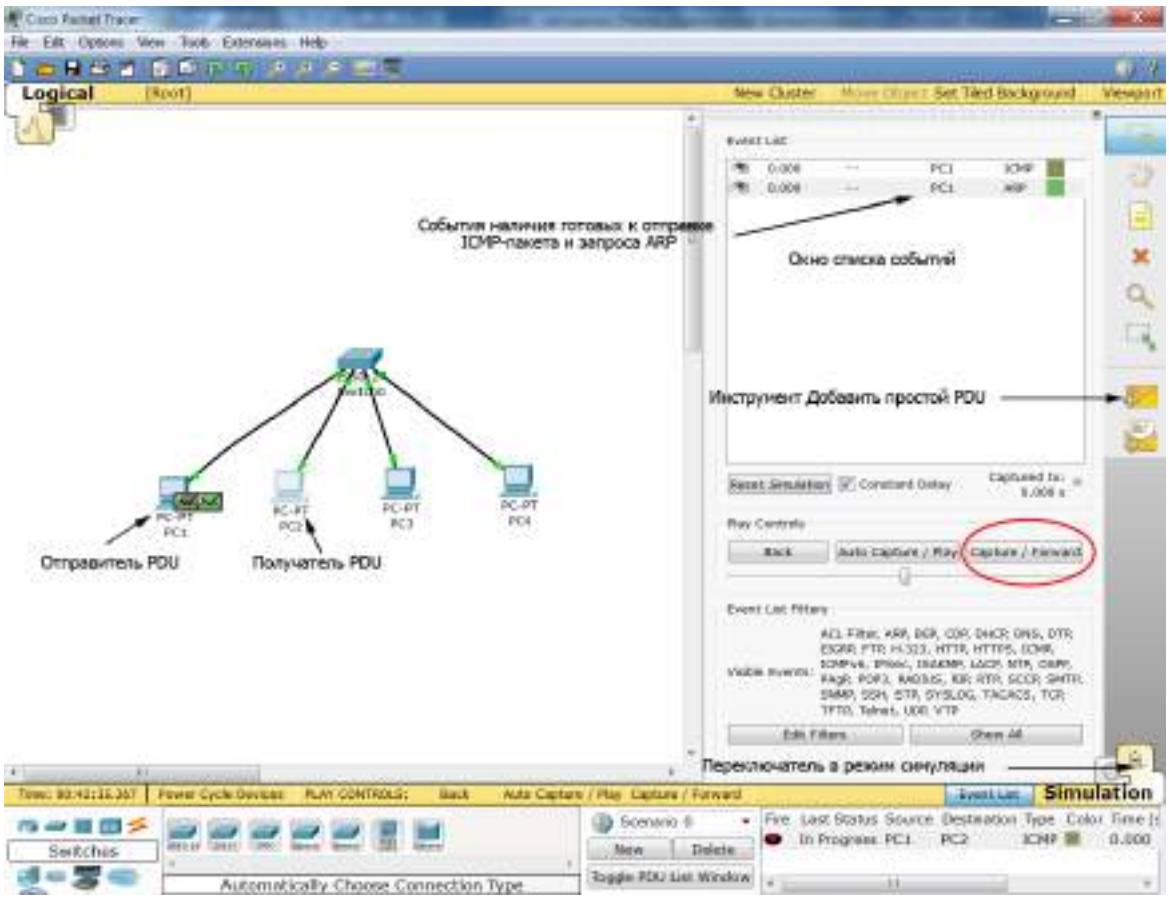



Рис. 78. Режим симуляции Wireshark

С помощью инструмента Inspect (Инспектировать) просмотрите ARP-таблицы PC1 и PC2, выбрав соответствующую команду, пока они должны быть пустыми. Выполните щелчок по кнопке Capture/Forward (Захват/Следующий шаг) и Вы увидите передачу ARP-запроса от PC1 коммутатору, обратите внимание на новое событие, появившееся в списке. С помощью инструмента Inspect (Инспектировать) просмотрите MAC-таблицу коммутатора, в ней уже должна быть запись адресов для PC1. Выполните ещё один щелчок по кнопке Capture/Forward (Захват/Следующий шаг) и Вы должны увидеть отправку полученного от PC1 ARP-запроса коммутатором всем остальным рабочим станциям, то есть широковещательную рассылку. На конвертиках у PC3 и PC4 должны появиться красные крестики, означающие, что в ARP-запросе не содержится их IP-адрес, а ARP-таблице PC2 должна появиться запись для PC1. Следующий щелчок по кнопке

Capture/Forward (Захват/Следующий шаг) приведёт к отправке ARP-ответа станцией PC2 коммутатору. После этого шага в таблице MAC-адресов коммутатора появится запись с MAC-адресом PC2. Следующий шаг приведёт к получению ARP-ответа станцией PC1 и добавлению записи для PC2 в её ARP-таблицу.

Последующие щелчки по кнопке Capture/Forward (Захват/Следующий шаг) приведут к отправке ICMP-пакета от PC1 через коммутатор PC2 и получению ICMP-отклика от PC2 через коммутатор PC1. Коммутатор знает, на каком порту находятся обе станции, поэтому коммутация выполняется без широковещательных рассылок (рис. 79).

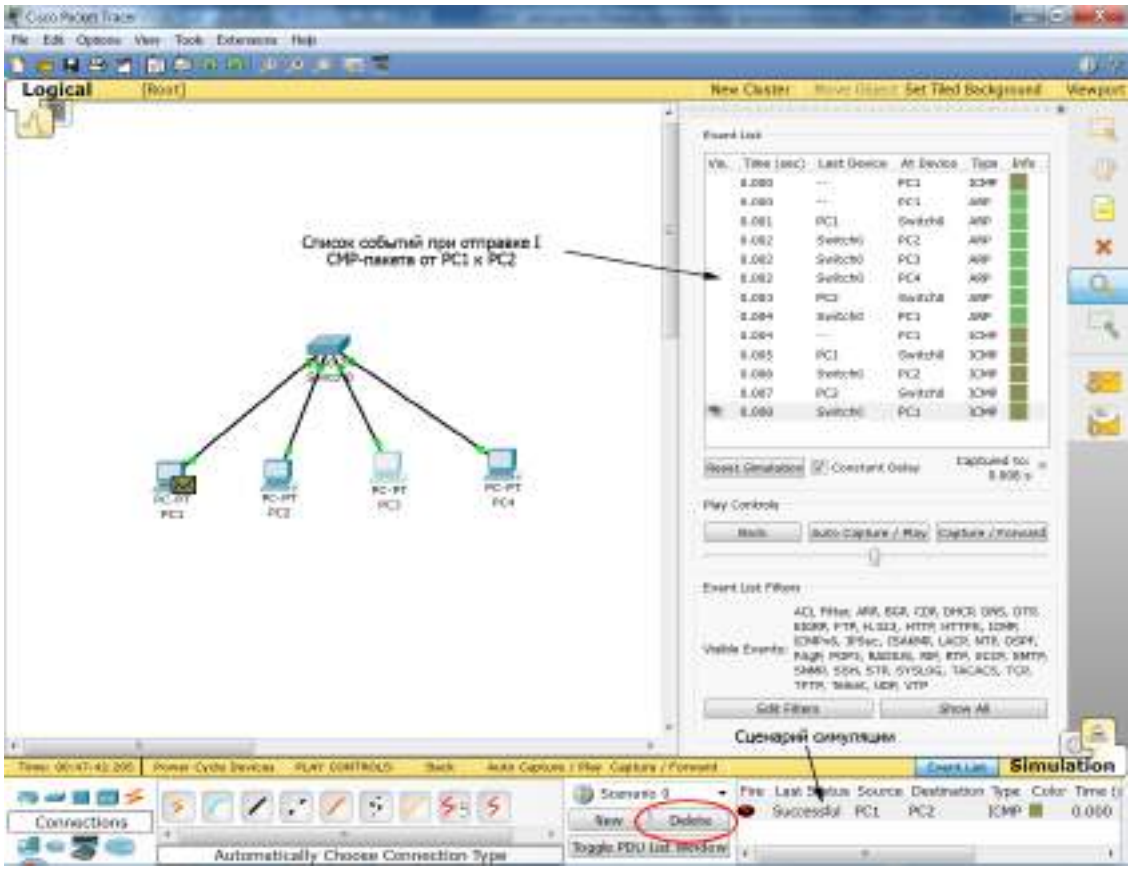



Рис. 79. Симуляция пересылки ICMP-пакетов между PC1 и PC2

Повторите выполненную симуляцию для пересылки ICMP-пакета от станции PC3 станции PC4. Занесите в отчёт в приведенную ниже таблицу список событий и записи в ARP-таблицах PC3 и PC4 и MAC-таблице коммутатора после выполнения каждого события (табл.3).

Таблица 3

Изучение ARP и работы коммутатора

| № события | Отправитель | Получатель | Тип пакета | ARP-таблица PC3 | ARP-таблица PC4 | MAC-таблица Switch0 |
|---|---|---|---|---|---|---|

Выполните просмотр ARP-кэшей PC3 и PC4 из командной строки каждой из них, приведите эту информацию в отчёт.

По аналогии с предыдущим заданием выполните исследование передачи ICMP-пакетов между PC1 и PC3 и затем между PC2 и PC4 в сети с двумя коммутаторами, приведенной на рис. 80.

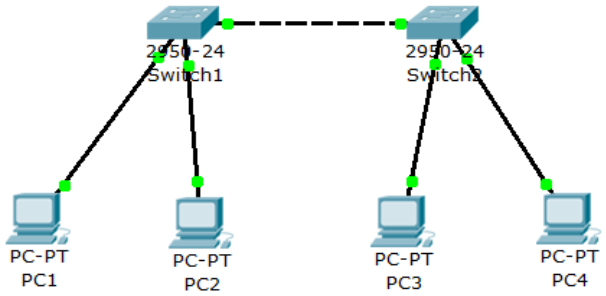



Рис. 80. Модель сети для изучения работы коммутаторов

Занесите в отчёт в приведенную ниже таблицу список событий и записи в MAC-таблицах коммутаторов Switch1 и Switch2 после выполнения каждого события (табл.4).

Таблица 4

Изучение принципа построения MAC-таблиц двух коммутаторов

| № события | Отправитель | Получатель | Тип пакета | MAC-таблица Switch1 | MAC-таблица Switch2 |
|---|---|---|---|---|---|

Существует возможность просмотра содержимого таблицы MAC-адресов коммутатора с помощью команд *Cisco IOS* (следует отметить, что реальные управляемые сетевые устройства могут не поддерживать графические инструментальные средства, подобные рассмотренным в процессе симуляции, но точно поддерживают управление из командной строки). Для просмотра таблицы MAC-адресов выполните щелчок на коммутаторе и откройте вкладку командной строки (Command Line Interface – CLI). Нажмите Enter и Вы увидите приглашение *режима пользователя* (*User Mode*), его признаком является приглашение '>'. Из режима пользователя можно перейти в *привилегированный режим* (*Privilege Mode*), его признаком является приглашение '#'. В первом режиме можно только просматривать конфигурацию устройства, во втором – осуществлять конфигурирование. Для того, чтобы войти в привилегированный режим необходим ввести команду enable (допускается сокращённая форма команды – en). Справку по каждой команде можно получить посредством её набора в командной строке и набора знака ? после неё. Для просмотра таблицы MAC-адресов коммутатора выполните в привилегированном режиме команду show mac-address-table (рис. 81).

Из привилегированного режима можно войти в *режим глобального конфигурирования* (*Global Configuration Mode*) командой configure terminal (config t), его признаком является слово (config), выводимое после имени устройства в приглашении. Выход из этого режима осуществляется командой end (или нажатием комбинации клавиш <CTL>+z).

```
#config t
(config)#end
```

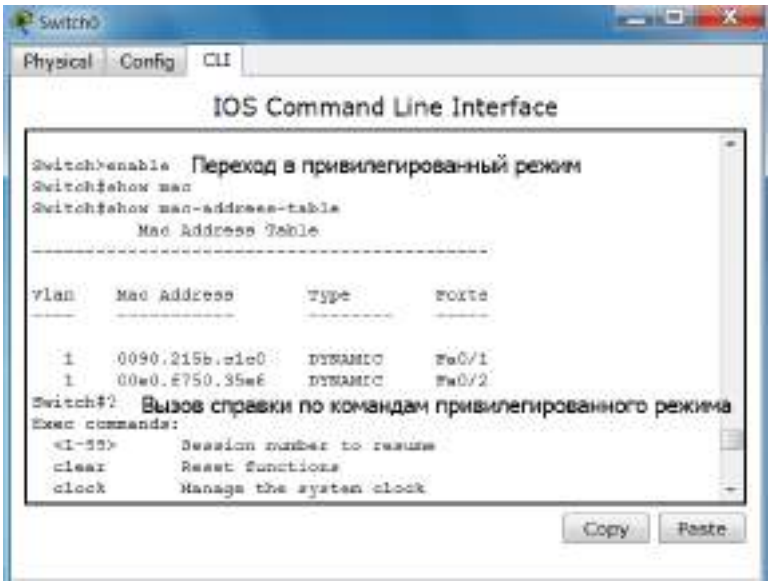



Рис. 81. Переход в привилегированный режим и просмотр таблицы MAC-адресов коммутатора командами Cisco IOS

Сетевые устройства могут иметь различные типы интерфейсов, например, token ring, FDDI, Ethernet, Serial, ISDN и др. В качестве имени интерфейса используется обычно название протокола и номер интерфейса, начиная с `0`, например, `ethernet0` (1 порт Ethernet), `serial0` (1 последовательный порт) и т.д. Достаточно часто сетевые устройства могут иметь несколько модулей с сетевыми интерфейсами, в этом случае идентификация интерфейса состоит из названия протокола, номера модуля/номера интерфейса, например, `FastEthernet0/1`. Для просмотра статуса всех интерфейсов устройства используют команду `show interfaces` (сокращение - `sh int`). Для просмотра информации об определенном интерфейсе вводится команда `show interfaces <имя_интерфейса>`. Из режима глобального конфигурирования можно войти в *режим конфигурирования интерфейса* (*Interface Configuration Mode*), выполнив команду `interface <имя_интерфейса>`, его признаком является слово `(config-if)` в приглашении. В приведенном ниже примере осуществляется переход из привилегированного режима в режим общего конфигурирования, а затем переход в режим конфигурирования интерфейса `FastEthernet0/1`. В этом режиме подаётся команда `no shutdown`, переводящая интерфейс в активное состояние.

```
#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
(config)#interface FastEthernet0/1
(config-if)#no shutdown
(config-if)#end
#
```

Команда `end` позволяет выйти из режима конфигурирования интер-

фейса.

Выполните в окне командной строки просмотр таблицы MAC-адресов коммутатора `Swith0` и скопируйте сеанс работы в отчёт.

Изучение форматов кадров, отличных от Ethernet II (DIX), на практике часто представляет сложность. Это объясняется тем, что в настоящее время стек протоколов TCP/IP вытеснил достаточно популярные ранее стеки IPX/SPX и NetBIOS (в Windows Vista/7 отсутствует их поддержка), а именно они используют формат кадра 802.3/LLC. Также достаточно сложно захватит кадры с форматом Ethernet SNAP. К счастью режим Simulation (Симуляция) Packet Tracer может нам помочь.

Создайте в Packet Tracer сеть, состоящую из двух соединённых между собой коммутаторов, к каждому из которых подсоединена рабочая станция (рис. 82). Назначьте сетевым интерфейсам рабочих станций IP-адреса `192.168.1.1` и `192.168.1.2` с маской `255.255.255.0`. Переключитесь в режим симуляции и добавьте простой PDU от одной станции к другой.

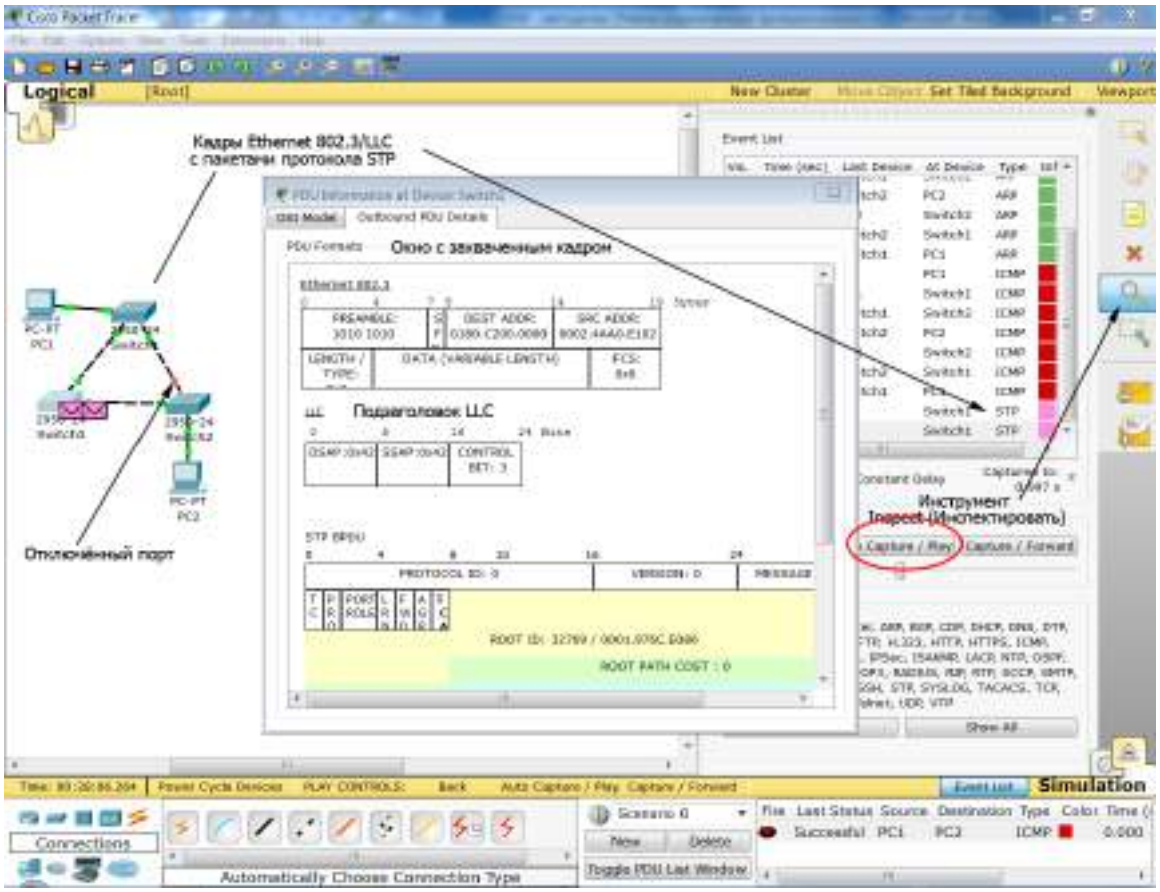



Рис. 82. Модель сети и захваченный кадр Ethernet формата 802.3/LLC

Выполните щелчок по кнопке Auto Capture/Play (Автозахват/Анимация) и Вы увидите автоматически сменяющиеся события в сети. Дождитесь появления в списке событий события с типом STP и выполните щелчок по кнопке Auto Capture/Play (Автозахват/Анимация) для остановки симуляции. *Протокол остовного дерева – Spanning Tree Protocol, STP* – это протокол, поддерживающийся коммутаторами Ethernet, основной задачей которого

является исключение кольцевых топологий в сети Ethernet путём автоматического блокирования создающих кольцевую топологию портов коммутатора. Для нас важно, что пакеты этого протокола транспортируются кадром Ethernet формата 802.3/LLC. Выполните щелчок на инструменте Inspect (Инспектировать), а затем на изображении конверта, соответствующего протоколу STP на схеме сети. Откроется окно PDU Information (Информация о протокольном блоке данных), в котором Вы увидите структуру заголовков кадра аналогично тому, как Вы наблюдали её в области анализа полей пакета анализатора Wireshark (рис. 82). В этом окне Вы видите структуру пакета с подзаголовками MAC и LLC Ethernet-кадра. В 13 и 14 байте указана длина поля данных (то есть длина пакета STP вместе с его заголовком), значения полей DSAP SSAP=$42_{H}$ в подзаголовке LLC идентифицируют переносимый в поле данных пакет STP.

Приведите в отчёт скриншот окна со структурой захваченного кадра.

Для захвата Ethernet-кадра формата SNAP создайте в *Packet Tracer* сеть, состоящую из соединённых между собой маршрутизаторов (рис. 83). Задайте IP-адреса интерфейсам маршрутизаторов `192.168.1.1` и `192.168.1.2` с маской `255.255.255.0` для непосредственно связанных интерфейсов `Router1` и `Router2` и `192.168.2.1` и `192.168.2.2` с маской `255.255.255.0` для непосредственно связанных интерфейсов `Router2` и `Router3`. После задания адресов, включите интерфейсы, установив отметку в чекбоксе Port Status (Состояние порта) на вкладке Config свойств интерфейсов маршрутизаторов. Далее, по аналогии с предыдущим заданием организуйте симуляцию передачи простого PDU от `Router1` к `Router3` и захватите кадр с пакетом *CDP – Cisco Discovery Protocol* (*протокол обнаружения устройств Cisco*) – протокол, разработанный компанией Cisco Systems, позволяющий обнаруживать подключённое сетевое оборудование Cisco, его название, версию IOS и IP-адреса. Пакет этого протокола переносится в кадрах Ethernet SNAP. Выполните анализ кадра в окне PDU Information (Информация о протокольном блоке данных) и приведите скриншот этого окна в отчёт. Также запишите в отчёт значения полей DSAP, SSAP, OUI и Type для захваченного кадра.

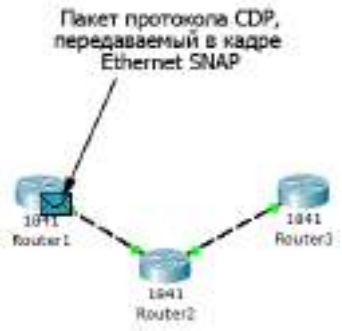



Рис. 83. Модель сети для изучения формата кадра Ethernet SNAP

## Вопросы для самоподготовки

1. Укажите, на каких уровнях модели взаимодействия открытых систем работает технология Ethernet.
2. Укажите название организации, разрабатывающей стандарты технологии Ethernet.
3. Укажите наиболее распространённые версии технологии Ethernet в настоящее время и скорости передачи данных этими технологиями.
4. Укажите наиболее скоростные в настоящее время и перспективные версии технологии Ethernet и скорости передачи данных этими технологиями.
5. Что собой представляет технология Wi-Fi, кто является разработчиком стандартов этой технологии?
6. Опишите обобщённый формат кадра Ethernet и укажите размеры его полей в байтах.
7. Что представляет собой контрольная сумма кадра Ethernet, какой алгоритм используется для её расчёта?
8. Опишите формат MAC-адреса. Дайте характеристику его полям.
9. Укажите типы MAC-адресов, каким образом выполняется идентификация типа по значению MAC-адреса?
10. Опишите форматы кадров Ethernet: Ethernet II (DIX) и Ethernet Raw 802.3/Novell 802.3, что обозначает аббревиатура DIX?
11. Опишите форматы кадров Ethernet 802.3/LLC и Ethernet SNAP. Какие функции выполняют подзаголовки LLC и SNAP?
12. Опишите алгоритм определения типа кадра Ethernet.
13. Перечислите основные функции анализаторов сетевых протоколов и опишите интерфейс и способы работы с анализатором Wireshark. Как осуществляется работа интерфейса в неразборчивом режиме?
14. Опишите назначение и алгоритм работы протокола ARP. Что собой представляет ARP-кэш и какой командой можно его просмотреть на рабочей станции?
15. Укажите, в каких пределах распространяются широковещательные кадры.
16. Опишите принцип работы коммутатора Ethernet. Что собой представляет таблица MAC-адресов и каким образом она заполняется?
17. Укажите, как коммутатор Ethernet передаёт широковещательные кадры и кадры с MAC-адресом получателя, для которого отсутствует запись в таблице MAC-адресов.
18. Приведите команду фильтров захвата: а) для захвата кадров с сообщениями, высылаемыми утилитой ping; б) для захвата кадров, отправляемых/получаемых рабочей станцией с IP-адресом `192.168.1.1`; в) для захвата кадров с ARP-пакетами.
19. Опишите возможности, предоставляемые программой Packet Tracer в режиме симуляции. Что называют протокольной единицей данных (PDU)?

20. Поясните записи, занесенные Вами в табл. 3 и табл. 4.
21. Назовите режимы работы Cisco IOS с сетевыми устройствами и команды перехода из режима в режим.
22. Приведите последовательность команд Cisco IOS для просмотра MAC-таблицы коммутатора Ethernet.
23. Укажите названия и назначения примеров протоколов, пакеты которых переносятся в кадрах форматов Ethernet 802.3/LLC и SNAP.

## Тесты для контроля усвоения знаний

1. Укажите номера битов MAC-адреса (нумерация начинается с нуля) для каждого из его полей:
   а) Поле U/L – уникальный в глобальном/локальном масштабе;
   б) Поле I/G – индивидуальный/групповой;
   в) Поле OUA – организационно-уникального идентификатора – порядкового номера сетевого контроллера, выпускаемого организацией;
   г) Поле OUI – организационно-уникального идентификатора – кода организации, выпускающей сетевое оборудование.
2. Выберите максимальную на сегодняшний день стандартизованную скорость передачи данных по технологии Ethernet:
   а) 10 Мбит/с;
   б) 100 Мбит/с;
   в) 1 Гбит/с;
   г) 10 Гбит/с;
   д) 40 Гбит/с;
   е) 100 Гбит/с;
   ж) 1 Тбит/с.
3. Укажите уровни модели взаимодействия открытых систем, на которых работает технология Ethernet:
   а) сетевой;
   б) канальный;
   в) прикладной;
   г) транспортный;
   д) представления данных;
   е) физический;
   ж) сеансовый.
4. Укажите размеры максимального кадров Ethernet (не учитывая опциональную возможность передачи гигантских кадров (Jambo Frame)):
   а) 32 байта;
   б) 64 байта;
   в) 128 байт;
   г) 256 байт;
   д) 512 байт;
   е) 1024 байта;

ж) 1518 байт;
з) 2000 байт.

