ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения Императора Александра I»
(ФГБОУ ВО ПГУПС)

Петрозаводский филиал ПГУПС

ОДОБРЕНО
на заседании цикловой комиссии
протокол № 11 от 30.06.2017
Председатель цикловой комиссии:
_____ (Сапанов М.М.)

УТВЕРЖДАЮ
Начальник УМО
_____ А.В. Калько
«13» 06 2017 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению практических занятий/лабораторных работ

По дисциплине/МДК/ПМ: УП.03.01 Диагностика и обслуживание сетей

Специальность: 09.02.02 Компьютерные сети

Выполнил (а): Лятти А.А. – Преподаватель Петрозаводского филиала ПГУПС.

2017г.

ВВЕДЕНИЕ

Методическое пособие по проведению учебной практики, входящей в состав ПМ.03 Эксплуатация объектов сетевой инфраструктуры составлено в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее СПО) 09.02.02 Компьютерные сети

Настоящее методическое пособие рассчитано на самостоятельную работу обучающихся в учебном кабинете под руководством преподавателя, а также является руководством для преподавателей при подготовке к проведению учебной практики.

Для успешного прохождения учебной практики могут быть использованы теоретические знания, полученные обучающимися при изучении ПМ.03 «Эксплуатация объектов сетевой инфраструктуры»

УП.03.01 «Диагностика и обслуживание сетей» направлена на:

- приобретение студентами профессиональных навыков и первоначального опыта в профессиональной деятельности;

- формирование основных профессиональных компетенций, соответствующих виду профессиональной деятельности (ВПД) Организация деятельности коллектива исполнителей

- воспитание сознательной трудовой и производственной дисциплины;

- усвоение студентами основ законодательства об охране труда, системы стандартов безопасности труда, требований правил гигиены труда и производственной санитарии, противопожарной защиты, охраны окружающей среды в соответствии с новыми нормативными и законодательными актами.

Результатом освоения учебной практики является овладение обучающимися видом профессиональной деятельности (ВПД): Организация деятельности коллектива исполнителей, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3.	Эксплуатация сетевых конфигураций
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
ПК 3.5	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования.
ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполненных заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Каждый студент обязан оформлять отчет о проделанной работе. Отчет должен содержать:

- титульный лист;

- цель работы;

- задание;

- выполненное практическое занятие в соответствии с заданием;

- вывод;

Правила охраны труда при проведении учебной практики.

1. Общие требования охраны труда.

1.1. К работе в учебном кабинете допускаются студенты, прошедшие инструктаж по охране труда, знающие правила пожарной безопасности.

1.2. При работе в кабинете должны соблюдаться правила поведения, расписание учебных занятий, установленный режим труда и отдыха.

1.3. При проведении занятий возможно воздействие на студентов следующих опасных факторов:

- нарушение осанки, искривление позвоночника, развитие близорукости при неправильном подборе мебели;

- нарушение остроты зрения при недостаточной освещенности в кабинете;

- поражение электрическим током при неисправном оборудовании кабинета;

1.4. В процессе занятий студенты должны соблюдать правила личной гигиены, содержать в чистоте рабочее место.

2. Требования безопасности перед началом занятия.

2.1. Включить полностью освещение в кабинете, убедиться в правильности работы светильников. Наименьшая освещенность в кабинете должна быть не менее 300Лк (20ВТ/м^2) при люминесцентных лампах.

2.2. Убедиться в исправности электрооборудования кабинета: коммуникационные коробки выключателей и розеток не должны иметь трещин, сколов, а также оголенных контактов.

2.3. Проверить санитарное состояние кабинета, убедиться в целостности стекол в окнах и провести сквозное проветривание кабинета.

3.Требование безопасности во время занятия.

3.1. Используемые в кабинете демонстрационные электрические приборы должны быть исправны и иметь заземление и зануление.

4. Требования безопасности в аварийных ситуациях.

4.1. При возникновении аварийных ситуаций немедленно эвакуировать студентов и сообщить администрации учреждения.

5. Требования безопасности по окончании занятия.

5.1. Выключить демонстрационные электрические приборы;

5.2. Закрыть окна и выключить свет

ПЕРЕЧЕНЬ

практических занятий по УП.03.01 «Диагностика и обслуживание сетей»

ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Для специальности 09.02.02 Компьютерные сети

Практическая работа №1

Тема: Основные операции по монтажу и тестирование витой пары на стороне клиента

Опрессовка прямого провода по стандарту Т568В

При монтаже локальных сетей сегодня наиболее распространена неэкранированная *витая пара* 5й категории (CAT-5E) – рис. 1.1.

Рис. 1.1. Так выглядит кабель витая пара

Обжим такого кабеля для соединения ПК (*PC*)-ХАБ (*HUB*) по стандарту T568B изображен на рис. 1.2.

Рис. 1.2. Прямой обжим для соединения ПК-ХАБ (Одинаковый цвет проводников с обеих сторон кабеля)

Примечание

Обжим (опрессовка) по варианту T568A - стандарт, имеющий хождение в США и Канаде, а в России, в основном, применяется стандарт T568B.

Для обжима (опрессовки) витой пары вам потребуются пара коннекторов RJ-45и специальные клещи (кримпер) - рис 1.3-1.5.

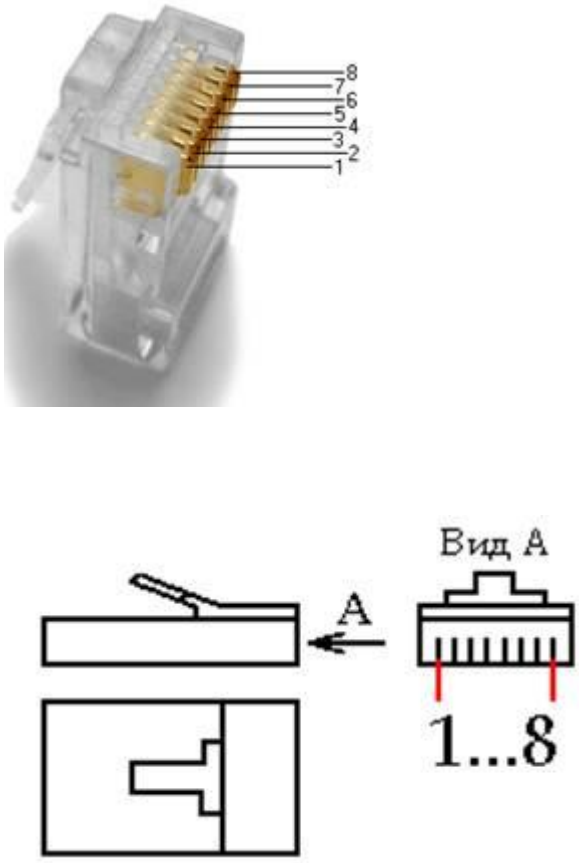


Рис. 1.3. Нумерация контактов разъема RJ-45

Рис. 1.4. Кримпер

Рис. 1.5. Коннектор вставлен в кримпер

Последовательность действий при обжиме:

- Аккуратно обрежьте конец кабеля резаком, встроенным в обжимной инструмент.
- Снимите с кабеля изоляцию ножом, встроенным в обжимной инструмент.
- Разведите и расплетите проводки, выровняйте их в один ряд. Обкусите проводки так, чтобы их осталось чуть больше сантиметра (см. примечание).

- Вставьте проводники в коннектор RJ-45. Убедитесь, все ли провода полностью вошли в разъем и уперлись в его переднюю стенку.
- Вставьте коннектор в устройство для обжима коннектора.
- Надавите на клещи так, чтобы контакты коннектора зажали проводники внутри него.

Примечание

На рис. 1.6 показан неправильный обжим витой пары. На примере слева оставлены слишком длинные жилы, из-за чего расстояние от коннектора до оплетки остается незащищенным. Также кабель теряет прочность. На втором примере жилы срезаны слишком коротко, оплетка входит в коннектор и длина концов проводников не позволяет создать их полноценный контакт с коннектором.

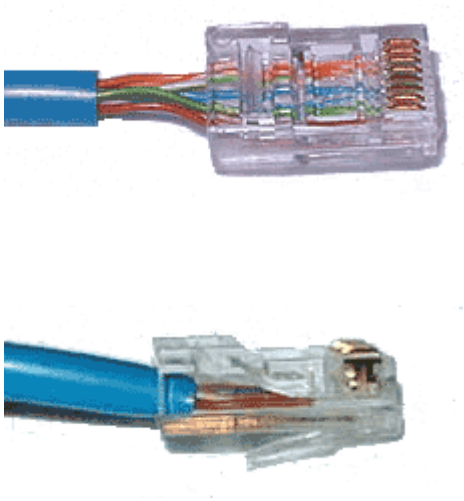


Рис. 1.6. Ошибки обжима кабеля

Контроль результата

Для проверки правильности обжима соедините кабелем сетевую карту и *HUB* (*коммутатор*, свич) и убедитесь в правильной работе такого кабеля. Другой вариант – использовать специальный тестер со светодиодной индикацией (рис. 1.7).

Рис. 1.7. Внешний вид тестера для проверки витых пар RJ-45 модели FA-7012B

В продаже представлено множество тестеров для проверки витых пар *RJ-45* разного уровня сложности и ценового диапазона. Однако, принцип работы их аналогичен. Так, например, кабельный тестер FA-7012B состоит из 2 функциональных блоков - передатчика и приемника, которые подключаются к концам кабельной линии через разъемы *RJ-45* или RJ-12. Он позволяет обнаружить оборванные пары, закороченные пары, перепутанные провода в одной паре, перепутанные пары и перепутанные провода между разными парами. Также прибор позволяет проверить *целостность* экрана кабеля. Блок-передатчик последовательно опрашивает состояние каждого провода в кабеле, а блок-приёмник возвращает ответ по неиспользуемой в конкретный момент паре. Последовательное загорание светодиодов сигнализирует о правильном соединении. Устройство питается от 1 батареи типа "Крона" 9 В.

Обжимаем розетку категории 5 под разъем RJ45

Стандартная схема подключения ПК к локальной или глобальной сети приведена на рис. 1.8.

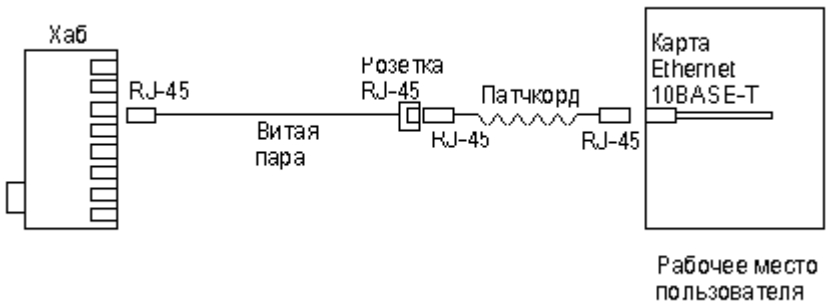


Рис. 1.8. Обычная схема подключения домашнего или офисного ПК к сети

Так же, как и сам *кабель*, *витая пара*, сетевые розетки различаются по категориям. В идеале, для профессионального монтажа вам понадобятся: розетка *RJ-45* категории 5е для настенного монтажа, устройство для зачистки и обрезки витой пары, устройство для заделки витой пары, 4-парный *кабель UTP*, категория 5е и маркеры для нанесения обозначений на *кабель* (рис. 1.9).

Рис. 1.9. Набор для монтажа розетки (слева инструмент для снятия изоляции, сверху – для обрезки концов проводников)

Все контакты в розетках категории 5 пронумерованы, поэтому никаких проблем с разводкой кабеля возникнуть не должно.

Ситуация 1. Розетка с одним гнездом на 8 проводов (видео)

Для работы потребуется отвертка с плоским тонким жалом, по толщине, не превышающей *диаметр* медного проводника витой пары – рис. 1.10. Также заталкивать провода в щели розетки можно ножом с тонким лезвием, например, канцелярским ножом, у которого лезвие выдвигается.

Рис. 1.10. Нумерация контактов в розетке с одним гнездом по стандарту Т568В (для стандарта Т568А цвета контактов розетки тоже обозначены)

Подготавливается для разделки *кабель*, снимается на длину не более 3 см его внешняя *оболочка*. Расплетаются пары на длину не более 13-15 мм. Далее, по схеме цветов, проводники по очереди заводятся в гребенку, заправляются боковой плоскостью лезвия отвертки и затем торцом лезвия заталкиваются до упора. В особых случаях (при необходимости) в одно гнездо можно вставить два кабеля витой пары, смонтированных на одну вилку (рис. 1.11).

Рис. 1.11. Особый вариант обжима кабеля

Понятно, что скорость информации при таком монтаже будет не 100, а 10 Мбит/сек.

Ситуация 2. Розетка на 2 гнезда по 8 проводов

Для надежной фиксации проводников в контактах розетки существует специальный инструмент, позволяющий поместить провод на максимальную глубину, хотя, можно обойтись обыкновенным пинцетом и отверткой. Провода перед вбиванием в клеммы зачищать не надо - щели оснащены специальной режущей кромкой, которая сама прекрасно снимает с них изоляцию.
Заведите *кабель* на *модуль* розетки. Подготавливается для разделки *кабель*, снимается на длину не более 3 см его внешняя *оболочка*. Расплетаются пары на длину не более 13-15 мм. Закрепите *кабель* стяжкой на печатной плате розетки. Обрежьте конец стяжки с помощью кусачек или ножниц. На самой розетке всегда есть схема, какой цвет кабеля, в какой контакт должен приходить. На печатной плате наклеена табличка, на которой прорисованы в цветах варианты T568B и T568A разделки проводников витой пары в гребенки – рис. 1.12.

Рис. 1.12. Цветовая маркировка проводов розетки стандарта T568B это: 1 бело-ор, 2 ор, 3 бело-зел, 4 син, 5 бело-син 6 зел 7 бело кор, 8 кор (для варианта T568A цвета тоже нарисованы)

После выбора места установки розетки нужно ее закрепить на стене с помощью двух шурупов или приклеить двусторонним скотчем (обычно прилагаются в комплекте с розеткой). Для крепления шурупами нужно снять крышку и печатную плату, чтобы добраться до крепежных отверстий в основании розетки. Чтобы снять крышку, нужно двумя пальцами сдавить ее с боков в месте, близком к основанию и потянуть на себя. Защелки выйдут из зацепления, и крышка легко отойдет в сторону. Далее снимается печатная *плата* отведением в стороны четырех защелок по углам.

Практическая работа № 2

Тема: Основные операции по монтажу и тестирование витой пары на стороне коммутационного шкафа

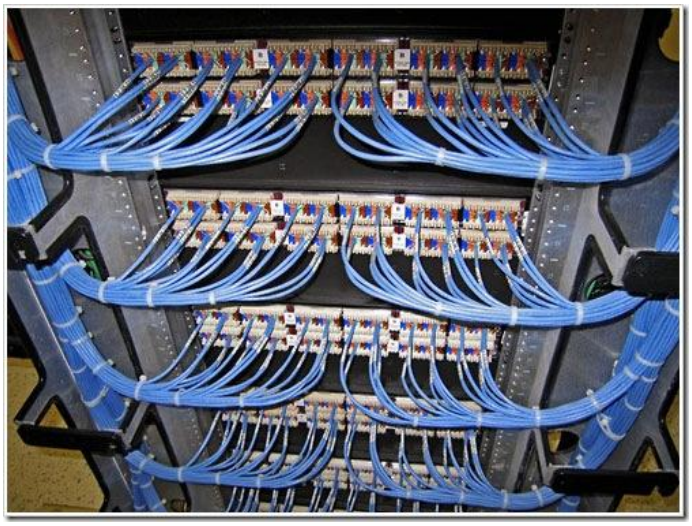
Инструменты для монтажа и заделки проводов.

