МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Колледж экономики, управления и права

Методические указания по организации практической работы студентов по учебной дисциплине Компьютерные сети

09.02.07 Информационные системы (по отраслям)

Ростов-на-Дону
2023

Методические рекомендации по учебной дисциплине «Компьютерные сети» разработаны с учетом по специальности среднего профессионального образования (далее – СПО) технического профиля: Информационные системы (по отраслям) предназначены для обучающихся и преподавателей колледжа.
Методические рекомендации разработаны на основе требований ФГОС среднего общего образования, предъявляемых к структуре, содержанию и результатам освоения учебной дисциплины «Компьютерные сети».

Составитель (автор): С.Н. Маловечко преподаватель колледжа ЭУП

Рассмотрены на заседании предметной (цикловой) комиссии специальности общеобразовательных дисциплин

Протокол № от «____ » _____ 2023 г

Председатель предметной (цикловой) комиссии _____ С.В.Шинакова
личная подпись

и одобрены решением учебно-методического совета колледжа.

Протокол № 1 от «31» августа 2021 г

Председатель учебно-методического совета колледжа
комиссии _____ С.В.Шинакова
личная подпись

Рекомендованы к практическому применению в образовательном процессе

Рецензенты:

Содержание:

Лабораторная работа №1 Изучение интерфейса эмулятора сети CISCO PACKET TRACER

Цели практической работы:

1. Знакомство с программой «Эмулятор сети Cisco Packet Tracer.
2. Изучение инструментов программы «Эмулятор сети Cisco Packet Tracer.

Теоретические сведения.

Эмулятор сети Cisco Packet Tracer это программа, позволяющая строить сети произвольной топологии на разнообразном оборудовании с поддержкой разных протоколов.

Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств:

- маршрутизаторов;
- коммутаторов;
- точек беспроводного доступа;
- персональных компьютеров;
- сетевых принтеров;
- IP-телефонов.

Для подключения и коммутации устройств в эмуляторе сети можно использовать различные соединители.

Для настройки устройств используют:

- графического вебинтерфейса;
- командную строку операционной системы;
- графическое меню.

Режим визуализации Cisco Packet Tracer позволяет отследить прохождение сигналов и пакетов через сетевые устройства, скорость их перемещения по сети.

Состав интерфейса Cisco Packet Tracer

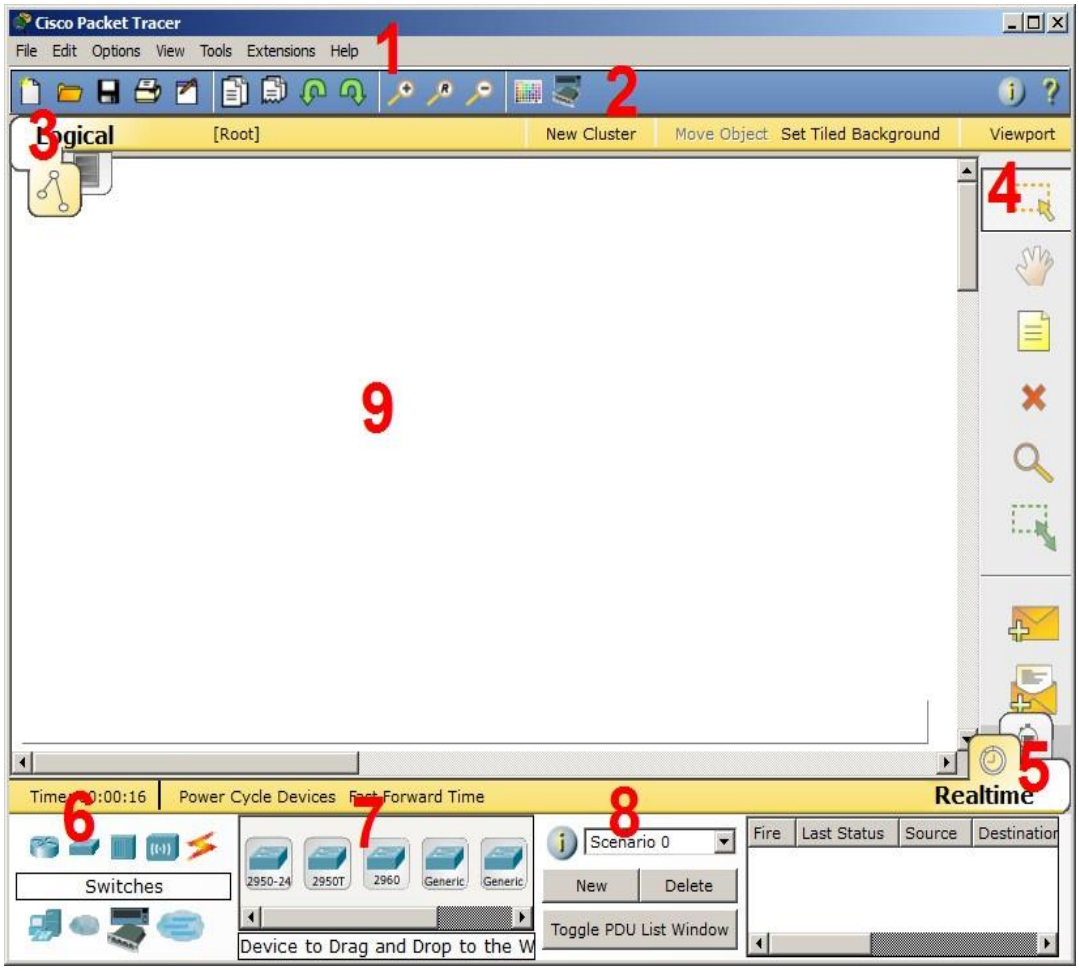


Рис.1.1. Интерфейс программы Cisco Packet Tracer

Методические рекомендации по выполнения

Введение

1. Главное меню программы со следующим содержимым:
   - Файл - содержит операции открытия/сохранения документов;
   - Правка - стандартные операции "копировать/вырезать, отменить/повторить";
   - Настройки - говорит само за себя;
   - Вид - масштаб рабочей области и панели инструментов;
   - Инструменты - цветовая палитра и кастомизация конечных устройств;
   - Расширения - мастер проектов, многопользовательский режим;
   - Помощь;
2. Панель инструментов, часть которых просто дублирует пункты меню;
3. Переключатель между логической и физической организацией;
4. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а также формирование произвольных пакетов;
5. Переключатель между реальным режимом (Real-Time) и режимом симуляции;
6. Панель с группами конечных устройств и линий связи;
7. Сами конечные устройства, здесь содержатся всевозможные коммутаторы, узлы, точки доступа, проводники.
8. Панель создания пользовательских сценариев;
9. Рабочее пространство.

Панель с группами конечных устройств и линий связи

Конечные устройства

Здесь представлены конечные узлы – хосты, серверы, принтеры, телефоны и пр.

Маршрутизаторы

Маршрутизаторы используется для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например, выбор маршрута с наименьшим числом транзитных узлов. Маршрутизаторы работают на сетевом уровне модели OSI.

Коммутаторы

Коммутаторы – устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор передаёт пакеты на основании внутренней таблицы – таблицы коммутации, следовательно, трафик идёт только на тот MAC-адрес, которому он предназначается, а не повторяется на всех портах (как на концентраторе).

Концентраторы

Концентратор повторяет пакет, принятый на одном порту, на всех остальных портах.

Линии связи

С помощью этих компонентов создаются соединения узлов в единую схему. Packet Tracer поддерживает широкий диапазон сетевых соединений (табл. 1.1). Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов

Беспроводные устройства

Беспроводные технологии Wi-Fi и сети на их основе. Включает в себя точки доступа.

Таблица 1.1. Типы кабелей

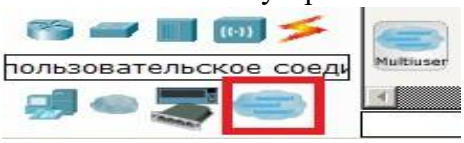
Тип кабеля	Описание
Консоль	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Должны быть выполнены некоторые требования для работы консольного сеанса с ПК. Скорость соединения с обеих сторон должна быть одинаковая, должно быть 7 или 8 бит данных для обеих сторон. Контроль четности должен быть одинаковый. Должно быть 1 или 2 стоповых бита, но они необязательно должны быть одинаковыми. Поток данных может быть любым для обеих сторон.
Медный прямой	Этот тип кабеля является стандартной средой передачи Ethernet, функционирующей на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).
Медный кроссовер	Этот тип кабеля является средой передачи Ethernet, функционирующей на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet)
Оптика	Оптоволоконная среда используется для соединения между оптическими портами (100 Мбит/с или 1000 Мбит/с).
Телефонный	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты. Стандартное представление модемного соединения – конечное устройство, например ПК, дозванивающееся в сетевое облако.
Коаксильный	Коаксиальная среда используется для соединения между коаксиальными портами, такими как кабельный модем, соединенный с облаком Packet Tracer.

 Серийный DCE Серийный DTE 	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCEустройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становиться DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

Эмуляция Интернета

Для эмуляции глобальной сети используются модем DSL или "облако".

Пользовательские устройства и облако для многопользовательской работы



Физическая комплектация оборудования

Установите в рабочее поле роутер Cisco 1841 и двойным щелчком мыши откройте его физическую конфигурацию
(рис.1.2).

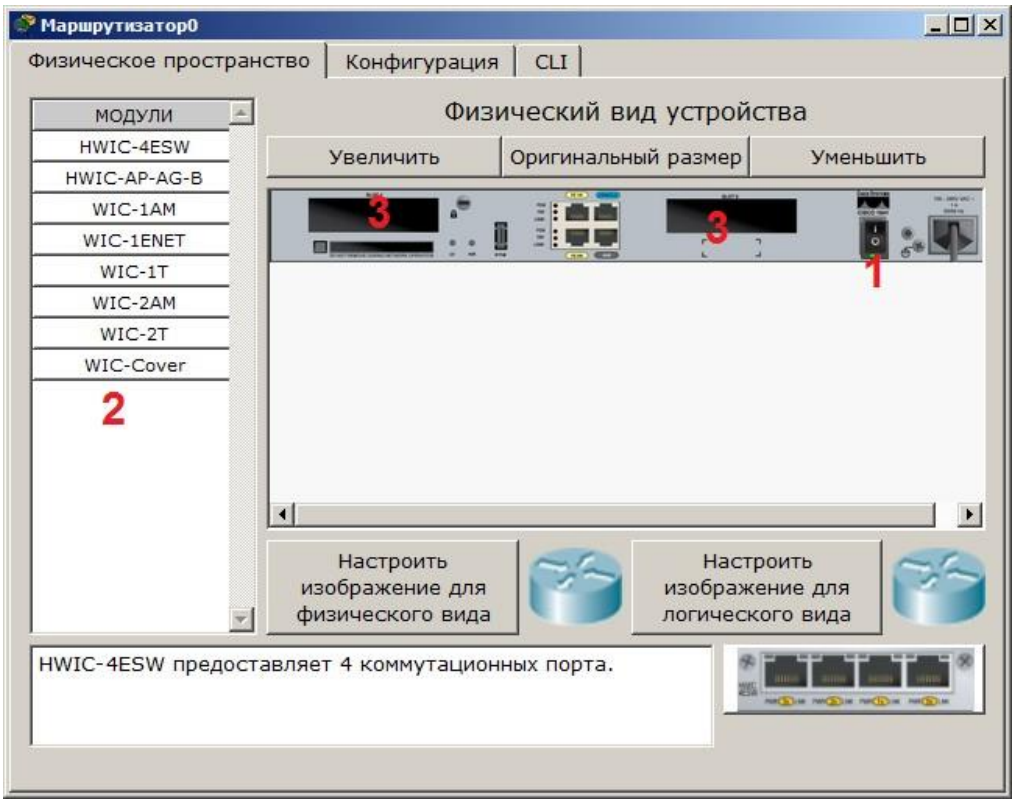


Рис.1.2. Физическая конфигурация устройства

Слева в области 2 находится список модулей, которыми можно укомплектовать данный роутер. Выбранные модули можно встроить в области 3 (в данный момент они пусты). Эту операцию следует производить при выключенном питании в области 1.

Модули – это платы, расширяющие функциональность устройства. Устройство можно рассматривать как системный блок со своей ОС и многими сетевыми картами, которые могут работать только с сетью.
Ниже представлена информация о каждом модуле:
HWIC - 4ESW – высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45. Позволяет сочетать в маршрутизаторе возможности коммутатора.
HWIC-AP-AG-B – высокоскоростная WAN-карта, обеспечивающая функционал встроенной точки доступа для роутеров линейки Cisco 1800 (модульных), Cisco 2800 и Cisco 3800. Модуль поддерживает радиоканалы Single Band 802.11b/g или Dual Band 802.11a/b/g.
WIC-1AM включает в себя два разъема RJ-11, используемых для подключения к базовой телефонной службе. Карта использует один порт для соединения с телефонной линией, другой может быть подключен к аналоговому телефону для звонков во время простоя модема.
WIC-1ENET – однопортовая 10 Мб/с Ethernet карта для 10BASE-T Ethernet LAN.
WIC-1T предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам, например, SDLC концентраторам, системам сигнализации и устройствам packet over SONET (POS).
WIC-2AM содержит два разъема RJ-11, используемых для подключения к базовой телефонной службе. В WIC-2AM два модемных порта, что позволяет использовать одновременно оба канала для соединения.
WIC-2T – 2-портовый синхронный/асинхронный серийный сетевой модуль предоставляет гибкую поддержку многих протоколов с индивидуальной настройкой каждого порта в синхронный или асинхронный режим. Применения для синхронной/асинхронной поддержки представляют:

- низкоскоростную агрегацию (до 128 Кб/с);
- поддержку dial-up модемов;
- синхронные или асинхронные соединения с портами управления другого оборудования и передачу устаревших протоколов типа Bi-sync и SDLC.

WIC-Cover – стенка для WIC слота для защиты электронных компонентов и для улучшения циркуляции охлаждающего воздушного потока.
Для изменения комплектации оборудования необходимо отключить питание, щелкнув мышью на кнопке питания, перетащить мышью модуль HWIC - 4ESW (или другой выбранный модуль) в свободный слот и включить питание. Дождаться окончания загрузки роутера. На вкладке Config увидим появившиеся 4 новых интерфейса (рис.1.3).

Рис.1.3. Конфигурация интерфейсов устройства

Остальные устройства комплектуются аналогично. Добавляются новые модули Ethernet (10/100/1000), оптоволоконные разъемы нескольких типов, адаптеры беспроводной сети. На рабочий компьютер есть возможность добавить, например, микрофон с наушниками, жесткий диск для хранения данных.

Контрольные вопросы

- Какая плата расширения обеспечивает функционал встроенной точки доступа?
- Какая плата расширения предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам?
- Как называется высокопроизводительный модуль с 4мя коммутационными портами Ethernet под разъем RJ-45?
- Перечислите сетевые карты, позволяющие подключаться к WAN сетям?
- Какой тип интерфейса следует выбрать при создании кластера?
- Назовите модели коммутаторов третьего уровня?
- Какой тип кабеля следует использовать при соединении роутеров между собой?
- Укажите серии магистральных маршрутизаторов.
- В каких случаях используется интерфейс SERIAL?
- Как организовать связь двух магистральных маршрутизаторов?
- Перечислите все возможные режимы работы программы Cisco Packet Tracer?
- Назовите модели коммутаторов второго уровня?
- Перечислите все типы связей, используемых в Cisco Packet Tracer, и укажите их назначение.

2. Режим симуляции Cisco Packet Tracer

Cisco Packet Tracer содержит инструмент для симуляции работы сети, в котором можно имитировать и симулировать состояние работы сети и сетевые события. Например, можно проследить, как будет реагировать сеть в случае сбоев или, например, что произойдет, если отсоединить какой–либо кабель или отключить питание одного из сетевых устройств.

Режим симуляции позволяет проследить структуру пакета и просмотреть, с какими параметрами пакет проходит по уровням модели OSI.

Выполнение лабораторной работы

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы между собой соединяются кроссоверным кабелем
(рис.1.4).

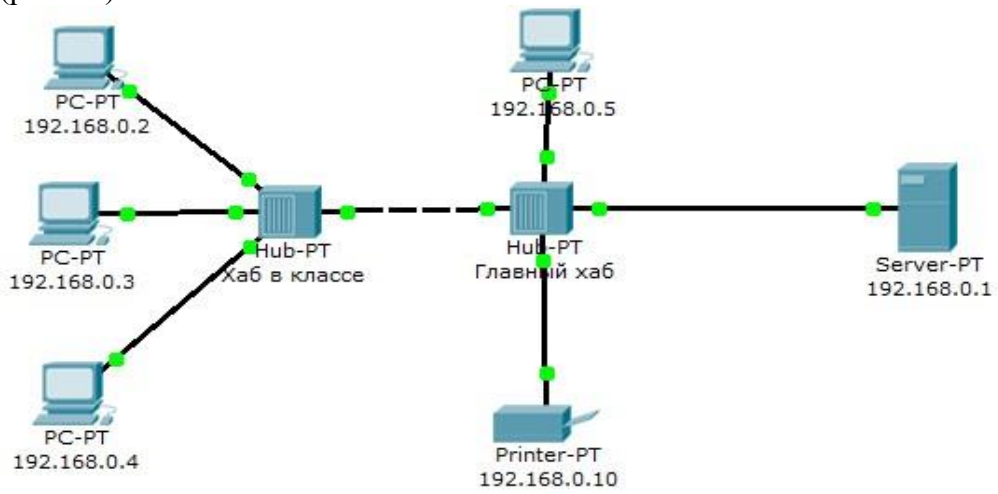


Рис. 1.4. Схема сети

Для перехода в режим симуляции нужно щелкнуть на иконке симуляции в правом нижнем углу рабочего пространства. В окне событий видим кнопку сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Из множества протоколов выберем только протокол ICMP. Он исключит случайный трафик между узлами.
Для перехода к следующему событию используем кнопку Вперёд, либо автоматический режим (рис.1.5).

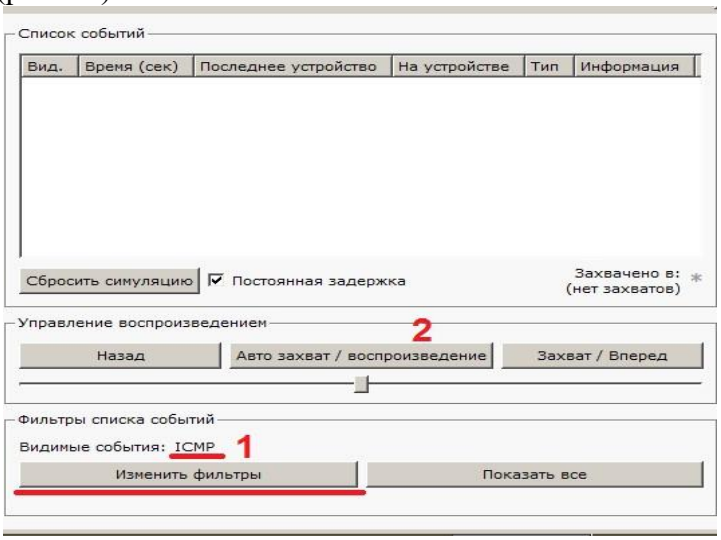


Рис.1.5. Интерфейс симулятора

С одного из узлов пошлем PING-запрос на другой узел. Выбираем далеко расположенные узлы, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции – начальный узел 4, конечный узел 5. На узле 4 образовался пакет (конвертик), который находится в стадии ожидания (иконка паузы на нём). Запустить пакет в сеть можно, нажав кнопку Вперёд в окне симуляции (рис.1.6).
В окне симуляции мы также увидим этот пакет – его тип ICMP и источник 192.168.0.4 (рис.1.7).

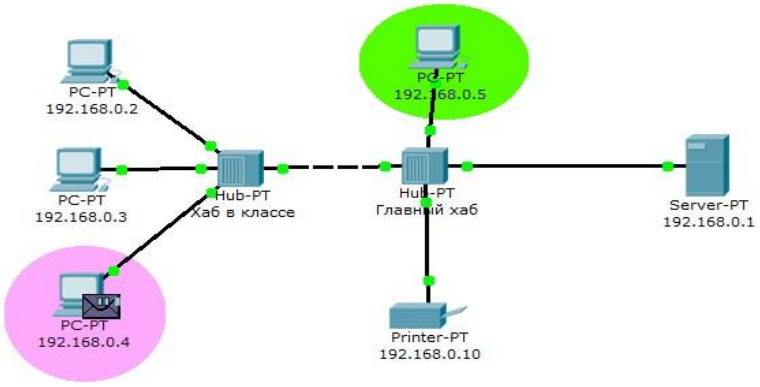


Рис.1.6. Демонстрация работы симулятора

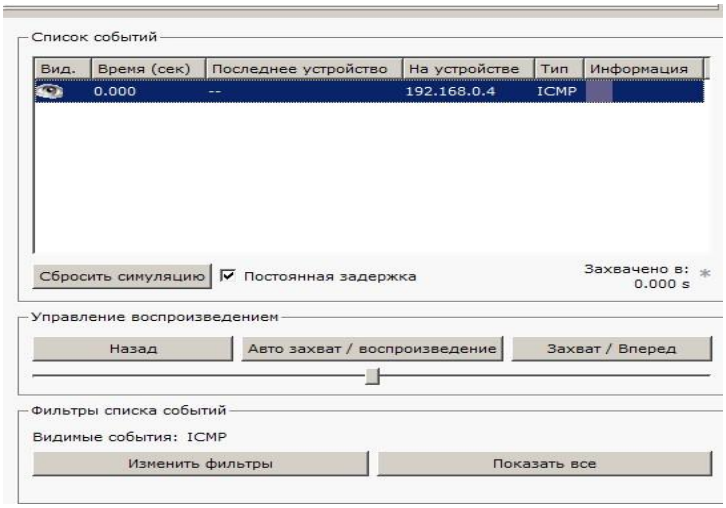


Рис.1.7. Мониторинг работы протоколов

Щелчок на пакете покажет нам подробную информацию. При этом мы увидим модель OSI. Сразу видно, что на третьем, сетевом, уровне возник пакет на исходящем направлении, который дойдёт сначала до второго, канального, уровня, затем до первого, физического, и передастся на следующий узел

(рис.1.8).

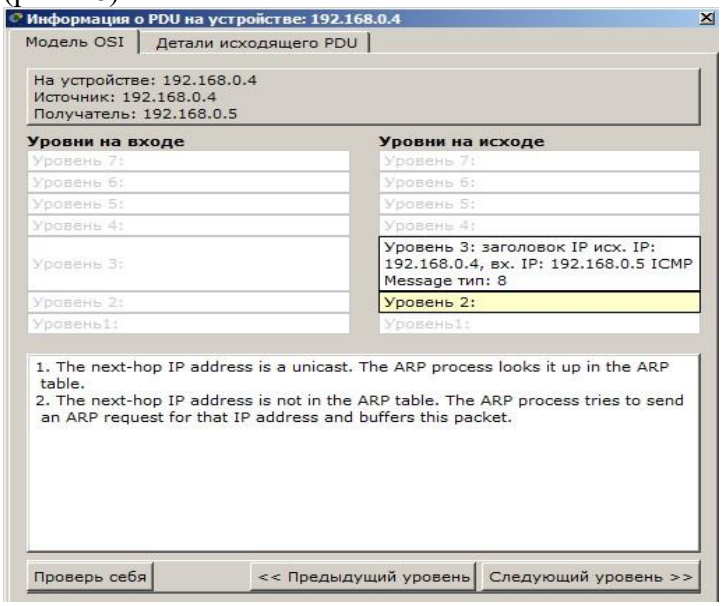


Рис.1.8. Мониторинг работы на модели OSI

А на другой вкладке можно посмотреть структуру пакета (рис.1.9).