5. Укажите размеры минимальных кадров Ethernet (не учитывая опциональную возможность увеличения минимального размера кадра до 512 байт в полудуплексном режиме работы технологии Gigabit Ethernet):
   а) 32 байта;
   б) 64 байта;
   в) 128 байт;
   г) 256 байт;
   д) 512 байт;
   е) 1024 байта;
   ж) 1518 байт;
   з) 2000 байт.
6. Укажите размер MAC-адреса:
   а) 2 байта;
   б) 3 байта;
   в) 4 байта;
   г) 6 байт;
   д) 8 байт.
7. Определите тип приведенных MAC-адресов (однопунктовый, групповой, широковещательный):
   а) `33:33:00:01:00:03` – это…
   б) `00:1c:f0:0d:66:11` – это…
   в) `ff:ff:ff:ff:ff:ff` – это…
8. Определите тип кадра Ethernet (DIX, Novell 802.3, 802.3/LLC, SNAP) по байтам заголовка канального уровня:
   а) `00:4F:49:02:D8:6A:00:A0:C9:83:16:16:08:00;`
   б) `00:A0:C9:85:17:B2:00:4F:4E:00:E5:8F:00:54:E0:E0:03;`
   в) `00:4F:4E:00:CD:4A:00:60:8C:41:DF:C7:00:96:AA:AA:03:00:00:00:08:00;`
   г) `00:00:F8:45:13:AC:00:00:C0:02:56:AB:00:78:FF:FF.`
9. Выберите неизвестную в общем случае адресную информацию при отправке пакета утилиты `ping` по IP-адресу назначения:
   а) MAC-адрес отправителя;
   б) MAC-адрес получателя;
   в) IP-адрес отправителя;
   г) IP-адрес получателя.
10. Укажите, откуда коммутатор Ethernet узнаёт MAC-адреса подключённых к нему компьютеров, необходимые для заполнения его таблицы MAC-адресов:
    а) выполняет последовательный опрос подключённых компьютеров;
    б) "подсматривает" адрес отправителя во входящих в него пакетах;
    в) опрашивает все компьютеры в широковещательном режиме.
11. Укажите, какие пакеты будет захватывать Wireshark при введённой команде фильтра `ether proto 0x0806`

а) только кадры Ethernet с любыми пакетами внутри;
б) только кадры Ethernet с IP пакетами внутри;
в) только кадры Ethernet с ARP-пакетами внутри.

12. Укажите команды (`enable, config t, interface имя_интерфейса`), позволяющие осуществлять вход в различные режимы работы Cisco IOS:
    а) войти в режим глобального конфигурирования можно командой…;
    б) войти в привилегированный режим можно командой…;
    в) войти в режим конфигурирования интерфейса можно командой….

## Литература


1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с.: ил.
2. Гук М. Аппаратные средства локальных сетей. Энциклопедия / М. Гук. – СПб. : Питер, 2000. – 576 с.
3. Амато В. Основы организации сетей Cisco : пер. с англ. / В. Амато. – М. : Вильямс, 2004. – 512 с.
4. Официальный сайт Cisco Systems. Программа Cisco Packet Tracer [электронный ресурс]. – режим доступа: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html.
5. Официальный сайт программы-анализатора сетевых протоколов Wireshark [электронный ресурс]. – режим доступа: http://www.wireshark.org.

# РАЗДЕЛ 4
# ИЗУЧЕНИЕ ПРОТОКОЛА IP И ТЕХНОЛОГИИ МАРШРУТИЗАЦИИ

## 4.1. Адресация хостов, сетей и подсетей с использованием IP

*Протокол Интернета* (*Internet Protocol – IP*), описываемый стандартом RFC 791 (*RFC – Request For Comment – запрос комментариев* – система стандартов протоколов Интернета), представляет собой системное программное обеспечение, работающее на сетевом уровне модели взаимодействия открытых систем (ПРИЛОЖЕНИЕ А) (здесь и далее подразумевается 4-я версия протокола IP). Основное назначение IP – передача пакетов (для IP они называются *дейтаграммами – datagram*) между рабочими станциями (для IP они называются *хостами – host*), находящимися в одной или разных *IP-сетях* или *IP-подсетях* (*IP-network*/*IP-subnetwork*) (подсети выделяются из сетей с помощью маски подсети, что будет рассмотрено далее в этом разделе). Для адресации отправителей и получателей дейтаграмм IP использует четырёхбайтовый адрес, значение каждого байта которого записывается в десятичной системе в виде `X.X.X.X`, где `X=0-255`. В отличие от MAC-адресации, не предусматривающей выделение группы MAC-адресов и назначение ей общего адреса, протоколы сетевого уровня выполняют такую группировку. Достигается это благодаря тому, что IP-адрес состоит из двух частей – сетевой (старшие биты IP-адреса) и хостовой (младшие биты IP-адреса). Например, в адресе **`192.168.1.1`** можно выделить сетевую часть – три старшие цифры **`192.168.1`** адреса и хостовую часть – одну младшую цифру **`1`** адреса, этот адрес принадлежит IP-сети с диапазоном адресов **`192.168.1.0`** - **`192.168.1.255`**. В качестве адреса всей сети используется первый из адресов этой сети, то есть **`192.168.1.0`** для приведенного примера, и он не может назначаться сетевым интерфейсам в качестве их адреса. В результате такого подхода становится возможной адресация групп компьютеров – *сетей* и *подсетей*, что позволяет с помощью *маршрутизаторов* (*Router*) – устройств, соединяющих сети/подсети в единую *составную сеть* (*internetworking*), реализовать технологию маршрутизации дейтаграмм между сетями/подсетями. Под *маршрутизацией* следует понимать определение маршрутизаторами оптимального пути передачи дейтаграммы по направлению к её получателю на основе информации об адресах сетей/подсетей и пересылку дейтаграммы по этому пути. На рис. 84 приведен пример составной сети, состоящей из четырёх IP-сетей, организованных на коммутаторах Ethernet, которые объединены с помощью двух маршрутизаторов (сеть между маршрутизаторами является пятой IP-сетью). Рядом с коммутаторами и возле связи между маршрутизаторами указаны IP-адреса сетей и так называемые *маски подсети* (*Subnet Mask*), позволяющие делить IP-сети на IP-подсети (об этой технологии будет рассказано далее). Обратите внимание, что в состав се-

тей входят не только сетевые интерфейсы хостов, подсоединённых к коммутатору, но и сетевой интерфейс маршрутизатора, через который он подключён к данной сети, на рис. 84 такие интерфейсы маршрутизаторов посечены стрелками. Эти интерфейсы маршрутизаторов называются *шлюзами* (*Gateway*), дейтаграммы проходят через шлюз только в случае, если они адресованы получателям, находящимся в другой сети/подсети (то есть в случае, когда IP-адреса сети/подсети отправителя и сети/подсети получателя различаются). IP-адрес шлюза указывается при конфигурировании сетевых интерфейсов всех хостов сети/подсети (рис. 12 раздела 1.1).

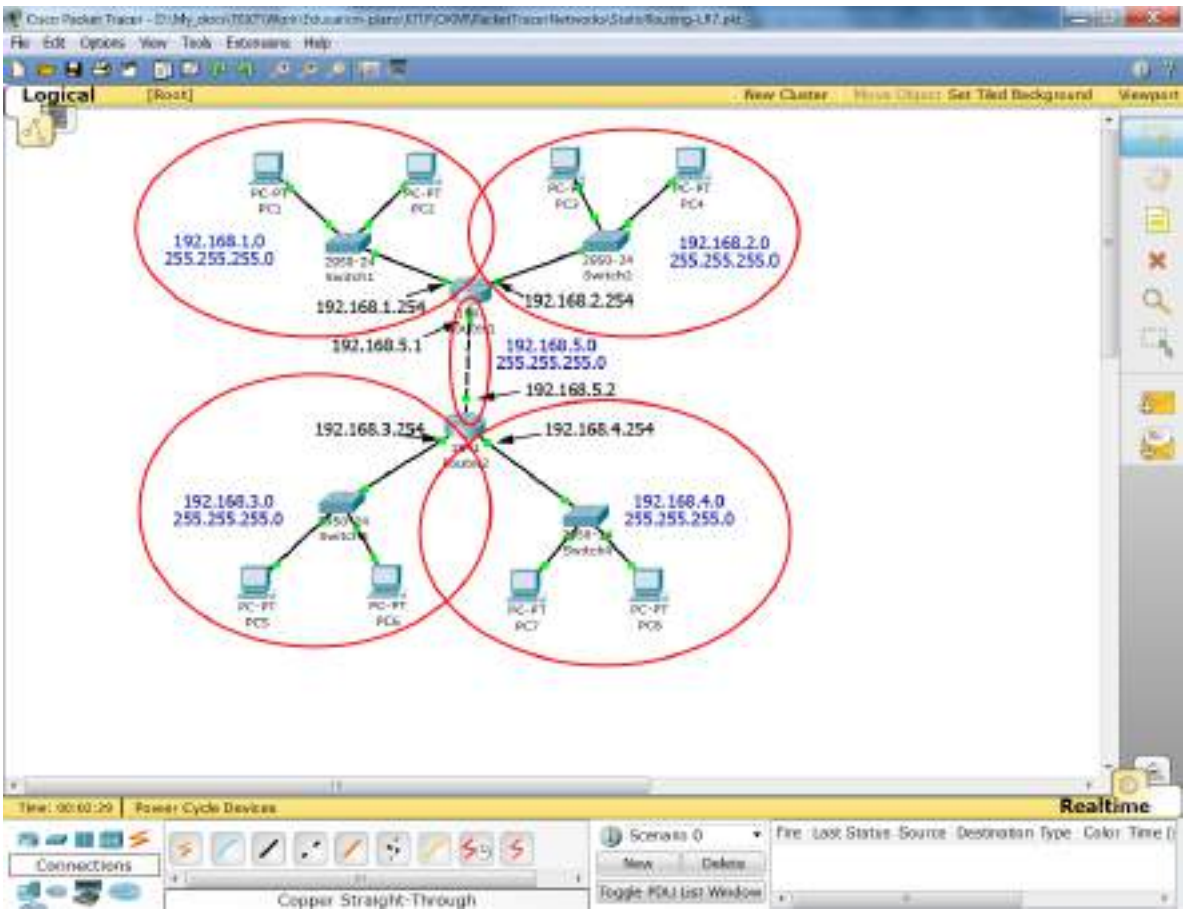



Рис. 84. Пример составной IP-сети

Кроме адресации интерфейсов хостов, сетей/подсетей и маршрутизации, IP может выполнять *фрагментацию/дефрагментацию дейтаграмм* при передаче их между сетями с различными максимально допустимыми значениями длины поля данных кадров канального уровня - так называемой *максимальной единицы передачи* (*Maximum Transfer Unit, MTU*). На практике фрагментация/дефрагментация может происходить, когда маршрутизатор объединяет сети с разной технологией канального уровня, например, при объединении сетей Ethernet и Token Ring. (Технология *маркерного кольца – Token Ring* разработки IBM характеризуется кольцевой топологией сети и детерминированным алгоритмом обработки кадров, для Token Ring характерно отличное от Ethernet значение MTU). При этом

фрагментацию/дефрагментацию могут осуществлять как маршрутизаторы, так и хосты.

Следует отметить, что в IP отсутствуют механизмы, гарантирующие доставку дейтаграммы получателю и её целостность. Эти функции возлагаются на транспортный уровень модели взаимодействия открытых систем (ПРИЛОЖЕНИЕ А) и будут рассмотрены в следующем разделе.

Поскольку размер адреса протокола IP 4-й версии составляет 4 байта= 32 бита, то пространство адресов составляет $2^{32} \approx 4{,}3$ млрд адресов. Из этого адресного пространства пользователям выделяются блоки смежных адресов – IP-сети (IP-подсети) и отдельные адреса. Выделение адресов координирует Международная организация Internet Assigned Numbers Authority (IANA) через пять организаций *региональных интернет-регистраторов*: African Network Information Centre (AfriNIC), American Registry for Internet Numbers (ARIN), Asia-Pacific Network Information Centre (APNIC), Latin American and Caribbean Internet Addresses Registry (LACNIC), Réseaux IP Européens Network Coordination Centre (RIPE NCC) (рис. 85). Эти организации выделяют блоки IP-адресов *локальным интернет-регистраторам* (*провайдерам услуг Интернет*). Последние выделяют из своих блоков субблоки IP-адресов и отдельные IP-адреса конечным пользователям. Поскольку каждый из Региональных Интернет-провайдеров и Локальных Интернет-провайдеров обладает неперекрывающимися блоками IP-адресов, обеспечивается уникальность IP-адреса в глобальном масштабе.


Рис. 85. Региональные Интернет-регистраторы

Поскольку для разных пользователей существует потребность в сетях различного масштаба, в протоколе IP предусмотрена классификация IP-сетей. Предусмотрено пять классов IP-адресов: основные классы A, B, C и дополнительные классы D и E. Идентификация класса сети, к которому принадлежит IP-адрес, выполняется по старшему байту адреса (рис. 86), распределение адресного пространства IP v4 между провайдерами и организациями с датой их распределения можно увидеть по адресу http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml.

| Класс | 1 байт | | | | | | | | 2 байт | | | | | | | | 3 байт | | | | | | | | 4 байт | | | | | | | | 1 дес. число | Примеч. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | 0 | № сети | | | | | | | № хоста | | | | | | | | | | | | | | | | | | | | | | | | 0 - 127 | 128 сетей по 16,777,216 адресов |
| **B** | 1 | 0 | № сети | | | | | | | | | | | | | | № хоста | | | | | | | | | | | | | | | | 128 - 191 | 16,384 сетей по 65,536 адресов |
| **C** | 1 | 1 | 0 | № сети | | | | | | | | | | | | | | | | | | | | | № хоста | | | | | | | | 192-223 | 2,097,152 сетей по 256 адресов |
| **D** | 1 | 1 | 1 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 224-239 | Multicast |
| **E** | 1 | 1 | 1 | 1 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | 240-247 | резерв |

Рис. 86. Классы IP-адресов

*Класс A* определяет самые крупные сети, 2, 3 и 4 байт IP-адреса этого класса содержат адрес хоста в сети (максимальное количество адресов в такой сети равно $2^{24} \approx 16{,}8$ млн). Сети класса A принадлежат региональным интернет-провайдерам, крупным компаниям и организациям (в основном американским, что связано с историей развития Интернета, именно их распределение указано в ipv4-address-space.xml по приведенному выше адресу). Признаком IP-адреса класса A является равный нулю старший бит старшего байта адреса, семь младших бит определяют адрес сети. Таким образом, десятичное значение старшего байта IP-адреса класса A лежит в диапазоне от `0` до `127` (максимальное количество сетей класса A равно 128).

*Класс B* определяет средние по масштабу сети, 3 и 4 байт IP-адреса этого класса содержат адрес хоста в сети (максимальное количество адресов в такой сети равно $2^{16} \approx 65{,}6$ тыс.). Сети класса B принадлежат в основном локальным интернет-провайдерам (провайдерам услуг Интернета) и крупным компаниям и организациям. Признаком IP-адреса класса B являются биты `10` в старших разрядах старшего байта адреса, шесть младших бит старшего байта (первого) и все биты второго байта определяют адрес сети. Таким образом, десятичное значение старшего байта IP-адреса класса B лежит в диапазоне от `128` до `191` (максимальное количество сетей класса B равно $2^{14} \approx 16{,}4$ тыс.).

*Класс C* определяет сети минимального масштаба, только 4 байт (младший) IP-адреса этого класса содержит адрес хоста в сети (максимальное количество адресов в такой сети равно $2^{8} \approx 256$ адресов). Сети класса C принадлежат в основном провайдерам услуг Интернета, различным компаниям и организациям. Признаком IP-адреса класса C являются биты `110` в старших разрядах старшего байта адреса, пять младших бит старшего байта (первого), все биты второго байта и все биты третьего байта определяют адрес сети. Таким образом, десятичное значение старшего байта IP-адреса

класса C лежит в диапазоне от `192` до `223` (максимальное количество сетей класса C равно $2^{22} \approx 2{,}1$ млн).

Существует возможность выяснить, кто является владельцем сети, в которую входит произвольный IP-адрес, а также координаты администратора этой сети, выполнив запрос к базе данных регионального или локального регистратора. Для европейских адресов это можно сделать на сайте RIPE NCC http://www.db.ripe.net/whois (рис. 87).

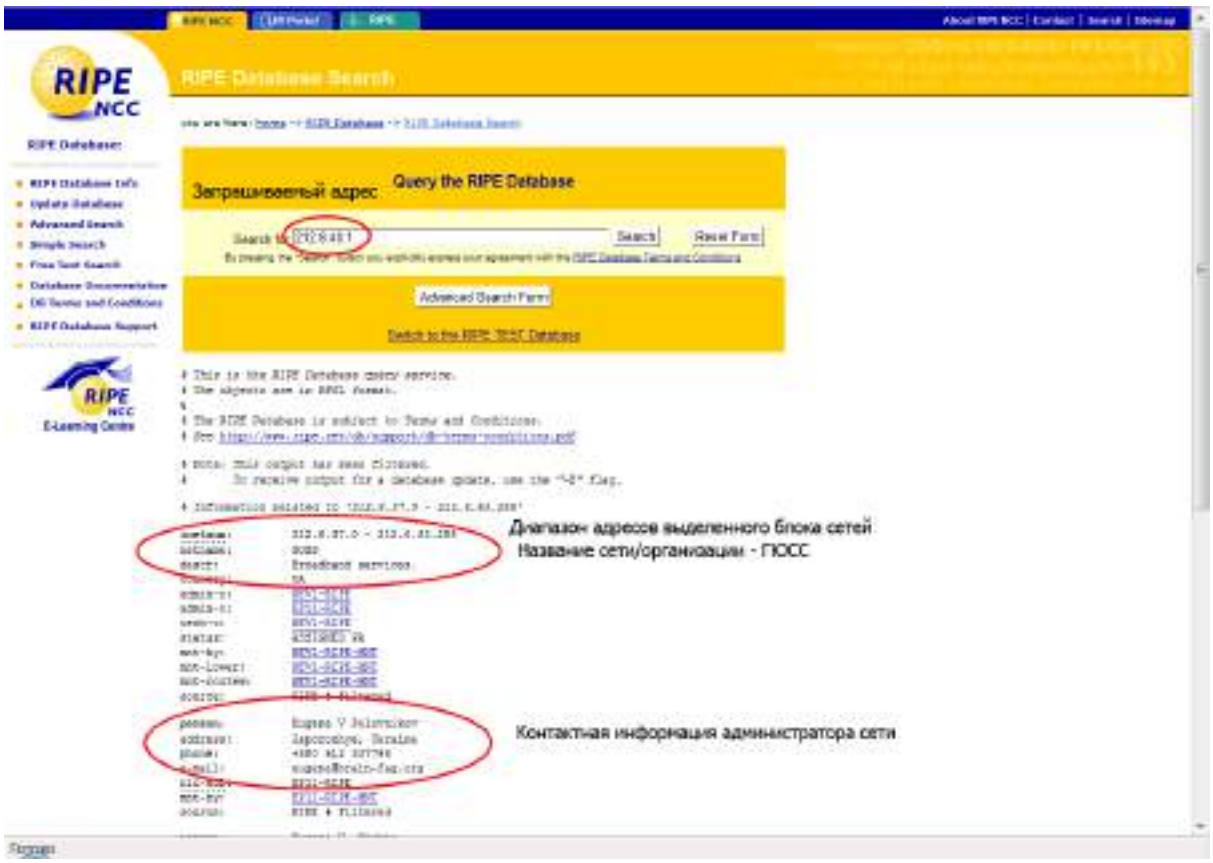



Рис. 87. Пример поиска информации о блоке IP-сетей, в который входит запрашиваемый IP-адрес

*Класс D* служит для обозначения групп IP-адресов, представляющих собой так называемые *мультикастовые группы* (*Multicast Group*), использующиеся технологией рассылки одного и того же потока дейтаграмм нескольким получателям одновременно. При этом вплоть до шлюза сети получателя этот поток не дублируется, а в качестве IP-адреса получателя в дейтаграммах указывается адрес мультикастовой группы. Признаком IP-адреса класса D являются биты `1110` в старших разрядах старшего байта адреса, четыре младших бит старшего байта (первого) и все биты второго, третьего и четвёртого байтов определяют адрес мультикастовой группы. Таким образом, десятичное значение старшего байта IP-адреса класса D лежит в диапазоне от `224` до `239` (максимальное количество мультикастовых групп равно $2^{28} \approx 268$ млн).

*Класс E* характеризуется адресом, старшие биты старшего байта которого равны `11110`, десятичное значение старшего байта IP-адреса класса E

лежит в диапазоне от 240 до 247, адреса этого класса зарезервированы для будущих применений.

Оставшиеся адреса с десятичным значением старшего байта от 248 до 255 также зарезервированы.

В адресном пространстве IP v4 также зарезервированы следующие адреса под специальные нужды:

- 0.0.0.0 – адрес хоста, сгенерировавшего пакет (используется только в некоторых сообщениях протокола управляющих сообщений Интернета – ICMP);
- 255.255.255.255 - пакет с таким IP-адресом получателя рассылается всем хостам, находящимся в той же сети, что и отправитель этого пакета – *ограниченное широковещательное сообщение* (*Limited Broadcast*);
- в поле номера сети IP-адреса получателя все биты равны нулю – хост-получатель принадлежит той же сети, что и хост-отправитель (например, 0.0.0.X, X=1-224);
- в поле номера хоста IP-адреса получателя все биты равны нулю – такой адрес является адресом сети с заданным в поле номера сети адресом (например, X.X.X.0, X=1-224);
- в поле номера хоста IP-адреса получателя все биты равны единице – пакет рассылается всем хостам сети с заданным в поле номера сети адресом – широковещательное сообщение (например, X.X.X.255, X=1-224);
- старший байт IP-адреса = 127 – *кольцевой адрес* (*Loopback Address*) – петля (обычно используется адрес 127.0.0.1) – используется для тестирования программ и взаимодействия процессов в пределах одного хоста;
- блоки адресов, зарезервированные для локальных сетей (без выхода в Интернет или использующих сетевую трансляцию адресов) – одна сеть класса A 10.0.0.0-10.255.255.255, 16 сетей класса B 172.16.0.0-172.31.255.255, 256 сетей класса C 192.168.0.0-192.168.255.255.

Любой маршрутизатор, работающий в Интернет, не будет передавать пакеты с адресами из диапазонов адресов для локальных сетей. В то же время такие адреса удобны, поскольку они могут присваиваться хостам локальных сетей их администраторами без согласования с провайдерами услуг Интернет. Для выхода в Интернет с этих адресов используется технология *сетевой трансляции адресов* (*Network Address Translation* – NAT), подменяющая локальный IP-адрес отправителя на разрешённый для передачи в Интернет адрес, полученный от провайдера. Таким образом, достигается существенная экономия адресов (и средств, оплачиваемых провайдерам за их аренду), однако все хосты с локальными адресами в Интернете видны как один хост с разрешённым для работы в Интернете адресом, что не позволяет размещать на внутренних хостах общедоступные для пользо-

вателей Интернета сервисы. Последнее обстоятельство одновременно является преимуществом с точки зрения безопасности: внутренние хосты с локальными адресами не видны из Интернета.

Недостатком выделения IP-адресов по классовой схеме является невозможность экономного выделения групп IP-адресов. Действительно, если в небольшой компании всего несколько компьютеров (например, 6), то она вынуждена арендовать сеть класса C как сеть минимально возможного масштаба. Однако при этом, даже, если компания увеличит парк компьютеров вдвое, более 240 адресов (с учётом зарезервированных под специальные нужды) останутся неиспользованными. Поэтому в настоящее время классовая схема адресации вытеснена бесклассовой схемой, согласно которой выделение блоков IP-адресов (так называемых *IP-подсетей* (*IP-subnetwork*)) основано на использовании *маски подсети* (*Subnet Mask*).

Маска подсети – это двоичное число с количеством разрядов, равным количеству разрядов IP-адреса, используемое вместе с IP-адресом. Маска содержит единицы в тех разрядах IP-адреса, которые должны интерпретироваться как номер подсети. Поскольку номер подсети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность битов в старшей части адреса. Непрерывная последовательность нулей в младшей части адреса определяет количество битов, используемых для нумерации хостов в подсети. Таким образом, количество адресов в IP-подсети $N=2^m$, где $m$ – количество нулевых битов в маске подсети (заметим, что речь идёт именно об IP-адресах, включающих и специальные адреса, а не только об адресах хостов).

Снабжая адрес маской, можно отказаться от понятия классов адресов для возможности более гибкого распределения адресов, например, разбиения полученной организацией сети класса C на подсети подразделений нужного размера с целью обеспечения локализации трафика подразделений и реализации внутрикорпоративной политики безопасности. При этом для внешних хостов и маршрутизаторов сеть организации по-прежнему выглядит как сеть класса C и отсутствует необходимость добавления маршрутов к подсетям на внешних маршрутизаторах (технология маршрутизации будет описана далее).

На рис. 88 приведены возможные маски подсети для сети класса C и количество доступных адресов в подсети для каждой из них. Количество адресов для нумерации хостов на два меньше, поскольку первый адрес – это адрес самой подсети, а последний адрес – широковещательный адрес этой подсети. Кроме того, один из доступных адресов хостов (часто первый или последний) обычно назначают интерфейсу маршрутизатора-шлюза, соединяющего данную подсеть с другими сетями.

С использованием технологии создания подсетей для небольшой компании с 6 компьютерами вместо 256 адресов сети класса C с помощью маски подсети `255.255.255.240` могут быть выделены 16 адресов, из которых для нумерации хостов и шлюза останутся 14. Отметим, что исполь-

зование 255.255.255.248 маски обеспечит только 6 адресов, которых хватит на нумерацию хостов, но IP-адреса для шлюза этой сети уже не хватит.

| Маска (дес) | Маска (двоичн) | Хостов | Подсетей | Примечание |
|---|---|---|---|---|
| 255.255.255.255 | 11111111.11111111.11111111.11111111 | все | нет | |
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | 16777214 | 126 | Класс A |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | 16382 | | Класс B |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | 254 | | Класс C |
| **Деление на подсети с количеством хостов менее 254** | | | | |
| 255.255.255.254 | 11111111.11111111.11111111.11111110 | 0 2 (адреса) | 128 | не имеют смысла |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | 2 (4 адреса) | 64 | |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | 6 (8 адреса) | 32 | |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | 14 (16 адр.) | 16 | |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | 30 (32 адр.) | 8 | |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | 62 (64 адр.) | 4 | |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | 126 (128 адр.) | 2 | |

Рис. 88. Маскирование IP-адресов

На рис. 89 приведен пример планирования подсетей для четырёх подразделений организации, в которых находится 77, 50, 29 и 15 компьютеров, соответственно.