Стриппер – электромонтажный инструмент. Предназначен для удаления изоляции с концов проводов и разделки кабеля (UTP, STP). Имеет соответствующие пазы для проводов

разного диаметра. Для зачистки и разделки кабелей диаметром до 9.5 мм.

Вруб – для зачистки и обработки витой пары. Инструмент с функцией «удара».

Коммутационная панель.



На лицевой панели находятся контакты, предназначенные для фиксированного соединения с кабелем.

Классификация патч-панелей.

1. **По составу разъёма.**

1.1. Фиксированное: -медная (RJ-12, RJ-45).

-волоконно-оптическая

-мультимедийн

1.2. Наборно-юнитовая – может содержать в корпусе различные разъёмы.

1.3. Наборная. Для установки в промежуточные конструктивы.

2. По количеству портов (12,24,48,96).

3. **По экранированию (экранированная, неэкранированная).**

4. **По способу крепления.**

4.1. В стену

4.2. В стойку

4.3. В промежуточные конструктивы.

5**. По способу представления портов**

5.1. Одинарное

5.2. Двойное

Ход работы:

1. Зачистить наружную изоляцию кабеля и развести провода «витой пары» по схеме А.

2. Произвести заправку проводников в разъем корпуса RJ-45 до упора, так, чтобы изоляция также вошла вовнутрь коннектора.

3. Вставить разъем в гнездо обжимного устройства - кримпера, и надавливаем до тех пор пока устройство полностью не закроется, до щелчка, и опрессовываем.

4. Те же операции проделать с другим концом кабеля.

5. Взять новый кабель и с помощью вруба врезать проводники в розетку. С другим концом данного кабеля проделать операции, указанные в первых трёх подпунктах.

6. Взять третий кабель и врезать с помощью вруба проводники в патч-панель. С другим концом данного кабеля проделать операции, указанные в первых трёх подпунктах.

7. Собрать и протестировать схему.

Практическая работа №3

Тема: Основные операции по монтажу и тестирование беспроводных сетей

Теоретические сведения

Беспроводные сети весьма перспективны. Несмотря на свои недостатки, главный из которых – незащищенность среды передачи, они обеспечивают простое подключение абонентов, не требующее кабелей, мобильность, гибкость и масштабируемость сети.

Как было сказано ранее (см. **Теоретические сведения: Беспроводные сети**), в сетях стандарта **IEEE 802.11b** используется два разных типа устройств для соединения:

Узловые передатчики (точки доступа) - небольшие устройства, которые используют порты **RJ-45** для подключения к обычной сети **Ethernet**, содержат ***приемопередатчик*** *(трансивер, transmitter + receiver = transceiver)*, а также программное обеспечение кодирования и связи. Трансивер транслирует сигналы обычной сети **Ethernet** в сигналы беспроводной сети **Ethernet** и передаёт их беспроводным сетевым адаптерам, а также преобразует сигналы в обратную сторону.

Сетевые адаптеры, оборудованные приемопередатчиками. Сетевые адаптеры, оборудованные для связи по беспроводным сетям **Ethernet**, имеют стационарную или съемную антенну вместо обычного кабельного разъёма.

Поскольку основной рынок сбыта для беспроводных **Ethernet** составляют пользователи портативных компьютеров, производители выпускают устройства беспроводной сети **Ethernet** не только в версии для ***PC CARD***, но и модели для различных шин (в основном *USB*). Т.о., к одной беспроводной сети можно подключать как портативные, так и стационарные компьютеры.

Стандарт **IEEE 802.11** утверждает, что все совместимые беспроводные ЛВС должны предоставлять девять типов сервисов (услуг). Их можно разделить на две категории: *сервисы распределения* (пять из девяти) и *станционные* (четыре сервиса).

Сервисы распределения связаны с управлением станциями, находящимися в данной соте, и взаимодействием с внешними станциями.

Станционные сервисы, наоборот, имеют отношение к управлению активностью внутри одной соты.

Пять сервисов распределения предоставляются базовой станцией и имеют дело с мобильностью станций при их входе в соту или выходе из нее:

- *Ассоциация.* Используется мобильными станциями для подключения к базовым станциям (БС). Мобильная станция передает идентификационную информацию и сообщает о своих возможностях (поддерживаемой скорости передачи данных, необходимости *PCF-услуг*, или опроса) и требованиях по управлению электропитанием. Базовая станция может принять или отвергнуть мобильную станцию. Если последняя принята, она должна пройти идентификацию.
- *Дизассоциация.* По инициативе мобильной или базовой станции может быть произведена дизассоциация, то есть разрыв отношений. Это требуется при выключении станции или ее уходе из зоны действия БС. Впрочем, базовая станция также может быть инициатором дизассоциации, если, например, она временно выключается для проведения технического обслуживания.
- *Реассоциация.* С помощью этого сервиса станция может сменить БС. Очевидно, данная услуга используется при перемещении станции из одной соты в другую. Если она проходит корректно и без сбоев, то при переходе никакие данные не теряются.
- *Распределение.* С помощью этой услуги определяется маршрутизация кадров (единицы данных, которыми обмениваются компьютеры в сети **Ethernet**), посылаемых базовой станции. Если адрес назначения является локальным с точки зрения БС, то кадры следуют просто напрямую (передаются в эфире). В противном случае их необходимо пересылать по проводной сети.
- *Интеграция.* Если кадру нужно пройти через сеть, не подчиняющуюся **стандарту 802.11** и использующую другую схему адресации и/или формат кадра, то на помощь приходит данный сервис. Он реализует трансляцию форматов.

Оставшиеся *четыре сервиса* — это внутренние услуги соты. Они предоставляются после прохождения ассоциации. Ниже перечислены станционные сервисы:

- *Идентификация.* Поскольку беспроводные коммуникации подразумевают очень легкое подключение к сети и возможность приема/отправки данных любыми станциями, попавшими в зону действия БС, то возникает необходимость идентификации. Только после идентификации станции разрешается обмен данными. После принятия мобильной станции в ряды текущих абонентов соты базовая станция посылает специальный кадр запроса, позволяющий понять, знает ли станция присвоенный ей секретный ключ (пароль). Подтверждение осуществляется путем шифрования кадра запроса и отсылки его назад базовой станции. Если шифрование выполнено

корректно, мобильная станция получает нормальные права доступа к сети.

- *Деидентификация.* Если станция, работавшая в сети, покидает ее, она должна произвести деидентификацию. После выполнения данного сервиса она больше не сможет использовать ячейку.
- *Конфиденциальность.* Чтобы сохранить передаваемые по сети данные в тайне от посторонних «ушей», их необходимо шифровать. Данный сервис осуществляет операции по шифрации и дешифрации информации. Применяется алгоритм *RC4*, изобретенный Рональдом Ривестом (*Ronald Rivest*).
- *Доставка данных.* Именно этот сервис является ключевым во всей работе сети, поскольку **стандарт 802.11** существует для обмена данными.

Среди изготовителей *Wi-Fi оборудования* такие известные компании, как ***Dlink, Cisco Systems, Intel, Texas Instruments и Proxim.***

В общем случае алгоритм работы с беспроводным адаптером сводится к следующим действиям:

1. подключить адаптер к компьютеру;
2. настроить адаптер для динамического или ручного получения IP-адреса;
3. просмотреть список доступных беспроводных сетей и подключиться к выбранной.

Программа ***Network Stumbler*** сканирует диапазон частот 2,4 ГГц и показывает все найденные в данном месте беспроводные точки доступа и адаптеры, работающие в режиме Ad-Hoc.

Network Stumbler выдает информацию о *MAC-адресах* обнаруженных беспроводных устройств, значения *SSID* (символьные имена сетей), имена устройств, каналы, сообщает о том, включено ли шифрование WEP и т. д.

При наличии GPS-приемника можно узнать координаты интересующей точки доступа.

Network Stumbler может определить правильно ли настроена беспроводная сеть, найти места с недостаточным радиопокрытием, установить наличие и характеристики других сетей, которые могут мешать работе сети.

Программа будет полезна также для обнаружения беспроводных устройств, работающих на территории предприятия без необходимого разрешения (часто сотрудники используют оборудование Wi-Fi в корпоративных сетях без согласования с кем бы то ни было).

Network Stumbler отображает качество связи в виде графиков уровня сигнала и шума. Данные сканирования можно сохранить в файле.

Выполнение работы

Задание 1. Настройте точку доступа беспроводной сети.

1. Физически подключите *точку доступа* (ТД) к компьютеру с помощью витой пары.
2. Откройте **окно настроек ТД**. Для этого:
   - запустите браузер;
   - введите *IP-адрес* ТД. Нажмите клавишу **ENTER** на клавиатуре для перехода по адресу;
   - введите в поле:
     - **Имя пользователя** – *admin*;
     - **Пароль** – *пароль_ТД*.
3. Запустите ***мастер настройки ТД***. Для этого щелкните по кнопке ***Wizard/Run Wizard***.
   Перед вами откроется диалоговое окно мастера настройки ТД.
4. Установите пароль ТД:
   - перейдите к окну **Set Password (Установка пароля)**, воспользовавшись кнопкой ***Next***  ;
   - введите новый пароль в поле **New Password** - *123*;
   - подтвердите введенный пароль в поле **Confirm Password**;
   - закройте окно кнопкой ***Next***.
5. Настройте параметры беспроводной сети LAN в диалоговом окне **Set Wireless LAN Connection**:
   - установите **SSID** (символьное имя) вашей точки доступа (*My_Wi-Fi*);
   - выберите **12 канал** (Channel), на котором будет работать ТД;
   - закройте окно кнопкой ***Next***.
6. Установите параметры шифрования передаваемой информации в диалоговом окне **Setup Encryption (Установка шифрования)**:
   - **Wep** – *Enabled*;
   - **Encription** – *128 bit*;
   - **Wep mode** – *ASCII*;
   - в поле **Key 1** введите *123456789ABCD*;
   - закройте окно кнопкой ***Next***.
7. Завершите процесс конфигурирования ТД, нажав на кнопку ***Restart***.
8. Разрешите ТД выполнять роль **DHCP-сервера**:
   - перейдите на вкладку **Home** и в раздел **LAN**;
   - установите переключатель ***Static IP Address (статический IP-адрес)***;

- в поле **IP Address** (IP-адрес) введите статический IP-адрес из диапазона вашей сети, например, *172.21.5.151*;
- в поле **Subnet Mask** (Маска подсети) введите маску (*255.255.0.0*);
- в поле **Gateway** (Шлюз) введите адрес шлюза в вашей сети (*172.21.5.123*);
- примените изменения с помощью кнопки ***Apply*** (применить)  . *ТД должна будет перезагрузиться и применить сделанные изменения;*
- перейдите в раздел **Home/DHCP**;
- выберите переключатель ***DHCP server enabled (DHCP сервер включен)***;
- введите в поле **Starting IP Address** (Начальный I- адрес) - *100*;
- введите в поле **Ending IP Address** (Конечный I- адрес) - *200*;
- введите в поле **DNS Server** (DNS сервер) IP-адрес сервера имен вашей сети, например *172.21.5.1*;
- выберите в поле **Lease Time** (время аренды/действия) - *1 weak*;
- примените внесенные изменения.

Задание 2. Настройте беспроводной сетевой адаптер.

1. Откройте окно настройки беспроводного адаптера:
   - перейдите в окно **Сетевые подключения**;
   - вызовите свойства элемента Wi-Fi (***Контекстное меню/Свойства***);
   - щелкните по кнопке ***Настроить***.
2. Установите смешанные режим работы беспроводного адаптера:
   - перейдите на вкладку **Дополнительно**;
   - установите для свойства **Configuration Profile** (конфигурация профиля) значение *Mixed* (смешанное);
   - примените параметры кнопкой **OK**.
3. Откройте окно настройки беспроводного сетевого адаптера.
4. Настройте параметры элемента ***Протокол Интернета (TCP/IP)***:
   - откройте окно свойств этого элемента;
   - выберите **Использовать Следующий IP-адрес**;
   - введите в соответствующие поля указанные значения:
     - **IP-адрес** - 172.21.5.155
     - **Маска подсети** – 255.255.0.0
     - **Основной шлюз** – 172.21.5.123
     - **Предпочитаемы DNS-сервер** – 172.21.5.1
     - **Альтернативный DNS-сервер** – 172.21.5.3
   - примените параметры кнопкой **OK**.
5. Разрешите компьютеру подключаться к любой доступной сети:

- перейдите на вкладку **Беспроводные сети** и щелкните по кнопке ***Дополнительно***;
- установите флажок *Автоматически подключаться к любой сети* и закройте окно кнопкой ***Закрыть***.

6. Завершите конфигурирования сетевого адаптера кнопкой **OK**.

Задание 3. Подключитесь к беспроводной сети.

1. Откройте окно просмотра доступных беспроводных сетей (***Контекстное меню значка беспроводного адаптера в области уведомления /Просмотр доступных беспроводных сетей***).
2. Обновите список сетей кнопкой ***Обновить список сетей***.
3. Выберите беспроводную сеть для подключения, например **My_Wi-Fi**.
4. Подключитесь к сети:
   - щелкните по кнопке ***Подключить***;
   - ведите *Ключ_ сети* в **первое поле**;
   - повторно ведите *Ключ_ сети* во **второе поле**;
   - щелкните по кнопке ***Подключить***.

Задание 4. Просмотрите параметры беспроводных сетей.

1. Запустите программу ***Network Stumbler***.
2. Просмотрите доступные сети по каналам. Для этого в левой области окне разверните узел **Channels**.
3. Просмотрите список доступных сетей по их именам. Для этого разверните узел **SSIDs.**
4. Определите сеть с наиболее мощным сигналом.
   Можно щелкнуть по любой сети в левом списке и справа отобразится график уровней сигнала.
5. Воспользуйтесь фильтром для поиска сетей без шифрования (***Filters/ Encryption off***).
6. Результаты мониторинга сообщите преподавателю.

Задание 5. Выполните самостоятельные задания 1-2.

Практическая работа № 4

Тема: Измерение характеристик проводных сетей

Нарушения нормального функционирования кабельных систем на базе витой пары могут быть вызваны грубыми ошибками при монтаже, скрытыми

дефектами конструкции кабеля и повреждением во время его прокладки, процессами старения самих витых пар и арматуры кабельных линий связи, а также другими причинами.

ОСНОВНЫЕ ПОВРЕЖДЕНИЯ ВИТОЙ ПАРЫ И ИХ ПРИЧИНЫ

К явным недостаткам монтажа относятся ошибки соединения жил витых пар в кроссах АТС, на стыках строительных длин, в распределительных шкафах и коробках, удаленных терминалах и т. д.