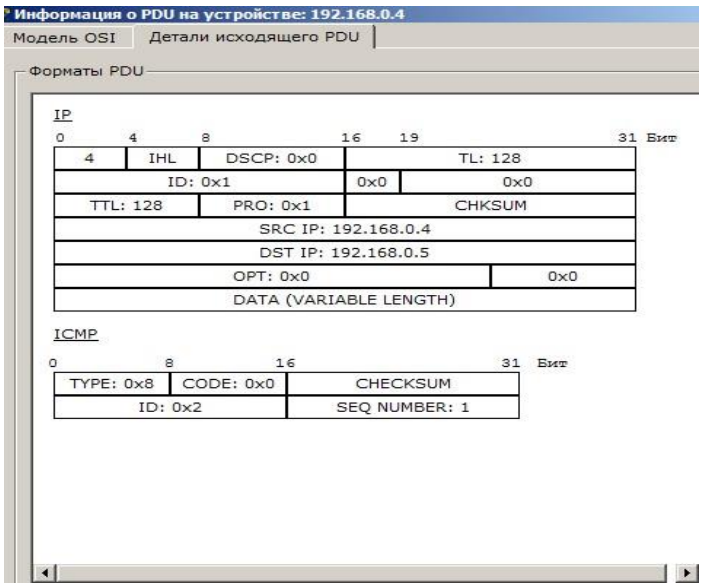


Рис.1.9. Структура пакета

Нажмём кнопку Вперёд. Пакет двинется к концентратору. Это единственное сетевое подключение с этой стороны (рис.
1.10).

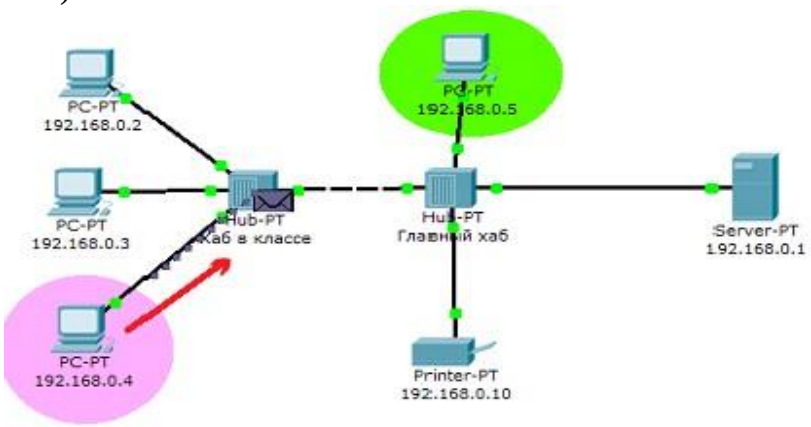


Рис.1.10. Прохождение пакета. Первый этап

Концентратор по определению повторяет пакет на всех остальных портах (рис.1.11)

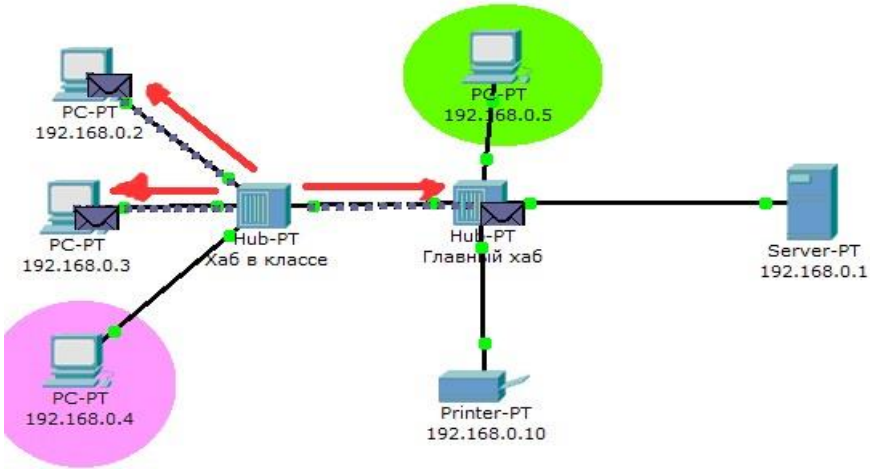


Рис.1.11. Прохождение пакета. Второй этап

Если пакеты каким-то узлам не предназначены, они просто игнорируют их (рис.1.12). Когда пакет вернётся обратно, мы увидим подтверждение соединения.

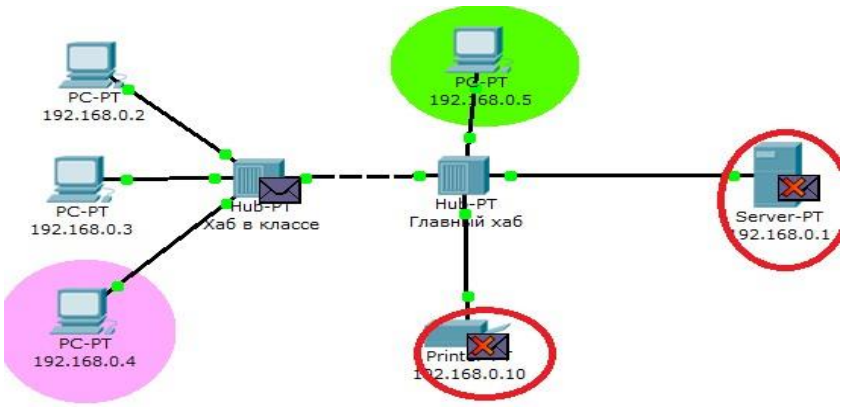


Рис.1.12. Прохождение пакета. Третий этап

Контрольные вопросы

- Для чего используется режим симуляции?
- Как просмотреть прохождение пакета по уровням модели OSI?
- Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?
- Укажите в составе пакета IP адреса отправителя и получателя.
- Как изменить фильтры списка событий?
- Как в режиме симуляции определить, какие протоколы были задействованы в работе сети?
- Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?
- Перечислите основные возможности режима симуляции.

Лабораторная работа №2. «Сетевые настройки.»

Цель работы: приобретение знаний и практических навыков, необходимых для присвоения имени компьютеру и рабочей группе, а также установки дополнительных сетевых настроек.

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

Теоретические сведения.

Каждый компьютер в сети должен иметь свое уникальное имя, чтобы компьютеры могли однозначно идентифицировать друг друга и взаимодействовать. Целесообразно присваивать компьютерам короткие (не более пятнадцати символов) и понятные имена.

Для имени компьютера рекомендуется использовать только стандартные символы Интернета. Такими символами являются числа от 0 до 9, заглавные и строчные буквы от A до Z, а также символ переноса (-). Имена компьютеров не могут состоять из одних цифр и содержать пробелы. Кроме того, в имена нельзя

включать специальные знаки, например:

< > ; : " * + = \ | ? ,

При настройке сети системой Windows автоматически создается рабочая группа, которой присваивается имя. Можно как присоединиться к уже существующей рабочей группе в сети, так и создать новую.

Домены, рабочие группы и домашние группы представляют разные методы организации компьютеров в сети. Основное их различие состоит в том, как осуществляется управление компьютерами и другими ресурсами.
Рабочая группа – это группа компьютеров, подключенных к сети, которые совместно используют ресурсы. При настройке сети операционная система Windows автоматически создает рабочую группу и присваивает ей имя по умолчанию.

Домен — это группа компьютеров одной сети, имеющих единый центр, использующий единую базу пользователей, единую групповую и локальную политики, единые параметры безопасности, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров.

Рабочие группы служат основой для общего доступа к файлам и принтерам, но не осуществляют фактическую настройку общего доступа.

1. **Ход выполнение работы.**
    1. Присвоение имени компьютеру.
    2. Откройте Панель управления - Система – Просмотр имени этого компьютера – Изменить параметры

3. При появлении запроса пароля администратора или подтверждения введите пароль или предоставьте подтверждение.

4. На вкладке Имя компьютера нажмите Изменить.

1. Присвоение имени рабочей группе.

1. Открыть окно «Система».

2. В группе Имя компьютера, имя домена и параметры рабочей группы нажмите кнопку Изменить параметры. При появлении запроса пароля администратора или подтверждения введите пароль или предоставьте подтверждение.

3. В диалоговом окне Свойства системы перейдите на вкладку Имя компьютера и затем нажмите кнопку Изменить.

4. В диалоговом окне Изменение имени компьютера или домена щелкните в разделе Член групп пункт Рабочая группа и выполните одно из следующих действий.

- Чтобы присоединиться к существующей рабочей группе, введите имя рабочей группы, к которой будет присоединен компьютер, а затем нажмите ОК.
- Чтобы создать новую рабочую группу, введите имя новой рабочей группы, а затем нажмите ОК.

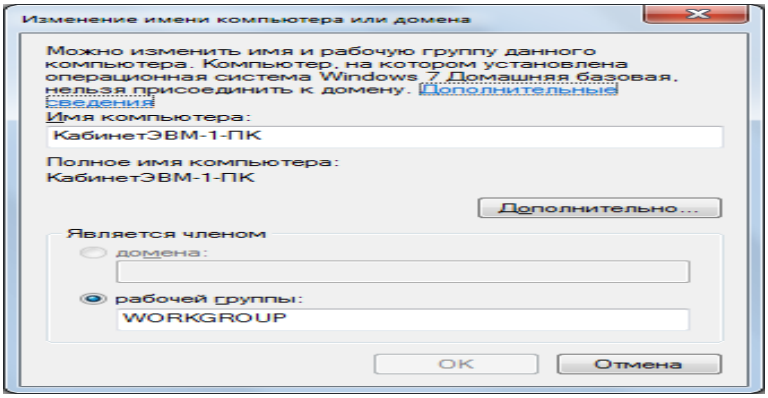


Рис.1. Диалоговое окно «Изменение имени компьютера или домена»

Если перед присоединением к рабочей группе компьютер входил в домен, то он будет удален из него, а учетная запись компьютера в домене будет отключена.

4. Присвойте старое имя компьютеру и рабочей группе.

5. Установка дополнительных сетевых настроек.

Настройке сетевого подключения на компьютере с Windows 7.

Зайдите в Панель управлении - Система и безопасность, а в нем — пункт Система.

Чтобы изменить имя рабочей группы или компьютера, нажмите на ссылку Изменить параметры (она находится справа). Лучше, если имена рабочих групп в обоих компьютерах совпадают, а имена самих компьютеров — нет.

Вернитесь в Панель управления и выберите пункт Сеть и Интернет, а в нем — Центр управления сетями и общим доступом. В боковом меню будет пункт Изменение параметров

адаптера, выберите его. В нем должен быть ярлык под названием Подключение по локальной сети. Если он имеет серый цвет и подписан Отключено, кликните правой кнопкой мыши и выберите пункт Включить. Затем в контекстном меню ярлыка выберите пункт Свойства. В диалоговом окне выберите пункт Протокол Интернета версии 4 (TCP/IPv4), снова нажмите на кнопку Свойства. Впишите IP-адрес (192.168.35.68.) и маску подсети (255.255.255.0), сохраните изменения.

Вернитесь в Центр управления сетями и общим доступом, в левом нижнем углу будет ссылка —Домашняя группа, нажмите на нее. В появившемся окне нажмите на ссылку Что такое расположение в сети?. В окне настроек сетевого размещения вам нужно выбрать расположение сети Неопознанная сеть — выберите пункт Домашняя сеть. Затем появится окно для настройки общего доступа к папкам — можно пропустить этот шаг, сняв все галочки и нажав кнопку Далее. Пароль для домашней группы настраивать тоже не обязательно, просто нажмите на кнопку Готово.

Снова зайдите в Центр управления сетями и общим доступом, сверху в левой колонке нажмите на ссылку Изменить дополнительные параметры общего доступа. Текущим профилем должен быть Домашний или рабочий. В этом профиле найдите последний пункт (Подключения домашней группы), установите переключатель на Использовать учетные записи пользователей и пароли для подключения к другим компьютерам, сохраните изменения, выйдите из системы и зайдите снова (Пуск — Завершение работы — Выйти из системы).

Для того, чтобы окончательно настроить сеть между Windows XP и Windows 7, зайдите в проводник и расшарьте папки на компьютере с Windows 7. Для этого щелкните по папке правой кнопкой мыши, выберите пункт контекстного меню Общий доступ, в нем — Конкретные пользователи. Здесь выбираются учетные записи Windows 7, с помощью которых можно будет подключиться к компьютеру с Windows XP. Нажмите кнопку Общий доступ

2. **Порядок выполнения работы:**

Создать у себя на компьютере папку с названием группы.

1. Настроить к ней общий доступ с полными правами.
2. В ней создать текстовый файл со следующими характеристиками: имя файла – фамилия (или фамилии студентов, работающих за этим компьютером), содержимое – IP адрес компьютера, его имя в сети, имя рабочей группы, перечислить все компьютеры в этой рабочей группе.
3. Передать свой файл по сети всем студентам на занятии.
4. Забрать такой же файл с компьютера справа, добавив к его имени знак «+».
5. Создать папку с ограниченными правами (только для чтения). Протестируйте свою папку с чужого компьютера на возможность записи в ней.

6. Задайте пароль для доступа к своей папке.

Вопросы к защите:

1. Каким образом внешний компьютер идентифицируется на вашем компьютере?
2. Дайте определение одноранговых локальных вычислительных сетей.
3. Как осуществить доступ к Вашим каталогам с другого ПК?

Лабораторная работа № 3. «Подключение ресурса сети в качестве сетевого диска. Ограничение доступа к ресурсам.»

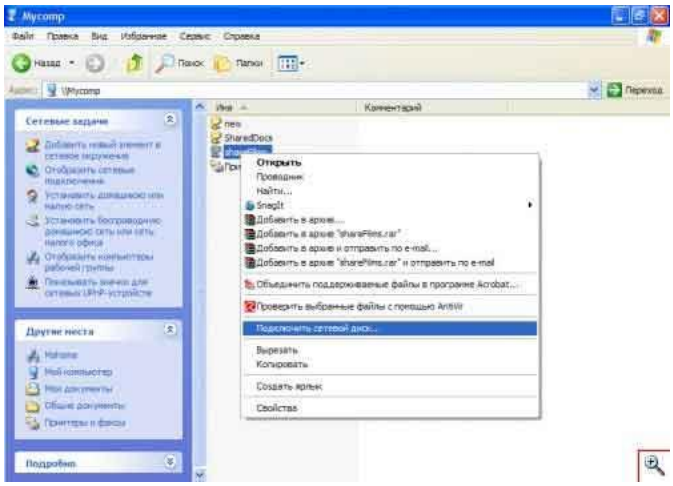
Цель работы: приобретение знаний и практических навыков, необходимых для присвоения подключения ресурса сети в качестве сетевого диска.

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

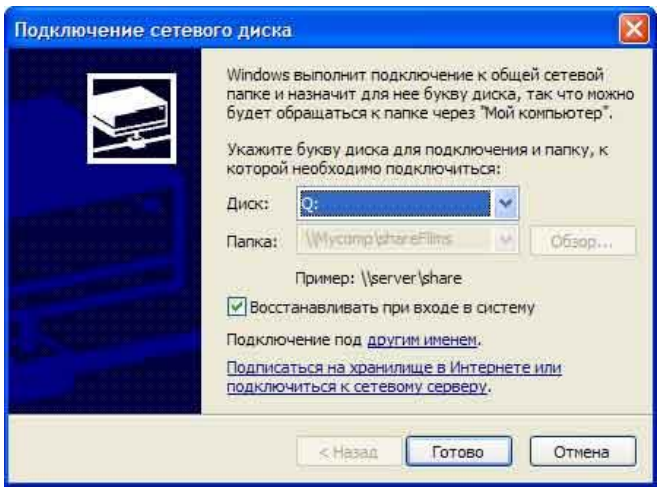
Теоретические сведения.

Как вы уже заметили, поиск сетевой папки занимает длительное время, а так же нагружает систему. Более практичным вариантом будет подключение сетевого диска к вашему компьютеру. Если сделать это, то вы будет видеть его в списке локальных дисков в папке «Мой компьютер». Так же это позволить ускорить процесс работы с расширенными папками.

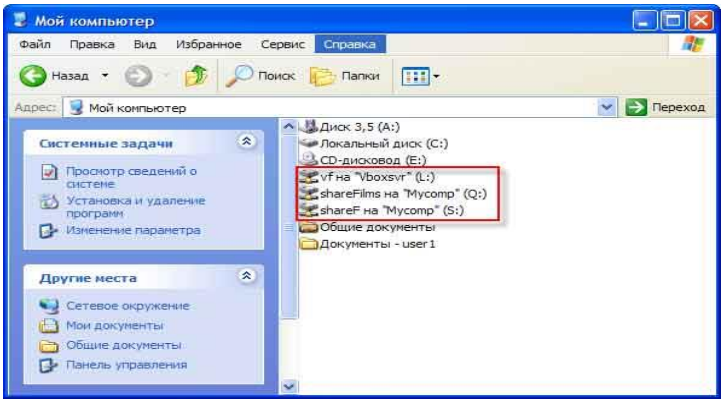
Для этого, мы переходив в «Сетевое окружение», по этому пути: «Пуск» -> «Сетевое окружение», здесь выберем интересующий нас компьютер который подключен к локальной сети и зайдя в него найдем папку с общим доступом, которую мы и будет подключать к вашему компьютеру как сетевой локальный диск. Кликаем по этой папке правой кнопкой мыши и в открывшемся диалоговом окне выбираем пункт «Подключить сетевой диск».



Далее откроется ещё одно окно, где нам будет предложено выбрать букву сетевого локального диска. Знайте, что два диска с одинаковыми именами на вашем ПК не может быть! Ещё нам нужно выделить пункт «Восстанавливать при входе в систему», этот пункт позволит автоматически производить процесс поиска данной папки и включать его в список ваших дисков в папке «Мой компьютер».



Теперь простым входом в «Мой компьютер» вы просто можете увидеть и воспользоваться локальным сетевым диском. Любую расширенную папку локальной сети можно подключить к вашему компьютеру в качестве локального сетевого диска. Так же вы можете их различить по иконкам, они имеют вот такой вид:



Чтобы произвести отключение локального сетевого диска, нужно кликнуть по нему правой кнопкой мыши и в открывшемся диалоговом окне выбрать пункт «Отключить». Так следует дополнить, что отключив компьютер на котором находиться данный локальный диск, то этот диск будет недоступен на других компьютерах.

Ход выполнение работы.

Подключите 3 сетевых диска с других ПК.

1. Покажите преподавателю.
2. Удалите, созданные вами диски.

Лабораторная работа №4 «Подключение и настройка сетевого адаптера»

Цель работы: приобретение знаний и практических навыков, необходимых для подключение и настройки сетевого адаптера

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

Теоретические сведения.

Как установить новый сетевой адаптер

1. Убедитесь, что компьютер выключен, а силовой кабель отключен от сети.

2. Откройте корпус компьютера. Попросите преподавателя помочь вам и проконсультировать вас, как открыть корпус компьютера.

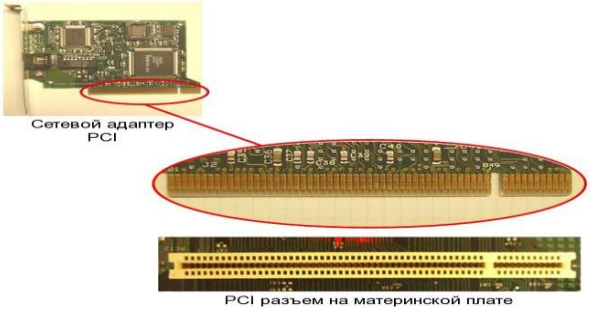


Схема 4.2

4. Найдите свободный PCI разъем в материнской плате. Разъемы PCI легко отличимы за счет своего белого или бежевого цвета. Посмотрите на схему 4.2.

5. Открутите винт и извлеките металлическую заглушку разъема из компьютера. Посмотрите на схему 4.3.

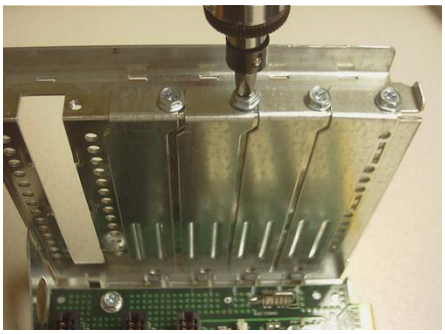


Схема 4.3

6. Вставьте сетевой адаптер в свободный PCI разъем. Убедитесь, что он полностью вошел в разъем. Посмотрите на схему 4.4.

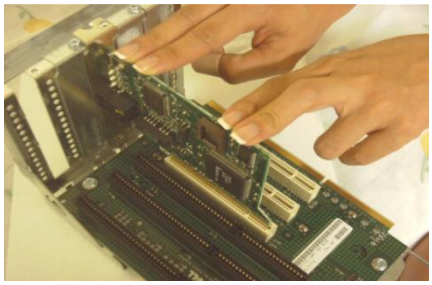


Схема 4.4

7. Надежно прикрутите плату к корпусу компьютера откученным ранее винтом. Заглушку слота, извлеченную из корпуса, следует сохранить. Посмотрите на схему 4.5.

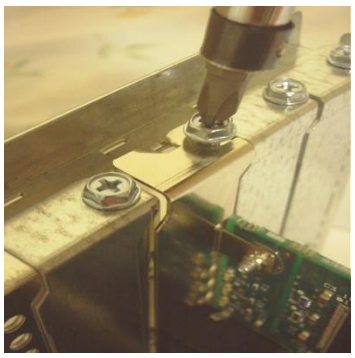


Схема 4.5

8. Закройте корпус компьютера.

Как сконфигурировать новый установленный сетевой адаптер

9. Включите компьютер и войдите в систему, используя имя пользователя и пароль, предоставленные вам преподавателем.

10. Драйверы Windows XP поддерживают много различных типов аппаратного обеспечения. Если Windows XP имеет подходящий драйвер для установленного сетевого адаптера, драйвер будет установлен автоматически. Вы можете получить или не получить сообщение о том, что драйвер был установлен.

11. Для того, чтобы проверить, успешно ли система Windows XP сконфигурировала и установила новое оборудование, правой кнопкой мыши щелкните на **Мой компьютер** и выберите **Управление**. Щелкните дважды по **Диспетчер устройств** и найдите компонент **Сетевые платы**. Раскройте компонент **Сетевые платы,** при этом должен появиться установленный сетевой адаптер. Если установленный сетевой адаптер не появился в списке, драйвер для него необходимо установить вручную. Переходите к следующему шагу нашей инструкции для того, чтобы установить драйвер вручную. Если у вас не возникло проблем с установкой драйвера, переходите к следующей секции нашей инструкции. Посмотрите на схему 4.6.

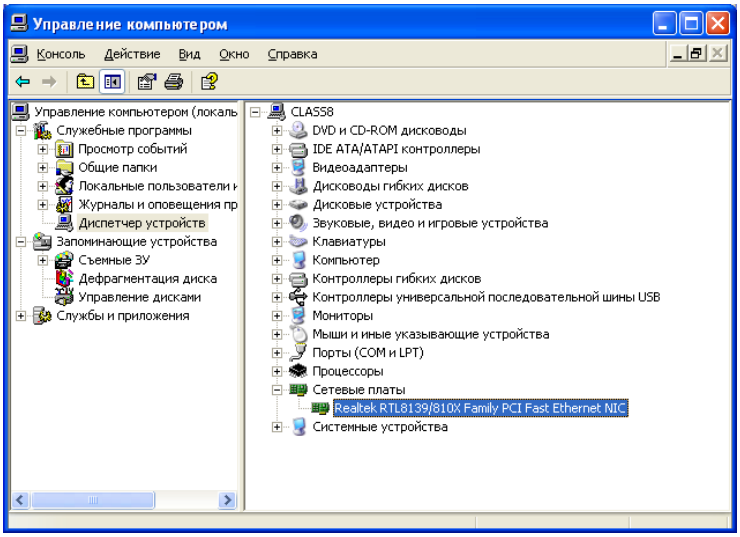


Схема 4.6

12. Щелкните **Пуск**, щелкните **Панель управления,** затем щелкните **Принтеры и другое оборудование**.