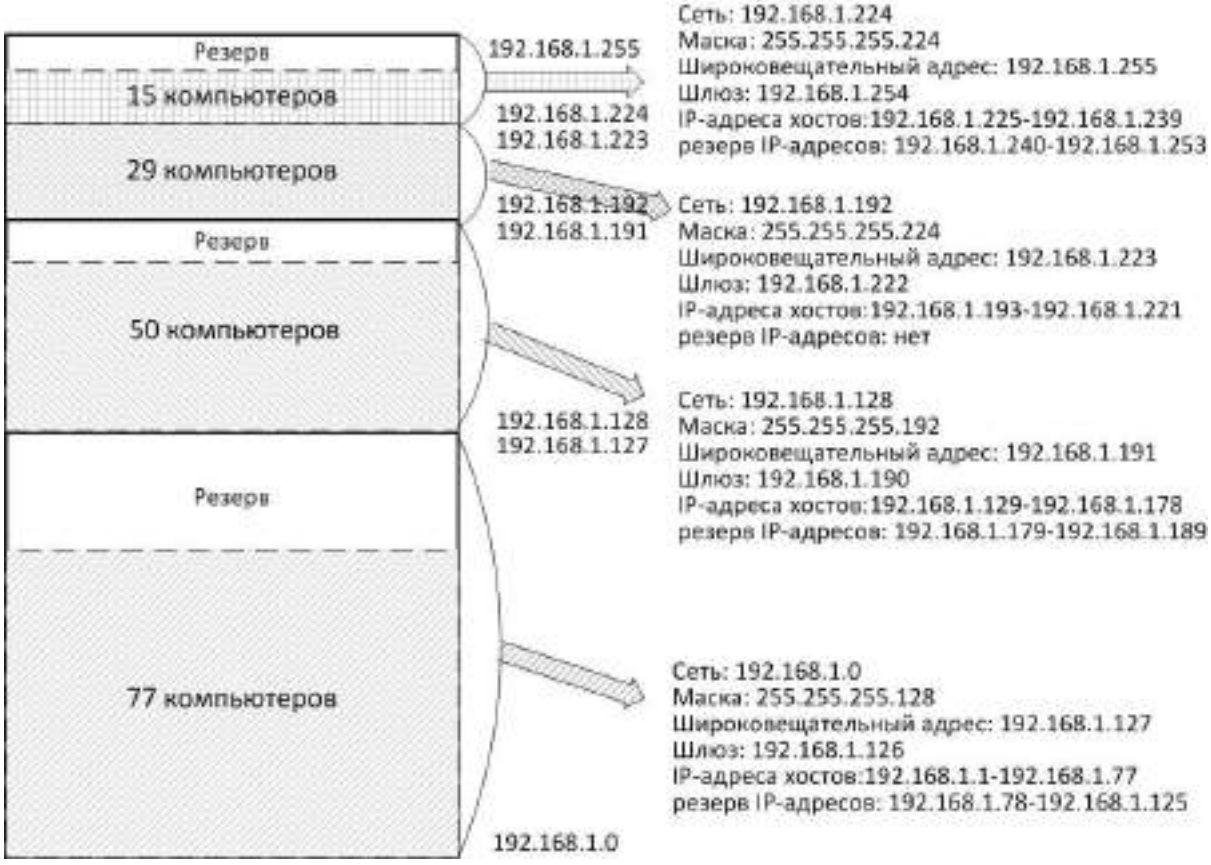



Рис. 89. Пример планирования IP-адресов для четырёх подсетей

Для каждой подсети приведены её адрес, маска подсети, широковещательный адрес, адрес, зарезервированный для шлюза, диапазон адресов хостов и диапазон резервных адресов (для будущих подключений). Этот пример иллюстрирует гибкость выделения адресов с помощью масок подсети в пределах одной сети класса C.

Механизм масок широко используется в технологии IP-маршрутизации. При получении маршрутизатором IP пакета из IP-адреса получателя определяется адрес подсети назначения путём логического умножения (операция AND) IP-адреса получателя на маску подсети, например:

```
    192.168.3.5 AND 255.255.255.240 =

    11000000 10101000 00000011 00000101
AND 11111111 11111111 11111111 11110000
  = 11000000 10101000 00000011 00000000 = 192.168.3.0.
```

Полученный номер подсети используется для нахождения маршрута (то есть адреса следующего маршрутизатора по пути к хосту-получателю) с помощью таблицы маршрутизации маршрутизатора (технология маршрутизации будет описана далее).

Следует отметить, что при планировании подсетей адресное пространство каждой следующей смежной подсети не может быть больше адресного пространства предыдущей. Пример неправильного планирования подсетей приведен на рис. 90: вначале выделены адреса для подсети с меньшим числом компьютеров (подсеть из 8 адресов 192.168.1.0-192.168.1.7, маска 255.255.255.**248**), а затем – для смежной с ней большей подсети (подсеть из 16 адресов 192.168.1.8-192.168.1.23, маска 255.255.255.**240**).

| Net→ | 192 | 168 | 1 | 0 | Broad Cast→ | 192 | 168 | 1 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| Net→ | 11000000 | 10101000 | 00000001 | 00000000 | Broad Cast→ | 11000000 | 10101000 | 00000001 | 00000111 |
| Mask→ | 11111111 | 11111111 | 11111111 | 11111000 | 248 | 11111111 | 11111111 | 11111111 | 11111000 |
| IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00000000 | IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00000000 |
| IP ⊗ MASK | 192 | 168 | 1 | 0 | IP ⊗ MASK | 192 | 168 | 1 | 0 |
| Net→ | 192 | 168 | 1 | 8 | Broad Cast→ | 192 | 168 | 1 | 23 |
| Net→ | 11000000 | 10101000 | 00000001 | 00001000 | Broad Cast→ | 11000000 | 10101000 | 00000001 | 00010111 |
| Mask→ | 11111111 | 11111111 | 11111111 | 11110000 | 240 | 11111111 | 11111111 | 11111111 | 11110000 |
| IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00000000 | IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00010000 |
| IP ⊗ MASK | 192 | 168 | 1 | 0 | IP ⊗ MASK | 192 | 168 | 1 | 16 |

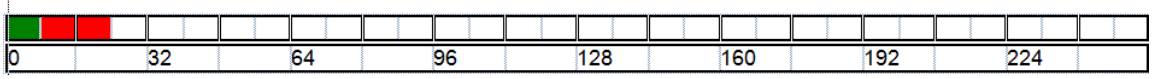



Рис. 90. Пример неправильного планирования IP-адресного пространства с помощью масок

При логическом умножении IP-адресов из диапазона `192.168.1.9-192.168.1.15` большей подсети на маску этой подсети получается то же значение IP-адреса подсети (`192.168.1.0`), что и для первой меньшей подсети (`192.168.1.0`). А при логическом умножении IP-адресов из диапазона `192.168.1.16-192.168.1.23` большей подсети на маску этой подсети получается значение IP-адреса несуществующей подсети (`192.168.1.16`). Такое планирование приведёт к неправильной маршрутизации пакетов, при которой пакеты, предназначенные первой половине компьютеров второй подсети, будут маршрутизироваться в первую подсеть (`192.168.1.0`), а пакеты, предназначенные второй половине компьютеров второй подсети, будут маршрутизироваться в несуществующую подсеть (с адресом `192.168.1.16`) – фактически они будут направляться компьютеру с таким адресом.

Для правильного планирования подсетей в приведенном примере (рис. 91) необходимо выделение 16-адресной подсети спланировать на границе 16-адресного блока, например, выделить ей блок `192.168.1.16-192.168.1.31`.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Net→ | 192 | 168 | 1 | 0 | Broad Cast→ | 192 | 168 | 1 | 7 |
| Net→ | 11000000 | 10101000 | 00000001 | 00000000 | Broad Cast→ | 11000000 | 10101000 | 00000001 | 00000111 |
| Mask→ | 11111111 | 11111111 | 11111111 | 11111000 | 248 | 11111111 | 11111111 | 11111111 | 11111000 |
| IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00000000 | IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00000000 |
| IP ⊗ MASK | 192 | 168 | 1 | 0 | IP ⊗ MASK | 192 | 168 | 1 | 0 |
| Net→ | 192 | 168 | 1 | 8 | Broad Cast→ | 192 | 168 | 1 | 15 |
| Net→ | 11000000 | 10101000 | 00000001 | 00001000 | Broad Cast→ | 11000000 | 10101000 | 00000001 | 00001111 |
| Mask→ | 11111111 | 11111111 | 11111111 | 11111000 | 248 | 11111111 | 11111111 | 11111111 | 11111000 |
| IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00000000 | IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00001000 |
| IP ⊗ MASK | 192 | 168 | 1 | 8 | IP ⊗ MASK | 192 | 168 | 1 | 8 |
| Net→ | 192 | 168 | 1 | 16 | Broad Cast→ | 192 | 168 | 1 | 31 |
| | 11000000 | 10101000 | 00000001 | 00010000 | Broad Cast→ | 11000000 | 10101000 | 00000001 | 00011111 |
| Mask→ | 11111111 | 11111111 | 11111111 | 11110000 | 240 | 11111111 | 11111111 | 11111111 | 11110000 |
| IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00010000 | IP ⊗ MASK | 11000000 | 10101000 | 00000001 | 00010000 |
| IP ⊗ MASK | 192 | 168 | 1 | 16 | IP ⊗ MASK | 192 | 168 | 1 | 16 |

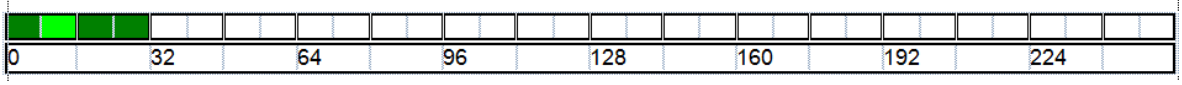



Рис. 91. Пример правильного планирования IP адресного пространства с помощью масок

Оставшийся незанятым блок адресов 192.168.1.8-192.168.1.15 можно выделить третьей подсети с таким количеством хостов или оставить пустым. Результат умножения любого из адресов подсети на маску приводит к получению для всех адресов всех подсетей IP-адреса данной подсети. Маршрутизация будет работать правильно. Фактически, при планировании подсетей количеством адресов предыдущей подсети задаются границы следующей смежной подсети, которые не должны пересекаться адресным полем следующей подсети. Для того, чтобы избежать ошибочного планирования, рекомендуется в начале адресного пространства размещать более крупные подсети, а затем более мелкие по мере уменьшения необходимого им количества адресов.

Следует отметить, что механизм масок в настоящее время используется не только для разбиения классовых сетей на подсети, но и для выделения сетей произвольного размера с помощью маски с любым необходимым количеством нулевых битов, определяющих размер сети, в любом месте адресного пространства. Такая технология получила название *бесклассовой междоменной маршрутизации* (*Classless InterDomain Routing – CIDR*), она позволяет гибко распределять адресное пространство и упрощать маршрутизацию. Технология CIDR предлагает описывать маску подсети добавленным к адресу сети суффиксом, в котором указано количество единичных битов маски. Например, запись 192.168.0.0/22 – определяет так называемую *суперсеть* с маской 11111111.11111111.11111100.00000000 = 255.255.252.0 с диапазоном адресов 192.168.3.0 - 192.168.3.255, эквивалентную четырём смежным сетям класса С. Такая сеть может быть выделена на бесклассовой основе организации, которой необходимо до 1024 адресов (вместо выделения сети класса В с 65536 адресами с использованием классов).

## 4.2. Маршрутизация IP-дейтаграмм

Важнейшей задачей сетевого уровня является *маршрутизация* (*Routing*) дейтаграмм в составной сети, суть которой, как уже отмечалось, сводится к поиску маршрутизаторами оптимального пути (маршрута) к получателю дейтаграммы. Маршрутизация выполняется сетевыми устройствами, называемыми *маршрутизаторы* (*Router*). Любой маршрутизатор обладает более чем одним сетевым интерфейсом, к которым подключены сети/подсети, которые он соединяет (функции маршрутизатора могут выполнять и компьютеры, оснащённые двумя и более сетевыми интерфейсами). Например, маршрутизатор R1 на рис. 92 связывает сети N1, N2 и N7, имеющие маски подсети M1, M2 и M7, соответственно, через свои интерфейсы R1(1), R1(2) и R1(3). Следует отметить, что даже если в сети отсутствуют пользовательские хосты, она все равно считается сетью/подсетью, имеет свой адрес и обладает другими свойствами, характерными для сетей/подсетей (такими сетями/подсетями являются сети с адресами N7, N8 и

N9 *связей "точка – точка"* (*Point-to-Point*) между маршрутизаторами на рис. 92).

Под *маршрутом* (*Route*) понимается последовательность маршрутизаторов, которые должна пройти дейтаграмма от хоста-отправителя до хоста-получателя. Выбор следующего шага маршрута выполняется каждым маршрутизатором и конечными хостами на основании имеющейся у них информации об адресах сетей/подсетей и некоторого критерия выбора маршрута, записанных в так называемой *таблице маршрутизации* (*Routing Table*).

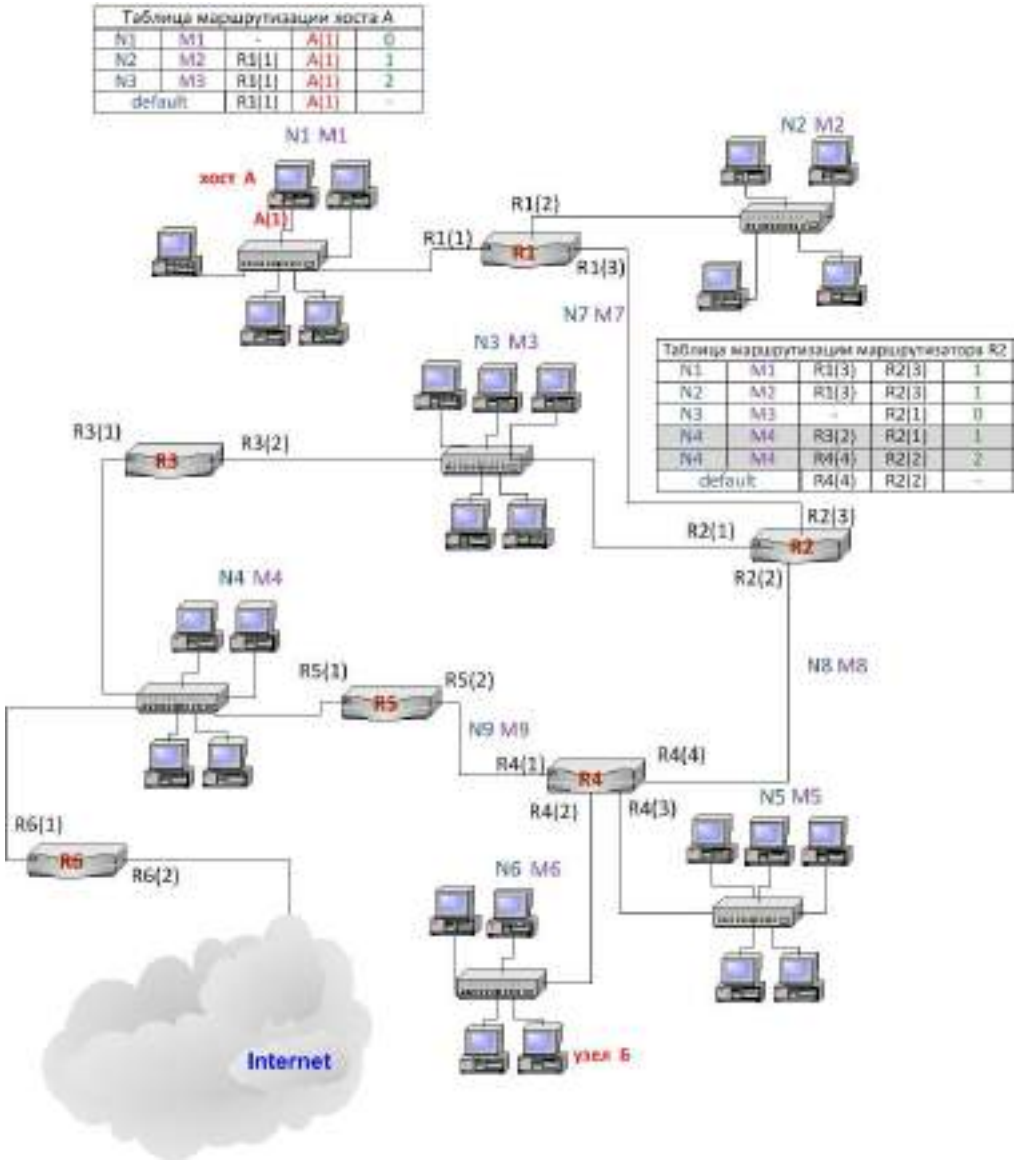



Рис. 92. Маршрутизация в составной сети

Критериями могут быть: количество маршрутизаторов на маршруте (hops), время прохождения тестового пакета до следующего по пути маршрутизатора, пропускная способность линии связи к следующему маршрутизатору и другие. Для каждой записи в первом столбце таблицы маршрутизации (рис. 92) указывается адрес сети/подсети/хоста назначения дейтаграммы, во втором – маска подсети назначения, в третьем – сетевой адрес

следующего по маршруту маршрутизатора, на который необходимо направить дейтаграмму, чтобы она продвигалась по рациональному маршруту к получателю. В четвёртом столбце указывается сетевой адрес порта текущего маршрутизатора, через который должна уйти по выбранному маршруту дейтаграмма. В пятом столбце указывается *метрика маршрута* – один из приведенных выше критериев выбора маршрута (в таблицах маршрутизации на рис. 92 в качестве метрики приведено *количество промежуточных маршрутизаторов на маршруте – hops*). Метрика маршрута указывается для выбора оптимального маршрута при наличии в таблице маршрутизации нескольких строк с маршрутами к одной и той же сети (например, маршруты к сети N4 в таблице маршрутизации маршрутизатора R2 на рис. 92). Количество записей в таблице маршрутизации может быть достаточно большим даже для относительно небольшой составной сети вследствие наличия альтернативных маршрутов, кроме того, в больших составных сетях (примером такой сети является Интернет) адреса удалённых сетей/подсетей просто неизвестны. Поэтому обычно в последней строке таблиц маршрутизации указывается так называемый *маршрут по умолчанию* (*default route*), по которому будет направлена дейтаграмма в случае неудачного поиска адреса сети назначения дейтаграммы в первом столбце таблицы маршрутизации. Для хостов в маршруте по умолчанию в качестве следующего маршрутизатора по маршруту обычно указывается адрес шлюза локальной сети (как для хоста A на рис. 92), а для маршрутизаторов – адрес маршрутизатора, следующего по маршруту, который используется большей частью исходящих дейтаграмм (как для маршрутизатора R2 на рис. 92). Достаточно часто маршрут по умолчанию граничного маршрутизатора организации указывает на маршрутизатор провайдера Интернета для этой организации, маршрутизатор этого провайдера Интернета в качестве маршрута по умолчанию может использовать маршрут к маршрутизатору интернет-провайдера более высокого уровня и т.д.

Записи в таблицу маршрутизации заносятся либо вручную, в этом случае маршрутизация называется *статической* (статическая маршрутизация обычно используется в относительно небольших составных сетях), или записи заносятся в результате работы протоколов *динамической маршрутизации*, задача которых – изучение топологии и адресной информации сетей/подсетей, формирующих составную сеть, и обмен записями маршрутных таблиц между маршрутизаторами составной сети. Популярными в настоящее время протоколами динамической маршрутизации являются *протокол маршрутной информации* (*Routing Information Protocol – RIP*), *протокол кратчайшего пути* (*Open Shortest Path First – OSPF*) и *протокол граничного шлюза* (*Border Gateway Protocol – BGP*).

Маршрутизаторы определяют следующий от них шаг маршрута дейтаграммы по следующему алгоритму:

- из заголовка дейтаграммы извлекается сетевой адрес получателя и выполняется поиск его значения в первом столбце таблицы марш-

рутизации, если адрес найден, дейтаграмма направляется по адресу следующего на пути маршрутизатора, указанный в третьем столбце строки с найденным адресом;
- если адрес получателя в первом столбце не найден, из адреса получателя восстанавливается адрес сети получателя путём умножения адреса получателя на маску подсети назначения во втором столбце первой строки;
- после получения адреса сети выполняется его сравнение с адресом сети/подсети назначения в первом столбце первой строки;
- если адреса совпадают, в качестве следующего адреса маршрута выбирается адрес из третьего столбца первой строки;
- если адреса не совпадают, адрес получателя умножается на маску подсети из второй строки и полученный адрес сети/подсети сравнивается с адресом сети назначения в первом столбце второй строки и если совпадение адресов получено, дейтаграмма передаётся по адресу маршрутизатора, указанному в третьем столбце второй строки;
- если адреса не совпадают, алгоритм вычисления сети/подсети и сравнения повторяются для остальных строк таблицы, пока не будет найдено совпадение;
- в последней строке таблицы указывается маршрут по умолчанию, для него в первом и втором столбце заносятся адреса `0.0.0.0` и `0.0.0.0`. Умножение любого IP-адреса на маску `0.0.0.0` приведёт к получению адреса сети `0.0.0.0`, поэтому совпадение будет достигнуто для любого адреса, для которого не получено совпадение в предыдущих строках таблицы маршрутизации и дейтаграмма будет направлена маршрутизатору, адрес которого указан в третьем столбце строки с маршрутом по умолчанию.

На рис. 93 приведен пример, иллюстрирующий обработку таблицы маршрутизации при поиске маршрута для дейтаграммы с адресом назначения `192.168.3.25` (`11000000 10101000 00000011 00011001`). Отметим, что сравнение адресов выполняется побитово с помощью логической операции `XOR`, а её нулевой результат свидетельствует о совпадении сравниваемых адресов. Совпадение вычисленного адреса сети назначения и адреса сети в первом столбце таблицы маршрутизации достигнуто в третьей строке, поэтому следующим маршрутизатором по пути будет выбран `192.168.2.2`, а маршрут по умолчанию проверяться не будет. Однако, если бы он проверялся, то совпадение было бы получено для любых проверяемых адресов-хоста получателя.

| Сеть назначения | Маска подсети назначения | Следующий маршрутизатор | Исходящий интерфейс | Метрика |
|---|---|---|---|---|
| 192.168.1.0 | 255.255.255.0 | 192.168.5.1 | 192.168.4.1 | 2 |
| 192.168.3.0 | 255.255.255.240 | 192.168.2.1 | 192.168.4.2 | 1 |
| 192.168.3.16 | 255.255.255.240 | 192.168.2.2 | 192.168.4.3 | 1 |
| 0.0.0.0 | 0.0.0.0 | 192.168.5.2 | 192.168.4.1 | - |

обработка 1-й строки

```
    11000000 10101000 00000011 00011001 = 192.168.3.25
AND 11111111 11111111 11111111 00000000 = 255.255.255.0
    11000000 10101000 00000011 00000000 = 192.168.3.0
XOR 11000000 10101000 00000001 00000000 = 192.168.1.0
    00000000 00000000 00000010 00000000 ≠ 0
```

обработка 2-й строки

```
    11000000 10101000 00000011 00011001 = 192.168.3.25
AND 11111111 11111111 11111111 11110000 = 255.255.255.240
    11000000 10101000 00000011 00010000 = 192.168.3.16
XOR 11000000 10101000 00000011 00000000 = 192.168.3.0
    00000000 00000000 00000000 00010000 ≠ 0
```

обработка 3-й строки

```
    11000000 10101000 00000011 00011001 = 192.168.3.25
AND 11111111 11111111 11111111 11110000 = 255.255.255.240
    11000000 10101000 00000011 00010000 = 192.168.3.16
XOR 11000000 10101000 00000011 00010000 = 192.168.3.16
    00000000 00000000 00000000 00000000 = 0
```

Рис. 93. Пример обработки записей таблицы маршрутизации для адреса 192.168.3.25

Следует отметить, что отправка дейтаграммы следующему по пути маршрутизатору, адрес которого найден в таблице маршрутизации, не означает замены адреса получателя в заголовке дейтаграммы. Такая замена сделала бы невозможным поиск дальнейших шагов маршрута. Полученный из третьего столбца таблицы маршрутизации адрес используется для определения адреса канального уровня этого порта (например, MAC адреса Ethernet) с помощью ARP-запроса. Заменяются только MAC-адрес отправителя (на MAC-адрес исходящего интерфейса маршрутизатора) и MAC-адрес получателя (на MAC-адрес, полученный с помощью ARP). Таким образом, IP-адреса отправителя и получателя не изменяются на всём протяжении маршрута, который проходит дейтаграмма, в то время как MAC-адреса (или другие адреса канального уровня) изменяются в каждой локальной сети, которую пересекает дейтаграмма.

В примере на рис. 94 IP-адреса отправителя (IP1) и получателя (IP2) не меняются на всём маршруте дейтаграммы, в то время как MAC-адреса меняются в каждой сети. IP-адреса маршрутизаторов используются только для ARP-запросов.

Задачу маршрутизации также решают пользовательские хосты. Так, если номер сети назначения совпадает с сетью, к которой принадлежит сам компьютер, то задачу маршрутизации решать не требуется и пакет просто передаётся канальному уровню вместе с определённым по протоколу ARP адресом канального уровня получателя. Если не совпадает, то необходима маршрутизация и узел-отправитель просматривает свою таблицу маршрутизации.