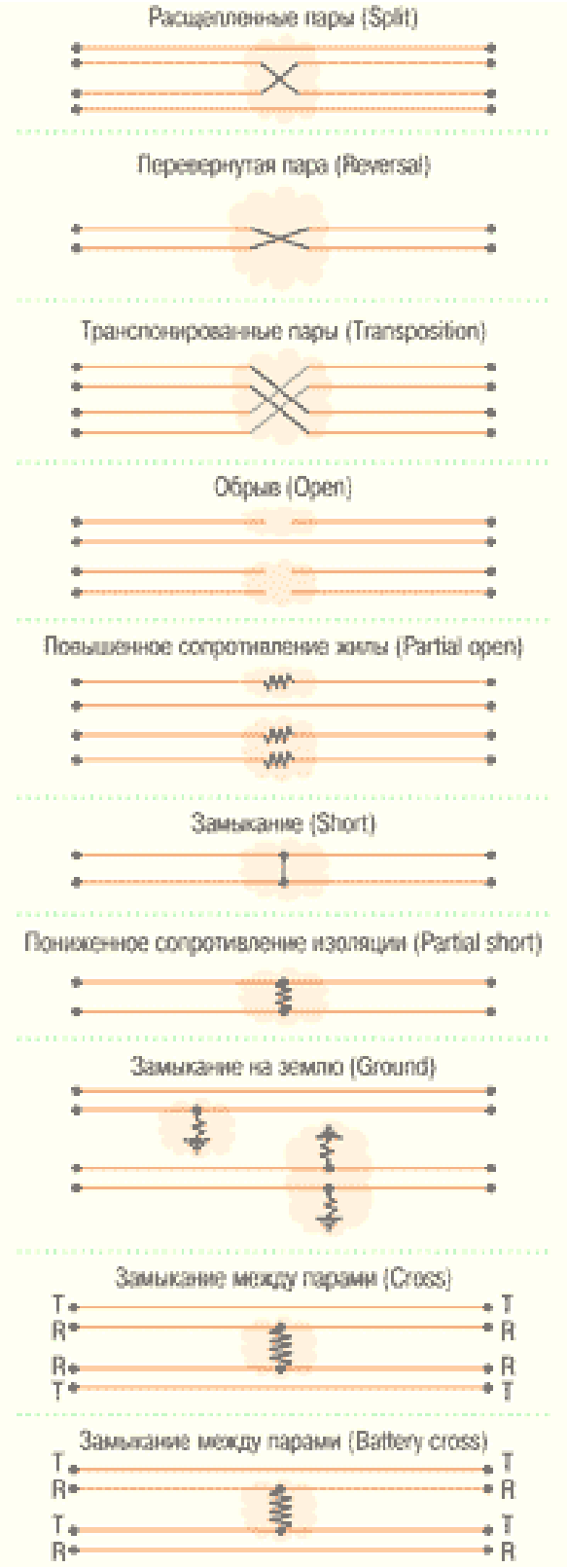
В соответствии с принятой терминологией, две пары, в которых нарушен правильный порядок подключения жил, называются расщепленными (split). Признаками расщепленных пар могут быть увеличенный резистивный и емкостной дисбаланс.

Неправильно смонтированная витая пара, где прямой и обратный провода переставлены местами, называется перевернутой, или скрещенной (reversal). В кабельных линиях СКС порядок подключения жил витой пары крайне важен.

Две витые пары с ошибочным подключением к зажимам терминала называются транспонированными парами (transposition). На телефонной сети такой дефект монтажа приведет к подключению неверного номера. В случае же СКС подключенное к линии оборудование может оказаться неработоспособным.

К основным скрытым дефектам кабельных линий связи относится некачественный монтаж муфт и сростков жил на стыках строительных длин. В первом случае нарушается герметичность оболочки кабеля и возникает опасность его намокания, а для второго характерно появление плохих контактов (partial open) и даже обрыв жил витой пары (open). К таким же результатам приводит коррозия контактов кроссовых устройств и некачественная кроссировка. Дефекты и пробои изоляции жил, влага в кабеле и загрязнение терминалов нередко ведут к замыканию жил пары между собой.

Замыкание может быть низкоомным (short) или высокоомным (partial short). Еще один аналогичный вид дефектов витой пары — замыкание на землю одной или нескольких ее жил (ground). Причем контакт жилы с землей совсем не обязательно будет находиться недалеко от места повреждения изоляции жилы — электрический путь от проводника жилы к земле пройдет через экран кабеля, металлические элементы конструкции терминалов и несущие элементы кабеля.

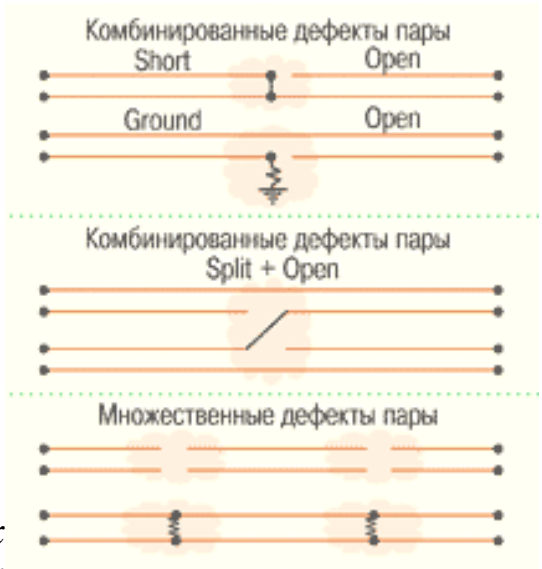


Замыкание случается и между жилами двух различных пар, причем замкнуты могут быть как одноименные, так и разноименные жилы (cross и battery cross, соответственно). Такой вид дефектов приводит к наличию постороннего напряжения на линии, переходным явлениям, ослаблению сигнала.

Естественный процесс старения витой пары проявляется в виде увеличения вносимого ею затухания вследствие ухудшения диэлектрических свойств изоляции витой пары.

При идентификации неисправностей пары всегда нужно иметь в виду, что ее дефекты могут быть множественными (несколько однотипных дефектов) или комбинированными (несколько разнотипных дефектов), а показания приборов при измерениях с различных сторон могут существенно отличаться.

Источниками помех витой пары служат внутренние и внешние помехи кабеля.



К основным источникам внутренних помех относят соседние витые пары того же кабеля, а к основным источникам внешних помех — помехи от сети переменного тока и атмосферные явления, включая разряды молнии и радиопомехи.

Нарушение нормальной работы любого из них может стать причиной повышенных шумов витой пары.

Задание: обследовать образцы витой пары и указать причину неисправностей. Оформить результаты в виде таблице.

Практическая работа № 5

Тема: Измерение характеристик беспроводных сетей

Развитие вычислительных сетей (ВС) приводит к сокращению разрыва между локальными и глобальными сетями, что во многом во многом обусловлено появлением высокоскоростных территориальных каналов связи, не уступающих по качеству кабельным системам локальных сетей. Изменяются и локальные сети. Вместо пассивного кабеля, соединяющего компьютеры, для ВС используют разнообразное коммуникационное оборудование – коммутаторы, маршрутизаторы, шлюзы. Появились беспроводные локальные вычислительные сети (БЛВС). БЛВС практически находятся вне конкуренции по оперативности развертывания, мобильности и цене, во многих случаях предоставляя единственное экономически оправданное решение. В связи с этим весьма актуальной является дальнейшая разработка фундаментальной теории в области передачи информации, методов проектирования и оценки характеристик беспроводной сети.

Данная работа посвящена оценке производительности беспроводных локальных сетях, соответствующих стандарту IEEE 802.11.

Для проведения исследований потребовалось:

- собрать стенд, представляющий собой фрагмент Wi-Fi сети, содержащий три рабочие станции и одну точку доступа;
- провести настройку исследуемого фрагмента Wi-Fi сети.
- провести эксперименты по исследованию влияния настраиваемых параметров на производительности канала Wi-Fi сети.

Исследования проводились на фрагменте Wi-Fi сети, содержащем три рабочие станции и одну точку доступа. Под настройкой сети понимается настройка роутера WL500gP v2 и клиентских станций подключаемых к данной локальной сети. Настройка роутера проводиться по инструкции, прилагаемой к роутеру.

В соответствии с задачами исследований требуется определить производительности сети:
для базовых параметров, настроенных по умолчанию,

для параметров с повышенной пропускной способность, которая получена в результате исследований, устанавливающих влияние на пропускную способность настраиваемых параметров и различных технологий, которые предлагают производители чипсетов для роутеров данного класса.

Для повышения производительности будут изменены параметры тонкой настройки и применены различные технологии, которые предлагают производители чипсетов для роутеров данного класса.

В соответствии с задачами исследований требуется произвести оценку изменения производительности.

Оценка повышенной пропускной способности производится сравнением с *базовой* пропускной способности, выраженной в Кбит/с

Методика решения поставленной задачи предусматривает определение используемых средств, измерение пропускной способности экспериментальной сети беспроводного доступа Wi-Fi.

Используемыми средствами являются:

Web-интерфейс роутера WL500gP v2 С помощью web-интерфейса происходит выбор и применение различных параметров Wi-Fi роутера

Программа INSSIDER от компании Metageek Программа INSSIDER является инструментом для поиска и сбора информации о Wi-Fi сетях в зоне нахождения компьютера. Для найденных сетей с помощью данной программы можно узнать MAC-адрес роутера из «соседней» сети, производителя роутера, канал, используемый данным роутером, идентификатор SSID или публичное название сети, тип безопасности. Кроме того, программа показывает уровень мощности передатчика в dBm и с помощью данной программы можно посмотреть диаграмму «соседних» сетей расположенных в диапазоне 2,4 ГГц и оценить загруженность каналов данного диапазона. На рис. 1. показана диаграмма диапазона 2,4 ГГц, на которой можно посмотреть «соседние сети», оценить их мощности передатчиков, что важно учитывать при настройке параметров сети.

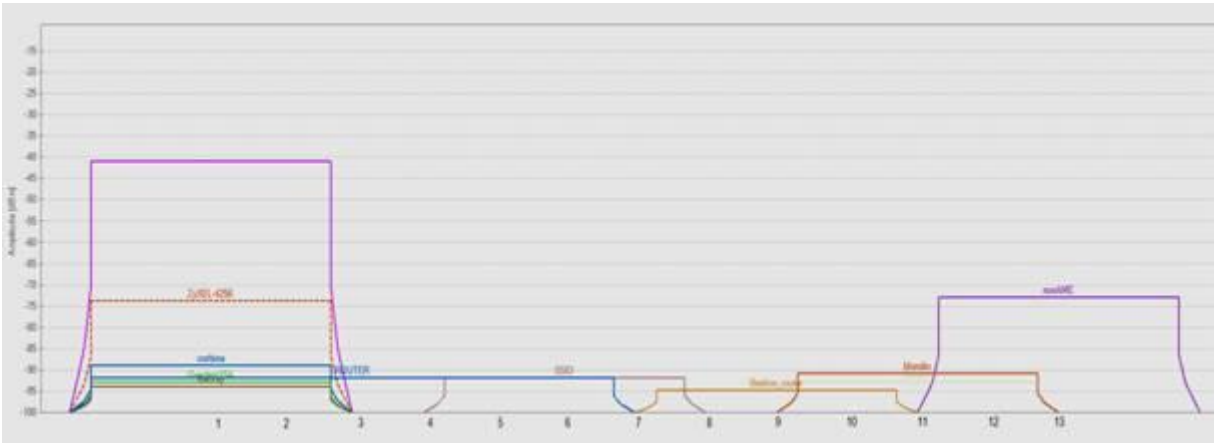


Рис. 1. Таблица «соседних» беспроводных сетей и аплитудно-частотная диаграмма всех сетей диапазона 2,4 ГГц в программе INSSIDER

Пояснения полей программы INSSIDER

Поле	Значение
SSID	Уникальный идентификатор сети
Channel	Канал, который использует данная Wi-Fi сеть
RSSI	Мощность передатчика в dbm
Security	Способ шифрования, передаваемой информации
MAC Address	MAC адрес точки доступа данной сети Wi-Fi
Max Rate	Максимальная скорость работы устройства на физическом уровне (максимальная теоретическая скорость)
Vendor	Производитель точки доступа

Программа Jperf, которая представляет собой графическую оболочку для консольной программы для измерения пропускной способности канала связи. С помощью программы можно замерить пропускную способность канала между двумя компьютерами в локальной сети, работает в режиме клиент-сервер.

Измерение пропускной способности экспериментальной сети беспроводного доступа Wi-Fi

Структура исследуемой сети

1) ASUS WL500 g.p. v2 (AP – *Access Point*) Мульти-функциональный беспроводной маршрутизатор фирмы ASUS, поддерживающий стандарты : IEEE 802.11b/g.

2) WS1 – WS3(WS – *work station*) – однородные рабочие станции представленные мобильными компьютерами с сетевыми Wi-Fiадаптерами фирмы Atheros поддерживающими стандарты : IEEE 802.11b/g. Третий компьютер используется для обеспечения конкуренции, он всегда посылает данные либо первому либо второму компьютеру.

Для того чтобы настроить сеть нужно выбрать ее архитектуру. Для установления связи между рабочими станциями (WS) стандарт 802.11 предусматривает 2 способа организации сети: по принципу «равный с равным» (рис. 2а) и виде структурированной сети [1] (рис. 2 б).

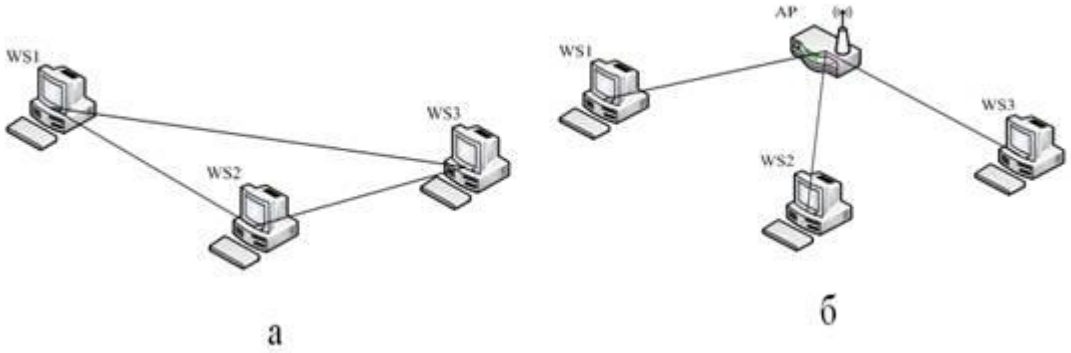


Рис. 2 Архитектуры сети: (а) - прямого беспроводного доступа, (б) - с использованием точки доступа

Связь между устройствами происходит только через AP. Далее выбирается именно такой способ организации сети для того, чтобы обеспечить данной ЛВС выход во внешние проводные сети. Также с помощью нескольких AP, объединенных проводной сетью Ethernet, можно увеличить зону покрытия сети. [1] Пример использования данной архитектура сети для увеличения зоны покрытия сети представлен на рис.3.

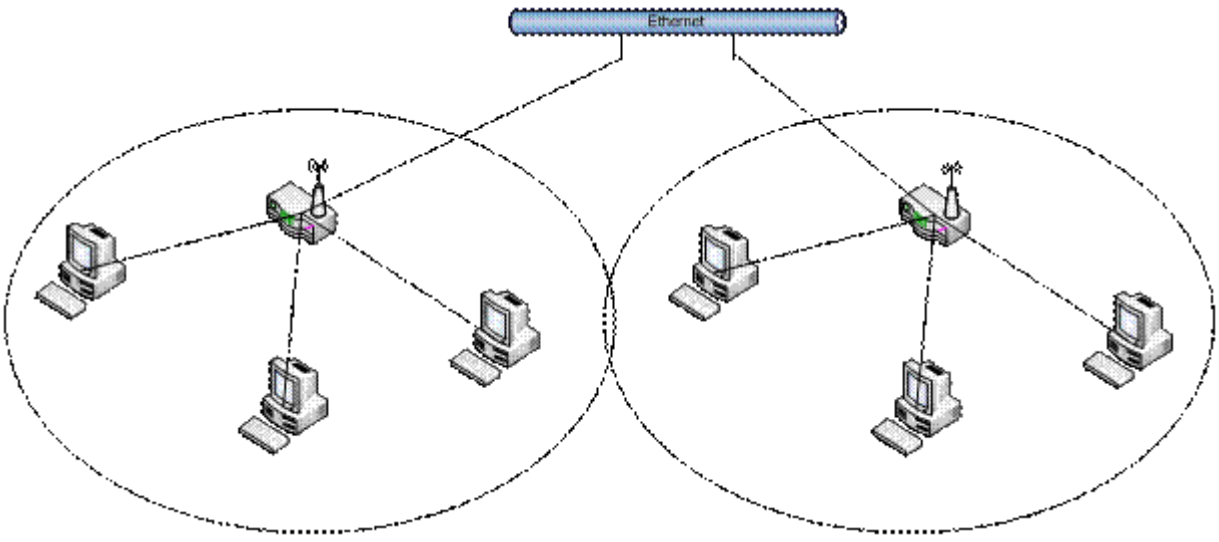


Рис. 3. Архитектура сети для увеличения зоны покрытия сети

Настройка исследуемой сети

Настройка основных характеристик Wi-Fi для работы роутера:

Поле **SSID** – название беспроводной WiFi сети.