13. В левой части окна щелкните **Установка оборудования**.

14. Запустится **Мастер установки оборудования**. Следуйте инструкциям, и когда получите запрос на дискету или CD, содержащий драйверы, предоставьте правильные файлы драйвера. Преподаватель может выдать учащимся требуемые файлы драйвера, если их нет в списке известных устройств Windows XP.

Как присоединить компьютер к рабочей группе

1. Правой кнопкой мыши щелкните **Мой компьютер,** затем выберите **Свойства**. Появится окно **Свойства системы**. Щелкните по вкладке **Имя компьютера**. Щелкните по кнопке **Изменить…** для того, чтобы начать процесс присоединения к рабочей группе. Посмотрите схему 4.7.

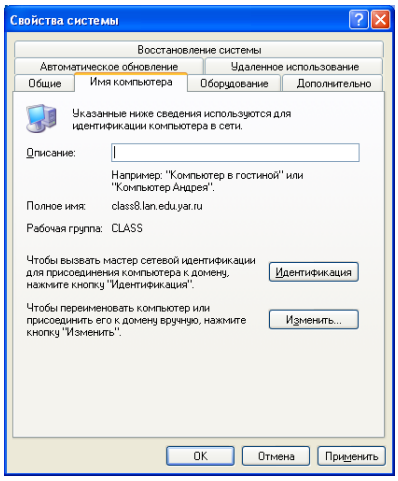


Схема 4.7

Появится окно Изменение имени компьютера. Выберите опцию Является членом рабочей группы. По умолчанию Windows XP использует WORKGROUP в качестве названия рабочей группы. Каждый компьютер должен иметь свое уникальное имя Имя компьютера. Посмотрите на схему 4.8.

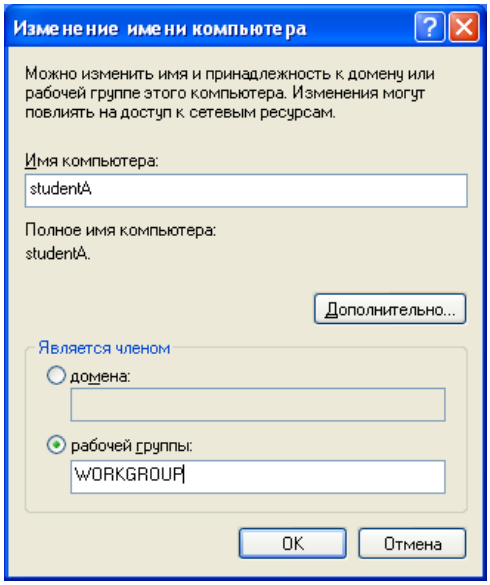


Схема 4.8

2. Щелкните **OK** для того, чтобы закрыть окно.

3. Щелкните **OK** для запуска процесса подсоединения к рабочей группе **WORKGROUP**.

4. Если процесс присоединения к рабочей группе прошел успешно, всплывет сообщение **Добро пожаловать в рабочую группу WORKGROUP**. Щелкните **OK** для того, чтобы закрыть его. Посмотрите на схему 4.9.

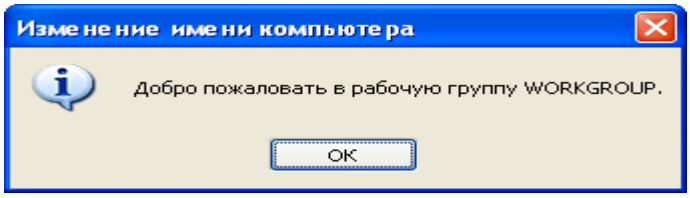


Схема 4.9

5. Далее система спросит вас, перезагрузить ли компьютер для завершения процесса. Щелкните **Да** для перезагрузки системы.

Как настроить конфигурацию сетевого адаптера для получения доступа к Интернет

Войдите в систему с соответствующим **Именем пользователя** и **Паролем**, который вы получите от преподавателя.

1. Правой кнопкой мыши щелкните **Сетевое окружение** на вашем рабочем столе, затем выберите **Свойства**. Появится окно **Сетевые подключения**, показывающее имеющиеся соединения локальной сети или соединения с Интернет. (Обратите внимание: схема 4.10 показывает два соединения **Подключение по локальной сети,** в вашем случае может быть только одно соединение.)

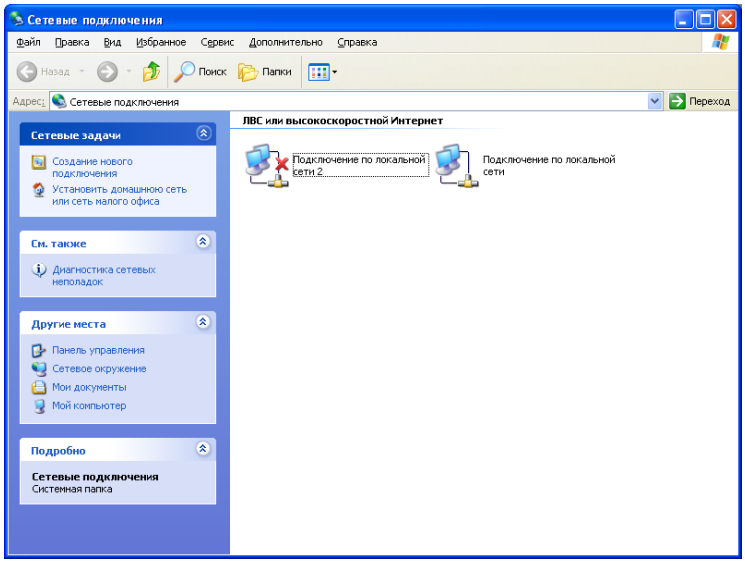


Схема 4.10

2. Правой кнопкой мыши щелкните **Подключение по локальной сети,** затем выберите **Свойства**. Появится окно **Подключение по локальной сети - свойства**. В окне **Отмеченные компоненты используются этим подключением:** щелкните **Протокол Интернета**, затем щелкните **Свойства**. Посмотрите на схему 4.11.

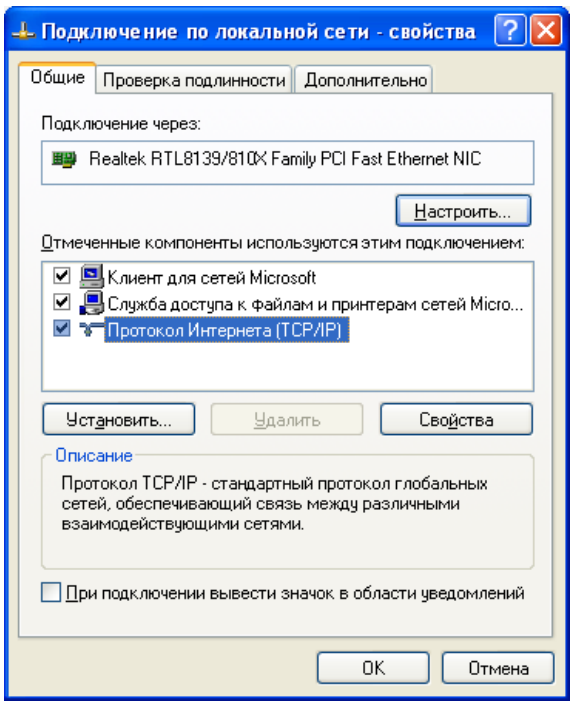


Схема 4.11

3. Появится окно **Свойства: Протокол Интернета (TCP/IP)**. Обратите внимание на вкладку **Общие**, где уже выбрано **Получить IP-адрес автоматически**. Щелкните **Использовать следующий IP-адрес**, при этом обратите внимание, что **Использовать следующие адреса DNS-серверов** также уже выбрано. Посмотрите на схему 4.12.

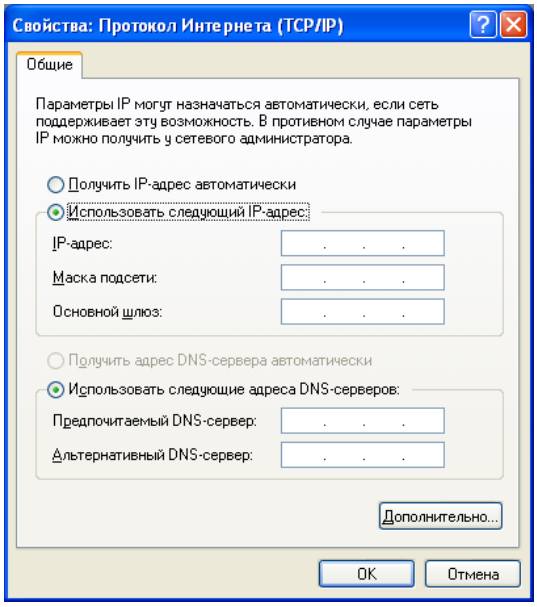


Схема 4.12

4. Используйте **IP-адрес**, **Маску подсети**, **Основной шлюз, Предпочитаемый DNS-сервер** и **Альтернативный DNS-сервер,** предоставленные вашим преподавателем. Посмотрите пример на схеме 4.13.

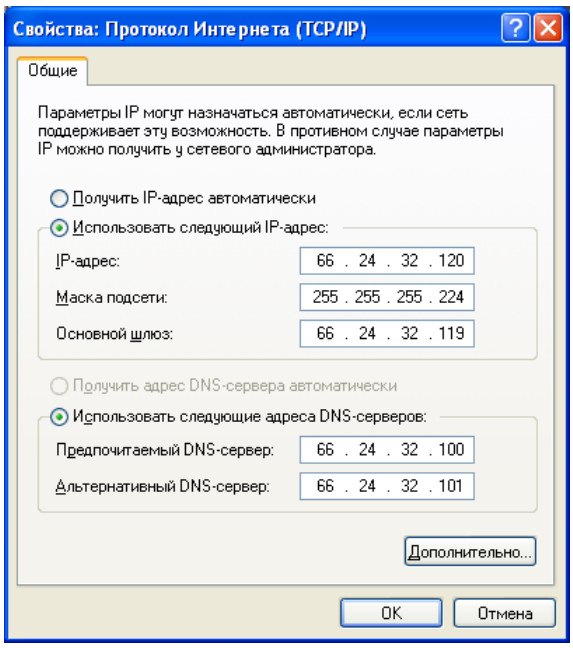


Схема 4.13

5. Щелкните **OK** в окне **Свойства: Протокол Интернета (TCP/IP)**, затем щелкните **OK** в **Подключение по локальной сети - свойства**.

6. Теперь ваше местное подсоединение настроено для связи с провайдером услуг Интернет и доступа к сети Интернет. Закройте все имеющиеся окна.

Проверьте свое подключение к Интернет

7. Для проверки Интернет-подключения откройте **Internet Explore.** Введите **http://www.microsoft.ru/** в адресную строку. Нажмите **Переход** или **Enter** для загрузки веб-страницы. Если ваше Интернет-подключение работает верно, то вы получите страницу, схожую с той, что показана на схеме 4.14.

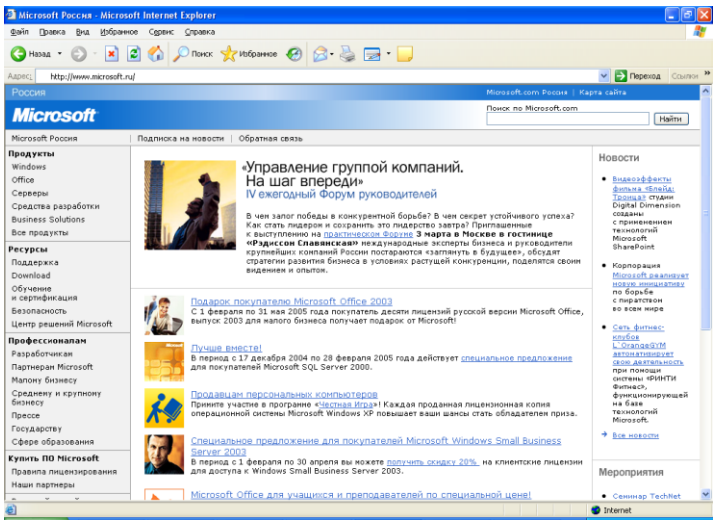


Схема 4.14

Лабораторная работа №5 ***«Оценка пропускной способности каналов связи»***

Цель работы: приобретение знаний и практических навыков, необходимых для оценки пропускной способности каналов связи.

Оборудование: ПЭВМ (15), интерактивная доска, локальная сеть.

Теоретические сведения.

Пропускная способность канала связи - Наибольшая скорость передачи информации по каналу связи. Скорость передачи зависит от физических свойств канала связи, статистических свойств помех, способа передачи и приема сигналов и др.

Пропускная способность двоичного канала

Нарисуем схему передачи информации.

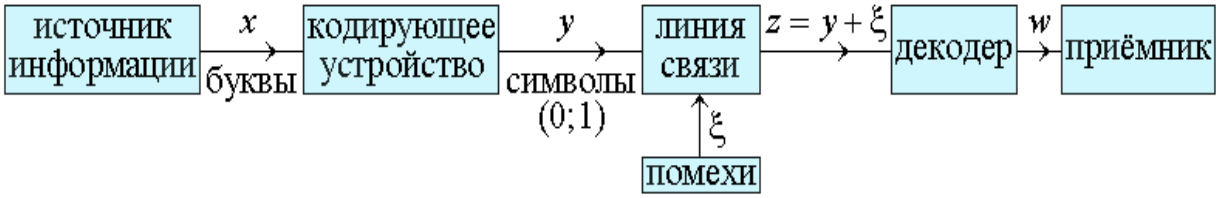


Рис. 2.9

Будем передавать по линии связи последовательность двоичных символов, состоящую из нулей и единиц. Помехи в линии связи могут превратить ноль в единицу и наоборот. Представим себе модель двоичной линии связи.

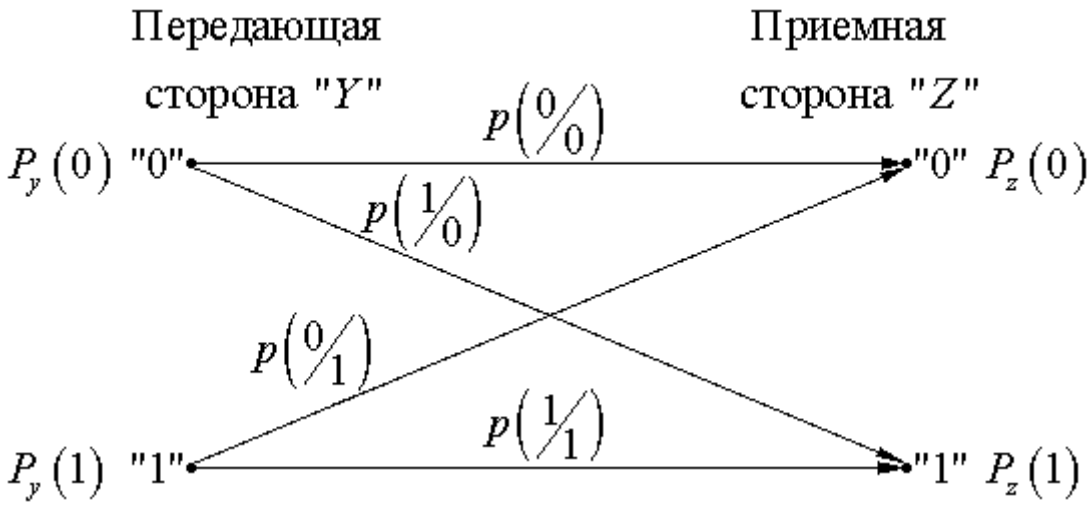


Рис. 2.10

Введены следующие обозначения:

вероятность безошибочной передачи "0" – , т.е. вероятность получения "0" на приёмной стороне, если передавался "0";

$p(1/0)$ – вероятность получения единицы на приёмной стороне, если передавался "0";

аналогично введем и ;

$P_y(0)$ и $P_y(1)$ – вероятности встречаемости нуля и единицы на передающей стороне;

$P_z(0)$ и $P_z(1)$ – вероятности встречаемости нуля и единицы на приёмной стороне.

Конечно, выполняются условия:

$$P_y(0)+P_y(1)=1; \quad p\left(\frac{0}{0}\right)+p\left(\frac{1}{0}\right)=1;$$

$$P_z(0)+P_z(1)=1; \quad p\left(\frac{1}{1}\right)+p\left(\frac{0}{1}\right)=1.$$

Подсчет пропускной способности линии связи будем вести по формуле:

$$C_{\text{лс}} = \max_{p_y(0)} I_{\text{на 1 символ}}(Z;Y) V_{\text{лс max}}, \quad (2.1)$$

где $V_{\text{лс max}}$ – максимальная скорость передачи импульсов по данной линии связи;

$\max_{p_y(0)} I_{\text{на 1 символ}}(Z;Y)$ – максимальное количество информации, приходящееся в среднем на один символ.

$V_{\text{лс max}}$ считается по формуле

$$V_{\text{лс max}} = \frac{1}{\Delta t_{\min}}\left[\text{имп}/\text{сек}\right], \quad (2.2)$$

где $\Delta t_{\min}$ – минимально допустимый интервал времени для передачи по данной линии связи. Он определяется физическими свойствами линии связи (тонкий или толстый коаксиал; витая пара; оптический канал). $\Delta t_{\min}$ определяется по формуле Котельникова В.А. (будет рассмотрена в главе 8) по формуле:

$$\Delta t_{\min} = \frac{1}{2F_{\max}}\left[\text{сек}\right], \quad (2.3)$$

где $F_{\max}$ – максимальная частота, пропускаемая этим каналом. Она определяется экспериментально путём подачи на вход канала сигнала постоянной амплитуды и переменной частоты. http://peredacha-informacii.ru/ Если амплитуда на выходе канала упадет до , то эта частота и принимается за максимальную (см. рис. 2.11).

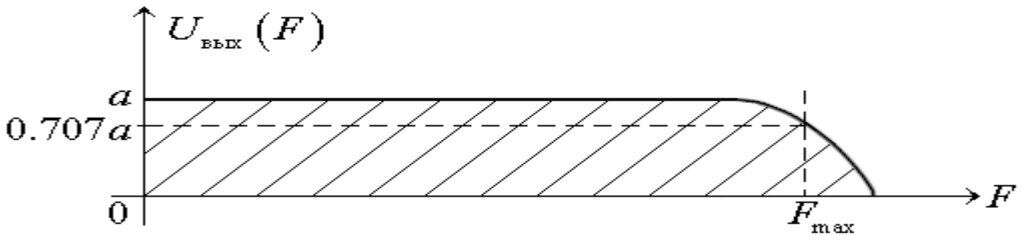


Рис. 2.11

$$\max_{p_y(0)} I_{\text{нал символ}}(Z;Y)$$

зависит от помех и от вероятностей встречаемости нулей и единиц на передающей стороне

$$I_{\text{нал символ}}(Z;Y) = H_{\text{апр}}(Z) - H_{\text{апост}}\left(Z/Y\right) \quad . \qquad (2.4)$$

$$H_{\text{апр}}(Z) = -P_z(0)\log P_z(0) - P_z(1)\log P_z(1) \quad . \qquad (2.5)$$

$$H_{\text{апост}}\left(Z/Y\right) = \sum_{i=1}^{2} P_y(i)\cdot H\left(Z/i\right) = P_y(0)\cdot H\left(Z/0\right) + P_y(1)\cdot H\left(Z/1\right) =$$
$$= P_y(0)\cdot\left[-P\left(0/0\right)\log P\left(0/0\right) - P\left(1/0\right)\log P\left(1/0\right)\right] + \qquad (2.6)$$
$$+\left[1-P_y(0)\right]\cdot\left[-P\left(1/1\right)\log P\left(1/1\right) - P\left(0/1\right)\log P\left(0/1\right)\right].$$

$H_{\text{апост}}(Z)$ – это остаточная неопределенность на приёмной стороне, если известно какой символ со стороны Y передавался.

$P_z(0)$ и $P_z(1)$ – определяют априорную неопределенность на стороне "Z". При этом

$$P_z(0) = P_y(0)\cdot P\left(0/0\right) + P_y(1)\cdot P\left(0/1\right) \quad ; \qquad (2.7)$$

$$P_z(1) = P_y(1)\cdot P\left(1/1\right) + P_y(0)\cdot P\left(1/0\right) \quad . \qquad (2.8)$$

Все необходимые для расчета пропускной способности линии связи формулы приведены.

Рассмотрим три частных случая.

1. Отсутствие ошибок, т.е. .

Тогда $P_z(0) = P_y(0)$ и $P_z(1) = P_y(1)$; ;

$$\boxed{C_{\text{пс}}} = \max_{p_y(0)} I_{\text{нал символ}}(Z;Y)\cdot V_{\text{пс max}} = \max_{p_y(0)} H_{\text{апр}}(y)\cdot V_{\text{пс max}} = \qquad (2.9)$$
$$= \underbrace{\max_{p_y(0)}\left(-P_y(0)\log P_y(0) - \left(1-P_y(0)\right)\log\left(1-P_y(0)\right)\right)}_{1}\cdot V_{\text{пс max}} = \boxed{V_{\text{пс max}}}.$$

То есть в этом случае максимальная пропускная способность линии связи равна максимальной скорости передачи нулей и единиц по этой линии связи при условии, что вероятность передачи нулей и единиц на передающей стороне одинакова, т.е.$P_y(0) = P_y(1) = 1/2$.

2. Имеет место , т.е. доля ошибок при передаче нулей и единиц одинакова. Это двоичный симметричный канал.

Подставив $p_{ош}$ в формулу 2.6, имеем:

$$H_{апост}\left(Z/Y\right) = \tag{2.10}$$
$$= P_y(0)\underbrace{\left[-p_{ош}\log p_{ош} - (1-p_{ош})\log(1-p_{ош})\right]}_{H(p_{ош})} + \left[1-P_y(0)\right]\cdot H(p_{ош}) =$$
$$= H(p_{ош}),$$

а формула 2.1 может быть видоизменена

$$\boxed{C_{лс}} = \max_{p_y(0)} I_{на1\,символ}(Z;Y)\cdot V_{лс\,max} = V_{лс\,max}\cdot \max_{p_y(0)}\left[H_{апр}(z) - H(p_{ош})\right] = \tag{2.11}$$
$$= V_{лс\,max}\cdot\left[\max_{p_y(0)} H_{апр}(z) - H(p_{ош})\right] = \underline{\boxed{V_{лс\,max}\left[1-H(p_{ош})\right]}}.$$

3. При придётся воспользоваться всем набором формул от 2.1 до 2.8. Лучше решать задачу не в общем виде, а подставлять числовые значения и .

Вероятность $P_y(0)$, дающую $\max\limits_{p_y(0)} I_{на1\,символ}(Z;Y)$, искать через приравнивание $I'_{на\ 1\ символ}(Z; Y)$ нулю. Решение уравнения $I'(Z; Y) = 0$ получить графически, задавая различные значения $P_y(0)$.

Задача для самостоятельного решения:

Задавшись разными значениями и , подсчитайте пропускную способность двоичного ассиметричного канала. В расчётах примите

$$p\left(1/0\right) = 2p\left(0/1\right) = 0.001\cdot n,$$

где n – ваш номер в списке группы.

При расчетах должно получиться p(0) > 0.5, если и наоборот.

Пропускная способность канала должна лежать между

$[1 – H(p_{ош\ min})]V_к$ и $[1 – H(p_{ош\ max})]V_к$.

Расчет приведите в рабочей тетради.