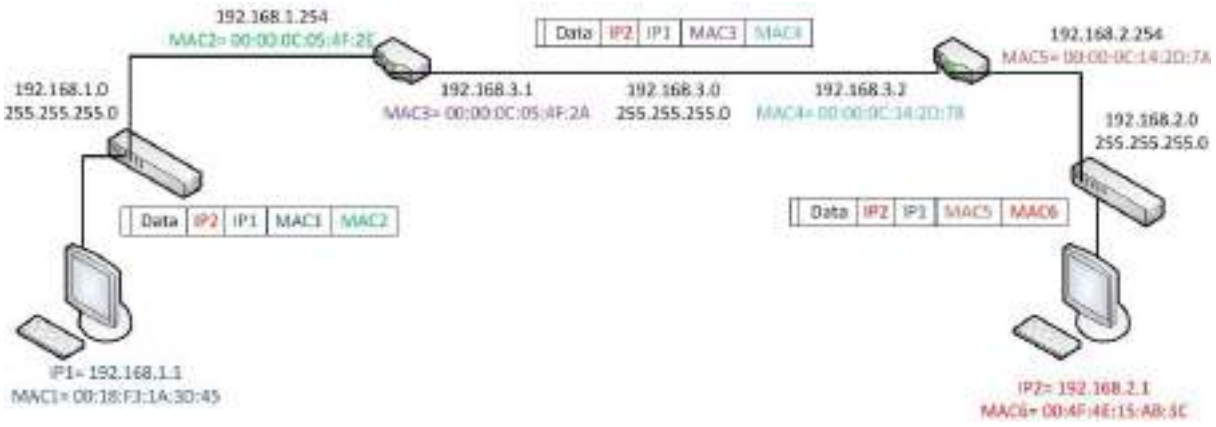



Рис. 94. Изменение адресов канального уровня при передаче дейтаграммы в составной сети

Команда `route print` в Windows выводит эту таблицу на экран, а также позволяет задавать и удалять маршруты (рис. 95). Хосты в большей степени, чем маршрутизаторы пользуются маршрутом по умолчанию, обычно в качестве следующего по маршруту маршрутизатора для маршрута по умолчанию указывается шлюз локальной сети хоста (с IP-адресом 192.168.1.129 для примера на рис. 95).

```
C:\WINNT\system32>route print
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 d0 b7 69 21 71 ...... Intel(R) PRO Adapter
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес             Маска сети         Адрес шлюза        Интерфейс   Метрика
          0.0.0.0           0.0.0.0   192.168.1.129   192.168.1.130       1
        127.0.0.0         255.0.0.0         127.0.0.1       127.0.0.1       1
    192.168.1.128 255.255.255.128   192.168.1.130   192.168.1.130       1
    192.168.1.130 255.255.255.255         127.0.0.1       127.0.0.1       1
    192.168.1.255 255.255.255.255   192.168.1.130   192.168.1.130       1
        224.0.0.0         224.0.0.0   192.168.1.130   192.168.1.130       1
  255.255.255.255 255.255.255.255   192.168.1.130   192.168.1.130       1
Основной шлюз:        192.168.1.129
===========================================================================

C:\WINNT\system32> route ADD 192.168.1.16 MASK 255.255.255.240  192.168.1.1
```

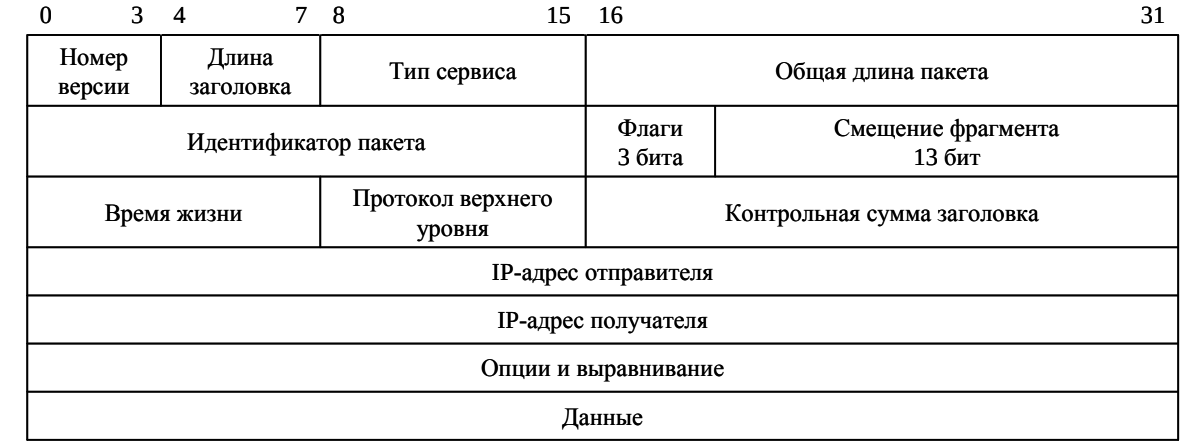
Рис. 95. Пример таблицы маршрутизации хоста и команда добавления маршрута

Следует отметить, что в таблицу маршрутизации автоматически заносится адрес сети `127.0.0.0`. Если в поле IP-адрес получателя находится адрес этой сети, то передачи пакета на канальный уровень (и, следовательно, в сеть) не происходит, а этот пакет возвращается отправителю (путём обмена адресов отправителя и получателя в соответствующих полях пакета). Аналогично может вноситься запись для сетевых адресов собственных портов маршрутизатора для них адресом следующего маршрутизатора и

выходного интерфейса указывается адрес `127.0.0.1` – loopback. Также в таблицу автоматически заносятся записи для сети с адресом `224.0.0.0` – они требуются для обработки групповых адресов (multicast address). Кроме того, в таблицу могут быть занесены адреса, предназначенные для обработки широковещательных рассылок в сетях, подсоединённых к портам маршрутизатора, – это адреса, заканчивающиеся на последовательность единиц (`255`). Одни указывают маршрут для отправки широковещательных сообщений в составной сети для определённых подсетей – сетевой адрес подключённого к этим сетям порта маршрутизатора, адрес `255.255.255.255` – адрес ограниченной широковещательной рассылки – пакет с таким адресом рассылается всем узлам, находящимся в той же подсети, что и отправитель.

## 4.3. Формат заголовка IP-пакета

IP-дейтаграмма состоит из заголовка (часто 20 байт) и поля данных, максимальная длина пакета – заголовок + данные составляет 65535 байт, минимальная – определяется минимальным размером переносящего IP-пакет кадра канального уровня (для Ethernet 64 байта). Структура IP-пакета приведена на рис. 96.




**Поле "Тип сервиса"**

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Приоритет | | | Задержка | Пропускная способность | Надежность доставки | Резерв (0) | |

**Поле "Флаги"**

| 0 | 1 | 2 |
|---|---|---|
| Резерв (0) | Do not Fragment | More Fragments |

**Поле "Протокол верхнего уровня"**

| Значение поля | 0= $00_н$ | 1= $01_н$ | 2= $02_н$ | 4= $04_н$ | 6= $06_н$ | 8= $08_н$ | 17= $11_н$ | 88= $58_н$ | 89= $59_н$ |
|---|---|---|---|---|---|---|---|---|---|
| Протокол | Резерв | ICMP | IGMP | IP | TCP | EGP | UDP | IGRP | OSPF |

Рис. 96. Структура IP-пакета

Поле *Номер версии* (*Version*) указывает версию протокола IP. Напомним, что в настоящее время широко используется 4 версия (IPv4) и начинается переход на 6 версию (IPv6) (формат заголовка IPv6 отличается от рассматриваемого заголовка IPv4).

Поле *Длина заголовка* (*Header Length*) указывает значение длины заголовка IP-пакета в 32-битных (четырёхбайтовых) словах. Обычно длина заголовка составляет 5 таких слов (20 байт), но может быть больше за счёт дополнительных байт в поле Опции (максимальная длина заголовка 60 байт = 15 четырёхбайтовых слов).

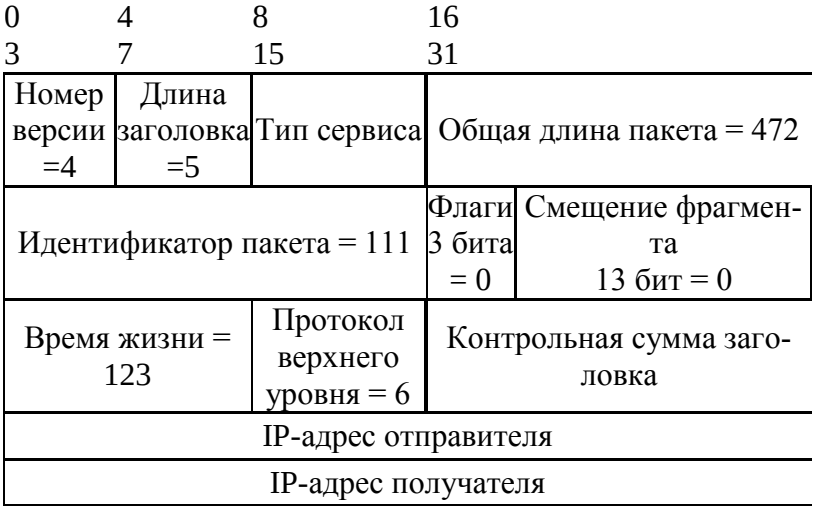
Младшие три бита поля *Тип сервиса* (*Type of Service*) (биты 0-2) задают приоритет пакета от самого низкого `000` (нормальный пакет) до самого высокого `111` (пакет с управляющей информацией). Биты 3-5 определяют критерий выбора маршрута, используемый в протоколах маршрутизации *OSPF* и *BGP*. Выбор осуществляется между тремя альтернативами: малой задержкой передачи дейтаграмм (бит 3 *Delay*= `1`), высокой пропускной способностью линии связи (бит 4 *Throughput*= `1`) и высокой надёжностью передачи дейтаграмм (бит 5 *Reliability*= `1`). Обычно улучшение одного параметра вызывает ухудшение другого, следовательно, выбирается один критерий выбора маршрута. Хосты обычно не используют возможность определения типа сервиса отправляемой дейтаграммы и указывают значение этого поля $00_{\text{H}}$.

Поле *Общая длина* (*Total Length*) содержит общую длину IP-пакета вместе с заголовком. Исходя из разрядности поля (2 байта), максимальная длина пакета составляет 65535 байт. Однако в большинстве случаев такие большие пакеты не используются, а размер пакета выбирается с учётом максимального поля данных несущего этот пакет кадра канального уровня (MTU). Для Ethernet MTU ≈ 1500 байт, для FDDI MTU ≈ 4096 байт.

При перенаправлении IP-пакета из одной сети в другую маршрутизатор может столкнуться с проблемой различных значений MTU в соседних сетях. В этом случае ему необходимо выполнить фрагментацию дейтаграммы (т.е. разбиение её на несколько самостоятельных дейтаграмм) при передаче в сеть с меньшим значением MTU и дефрагментацию (то есть объединение нескольких дейтаграмм, полученных при фрагментации, в одну исходную) при передаче пакета в сеть с большим значением MTU. В целях распознавания пакетов, образованных в результате фрагментации используется поле *Идентификатор пакета* (*Identification*). Все фрагменты фрагментированного пакета имеют одинаковое значение этого поля.

Поле *Флаги* (*Flags*) содержит биты: 0 бит - резерв = `0`, 1 бит - *DF - Do not Fragment* в случае установки в `1` запрещает фрагментацию пакета, 2 бит – *MF – More Fragments* в случае установки в `1` свидетельствует о том, что данная дейтаграмма является промежуточным (не последним) фрагментом.

В поле *Смещение фрагмента* (*Fragment Offset*) указывается смещение в 8-байтных блоках поля данных этого пакета-фрагмента от начала общего поля данных исходного пакета, подвергнутого фрагментации (8 байт x $2^{13}$ = $2^{16}$ – максимальный размер пакета). Первый фрагмент имеет значение этого поля, равное `0`. На рис. 97 приведен пример фрагментации дейтаграммы длиной 472 байта при маршрутизации её в сеть с MTU = 280 байт.




*а)*


*б)*


*в)*

Рис. 97. Пример фрагментации дейтаграммы: а) IP-заголовок исходной дейтаграммы; б) IP-заголовок первого фрагмента; в) IP-заголовок второго фрагмента

Идентификаторы исходного пакета и фрагментов одинаковы (111). Значение смещения фрагмента для первого фрагмента равно нулю. Длина поля данных первого фрагмента (рис. 97б) = 276 байт (*Общая длина пакета*) – 20 байт (*Длина заголовка*) = 256 байт/8 = 32 8-байтовых блока, что и указано в поле *Смещение фрагмента* второго фрагмента. Значение флагов

для первого фрагмента = 1 (001), то есть указывается, что этот фрагмент не последний. Для второго фрагмента значение флагов = 0 (000), то есть фрагмент последний.

Поле *Время жизни* (*Time To Live – TTL*) указывает предельный срок времени, в течение которого дейтаграмма может перемещаться по сети. Это время задаётся отправителем дейтаграммы в секундах. При пересылке пакета через маршрутизатор значение TTL уменьшается на 1 (даже если время передачи через маршрутизатор менее 1 секунды). Поэтому иногда говорят, что это время измеряется в количестве переходов через маршрутизаторы (hops). При достижении этим значением 0 пакет далее не передаётся.

Поле *Протокол верхнего уровня* (*Protocol*) содержит идентификатор протокола, переносящего информацию, размещённую в поле данных IP-пакета. Наиболее популярными идентификаторами являются $06_{Н}$ – для *протокола управления транспортом* (*Transport Control Protocol – TCP*), $11_{Н}$ – для *протокола пользовательских дейтограмм* (*User Datagram Protocol – UDP*) и $01_{Н}$ – для *протокола управляющих сообщений Интернет* (*Internet Control Message Protocol – ICMP*).

Поле *Контрольная сумма* (*Header Checksum*) рассчитывается только для заголовка IP-дейтаграммы. При каждом изменении полей заголовка промежуточными маршрутизаторами контрольная сумма заголовка пересчитывается. Алгоритм расчёта – дополнение к сумме всех 16-битовых слов заголовка. При вычислении контрольной суммы значение самого поля "Контрольная сумма" выставляется в 0.

Поля *IP-адрес отправителя* (*Source IP Address*) и *IP-адрес получателя* (*Destination IP Address*) содержат соответствующие адреса.

Поле *Опции* (*IP Options*) является необязательным и обычно не используется. В нем могут указываться точный маршрут прохождения дейтаграммы, данные о безопасности, различные временные отметки и т.д. Поле может иметь произвольную длину в пределах от 0 до 40 байтов, для выравнивания размера дейтаграммы по 32-битной границе используется поле *Выравнивание* (*Padding*). Это поле, например, используется для дополнения размера дейтаграммы нулевыми байтами до минимального размера поля данных кадра канального уровня (для Ethernet 64 байта).

## Задание для самостоятельной работы

В программе Cisco Packet Tracer постройте составную сеть, изображённую на рис. 84 без задания адресов хостам и маршрутизаторам.

По аналогии с примером на рис. 89 выполните планирование адресного пространства для составной компьютерной сети, состоящей из четырёх IP-подсетей сетей с $N_1$, $N_2$, $N_3$ и $N_4$ хостами и пятой подсетью между маршрутизаторами. Количество пользовательских хостов в подсетях вычисляется следующим образом:

$N_1$ = порядковому номеру студента в журнале академгруппы;
$N_2 = N_1 + 15$;
$N_3 = N_1 + 2N_2$;
$N_4 = N_1 + N_2 + N_3$.

Количество адресов в подсетях должно быть минимально возможным для рассчитанного числа хостов с учётом шлюза подсети. Используйте диапазон адресов 192.168.1.0 – 192.168.1.255 (при необходимости используйте следующую сеть класса С – 192.16.2.0). Количество адресов в пятой подсети выбирайте равным четырём: первый – адрес подсети, последний – широковещательный, оставшиеся два – для интерфейсов маршрутизаторов, соединённых связью "точка – точка". Адресное пространство подсети между маршрутизаторами должно находиться за последней из пользовательских подсетей.

Приведите в отчёт адресную информацию для всех подсетей, указав для каждой подсети:

- адрес подсети;
- маску подсети;
- широковещательный адрес подсети;
- адрес шлюза;
- диапазон адресов хостов подсети;
- диапазон резервных адресов для хостов подсети.

Выполните конфигурирование сетевых интерфейсов пользовательских хостов IP-подсетей в программе Packet Tracer в соответствии с разработанным планом адресов. Адрес шлюза подсети указывайте в строке Gateway (Шлюз) вкладки Config (Конфигурирование) (рис. 29 а). Выполните проверку правильности конфигурирования хостов пересылкой пакетов утилиты `ping` между хостами подсети внутри каждой пользовательской подсети.

Выполните настройку интерфейсов маршрутизаторов. Для этого на вкладке Config (Конфигурирование) выберите из меню Interfaces (Интерфейсы) слева интерфейс, к которому подключена первая сеть и назначьте этому интерфейсу IP-адрес шлюза и маску первой подсети. После чего включите интерфейс, установив отметку в чекбоксе Port Status (рис. 98). Обратите внимание на команды Cisco IOS, автоматически отображаемые в нижнем поле при конфигурировании. Приведите эти команды в отчёт и поясните их назначение.

Повторите конфигурирование для остальных интерфейсов маршрутизатора, которые связаны со второй подсетью и вторым маршрутизатором. Приведите в отчёт команды Cisco IOS, выполняющие конфигурацию интерфейсов.

Выполните проверку сети посылкой пакетов утилиты `ping`:

- от хоста первой подсети интерфейсу шлюза этой подсети;
- от хоста первой подсети интерфейсу шлюза второй подсети;
- от хоста первой подсети хосту второй подсети.

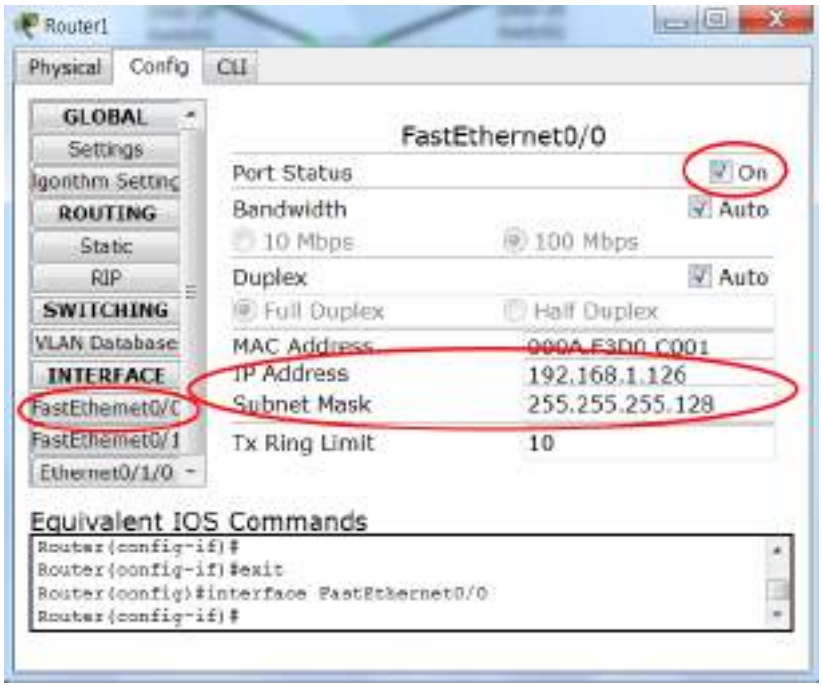



Рис. 98. Конфигурирование интерфейсов маршрутизатора

Аналогичным образом выполните конфигурирование интерфейсов второго маршрутизатора – шлюзов третьей, четвертой подсети и интерфейса связи с первым маршрутизатором. Проверьте их функционирование с помощью утилиты `ping`. Обратите внимание, что связь между первой и второй подсетями, а также между третьей и четвёртой подсетями организуется без всяких дополнительных настроек, только заданием IP-адресов и включением интерфейсов. Это происходит потому, что маршрутизатор фактически участвует в соседних сетях своими интерфейсами и "знает" об их существовании. В то же время первый маршрутизатор ничего "не знает" о существовании удалённых от него третьей и четвёртой подсетях. Адреса этих сетей необходимо сообщить ему путём ввода двух правил статической маршрутизации, задающих маршруты к этим сетям. В этих правилах указывается:

- IP-адрес удалённой подсети назначения (он будет фигурировать в первом столбце таблицы маршрутизации);
- маска этой удалённой подсети (она появится во втором столбце);
- IP-адрес следующего по пути в эту удалённую подсеть маршрутизатора (он будет указан в третьем столбце таблицы маршрутизации).

Для задания правил маршрутизации откройте вкладку Config (Конфигурирование) маршрутизатора и выберите из меню Routing (Маршрутизация) команду Static (Статическая). В полях Network (Сеть), Mask (Маска) и Next Hop (Следующий маршрутизатор) укажите, соответственно, IP-адрес подсети назначения, её маску и адрес следующего по пути к ней маршрутизатора. Нажмите на кнопку Add (Добавить). Маршрут будет добавлен в список маршрутов ниже кнопки (рис. 99).

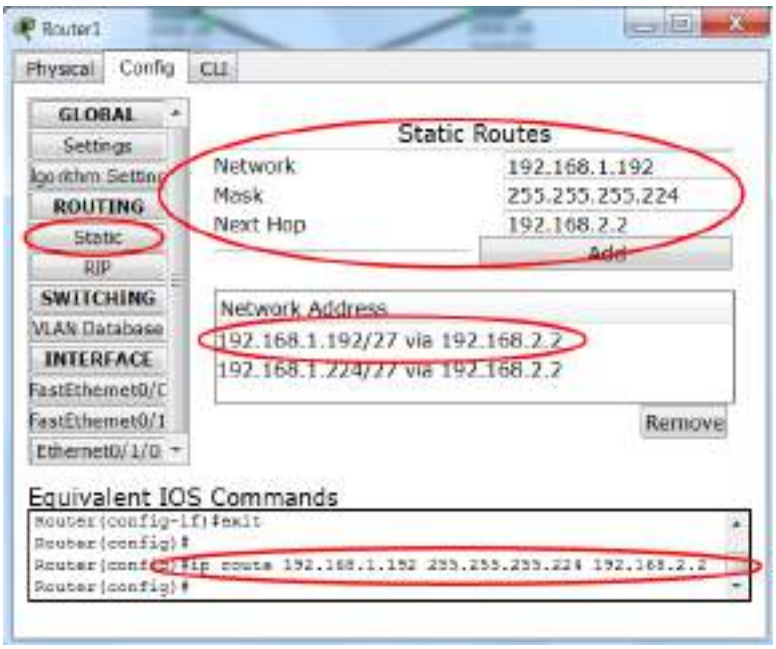



Рис. 99. Задание правил маршрутизации

Добавьте аналогичным способом маршрут к другой удалённой подсети. Обратите внимание, что в нижнем поле автоматически указывается команда Cisco IOS добавления маршрута. Приведите команды добавления обоих маршрутов в отчёт.

Аналогичным образом сконфигурируйте правила статической маршрутизации к удалённым сетям на другом маршрутизаторе. Приведите команды Cisco IOS добавления маршрутов к ним в отчёт.

Проверьте работоспособность всей составной сети посылкой пакетов утилиты `ping` от хоста первой подсети хостам остальных подсетей.

Для просмотра конфигурации маршрутизаторов используйте инструмент Inspect (Инспектировать), выполнив щелчок которым по маршрутизатору, выберите команду Routing Table (Таблица маршрутизации) (рис. 100). Эту информацию также можно просмотреть командой Cisco IOS `sh ip route`. Приведите в отчёт листинги команд `sh ip int brief` (выводит адресную информацию интерфейсов) и `sh ip route` для обоих маршрутизаторов.

С целью изучения формата IP-дейтаграммы выполните захват анализатором Wireshark пакетов утилиты `ping`, отправленных с Вашего компьютера на соседний. После захвата выделите заголовок IP-дейтаграммы, как на рис. 101, и приведите в отчёт шестнадцатеричные значения всех полей её заголовка с их расшифровкой.