Поле **Channel** - выбор канала для беспроводной Wi-Fi связи.

Поле **Wireless mode** — определяет поддержку различных стандартов Wi-Fi связи.

Далее расположены настройки безопасности беспроводной сети(Тестирование безопасности в данной работе не рассматривалось):

В поле **Authentication Method** регулируется выбор типа шифрования в сети Wi-Fi. С учетом уязвимости WEP протокола, мы рекомендуется использовать в своей сети исключительно **WPA/WPA2** шифрование. Поэтому останавливаем свой выбор на варианте **WPA.**

В поле **WPA Encryption** мы назначаем алгоритм шифрования в беспроводной сети: **TKIP**.

В поле **WPA Pre-Shared Key** необходимо указать ключ шифрования (пароль) беспроводной сети. Он должен быть длиной не менее 8 символов.

Таким образом была проведена базовая настройка сети. Но такая настройка не является эфективной т.к.:

- Не рекомендается использовать канал авто, канал выбираемый автоматически, обычно 1, может быть занят другими «соседними» сетями, что скажется на качестве соединения
- Выбрав канал, нужно задать мощность передатчика, достаточную для обеспечения нужного качества соединения.
- Производитель чипсетов для сетевого оборудования предусматривают различные технологие, повышаюшие пропускную способность сети, следует по возможности использовать их.
- Для настройки клиентских станций требуется настроить подключение к сети, охватываемой роутером.
- Для настройки предельной производительности исследуемой сети Wi-Fi необходимо выполнить:

- Выбор частотного канала работы точки доступа.
- Настроить мощность передатчика Wi-Fi.
- Выбор стандарта беспроводной локальной вычислительной сети
- Использовать технологии AfterBurner, Frame Bursting,
- Выбор интервала сигнального фрейма
- Выбор интервала DTIM

Выбор частотного канала работы точки доступа

В основе стандарта 802.11 для метода передачи на физическом уровне используется технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне частот 2,4 ГГц. Технологии расширения спектра используют метод модуляции, при котором для передачи информации используется сигнал, спектр которого намного шире того, который необходим для передачи информации, и передастся она с намного меньшей скоростью. Каждый бит заменяется или расширяется кодом, расширяющим полосу частот. Во многом благодаря кодированию (поскольку информация заменяется намного большим числом информационных битов) эта технология позволяет передавать информацию при малом соотношении сигнал/шум, обусловленным или помехами, или недостаточной мощностью передатчика. При использовании DSSS переданный сигнал, по сути, усиливается за счет применения расширяющей последовательности, совместно используемой передатчиком и приемником [4].

Исходя из этой технологии, имеем следующую схему организации каналов: полоса частот 22 МГц, 11 каналов, 3 неперекрывающихся, диапазон частот 2,4 ГГц.

С помощью утилиты INSSIDER определим наименее загруженный канал и перенастроим точку доступа на него для снижения помех, создаваемых точками доступа «соседних» сетей. На рис.4. первый SSID (идентификатор сети) принадлежит нашей точки доступа, сеть работает на первом канале (на первом канале больше всего сетей, часто этот канал является установкой по умолчанию). Для того чтобы сигналы не накладывались, стоит перенести сеть на 5 канал, т.к. независимые каналы 1, 5, 11, но занят 13 и он заходит на 11 канал.

SSID	Channel	RSSI	Security	MAC Address	Max Rate	Vendor
	1	**-41**	**WPA2-Personal**	**E0:CB:4E:ED:25:B7**	**54**	
ZyXEL-4256	1	-74	WEP	00:23:F8:5B:CD:1E	54	
WiFi Heaven2	1	-95	WPA2-Personal	BC:AE:C5:C4:7A:7D	144	
corbina	1	-89	WPA-Personal	00:1C:F0:CD:5F:F5	54	
Banzay	1	-94	WPA2-Personal	C8:6C:87:3F:29:53	150	
Stream	11	-93	WPA2-Personal	00:23:54:8D:4D:4B	54	
nonAME	13	-73	WPA2-Personal	00:14:D1:A9:C2:6A	54	
Beeline_router	9	-95	WPA2-Personal	00:14:D1:66:A3:64	54	TRENDnet
RT-G32	10	-91	WPA2-Personal	F4:6D:04:DF:DB:AC	54	ASUSTek COMPUTER INC.
MGTS_652933	6	-92	WPA-Personal	C8:64:C7:01:A4:98	54	zte corporation
GosdepUSA	1	-93	WPA2-Personal	F8:C0:91:13:20:9C	300	Highgates Technology
SSID	6	-92	WPA2-Personal	00:1E:58:C0:2D:19	54	D-Link Corporation
95d534	11	-89	WPA-Personal	70:71:BC:2C:74:E5	54	PEGATRON CORPORATION
blondin	11	-91	WPA2-Personal	10:BF:48:E6:1E:B2	144	
FON_MTS	6	-91	Open	C8:64:C7:01:A4:99	54	zte corporation
ROUTER	1 + 5	-92	WPA2-Personal	00:14:D1:C4:B9:70	300	TRENDnet
Onlime27	1	-94	WPA2-Personal	00:14:D1:B9:50:D3	54	TRENDnet

Рис. 4. Просмотр сетей для БЛВС с помощью утилиты INSSIDER

Мощность передатчика Wi-Fi

Для обеспечения скорости передачи данных 11 Мбит/с минимальная мощность передатчика AP со стороны приемной станции должна составлять -76 dBm (максимальная мощность передатчика составляет -30 dBm), а отношение мощности от соседнего канала передатчика другой станции должно быть не менее 35 dBm.[4]

Мощность передатчика SSID (W_{SSID}) составляет -93 dBm, мощность передатчика нашей станции (W) составляет -44 dBm:

$$\Delta = W - W_{SSID} = 93 - 44 = 49 \text{ dBm} > 35 \text{ dBm};$$

Значение мощности передатчика AP находится на приемлемом уровне.

Выбор стандарта беспроводной локальной вычислительной сети

Основное назначение физических уровней стандарта 802.11 — обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Подготавливая эти механизмы передачи независимо от подуровня MAC, стандарт 802.11 усовершенствовал как подуровень MAC, так и подуровень PHY (физический), а также поддерживаемый последним интерфейс. Именно независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.11b и 802.11g [4].

Каждый из физических уровней стандарта 802.11 имеет два подуровня.

Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.

Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

Подуровень PLCP по существу является уровнем обеспечения взаимодействия (handshaking layer), на котором осуществляется перемещение элементов данных протокола MAC (MAC protocol data units, MPDU) между MAC-станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную среду. Можно считать, что PMD выполняет функцию службы беспроводной передачи; взаимодействие этих служб осуществляется посредством PLCP. Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11 [4].

Стандарт 802.11b регламентирует правила использования высокоскоростной технологии DSSS (HR-DSSS), обеспечивающей скорость передачи в локальных беспроводных сетях диапазона 2,4 ГГц до 5,5 и 11 Мбит/с. При этом используется кодирование с использованием комплементарных кодов (complementary code keying, CCK) или технология двоичного пакетного сверточного кодирования (packet binaryconvolutional coding, PBCC). В технологии HR-DSSS используется та же схема организации каналов, что и в технологии DSSS, — полоса частот шириной 22 МГц, 11 каналов, 3 неперекрывающихся, диапазон 2,4 ГГц [4].

Рассмотрим подуровень PLCP технологии DSSS стандарта 802.11, добавляется два поля во фрейм MAC, чтобы сформировать PPDU (PHY Protocol Data Unit - Поле данных физического уровня): преамбулу PLCP и заголовок PLCP.

По полученным характеристикам, представленным на рис 5, можно сделать вывод, что использование стандарта 802.11.b или стандарта 802.11.g с поддержкой 802.11.b является далеко не лучшим вариантом для данной сети, т. к. все устройства поддерживают стандарт 802.11.g, а по временным характеристикам он наиболее выгоден.

В дальнейшем точка доступа будет работать только с устройствами стандарта 802.11g и будут исследоваться поведение производительности различными методами для стандарта 802.11g.

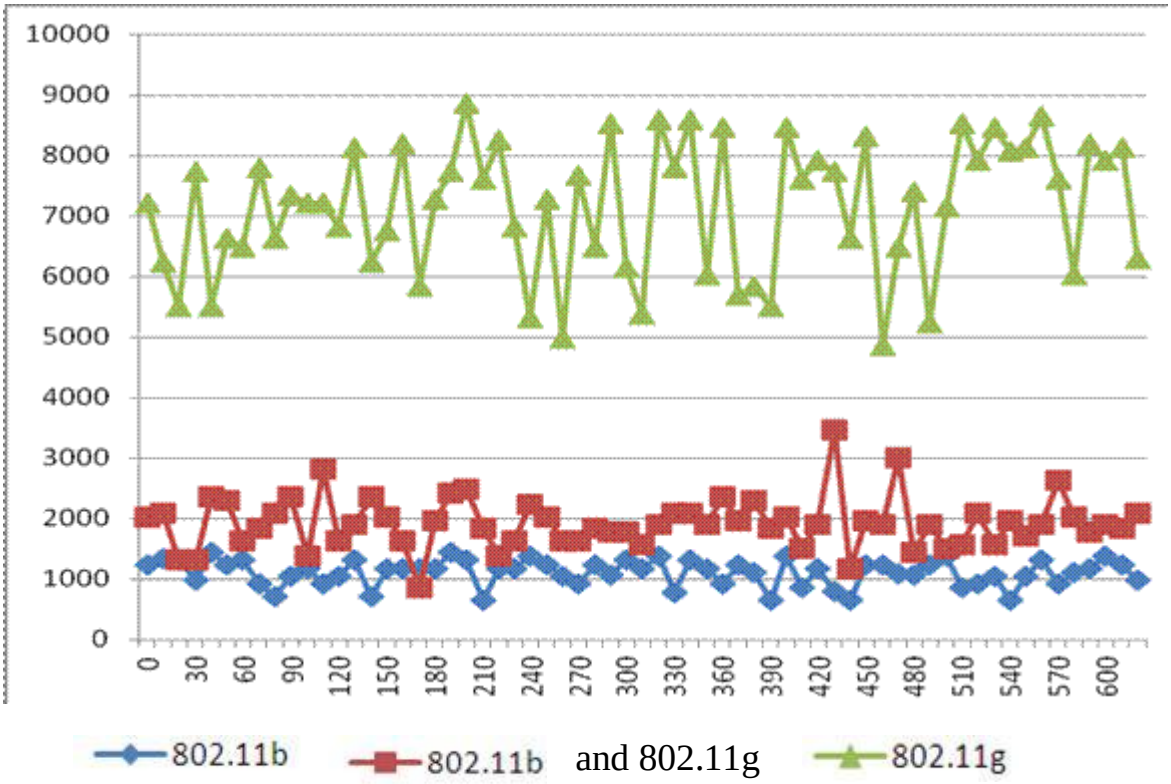


Рис.5. График зависимости производительности от используемого стандарта связи

Анализ результатов исследований

На рис. 6 изображена зависимости пропускной способности сети с базовой настройкой и с расширенной.

Математическое ожидание и среднеквадратическое отклонение для базовой настройки:

$M_{\text{базовая}} = 5012\ \ Kbits/s;$

$\sigma_{\text{базовая}} = 890\ Kbits/s;$

Математическое ожидание и среднеквадратическое отклонение для расширенной настройки:

$M_{\text{расширенная}} = 7972\ \ Kbits/s;$

$\sigma_{\text{расширенная}} = 536\ Kbits/s;$

В среднем выигрыш в производительности составил 59 %. Наибольшее значение в повышении производительности обеспечивала технология Frame Bursting. Также на производительности повлияло, что все устройства поддерживают стандарт 802.11g, иначе повышениепроизводительности было бы меньше. (рис. 6).

Рис. 6. Зависимость производительности от времени при базовой и расширенной настройках

Была произведена «тонкая» настройка локальной Wi-Fi сети. С помощью данной настройки удалось добиться повышения производительности на 59 %. Это свидетельствует о том, что базовая настройка не является эффективной. Для повышения производительности нужно выбрать стандарт используемой связи, оборудование, которое будет поддерживать данный стандарт. Также были использованы различные технологии, для увеличения пропускной способности.

Технология Afterburner не дала существенного выигрыша производительности, при ее использовании часто возникали коллизии, что еще больше снижает производительность.

Зато с использованием технологии Frame Bursting при обоснованной настройке ее параметров был получен существенный прирост производительности.

Технология Wi-Fi достаточна перспективная, важно правильно подбирать параметры БЛВС для достижения максимальной производительности, которая сможет конкурировать с производительностью проводных сетей.

Практическая работа № 6,7

Тема: Диагностика неисправностей в пассивном оборудовании. Предложения по ремонту. Диагностика неисправностей в активном оборудовании. Предложения по ремонту.

Основных причин неудовлетворительной работы прикладного ПО в сети может быть несколько: повреждения кабельной системы, дефекты активного оборудования, перегруженность сетевых ресурсов (канала связи и сервера), ошибки самого прикладного ПО. Часто одни дефекты сети маскируют другие. Таким образом, чтобы достоверно определить, в чем причина неудовлетворительной работы прикладного ПО, локальную сеть требуется подвергнуть комплексной диагностике. Комплексная диагностика предполагает выполнение следующих работ (этапов).

- Выявление дефектов физического уровня сети: кабельной системы, системы электропитания активного оборудования; наличия шума от внешних источников.

- Измерение текущей загруженности канала связи сети и определение влияния величины загрузки канала связи на время реакции прикладного ПО.
- Измерение числа коллизий в сети и выяснение причин их возникновения.
- Измерение числа ошибок передачи данных на уровне канала связи и выяснение причин их возникновения.
- Выявление дефектов архитектуры сети.
- Измерение текущей загруженности сервера и определение влияния степени его загрузки на время реакции прикладного ПО.
- Выявление дефектов прикладного ПО, следствием которых является неэффективное использование пропускной способности сервера и сети.

В рамках данной статьи мы рассмотрим первые четыре этапа комплексной диагностики локальной сети, а именно: диагностику канального уровня сети.

Мы не будем подробно описывать методику тестирования кабельной системы сети. Несмотря на важность этой проблемы, ее решение тривиально и однозначно: полноценно кабельная система может быть протестирована только специальным прибором - кабельным сканером. Другого способа не существует. Нет смысла заниматься трудоемкой процедурой выявления дефектов сети, если их можно локализовать одним нажатием клавиши AUTOTEST на кабельном сканере. При этом прибор выполнит полный комплекс тестов на соответствие кабельной системы сети выбранному стандарту.

Хотелось бы обратить ваше внимание на два момента, тем более что о них часто забывают при тестировании кабельной системы сети с помощью сканера.

Режим AUTOTEST не позволяет проверить уровень шума создаваемого внешним источником в кабеле. Это может быть шум от люминесцентной лампы, силовой электропроводки, сотового телефона, мощного копировального аппарата и др. Для определения уровня шума кабельные сканеры имеют, как правило, специальную функцию. Поскольку кабельная система сети полностью проверяется только на этапе ее инсталляции, а шум в кабеле может возникать непредсказуемо, нет полной гарантии того, что шум проявится именно в период полномасштабной проверки сети на этапе ее инсталляции.