Лабораторная работа № 6 «Объединение компьютеров в локальную вычислительную сеть»

Цель работы:

- Получить практические навыки в соединении компьютеров в локальную сеть;
- Выполнить диагностику и устранить неполадки, возникающие в процессе соединения.

Необходимое оборудование и материалы:

- Компьютеры.
- Кабель UTP категории 5.
- Разъемы RJ-45.
- Щипцы для обжима.
- LAN-Tester (Устройство для проверки правильности и качества обжима).
- Сетевые карты.
- Коммутатор или концентратор.

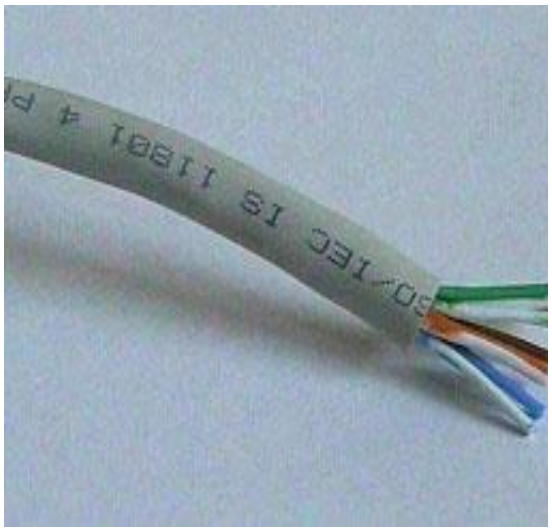
Теоретические сведения.

Разъемы RJ-45

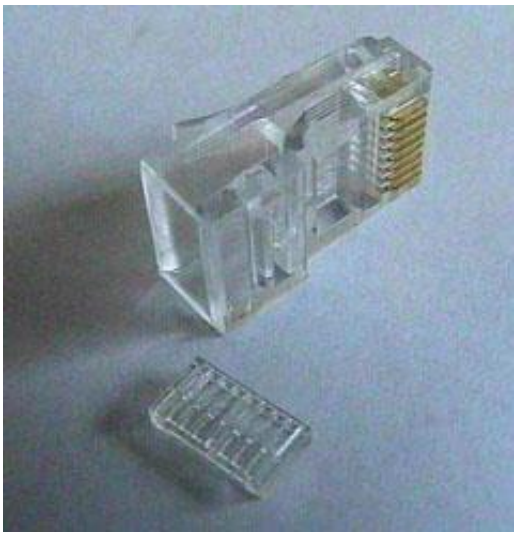
Для подключения витых пар используются разъемы стандарта RJ-45 , которые в зависимости от вида кабеля витой пары бывают:

- экранированными или неэкранированными;
- для одножильных или многожильных витых пар;
- конструктивно выполненными со вставками или без вставок. Вставки выполняют роль направляющих для проводников витой пары, упрощающих заправку проводников в корпус разъема.

Кабель из 4-х неэкранированных витых пар



Разъем RJ-45 для витой пары со вставкой



Корпуса разъемов выполнены из прозрачного пластика, поэтому внутренние части контактов разъема хорошо различимы. Нужно обратить внимание на конструктивное выполнение тех частей контактов, которые предназначены для соединения с проводниками витой пары. Контакты разъемов для многожильных проводников имеют вид двухзубой вилочки, внутренние поверхности зубцов которой имеют заточку по типу ножа и при обжимке прорезают изоляцию проводника, раздвигая его жилы, таким образом создается контакт.

В разъемах для одножильных проводников зубцы вилочки слегка раздвинуты в стороны и при обжимке охватывают жилу с двух сторон, прорезая изоляцию и создавая контакт.

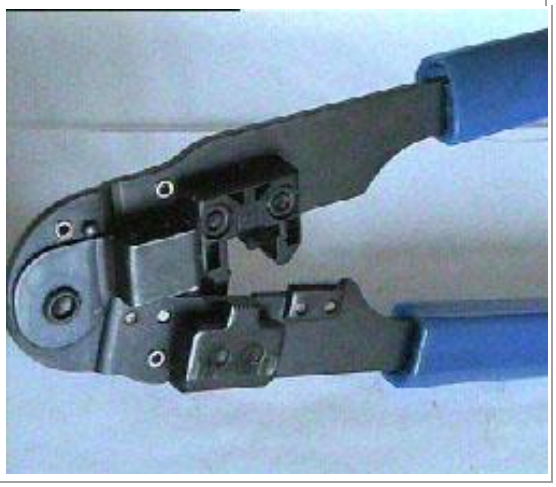
Для разделки витых пар используют специальное устройство (обжим), которое имеет три рабочие области и соответственно выполняет три функции.

Ближе всего к рукояткам устройства располагается область, в которой установлен нож для обрезания проводников витой пары.

В центре находится гнездо для обжима разъема.

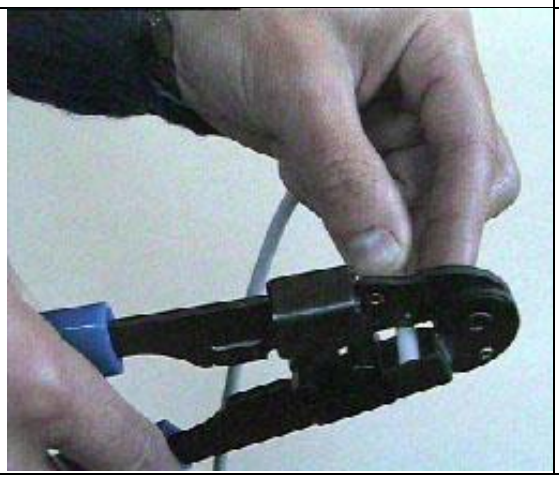
В верхней части устройства--область для зачистки наружной изоляции витой пары (внутренняя изоляция проводников не зачищается, а как уже было сказано прорезается контактами разъема).

Устройство для зачистки и обжима витых пар



1. Последовательность операций при разделке разъема витой пары

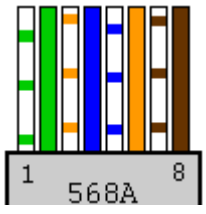
Вначале проводят зачистку наружной изоляции кабеля. При зачистке плоского кабеля его упирают в специальный выступ на устройстве, расположенный в области зачистки, чтобы получить глубину зачистки под стандартный разъем, зажимают кабель и рывком производят зачистку. Немного более сложным выглядит процесс зачистки круглых кабелей витых пар. Наружную изоляцию круглого кабеля лучше только слегка надрезать, осторожно поворачивая его в области зачистки, а затем снять кусочек изоляции по кольцевому надрезу вручную.

Зачистка наружной изоляции круглого кабеля витой пары	Удаление наружной изоляции по кольцевому надрезу
	

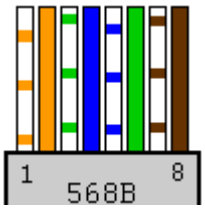
После зачистки разводят провода витой пары в одной плоскости в определенном порядке, выравнивают длину всех проводов и еще раз ровно подрезают. Порядок разводки проводов для разъемов RJ-45 определяется стандартом EIA/TIA568A или EIA/TIA568B.

Стандарт EIA/TIA568B более распространен, хотя принципиальной разницы между этими двумя стандартами нет. Для получения прямого кабеля для подключения к активному оборудованию нужно, чтобы порядок разводки с обоих концов кабеля был одинаковым. Для получения перекрестного (CROSSOVER) кабеля для соединения двух сетевых адаптеров напрямую необходимо с разных концов кабеля использовать разные стандарты.

1	белый/зеленый
2	зеленый
3	белый/оранжевый
4	синий
5	белый/сини
6	оранжевый
7	белый/коричневый
8	коричневый

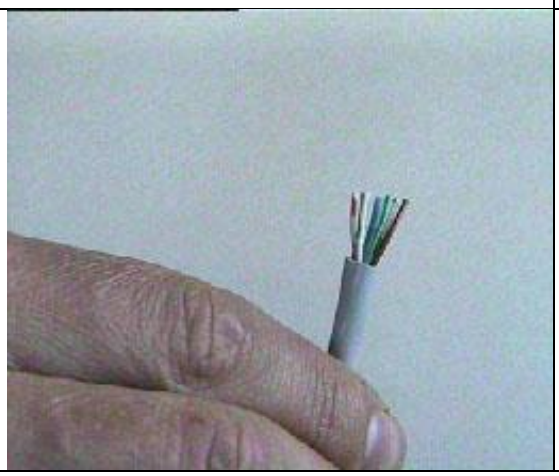
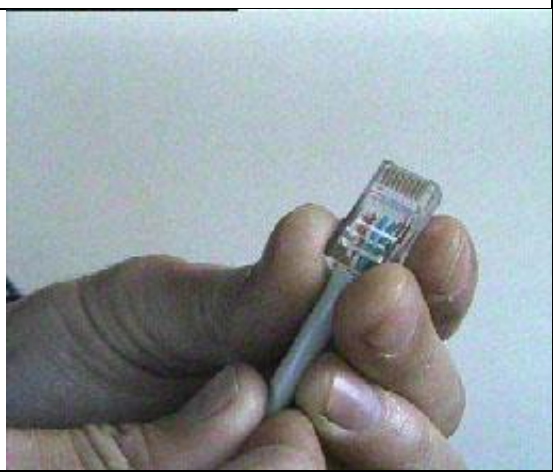


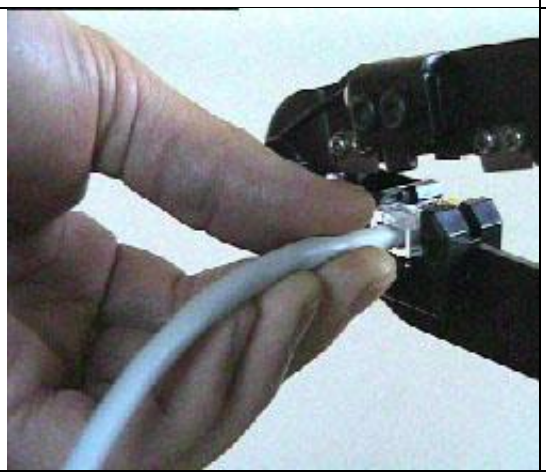
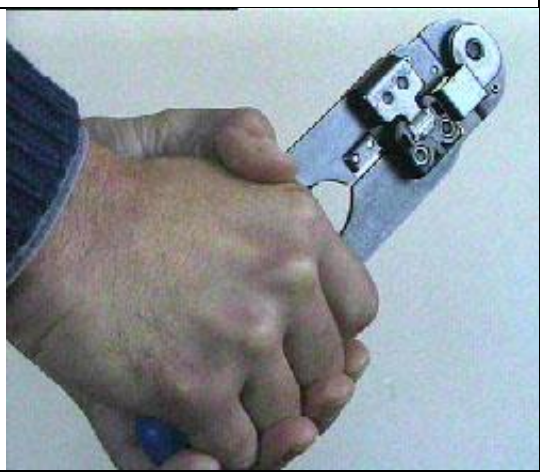
1	белый/оранжевый
2	оранжевый
3	белый/зеленый
4	синий
5	белый/синий
6	зеленый
7	белый/коричневый
8	коричневый



Затем производят заправку проводников в разъем и обжимку. Рекомендуется по возможности использовать разъемы без вставки, так как процесс заправки проводников в корпус такого разъема выполняется проще.

Если конструктивно разъем выполнен без вставки, то проводники аккуратно заправляются в его корпус до упора в торец разъема. Затем вставляют разъем в гнездо обжимного устройства и надавливают до тех пор, пока устройство полностью не закроется.

Кабель витой пары, подготовленный для заправки в разъем	Заправка проводников витой пары в разъем RG-45 без вставки
	

Установка разъема RJ-45 в гнездо обжимного устройства	Обжимка разъема
	

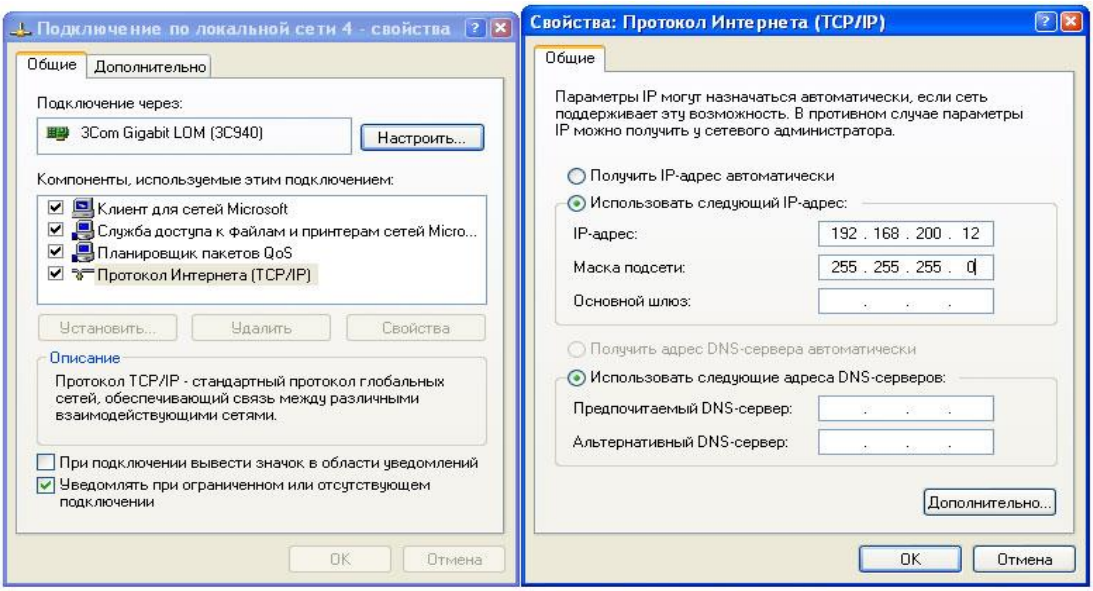
Если в конструкцию разъема входит вставка, то сначала на проводники витой пары надевается вставка. Вставка имеет форму крышки спичечного коробка, на одной из поверхностей которого имеются прорези по количеству проводников в витой паре. Вставку надевают на проводники таким образом: чтобы прорези были обращены к корпусу разъема. После насаживания вставки проводники витой пары еще раз подрезают и выравнивают срез с краем вставки. Для закрепления вставки в этом положении полезно у ее противоположного конца обжать проводники пальцами, чтобы вставка не смещалась. Затем вставку с проводниками вставляют в корпус разъема до тех пор, пока она не упрется в торец разъема, и обжимают разъем также как в случае разъема без вставки.

4. Порядок выполнения работы

Задание 1. Соединить два компьютера между собой без использования активного сетевого оборудования типа коммутатора, концентратора.

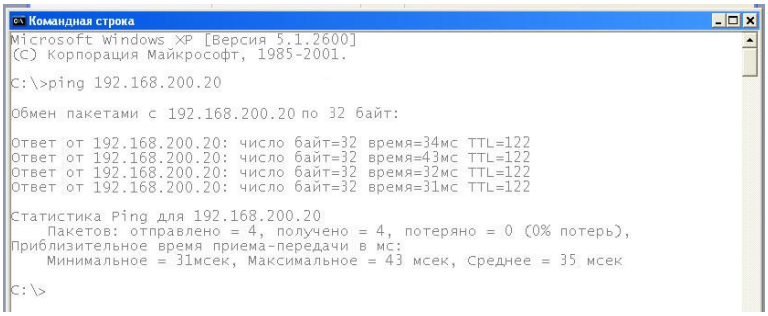
1. Для выполнения работы подгруппа разделяется на несколько бригад. Каждой бригаде студентов предоставляются 2 компьютера, которые необходимо объединить в сеть.
2. Включить компьютеры и проверить их работоспособность.
3. Установить в компьютеры сетевые карты. Перед установкой сетевых карт необходимо ВЫКЛЮЧИТЬ питание. Обязательно закрепить карты при помощи винта.
4. Обжать кабель для соединения двух компьютеров. Обжим выполняется перекрестным способом. Убедиться в успешности обжимки при помощи тестера.
5. Соединить компьютеры обжатым кабелем.
6. Включить компьютеры.
7. Убедиться в исправности сетевых карт. Обычно на сетевых картах имеется индикатор «LINK». Он показывает наличие физического соединения по сетевому кабелю. Соответственно, при отключенном кабеле индикатор гореть не должен, а при правильно подключенном с обоих концов кабеле – должен. Если это так – сетевая карта скорее всего физически исправна.
8. Если индикатор не включен, проверить правильность обжима кабеля с помощью тестера и при необходимости повторить обжим кабеля.
9. Установить драйверы сетевых карт. Операционная система обнаруживает новое оборудование, если оно поддерживает стандарт Plug and Play. Далее, если драйвер устройства входит в дистрибутив системы – он устанавливается оттуда, если не входит – с носителя, поставляемого вместе с устройством. Дистрибутив Windows находится на диске C в папке \win 98 SE. Драйверы устройств записаны на диске C в папке \ drivers\. Беспроблемное обнаружение устройства, установка драйверов и отображение сообщения «устройство работает нормально» в свойствах устройства в диспетчере устройств свидетельствуют об исправности сетевой карты. При неисправности сетевой карты заменить ее и повторить проверку.
10. Произвести настройку протокола IP. Назначить компьютерам статические
11. IP-адреса (не одинаковые и принадлежащие одной подсети) и указать маску подсети.

Например:



Убедиться в наличии соединения между компьютерами. Проверку связи между компьютерами можно выполнить с помощью утилиты ping. Для этого в командной строке вводится ping и адрес проверяемого компьютера. Можно использовать IP-адрес, Net BIOS имя.

Например:



Если проверка проходит нормально, значит сеть полностью работоспособна.

Создать на диске временную папку, установить на нее общий доступ. Со второго компьютера попробовать скопировать в нее файлы. Нормальное копирование данных подтверждает работоспособность сети.

Задание 2. Соединить компьютеры между собой с использованием активного сетевого оборудования.

1. Задание 2 выполняется, после того, как все бригады выполнили задание №1.

2. Для соединения компьютеров с активным оборудованием необходимо обжать дополнительные кабели (по одному на каждый компьютер). Кабель должен быть прямым, а не перекрестным, то есть иметь одинаковый стандарт обжима с обоих концов. Хотя, в настоящее время часто встречается оборудование, автоматически определяющее тип подключенного кабеля, и способное работать как с тем, так и с другим.

3. Подключить все компьютеры к коммутатору или концентратору с помощью подготовленных кабелей.

4. Проверить, что все компьютеры находятся в одной подсети, и если это не так, изменить IP-адреса должным образом.

5. Проверить, есть ли доступ к общим ресурсам всех компьютеров. При отсутствии доступа проверить правильность обжима кабелей и исправность сетевых карт. Добиться работоспособности всей сети.

Возможные проблемы при соединении компьютеров:

– Неверно или некачественно обжат кабель. В этом случае процедуру обжимки придется повторить с самого начала.

– Разъем неплотно вставлен в гнездо сетевой карты. Вставлять разъем нужно до защелкивания собачки.

– Неисправна сетевая карта. В этом случае сетевую карту необходимо заменить.

– Неверно прописан IP адрес машины. Оба компьютера должны находиться в одной подсети. Это означает, что маски подсети у них одинаковы, номера подсетей совпадают, а номера хостов могут быть любыми допустимыми, но не одинаковыми.

5 Содержание отчета:

– Тема и цель работы

– Теоретические сведения о стандартах обжима витой пары (различие в использовании)

– Последовательность выполнения задания

– Анализ обнаруженных неисправностей и способы их устранения

– Вывод по лабораторной работе (рекомендации по устранению неполадок, порядок проверки неисправностей)

6 Контрольные вопросы:

1. Какое оборудование необходимо использовать при объединении двух компьютеров в сеть без активного сетевого оборудования ?

2. Как проверить правильность обжима сетевого кабеля?

3. Какой способ обжима кабеля используется при подключении компьютера к коммутатору?

4. Как определить исправность сетевой карты?

5/ Как проверить наличие связи между компьютерами?

6. В каком случае используются сетевые кабели с перекрестным обжимом?

7. Как должны быть назначены адреса компьютеров одной сети?

8. Как проверить возможность доступа к общим ресурсам сети?

9. Что может быть причиной нарушения связи между компьютерами сети?

10. В чем заключается настройка протокола IP при объединении компьютеров в сеть?

Лабораторная работа №7 Тема: Применение сетевых утилит для определения работоспособности сети.

Цель занятия: Получить навыки использования стандартных сетевых утилит ОС Windows.
Продолжительность занятия: 4 часа.

Краткие теоретические и справочно-информационные материалы по теме занятия.
Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для решения этих задач регулярно производится сбор данных, который дает базу для измерения реакции сети на изменения и перегрузки. Чтобы осуществить сетевую передачу, нужно проверить корректность подключения клиента к сети, наличие у клиента хотя бы одного протокола сервера, знать IP-адрес компьютеров сети и т. д. Поэтому в сетевых операционных системах, и в частности, в Windows, существует множество мощных утилит для пересылки текстовых сообщений, управления общими ресурсами, диагностике сетевых подключений, поиска и обработки ошибок. Утилиты запускаются из сеанса интерпретатора команд Windows XP (Пуск -> Выполнить -> cmd).
Сетевые утилиты
Утилита *hostname*
Выводит имя локального компьютера (хоста). Она доступна только после установки поддержки протокола TCP/IP. Пример вызова команды *hostname:*
C:\Documents and Settings\Администратор>hostname
1.2. Утилита *ipconfig*
Выводит диагностическую информацию о конфигурации сети TCP/IP. Эта утилита позволяет просмотреть текущую конфигурацию IP-адресов компьютеров сети. Синтаксис утилиты *ipconfig:*
ipconfig [/all | */renew* [адаптер] | */release* [адаптер]],
где *all* - выводит сведения о имени хоста, DNS (Domain Name Service), типе узла, IP-маршрутизации и др. Без этого параметра команда *ipconfig* выводит только IP-адреса, маску подсети и основной шлюз;
/renew [адаптер] - обновляетпараметры конфигурации DHCP (Dynamic Host Configuration Protocol - автоматическая настройка IP- адресов). Эта возможность доступна только на компьютерах, где запущена служба клиента DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров;
/release [адаптер] - очищает текущую конфигурацию DHCP. Эта возможность отключает TCP/IP на локальных компьютерах и доступна только на клиентах DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров. Эта команда часто используется перед перемещением компьютера в другую сеть. После использования утилиты *ipconfig /release*, IP-адрес становиться доступен для назначения другому компьютеру.
Запущенная без параметров, команда *ipconfig* выводит полную конфигурацию TCP/IP, включая IP адреса и маску подсети.
Пример использования *ipconfig* без параметров: *C:\Documents and Settings\Администратор>ipconfig*
Настройка протокола IP для Windows Подключение по локальной сети - Ethernet адаптер:
DNS-суффикс этого подключения . . :
IP-адрес . . . . . : 10.10.11.70
Маска подсети . . . . . : 255.255.252.0
Основной шлюз . . . . . : 10.10.10.1

Утилита *net view*
Просматривает список доменов, компьютеров или общих ресурсов на данном компьютере.
Синтаксис утилиты *netview:*
net view [\\компьютер | */domain[:*домен]]; *net view /network:nw* [\\компьютер] - используется в сетях Novell NetWare,

где *компьютер* - задает имя компьютера для просмотра общих ресурсов;
*/domain[:*домен] - задает домен (рабочую группу), для которого выводится список компьютеров. Если параметр не указан, выводятся сведения обо всех доменах в сети;
/network:nw - выводит все доступные серверы в сети Novell NetWare. Если указано имя компьютера, выводится список его ресурсов в сети NetWare. С помощью этого ключа могут быть просмотрены ресурсы и в других локальных сетях.
Вызванная без параметров, утилита выводит список компьютеров в текущем домене (рабочей группе).