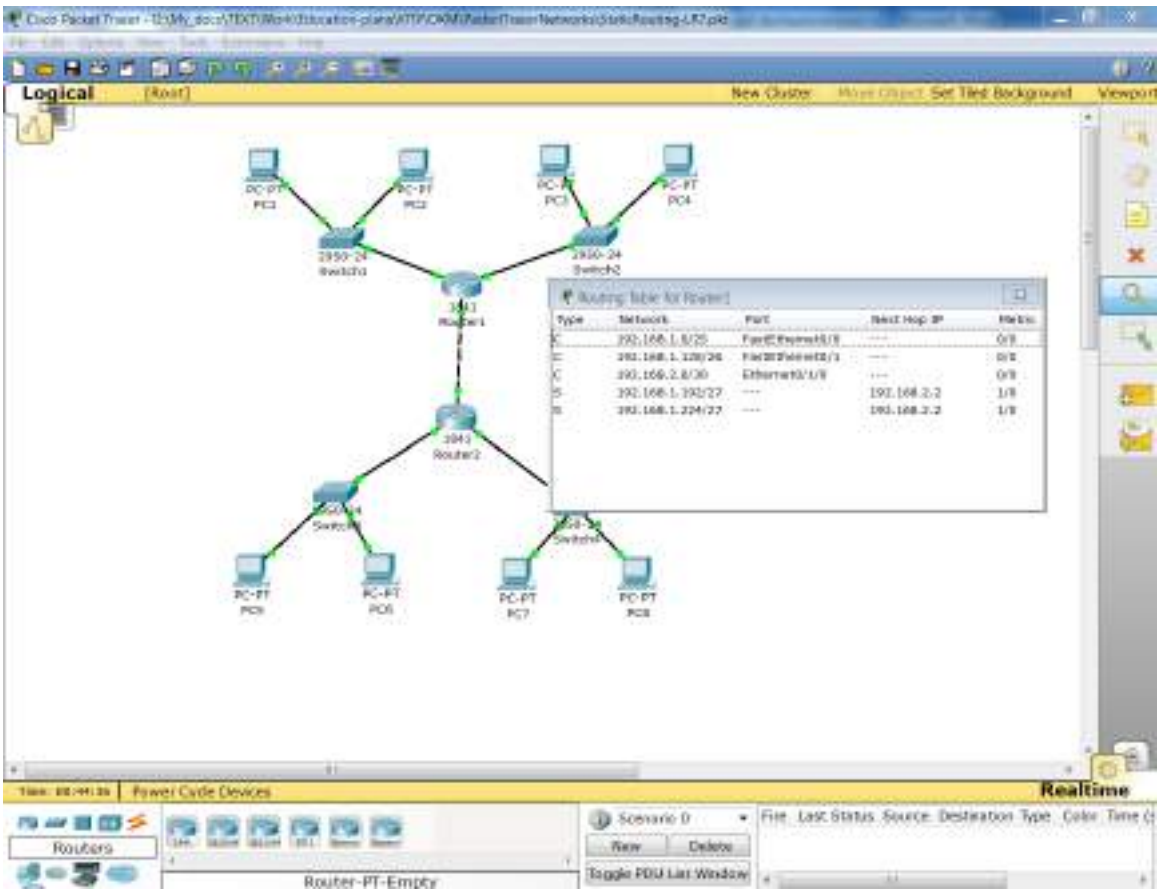



Рис. 100. Просмотр таблицы маршрутизации маршрутизатора

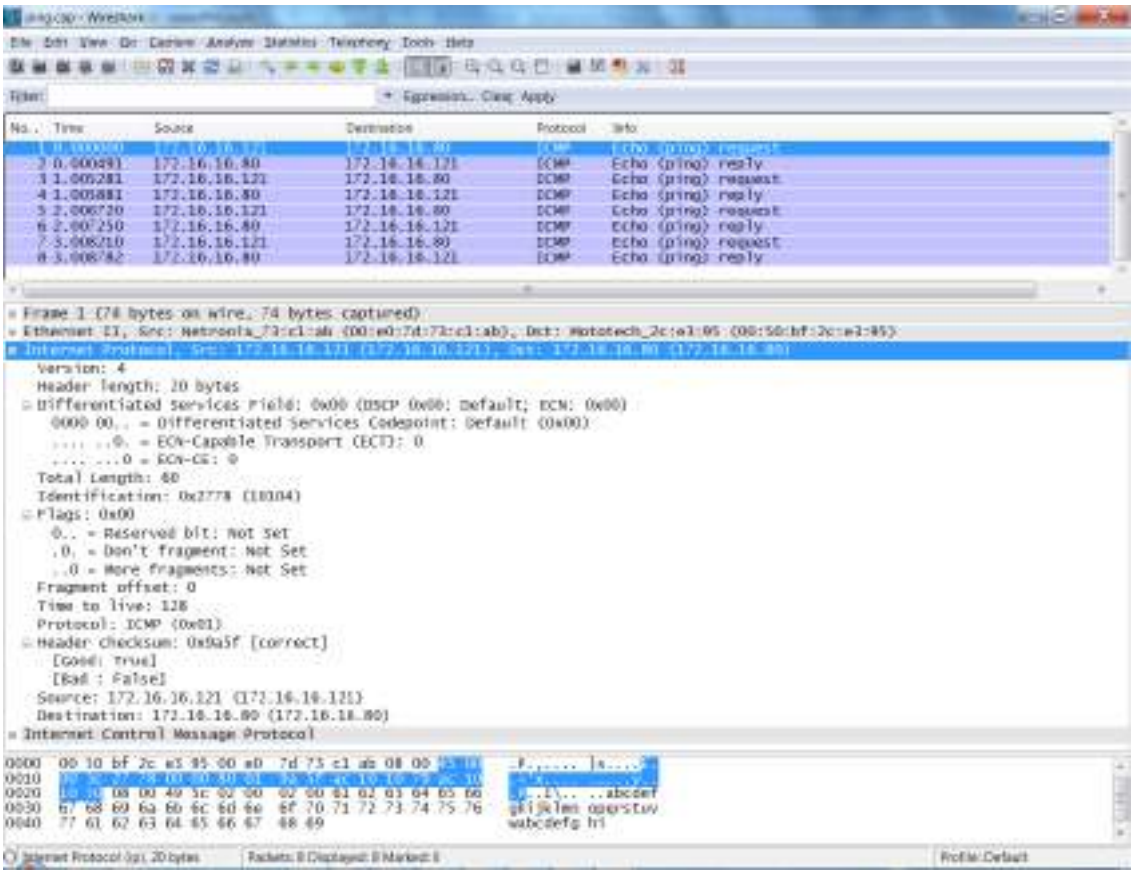



Рис. 101. Анализ заголовка IP-дейтаграммы в Wireshark

Повторите эксперимент, захватив отправленные с Вашего компьютера на соседний пакеты утилиты `ping` размером `L=(N+1)*1500` байт (где `N` – десятичное значение Вашего порядкового номера в журнале академгруппы). Для задания размера пакетов используйте ключ команды `ping –l`, например, `ping -l 3700` (для `L= 3700` байт). Приведите в отчёт значения полей идентификатора пакета, флагов и смещения фрагмента для каждого фрагмента пакета в следующей таблице.

| № п/п фрагмента | Идентификатор пакета | Флаг DF | Флаг MF | Смещение фрагмента |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| … | | | | |

## Вопросы для самоподготовки

1. Опишите основное назначение протокола IP. Сравните пределы передачи IP-дейтаграмм и Ethernet-кадров.
2. Опишите формат IP-адреса протокола IP v4, назовите его принципиальное отличие от MAC-адреса.
3. Дайте определение технологии маршрутизации.
4. Что называют шлюзом сети/подсети. В каком случае пакеты проходят через шлюз?
5. Что представляет собой фрагментация/дефрагментация дейтаграмм? В каком случае она выполняется? Что такое MTU?
6. Оцените объем пространства адресов IP v4 и опишите, как организовано их выделение конечным пользователям.
7. Назовите классы IP адресов и их характеристики. Каким образом маршрутизаторы определяют принадлежность IP-адреса получателя к тому или иному классу?
8. Опишите особые (выделенные под специальные нужды) IP адреса и их назначение.
9. Что представляют собой локальные IP-адреса, назовите диапазоны сетей таких адресов. Для чего служит технология сетевой трансляции адресов?
10. Опишите формат и использование маски подсети. Как по значению маски определить количество адресов, которое она выделяет? Перечислите известные Вам маски и их характеристики для сети класса C.
11. Определите, входят ли два IP-адреса (например, `192.168.1.67` и `192.168.117`) в одну и ту же подсеть с маской `255.255.255.192`.
12. Что представляет собой технология бесклассовой междоменной маршрутизации? Запишите адрес и маску суперсети для 2000 хостов.
13. Опишите структуру таблицы маршрутизации и способ нахождения маршрута маршрутизатором по IP-адресу получателя.

14. Что представляет собой маршрут по умолчанию, для чего он используется? Каким образом маршрут по умолчанию указывается в таблице маршрутизации?
15. Что такое метрика маршрута, какие параметры могут служить метрикой?
16. Чем отличается статическая маршрутизация от динамической? Приведите названия популярных протоколов динамической маршрутизации.
17. Опишите алгоритм нахождения маршрутизаторами следующего от них шага маршрута. Каким образом адресуется интерфейс, на который необходимо переслать пакет, на следующем шаге маршрута?
18. Выведите на экран Вашего компьютера таблицу маршрутизации для его интерфейсов.
19. Опишите формат заголовка IP и назначение его полей. Какова минимальная и максимальная длина IP пакета?
20. Опишите, каким образом выполняется фрагментация и дефрагментация пакетов при пересечении ними сетей с различным значением MTU.
21. Что такое время жизни пакета и для чего служит этот параметр?
22. Укажите идентификаторы наиболее популярных протоколов, пакеты которых переносятся в поле данных IP.

## Тесты для контроля усвоения знаний

1. Хост имеет IP-адрес `192.168.1.47` и маску подсети `255.255.255.224`. Укажите адрес подсети и широковещательный адрес подсети, в которую входит данный хост.
2. Укажите класс (A, B или C) следующих IP-адресов:
   - `172.16.2.2;`
   - `10.15.234.28;`
   - `192.168.5.137.`
3. В Вашей сети находится 31 компьютер. Укажите маску подсети, обеспечивающую выделение этих компьютеров в подсеть с минимально возможным числом IP-адресов
   а) `255.255.255.248;`
   б) `255.255.255.240;`
   в) `255.255.255.224;`
   г) `255.255.255.192;`
   д) `255.255.255.128.`
4. Находятся ли в одной подсети компьютеры с IP-адресами `172.16.2.65` и `172.16.2.94`, если у них маска подсети `255.255.255.224`?
5. Выберите условие, при выполнении которого хост/маршрутизатор пересылает IP-дейтаграмму шлюзу:
   а) IP-адрес отправителя и IP-адрес получателя принадлежат разным сетям/подсетям;

б) IP-адрес отправителя и IP-адрес получателя принадлежат одной и той же сети/подсети;

6. Выберите правильное определение для максимальной единицы передачи (Maximum Transfer Unit, MTU):
   а) MTU – это максимально допустимый размер заголовка IP-пакета;
   б) MTU – это максимально допустимый размер IP-пакета;
   в) MTU – это максимально допустимое значение длины поля данных кадров канального уровня.
7. Выберите адрес, по которому не будут передаваться IP-дейтаграммы в Интернете:
   а) `141.25.13.48;`
   б) `172.31.204.1;`
   в) `191.15.26.147.`
8. Выберите логическую операцию, которая используется для определения адреса сети/подсети из IP-адреса получателя дейтаграммы:
   а) IP-адрес получателя XOR маска сети/подсети;
   б) IP-адрес получателя OR маска сети/подсети;
   в) IP-адрес получателя AND маска сети/подсети.
9. Укажите маску суперсети с 2000 хостами, если адрес такой сети `212.14.17.0:`
   а) `255.255.255.0;`
   б) `255.255.254.0;`
   в) `255.255.252.0;`
   г) `255.255.248.0.`
10. Укажите порядковый номер (от 1 до 5) для столбцов таблицы маршрутизации:
   а) IP-адрес следующего по маршруту маршрутизатора = …;
   б) метрика маршрута = …;
   в) адрес сети/подсети/хоста назначения = …;
   г) IP-адрес исходящего порта текущего маршрутизатора = …;
   д) маска подсети назначения = ….
11. Выберите правильное утверждение об изменениях MAC- и IP-адресов в пересылаемых в составной сети сетевых пакетах при следовании их по маршруту:
   а) MAC-адрес отправителя на каждом шаге изменяется, MAC-адрес получателя остаётся неизменным, IP-адреса остаются неизменными;
   б) MAC-адрес отправителя и MAC-адрес получателя остаются неизменными на каждом шаге, IP-адреса также остаются неизменными;
   в) MAC-адрес отправителя и MAC-адрес получателя изменяются на каждом шаге изменяется, IP-адреса остаются неизменными;
   г) MAC-адрес отправителя и MAC-адрес получателя остаются неизменными на каждом шаге, IP-адреса изменяются;

12. Укажите, какя информация служит указателем на первый фрагмент дейтаграммы:
    а) нулевое значение флага MF – More Fragments;
    б) нулевое значение поля Смещение фрагмента;
    в) нулевое значение поля Идентификатор пакета.

## Литература

1. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – 4-е изд. – СПб. : Питер, 2009. – 992 с.

2. TCP/IP: Архитектура, протоколы, реализация / Сидни Фейт – 2-е изд. – McGraw-Hill, 2000. – 424 с.

3. Усманов Р. Протокол IP [электронный ресурс] / Р. Усманов. – режим доступа: http://www.citforum.ru/nets/tcp/ipspec.shtml.

# РАЗДЕЛ 5
# ИССЛЕДОВАНИЕ РАБОТЫ ПРОТОКОЛА УПРАВЛЯЮЩИХ СООБЩЕНИЙ ИНТЕРНЕТ ICMP И ПРОТОКОЛОВ ТРАНСПОРТНОГО УРОВНЯ UDP И TCP

## 5.1. Протокол управляющих сообщений Интернет ICMP

Дейтаграммный характер протокола IP (отсутствие предварительной установки соединения и гарантий доставки пакета) в определённом смысле является проблемой при передаче данных. Тот факт, что на уровнях, лежащих выше сетевого (обычно на транспортном), реализуются механизмы, обеспечивающие надёжную передачу данных, не спасает, поскольку, например, при выключении хоста-получателя посредине сеанса работы отправитель, не зная о проблеме, будет продолжать отправлять пакеты, по крайней мере, ещё некоторое время (рис. 102).

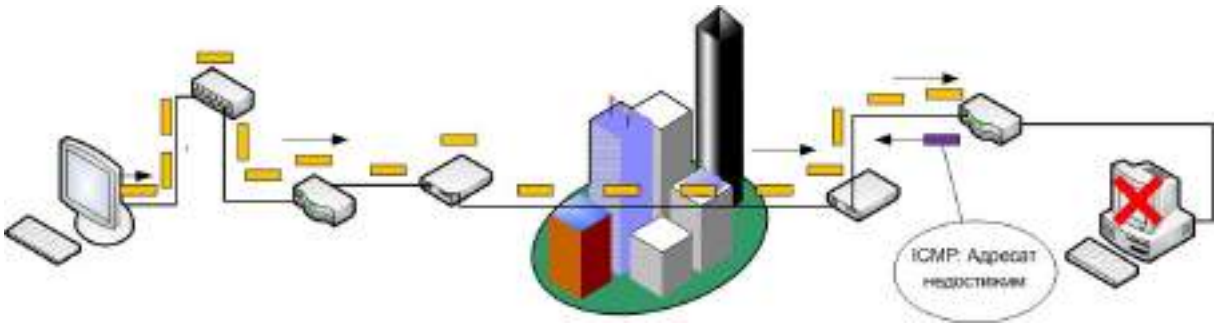



Рис. 102. Извещение отправителя о недоступности получателя с помощью ICMP-сообщения

Также во время сеанса может отказать промежуточный маршрутизатор, либо реконфигурироваться промежуточная сеть, либо завершить работу приложение, получающее информацию черезь сеть, и т.д. Необходим механизм, обнаруживающий ошибки подобного рода и извещающий конечного (хоста) и промежуточных (маршрутизаторов) отправителей пакетов о проблеме. Такую задачу решает *протокол управляющих сообщений Интернета* (*Internet Control Message Protocol – ICMP*). Сообщение ICMP пересылается в поле данных IP-пакета (рис. 103), при этом размер заголовка ICMP обычно составляет восемь байт.


Рис. 103. Схема инкапсуляции сообщений ICMP

Формат заголовка ICMP приведен на рис. 104. Расшифровка значений полей Тип и Код приведена в табл. 5.


Рис. 104. Формат ICMP-пакета

Таблица 5

Типы ICMP-сообщений

| Тип | Код | Описание | Тип | Код | Описание |
|---|---|---|---|---|---|
| 0 | 0 | Эхо-ответ | 5 | 2 | Перенаправление для каждого типа обслуживания (TOS) |
| 3 | 0 | Невозможно передать дейтаграмму в локальную сеть адресата | 5 | 3 | Перенаправление пакета к узлу для каждого типа обслуживания |
| 3 | 1 | Невозможно передать дейтаграмму на хост-компьютер адресата | 8 | 0 | Эхо-запрос |
| 3 | 2 | Нельзя воспользоваться указанным протоколом | 11 | 0 | Время жизни пакета (TTL) истекло при транспортировке |
| 3 | 3 | Нельзя передать данные на указанный порт | 11 | 1 | Время жизни пакета (время сборки фрагментов) истекло при дефрагментации |
| 3 | 4 | Необходима фрагментация, но установлен флаг её запрета (DF) | 12 | 0 | Ошибка параметра, указатель показывает ошибку |
| 3 | 5 | Сбой в маршрутизации при отправлении | 13 | 0 | Запрос метки времени |
| 4 | 0 | Сдерживание отправителя (отключение отправителя при переполнении входного буфера) | 14 | 0 | Ответ с меткой времени |
| 5 | 0 | Перенаправление пакетов в сеть | 15 | 0 | Запрос информации |
| 5 | 1 | Перенаправление пакетов к узлу | 16 | 0 | Ответ на запрос информации |

Протокол ICMP служит для сообщения об ошибках, но не для исправления ошибок, отправитель сам должен определить источник ошибки и предпринять меры по устранению ошибок.

Пользователь может использовать сообщения Эхо-запрос (Тип = 8) и Эхо-ответ (Тип = 0) для проверки достижимости адресата (получателя) IP-пакета, его способности отвечать на запросы, а также о работоспособности

системы маршрутизации. В ICMP-сообщении Эхо-ответ меняются местами IP-адреса получателя и отправителя. Использующая такие ICMP-сообщения программа `ping`.

Программа `tracert` (`traceroute`) высылает пакет по указанному IP-адресу или DNS-имени со значением `TTL=1`. Поскольку на первом маршрутизаторе `TTL` станет равным 0, пакет вернется на адрес отправителя с сообщением об ICMP-ошибке Контрольное время истекло, `tracert` (`traceroute`) при этом отображает имя и адрес первого маршрутизатора, а также время между отправкой пакета и получением ICMP-сообщения – (*Round Trip Time – RTT*). Затем `tracert` (`traceroute`) высылает пакет по указанному IP-адресу или DNS-имени со значением `TTL = 2`, второй маршрутизатор высылает ICMP-пакет отправителю и его адресная информация отображается на экране. Так продолжается до тех пор, пока отправитель не получит ICMP-пакет от последнего узла в цепочке, которым является узел с адресом, указанным `tracert` (`traceroute`) (рис. 105).

```
C:\WINNT\system32>tracert www.rada.kiev.ua
Трассировка маршрута к alpha.rada.kiev.ua [195.230.148.11]
с максимальным числом прыжков 30:
  1   <10 мс   <10 мс   <10 мс  cit-gw.zgia.zp.ua [192.168.1.129]
  2   <10 мс   <10 мс   <10 мс  Eagle.zgia.zp.ua [192.168.1.1]
  3   <10 мс   <10 мс   <10 мс  lix.ZSEA.zp.ua [212.8.40.6]
  4   <10 мс    10 ms   <10 мс  zssm.IX.zp.ua [212.8.32.241]
  5   120 ms    30 ms    60 ms  center-E1-apex-1.apex.dp.ua [195.24.137.130]
  6    70 ms    30 ms    40 ms  kiev-dnepr.apex.dp.ua [212.3.111.61]
  7    30 ms    30 ms    20 ms  infocom-gw.ix.net.ua [195.35.65.35]
  8    40 ms    50 ms    60 ms  plus.ukrpack.net [195.230.150.9]
  9     *       60 ms   141 ms  S94.plus.ukrpack.net [195.230.151.94]
 10   130 ms   120 ms    60 ms  alpha.rada.kiev.ua [195.230.148.11]
Трассировка завершена.
```

Рис. 105. Использование программы tracert для трассировки маршрута

## 5.2. Общая характеристика протоколов транспортного уровня стека TCP/IP

К протоколам транспорного уровня сетевого стека TCP/IP относятся *протокол пользовательских дейтаграмм* (*User Datagram Protocol – UDP*) и *протокол управления транспортом* (*Transport Control Protocol – TCP*). Общей задачей этих протоколов является дополнительная (к MAC-адресу канального уровня и IP-адресу сетевого уровня) адресация. Её необходимость проиллюстрирована на рис. 106. Действительно, если два компьютера, расположенные в одной IP-сети, выполняют сетевое взаимодействие, пересылая несколько последовательностей пакетов различными приложениями, то адресная информация в заголовках канального и сетевого уровня у них не отличается (для компьютеров, расположенных в разных IP-сетях, не будут отличаться IP-адреса отправителя и получателя). В то же время, каждое приложение выполняется в определённой области памяти, выделенной ему

операционной системой компьютера, и потоки пакетов должны попадать именно в "свои" области памяти.

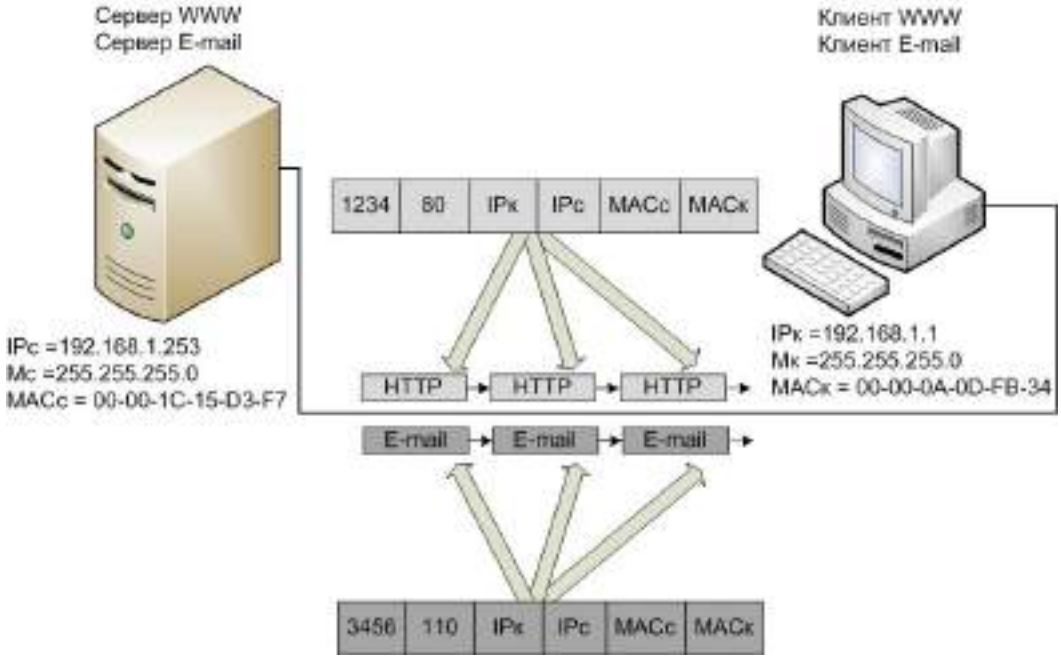



Рис. 106. Пересылка нескольких потоков пакетов различными приложениями

Для решения этой проблемы в протоколах UDP и TCP используется дополнительная адресация с помощью двухбайтовых *портов транспортного уровня* (термин "порт" является не совсем удачным, поскольку он не имеет отношения к портам оборудования). При этом порты с номерами от 0 до 1023 стандартом *RFC 1700 Assigned Numbers* закреплены за *стандартными службами* (*well-known services*), исполняющимися на серверах (табл. 6). Оставшиеся номера портов (выше 1023) предоставляются клиентскому программному обеспечению по мере необходимости путем выделения номера порта из пула доступных портов.

Таблица 6

Порты протоколов транспортного уровня общеизвестных служб

| **Служба** | **Протокол*** | **Порт** | **Описание** |
|---|---|---|---|
| FTP-Data | TCP | 20 | Пересылка данных FTP |
| FTP | TCP | 21 | Пересылка команд FTP |
| TELNET | TCP | 23 | Порт telnet |
| SMTP | TCP | 25 | Порт простого протокола пересылки почты |
| Nameserver (DNS) | UDP | 53 | Служба имен доменов |
| Bootps/DHCP | UDP | 67 | Порт сервера загрузки конфигурационной информации |
| Bootpc/DHCP | UDP | 68 | Порт клиента, получающего конфигурационную информацию |

| | | | |
|---|---|---|---|
| TFTP | UDP | 69 | Простейший протокол пересылки файлов |
| HTTP | TCP | 80 | Протокол пересылки гипертекстовых страниц |
| POP3 | TCP | 110 | Служба выборки почтовых сообщений для ПК |
| SunRPC | UDP | 111 | Вызов удаленных процедур |
| NNTP | TCP | 119 | Протокол пересылки сетевых новостей |
| NTP | UDP | 123 | Служба Network Time Protocol |
| NetBIOS-NS | UDP | 137 | Служба имён NetBIOS |
| NETBIOS-SSN | TCP | 139 | Служба сеанса NetBIOS |
| SNMP | UDP | 161 | Получение сетевых запросов обслуживания |
| SNMP-trap | UDP | 162 | Получение отчетов о проблемах в сети |
| HTTPS | TCP | 443 | Безопасный протокол пересылки гипертексто-вых страниц |
| MDS/SMB | TCP | 445 | MDS (Microsoft Directory Services) SMB (Server Message Blocks over IP) - Служба поддержки TCP/IP NetBIOS |

* Для всех служб зарегистрированы и TCP, и UDP-порты с одинаковым номером, в столбце Протокол указан наиболее часто встречаемый протокол для служб.

Используемая для адресации комбинация `IP-адрес:номер порта` называется *адресом сокета (socket address)*. Адрес сокета обеспечивает для сервера и клиента всю информацию, необходимую для идентификации партнера по коммуникации, пара адресов сокетов клиента и сервера является уникальной во всей сети Интернет. Командой `netstat - na` можно вывести список текущих коммуникаций хоста с отображением пар адресов сокетов (рис. 107).

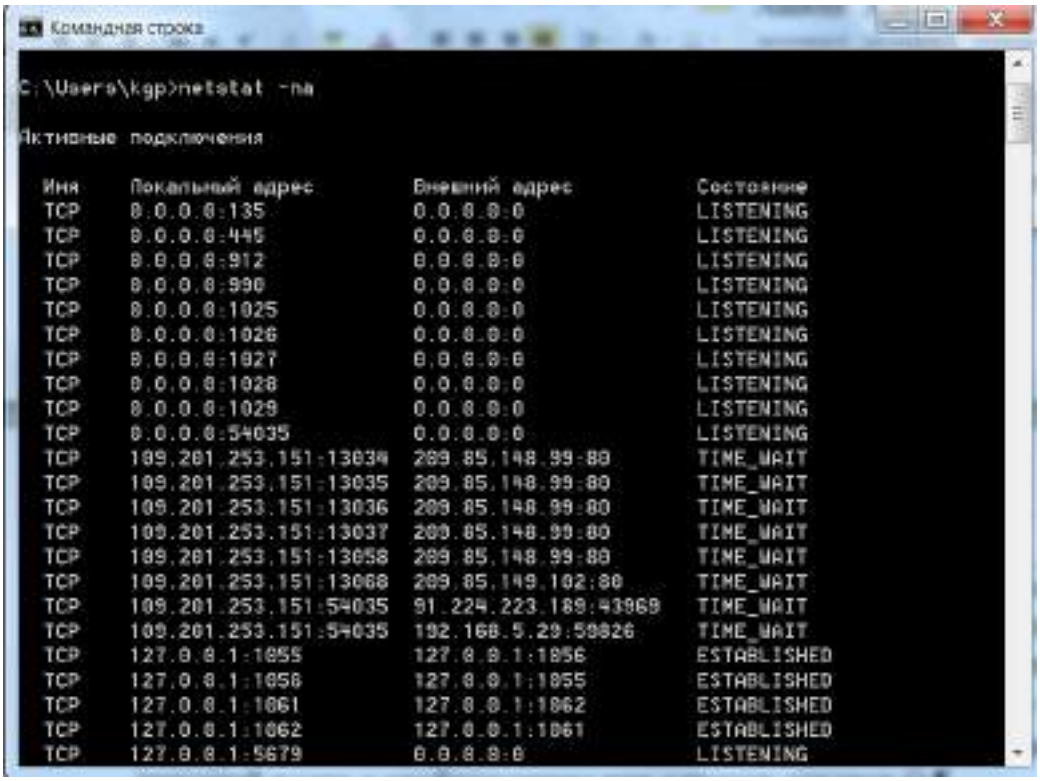



Рис. 107. Вывод адресов сокетов с их состоянием

В первом столбце указывается протокол транспортного уровня, во втором – адрес сокета локального комьютера (то есть IP-адрес и через двое точие порт транспортного уровня), в третьем столбце адрес сокета удалённого комьютера (`0.0.0.0:0` - для "слушающих" портов локального компьютера, приписанных к серверным процессам ожидающим соединений) и в четвёртом столбце - состояние коммуникации (например, `LISTENING` – ожидание соединения, `TIME-WAIT` – отработавшая коммуникация нормально закрыта, но будет ещё доступна для пакетов в течение примерно 30–120 секунд, `ESTABLISHED` – соединение установлено).