При проверке сети кабельным сканером вместо активного оборудования к кабелю подключаются с одного конца - сканер, с другого - инжектор. После проверки кабеля сканер и инжектор отключаются, и подключается активное оборудование: сетевые платы, концентраторы, коммутаторы. При этом нет полной гарантии того, что контакт между активным оборудованием и кабелем будет столь же хорош, как между оборудованием сканера и кабелем. Мы неоднократно встречались со случаями, когда незначительный дефект

вилки RJ-45 не проявлялся при тестировании кабельной системы сканером, но обнаруживался при диагностике сети анализатором протоколов.

В рамках предлагаемой методики мы не будем рассматривать ставшую хрестоматийной методику упреждающей диагностики сети (см. врезку "Методика упреждающей диагностики сети"). Не подвергая сомнению важность упреждающей диагностики, заметим только, что на практике она используется редко. Чаще всего (хоть это и неправильно) сеть анализируется только в периоды ее неудовлетворительной работы. В таких случаях локализовать и исправить имеющиеся дефекты сети требуется быстро. Предлагаемую нами методику следует рассматривать как частный случай методики упреждающей диагностики сети.

Организация процесса диагностики сети

Любая методика тестирования сети существенно зависит от имеющихся в распоряжении системного администратора средств. По нашему мнению, в большинстве случаев необходимым и достаточным средством для обнаружения дефектов сети (кроме кабельного сканера) является анализатор сетевых протоколов. Он должен подключаться к тому домену сети (collision domain), где наблюдаются сбои, в максимальной близости к наиболее подозрительным станциям или серверу (см. Правило #3.3).

Если сеть имеет архитектуру с компактной магистралью (collapsed backbone) и в качестве магистрали используется коммутатор, то анализатор необходимо подключать к тем портам коммутатора, через которые проходит анализируемый трафик. Некоторые программы имеют специальные агенты или зонды (probes), устанавливаемые на компьютерах, подключенных к удаленным портам коммутатора. Обычно агенты (не путать с агентами SNMP) представляют собой сервис или задачу, работающую в фоновом режиме на компьютере пользователя. Как правило, агенты потребляют мало вычислительных ресурсов и не мешают работе пользователей, на компьютерах которых они установлены. Анализаторы и агенты могут быть подключены к коммутатору двумя способами.

При первом способе (см. Рисунок 1а) анализатор подключается к специальному порту (порту мониторинга или зеркальному порту) коммутатора, если таковой имеется, и на него по очереди направляется трафик со всех интересующих портов коммутатора.

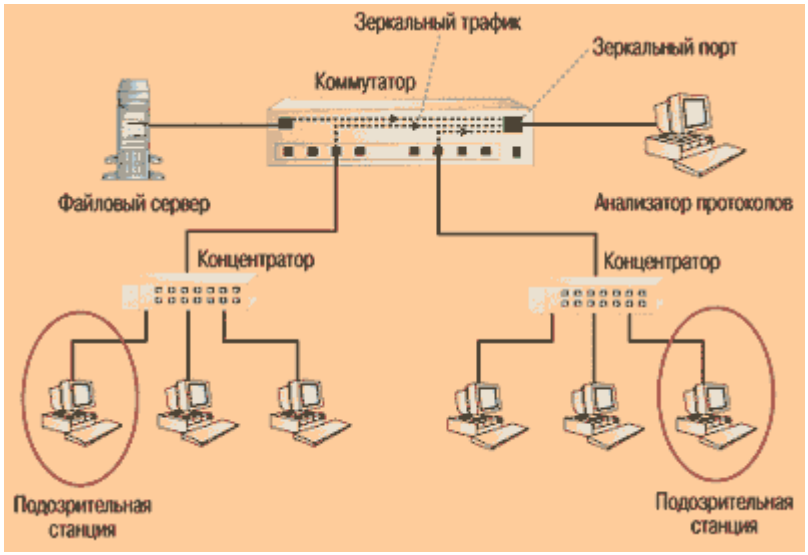


Рисунок 1а. Зеркальный трафик со всех портов коммутатора по очереди направляется на порт коммутатора, к которому подключен анализатор протоколов.

Если в коммутаторе специальный порт отсутствует, то анализатор (или агент) следует подключать к портам интересующих доменов сети в максимальной близости к наиболее подозрительным станциям или серверу (см. Рисунок 1б). Иногда это может потребовать использования дополнительного концентратора. Согласно Правилу #3.3, данный способ предпочтительнее первого. Исключение составляет случай, когда один из портов коммутатора работает в полнодуплексном режиме. Если это так, то порт предварительно необходимо перевести в полудуплексный режим.

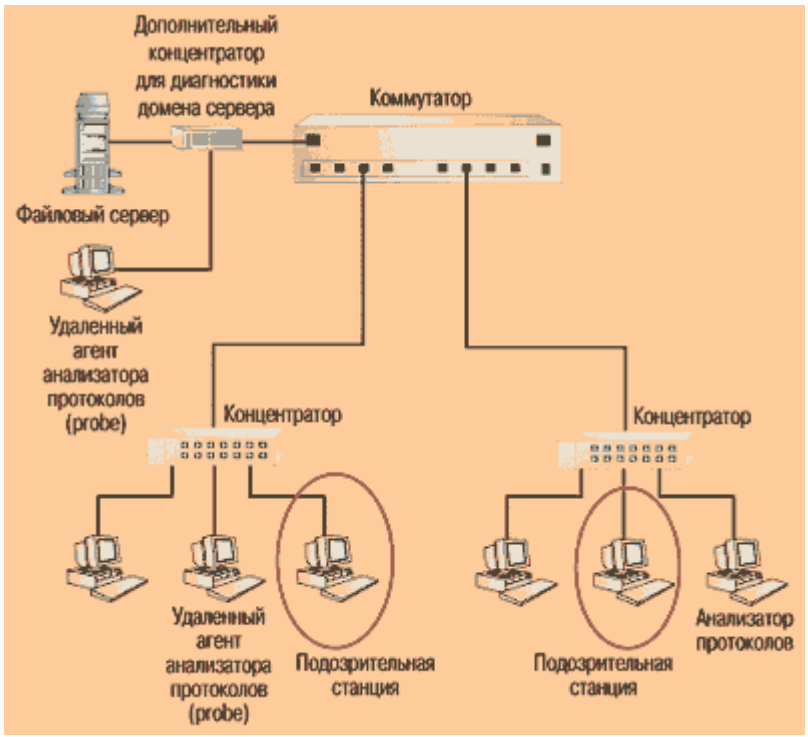


Рисунок 1б. Анализатор протоколов и удаленные агенты контролируют основные домены сети. Для диагностики домена сервера используется дополнительный концентратор.

На рынке имеется множество разнообразных анализаторов протоколов - от чисто программных до программно-аппаратных. Несмотря на функциональную идентичность большинства анализаторов протоколов, каждый из них обладает теми или иными достоинствами и недостатками. В этой связи мы хотели бы обратить внимание на две важные функции, без которых эффективную диагностику сети провести будет затруднительно.

Во-первых, анализатор протоколов должен иметь встроенную функцию генерации трафика (см. Правило #3.4). Во-вторых, анализатор протоколов должен уметь "прореживать" принимаемые кадры, т. е. принимать не все кадры подряд, а, например, каждый пятый или каждый десятый с обязательной последующей аппроксимацией полученных результатов. Если эта функция отсутствует, то при сильной загруженности сети, какой бы производительностью ни обладал компьютер, на котором установлен анализатор, последний будет "зависать" и/или терять кадры. Это особенно важно при диагностике быстрых сетей типа Fast Ethernet и FDDI.

Предлагаемую методику мы будем иллюстрировать на примере использования чисто программного анализатора протоколов Observer компании Network Instruments, работающего в среде Windows 95 и Windows NT. С нашей точки зрения, этот продукт обладает всеми необходимыми функциями для эффективного проведения диагностики сетей.

Итак, предположим, что прикладное программное обеспечение в вашей сети Ethernet стало работать медленно, и вам необходимо оперативно локализовать и ликвидировать дефект.

Первый этап

Измерение утилизации сети и установление корреляции между замедлением работы сети и перегрузкой канала связи.

Утилизация канала связи сети - это процент времени, в течение которого канал связи передает сигналы, или иначе - доля пропускной способности канала связи, занимаемой кадрами, коллизиями и помехами. Параметр "Утилизация канала связи" характеризует величину загруженности сети.

Канал связи сети является общим сетевым ресурсом, поэтому его загруженность влияет на время реакции прикладного программного обеспечения. Первоочередная задача состоит в определении наличия взаимозависимости между плохой работой прикладного программного обеспечения и утилизацией канала связи сети.

Предположим, что анализатор протоколов установлен в том домене сети (collision domain), где прикладное ПО работает медленно . Средняя

утилизация канала связи составляет 19%, пиковая доходит до 82%. Можно ли на основании этих данных сделать достоверный вывод о том, что причиной медленной работы программ в сети является перегруженность канала связи? Вряд ли.

Часто можно слышать о стандарте де-факто, в соответствии с которым для удовлетворительной работы сети Ethernet утилизация канала связи "в тренде" (усредненное значение за 15 минут) не должна превышать 20%, а "в пике" (усредненное значение за 1 минуту) - 35-40%. Приведенные значения объясняются тем, что в сети Ethernet при утилизации канала связи, превышающей 40%, существенно возрастает число коллизий и, соответственно, время реакции прикладного ПО. Несмотря на то что такие рассуждения в общем случае верны, безусловное следование подобным рекомендациям может привести к неправильному выводу о причинах медленной работы программ в сети. Они не учитывают особенности конкретной сети, а именно: тип прикладного ПО, протяженность домена сети, число одновременно работающих станций.

Чтобы определить, какова же максимально допустимая утилизация канала связи в вашем конкретном случае, мы рекомендуем следовать приведенным ниже правилам.

Правило # 1.1.

Если в сети Ethernet в любой момент времени обмен данными происходит не более чем между двумя компьютерами, то любая сколь угодно высокая утилизация сети является допустимой.

Сеть Ethernet устроена таким образом, что если два компьютера одновременно конкурируют друг с другом за захват канала связи, то через некоторое время они синхронизируются друг с другом и начинают выходить в канал связи строго по очереди. В таком случае коллизий между ними практически не возникает.

Если рабочая станция и сервер обладают высокой производительностью, и между ними идет обмен большими порциями данных, то утилизация в канале связи может достигать 80-90% (особенно в пакетном режиме - burst mode). Это абсолютно не замедляет работу сети, а, наоборот, свидетельствует об эффективном использовании ее ресурсов прикладным ПО.

Таким образом, если в вашей сети утилизация канала связи высока, постарайтесь определить, сколько компьютеров одновременно ведут обмен данными. Это можно сделать, например, собрав и декодировав пакеты в интересующем канале в период его высокой утилизации.

Правило # 1.2.

Высокая утилизация канала связи сети только в том случае замедляет работу конкретного прикладного ПО, когда именно канал связи является "узким местом" для работы данного конкретного ПО.

Кроме канала связи узкие места в системе могут возникнуть из-за недостаточной производительности или неправильных параметров настройки сервера, низкой производительности рабочих станций, неэффективных алгоритмов работы самого прикладного ПО.

В какой мере канал связи ответственнен за недостаточную производительность системы, можно выяснить следующим образом. Выбрав наиболее массовую операцию данного прикладного ПО (например, для банковского ПО такой операцией может быть ввод платежного поручения), вам следует определить, как утилизация канала связи влияет на время выполнения такой операции.

Проще всего это сделать, воспользовавшись функцией генерации трафика, имеющейся в ряде анализаторов протоколов (например, в Observer). С помощью этой функции интенсивность генерируемой нагрузки следует наращивать постепенно, и на ее фоне производить измерения времени выполнения операции. Фоновую нагрузку целесообразно увеличивать от 0 до 50-60% с шагом не более 10%.

Если время выполнения операции в широком интервале фоновых нагрузок не будет существенно изменяться, то узким местом системы является не канал связи. Если же время выполнения операции будет существенно меняться в зависимости от величины фоновой нагрузки (например, при 10% и 20% утилизации канала связи время выполнения операции будет значительно различаться), то именно канал связи, скорее всего, ответственнен за низкую производительность системы, и величина его загруженности критична для времени реакции прикладного ПО. Зная желаемое время реакции ПО, вы легко сможете определить, какой утилизации канала связи соответствует желаемое время реакции прикладного ПО.

В данном эксперименте фоновую нагрузку не следует задавать более 60-70%. Даже если канал связи не является узким местом, при таких нагрузках время выполнения операций может возрасти вследствие уменьшения эффективной пропускной способности сети.

Правило # 1.3.

Максимально допустимая утилизация канала связи зависит от протяженности сети.

При увеличении протяженности домена сети допустимая утилизация уменьшается. Чем больше протяженность домена сети, тем позже будут обнаруживаться коллизии. Если протяженность домена сети мала, то

коллизии будут выявлены станциями еще в начале кадра, в момент передачи преамбулы. Если протяженность сети велика, то коллизии будут обнаружены позже - в момент передачи самого кадра. В результате накладные расходы на передачу пакета (IP или IPX) возрастают. Чем позже выявлена коллизия, тем больше величина накладных расходов и большее время тратится на передачу пакета. В результате время реакции прикладного ПО, хотя и незначительно, но увеличивается.

Выводы. Если в результате проведения диагностики сети вы определили, что причина медленной работы прикладного ПО - в перегруженности канала связи, то архитектуру сети необходимо изменить. Число станций в перегруженных доменах сети следует уменьшить, а станции, создающие наибольшую нагрузку на сеть, подключить к выделенным портам коммутатора.

Второй этап

Измерение числа коллизий в сети.

Если две станции домена сети одновременно ведут передачу данных, то в домене возникает коллизия. Коллизии бывают трех типов: местные, удаленные, поздние.

Местная коллизия (local collision) - это коллизия, фиксируемая в домене, где подключено измерительное устройство, в пределах передачи преамбулы или первых 64 байт кадра, когда источник передачи находится в домене. Алгоритмы обнаружения местной коллизии для сети на основе витой пары (10BaseT) и коаксиального кабеля (10Base2) отличны друг от друга.

В сети 10Base2 передающая кадр станция определяет, что произошла локальная коллизия по изменению уровня напряжения в канале связи (по его удвоению). Обнаружив коллизию, передающая станция посылает в канал связи серию сигналов о заторе (jam), чтобы все остальные станции домена узнали, что произошла коллизия. Результатом этой серии сигналов оказывается появление в сети коротких, неправильно оформленных кадров длиной менее 64 байт с неверной контрольной последовательностью CRC. Такие кадры называются фрагментами (collision fragment или runt).

В сети 10BaseT станция определяет, что произошла локальная коллизия, если во время передачи кадра она обнаруживает активность на приемной паре (Rx).

Удаленная коллизия (remote collision) - это коллизия, которая возникает в другом физическом сегменте сети (т. е. за повторителем). Станция узнает, что произошла удаленная коллизия, если она получает неправильно оформленный короткий кадр с неверной контрольной последовательностью CRC, и при этом уровень напряжения в канале связи остается в установленных пределах (для сетей 10Base2). Для сетей 10BaseT/100BaseT

показателем является отсутствие одновременной активности на приемной и передающей парах (Tx и Rx).

Поздняя коллизия (late collision) - это местная коллизия, которая фиксируется уже после того, как станция передала в канал связи первые 64 байт кадра. В сетях 10BaseT поздние коллизии часто фиксируются измерительными устройствами как ошибки CRC.

Если выявление локальных и удаленных коллизий, как правило, еще не свидетельствует о наличии в сети дефектов, то обнаружение поздних коллизий - это явное подтверждение наличия дефекта в домене. Чаще всего это связано с чрезмерной длиной линий связи или некачественным сетевым оборудованием.