Пример с параметром *компьютер:*

C:\Documents and Settings\Администратор>net view \\- /Domain:Lab-261 Общие ресурсы на \\-

Имя общего ресурса Тип Используется как Комментарий
---------- NONE (H) Диск
Команда выполнена успешно.

Утилита ping
Проверяет соединения с удаленным компьютером или компьютерами. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты *ping:*
ping [-t] [-a] [-n счетчик] [-l длина] [-f] [-i ttl] [-v тип] [-r счетчик] [-s число] [[-j список комп] | [-k список комп]] [-w интервал] список назн,
где *-t* - повторяет запросы к удаленному компьютеру, пока программа не будет остановлена;
-a - разрешает имя компьютера в адрес;
-n счетчик - передается число пакетов ECHO, заданное параметром. По умолчанию - 4;
-l длина - отправляются пакеты типа ECHO, содержащие порцию данных заданной длины. По умолчанию - 32 байта, максимум - 65500; -f - отправляет пакеты с флагом запрещения фрагментации (Do not Fragment). Пакеты не будут разрываться при прохождении шлюзов на своем маршруте;
-i ttl - устанавливает время жизни пакетов TTL (Time To Live); -v *тип* - устанавливает тип службы (Type Of Service) пакетов; *-r счетчик* - записывает маршрут отправленных и возвращенных пакетов в поле записи маршрута Record Route. Параметр счетчик задает число компьютеров в интервале от 1 до 9;
-s число - задает число ретрансляций на маршруте, где делается отметка времени;
-j список комп - направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке могут быть разделены промежуточными шлюзами (свободная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;
-k список комп - направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке не могут быть разделены промежуточными шлюзами (ограниченная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;
-список назн - указывает список компьютеров, которым направляются запросы; Пример использования утилиты ping с параметром *список назн:* ***C****:\Documents and Settings\Администратор>ping 10.10.10.1*
Обмен пакетами с 10.10.10.1 по 32 байт:
Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128 Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128 Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128 Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128 Статистика Ping для 10.10.10.1:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь), Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
Утилита *netstat*
Выводит статистику протокола и текущих подключений сети TCP/IP. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утили ты *netstat:*

netstat [-a] [-e] [-n] [-s] [-p протокол] [-r] [интервал],
где *-a* - выводит все подключения и сетевые порты. Подключения сервера обычно не выводятся;
-e - выводит статистику Ethernet. Возможна комбинация с ключом *-s;*
-n - выводит адреса и номера портов в шестнадцатеричном формате (а не имена);
s - выводит статистику для каждого протокола. По умолчанию выводится статистика для TCP, UDP, ICMP (InternetControl Message Protocol) и IP. Ключ *-p* может быть использован для указания подмножества стандартных протоколов;
-p протокол - выводит соединения для протокола, заданного параметром. Параметр может иметь значения *tcp* или*udp.* Если используется с ключом *-s* для вывода статистики по отдельным протоколам, то параметр может принимать значения *tcp, udp, icmp* или *ip; -r* - выводит таблицу маршрутизации;
интервал - обновляет выведенную статистику с заданным в секундах интервалом. Нажатие клавиш CTRL+Сстанавливает обновление статистики. Если этот параметр пропущен, *netstat* выводит сведения о текущей конфигурации один раз.

Утилита tracert

Диагностическая утилита, предназначенная для определения маршрута до точки назначения с помощью посылки эхо-пакетов протокола ICMP с различными значениями срока жизни (TTL, Time-To-Live). При этом требуется, чтобы каждый маршрутизатор на пути следования пакетов уменьшал эту величину по крайней мере на 1 перед дальнейшей пересылкой пакета. Это делает параметр TTL эффективным счетчиком числа ретрансляций. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе- источнику сообщение ICMP «Time Exceeded». Утилита *tracert* определяет маршрут путем посылки первого эхо-пакета с параметром TTL, равным 1, и с последующим увеличением этого параметра на единицу до тех пор, пока не будет получен ответ из точки назначения или не будет достигнуто максимальное допустимое значение TTL. Маршрут определяется проверкой сообщений ICMP «TimeExceeded», полученных от промежуточных маршрутизаторов. Однако некоторые маршрутизаторы сбрасывают пакеты с истекшим временем жизни без отправки соответствующего сообщения. Эти маршрутизаторы невидимы для утилиты*tracert.*
Синтаксис утилиты *tracert:*
tracert [-d] [-h макс_узл] [-j список компьютеров] [-w интервал] точка назн,
где *-d* - отменяет разрешение имен компьютеров в их адреса;
-h макс_узл - задает максимальное количество ретрансляций, используемых при поиске точки назначения;
-j список компьютеров - задает список_компьютеров для свободной маршрутизации;
-w интервал - задает интервал в миллисекундах, в течение которого будет ожидаться ответ;
точка назн - указывает имя конечного компьютера.
Пример использования утилиты *tracert:*
C:\Documents and Settings\Администратор>tracert 10.10.10.1

Трассировка маршрута к 10.10.10.1 с максимальным числом прыжков 30 1 <1 мс <1 мс <1 мс 10.10.10.1

Трассировка завершена.

1.3. Утилита *net use*

Подключает общие сетевые ресурсы или выводит информацию о подключениях компьютера. Команда также управляет постоянными сетевыми соединениями. Синтаксис утилиты *net use:*
*net use [устройство | *] [\\компьютер\ресурс[\том]] [пароль | *]] [/user:[домен\]имя пользователя] [[/delete] | [/persistent:{yes | no}]] net use устройство [/home[пароль | *]] [/delete: {yes | no}] net use [/persistent:{yes | no}],*

где *устройство* - задает имя ресурса при подключении/отключении. Существует два типа имен устройств: дисководы (от D: до Z:) и принтеры (от LPT1: до LPT3:). Ввод символа звездочки обеспечит подключение к следующему доступному имени устройства;

\\компьютер\ ресурс - указывает имя сервера и общего ресурса. Если параметр компьютер содержит пробелы, все имя компьютера от двойной обратной черты (\\) до конца должно быть заключено в кавычки (" "). Имя компьютера может иметь длину от 1 до 15 символов; *\том* - задает имя тома системы Novell NetWare. Для подключения к серверам Novell NetWare должна быть запущена служба клиента сети Novell NetWare (для Windows 2000 Professional) или служба шлюза сети Novell NetWare (для Windows 2000 Server);

пароль - задает пароль, необходимый для подключения к общему ресурсу;

* - выводит приглашение для ввода пароля. При вводе с клавиатуры символы пароля не выводятся на экран;

/user - задает другое имя пользователя для подключения к общему ресурсу;

домен - задает имя другого домена. Если домен не указан, используется текущий домен;

имя пользователя - указывает имя пользователя для подключения;

/delete - отменяет указанное сетевое подключение. Если подключение задано с символом звездочки, будут отменены все сетевые подключения;

/home - подключает пользователя к его основному каталогу;

/persistent -управляет постоянными сетевыми подключениями. По умолчанию берется последнее использованное значение. Подключения без устройства не являются постоянными;

yes - сохраняет все существующие соединения и восстанавливает их при следующем подключении;

no - не сохраняет выполняемые и последующие подключения. Существующие подключения восстанавливаются при следующем входе в систему. Для удаления постоянных подключений используется ключ */delete.* Вызванная без параметров утилита *net use* извлекает список сетевых подключений.

Пример вызова команды *net use:*

C:\Documents and Settings\Администратор>net use

1.4. Утилита *Net share*

Управление общими ресурсами. При вызове команды *net share* без параметров выводятся сведения обо всех общих ресурсах локального компьютера.

Синтаксис

net share [*имя_ресурса*] **net share** [*имя_ресурса*=*диск*:*путь* [{**/users:***число*|**/unlimited**}]
[**/remark:"***текст***"**]
[/**cache:** {**manual**|**automatic**|**no**}]]**netshare** [*имя_ресурса* [{**/users:***число*|**unlimited**}]
[**/remark:"***текст***"**]
[/**cache:** {**manual**|**automatic**|**no**}]] **net share** [{*имя_ресурса*|*диск*:*путь*} **/delete**]

Параметры

имя_ресурса- Сетевое имя общего ресурса. Команда **net share** *имя_ресурса* выводит сведения об отдельном ресурсе.

диск:*путь*- Абсолютный путь к папке, которую требуется сделать общей.

/users:*число*- Максимальное количество пользователей, которым разрешен одновременный доступ к общему ресурсу.

/unlimited- Отмена ограничения на число пользователей, которым разрешен одновременный доступ к общему ресурсу.

/remark:"*текст***"**-Добавление описательного комментария к ресурсу. Текст следует заключать в кавычки.

/cache:automatic- Включение автономного кэширования клиентов с автоматической реинтеграцией.

/cache:manual- Включение автономного кэширования клиентов с реинтеграцией вручную.

/cache:no- Оповещение клиента о невозможности автономного кэширования.

/delete- Отмена общего доступа к ресурсу.

net help *команда* -Отображение справки для указанной команды **net**. **Заметки**

Чтобы предоставить общий доступ к папке, имя которой содержит пробелы, заключите диск и путь к папке в кавычки (например, **"C:\Новая папка"**).

При запросе списка всех общих ресурсов компьютера выводятся: имя общего ресурса, имена устройств или путь, связанный с устройством, а также комментарий к этому ресурсу.

Когда общий ресурс создается на сервере, его конфигурация сохраняется. После остановки службы «Сервер» все общие ресурсы отключаются, но после следующего запуска службы «Сервер» они будут восстановлены. Имена общих ресурсов, заканчивающиеся знаком **$**, не отображаются при обзоре локального компьютера с удаленного компьютера.

Примеры

Чтобы вывести сведения об общих ресурсах компьютера, введите: **net share**

Чтобы сделать папку «C:\Данные» общим ресурсом и включить примечание к нему, введите:

net share ОбщиеДанные=c:\Данные /remark:"Для отдела 123"

Чтобы отменить общий доступ к ресурсу Общие Данные, созданному в предыдущем примере, введите:

net share ОбщиеДанные /delete

Чтобы сделать папку «C:\Список рисунков» общим ресурсом Список, введите: **net share Список="c:\Список рисунков"**

3. Рекомендации и замечания

На основе рассмотренных сетевых утилит ОС Windows разрабатываются пользовательские приложения, реализующие мониторинг и диагностику локальных сетей. Они позволяют минимизировать усилия по поиску и исправлению ошибок в конфигурации сети и помогают системному администратору контролировать трафик. В настоящее время создано большое количество программ этого направления: Monitor It, Nautilus NetRanger, CiscoWorks2000, ServiceSentinel и д.р. Они распространяются через Internet на условиях freeware. Windows NT Server обладает встроенными инструментами мониторинга: Event Viewer, Performance Monitor, Network Monitor.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Получите имя своего компьютера;
3. Выведите список доступных сетевых ресурсов своего компьютера;
4. Спросив у соседа слева имя компьютера, просмотрите его общие ресурсы;
5. Получив свой IP адрес, «опросите» его. Сначала с минимальным размером пакета, затем с максимально возможным;
6. Используя ранее полученное от соседа слева имя компьютера, определите его IP адрес;
7. Используя IP адрес полученный в предыдущем пункте, проверьте подключение к нему, используя число ретрансляций на маршруте, где делается отметка времени, равное количеству его общих сетевых ресурсов;
8. Просмотрите список всех сетевых портов на вашем компьютере и сосчитайте количество открытых (прослушиваемых);
9. Определите маршрут до сайта yandex.ru, с максимальным числом прыжков, равным значению, полученному в предыдущем пункте;
10. Очистите текущую конфигурацию DHCP, затем обновите её;
11. Изучив утилиту **netsh**, измените с ее помощью свой IP адрес на статический – 192.168.1., маска подсети – 255.255.255.0;
12. Проверьте подключение к IP адресу из п.2.5;
13. Используя **netsh**, верните свой IP адрес на получение по DHCP;
14. Сделайте диск C:\ общим сетевым ресурсом, используя в качестве имени Фамилию, а в качестве комментария строку «Моя первая Шара»;
15. Выведите список общих сетевых ресурсов соседа слева;
16. Подключите созданный соседом ресурс в качестве сетевого диска «Z:»;

17. Выведите список подключений вашего компьютера;
18. Отключите сетевой диск «Z:» ;
19. Сделайте выводы;

Контрольные вопросы

1. Какой протокол необходим для работы с утилитой ***ping***? Найти описание и характеристики протокола.
2. Можно ли утилитой ***tracert*** задать максимальное число ретрансляций?
3. Какой результат выдаст утилита ***netstat*** с параметрами ***-a -s -r?*** Поясните полученный результат.
4. Что такое localhost?

Найти самостоятельно любую стандартную сетевую утилиту Windows.

Лабораторная работа № 8 «Преобразование форматов ip–адресов»

Цель: обобщение и систематизация знаний по теме «Адресация в сетях»

Задания к работе:

Задание 1. Переведите следующие двоичные числа в десятичные.

Двоичное значение

1. 1111011
2. 1001001101
3. 101101111
4. 1011110001
5. 10101100.00101000.00000000.00000000
6. 01011110.01110111.10011111.00000000
7. 10010001 0110000 10000000 00011001
8. 01111111 00000000 00000000 00000001

Задание 2. Переведите следующие десятичные числа в двоичные.

Десятичное значение

1. 250
2. 19
3. 348
4. 93
5. 874
6. 109.128.255.254
7. 131.107.2.89
8. 129.46.78.0

Задание 3. Укажите классы следующих IP-адресов.

Адрес

1. 126.102.128.0
2. 1.191.248.0
3. 185.74.41.184
4. 96.247.128.0
5. 168.224.0.1
6. 201.76.98.5
7. 186.112.0.10
8. 28.0.0.0

Задание 4. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

1. 131.107.256.80
2. 222.222.255.222
3. 31.200.1.1
4. 126.1.0.0
5. 190.7.2.0
6. 127.1.1.1
7. 198.121.254.255
8. 255.255.255.255

Контрольные вопросы:

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

2. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему?

Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?

3. Когда необходим уникальный идентификатор сети?

4. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

Лабораторная работа № 9 «Адресация в IP сетях. Подсети и маски»

Цель:

- Изучить принципы адресации в IP-сетях
- Выяснить назначение масок в IP-адресации.

Ход работы

- Изучение теоретического материала
- Задание 1
- Задание 2
- Задание 3
- Задание 4

Теоретическая часть

"Принципы IP-адресации"

- Типы адресов стека TCP/IP
- Классы IP-адресов
- Особые IP-адреса
- Порядок распределения IP-адресов

Теоретические сведения

Типы адресов стека TCP/IP

В стеке TCP/IP используются три типа адресов: локальные (называемые также аппаратными), IP-адреса и символьные доменные имена.

В терминологии TCP/IP под локальным адресом понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети. В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека TCP/IP предполагалось наличие разных типов локальных адресов. Если подсетью интерсети является локальная сеть, то локальный адрес - это MAC - адрес. MAC - адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов. MAC - адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC - адрес имеет формат 6 байт, например 11-AO-17-3D-BC-01.

Классы IP-адресов

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 - традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая - к номеру узла, определяется значениями первых бит адреса. Значения этих бит являются также признаками того, к какому классу относится тот или иной IP-адрес.

На рис. 1 показана структура IP-адреса разных классов.

Рис. 1. Структура IP-адреса

Если адрес начинается с 0, то сеть относят к классу A и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) Сетей класса A немного, зато количество узлов в них может достигать 2^{24}, то есть 16 777 216 узлов.

Если первые два бита адреса равны 10, то сеть относится к классу B. В сетях класса B под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса B является сетью средних размеров с максимальным числом узлов 2^{16}, что составляет 65 536 узлов.

Если адрес начинается с последовательности 110, то это сеть класса C. В этом случае под номер сети отводится 24 бита, а под номер узла - 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено 28, то есть 256 узлами.

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.

Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу E, Адреса этого класса зарезервированы для будущих применений.

В табл. 1 приведены диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей.

Таблица 1. Характеристики адресов разного класса

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

Большие сети получают адреса класса A, средние - класса B, а маленькие класса C.

Задание1. Выясните, каков будет порядок отправки информацию по адресам 192.168.193.31 и 192.167.192.3 для хоста с адресом 192.167.12.3 и маской подсети 255.255.0.0. Решение задачи запишите в отчет.

Как происходит передача данных

1. IP-адрес в двоичном представлении разбивается на 2 части - адрес сети (левая часть адреса) и адрес хоста (правая часть адреса).

Например, в адресе 190.167.34.2 первые 24 бита могут быть адресом сети, а последние 8 - адресом хоста.
Тогда наш адрес будет выглядеть как 10111110101001110010001000000010, где зеленым цветом выделена сетевая часть адреса (она одинакова для всех хостов локальной сети), а красным - часть адреса, адресующая хост внутри локальной сети.

Для того, чтобы быстро вычислять по IP-адресу адрес сети или хоста, используется понятие **маски подсети (subnet mask)**. Это двоичное число, в котором все биты адреса сетевой части адреса равны 1, а все остальныебиты равны нулю. В нашем случае для адреса 10111110101001110010001000000010 получим маску подсети 11111111111111111111111100000000.

2. Маску подсети принято записывать в том же десятичном формате, что и IP-адрес. Для этого нужно каждый байт маски перевести в десятичное число и записать полученные десятичные числа через точки.
В нашем случае
Ответ:

$11111111_2=255$
$11111111_2=255$
$11111111_2=255$
$00000000_2=0$

255.255.255.0 - маска подсети.

Маску подсети в настоящее время все чаще называют маской сети, что точней отображает ее смысл.

3. Информационные пакеты пересылаются напрямую от компьютера-отправителя к компьютеру-получателю только в пределах одной сети. Если компьютер-получатель находится

в другой сети, то информация пересылается специальному компьютеру сети, который называется шлюзом (gateway). Его адрес всегда известен. Об этом заботится системный администратор. Компьютер-шлюз имеет связь с как минимум с одной другой сетью и ретранслирует информацию в нужном направлении. Этот процесс называется маршрутизацией (routing).

4. Если ваш компьютер, имеющий IP адрес 192.169.204.12 и маску подсети 255.255.192.0 должен отправить информацию компьютеру с адресом 192.169.198.15, то прежде всего ваш компьютер проверит, находится ли получатель информации в той же сети. Для этого двоичное представление адреса получателя он побитово умножит на двоичное представление маски подсети, то в результате получится адрес сети:

```
11000000101010001100011000001100 (адрес компьютера - получателя)
*
11111111111111111100000000000000 (текущая маска подсети)
--------------------------------------------------
11000000101010001100000000000000 (адрес сети получателя)
```

Аналогичную процедуру компьютер проделает со своим адресом для того, чтобы узнать адрес своей собственной сети:

```
11000000101010011100110000001100 (адрес компьютера - отправителя)
*
11111111111111111100000000000000 (текущая маска подсети)
--------------------------------------------------
11000000101010011100000000000000 (адрес своей собственной сети)
```

Если адрес сети получателя совпадает с адресом собственной сети, следовательно, получатель находится в локальной сети, и информация может быть послана напрямую. Если бы совпадения нет, то информация будет отправлена шлюзу (с адресом, например,192.168.192.2) с указанием адреса получателя 192.169.204.12, а он переслал бы ее в другую сеть. Этот процесс будет продолжаться до тех пор, пока информация не дойдет до получателя.

Задание2. Определение настроек протокола IP вашего компьютера
Для этого достаточно запустить программу ipconfig (в Windows 9X есть еще программа с графическим интерфейсом winipcfg). Получить доступ к командной строке и напечатайте ipconfig. Нажмите клавишу :

```
C:\>ipconfig

Настройка протокола IP для Windows

        DNS-суффикс этого подключения . . :
        IP-адрес  . . . . . . . . . . . . : 192.168.0.1
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 192.168.0.10

C:\>_
```

Занесите полученные параметры в отчет.

Примечание. Настройка протокола IP на каждом компьютере локальной сети - одна из задач системного администратора. Он может в принципе задать все параметры вручную. Но если число компьютеров в сети больше десятка, то удобней назначать настройки автоматически в момент загрузки компьютера. Для этого разработан специальный протокол DHCP (Dynamic Host Configuration Protocol). Наличие у компьютера правильного IP-адреса является совершенно необходимым условием его работы в Интернет.

Задание 3. Дополнить конспект лекции "Принципы адресации в IP-сетях" по плану:

1. Классы IP-адресов
2. Особые IP-адреса
3. Порядок распределения IP-адресов
4. Использование масок в IP-адресации

Задание 4. По IP -адресу определить идентификатор сети и идентификатор узла (подразумеваются стандартные классы IP-адресов):

192.168.1.1

126.15.25.5

221.186.52.65

125.14.7.8

1. Расчет адресного пространства локальной сети

2. ***Выполнить расчет пула адресов, для локальной сети исходя из выбранного варианта.***
3. ***Задание 2.1***
4. Локальная сеть состоит из 14 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 190.134.29.33/24. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть. (

5. ***Задание 2.2***
6. Локальная сеть состоит из 4 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 233.85.1.7/29. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

7. ***Задание 2.3***
8. Локальная сеть состоит из 114 компьютеров и двух серверов, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 85.45.35.69/25. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

9. ***Задание 2.4***
10. Локальная сеть состоит из 50 компьютеров и четыре сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 125.25.68.70/25. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

11. ***Задание 2.5***

12. Локальная сеть состоит из 2500 компьютеров и 20 серверов, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 25.25.68.70/17. Разбить сеть на 4 подсети, определить сколько компьютеров можно добавить в каждую сеть.

13. Задание 2.6

14. Локальная сеть состоит из 115 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 223.125.168.170/25. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

15. Задание 2.7

16. Локальная сеть состоит из 8 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 92.18.16.7/26. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

17. Задание 2.8

18. Локальная сеть состоит из 62 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 64.166.68.79/26. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

19. Задание 2.9

20. Локальная сеть состоит из 1400 компьютеров и десяти серверов, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 54.144.37.77/20. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

21. Задание 2.10

22. Локальная сеть состоит из 140 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 156.100.30.45/24. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

23. Задание 2.11

24. Локальная сеть состоит из 114 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 190.134.29.33/20. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

25. Задание 2.12

26. Локальная сеть состоит из 1440 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 233.85.1.7/19. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

27. Задание 2.13

28. Локальная сеть состоит из 124 компьютеров и двух серверов, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 85.45.35.69/25. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

29. Задание 2.14

30. Локальная сеть состоит из 150 компьютеров и четыре сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 125.25.68.70/25. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

31. Задание 2.15

32. Локальная сеть состоит из 700 компьютеров и 10 серверов, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 25.25.68.70/17. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

33. Задание 2.16

34. Локальная сеть состоит из 1105 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 223.125.168.170/21. Разбить сеть на 2 подсети, определить сколько компьютеров можно добавить в каждую сеть.

35. Задание 2.17

36. Локальная сеть состоит из 128 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 92.18.16.7/26. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

37. Задание 2.18

38. Локальная сеть состоит из 62 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 64.166.68.79/26. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

39. Задание 21.9

40. Локальная сеть состоит из 145 компьютеров и десяти серверов, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 54.144.37.77/20. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

41. Задание 2.20

42. Локальная сеть состоит из 250 компьютеров и одного сервера, рассчитать адреса каждого компьютера в сети, определить адрес сети и широковещательный адрес в сети. IP адрес одного из компьютеров 156.100.30.45/24. Определить, IP адрес сети, минимальный и максимальный адрес ПК, сколько компьютеров можно добавить в эту сеть.

43.

Занести в отчет

Вопросы:

2. IP-адрес, формат записи
3. Классы IP-адресов
4. Значения выделенных IP-адресов
5. Порядок распределения IP-адресов
6. Использование масок в IP-адресации
7. Утилита ipconfig. Назначение.