Наличие двух протоколов транспортного уровня в стеке TCP/IP связано с их особенностями, определяющими область использования этих протоколов (табл. 7).

**Таблица 7**

**Сравнительная характеристика протоколов UDP и TCP**

| User Datagram Protocol - UDP | Transport Control Protocol - TCP |
|---|---|
| **Преимущества протоколов** | |
| Быстрый за счёт отсутствия средств гарантирования доставки пакета и обеспечения целостности информации | Гарантирует надежную доставку пакетов |
| Позволяет организовывать многоадресные и широковещательные рассылки на сетевом уровне | Гарантирует целостность информации в пакетах |
| **Недостатки протоколов** | |
| Не гарантирует доставку пакетов | Относительно медленный за счёт поддержки средств гарантирования доставки пакета и обеспечения целостности информации |
| Не гарантирует целостность информации в пакетах (при отсутствии расчёта контрольной суммы) | Использует соединения "точка – точка", что не позволяет осуществлять многоадресные и широковещательные рассылки на сетевом уровне |
| **Области применения протоколов** | |
| Внутри надёжных сетей канального уровня небольшого масштаба (например, локальных сетей Ethernet) | В территориальных и глобальных сетях, надёжность которых сложно обеспечить как из-за их размера, так и из-за отсутствия единого администрирования |
| При передаче оцифрованного звука и видео, когда потеря нескольких пакетов не приводит к проблемам при воспроизведении информации | При передаче файлов и сообщений, когда важными являются каждый пакет и каждый байт в пакете |
| При организации многоадресной рассылки в составных сетях (например, видео по требованию) | – |

## 5.3. Протокол пользовательских дейтаграмм UDP

*Протокол пользовательских дейтаграмм (User Datagram Protocol – UDP)* является службой, пересылающей информацию в IP-пакетах без использования механизмов, гарантирующих доставку пакетов получателю и целостность информации (следует отметить, что целостность может гарантировать наличие контрольной суммы в заголовке UDP, однако её расчёт в случае использования IPv4 является опциональным). В поле заголовка IP пакета *Протокол верхнего уровня* указывается код, равный 17 ($11_H$) (рис. 108). Заголовок UDP дейтаграммы представлен на рис. 109.

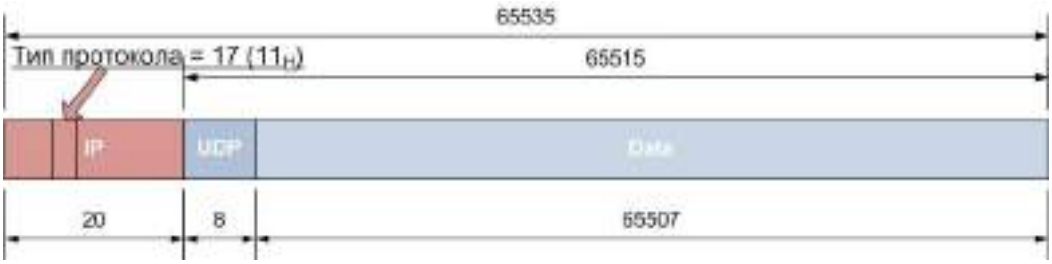



Рис. 108. UDP-дейтаграмма максимального размера внутри IP-пакета

| 0 | 15 16 | 31 |
|---|---|---|
| Порт отправителя | | Порт получателя |
| Длина UDP дейтаграммы, включая UDP заголовок | | Контрольная сумма псевдозаголовка и UDP дейтаграммы |

Рис. 109. Структура заголовка UDP

Поле *Длина UDP дейтаграммы* определяет общее количество байт в заголовке UDP и области данных. Максимальная длина UDP-дейтаграммы определяется максимальным размером IP-пакета, в котором она находится, в случае минимального размера заголовка IP в 20 байт, максимальный размер UDP-дейтаграммы составляет 65515 байт (рис. 108).

Поле *Контрольная сумма псевдозаголовка и UDP дейтаграммы* вычисляется для виртуальной структуры данных, представляющей собой псевдозаголовок (рис. 110), к которому присоединена UDP-дейтаграмма, при необходимости в конце дополненная нулями так, чтобы общий размер структуры данных был кратен 16 битам. Псевдозаголовок и дополнение не пересылаются по сети, однако они могут быть восстановлены из IP-пакета и размера UDP-дейтаграммы получателем.

| 0 | 7 8 | 15 16 | 31 |
|---|---|---|---|
| IP-адрес отправителя (Source Address) | | | |
| IP-адрес получателя (Destination Address) | | | |
| 0 0 0 0 0 0 0 0 | | Протокол = 17 | Длина UDP дейтаграммы |

Рис. 110. Структура псевдозаголовка UDP дейтаграммы

Наличие псевдозаголовка позволяет защитить контрольной суммой адреса сокетов, образующих коммуникацию, а не только адреса портов. Следует отметить, что протокол UDP не предусматривает стандартного механизма повторения передачи потерянных пакетов.

## 5.4. Протокол управления транспортом TCP

*Протокол управления транспортом* (*Transport Control Protocol – TCP*) обеспечивает гарантированную доставку пакетов, соответствующий исходному сообщению порядок следования байт, исключает ошибки передачи, а также реализует управление потоком и производительностью соединения. Надёжность передачи данных обеспечивается поддержкой TCP следующих механизмов:

- последовательной нумерации байтов в передаваемых блоках данных;
- подтверждения приема данных с реализацией таймаутов и повторных передач (ретрансмиссий) неподтверждённых данных;
- предварительной установки соединения между отправителем и получателем;
- процедуры нормального и внештатного завершения соединения между отправителем и получателем;
- обязательного использования контрольной суммы для защиты TCP-пакета.

Рассмотрим обобщённую схему взаимодействия отправителя и получателя с использованием протокола TCP. Сетевое приложение, выполняющееся на компьютере отправителя, передает отправляемые по сети данные программному обеспечению TCP, которое размещает данные в своём *выходном буфере* (*send buffer*) (рис. 111). Затем TCP вырезает так называемый *сегмент данных* (*segments*) из буфера, добавляет к нему TCP-заголовок и передает протоколу IP для доставки в виде отдельной дейтаграммы. *Максимальный размер сегмента* (*Maximum Segment Size – MSS*) определяется значением параметра максимальной единицы передачи (*Maximum Transfer Unit – MTU*) технологии канального уровня и суммарным размером заголовков TCP и IP:

MSS = MTU – заголовок TCP – заголовок IP

В случае, если TCP-сегмент передаётся в IP-сети, работающей поверх Ethernet (напомним, что Ethernet характеризуется значением MTU = 1500 байт), то при размерах заголовков TCP и IP (без опций), равных по 20 байт, значение MSS будет составлять 1460 байт. Пакетирование данных в сегменты максимального размера обеспечивает максимальную производительность соединения, поэтому до создания сегмента TCP будет ожидать, пока в выходном буфере не появится соответствующее количество данных.


Рис. 111. Формирование сегмента TCP

На практике не всегда размер отправляемого сегмента равен MSS (такие случаи будут рассмотрены далее), однако следует заметить, что при равном MSS размере сегмента при прочих равных условиях производительность соединения будет наибольшей.

Как и для UDP, протокол TCP идентифицирует приложения на стороне отправителя и получателя указанием номеров портов (табл. 6). Номера портов TCP также находятся в диапазоне от 0 до 65535, а порты от 0 до 1023 называются общеизвестными и используются для доступа к стандартным службам, а порты выше 1023 выделяются клиентскому программному обеспечению.

TCP предусматривает присвоение порядкового номера каждому пересылаемому по соединению байту данных. В заголовке сегмента указывается *порядковый номер* (*Sequence Number – SEQ#*) первого байта поля данных этого сегмента. В подтверждении TCP, высылаемом отправителю, указывается *номер подтверждения* (*Acknowledgement Number – ACK#*), представляющий собой номер байта следующего за последним байтом в текущем сегменте, полученном получателем. Если подтверждение не приходит за интервал *тайм-аута* (*timeout*), данные передаются повторно. Такой механизм называется *позитивным подтверждением с ретрансляцией* (*positive acknowledgment with retransmission*) (рис. 112).


Рис. 112. Позитивное подтверждение с ретрансляцией в TCP

Перед высылкой первого сегмента получателю отправитель инициирует *процедуру установления соединения*, которую часто называют *трой-*

*ным рукопожатием* (*three-way handshaking*), поскольку для установки соединения партнеры обмениваются тремя сообщениями (рис. 113).

Инициатором соединения является клиент. Во время установления соединения партнеры обмениваются значениями следующих параметров:

- *начальным порядковым номером* (*Initial Sequence Number – ISN*) первого байта отправляемого сегмента (его значение выбирается случайным образом с использованием системного таймера), в примере на рис. 113 ISN клиента равен 1000, а ISN сервера – 8000;
- размером буферного пространства для приема данных (так называемого *окна* (*Window*) – будет рассмотрено далее), на рис. 113 показано, что размер окна сервера (64 кбайта) превышает размер окна клиента (8 кбайт), что часто встречается на практике;
- значением максимального размера сегмента (MSS).

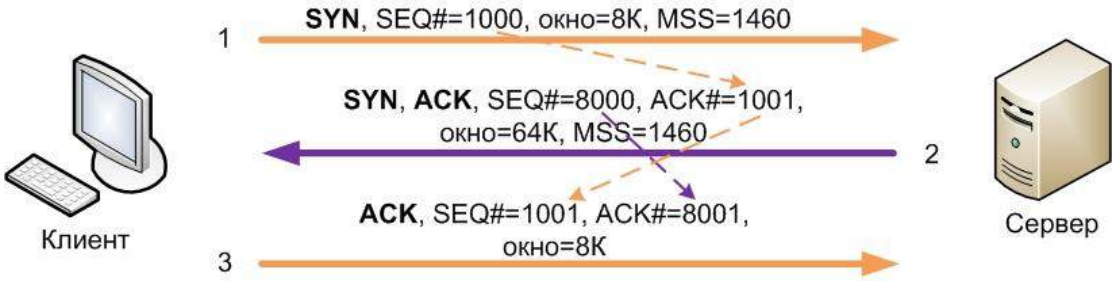



Рис. 113. Установление соединения TCP

TCP обеспечивает полнодуплексный режим работы, одновременно обслуживая два потока данных в разных направлениях. В ответ на инициирующий соединение пакет клиента сервер открывает встречное соединение, пересылая вместе с подтверждением принятия клиентского пакета свои значения указанных выше параметров. В третьем пакете высылается подтверждение клиентом факта установки инициированного сервером соединения. После завершения установления соединения происходит одновременная передача данных в обоих направлениях с присвоением передаваемым байтам последовательных, начиная с ISN + 1, номеров. Например, пакеты данных с сервера передаются одновременно с подтверждениями получения ранее принятых данных в пакетах с клиента.

При пересылке данных TCP подтверждения включаются в пересылаемые сегменты и содержат номер следующего байта, который ожидает получатель в поле данных сегмента.

На рис. 114 первый посланный клиентом сегмент содержит байты с номерами от 1001 до 2000, в его поле ACK указывается значение номера байта 3001, ожидаемого от сервера. Сервер отвечает клиенту сегментом с номерами байтов от 3001 до 4000, в его поле ACK указано значение 2001, означающее, что предыдущая посылка клиента успешно получена. Далее клиент посылает несколько сегментов, не дожидаясь подтверждений от сервера. Сервер использует единственный ACK для подтверждения приня-

тия этих сегментов, экономя полосу пропускания соединения. На рис. 114 также показана пересылка данных при потере сегмента.

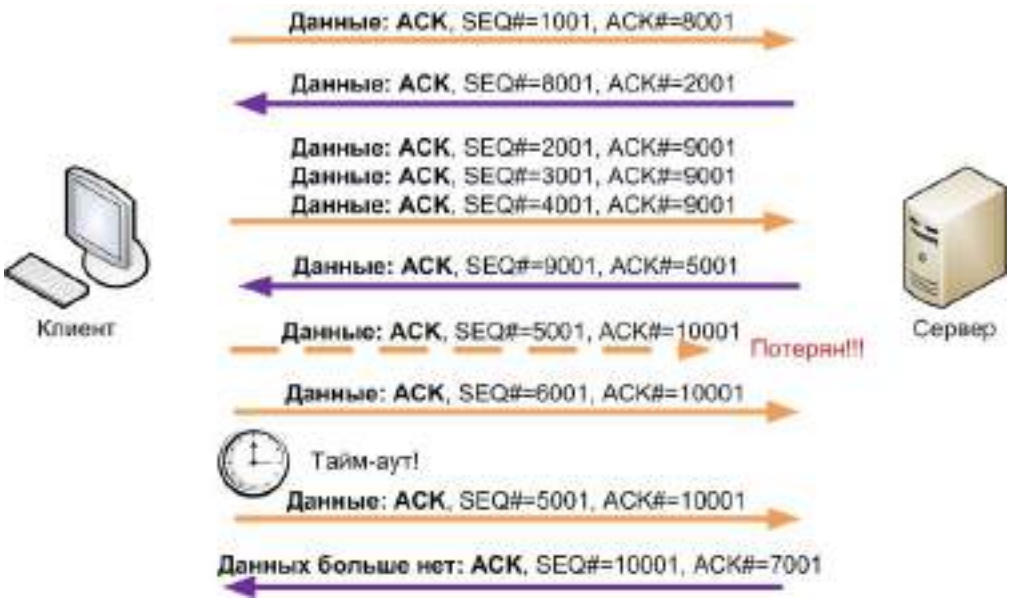



Рис. 114. Пересылка данных TCP

Нормальное завершение TCP соединения может быть инициировано любой стороной (клиентом или сервером). На рис. 115 иллюстрируется завершения сеанса при его инициализации сервером (например, после ввода команды `logout` пользователем в сеансе telnet). В этом случае выполняются следующие действия:

- приложение на сервере указывает TCP на закрытие соединения;
- TCP сервера посылает *заключительный сегмент* (*Final Segment – FIN*), информируя своего партнера о том, что данных для отправки больше нет;
- TCP клиента посылает ACK;
- клиентское приложение сообщает своему TCP о закрытии соединения;
- TCP клиента посылает сообщение FIN;
- TCP сервера получает FIN от клиента и отвечает на него сообщением ACK;
- TCP сервера указывает своему приложению на закрытие соединения.


Рис. 115. Завершение соединения TCP

Обе стороны могут одновременно начать закрытие. В этом случае обычное закрытие соединения завершается после отправки каждым из партнеров сообщения ACK. Каждая из сторон может запросить *внезапное завершение соединения* (*abrupt close*). Это допустимо, когда приложение желает завершить соединение или когда TCP обнаруживает серьезную коммуникационную проблему, которую не может разрешить собственными средствами. Внезапное завершение запрашивается посылкой партнеру одного или нескольких сообщений *Сброс* (*Reset – RST*), что указывается соответствующим флагом в заголовке TCP (флаги будут описаны далее).

Протокол TCP реализует механизмы управления потоком поступающих хосту-приемнику данных с целью предотвращение переполнения пакетами входного буфера. Во время установки соединения каждый из партнеров выделяет пространство памяти для входного буфера соединения и уведомляет об этом противоположную сторону. *Приемное окно* (*Receive Window*) – это пространство во входном буфере, ещё не занятое данными. Освобождение буфера от принятых данных выполняет приложение получателя. Этот процесс зависит от производительности и загруженности процессора хоста получателя (причем не только обработкой данных TCP соединения). Каждый посланный приемником ACK содержит сведения о текущем состоянии приемного окна в поле *Окно* (*Window*), в зависимости от которого регулируется поток данных от источника. Обычно подтверждения ACK высылаются не на каждый пересланный сегмент, а на непрерывный блок из нескольких сегментов, собранный в приемном окне. Это позволяет не отбрасывать пришедшие не по порядку сегменты, а упорядочивать их в соответствии с последовательными номерами и размерами сегментов.

В некоторых случаях требуется пересылка сегментов, размер которых меньше MSS (например, при работе в командном режиме, когда каждый пакет содержит только байты одной команды). Для этого используется так называемое *выталкивание* (*Push*) *данных из выходного буфера*, при этом отправителем в заголовке TCP выставляется флаг Push.

Также TCP может пересылать в сегменте *срочные данные* (*Urgent Data – URG*) вместе с другими данными. В этом случае сегмент маркируется флагом URG, а двухбайтовое поле Указатель срочности содержит смещение в байтах, которое должно быть добавлено к значению SEQ# заголовка TCP для получения SEQ# последнего байта срочных данных в данном сегменте. Принимающее приложение должно быть в состоянии определить, когда появится указатель срочности. Приложение находится в *режиме срочности* (*Urgent Mode*) все время, пока читает данные с текущей позиции до указателя срочности. После того как указатель срочности принят, приложение возвращается в нормальный режим. Примером использования режима срочности является ситуация, когда пользователь прерывает загрузку данных, при этом в поток передаваемых данных вставляется команда, на которую указывает указатель срочности и которую должно распознать и обработать приложение.

Описанные механизмы поддерживаются значениями полей заголовка TCP, формат которого приведен на рис. 116.

Поля *Порт источника* (отправителя) и *Порт назначения* (получателя) содержат 16 битовые значения портов, указывающих на области памяти с приложениями отправителя и получателя соответственно.

Поле *Порядковый номер* содержит 32-битовые значение номера первого байта данного сегмента, начиная от ISN. Поле *Номер подтверждения* содержит значение последовательного номера, ожидаемого от противоположной стороны следующим.


Рис. 116. Заголовок TCP

Четырёхбитовое поле *Длина заголовка* содержит размер заголовка в четырёхбайтовых словах (если заголовок не содержит опций, то его размер равен 5 × 4 байта = 20 байт).

Следующие 6 бит за полем длины заголовка зарезервированы и обычно равны 0.

Поле флагов TCP содержит шесть однобитовых флагов, передающих назначение пакета:

- URG – устанавливается в единицу для данных, которые должны быть обработаны получателем срочно, в этом случае в поле *Указатель срочности* указывается последний байт срочных данных;
- ACK – устанавливается в единицу для сегментов, выполняющих подтверждение принятых сегментов (на практике для всех пакетов TCP-сеанса, кроме первого);
- PSH – устанавливается в единицу приложением, отправляющим данные, чтобы указать TCP, что нужно отправлять данные из выходного буфера, не дожидаясь его заполнения до максимального размера сегмента;
- RST – устанавливается в единицу для завершения сеанса в связи с ошибкой или внештатной ситуацией;

- SYN – устанавливается в единицу при установлении соединения;
- FIN – устанавливается в единицу при нормальном завершении соединения.

Поле *Окно* предназначено для указания текущего размера окна входного буфера получателя.

*Контрольная сумма* вычисляется как 16-битовое дополнение до единицы суммы дополнений до единицы всех 16-битовых слов псевдозаголовка, аналогичного псевдозаголовку UDP (рис. 110) (значение поля Протокол в случае TCP = 6) и заголовка TCP.

*Опции* TCP могут занимать целое число байт, в качестве примера опций можно привести опцию, передающую значение MSS при установке соединения. Заголовок TCP должен заканчиваться на 32-битной границе, для этого может использоваться заполнение нулями.

## Задание для самостоятельной работы

Наиболее простой способ исследовать сообщения ICMP – использование программы `ping`. Откройте окно командной строки (терминал) и подготовьте в нём команду `ping`, в качестве параметра которой укажите IP-адрес соседнего компьютера сети. Запустите анализатор протоколов *Wireshark* и настройте в нём фильтр на захват только ICMP-пакетов (для этого необходимо в окне, открытом командой Capture-Options в поле Capture Filter прописать `icmp`). Запустите анализатор на захват пакетов, перейдите в окно командной строки (терминала) и нажмите клавишу Enter, инициируя отправку `ping`-пакетов. Приведите в отчёт структуру ICMP-заголовка и значения его полей для эхо-запроса и эхо-ответа. Для расшифровки полей сообщений используйте описание стандарта на ICMP (RFC-792) [3].

Повторите эксперимент по захвату пакетов, но уже используйте программу `tracert` (`traceroute`), в качестве параметра которой укажите имя любого интернет-сервера (если администратор сети запретил пересылку ICMP-пакетов в Интернете, попробуйте в качестве целевого сервера использовать имя или IP-адрес компьютера из соседней с Вами сети/подсети). Фильтр в Wireshark должен оставаться таким же, поскольку сообщения `tracert` (`traceroute`) – это также ICMP-сообщения. Захватите последовательность ICMP-пакетов и приведите в отчёт значение поля TTL заголовка IP, структуру ICMP-заголовка и значения его полей для первых двух запросов, а также аналогичные параметры для ответов на эти запросы. Для расшифровки полей сообщений используйте описание стандарта на ICMP (RFC-792) [3].

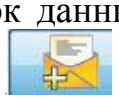
Для захвата пакетов с сообщениями ICMP о недостижимости адресата постройте в программе Cisco Packet Tracer сеть, приведенную на рис. 117 . Задайте конфигурацию хостам и маршрутизаторам, например такую, которая указана в табл. 8.

Таблица 8

Адресная информация сети, использующейся для исследования ICMP

| Название | IP-адрес | Маска | Шлюз | Примечание |
|---|---|---|---|---|
| PC0 | 192.168.1.1 | 255.255.255.0 | 192.168.1.254 | Отправитель пакетов |
| PC1 | 192.168.2.1 | 255.255.255.0 | 192.168.2.254 | Получатель пакетов |
| Router0-Fa0/0 | 192.168.1.254 | 255.255.255.0 | | Шлюз отправителя |
| Router0-Fa0/1 | 192.168.3.1 | 255.255.255.252 | | Связь между маршрутизаторами |
| Router1-Fa0/0 | 192.168.3.2 | 255.255.255.252 | | Связь между маршрутизаторами |
| Router1-Fa0/1 | 192.168.2.254 | 255.255.255.0 | | Шлюз получателя |

Если не сконфигурировать правило маршрутизации для Router0, из которого он понимал бы, что сеть 192.168.2.0/24 находится за Router1 и пакеты необходимо принимать именно ему, то при получении пакетов, направляемых в эту сеть, маршрутизатор не знает, куда их передавать. В этом случае он должен выслать отправителю ICMP-сообщение о недостижимости адресата.

Создайте расширенный протокольный блок данных (Complex PDU), выполнив щелчок на соответствующей кнопке  и заполнив информацию, помеченную на рис. 117 (здесь имитируется отправка сообщения протокола прикладного уровня *telnet*).

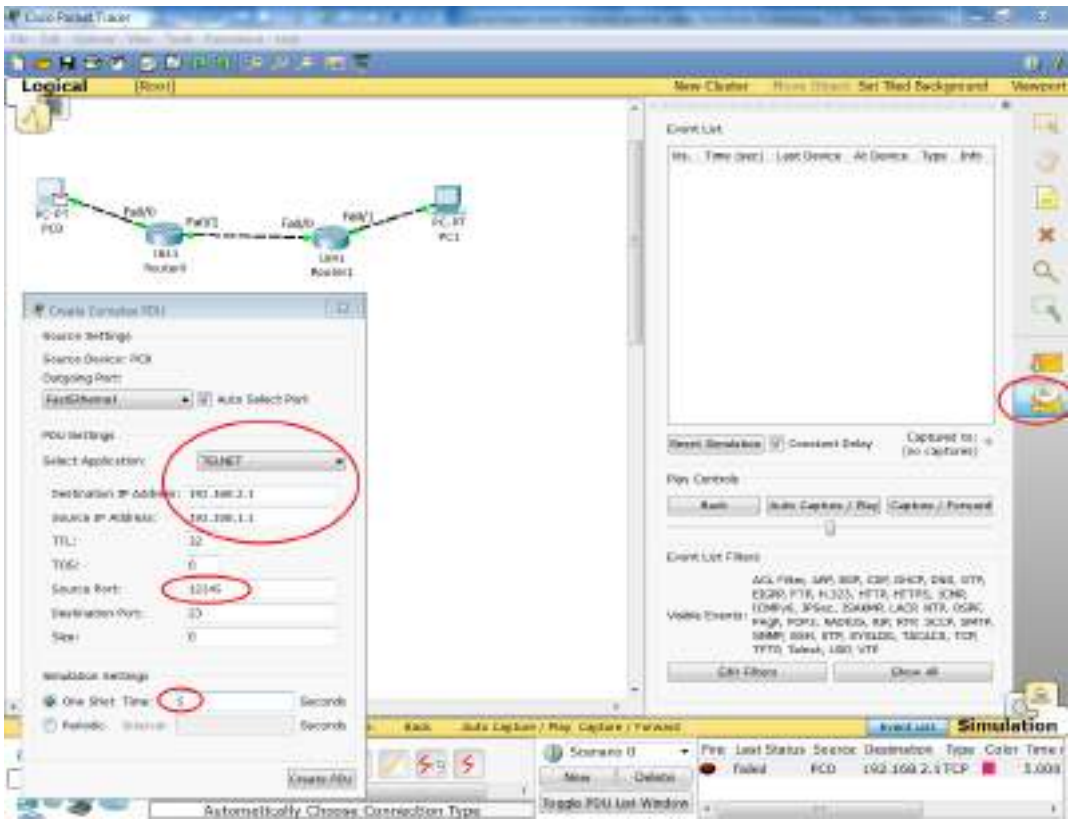



Рис. 117. Исследование ситуации, в которой адресат недостижим

Запустите симуляцию, выполнив щелчок по кнопке Auto Captire/Play, Вы увидите, что после получения пакета с сообщением *telnet* Router0 высылает

хосту ICMP-сообщение. Просмотрите его в виртуальном анализаторе протоколов, дважды выполнив щелчок по сообщению в списке Event List. Приведите в отчёт структуру и значения полей ICMP-заголовка.