Помимо высокого уровня утилизации канала связи коллизии в сети Ethernet могут быть вызваны дефектами кабельной системы и активного оборудования, а также наличием шумов.

Даже если канал связи не является узким местом системы, коллизии несущественно, но замедляют работу прикладного ПО. Причем основное замедление вызывается не столько самим фактом необходимости повторной передачи кадра, сколько тем, что каждый компьютер сети после возникновения коллизии должен выполнять алгоритм отката (backoff algorithm): до следующей попытки выхода в канал связи ему придется ждать случайный промежуток времени, пропорциональный числу предыдущих неудачных попыток.

В этой связи важно выяснить, какова причина коллизий - высокая утилизация сети или "скрытые" дефекты сети. Чтобы это определить, мы рекомендуем придерживаться следующих правил.

Правило # 2.1.

Не все измерительные приборы правильно определяют общее число коллизий в сети.

Практически все чисто программные анализаторы протоколов фиксируют наличие коллизии только в том случае, если они обнаруживают в сети фрагмент, т. е. результат коллизии. При этом наиболее распространенный тип коллизий - происходящие в момент передачи преамбулы кадра (т. е. до начального ограничителя кадра (SFD)) - программные измерительные средства не обнаруживают, так уж устроен набор микросхем сетевых плат Ethernet. Наиболее точно коллизии обнаруживают аппаратные измерительные приборы, например LANMeter компании Fluke.

Правило # 2.2.

Высокая утилизация канала связи не всегда сопровождается высоким уровнем коллизий.

Уровень коллизий будет низким, если в сети одновременно работает не более двух станций (см. Правило # 1.1) или если небольшое число станций одновременно ведут обмен длинными кадрами (что особенно характерно для пакетного режима). В этом случае до начала передачи кадра станции "видят" несущую в канале связи, и коллизии редки.

Правило # 2.3.

Признаком наличия дефекта в сети служит такая ситуация, когда невысокая утилизация канала (менее 30%) сопровождается высоким уровнем коллизий (более 5%).

Если кабельная система предварительно была протестирована сканером, то наиболее вероятной причиной повышенного уровня коллизий является шум в линии связи, вызванный внешним источником, или дефектная сетевая плата, неправильно реализующая алгоритм доступа к среде передачи (CSMA/CD).

Компания Network Instruments в анализаторе протоколов Observer оригинально решила задачу выявления коллизий, вызванных дефектами сети. Встроенный в программу тест провоцирует возникновение коллизий: он посылает в канал связи серию пакетов с интенсивностью 100 пакетов в секунду и анализирует число возникших коллизий. При этом совмещенный график отображает зависимость числа коллизий в сети от утилизации канала связи.

Долю коллизий в общем числе кадров имеет смысл анализировать в момент активности подозрительных (медленно работающих) станций и только в случае, когда утилизация канала связи превышает 30%. Если из трех кадров один столкнулся с коллизией, то это еще не означает, что в сети есть дефект.

В анализаторе протоколов Observer график, показанный на Рисунке 3, меняет цвет в зависимости от числа коллизий и наблюдаемой при этом утилизации канала связи.

Правило # 2.4.

При диагностике сети 10BaseT все коллизии должны фиксироваться как удаленные, если анализатор протоколов не создает трафика.

Если вы пассивно (без генерации трафика) наблюдаете за сетью 10BaseT и физический сегмент в месте подключения анализатора (измерительного прибора) исправен, то все коллизии должны фиксироваться как удаленные.

Если тем не менее вы видите именно локальные коллизии, то это может означать одно из трех: физический сегмент сети, куда подключен измерительный прибор, неисправен; порт концентратора или коммутатора, куда подключен измерительный прибор, имеет дефект, или измерительный прибор не умеет различать локальные и удаленные коллизии.

Правило # 2.5.

Коллизии в сети могут быть следствием перегруженности входных буферов коммутатора.

Следует помнить, что коммутаторы при перегруженности входных буферов эмулируют коллизии, дабы "притормозить" рабочие станции сети. Этот механизм называется "управление потоком" (flow control).

Правило # 2.6.

Причиной большого числа коллизий (и ошибок) в сети может быть неправильная организация заземления компьютеров, включенных в локальную сеть.

Если компьютеры, включенные в сеть не имеют общей точки заземления (зануления), то между корпусами компьютеров может возникать разность потенциалов. В персональных компьютерах "защитная" земля объединена с "информационной" землей. Поскольку компьютеры объединены каналом связи локальной сети, разность потенциалов между ними приводит к возникновению тока по каналу связи. Этот ток вызывает искажение информации и является причиной коллизий и ошибок в сети. Такой эффект получил название ground loop или inter ground noise.

Аналогичный эффект возникает в случае, когда сегмент коаксиального кабеля заземлен более чем в одной точке. Это часто случается, если Т-соединитель сетевой платы соприкасается с корпусом компьютера.

Обращаем ваше внимание на то, что установка источника бесперебойного питания не снимает описанных трудностей. Наиболее подробно данные проблемы и способы их решения рассматриваются в материалах компании APC (American Power Conversion) в "Руководстве по защите электропитания" (Power Protection Handbook).

При обнаружении большого числа коллизий и ошибок в сетях 10Base2 первое, что надо сделать, - проверить разность потенциалов между оплеткой коаксиального кабеля и корпусами компьютеров. Если ее величина для любого компьютера в сети составляет более одного вольта по переменному току, то в сети не все в порядке с топологией линий заземления компьютеров.

Третий этап

Измерение числа ошибок на канальном уровне сети.

В сетях Ethernet наиболее распространенными являются следующие типы ошибок.

Короткий кадр - кадр длиной менее 64 байт (после 8-байтной преамбулы) с правильной контрольной последовательностью. Наиболее вероятная причина

появления коротких кадров - неисправная сетевая плата или неправильно сконфигурированный или испорченный сетевой драйвер.

Последнее время мы наблюдаем большое число ошибок этого типа на относительно медленных компьютерах (486/SX), работающих под Windows 95 с сетевыми платами NE2000. Причина нам неизвестна.

Длинный кадр (long frame) - кадр длиннее 1518 байт. Длинный кадр может иметь правильную или неправильную контрольную последовательность. В последнем случае такие кадры обычно называют jabber. Фиксация длинных кадров с правильной контрольной последовательностью указывает чаще всего на некорректность работы сетевого драйвера; фиксация ошибок типа jabber - на неисправность активного оборудования или наличие внешних помех.

Ошибки контрольной последовательности (CRC error) - правильно оформленный кадр допустимой длины (от 64 до 1518 байт), но с неверной контрольной последовательностью (ошибка в поле CRC).

Ошибка выравнивания (alignment error) - кадр, содержащий число бит, не кратное числу байт.

Блики (ghosts) - последовательность сигналов, отличных по формату от кадров Ethernet, не содержащая разделителя (SFD) и длиной более 72 байт. Впервые данный термин был введен компанией Fluke с целью дифференциации различий между удаленными коллизиями и шумами в канале связи.

Блики являются наиболее коварной ошибкой, так как они не распознаются программными анализаторами протоколов по той же причине, что и коллизии на этапе передачи преамбулы. Выявить блики можно специальными приборами или с помощью метода стрессового тестирования сети (мы планируем рассказать об этом методе в последующих публикациях).

Рискуя навлечь на себя праведный гнев дистрибьюторов программ сетевого управления на основе SNMP, мы осмелимся тем не менее утверждать, что степень влияния ошибок канального уровня сети на время реакции прикладного ПО сильно преувеличена.

В соответствии с общепринятым стандартом де-факто число ошибок канального уровня не должно превышать 1% от общего числа переданных по сети кадров. Как показывает опыт, эта величина перекрывается только при наличии явных дефектов кабельной системы сети. При этом многие серьезные дефекты активного оборудования, вызывающие многочисленные сбои в работе сети, не проявляются на канальном уровне сети (см. Правило # 3.8).

Правило # 3.1.

Прежде чем анализировать ошибки в сети, выясните, какие типы ошибок могут быть определены сетевой платой и драйвером платы на компьютере, где работает ваш программный анализатор протоколов.

Работа любого анализатора протоколов основана на том, что сетевая плата и драйвер переводятся в режим приема всех кадров сети (promiscuous mode). В этом режиме сетевая плата принимает все проходящие по сети кадры, а не только широковещательные и адресованные непосредственно к ней, как в обычном режиме. Анализатор протоколов всю информацию о событиях в сети получает именно от драйвера сетевой платы, работающей в режиме приема всех кадров.

Не все сетевые платы и сетевые драйверы предоставляют анализатору протоколов идентичную и полную информацию об ошибках в сети. Сетевые платы 3Com вообще никакой информации об ошибках не выдают. Если вы установите анализатор протоколов на такую плату, то значения на всех счетчиках ошибок будут нулевыми.

EtherExpress Pro компании Intel сообщают только об ошибках CRC и выравнивания. Сетевые платы компании SMC предоставляют информацию только о коротких кадрах. NE2000 выдают почти полную информацию, выявляя ошибки CRC, короткие кадры, ошибки выравнивания, коллизии.

Сетевые карты D-Link (например, DFE-500TX) и Kingstone (например, KNE 100TX) сообщают полную, а при наличии специального драйвера - даже расширенную, информацию об ошибках и коллизиях в сети.

Ряд разработчиков анализаторов протоколов предлагают свои драйверы для наиболее популярных сетевых плат.

Правило # 3.2.

Обращайте внимание на "привязку" ошибок к конкретным MAC-адресам станций.

При анализе локальной сети вы, наверное, обращали внимание, что ошибки обычно "привязаны" к определенным MAC-адресам станций . Однако коллизии, произошедшие в адресной части кадра, блики, нераспознанные ситуации типа короткого кадра с нулевой длиной данных не могут быть "привязаны" к конкретным MAC-адресам.

Если в сети наблюдается много ошибок, которые не связаны с конкретными MAC-адресами, то их источником скорее всего является не активное оборудование. Вероятнее всего, такие ошибки - результат коллизий, дефектов кабельной системы сети или сильных внешних шумов. Они могут быть также вызваны низким качеством или перебоями питающего активное оборудование напряжения.

Если большинство ошибок привязаны к конкретным MAC-адресам станций, то постарайтесь выявить закономерность между местонахождением станций, передающих ошибочные кадры, расположением измерительного прибора (см. Правила # 3.3, # 3.4) и топологией сети.

Правило # 3.3.

В пределах одного домена сети (collision domain) тип и число ошибок, фиксируемых анализатором протоколов, зависят от места подключения измерительного прибора.

Другими словами, в пределах сегмента коаксиального кабеля, концентратора или стека концентраторов картина статистики по каналу может зависеть от места подключения измерительного прибора.

Многим администраторам сетей данное утверждение может показаться абсурдным, так как оно противоречит принципам семиуровневой модели OSI. Впервые столкнувшись с этим явлением, мы также не поверили результату и решили, что измерительный прибор неисправен. Мы проверяли данный феномен с разными измерительными приборами, от чисто программных до программно-аппаратных. Результат был тот же.

Одна и та же помеха может вызвать фиксацию ошибки CRC, блика, удаленной коллизии или вообще не обнаруживаться в зависимости от взаимного расположения источника помех и измерительного прибора. Одна и та же коллизия может фиксироваться как удаленная или поздняя в зависимости от взаимного расположения конфликтующих станций и измерительного прибора. Кадр, содержащий ошибку CRC на одном концентраторе стека, может быть не зафиксирован на другом концентраторе того же самого стека.

Следствием приведенного эвристического правила является тот факт, что программы сетевого мониторинга на основе протокола SNMP не всегда адекватно отражают статистику ошибок в сети. Причина этого в том, что встроенный в активное оборудование агент SNMP всегда следит за состоянием сети только из одной точки. Так, если сеть представляет собой несколько стеков "неинтеллектуальных" концентраторов, подключенных к "интеллектуальному" коммутатору, то SNMP-агент коммутатора может иногда не видеть части ошибок в стеке концентраторов.

Подтверждение приведенного правила можно найти на серверах Web компаний Fluke (www.fluke.com) и Net3 Group (www.net3group.com).

Рекомендациям по разрешению описанного феномена посвящены Правила ## 3.4 и 3.5.

Правило # 3.4.

Для выявления ошибок на канальном уровне сети измерения необходимо проводить на фоне генерации анализатором протоколов собственного трафика.

Генерация трафика позволяет обострить имеющиеся проблемы и создает условия для их проявления. Трафик должен иметь невысокую интенсивность (не более 100 кадров/с) и способствовать образованию коллизий в сети, т. е. содержать короткие (<100 байт) кадры.

При выборе анализатора протоколов или другого диагностического средства внимание следует обратить прежде всего на то, чтобы выбранный инструмент имел встроенную функцию генерации трафика задаваемой интенсивности. Эта функция имеется, в частности, в анализаторах Observer компании Network Instruments и NetXray компании Cinco (ныне Network Associates).

Правило # 3.5.

Если наблюдаемая статистика зависит от места подключения измерительного прибора, то источник ошибок, скорее всего, находится на физическом уровне данного домена сети (причина - дефекты кабельной системы или шум внешнего источника). В противном случае источник ошибок расположен на канальном уровне (или выше) или в другом, смежном, домене сети.

Правило # 3.6.

Если доля ошибок CRC в общем числе ошибок велика, то следует определить длину кадров, содержащих данный тип ошибок.

Как мы уже отмечали, ошибки CRC могут возникать в результате коллизий, дефектов кабельной системы, внешнего источника шума, неисправных трансиверов. Еще одной возможной причиной появления ошибок CRC могут быть дефектные порты концентратора или коммутатора, которые добавляют в конец кадра несколько "пустых" байтов.

При большой доле ошибок CRC в общем числе ошибок целесообразно выяснить причину их появления. Для этого ошибочные кадры из серии надо сравнить с аналогичными хорошими кадрами из той же серии. Если ошибочные кадры будут существенно короче хороших, то это, скорее всего, результаты коллизий. Если ошибочные кадры будут практически такой же длины, то причиной искажения, вероятнее всего, является внешняя помеха. Если же испорченные кадры длиннее хороших, то причина кроется, вероятнее всего, в дефектном порту концентратора или коммутатора, которые добавляют в конец кадра "пустые" байты.

Какие параметры необходимо отслеживать при диагностике сети?

Методика упреждающей диагностики сети

Методика упреждающей диагностики заключается в следующем. Администратор сети должен непрерывно или в течение длительного времени наблюдать за работой сети. Такие наблюдения желательно проводить с момента ее установки. На основании этих наблюдений администратор должен определить, во-первых, как значения наблюдаемых параметров влияют на работу пользователей сети и, во-вторых, как они изменяются в течение длительного промежутка времени: рабочего дня, недели, месяца, квартала, года и т. д.

Наблюдаемыми параметрами обычно являются:

- параметры работы канала связи сети - утилизация канала связи, число принятых и переданных каждой станцией сети кадров, число ошибок в сети, число широковещательных и многоадресных кадров и т. п.;
- параметры работы сервера - утилизация процессора сервера, число отложенных (ждущих) запросов к диску, общее число кэш-буферов, число "грязных" кэш-буферов и т. п.

Зная зависимость между временем реакции прикладного ПО и значениями наблюдаемых параметров, администратор сети должен определить максимальные значения параметров, допустимые для данной сети. Эти значения вводятся в виде порогов (thresholds) в диагностическое средство. Если в процессе эксплуатации сети значения наблюдаемых параметров превысят пороговые, то диагностическое средство проинформирует об этом событии администратора сети. Такая ситуация свидетельствует о наличии в сети проблемы.

Наблюдая достаточно долго за работой канала связи и сервера, вы можете установить тенденцию изменения значений различных параметров работы сети (утилизации ресурсов, числа ошибок и т. п.). На основании таких наблюдений администратор может сделать выводы о необходимости замены активного оборудования или изменения архитектуры сети.