Лабораторная работа № 10 «Настройка протокола TCP/IP в операционных системах»

Цель работы: изучить принципы работы протоколов TCP/IP и научиться их настраивать для работы в сети Интернет

Теоретическая справка

Хотя Windows поддерживает большое количество сетевых протоколов, TCP/IP используется чаще всего по целому ряду причин:

• обеспечивает межсетевое взаимодействие компьютеров с разной аппаратной архитектурой и операционными системами;

• является основным протоколом, используемым в сетиИнтернет;
• необходим для функционирования Active Directory.

TCP/IP - это аббревиатура термина Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Протокол Internet). В терминологии вычислительных сетей протокол - это заранее согласованный стандарт, который позволяет двум компьютерам обмениваться данными. Фактически TCP/IP не один протокол, а несколько. Именно поэтому вы часто слышите, как его называют набором, или комплектом протоколов, среди которых TCP и IP - два основных.

В Windows параметры протокола TCP/IP являются частью параметров настройки сетевого адаптера, поэтому все изменения, связанные с этим протоколом, осуществляются через Панель управления.

Для настройки сетевых адаптеров и протоколов дважды щелкните значок Сеть и удаленный доступ к сети в Панели управления. Вы также можете выбрать пункт Свойства в контекстном меню папки МоеВ появившемся окне представлены различные соединения вашего компьютера с внешним миром. После успешной установки сетевого адаптера (во время установки или позже) в окне должен присутствовать как минимум один значок с именем Подключение по локальной сети.

Двойной щелчок значка выводит окно с информацией о состоянии соединения. Можно узнать длительность соединения, его скорость, количество отправленных и принятых пакетов данных.

Кнопка Отключить позволяет выключить сетевой адаптер, прекратив тем самым обмен данными через него. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения. Отключенные соединения отображаются в виде "серых" значков.

Кнопка Свойства вызывает окно настройки свойств соединения, в том числе и параметров используемых протоколов. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения

В этом окне можно получить информацию о сетевом адаптере, через который осуществляется соединение. Щелкнув кнопку *Настроить,* вы откроете окно свойств сетевого адаптера и сможете их изменить.

Установив флажок *Вывести значок подключения на панель задач,* вы включите отображение значка, представляющего соединение, на панели задач Windows. Это позволит наблюдать за активностью соединения и быстро осуществлять его настройку, не используя *Панель управления.*

В центральной части окна в списке представлены все клиенты, службы и протоколы, связанные соединением Для нормального функционирования домена или рабочей группы Windows необходимо наличие следующих компонентов

Компонент	Описание
Клиент для сетей Microsoft	Обеспечивает компьютеру доступ к ресурсам сети Microsoft
Служба доступа к файлам и принтерам сетей Microsoft	Позволяет предоставлять папки и принтеры компьютера в совместный доступ в сетях Microsoft
Протокол Интернета (TCP/IP)	Обеспечивает связь компьютеров в локальных и глобальных сетях

Настройка основных параметров TCP/IP

Стек протоколов TCP/IP, входящий в состав Windows, поддерживает два режима настройки: с использованием статического или динамического IP-адреса. Каждый из этих режимов имеет свои преимущества и недостатки и должен использоваться в зависимости от конфигурации вашей локальной сети:

Преимущества:

Статический IP-адрес	**Динамический IP-адрес**
Не требуются дополнительные серверы и дополнительная подготовка администратора сети. Соответствие имени компьютера и IP-адреса практически	Все параметры настройки TCP/IP определяются один раз на сервере и автоматически используются рабочими станциями. Нет необходимости вести учет

никогда не изменяется.	используемых IP-адресов. Изменение одного или нескольких глобальных параметров IP-сети требует изменения параметров настройки только на сервере. Общее количество компьютеров может превышать количество выделенных IP-адресов, так как адрес выделяется на время работы компьютера в сети. Удобство настройки TCP/IP на компьютерах временных пользователей.

Недостатки:

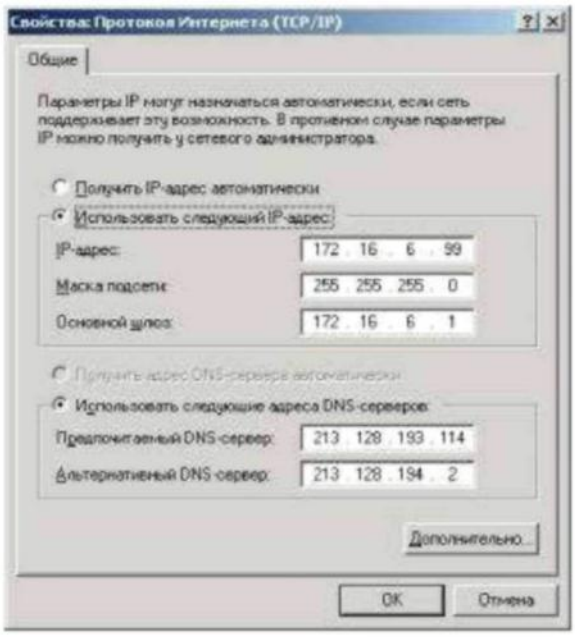
Статический IP-адрес	Динамический IP-адрес
Параметры необходимо изменять вручную на каждом компьютере в сети. Администратор должен вести учет используемых IP-адресов во избежание конфликтов. Изменение одного или нескольких глобальных параметров IP-сети (например адреса DNS-сервера) требует перенастройки TCP/IP на каждом компьютере.	Необходимо наличие сервера, осуществляющего выделение IP-адресов и передачу параметров настройки протокола TCP/IP. DHCP-сервер, входящий в состав Windows Server, обеспечивающий механизм динамического распределения адресов, требует наличия Active Directory и своей авторизации в домене, что существенно усложняет администрирование сети. Постоянное закрепление за компьютером одного и того же адреса не гарантируется. Существуют определенные трудности при использовании DHCP в сложных маршрутизируемых сетях. Работоспособность рабочих станций с динамическими IP-адресами может быть нарушена при выходе из строя или недоступности DHCP-сервера.

В общем случае статическая адресация удобна в небольших (10-20 компьютеров) одноранговых сетях, состав которых редко изменяется. Если количество компьютеров в сети

превышает 20, а компьютеры входят в домен Windows, гораздо проще и удобнее использовать динамическое выделение адресов.

Использование статического IP-адреса

По умолчанию Windows настраивает стек TCP/IP на использование динамически выделяемого IP-адреса. Чтобы использовать статический адрес, это необходимо указать в свойствах протокола TCP/IP. После этого вы должны задать следующие параметры.



IP-адрес - 32-разрядный адрес, представленный в формате W.X.Y.Z. Адрес должен быть уникальным не только в пределах локальной, но и в пределах всего Интернета. Обычно используется один из IP-адресов, выделенный провайдером.

Маска подсети - 32-разрядное число, представленное в формате W.X.Y.Z, которое используется для разделение крупных сетей на несколько более мелких.

Основной шлюз - IP-адрес маршрутизатора, используемого для выхода в глобальные сети и взаимодействия с другими сетями.

Предпочтительный и альтернативный *DNS-серверы* - IP-адреса основного и резервного DNS-серверов, которые будут использоваться стеком TCP/IP для разрешения символьных имен компьютеров в их IP-адреса.

Настроив параметры протокола, щелкните кнопку *ОК.* Для применения новых параметров TCP/IP щелкните кнопку *(Ж* в окне свойств соединения

Использование динамически выделяемого IP-адреса

Для использование динамически выделяемого IP-адреса необходимо в настройках протокола TCP/IP указать автоматическое получение IP-адреса. Также рекомендуется указать автоматическое получение адресов DNS-серверов, хотя можно указать эту информацию вручную.

Для динамического выделения IP-адреса в локальной сети должен быть установлен и настроен DHCP-сервер.

При недоступности DHCP-сервера используется служба APIPA (автоматическая настройка частных LP-адресов), которая генерирует IP-адрес вида 169.254.Y.Z и маску подсети 255.255.0.0. Если выбранный адрес уже используется, служба генерирует следующий адрес.

Отключение автоматической адресации

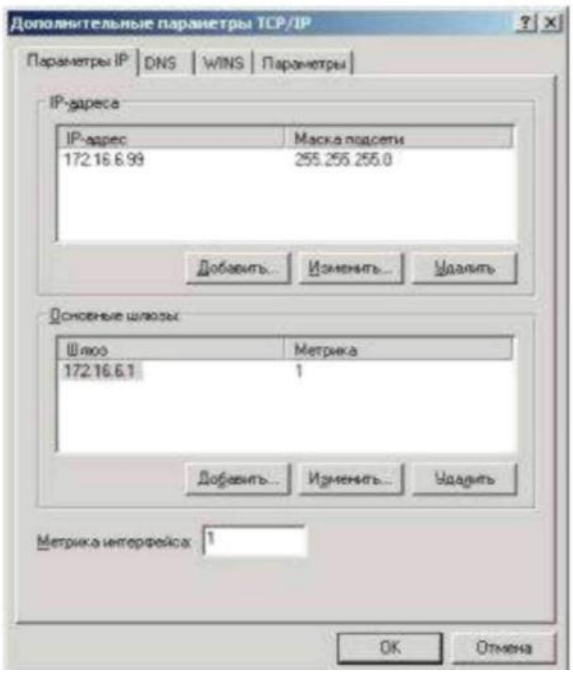
По умолчанию функция автоматической настройки частных IP-адресов включена, но можно ее отключить, добавив в системный реестр соответствующий параметр.

Дерево реестра	HKEY_LOCAL_MACHINE
Раздел реестра	SYSTEM\CurrentControlSet\Services\Tcpip \Parameters\Interfaces\{GUID_адаптера}
Имя параметра	IPAutoConfigurationEnabled
Тип параметра	REG_DWORD
Значение	0 - отключить автоматическую адресацию; 1 - включить автоматическую адресацию

Чтобы изменения вступили в силу, необходимо перезагрузить компьютер.

Настройка дополнительных параметров TCP/IP

Стек протоколов TCP/IP в Windows достаточно сложен и позволяет настраивать множество дополнительных параметров. Доступ к ним можно получить, щелкнув кнопку *Дополнительно* в окне свойств протокола **TCP/IP.**



На вкладке ***Параметры IP*** можно связать с сетевым адаптером несколько LP-адресов и

задать несколько основных шлюзов.

Стек TCP/IP Windows позволяет связать с любым сетевым адаптером несколько IP-адресов. Для каждого из адресов может быть задана своя маска подсети.

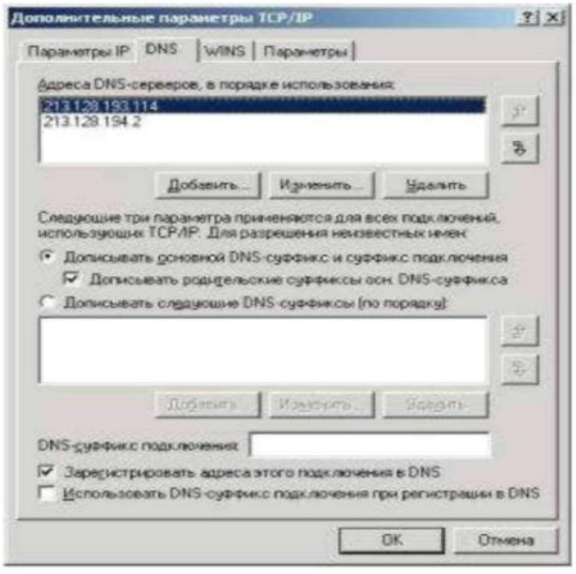
Несколько IP-адресов для одного сетевого адаптера принято использовать в следующих случаях:

- на web и ftp-серверах, обслуживающих большое количество сайтов, каждому из которых должен быть выделен отдельный ЕР-адрес;

- при подключении компьютера к локальной сети с несколькими наложенными IP-сетями; при постоянном перемещении компьютера из одной сети в другую.

Добавить адрес можно, щелкнув кнопку *Добавить.* Первый адрес из списка будет считаться основным и отображаться в окне основных свойств протокола TCP/IP. При использовании нескольких IP-адресов, особенно из разных сетей, необходимо указать несколько основных шлюзов, чтобы обеспечить возможность связи с компьютером извне по любому из связанных с ним адресов. Кроме того, для повышения надежности можно использовать несколько маршрутизаторов, соединяющих вашу сеть с другими. В этом случае имеет смысл указать в параметрах адреса нескольких основных шлюзов. Для каждого шлюза кроме его адреса задается метрика - целое число от 1 до 9999. Метрики служат для определения приоритета шлюзов. В любой момент времени используется первый доступный шлюз с минимальной метрикой. Таким образом, альтернативный шлюз с метрикой 2 будет использован только при недоступности основного с метрикой I..

Кроме того, можно задать метрику и самого интерфейса. Метрики интерфейсов служат для определения интерфейса, используемого для установления нового соединения. При использовании нескольких сетевых адаптеров метрики применяются для определения приоритета этих адаптеров.

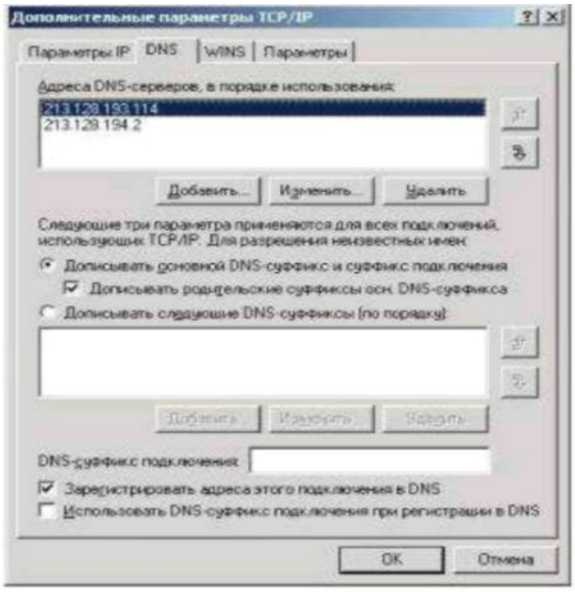


На вкладке *DNS* можно настроить все параметры, связанные со службой DNS. По аналогии с IP-адресами можно задать несколько (более двух) адресов DNS-серверов и определить порядок их использования. Метрики для определения порядка здесь не используются, т. к. при недоступности первого сервера будет использован второй, при недоступности второго - третий и т. д.

В работе DNS используются два параметра, отвечающие за разрешение неполных имен. Первый - основной суффикс DNS - задается на вкладке *Сетевая идентификация* свойств системы и обычно является полным DNS-именем домена, в который входит компьютер. При работе в рабочей группе этот суффикс может быть произвольным и задается при настройке Windows. Второй - DNS-суффикс подключения - задается на вкладке DNS свойств каждого подключения.

Если в параметрах настройки DNS указано *Дописывать основной DNS-суффикс и суффикс подключения,* то при разрешении неполных имен будет использованы соответствующие суффиксы. Например, при использовании основного суффикса msk.net.fio.ru и суффикса подключения lab.msk.net.fio.ru при вводе команды **ping xyz** будет предпринята попытка разрешения имен xyz.msk.net.fio.ru и xyz.lab.msk.net.fio.ru Кроме того, если включен параметр *Дописывать родительские суффиксы,* то при разрешении будут проверены еще и имена xyz.net.fio.ru, xyz.fio.ru и xyz.ru.

Если в параметрах настройки DNS указано *Дописывать следующие DNS-суффиксы,* то основной суффикс и суффикс подключения использованы не будут, а будет использован (последовательно) указанный список суффиксов. При разрешении неполных имен этот список будет использован аналогично приведенному примеру. Параметр *Зарегистрировать адреса* ***этого*** *подключения в DNS* использует основной DNS-суффикс для определения DNS-сервера, обеспечивающего функционирование соответствующей зоны, и автоматически регистрирует на нем запись A со своим именем и IP-адресом соединения. Если для соединения задано несколько IP-адресов или используется несколько соединений, то в DNS будут зарегистрированы несколько записей A с одним и тем же именем, но разными IP-адресами ■*■. Параметр *Использовать DNS-суффикс подключения при регистрации в DNS* позволяет осуществить регистрацию соответствующей записи A на DNS-сервере по аналогии с предыдущим параметром.

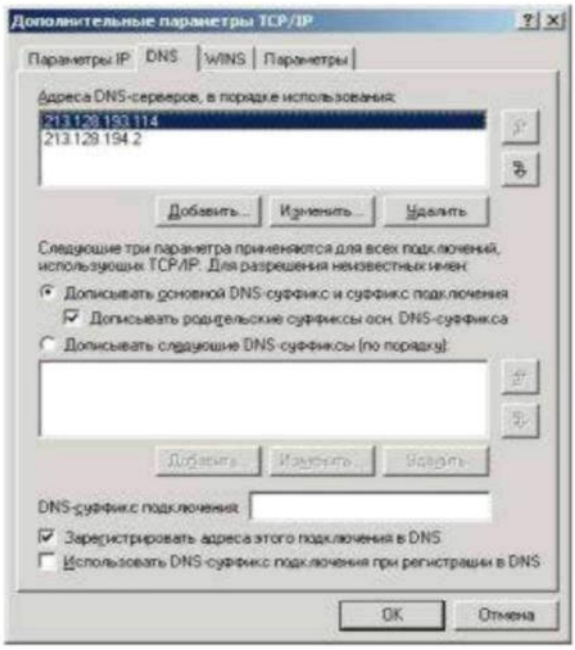


служба предназначена для разрешения имен NetBIOS в IP-адреса. При использовании домена и клиентов Windows использование этой службы не требуется - все ее функции выполняются службой DNS.

Для работы этой службы требуется WINS-сервер, адрес (адреса) которого добавляется в соответствующий список.

Помимо использования WINS-сервера Windows поддерживает устаревший способ разрешения имен NetBIOS- файл LMHOSTS. Можно включить использование этого файла и при необходимости импортировать уже существующий файл. Файл LMHOSTS можно редактировать самостоятельно в любом текстовом редакторе. Этот файл расположен в папке **%systemroot%\ system32\drivers\etc**

Кроме того, на этой вкладке осуществляется управление поддержкой NetBIOS поверх TCP/IP. Такая поддержка требуется для обеспечения совместной работы со старыми NetBIOS-клиентами (Windows 9x, NT). При использовании в локальной сети только Windows, NetBIOS поверх TCP/IP может быть отключен. При использовании динамически выделяемого IP-адреса можно задавать этот параметр через DHCP.



На вкладке ***Параметры*** можно настроить ряд необязательных параметров стека TCP/IP. Windows поддерживает настройку IP-безопасности (протокол IPSec) и фильтрации TCP/IP. Для настройки необходимо выбрать параметр из списка и щелкнуть кнопку *Свойства.*

Порядок выполнения работы

44. Изучить состав и назначение протоколов стека TCP/IP.
45. В системе Windows выполнить настройку стека протоколов TCP/IP для организации работы в сети Интернет. Для этого получить необходимые данные у преподавателя.
46. Создать группу в сети. Добавить в эту группу несколько компьютеров.
47. Поэкспериментировать с настройками Firewall, (пропускание/блокирование ping, HTTP и др.)

Контрольные вопросы.

1. Сколько протоколов образуют стек TCP/IP?
2. Какие уровни протоколов содержит стек TCP/IP?
3. что такое IP - адресация?
4. На каком уровне применяется IP - адресация?
5. Является ли IP - адресация абсолютной или относительной?
6. Поясните понятия статический и динамический IP - адрес.
7. Что такое шлюз?
8. Что такое маршрутизатор?
9. Для чего применяется маска подсети
10. Какие службы, устройства, клиенты необходимы для работы в сетях
11. Какие три основных вида угроз безопасности при работе в сети Internet?

12. Рассказать о каждой угрозе при работе в сети Internet.
13. Виды программ-паразитов (и в чем их различие)
14. Адресация в сети Internet.
15. Основные сетевые протоколы (TCP, IP, UDP, POP, SMTP, DNS, WINS, 1CMP, HTTP, FTP,). Рассказать о любом по выбору преподавателя.

Какие средства сетевой защиты существуют?

Лабораторная работа № 11 «Решение проблем с TCP/IP»

Цель: обобщение и систематизация знаний по теме «Организация межсетевого взаимодействия»

Задания к работе

1. Открыть окно командной строки, ввести команду ping с IP адресом машины, при взаимодействии с которой возникают проблемы. Определить, использует ли проблемная машина конфигурацию статичного или динамичного IP адреса. Для этого откройте панель управления и выберите опцию Сетевые подключения. Теперь правой клавишей нажмите на подключении, которое собираетесь диагностировать, затем выберите опцию Свойства в появившемся меню быстрого доступа.

2. Перейдите по спискам элементов, используемых подключением, пока не дойдете до TCP/IP протокола. Выберите этот протокол, нажмите на кнопке Свойства, чтобы открыть страницу свойств для Internet Protocol (TCP/IP).

3. Запишите IP конфигурацию машины. Особенно важно сделать заметки следующих элементов:

1. Использует ли машина статичную или динамичную конфигурацию?

2. Если используется статичная конфигурация, запишите значение IP адреса, маски подсети и основного шлюза?

3. Получает ли машина адрес DNS сервера автоматически?

4. Если адрес DNS сервера вводится вручную, то какой адрес используется?

4. Если на компьютере установлено несколько сетевых адаптеров, то в панели управления будут перечислены несколько сетевых подключений.

5. Проверьте тип адаптера.

6. Определите, принимает ли Windows такую конфигурацию. Для этого откройте окно командной строки и введите следующую команду: IPCONFIG /ALL.

7. Определите правильный сетевой адаптер. В этом случае определение нужного адаптера довольно простое, поскольку в списке есть всего лишь один адаптер.

8. Отправьте ping запрос на адрес локального узла. Существует два различных способа того, как это сделать. Одним способом является ввод команды: *PING LOCALHOST.*

9. Введите команду Nslookup, за которой должно идти полное доменное имя удаленного узла. Команда Nslookup должна суметь разрешить полное доменное имя в IP адрес.

11. Необходимо просканировать клиентскую машину на предмет вредоносного ПО. Если на машине не обнаружено вредоносного ПО, сбросьте DNS кэш путем ввода следующей команды: *IPCONFIG /FLUSHDNS.*

Контрольные вопросы

1. Поясните, что может означать, если время TTL закончилось до получения ответа.
2. Как подтвердить наличие сетевого соединения?
3. Что показывает команда IPCONFIG /ALL?
4. Что означает наличие IP адрес со значением 0.0.0.0.?
5. С помощью какой команды можно проверить то, что конфигурация IP адреса работает корректно, и что отсутствуют проблемы с стеком локального протокола TCP/IP?
6. Как производится опрос основного шлюза?
7. Как производится опрос DNS сервера?

Лабораторная работа №12. ПРОТОКОЛЫ ARP И ICMP

Цель работы: рассмотреть режим симуляции **Cisco Packet Tracer**, изучить протоколы **ARP** и **ICMP,** используя утилиты **ping** и **tracert**.

Содержание:

1. Построение топологии сети, настройка конечных узлов.
2. Настройка маршрутизатора.
3. Проверка работы сети в режиме симуляции.
4. Создание ping-запроса внутри сети.
5. Создание ping-запроса во внешнюю сеть.
6. Создание ping-запроса на несуществующий IP-адрес узла.
7. Выполнение индивидуального задания.

1. Теоретические сведения

Протокол ARP

Для определения физического адреса по IP-адресу используется протокол разрешения адреса **Address Resolution Protocol** (**ARP**). Протокол ARP предоставляет возможность широковещательного доступа одновременно ко всем узлам сети и позволяет динамически определить **MAC-адрес** по **IP-адресу**.

В лабораторной работе локальная сеть строится по технологии **Ethernet**. В сетях Ethernet, использующих стек **TCP/IP**, сетевой интерфейс имеет физический адрес длиной в **48 бит**. Кадры, которыми обмениваются конечные узлы на канальном уровне, должны содержать аппаратный адрес сетевого интерфейса. А **TCP/IP** использует **32-битные** IP-адреса. Знание IP-адреса приемника недостаточно, чтобы отправить дейтаграмму этому хосту.