Протокол транспортного уровня UDP используется, в частности, *системой доменных имен* (*Domain Name System – DNS*), позволяющей определять значение IP-адреса по доменному имени типа zhu.edu.ua. Сообщения DNS от хоста-клиента до DNS-сервера локальной сети и обратно обычно пересылаются в поле данных UDP-пакетов, поскольку обычно локальные сети считаются надёжными. В операционных системах Windows и Linux с установленным по умолчанию сетевым стеком TCP/IP имеется программа `nslookup`, позволяющая выполнять интерактивные запросы к DNS.

Откройте окно командной строки в Windows (либо окно терминала в Linux) и введите команду `nslookup <DNS-имя сервера>`, пока не нажимайте клавишу Enter (в качестве имени сервера может быть выбрано любое имя известного Вам, например, WWW-сервера). Запустите анализатор протоколов *Wireshark*, выполните команду Capture-Options и в открывшемся окне в поле Capture Filter: введите `udp` (то есть будут захватываться только кадры, содержащие UDP-пакеты). Нажмите на кнопку Start, перейдите в окно командной строки (терминала) и нажмите клавишу Enter. Выполните анализ захваченных кадров. Приведите в отчет дамп заголовка UDP-пакета и его расшифровку.

Ещё одним протоколом, использующим в качестве транспортного UDP, является *протокол динамического конфигурирования хоста* (*Dynamic Host Configuration Protocol – DHCP*), позволяющий, в частности, автоматически задавать узлам сети адресную информацию сетевого уровня (IP-адрес, маску подсети и т.д.). Мы сможем исследовать протокольные блоки данных, передаваемые этим протоколом путём моделирования в программе *Cisco Packet Tracer*. Для этого запустите программу и создайте в ней простейшую сеть, состоящую из сервера, соединённого с коммутатором и компьютера, пока не подсоединённого к коммутатору (рис. 118).

Выполните настройку адресной информации сервера, компьютер по умолчанию использует протокол DHCP (рис. 118). Выполните щелчок на команде Services в окне настроек сервера и выберите команду DHCP. В открывшемся окне Вы можете задать размер пула адресов с помощью параметров Start IP Address и SubnetMask (в примере на рис. 119 адрес пула начинается с `192.168.1.10` и заканчивается `192.168.1.254`, что составляет `246` адресов). Здесь также можно указать IP-адреса шлюза данной сети и локального DNS-сервера, в этом случае эти параметры также автоматически назначаются хостам сети.

Процедуру автоматического назначения адресной информации, а также протокольные передаваемые при этом блоки данных можно увидеть в режиме Simulation. Перейдите в этот режим и настройте фильтрацию только пакетов с DHCP-сообщениями в окне, открывающемся щелчком по кнопке Edit Filters (рис. 120).

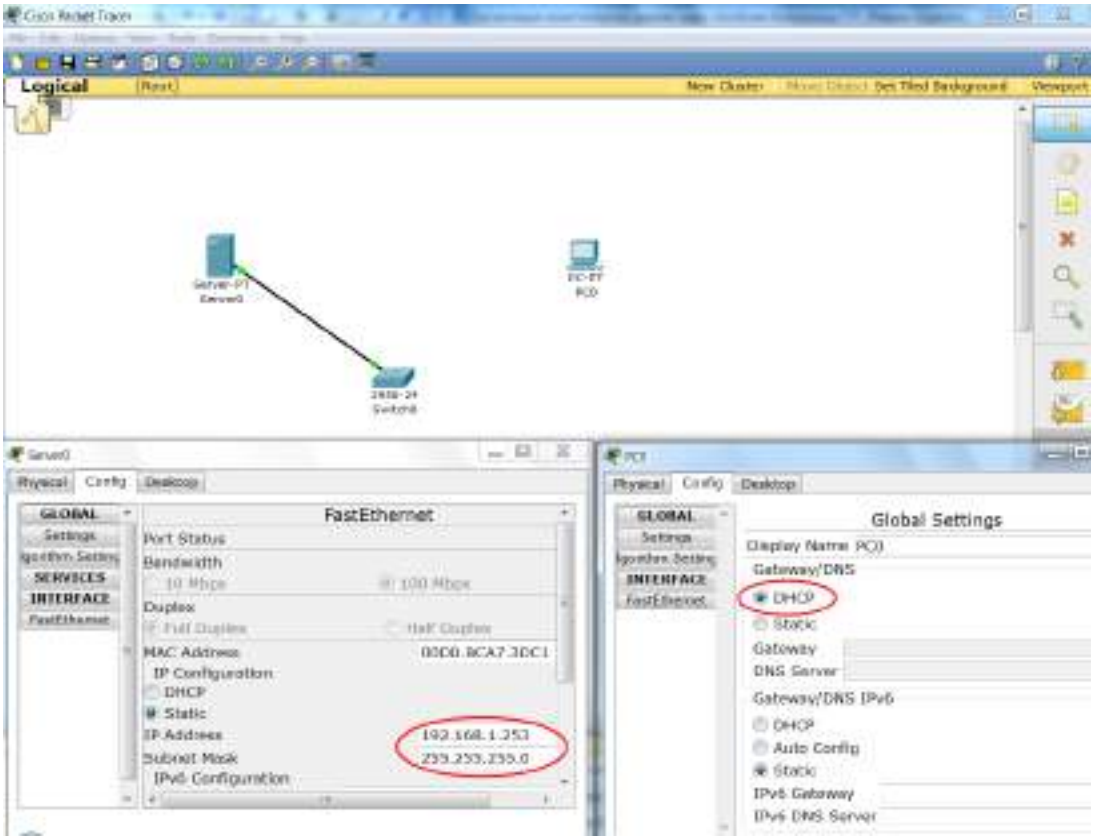



Рис. 118. Сеть с DHCP сервером

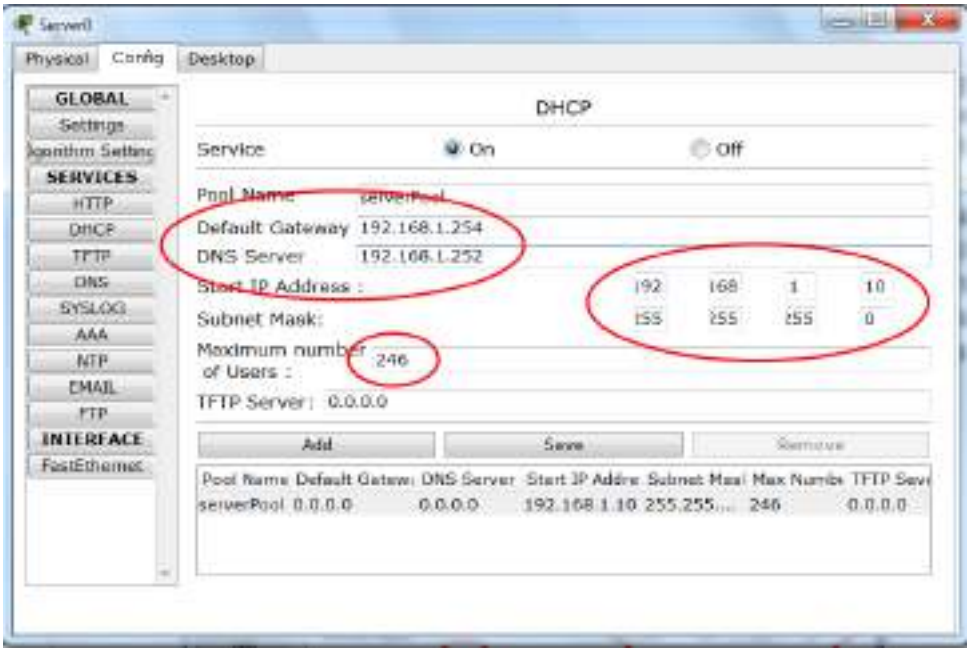



Рис. 119. Настройки DHCP сервера

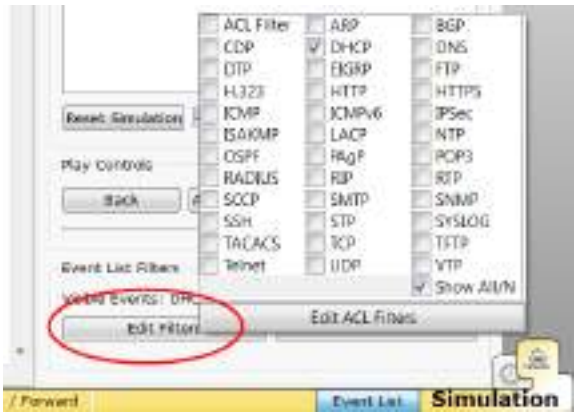



Рис. 120. Настройка фильтрации DHCP-сообщений

Далее подсоедините компьютер к коммутатору и запустите симуляцию, нажав кнопку Auto Capture/Play. После этого по сети будут переданы несколько пакетов с сообщениями DHCP между компьютером и сервером. Выполните щелчок по одному из них для просмотра структуры захваченного кадра (рис. 121).

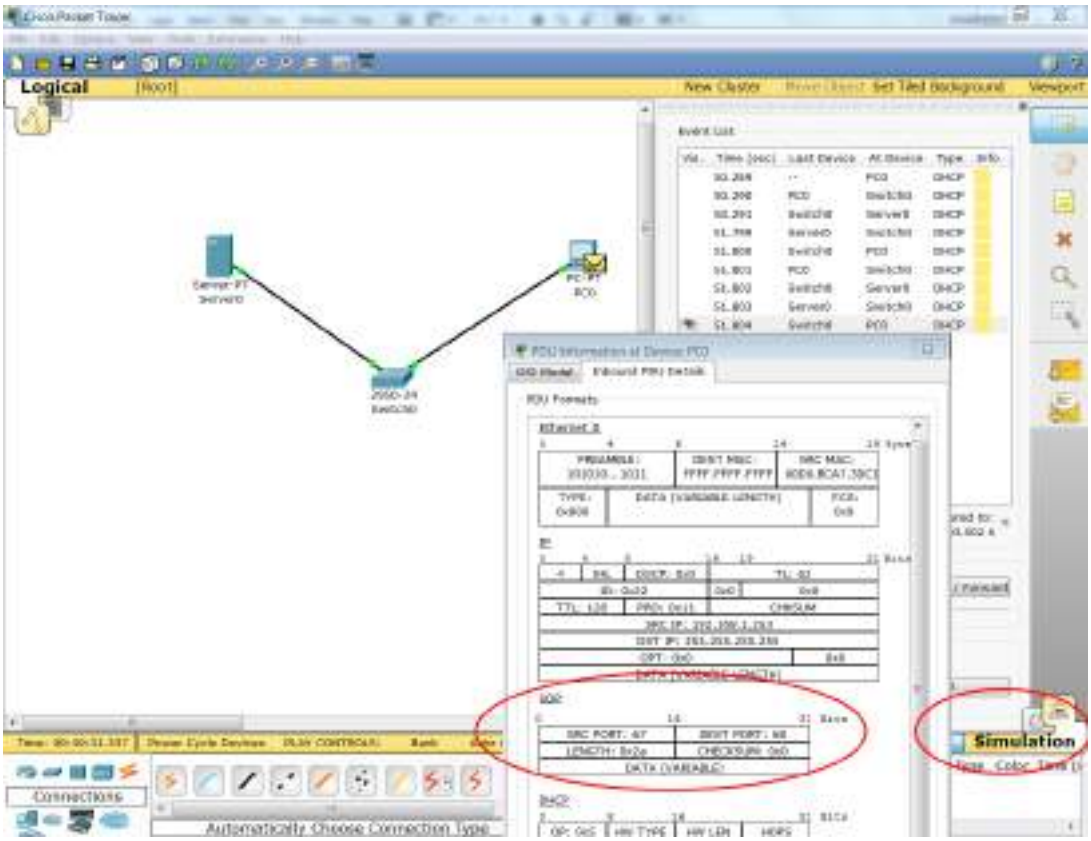



Рис. 121. Захват кадров с DHCP-сообщениями

Откройте окно с конфигурацией компьютера и убедитесь, что он автоматически получил адрес из сконфигурированного Вами пула.

Повторите описанный эксперимент, установив в качестве начального адреса пула адрес `192.168.1.X`, где `X` = Вашему порядковому номеру в журнале академгруппы. Приведите в отчёт заголовок UDP вместе с расшифровкой его полей.

Протокол транспортного уровня TCP используется большинством популярных протоколов прикладного уровня, в частности, при пересылке HTTP-пакетов между клиентами (браузерами) и HTTP-серверами (Web-серверами). Запустите программу-браузер и задайте в ней адрес любого сервера в Интернете, но пока не инициируйте соединение с ним (рекомендуется выбрать сервер с небольшим количеством информации на его главной странице, например, http://ya.ru).

Запустите программу анализатор протоколов *Wireshark* и настройте в ней фильтр для захвата пакетов TCP. Включите захват и инициируйте соединение с выбранным сервером в браузере. По окончании загрузки страницы остановите захват. Вы должны были захватить пакеты HTTP-сеанса, начиная с пакетов, устанавливающих соединение, и заканчивая пакетами, осуществляющими нормальное завершение соединения. Поскольку могли захватиться пакеты, направленные другим серверам, можно их отфильтровать, подав команду, оставляющую только пакеты, отправленные выбранному Вами серверу или полученные от него. Для этого необходимо из окна захваченных пакетов выяснить IP-адрес сервера (для http://ya.ru он `77.88.21.3`), ввести в поле Filter команду `ip.dst == 77.88.21.3 or ip.src == 77.88.21.3` и нажать кнопку Apply (рис. 122).

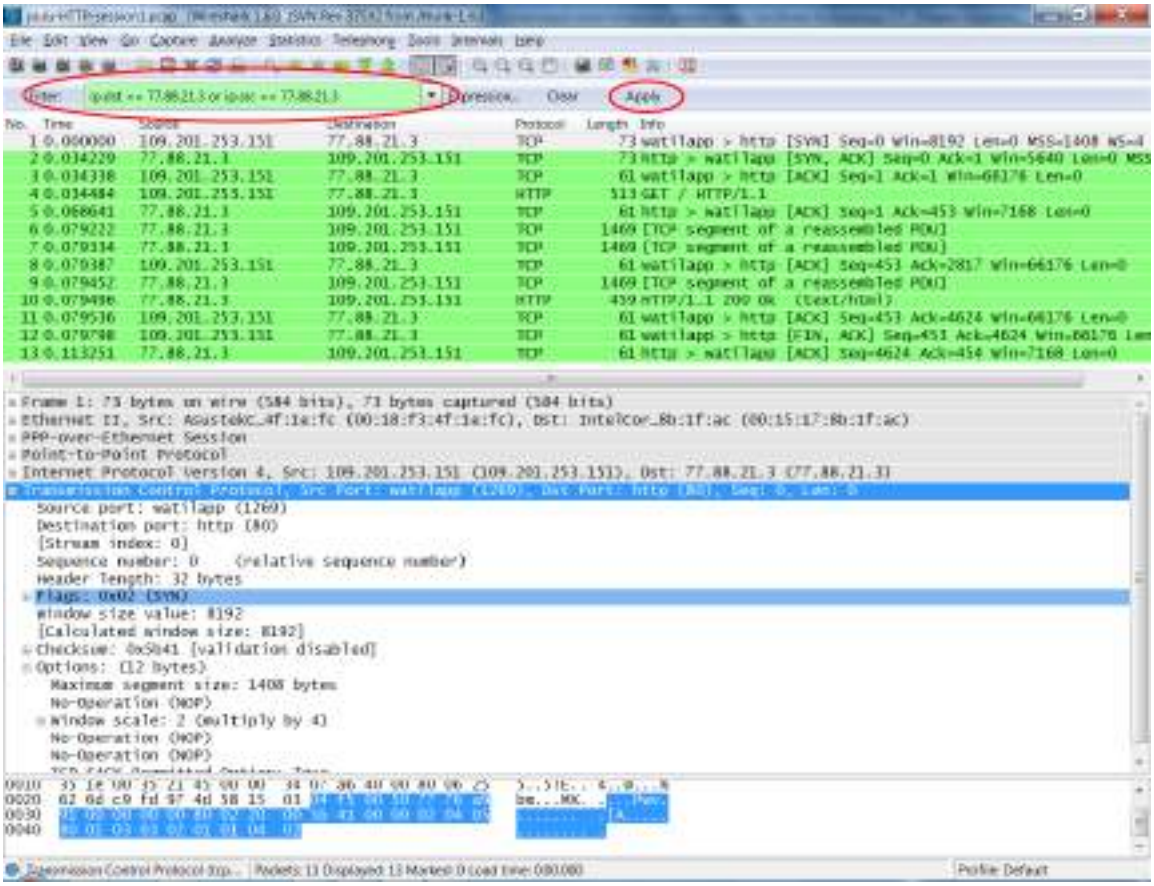



Рис. 122. Захват кадров с DHCP-сообщениями

Выполните анализ захваченных кадров, заполнив приведенную ниже таблицу, подставляя вместо данных примера свои данные (табл. 9).

Таблица 9

Данные TCP-сеанса

| **Клиент:** | | IP = 109.201.253.151 | | Порт = 1269 | | MSS = 1408 | |
|---|---|---|---|---|---|---|---|
| **Сервер:** | | IP = 77.88.21.3 | | Порт = 80 | | MSS = 1410 | |
| **№ пакета** | **Отправитель** | **Получатель** | **SEQ# hex** | **ACK# hex** | **Разность dec** | **Flags** | **Длина данных** |
| 1 | Клиент | Сервер | 7776A991 | 0 | | SYN | 0 |
| 2 | Сервер | Клиент | 2C815468 | 7776A992 | | SYN, ACK | 0 |
| 3 | Клиент | Сервер | 7776A992 | 2C815469 | | ACK | 0 |
| 4 | Клиент | Сервер | **7776A992** | 2C815469 | **453** | PSH, ACK | **453** |
| 5 | Сервер | Клиент | 2C815469 | **7776AB56** | | ACK | 0 |
| 6 | Сервер | Клиент | 2C815469 | 7776AB56 | | ACK | 1408 |
| … | | | | | | | |

В поля SEQ# и ACK# вводите не относительные номера, которые предлагает *Wireshark* в окне анализа структуры заголовков, а абсолютные значения этих параметров из дампа. Рассчитайте для пакетов с ненулевым размером поля данных разность ACK# следующего пакета с противоположной стороны и SEQ# текущего пакета. Учитывая, что SEQ# является номером первого байта текущего сегмента, добавьте к полученному значению единицу, переведите в десятичную систему и запишите результат в столбец Разность.

Пример в таблице: $7776AB56_{н}$ - $7776A992_{н}$ = $1C4_{н}$ + 1 = $1C5_{н}$ = $453_{10}$.

Укажите в отчёте диапазон номеров пакетов, устанавливающих TCP-соединение, передающих данные в этом соединении и завершающих его.

## Вопросы для самоподготовки

1. Назовите назначение портов транспортного уровня и приведите примеры портов.
2. Назовите диапазон портов, закреплённый за стандартными серверными службами.
3. Приведите примеры портов служб, обычно использующих UDP и портов служб, обычно использующих TCP.
4. Назовите сходство и отличие функций протоколов UDP и TCP.
5. Что называют адресом сокет? Назовите команду, позволяющую отобразить пары сокетов, образующих коммуникации.
6. Опишите заголовок UDP. Как вычисляется контрольная сумма заголовка?
7. Перечислите механизмы обеспечения протоколом TCP надежности передачи данных.
8. Что называют максимальным размером сегмента и как он рассчитывается?
9. Опишите алгоритм позитивного подтверждения с ретрансляцией и его использование TCP.
10. Опишите процедуру установления соединения протоколом TCP. Какие поля заголовка транспортного уровня при этом задействованы?

11. Опишите алгоритмы передачи данных и завершения соединения протоколом TCP. Какие поля заголовка транспортного уровня при этом задействованы?
12. Каким образом протокол TCP может регулировать поток поступающих хосту-получателю данных?
13. Опишите механизмы выталкивания данных из выходного буфера и пересылки срочных данных, поддерживаемых TCP. Приведите примеры их использования.
14. Опишите формат заголовка TCP.

## Тесты для контроля усвоения знаний

1. В пакете, пересылаемом в локальной сети порт отправителя = 80, порт получателя = 24561. Выберите из списка тип протокола и привязку портов к клиенту и серверу:
   а) протокол UDP, отправитель – сервер, получатель – клиент;
   б) протокол UDP, отправитель – клиент, получатель – сервер;
   в) протокол TCP, отправитель – сервер, получатель – клиент;
   г) протокол TCP, отправитель – клиент, получатель – сервер.
2. Выберите, что характеризует порт транспортного уровня:
   а) порт сетевого адаптера, через который хост работает с сетью;
   б) область памяти, связанную с сетевым приложением;
   в) порт ввода-вывода, закреплённый за сетевым адаптером.
3. Выберите соответствия для названий стандартных служб и закреплённых за ними номеров портов: а) 80, б) 21, в) 67, г) 53, д) 25:
   - FTP – …;
   - HTTP – …;
   - DNS – …;
   - DHCP – …;
   - SMTP – ….
4. Команда `netstat -an` вывела на экран следующие строки. Укажите, какие из них описывают сокеты установленного соединения:
   а) `TCP 0.0.0.0:135 0.0.0.0:0 LISTENING;`
   б) `TCP 109.201.253.151:3603 74.125.39.104:80 ESTABLISHED;`
   в) `TCP 109.201.253.151:54035 62.165.4.118:33016 TIME_WAIT;`
   г) `TCP 109.201.253.151:54035 90.176.90.125:11740 SYN_RECEIVED.`
5. Укажите десятичное значение, идентифицирующее UDP в поле Протокол IP-заголовка:
   а) 01;
   б) 06;
   в) 17.
6. Укажите поля, которые входят в псевдозаголовок, используемый при расчёте контрольной суммы UDP или TCP:
   а) MAC-адрес отправителя;
   б) MAC-адрес получателя;

в) IP-адрес отправителя;
г) IP-адрес получателя;
д) порт отправителя;
е) порт получателя;
ж) идентификатор протокола;
з) длина пакета с заголовком.

7. Выберите, чему равняется максимальный размер сегмента для заголовка Ipv4 без опций и заголовка TCP длиной 28 байт:
   а) 1452 байта;
   б) 1460 байт;
   в) 1472 байта;
   г) 1500 байт.
8. TCP-пакет с полем данных 500 байт имеет десятичное значение SEQ#=15246, а десятичное значение ACK#=32412. Выберите, какими будут десятичные значения этих полей в ответе на данный пакет, если в нём пересылается 300 байт данных:
   а) SEQ#=15746, ACK#=32712;
   б) SEQ#=32712, ACK#=15746;
   в) SEQ#=15747, ACK#=32713;
   г) SEQ#=15745, ACK#=32711
9. Из захваченных пакетов сеанса TCP извлечены три пакета с флагами:
   а) PSH, ACK;
   б) SYN;
   в) FYN, ACK;
   г) SYN, ACK.

   Укажите, какие из них относятся к:
   - пакетам, устанавливающим соединение, – …;
   - пакетам, передающим данные в сеансе, – …;
   - пакетам, завершающим соединение, – ….
10. Выберите название поля заголовка TCP, позволяющего регулировать поток данных с противоположной стороны соединения:
    а) Длина заголовка;
    б) Окно;
    в) Контрольная сумма;
    г) Указатель срочности.

## Литература

1. Стивенс У.Р. Протоколы TCP/IP. Практическое руководство / У.Р. Стивенс. СПб. 2003. – 672 с.

2. TCP/IP: Архитектура, протоколы, реализация / Сидни Фейт – 2-е изд. – McGraw-Hill, 2000. – 424 с.

3. Амато В. Основы организации сетей Cisco : пер. с англ. / В. Амато. – М. : Вильямс, 2004. – 512 с.

4. Усманов Р. Протокол UDP [электронный ресурс] / Р. Усманов. – режим доступа: http://citforum.ru/internet/tifamily/ udpspec.shtml.

5. Усманов Р. Протокол TCP [электронный ресурс] / Р. Усманов. – режим доступа: http://www.citforum.ru/nets/tcp/tcpspec.shtml.

# СЛОВАРЬ ТЕРМИНОВ

## A

**ACL** (Access Control List – список контроля доступа) – список, который определяет, кто или что может получать доступ к конкретному объекту и какие именно операции разрешено или запрещено этому субъекту проводить над объектом.

**ARP** (Address Resolution Protocol – протокол определения адреса) – используется в компьютерных сетях для определения адреса канального уровня по известному адресу сетевого уровня.

**ASCII** (American Standard Code for Information Interchange) – американский стандартный код для обмена информацией. ASCII представляет собой 8-битную кодировку для представления десятичных цифр, латинского и национального алфавитов, знаков препинания и управляющих символов.

## C

**CISCO IOS** (Internetwork Operating System – Межсетевая операционная система) – программное обеспечение, используемое в маршрутизаторах Cisco и некоторых сетевых коммутаторах. Cisco IOS – многозадачная операционная система, выполняющая функции сетевой организации, маршрутизации, коммутации и передачи данных.

## D

**DHCP** (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

**DNS** (Domain Name System – система доменных имён) – компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста.

## E

**ETHERNET** – пакетная технология передачи данных преимущественно локальных компьютерных сетей. Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде – на канальном уровне модели OSI. Скорость передачи данных в классической Ethernet составляла 10 Мбит/с. Наследованные технологии – Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1 Гбит/с), 10 Gigabit Ethernet (10 Гбит/с), 40/100 Gigabit Ethernet (40/100 Гбит/с).