Практическая работа № 8

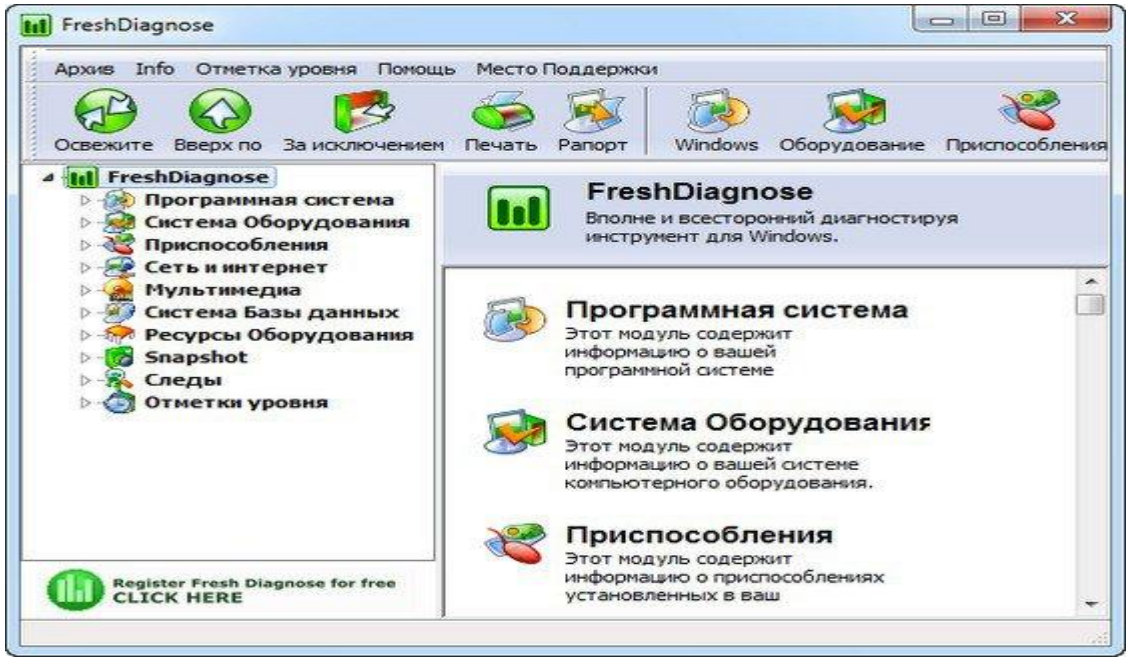
Тема: Диагностика и устранение неисправностей в ОС на компьютерах

Оборудование. ПК, ОС Windows 7.0, инструкция по выполнению лабораторной работы

Теоретическая часть

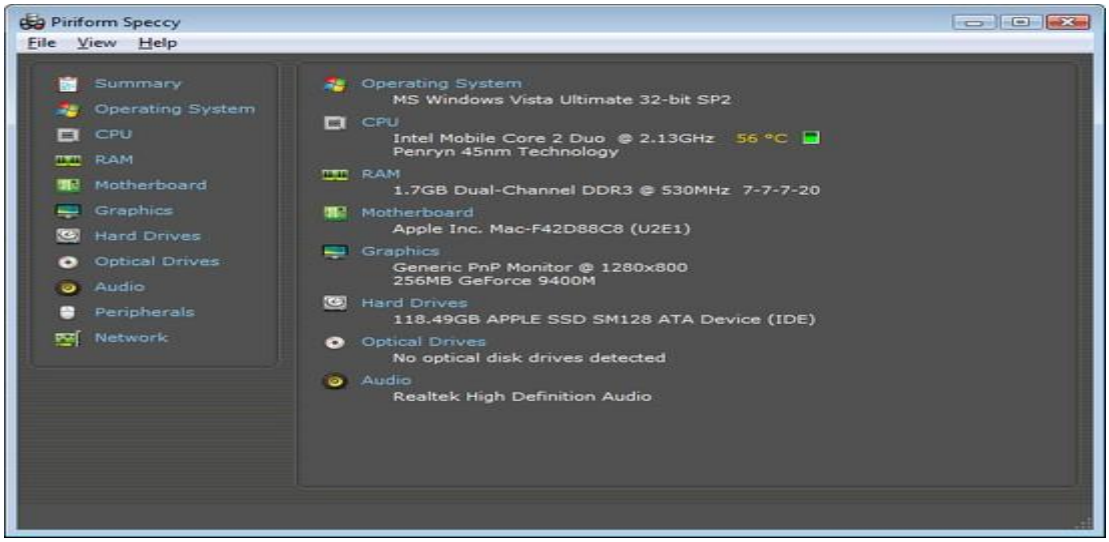
Fresh Diagnose 8.61: бесплатная диагностика

Новая версия утилиты из известного семейства бесплатных программ Fresh Devices. Предназначение Fresh Diagnose – анализ и тестирование системы. После сканирования программа выдаст полную информацию о периферийных устройствах, сети, программном обеспечении. Fresh Diagnose может тестировать практически все «железные» компоненты компьютера – процессор, винчестер, видеокарту, материнскую плату и пр. Кроме этого, Fresh Diagnose может сравнить вашу систему с другими. Программа имеет русский интерфейс.



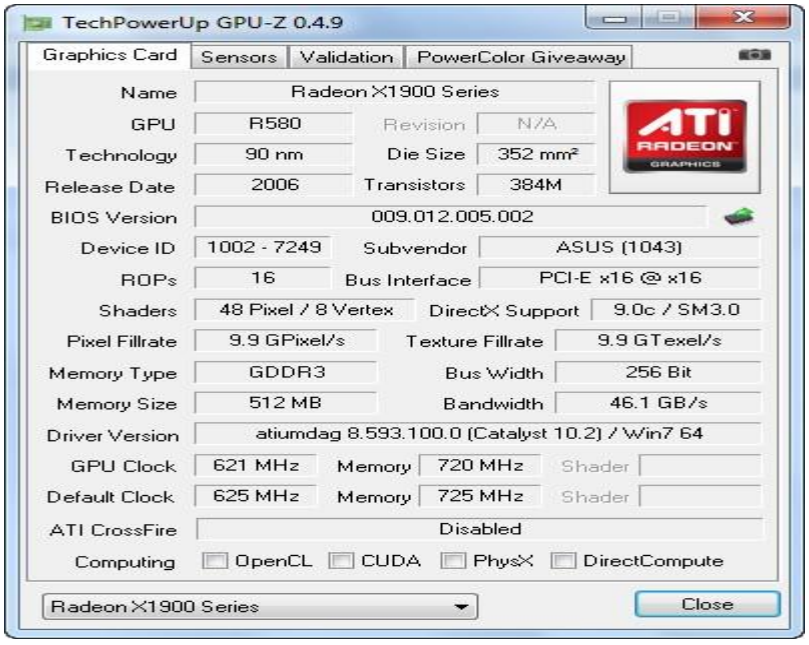
Speccy 1.15: информация о компонентах компьютера

Выпущена новая версия бесплатной программы, которая предоставляет информацию о компьютере. С ее помощью можно узнать модель процессора, размер и скорость работы жесткого диска, количество установленной оперативной памяти, получить информацию о графическом адаптере, аудиокарте, приводах для работы с оптическими дисками и об операционной системе. Программа также измеряет температуру разных компонентов ПК.



GPU-Z 0.5.8: тестирование видеокарты

Вышла новая версия программы для вывода информации о графическом адаптере. В последней версии добавлена поддержка NVIDIA Tesla C2075, GeForce GT 630M; AMD FirePro V7900, HD 6930, HD 7690M, HD 6410D; улучшен мониторинг для HD 7970, а также внесены другие улучшения.

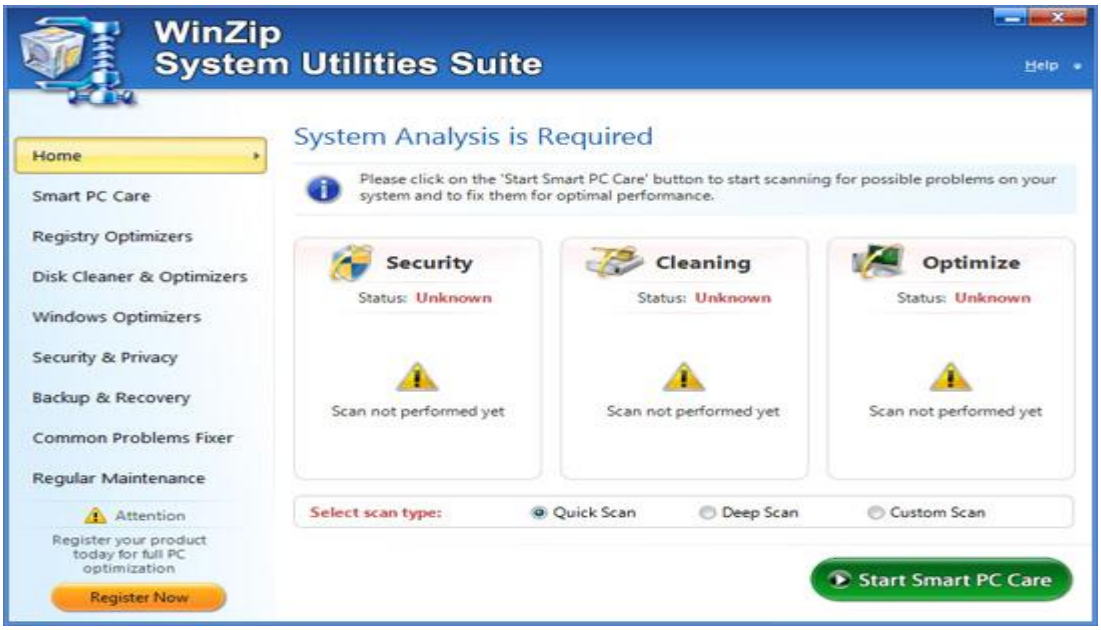


GPU-Z поддерживает и карты NVIDIA, и ATI. Она поможет определить, какая у вас модель видеокарты, узнать интерфейс подключения, расскажет о том, какой используется графический процессор (версия BIOS, номер ревизии чипа, частота в 2D, 3D-режимах и при разгоне, сведения о поддержке DirectX). Кроме этого, GPU-Z предоставляет информацию о видеопамяти, а именно ее тип, объем, разрядность шины.

WinZip System Utilities Suite

Компания WinZip Computing, являющаяся дочерним подразделением корпорации Corel, объявила о расширении портфеля программных продуктов на российском рынке и начале продаж нового комплексного решения WinZip System Utilities Suite, предназначенного для устранения распространённых проблем с программным и аппаратным обеспечением компьютера, увеличения скорости и стабильности работы системы.

Представленный инструментарий функционирует в среде Windows и включает средства обновления устаревших драйверов установленного оборудования, утилиты для оптимизации ОС, управления ресурсами памяти, проверки жёсткого диска, файловой системы и системного реестра на наличие ошибок, восстановления случайно удалённой информации, а также ряд других решений для очистки, защиты и ускорения работы ПК.

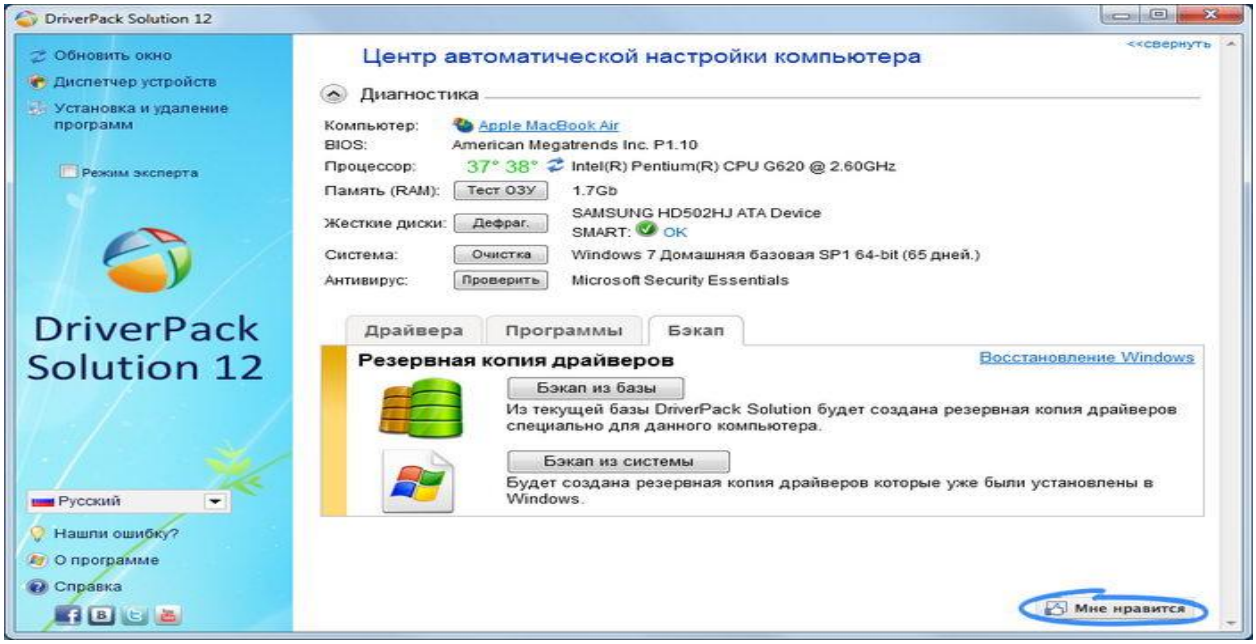


DriverPack Solution 12

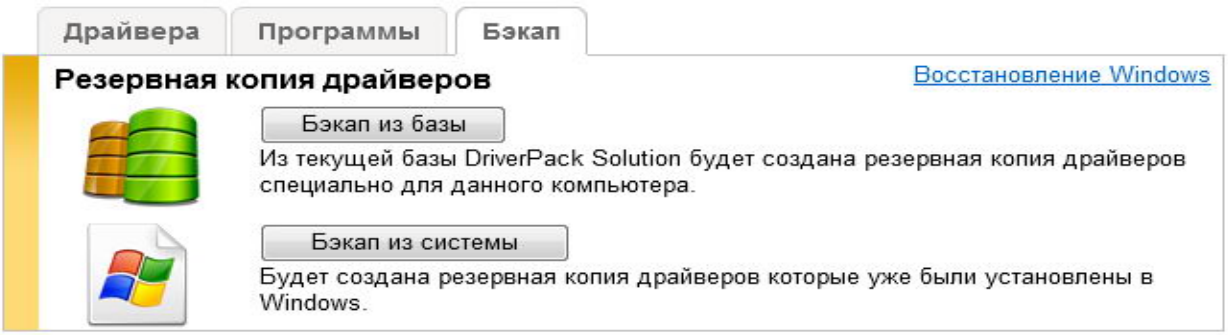
Установка драйверов зачастую доставляет системным администраторам лишние хлопоты, особенно при настройке незнакомых компьютеров, а неопытным пользователям — настоящую головную боль. Чтобы решить данную проблему, в 2008 году была выпущена первая версия программы DriverPack Solution. Как отмечают создатели, на сегодняшний день это не только программа для установки драйверов, а система автоматической настройки компьютеров. По данным разработчиков, ежемесячная посещаемость официального сайта превышает 3 млн уникальных пользователей.

Выход 12 версии программы был объявлен на февраль 2012 года, однако распространение релиза началось за два месяца до назначенного срока, что

вызвало у пользователей недоверие к свободно распространяемой через torrent-сети и файлообменные службы DriverPack Solution 12. Главный разработчик Артур Кузяков так прокомментировал данную ситуацию: «Мы всегда шли навстречу, в первую очередь, нашим постоянным пользователям. Вот и в прошлом году, когда DriverPack Solution 12 ещё только планировалась к выпуску, мы получили огромное количество просьб и пожеланий, относительно даты релиза новой версии. Я поставил задачу перед своей командой завершить 12 версию до конца ноября 2011 года. И это не бета-версия, а полноценный продукт, который уже сейчас [до официального выхода] скачали более 300 000 пользователей».