Драйвер Ethernet должен знать **MAC-адрес** интерфейса назначения. В задачу **ARP** входит обеспечение динамического соответствия между 32-битными IP-адресами и 48битными MAC-адресами, используемыми различными сетевыми технологиями. Протокол ARP работает в пределах одной подсети и автоматически запускается, когда возникает необходимость преобразования IP-адреса в аппаратный адрес.

Работу протокола ARP иллюстрирует **рис. 2.1**.

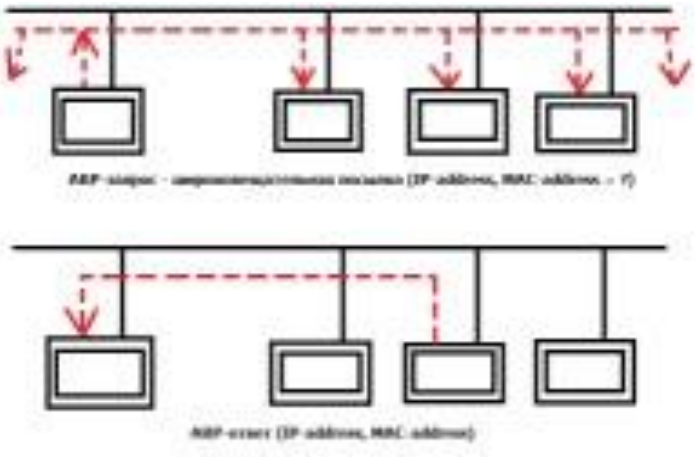


Рис. 2.1. ARP-запрос и ARP-ответ

Узел, которому нужно узнать **MAC-адрес** интерфейса назначения, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем **IP-адрес узла назначения** и свой **MAC-адрес**, и рассылает широковещательный запрос. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес со своим. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой **IP-адрес** и свой **MAC-адрес,** и отправляет его уже направленно, так как в ARP-запросе отправитель указал свой локальный адрес.

Для того, чтобы уменьшить количество посылаемых ARPзапросов, каждое устройство в сети должно иметь специальную буферную память. В ней хранятся пары адресов узлов сети –

IPадрес, **MAC-адрес**. Всякий раз, когда устройство получает ARPответ, оно сохраняет в буферной памяти соответствующую пару. Если адрес есть в списке пар, то нет необходимости посылать ARP-запрос. Эта буферная память называется **ARP-таблицей**.
В ARP-таблице могут содержаться как статические, так и динамические записи. Динамические записи добавляются и удаляются автоматически, статические заносятся вручную. Большинство устройств в сети поддерживает динамическое разрешение адресов, поэтому администратору нет необходимости вручную указывать записи протокола ARP в таблице адресов.
Каждая запись в ARP-таблице имеет время жизни. Периоды очистки ARP-таблицы зависят от используемой ОС. При добавлении для каждой записи активируется таймер.
Сообщения протокола ARP при передаче по сети встраиваются в поле данных кадра. Они не содержат IP заголовка.
В отличие от сообщений большинства протоколов, сообщения ARP не имеют фиксированного формата заголовка. Это объясняется тем, что протокол был разработан для использования в различных сетях. Запросы и ответы используют один и тот же формат пакета. Так как локальные адреса в различных типах сетей могут иметь различную длину, то формат пакета протокола ARP зависит от типа сети.

Протокол ICMP

Протокол **Internet Control Message Protocol** (ICMP) предназначен для передачи управляющих и диагностических сообщений – сообщений об ошибках, а также о возникновении ситуаций, требующих повышенного внимания. Протокол относится к **сетевому уровню** модели **TCP/IP**. Сообщения ICMP генерируются и обрабатываются протоколами сетевого (IP) и более высоких уровней (TCP или UDP). При появлении некоторых ICMP-сообщений генерируются сообщения об ошибках, которые передаются пользовательским процессам. ICMP-сообщения передаются внутри IP-дейтаграмм (**рис. 2.2**).

Рис. 2.2. Инкапсуляция ICMP-сообщений в IPдейтаграммы

Заголовок ICMP включает 8 байт, но только первые 4 байта одинаковы для всех сообщений, остальные поля заголовка и тела сообщения определяются типом сообщения. Тип сообщения определяется значением поля **Тип** заголовка.

Программа ping

Программа **ping** была разработана для проверки доступности удаленного узла. Программа посылает **ICMP-эхозапрос** на узел и ожидает возврата **ICMP-эхо-отклика**. Программа **ping** обычно является первым диагностическим средством, с помощью которого начинается идентификация какой-либо проблемы в сетях. С помощью **ping** можно также оценить время возврата пакета от узла. Это позволяет оценить как далеко находится узел. Программа **ping** имеет опции записи маршрута и временной метки. Сообщения **эхо-запроса** и **эхоотклика** имеют один и тот же формат (**рис 2.3**).

Тип	**Код**	**Контрольная сумма**
Идентификатор		**Последовательный номер**
Необязательные данные		

Рис. 2.3. Формат пакета ICMP-сообщения

Тип – тип пакета: эхо-запрос/ эхо-отклик;
Код – расшифровка назначения пакета внутри типа;
Контрольная сумма вычисляется для всего пакета;
Идентификатор – номер потока сообщений;
Последовательный номер – номер пакета в потоке.

В **эхо-отклике** должны содержаться поля идентификатора и номера последовательности, а любые дополнительные данные, посланные компьютером, должны быть отражены в **эхо-отклике**.
В поле идентификатора ICMP сообщения устанавливается идентификатор процесса, отправляющего запрос. Это позволяет программе **ping** идентифицировать вернувшийся ответ, если на одном и том же хосте одновременно запущено несколько программ **ping**.
Номер последовательности **начинается с 0** и увеличивается на единицу с каждым следующим эхо-запросом.
Вывод программы показан на **рис. 2.4**. Первая строка вывода содержит IP-адрес хоста назначения, даже если было указано имя. Поэтому программу ping часто используют для определения **IP-адреса удаленного узла**.
Рис. 2.4. Вывод программы ping

```
C:\>ping yandex.ru

Обмен пакетами с yandex.ru [93.158.134.11] с 32 байтами данных:
Ответ от 93.158.134.11: число байт=32 время=48мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=27мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=29мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=29мс TTL=51

Статистика Ping для 93.158.134.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 27мсек, Максимальное = 48 мсек, Среднее = 33 мсек
```

Программа tracert

Программа **tracert** позволяет просмотреть маршрут, по которому двигаются IP-дейтаграммы от хоста к хосту.
Программа tracert не требует никаких специальных серверных приложений. В ее работе используются стандартные функции протоколов **ICMP** и **IP**. Для понимания работы программы следует вспомнить порядок обработки поля TTL в заголовке IP-дейтаграммы.
Каждый маршрутизатор, обрабатывающий дейтаграмму, уменьшает значение поля TTL в ее заголовке на единицу. При получении дейтаграммы с TTL, **равным 1**, маршрутизатор уничтожает ее и посылает хосту, который ее отправил, ICMP сообщение, что время истекло. При этом дейтаграмма, содержащая это ICMP-сообщение, имеет в качестве адреса источника IP-адрес маршрутизатора.
Это и используется в программе tracert. На хост назначения отправляется IP-дейтаграмма, в которой поле TTL установлено в 1. Первый маршрутизатор на пути дейтаграммы, уничтожает ее, так как TTL равно 1, и отправляет ICMP-сообщение об истечении времени. Таким образом, определяется первый маршрутизатор в маршруте.
Затем tracert отправляет дейтаграмму с полем TTL равным 2, что позволяет получить IP-адрес второго маршрутизатора. Аналогичные действия продолжаются до тех пор, пока дейтаграмма не достигнет хоста назначения. При получении ответа от этого узла процесс трассировки считается завершённым.
Пример вывода программы показан на рис. 2.5.

```
PC>tracert 192.168.5.4
Tracing route to 192.168.5.4 over a maximum of 30 hops:
1     4 ms     4 ms     4 ms     192.168.3.1
2     *        8 ms     8 ms     192.168.5.4
```

Рис. 2.5. Вывод программы tracert

Первая строка, без номера содержит имя и IP адрес пункта назначения и указывает на то, что величина TTL не может быть больше 30.
Следующие строки вывода начинаются с распечатки значения TTL (1, 2, 3 и т.д.) и содержат имя (IP-адрес) хоста или маршрутизатора и время возврата ICMP-сообщения.
Для каждого значения TTL отправляется 3 дейтаграммы. Для каждого возвращенного ICMP-сообщения рассчитывается и печатается время возврата.
Если ответ на дейтаграмму не получен в течение пяти секунд, печатается звездочка, после чего отправляется следующая дейтаграмма.

2. Практическая часть работы

Создать топологию сети, состоящую из
1сеть 5 ПК соединенных коммутатором
2 сеть 2 ПК и 1 ноутбук соединенных коммутатором
1 и 2 сети подключены к маршрутизатору
Пример на **рис. 2.6**:

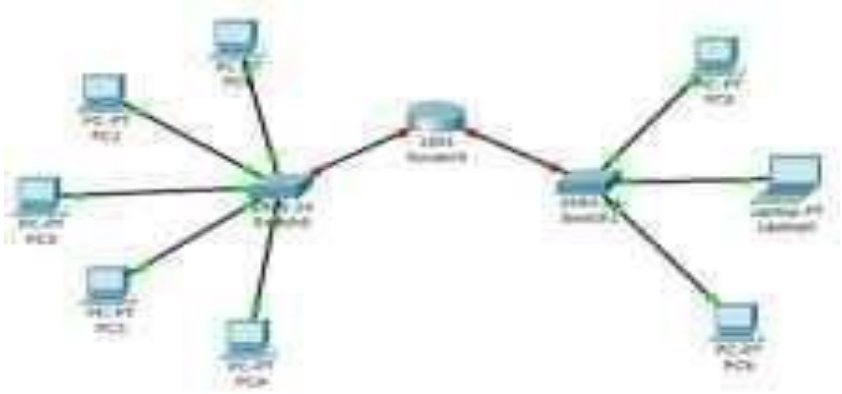


Рис. 2.6. Тестовая топология сети
Маршрутизатор **Router0** имеет два интерфейса и соединяет две подсети.
Настройка конечных узлов
На устройствах **PC0-PC4** установим заданные IP-адреса и маску подсети в соответствии с таблицей **2.1**. IP-адрес шлюза для всех узлов – **192.168.3.1**. IP-адрес DNS-сервера указывать необязательно, так как в этой работе он использоваться не будет.
Таблица 2.1

Хост	IP-адрес	Маска подсети
PC0	**192.168.3.3**	**255.255.255.0**
PC1	**192.168.3.4**	**255.255.255.0**
PC2	**192.168.3.5**	**255.255.255.0**
PC3	**192.168.3.6**	**255.255.255.0**
PC4	**192.168.3.7**	**255.255.255.0**

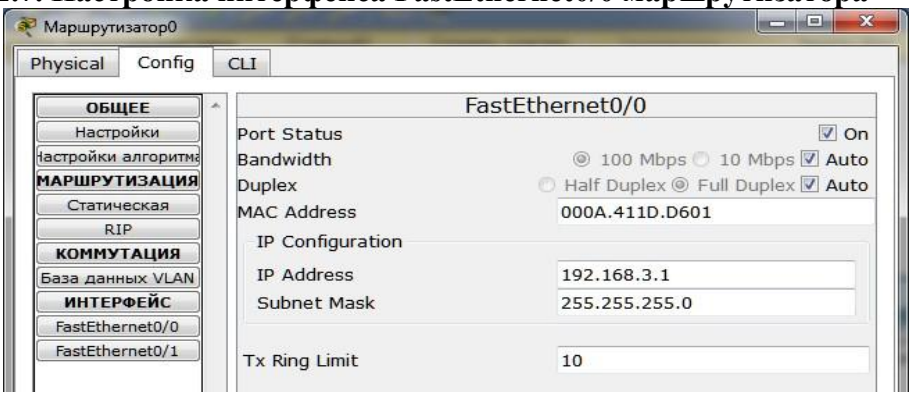
На устройствах **PC5**, **Laptop0**, **PC6** установим заданные IPадреса и маску подсети в соответствии с таблицей **2.2**. IP-адрес шлюза для всех узлов – **192.168.5.1**. IP-адрес DNS-сервера указывать необязательно.
Таблица 2.2

Хост	IP-адрес	Маска подсети
PC5	**192.168.5.3**	**255.255.255.0**
Laptop0	**192.168.5.4**	**255.255.255.0**
PC6	**192.168.5.5**	**255.255.255.0**

Каждый узел переименуем его же IP-адресом.
Настройка маршрутизатора

Как уже упоминалось, маршрутизатор в данной топологии имеет два интерфейса. Произведем настройку интерфейса маршрутизатора **FastEthernet0/0**:
Щелкаем мышью по маршрутизатору.
Выбираем вкладку **Config**.
Находим интерфейс **FastEthernet0/0**, задаем IP-адрес интерфейса, равный IP-адресу шлюза подключенной сети, и маску подсети (**рис. 2.7**).
Интерфейс маршрутизатора по умолчанию отключен. Его следует включить, установив флажок на опции Port Status рядом с On**.**

Рис. 2.7. Настройка интерфейса FastEthernet0/0 маршрутизатора



Закрываем окно маршрутизатора и смотрим на топологию сети. Зеленые индикаторы состояния на линии связи между **Router0** и **Switch0** сигнализируют, что интерфейс подключен правильно.

Аналогично производим настройку интерфейса **FastEthernet0/1** (**рис. 2.8**).

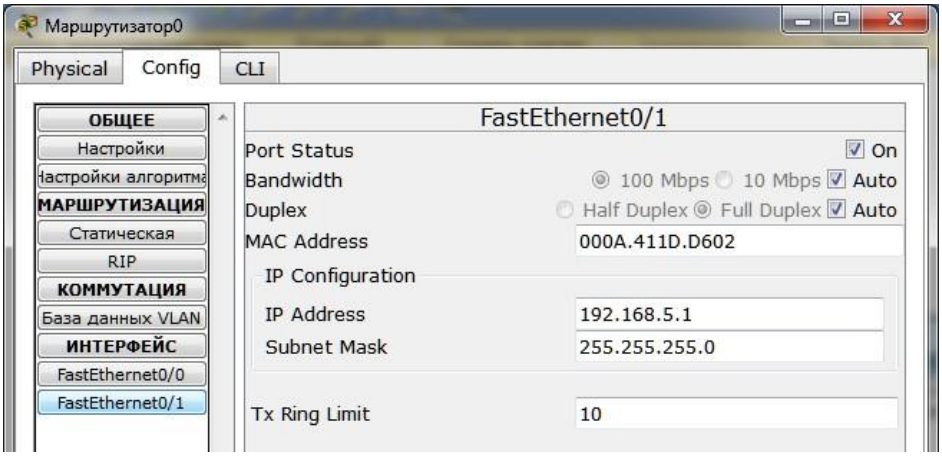


Рис. 2.8. Настройка интерфейса FastEthernet0/1 маршрутизатора

Сделать надписи к интерфейсам маршрутизатора, можно с помощью инструмента **Place Note** на панели **Common Tools**

.

Для этого нужно сначала щелкнуть на инструменте, а затем – в нужном месте на рабочей области. Получим следующий вид рабочей области (**рис. 2.9**).

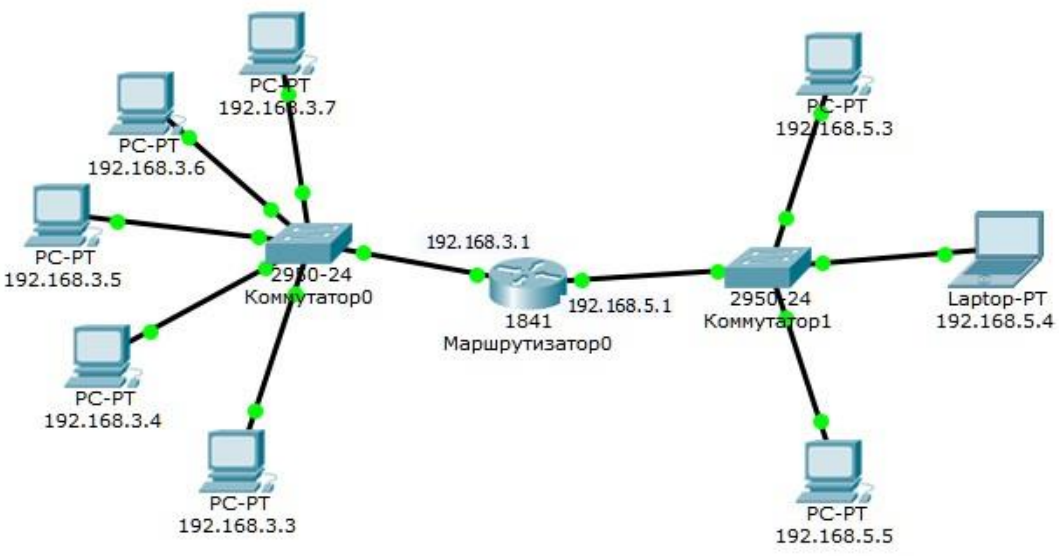


Рис. 2.9. Вид рабочей области

Режим симуляции Cisco Packet Tracer

Для того, чтобы убедиться, что включен режим симуляции, следует щелкнуть по иконке симуляции в правом нижнем углу рабочей области. Откроется окно событий, в котором виден список событий, управляющие кнопки, заданные фильтры (**рис. 2.10**).

По умолчанию фильтруются, то есть отображаются, пакеты всех возможных протоколов, поэтому необходимо изменить и ограничить этот список до исследуемых протоколов.

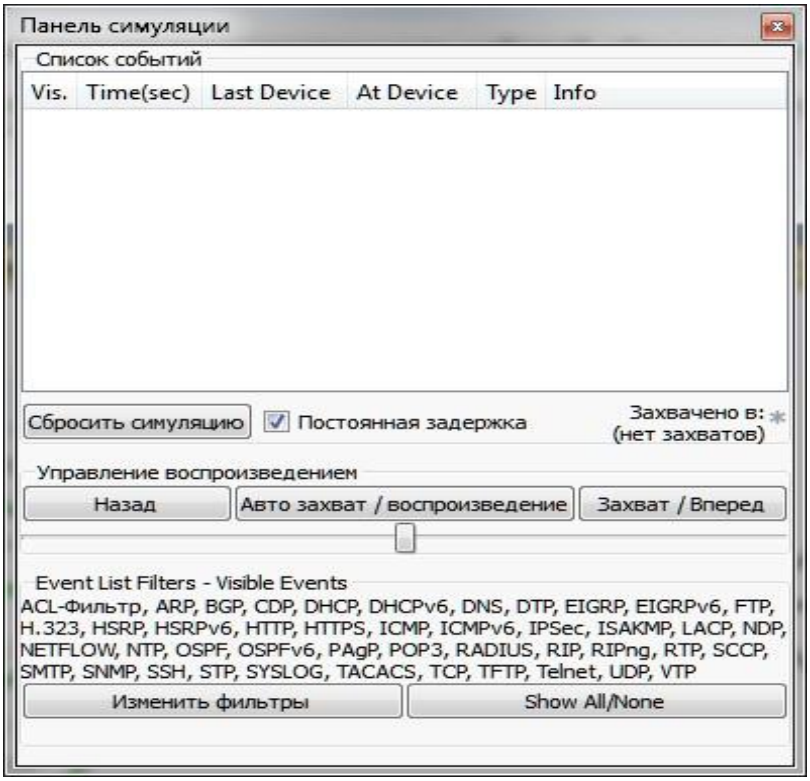


Рис. 2.10. Окно событий режима симуляции

Управляющие кнопки:

Back – **Назад**;

Auto Capture/Play – **Автозахват/воспроизведение**, автоматический захват пакетов от источника до приемника и обратно;

Capture/Forward – **Захват/Вперед**, захват пакетов только от одного устройства до другого.
В этой лабораторной работе будут использованы пакеты двух типов **ARP** и **ICMP,** поэтому нужно поставить фильтры только на сообщения заданного типа (**рис. 2.11**):
Щелкаем по кнопке **Edit Filters** – **Изменить фильтры**.
Удаляем флажки со всех фильтров, кроме **ARP** и **ICMP**.
Убеждаемся, что заданные протоколы для фильтрации назначены.

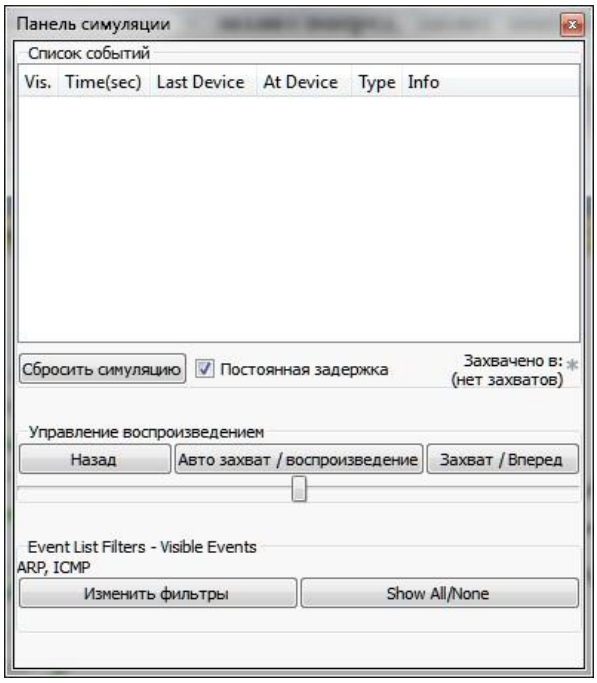


Рис. 2.11. Добавление фильтров на протоколы ARP и ICMP Проверка работы сети в режиме симуляции

Отправим тестовый **ping-запрос** с конечного узла с IPадресом **192.168.3.3** на хост с IP-адресом **192.168.3.5**.

Обратите внимание, что оба узла находятся в пределах одного сегмента сети.

Щелкаем по выбранному устройству.
Выбираем вкладку **Desktop**, в которой содержатся симуляторы некоторых программ, доступных на компьютере.
Выбираем **Command Prompt** – программу, имитирующую командную строку компьютера.
Вводим **ping-запрос PC>ping 192.168.3.5** и нажимаем **Enter**.
На устройстве-источнике формируются два пакета протоколов **ARP** и **ICMP** (**рис. 2.12**). **ARP-запрос** необходим всегда, когда хост пытается связаться с другим хостом.

Нажимаем на кнопку **Auto Capture/play** или **Capture/Forward.**

Последняя команда позволяет самим управлять движением пакетов от устройства к устройству. Видим, что первым отправляется пакет протокола **ARP**, так как ARPтаблица хоста **192.168.3.3** пуста, и он еще **не знает**, кому отправлять ping-запрос. Щелкните по самому пакету – конверту и ознакомьтесь на вкладке OSI Model, какие уровни модели OSI задействованы (**рис. 2.13**). Перейдите на вкладку **Inbound PDU Details** и ознакомьтесь со структурой пакета.