## H

**HTTP** (HyperText Transfer Protocol – протокол передачи гипертекста) – протокол прикладного уровня передачи данных. Основой HTTP является технология «клиент – сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получе-

ния запроса, производят необходимые действия и возвращают обратно сообщение с результатом. HTTP в настоящее время повсеместно используется во Всемирной паутине для получения информации с Web-сайтов.

**I**

**ICMP –** (Internet Control Message Protocol – протокол управляющих сообщений Интернет) – 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, хост или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

**IEEE – ИНСТИТУТ ИНЖЕНЕРОВ ПО ЭЛЕКТРОТЕХНИКЕ И ЭЛЕКТРОНИКЕ** (Institute of Electrical and Electronics Engineers) – международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов радиоэлектроники и электротехники, компьютерной техники и компьютерных сетей.

**IEEE 802.11 –** набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4; 3,6 и 5 ГГц. Пользователям более известен по названию Wi-Fi, фактически являющимся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance. Получил широкое распространение благодаря развитию в мобильных электронно-вычислительных устройствах: КПК и ноутбуках. Скорость передачи данных 1 – 2 Мбит/с в полосе частот в области 2,4 ГГц. Наследованные технологии 802.11a (54 Мбит/с 5 ГГц), 802.11b (11 Мбит/с 2,4 ГГц), 802.11g (54 Мбит/с 2,4 ГГц), 802.11n (до 600 Мбит/с 2,4 ГГц и 5 ГГц).

**INTERNET PROTOCOL (IP) –** маршрутизируемый сетевой протокол, протокол сетевого уровня сетевого стека TCP/IP. Протокол IP используется для негарантированной доставки данных, разделяемых на так называемые пакеты от одного узла сети к другому.

**IP-АДРЕС (INTERNET PROTOCOL ADDRESS) –** уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети. Для IP версии 4 имеет длину 4 байта.

**M**

**MAC-АДРЕС (**Media Access Control – управление доступом к среде) – уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей на уровне оборудования.

**MTU** (Maximum Transmission Unit) – максимальный размер блока (в байтах), который может быть передан на канальном уровне сетевой модели OSI.

**MULTICAST** (групповая передача) – специальная форма широковещания, при которой сетевой пакет одновременно направляется определённому подмножеству адресатов – не одному (unicast) и не всем (broadcast).

**N**

**NTFS (**New Technology File System**)** – файловая система, использующая механизмы управления доступом к файловым ресурсам по идентификаторам пользователей/групп и спискам разрешений на операции с этими ресурсами.

**P**

**PDU** (Protocol Data Unit – "протокольная единица данных") – обобщённое название фрагмента данных на разных уровнях модели OSI: кадр Ethernet, IP-пакет, UDP-дейтаграмма, TCP-сегмент и т.д.

**T**

TCP (Transmission Control Protocol – протокол управления передачей) – один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP. Выполняет функции протокола транспортного уровня модели OSI. TCP – это транспортный механизм, предоставляющий поток данных, с предварительной установкой соединения, за счёт этого дающий уверенность в достоверности получаемых данных, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета. В отличие от UDP гарантирует, что приложение получит данные точно в такой же последовательности, в какой они были отправлены, и без потерь.

**TCP/IP** (Transmission Control Protocol/Internet Protocol – протокол управления передачей/интернет-протокол) – стек сетевых протоколов, являющийся основным стеком для работы Интернета, основан на модели сетевого взаимодействия DOD и включает в себя протоколы четырёх уровней: прикладного (application), транспортного (transport), сетевого (network), канального (data link).

**U**

**UDP** (User Datagram Protocol – протокол пользовательских дейтаграмм) – это транспортный протокол для передачи данных в сетях IP без установления соединения. Он является одним из самых простых протоколов транспортного уровня модели OSI. В отличие от TCP, UDP не гарантирует доставку пакета, поэтому аббревиатуру иногда расшифровывают как Unreliable Datagram Protocol (протокол ненадёжных дейтаграмм). Это позволяет ему гораздо быстрее и эффективнее доставлять данные для приложений, которым требуется большая пропускная способность линий связи, либо требуется малое время доставки данных.

**V**

**VLAN** (Virtual Local Area Network) – виртуальная локальная компьютерная сеть – представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся

в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

**W**

**WI-FI** (Wireless Fidelity – «беспроводная точность») – торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

**Д**

**Дейтаграмма** (datagram) – блок информации, посланный как пакет сетевого уровня через передающую среду без предварительного установления соединения и создания виртуального канала.

**К**

**КАДР** (Frame) – единица передачи данных на канальном уровне эталонной модели взаимодействия открытых систем (OSI).

**КЛИЕНТ (ПРОГРАММА) –** программное обеспечение, позволяющее компьютеру обращаться к сетевым ресурсам серверов компьютерных сетей: файловым ресурсам, принтерам, каналам доступа к Интернет.

**КОМПЬЮТЕРНАЯ СЕТЬ (ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ, СЕТЬ ПЕРЕДАЧИ ДАННЫХ) –** система связи компьютеров и/или компьютерного оборудования (серверы, маршрутизаторы и другое оборудование). Для передачи информации могут быть использованы различные физические явления, как правило, различные виды электрических сигналов, световых сигналов или электромагнитного излучения.

**КОММУТАТОР ЛОКАЛЬНОЙ СЕТИ (SWITCH) –** активное сетевое оборудование, осуществляющее передачу кадров с одного своего порта на другой, основываясь на анализе MAC-адресов в их заголовках.

**КОНТРО́ЛЬНАЯ СУ́ММА** (Frame Check Sequence – FCS) – некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Так же контрольные суммы могут использоваться для быстрого сравнения двух наборов данных на неэквивалентность: с большой вероятностью различные наборы данных будут иметь неравные контрольные суммы.

**КОНЦЕНТРАТОР (HUB) –** активное сетевое оборудование, осуществляющее передачу сигналов со своего входящего порта на все остальные порты.

**КРОССПЛАТФОРМЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ** – программное обеспечение, работающее более чем на одной аппаратной платформе и/или операционной системе.

**Л**

**ЛОКАЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ (LOCAL AREA NETWORK – LAN) –** набор компьютеров (часто называемых *рабочими станциями*

(*Workstation*)), серверов, сетевых принтеров, коммутаторов (Switch), маршрутизаторов (Router), точек доступа (Access Point), другого оборудования, а также соединяющих их кабелей, обычно расположенных на относительно небольшой территории или в небольшой группе зданий (учебный класс, квартира, офис, университет, дом, фирма, предприятие).

**М**

**МАСКА ПОДСЕТИ (SUBNET MASK) –** битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети.

**МАРШРУТИЗА́ТОР** (router) **–** сетевое устройство, пересылающее пакеты данных между различными сегментами сети и принимающее решения на основании информации о топологии сети и определённых правил, заданных администратором. Маршрутизатор работает на сетевом уровне сетевой модели OSI.

**МАРШРУТИЗАЦИЯ** (Routing) **–** процесс определения маршрута следования информации в сетях связи. Маршруты могут задаваться административно (статические маршруты), либо вычисляться с помощью алгоритмов маршрутизации, базируясь на информации о топологии и состоянии сети, полученной с помощью протоколов маршрутизации (динамические маршруты).

**МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ (OPEN SYSTEM INTERCONNECTION – OSI) –** абстрактная семиуровневая сетевая модель для коммуникаций и разработки сетевых протоколов.

**Н**

**НЕЭКРАНИРОВАННАЯ ВИТАЯ ПАРА (UNSHIELDED TWISTED PAIR – UTP) –** популярная среда передачи данных в сети, представляющая собой свитые попарно четыре пары проводов.

**О**

**ОДНОРА́НГОВАЯ ИЛИ ПИ́РИНГОВАЯ** (Peer-To-Peer, P2P **–** равный к равному) **СЕТЬ –** компьютерная сеть, основанная на равноправии участников. В такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером.

**П**

**ПАКЕТ (СЕТЕВОЙ) –** это отформатированный блок данных, передаваемых по сети в пакетном режиме.

**ПОЛНОДУПЛЕКСНЫЙ РЕЖИМ** – режим, при котором передача и приём данных происходят одновременно.

**ПОЛУДУПЛЕКСНЫЙ РЕЖИМ –** режим, при котором передача и приём данных происходят по очереди.

**ПОРТ** (TCP/IP) **–** в протоколах TCP и UDP (семейства TCP/IP) порт **–** идентифицируемый номером системный ресурс, выделяемый приложению, выполняемому на некотором сетевом хосте, для связи с приложениями, выполняемыми на других сетевых хостах (в том числе с другими приложениями на этом же хосте). Для каждого из протоколов TCP и UDP

стандарт определяет возможность одновременного выделения на хосте до 65536 уникальных портов, идентифицирующихся номерами от 0 до 65535. При передаче по сети номер порта в заголовке пакета используется (вместе с IP-адресом хоста) для адресации конкретного приложения (и конкретного, принадлежащего ему, сетевого соединения).

## С

**СЕТЕВАЯ СЛУЖБА –** программное обеспечение, работающее на сервере и обеспечивающее обслуживание клиентских запросов к сетевым ресурсам этого сервера.

**СЕТЕВОЙ АДАПТЕР (СЕТЕВАЯ ПЛАТА, СЕТЕВАЯ КАРТА, NETWORK INTERFACE CARD – NIC) –** периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети. В настоящее время, особенно в персональных компьютерах, сетевые платы довольно часто интегрированы в материнские платы для удобства и удешевления всего компьютера в целом.

**СЕТЕВОЙ ПРОТОКОЛ –** программное обеспечение, реализующее набор правил, позволяющих осуществлять соединение и обмен данными между двумя и более подключёнными к сети устройствами. Основными задачами протоколов являются разбиение потока информации на пакеты, формирование заголовков пакетов с адресной и другой информацией, позволяющей реализовывать различные механизмы протоколов по надёжной доставке данных, обеспечению целостности данных, безопасности передачи и др. Обязательным условием работы сети является наличие одинаковых стеков сетевых протоколов на компьютерах – участниках сети.

**СО́КЕТ** (socket – углубление, гнездо, разъём) – название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене могут исполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой сетью. Сокет – абстрактный объект, представляющий конечную точку соединения. В TCP/IP сокет определяется IP-адресом хоста и портом, являющимся конечной точкой коммуникации.

**СТЕК СЕТЕВЫХ ПРОТОКОЛОВ –** набор сетевых протоколов разных уровней модели сетевого взаимодействия, используемых в сетях.

## Т

**ТОЧКА ДОСТУПА (ACCESS POINT)** – активное сетевое оборудование, организующее радиоканалы между участниками беспроводной сети.

## Х

**ХОСТ** (от англ. host – хозяин , принимающий гостей) – любой компьютер, сервер, подключённый к локальной или глобальной сети.

## Ш

**ШИРОКОВЕЩАНИЕ** (broadcasting) – метод передачи данных в компьютерных сетях, при котором поток данных (каждый переданный пакет в случае пакетной передачи) предназначен для приёма всеми участниками сети.

**ШЛЮЗ ОСНОВНОЙ (GATEWAY) –** точка сети, которая служит выходом в другую сеть.

# РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА


1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с.: ил.
2. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – 4-е изд. – СПб. : Питер, 2009. – 992 с.
3. Новиков Ю.В. Основы локальных сетей: курс лекций : учеб. пособие: для студентов вузов, обучающихся по специальностям в обл. информ. технологий / Ю.В. Новиков, С.В. Кондратенко. – М.: Интернет-ун-т информ. технологий, 2005. – 360с.
4. Гук М. Аппаратные средства локальных сетей. Энциклопедия / М. Гук. – СПб. : Питер, 2000. – 576 с.
5. TCP/IP: Архитектура, протоколы, реализация / Сидни Фейт – 2-е изд. – McGraw-Hill, 2000. – 424 с.
6. Стивенс У.Р. Протоколы TCP/IP. Практическое руководство / У.Р. Стивенс. СПб. 2003. – 672 с.
7. Амато В. Основы организации сетей Cisco : пер. с англ. / В. Амато. – М. : Вильямс, 2004. – 512 с.
8. Мак-Федрис П. Microsoft Windows 7. Полное руководство / П.Мак-Федрис. – М. : Вильямс, 2010. – 800 с.
9. Официальный сайт Windows 7. Раздел Помощь - Интернет, электронная почта и локальная сеть [электронный ресурс]. – режим доступа: http://windows.microsoft.com/ru-RU/windows7/help/ networking-e-mail-getting-online.
10. Усманов Р. Протокол IP [электронный ресурс] / Р. Усманов. – режим доступа: http://www.citforum.ru/nets/tcp/ipspec.shtml.
11. Усманов Р. Протокол UDP [электронный ресурс] / Р. Усманов. – режим доступа: http://citforum.ru/internet/tifamily/ udpspec.shtml.
12. Усманов Р. Протокол TCP [электронный ресурс] / Р. Усманов. – режим доступа: http://www.citforum.ru/nets/tcp/tcpspec.shtml.
13. Официальный сайт ASPLinux [электронный ресурс]. – режим доступа: http://www.asplinux.ru/.
14. Официальный сайт программы-анализатора сетевых протоколов Wireshark [электронный ресурс]. – режим доступа: http://www.wireshark.org.
15. Официальный сайт Cisco Systems. Программа Cisco Packet Tracer [электронный ресурс]. – режим доступа: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html.

# ПРИЛОЖЕНИЕ А

**Модель взаимодействия открытых систем – Open System Interconnect**

*Принцип передачи данных по сети* состоит в том, что файл (или сообщение), которые представляют собой совокупность байт, пересылается порциями конечной длины последовательных бит, составляющих байт. Файлы разделяются на более мелкие объекты с целью эффективного использования каналов передачи данных: а) за счет предотвращения использования канала только двумя участниками и б) за счет минимизации объема повторной передачи в случае ошибки в принятой части файла. Последовательные биты обрамляются управляющей информацией (в частности адресами источника и приёмника данных) и контрольной суммой (которая позволяет контролировать правильность передачи данных), создавая структуры данных, называемые *кадрами*. Кадры обычно вкладываются в сетевые *пакеты*, которые, в свою очередь, добавляют к кадру заголовок с управляющей информацией. Использование пакетов позволяет передавать данные в гетерогенных разветвленных сетях. Пакеты переносят сегменты данных и сообщения со своей управляющей информацией.

Организация сетевого взаимодействия представляет собой сложную задачу. Для ее решения используют *декомпозицию* на подзадачи, включая функциональное описание уровней, решающих эти подзадачи, и описание связей между соседними уровнями. В начале 80-х гг. прошлого века несколько международных организаций по стандартизации (*Международная организация по стандартизации – International Standard Organization* (*ISO*), *Международный телекоммуникационных союз – International Telecommunications Unit* (*ITU*) и ряд других) разработали модель сетевого взаимодействия, названную *моделью взаимодействия открытых систем* (*Open System Interconnect – OSI*). В этой модели все задачи сетевого взаимодействия систем сгруппированы на семи уровнях и определено функциональное взаимодействие соседних уровней иерархии. На рис. А1 приведены названия уровней и схема их взаимодействия. Ключевым моментом модели при передаче данных является добавление заголовка со служебной информацией к блоку данных, поступившему от вышележащего уровня (или от приложения, отправляющего эти данные), и передача полученного блока данных с заголовком текущего уровня нижележащему уровню. При этом структуры данных вышележащих уровней *вкладываются* (*инкапсулируются*) в поля данных структур текущих уровней. Поскольку блоки данных различных уровней называют по-разному (пакеты, кадры, сегменты, сообщения и др.), удобным является введение для них общего названия – *протокольный блок данных* (*Protocol Data Unit – PDU*). При получении информации происходит передача полученных PDU снизу вверх, при этом текущий уровень анализирует информацию в соответствующем этому уровню заголовке, после чего отбрасывает заголовок, обрабатывает блок данных в соответствии с полученной служебной информацией и передаёт обработанный блок вышележащему уровню для аналогичной обработки.

При этом происходит *извлечение* (*декапсуляция*) блоков данных вышележащих уровней с PDU текущего уровня. Верхний уровень после декапсуляции получает данные, переданные отправителем, которые он передаёт сетевому приложению получателя.

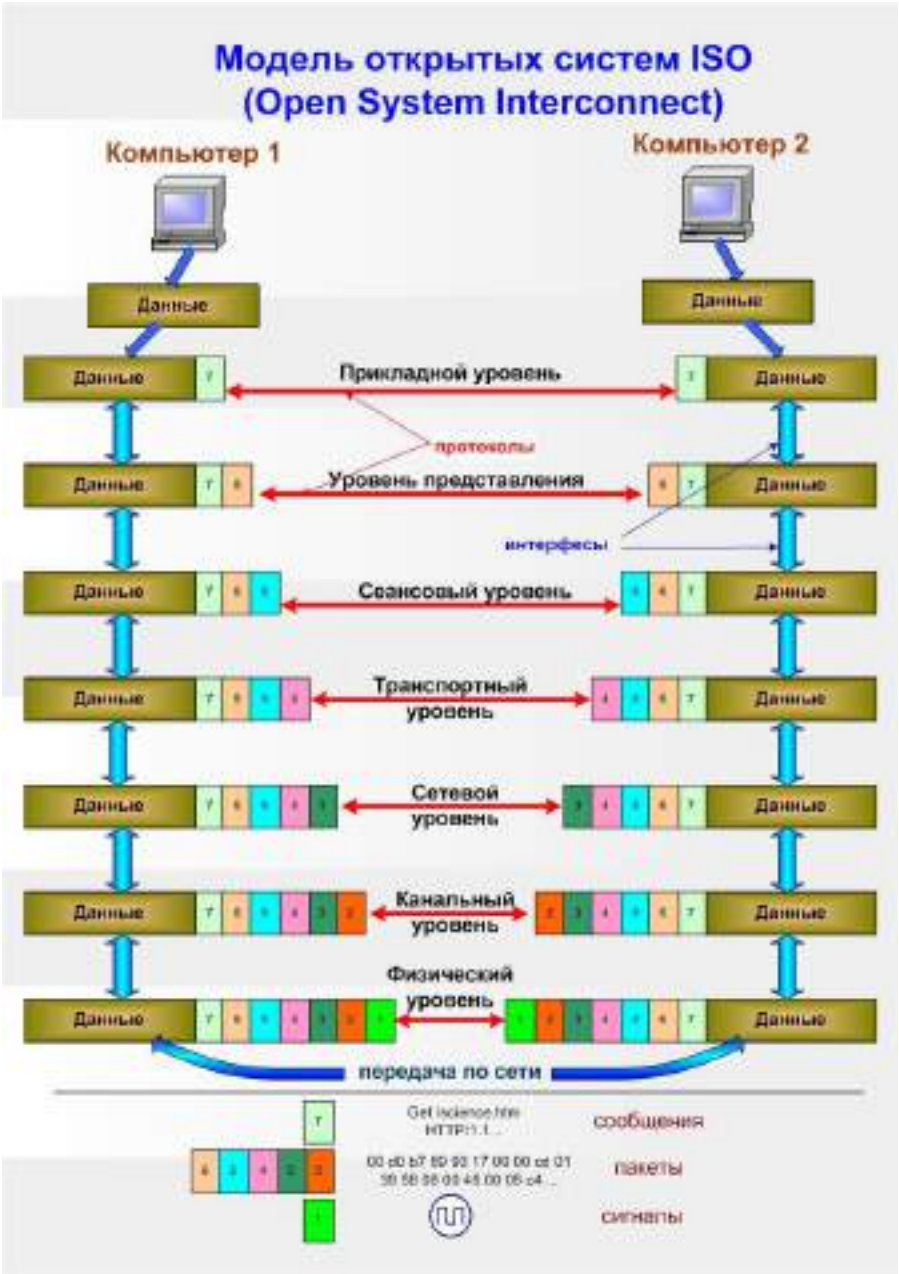



Рис. А1. Модель взаимодействия открытых систем ISO/OSI

Набор правил, определяющих взаимодействие одинаковых уровней на стороне отправителя и получателя, называется *коммуникационным протоколом*. Протоколы предусматривают определенный формат заголовка для PDU текущего уровня и передаваемую в нем служебную информацию, допустимый размер PDU, типы преобразований над данными, выполняемые на этом уровне, и алгоритмы таких преобразований. Кроме протоколов, для уровней определяются интерфейсы взаимодействия с соседними уровнями, представляющие собой наборы правил взаимодействия посредством

обмена сообщениями стандартизированных форматов. По сути, *интерфейс* – это набор сервисов, предоставляемых данным уровнем соседним уровням. В частности, интерфейс определяет способ передачи блока данных и служебной информации, например адреса получателя. *Стек протоколов* – стандартизованный набор протоколов разных уровней, организующих взаимодействие компьютеров в сети. Следует отметить, что протоколы нижних уровней часто реализуются в сетевых аппаратных средствах, в то время как протоколы верхних уровней обычно представляют собой программное обеспечение.

**Характеристика уровней модели OSI**

*Физический уровень* (*Physical Layer*) – обеспечивает передачу битов блоков данных по физической передающей среде. К его задачам относятся: модулирование битового потока с целью получения оптимальной для передачи последовательности импульсных сигналов, проверка целостности линии связи, формирование импульсов с соответствующими протоколу физического уровня характеристиками и др. На физическом уровне определяются требования к кабельным системам и частоты передачи сигналов, правила монтажа коннекторов, типы коннекторов и т.д.

Примерами протоколов физического уровня являются: EIA-RS-232 – определяет характеристики сигналов и коннекторов COM-портов, спецификация 100 Base-TX – определяет аналогичные характеристики для реализации Fast Ethernet на витой паре и др.

*Канальный уровень* (*Data Link Control – DLC*). Основные задачи канального уровня: а) проверка доступности передающей среды; б) реализация механизмов определения и коррекции ошибок; в) реализация адресации сетевых интерфейсов. Примеры механизмов контроля ошибок передачи: а) биты чётности; б) контрольные суммы (дополнение суммы байтов (или двухбайтовых слов) до единицы или контрольные суммы, полученные с использованием циклических избыточных кодов CRC). Популярные протоколы канального уровня: Ethernet, Token Ring, Frame Relay.

*Сетевой уровень* (*Network Layer*). Основные задачи сетевого уровня: а) адресация сетей и рабочих станций; б) передача пакетов данных из сети в сеть с выбором оптимального маршрута к получателю (маршрутизация); в) преобразование пакетов данных к формату, определенному протоколом канального уровня сети, в которую они поступают. Типы протоколов сетевого уровня: а) протоколы передачи данных маршрутизаторам и между ними; б) протоколы обмена маршрутной информацией; в) протоколы, связывающие адреса канального и сетевого уровней. Популярные протоколы сетевого уровня: 1-го типа – протокол Интернета (Internet Protocol – IP), протокол межсетевого обмена пакетами (Internetwork Packet eXchange – IPX); 2-го типа – протокол маршрутной информации (Routing Information Protocol – RIP), протокол "кратчайший путь первым "(Open Shortest Path First – OSPF); 3 типа – протокол определения адреса (Address Resolution Protocol – ARP).

*Транспортный уровень* (*Transport Layer*). Основные задачи транспортного уровня: а) обеспечение одновременной передачи отправителем и получения получателем нескольких потоков данных (как различных типов, так и одинакового типа); б) обеспечение надежной передачи данных. Первая задача реализуется добавлением на этом уровне такой адресной информации, как порты, а вторая – использованием различных механизмов обеспечения надежности передачи, включая предварительную установку логического соединения, контроль целостности пакетов с помощью контрольных сумм, нумерацию пакетов и высылку подтверждения доставки и др. Популярные протоколы транспортного уровня: протокол управления передачей (Transmission Control Protocol – TCP), протокол пользовательских дейтаграмм (User Datagram Protocol – UDP), протокол обмена последовательностями пакетов (Sequenced Packet eXchange – SPX).

*Сеансовый уровень* (*Session Layer*). Основные задачи уровня: а) определение активной в данный момент стороны (это предотвращает попытки выполнения в один и тот же момент времени одной и той же операции сервером и клиентом); б) синхронизация соединения с возможностью установки контрольных меток в сеансе. Это позволяет восстановить сеанс с последней контрольной метки при потере соединения. Примерами протоколов сеансового уровня являются протокол вызова удалённых процедур (Remote Procedure Call – RPC) и NetBIOS.

*Уровень представления данных* (*Presentation Layer*). Основные задачи: а) обеспечение преобразования данных в некоторый общий формат представления данных (например, ASCII или Unicode) и наоборот; б) шифрование/дешифрование данных для обеспечения секретности передачи (примером может служить протокол Secure Socket Layer – SSL, обеспечивающий секретность передачи данных с использованием стека TCP/IP).

*Прикладной уровень* (*Application Layer*). Задача прикладного уровня – предоставлять пользовательским приложениям сетевые протоколы и службы уровня для обеспечения передачи данных по сети. Существует большое количество протоколов прикладного уровня. Примеры протоколов прикладного уровня: протокол пересылки гипертекста (HyperText Transfer Protocol – HTTP), протокол пересылки файлов (File Transfer Protocol – FTP), Telnet, простой протокол пересылки почты (Simple Mail Transfer Protocol – SMTP) и др.

Наиболее популярным стеком коммуникационных протоколов благодаря распространению Интернета стал стек TCP/IP. Этот стек является родным для операционных систем UNIX и Linux, в настоящее время он также является основным стеком для систем Windows. Примерами других стеков коммуникационных протоколов можно назвать стек IPX/SPX, разработанный фирмой Novell и стек NetBIOS/SMB, разработанный совместно IBM и Microsoft. Следует отметить, что стеки коммуникационных протоколов обычно включают не все уровни модели OSI (зачастую отсутствуют сеансовый уровень и уровень представления данных).

Учебное издание

**Коломоец** Геннадий Павлович

# Организация компьютерных сетей

Учебное пособие

Редактор А.І. Гутман
Коректор Ю.А. Сімакова
Технічний редактор О.О. Івченко

Підписано до друку 21.06.2012.
Формат 60х84/16. Папір офсетний. Друк різографний. Гарнітура Times.
Умовн.-друк. арк. 9,07. Обл.-вид. арк. 10,88. Тираж 500 пр. Зам. № 04-11 п.

---

Видавець та виготовлювач
Класичний приватний університет
69002, м. Запоріжжя, вул. Жуковського, 70-б

Свідоцтво суб'єкта видавничої справи
серія ДК, № 3321 від 25.11.2008 р.