Рис. 2.12. Вид рабочей области

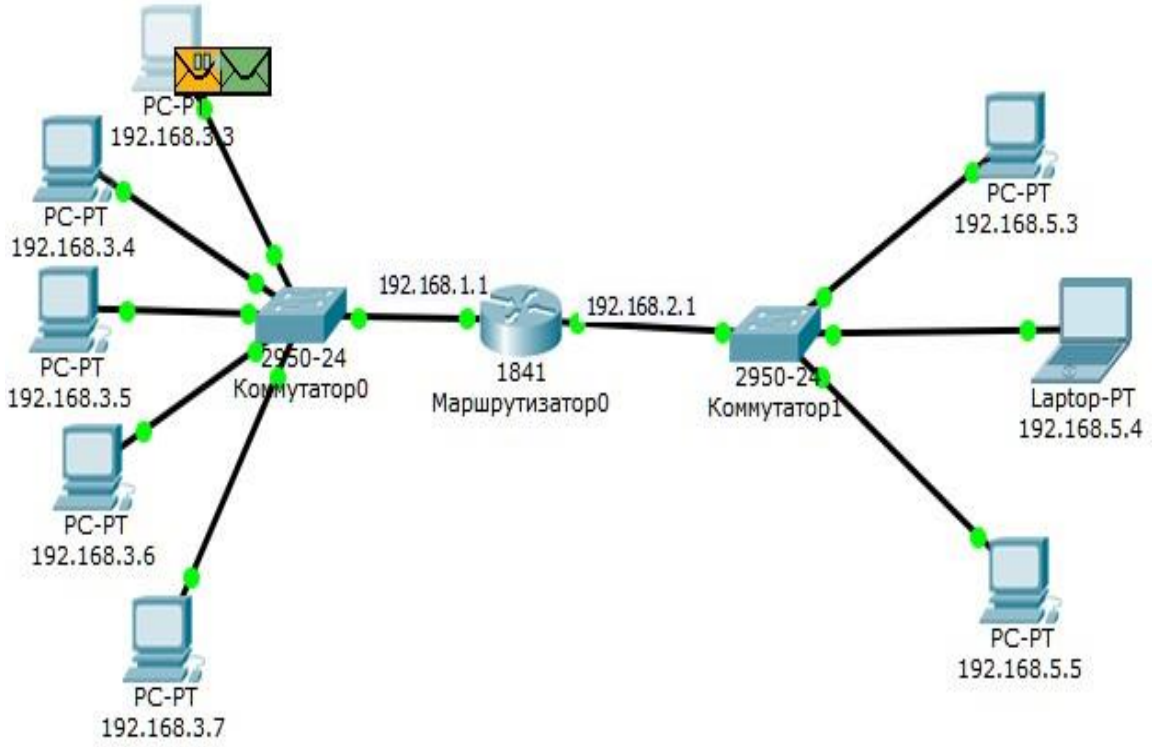


Рис. 2.13. Формат пакета ARP-запроса

Узел **192.168.3.3** построил запрос и посылает его широковещательным сообщением всем хостам подсети. Помимо IP-адреса назначения, запрос содержит IP-адрес и MAC-адрес отправителя, чтобы приемная сторона могла ответить.

При просмотре прохождения пакетов убедитесь, что на ARP-запрос ответит только хост **192.168.3.5**. Каждый хост в подсети получает запрос и проверяет на соответствие свой IPадрес. Если он не совпадает с указанным адресом в запросе, то запрос игнорируется.

Посмотрите и зафиксируйте содержимое пакета **ARPответа**, пришедшего на хост **192.168.3.3** (**рис. 2.14**). Узел **192.168.3.5** послал **ARP-ответ** непосредственно отправителю, используя его MAC-адрес, с указанием собственного MAC-адреса в поле **Target MAC**.

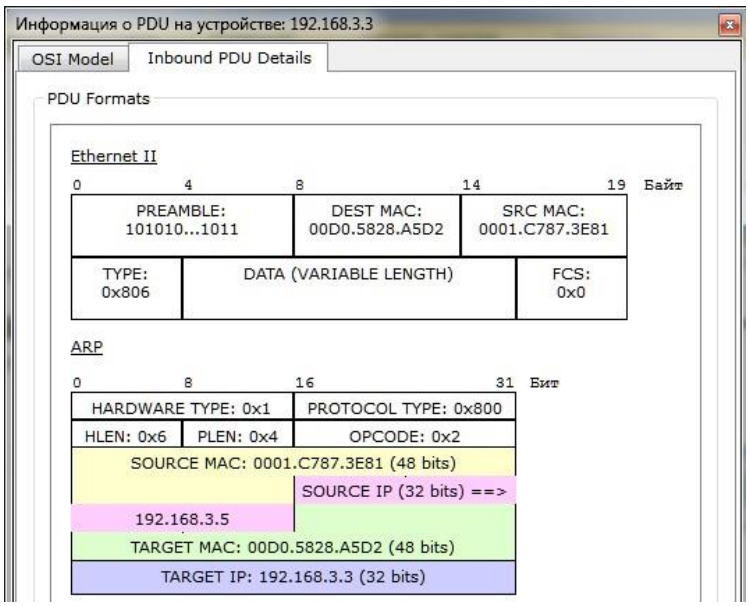


Рис. 2.14. Формат пакета ARP-ответа

Далее отправляется **ICMP-сообщение** ping-запроса. Посмотрите и зафиксируйте содержимое пакета, сделав щелчок мышью по пакету-конверту.

Физические адреса узлов известны. **IP-адрес источника – 192.168.3.3**. **IP-адрес назначения – 192.168.3.5**. Тип ICMPсообщения-**8** – **эхо-запрос** (**рис. 2.15**).

Запрос производится на хост **192.168.3.5** через коммутатор.

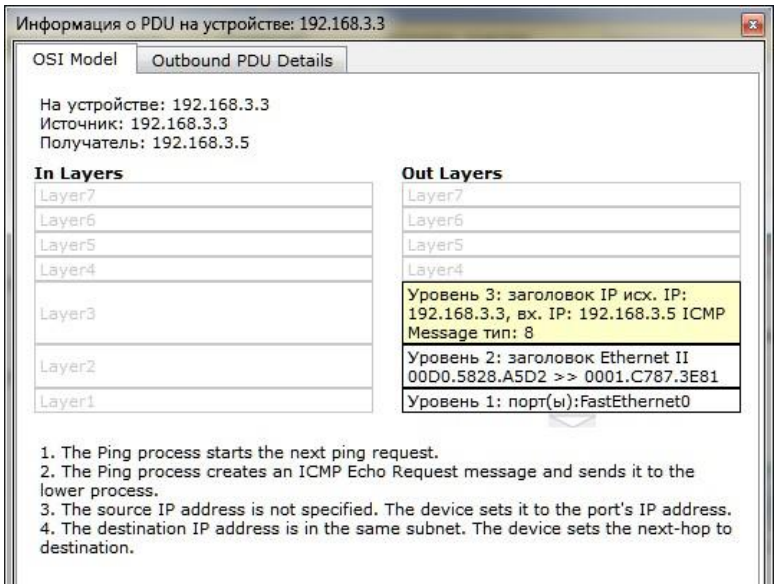


Рис. 2.15. Формат пакета ICMP – эхо-запроса

Посмотрите и зафиксируйте содержимое пакета pingответа, пришедшего на хост **192.168.3.3** (**рис. 2.16**).

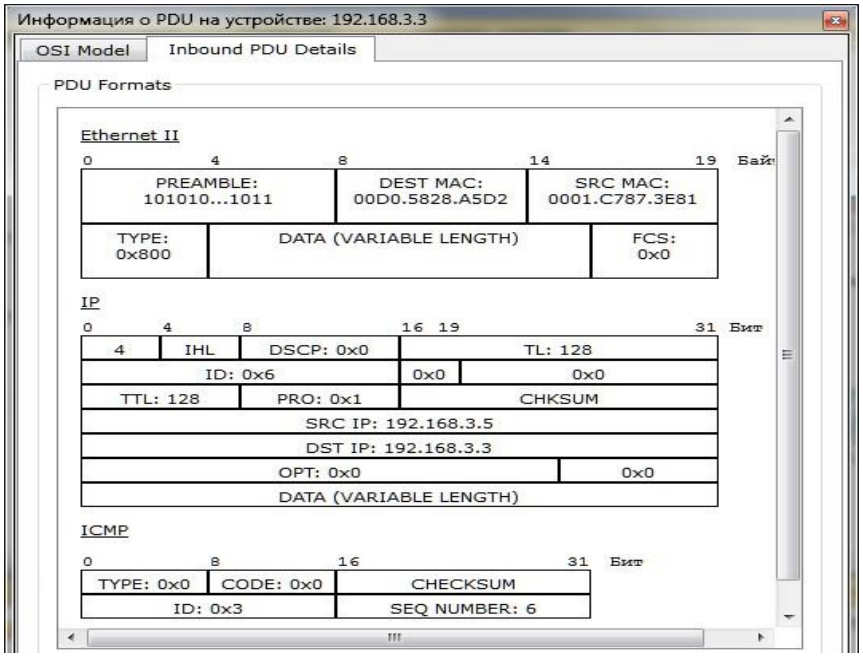


Рис. 2.16. Формат пакета ICMP – эхо-ответа

IP-адрес источника – **192.168.3.5**. IP-адрес назначения – **192.168.3.3**. Тип ICMP-сообщения - **0** – **эхо-ответ**.

Посмотрите **ping-ответ** в командной строке хоста **192.168.3.3** (**рис. 2.17**).

PC>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Reply from 192.168.3.5: bytes=32 time=8ms TTL=128

Reply from 192.168.3.5: bytes=32 time=4ms TTL=128

Reply from 192.168.3.5: bytes=32 time=4ms TTL=128

Reply from 192.168.3.5: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.5:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 4ms, Maximum = 8ms, Average = 5ms

Рис. 2.17. Вывод программы ping

В окне событий указаны маршруты запросов **ARP** и **ICMP,** то есть, через какие устройства прошли пакеты (**рис. 2.18**).

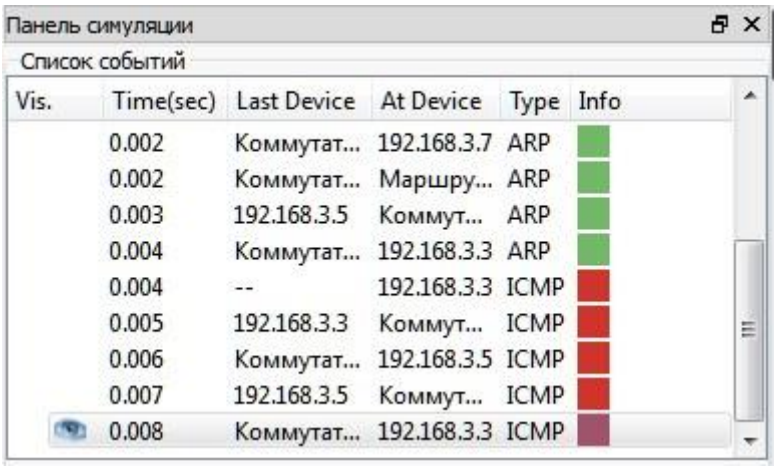


Рис. 2.18. Окно событий режима симуляции

Удалить сценарий симуляции можно с помощью кнопки **Reset Simulation** или кнопки **Delete** в области **User Created Packet Window**.
Теперь ARP-таблицы хостов **192.168.3.3** и **192.168.3.5** не пусты, в них содержится одна запись. Чтобы просмотреть содержимое ARP-таблицы, нужно в командной строке выполнить команду **arp -a** (**рис. 2.19**).

Содержимое ARP-таблицы узла **192.168.3.3**:
PC>arp -a
Internet Address Physical Address Type
192.168.3.5 0001.c787.3e81 dynamic
Рис. 2.19. ARP-таблица узла 192.168.3.3 в командной строке
Можно воспользоваться другим способом: щелкнуть кнопку

Inspect  , нажать на выбранное устройство, выбрать **ARP table** и просмотреть записи **ARP-таблицы** узла (**рис. 2.20**).

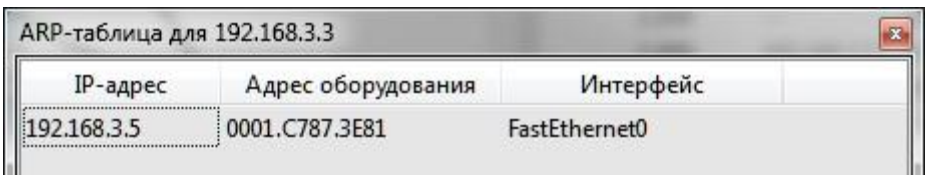


Рис. 2.20. ARP-таблица узла 192.168.3.3, показанная с помощью инструмента Inspect
Если снова задать ping-запрос на хост **192.168.3.5**, то будет сформирован только один пакет ICMP-сообщения, так как в ARP-таблице компьютера-источника уже хранится соответствующий локальный адрес.
Отправьте ping-запрос снова.
Чтобы удалить все записи ARP-таблицы следует воспользоваться командой **arp -d**.
Проверьте выполнение этой команды.
Формирование ping-запроса во внешнюю сеть
Отправим тестовый ping-запрос с конечного узла с IPадресом **192.168.3.4** на хост с IP-адресом **192.168.5.5** (***узлы находятся в разных сетях*****).**
Выше был рассмотрен случай посылки ARP-запроса внутри локальной сети. Протокол ARP в этом случае определял непосредственно **MAC-адрес** узла-приемника запроса. Теперь рассмотрим ситуацию, когда узел-источник и узел-приемник находятся в разных сетях. Протокол ARP работает в пределах сегмента сети, поэтому в данном случае он будет использоваться для определения **MAC-адреса** маршрутизатора. Таким образом, пакет будет передан маршрутизатору для дальнейшей ретрансляции.

Открываем **Command Prompt**, имитирующую командную строку на компьютере **192.168.3.4,** и посылаем ping-запрос на хост **192.168.5.5**. Инициируется ARP-запрос маршрутизатору, который пересылает пакеты в сеть назначения. На узле-источнике формируются два пакета протокола ARP и ICMP. Формат пакета ARP-запроса содержит те же сведения, что и для разрешения локального адреса устройства, и рассылается широковещательно всем узлам подсети (**рис. 2.21**). Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался.

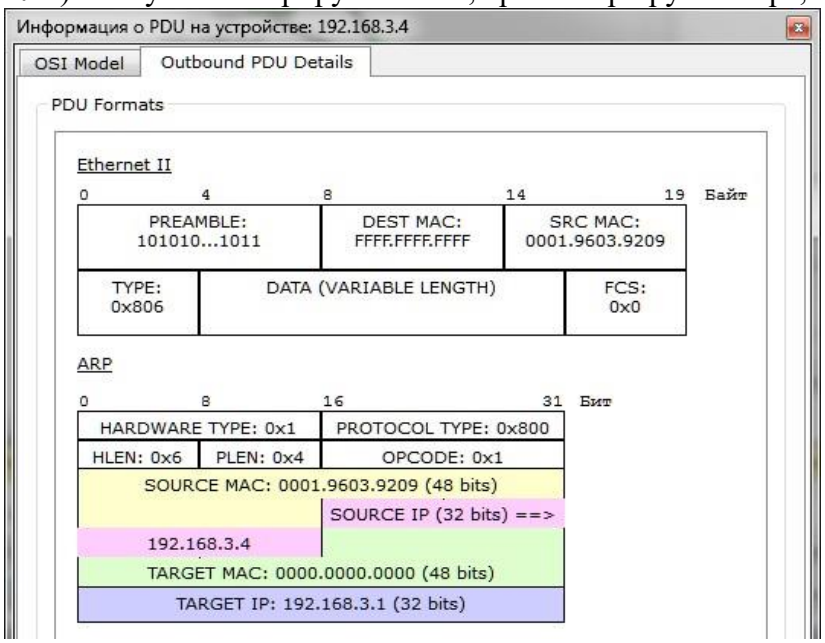


Рис. 2.21. Формат пакета ARP-запроса

Маршрутизатор формирует ARP-ответ, указывая свой физический адрес, и отправляет его узлу **192.168.3.4**.

После получения ARP-ответа хост **192.168.3.4** посылает ICMP-сообщение ping-запроса через маршрутизатор в сеть назначения.

Посмотрите содержимое пакета, щелкнув по пакету – конверту (**рис. 2.22**).

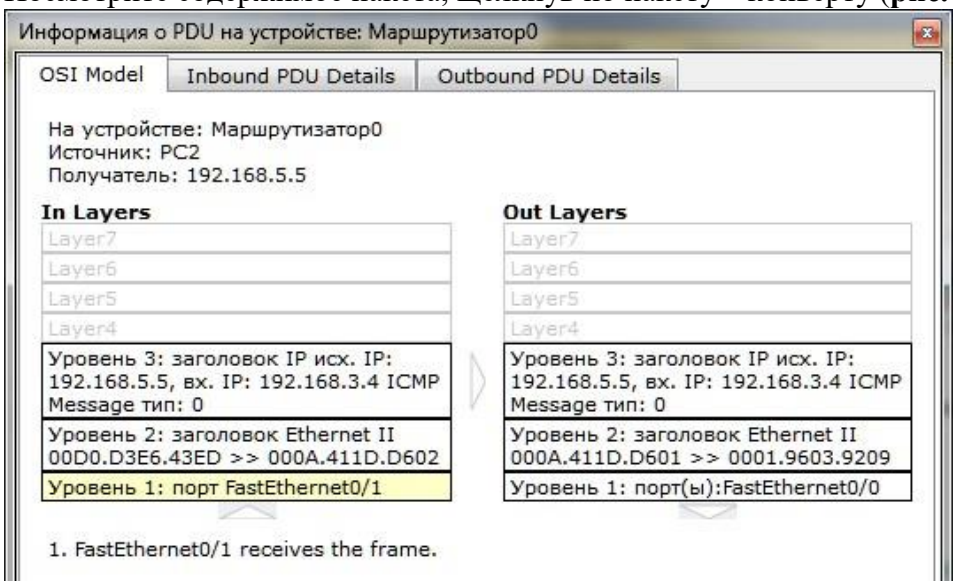


Рис. 2.22. Формат пакета ICMP-эхо-запроса

Когда запрос приходит в сеть назначения, то маршрутизатор определяет MAC-адрес получателя, если его нет в ARP-таблице маршрутизатора. Таким образом, снова решается задача разрешения локального адреса.

Маршрутизатор вынужден сначала узнать физический адрес получателя, прежде чем он сможет отправить ping-запрос по назначению, поэтому пакет с ping-запросом, пришедший на маршрутизатор, отклонен.
Новый ARP-запрос отправляется широковещательным сообщением от маршрутизатора. Он содержит его IP- и MACадреса. IP-адрес назначения – узел **192.168.5.5**.
Узлы подсети, которым пакет не предназначен, его игнорируют. Узел **192.168.5.5** формирует ARP-ответ и отправляет его обратно маршрутизатору, указав свой MAC-адрес, о чем свидетельствует содержимое пакета.
Узел **192.168.3.4** снова отправляет ping-запрос во внешнюю сеть узлу **192.168.5.5**. Его маршрут должен лежать через коммутатор Switch0, маршрутизатор Router0, коммутатор Switch1 и достигнуть узла назначения. **Проследите маршрут пакета**.
Узел формирует ping-ответ, который отправляется обратно узлу 192.168.3.4.
Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.4. IP-адрес источника – 192.168.5.5, IP-адрес назначения – 192.168.3.4. Тип ICMP-сообщения – 0 –эхо-ответ.
Посмотрите ping-ответ в командной строке хоста 192.168.3.4.
Маршрут пакета можно посмотреть с помощью команды tracert. Выполним эту команду, например, в командной строке компьютера 192.168.3.5 (**рис. 2.23**):

PC>tracert 192.168.5.4
Tracing route to 192.168.5.4 over a maximum of 30 hops:
1 4 ms 4 ms 4 ms 192.168.3.1 2 * 8 ms 8 ms 192.168.5.4
Trace complete.
Рис. 2.23. Вывод программы tracert
На пути пакета до хоста 192.168.5.4 один промежуточный маршрутизатор.
Посылка ping-запроса на несуществующий хост
Отправим ping-запрос на несуществующий адрес в сеть **192.168.5.0/24**. для этого откроем программу **Command Promt** на узле **192.168.3.7** и отправим ping-запрос на несуществующий хост с IP-адресом **192.168.5.6**.
ARP-таблица на узле-источнике не содержит соответствующей записи о MAC-адресе узла **192.168.5.6**, поэтому формируется ARP-запрос. Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался.
Узел **192.168.3.7** получает ARP-ответ с MAC-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос на несуществующий узел **192.168.5.6**.
Маршрутизатор пришедший пакет уничтожает, так как не может его перенаправить на указанный адрес, потому что соответствующего MAC-адреса он **не знает**. В связи с этим маршрутизатор формирует ARP-запрос по адресу **192.168.5.6**.
Все узлы подсети игнорируют пакет, потому что IP-адрес в запросе не соответствует их собственным IP-адресам. Маршрутизатор ни от кого не получает ответа. Процедура прохождения пакетов повторяется в течение всего сценария симуляции: маршрутизатор по-прежнему **не знает** MAC-адреса указанного в ping-запросе IP-адреса **192.168.5.6** и продолжает рассылать ARP-запросы. Ни один из узлов подсети на эти запросы не реагирует. Не получив ответа, маршрутизатор и сам **молчит**, никак не уведомляя об ошибке хост-источник ping-запроса.
Проследите в рабочей области все описанные выше действия.
Посмотрим ответ на ping-запрос в командной строке узлаисточника 192.168.3.7: превышено время ожидания (**рис. 2.24**).

PC>ping 192.168.5.6
Pinging 192.168.5.6 with 32 bytes of data:
Request timed out.
Рис. 2.24. Вывод программы ping

Проанализируйте результат ping-запроса, содержащего IP-адрес узла, в сеть, на которую нет маршрута. Откройте окно **Command Promt** на узле **192.168.3.6** и отправьте ping-запрос на несуществующий хост с IP-адресом
192.168.6.6. **Посмотрите содержимое пакета**,
сформированного маршрутизатором. Этот пакет приходит на узел **192.168.3.6**. Тип ICMP-сообщения – **3** с кодом **1**, что означает, **хост недостижим**. Таким образом, маршрутизатор ответил на ping-запрос, для которого у него не было соответствующего маршрута, новым ICMP-сообщением – **хост недостижим**.

Индивидуальные задания
В соответствии с вариантом отфильтруйте ARP и ICMP сообщения для указанных пар **источник - приемник**. В каждом варианте предусмотрены **2 варианта** ping-запроса: внутри сети и во внешнюю сеть. С помощью команды **tracert** посмотрите маршрут пакета, адресованного во внешнюю сеть.
В отчете для каждого теста приведите маршруты пакетов, их содержимое и объясните полученные результаты.
Варианты заданий представлены в таблице.

Вариант	**Источник**	**Приемник**
1	192.168.3.3 192.168.3.4	192.168.3.4 192.168.5.4
2	192.168.3.4 192.168.3.5	192.168.3.7 192.168.5.3
3	192.168.3.5 192.168.3.6	192.168.3.6 192.168.5.5
4	192.168.3.6 192.168.3.7	192.168.3.4 192.168.5.4
5	192.168.3.3 192.168.3.7	192.168.3.7 192.168.5.5
6	192.168.5.3 192.168.3.6	192.168.5.4 192.168.5.4
7	192.168.3.3 192.168.3.5	192.168.3.7 192.168.5.4
8	192.168.3.3 192.168.3.4	192.168.5.4 192.168.3.5
9	192.168.3.4 192.168.3.5	192.168.5.3 192.168.3.4
10	192.168.5.4 192.168.3.6	192.168.5.5 192.168.5.3
11	192.168.3.4 192.168.3.7	192.168.5.3 192.168.3.4
12	192.168.3.5 192.168.3.6	192.168.5.5 192.168.3.7
13	192.168.3.5 192.168.3.7	192.168.5.4 192.168.3.3
14	192.168.3.6 192.168.3.7	192.168.5.3 192.168.3.5
15	192.168.3.5 192.168.3.6	192.168.3.6 192.168.5.5

16	192.168.5.3 192.168.3.6	192.168.5.4 192.168.5.4
17	192.168.3.3 192.168.3.5	192.168.3.7 192.168.5.4
18	192.168.3.3 192.168.3.4	192.168.5.4 192.168.3.5
19	192.168.3.4 192.168.3.7	192.168.5.3 192.168.3.4
20	192.168.3.5 192.168.3.6	192.168.5.5 192.168.3.7