Программа автоматически находит и устанавливает последние драйверы для Windows 7, Vista и XP (32- и 64-битные версии), причём пользователь может сохранить базу используемых драйверов при помощи функции создания резервной копии, что может оказаться полезным для уменьшения рисков потери времени при переустановке операционной системы.



Среди дополнительных возможностей DriverPack Solution присутствует диагностика компьютера, которая осуществляет такие операции, как контроль температуры процессора, состояния жёсткого диска по данным

SMART, тестирование оперативной памяти и обнаружение конфликтов антивирусного ПО.

Если ваш компьютер имеет низкую производительность, то вы можете повысить скорость работы его работы и загрузки ОС, отказавшись от определенных функций и неиспользуемых служб.

1. Убрать неиспользуемые элементы автоматической загрузки Установка стандартной темы оформления для этого зайдите в меню **Пуск,** выберите **Панель управления**, **Экран**, **Персонализация**, зайдите в раздел Изменение темы, Базовые темы и там уже можно выбрать тему «Классическая».
2. Убрать прозрачность окон меню Пуск, выберите пункт, Панель управления, там найдите Оформление и персонализация, Изменение темы, выберите Цвет окна, уберите галочку возле пункта «Включить прозрачность», Сохраните сделанные изменения
3. Уберите визуальные эффекты: Перейдите в меню Пуск, Панель управления, выберите Система и безопасность, затем Система, в левой части есть пункт «Дополнительные параметры системы», там выберите пункт Быстродействие, кнопка «Параметры», Визуальные эффекты → Обеспечить оптимальное быстродействие.
4. Если вы имеете какую-нибудь неиспользуемую флэшку, воспользуйтесь ReadyBoost (это технология, которая позволяет ОС использовать доступную память флэш-накопителей и твердотельные накопители для увеличения объёма виртуальной памяти): нажмите правой кнопкой мышки на иконку необходимой флэшки, зайдите в раздел Свойства, ReadyBoost, выберите функцию Предоставлять это устройство для ReadyBoost.
5. Если ОС установлена на вашем ПК уже давно, и в течение всего этого времени она активно использовалась, есть смысл выполнить дефрагментацию жесткого диска. Перейдите в меню Пуск, выберите пункт, Все программы, перейдите в Стандартные, затем в Служебные, и там будет кнопка Дефрагментация диска
6. Выключите неиспользуемые службы: перейдите в меню Пуск, зайдите в Панель управления, выберите Система и безопасность, затем Администрирование, там будет пункт Службы, нажмите 2 раза на нужную службу, выберите Тип запуска, выберите пункт Отключить.
7. Windows Search – предназначен для поиска, индексации файлов, если вы не используете поиск, то она вам не нужна.
8. Сведения о совместимости приложений – берет сведения о совместимости софта с ОС Windows 7 и предупреждает об этом человека.
9. Служба политики диагностики – диагностирует проблемы при работе с ОС.

10. Темы – служба тем оформления, если у вас включена стандартная тема оформления, служба вам не нужна.
11. Установщик модулей – убираем автоматическую установку обновлений.
12. Брандмауэр ОС Windows – защищает от нежелательных подключений.
13. Защита ОС – поиск и защита от нежелательного и вредоносного софта.
14. Центр обеспечения безопасности – выключаем центр вместе с бесполезными предупреждениями.
15. Центр обновления ОС – с отключенными обновлениями он не нужен.

Практическая часть

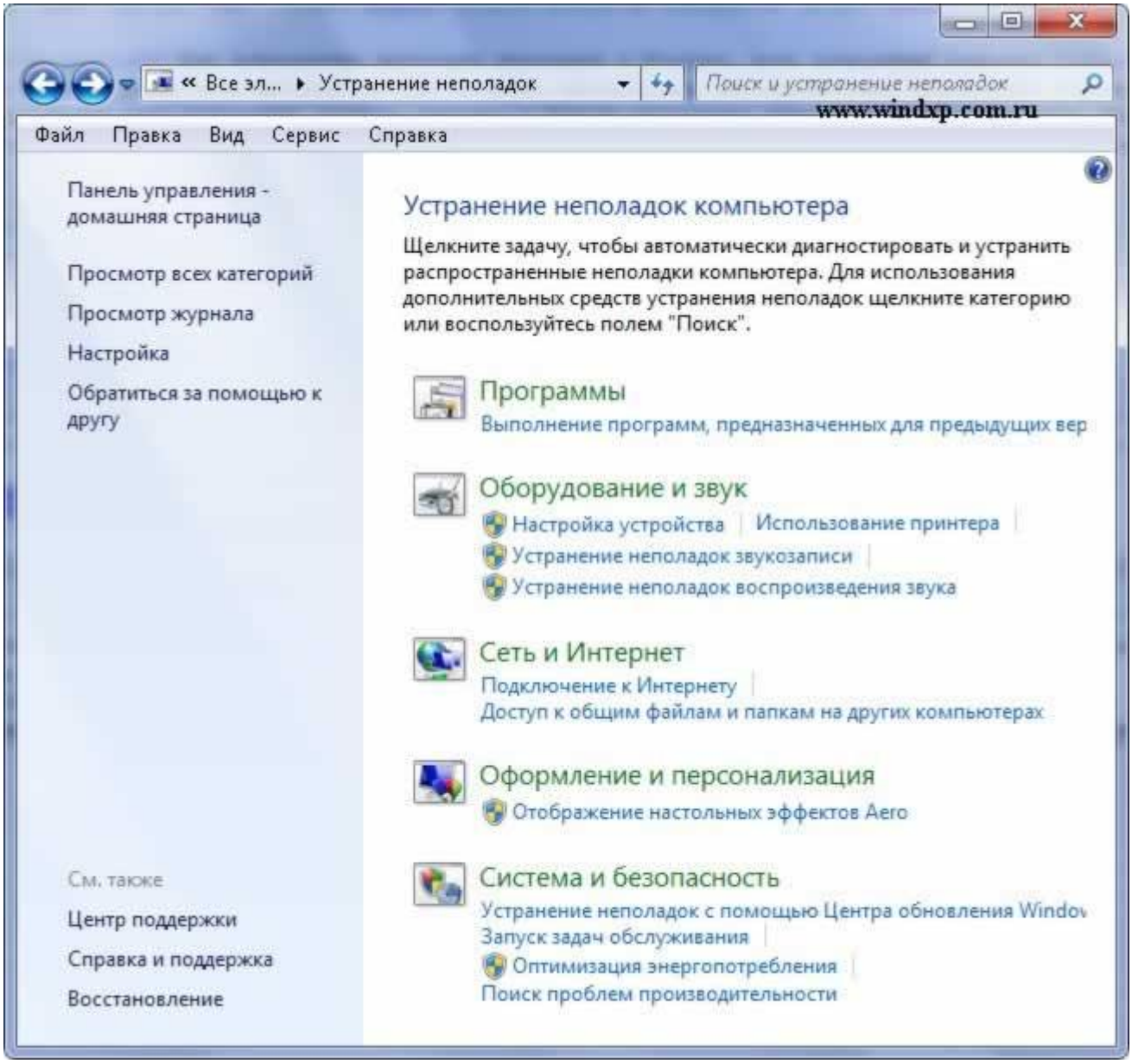
1. Определите объём оперативной памяти, занимаемый операционной системой и время загрузки
2. Выполните оптимизацию функций системы
3. Повторите тестирование вашего компьютера
4. Сделайте вывод о проделанной работе

Практическая работа № 9

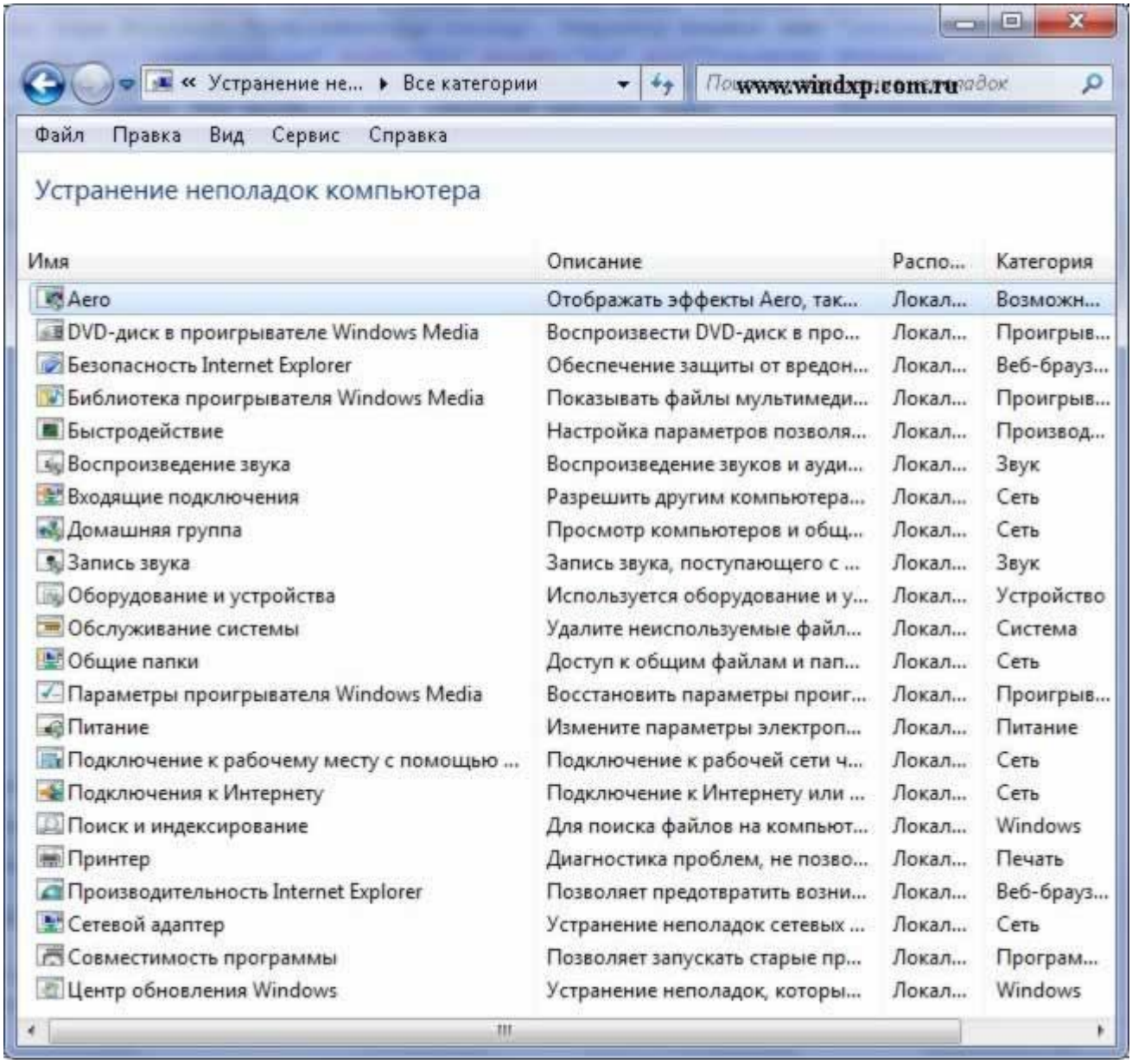
Тема: Диагностика и устранение неисправностей в ПО на компьютерах

Для исправления некоторых неполадок в Windows, есть встроенный компонент "**Устранение неполадок**". Пусть он и не решит всех проблем, но как средство диагностики для определения направления устранения неполадки, вполне подойдет. Для просмотра всех встроенных средств откройте в **Панели управления**пункт **Устранение неполадок**. Или нажмите клавиши Win+Rи введите команду:
control.exe /name Microsoft.Troubleshooting

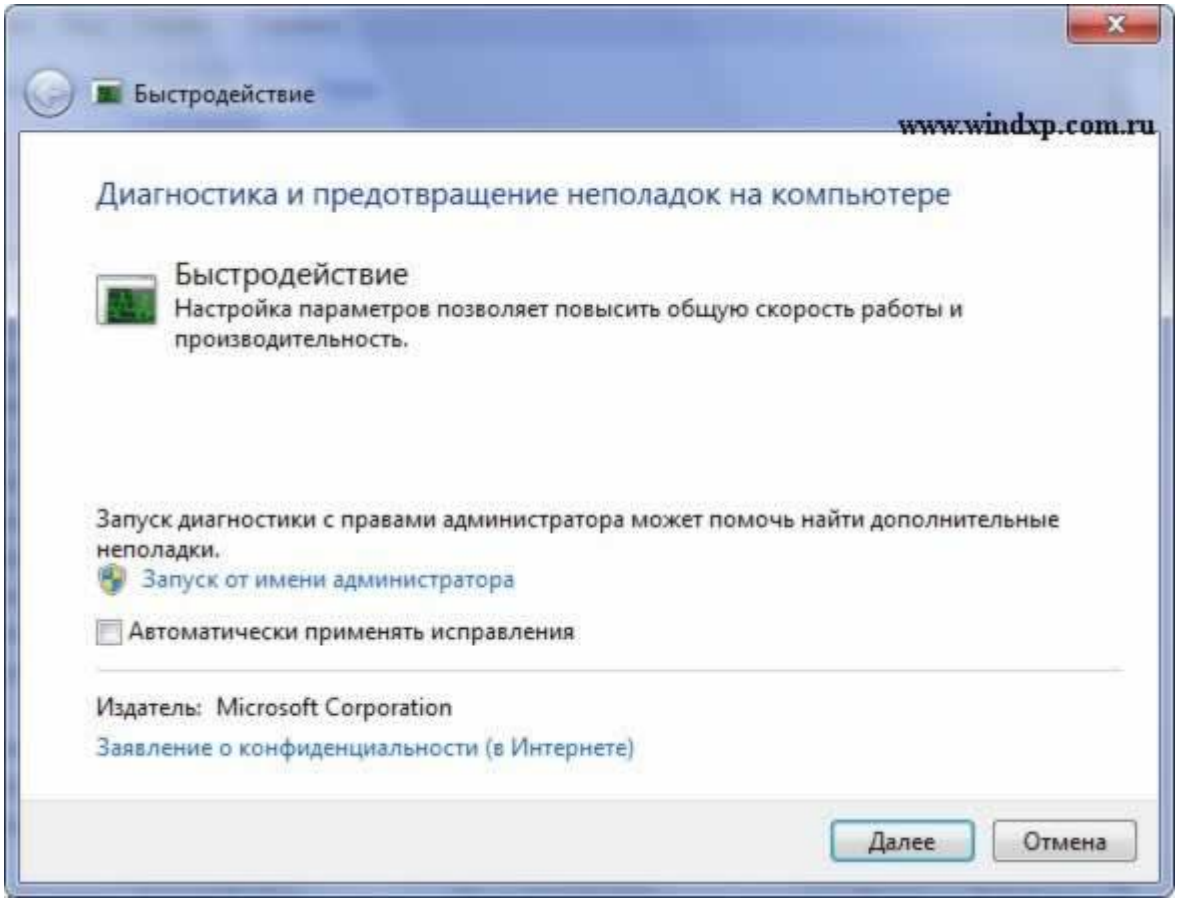
Откроется главное окно "**Устранение неполадок компьютера**"



Прежде всего проверьте во вкладке **Настройка** пункт **Обслуживание компьютера**, где необходимо, чтобы этот пункт был включен. Для просмотра всех категорий выберите пункт "**Просмотр всех категорий**"

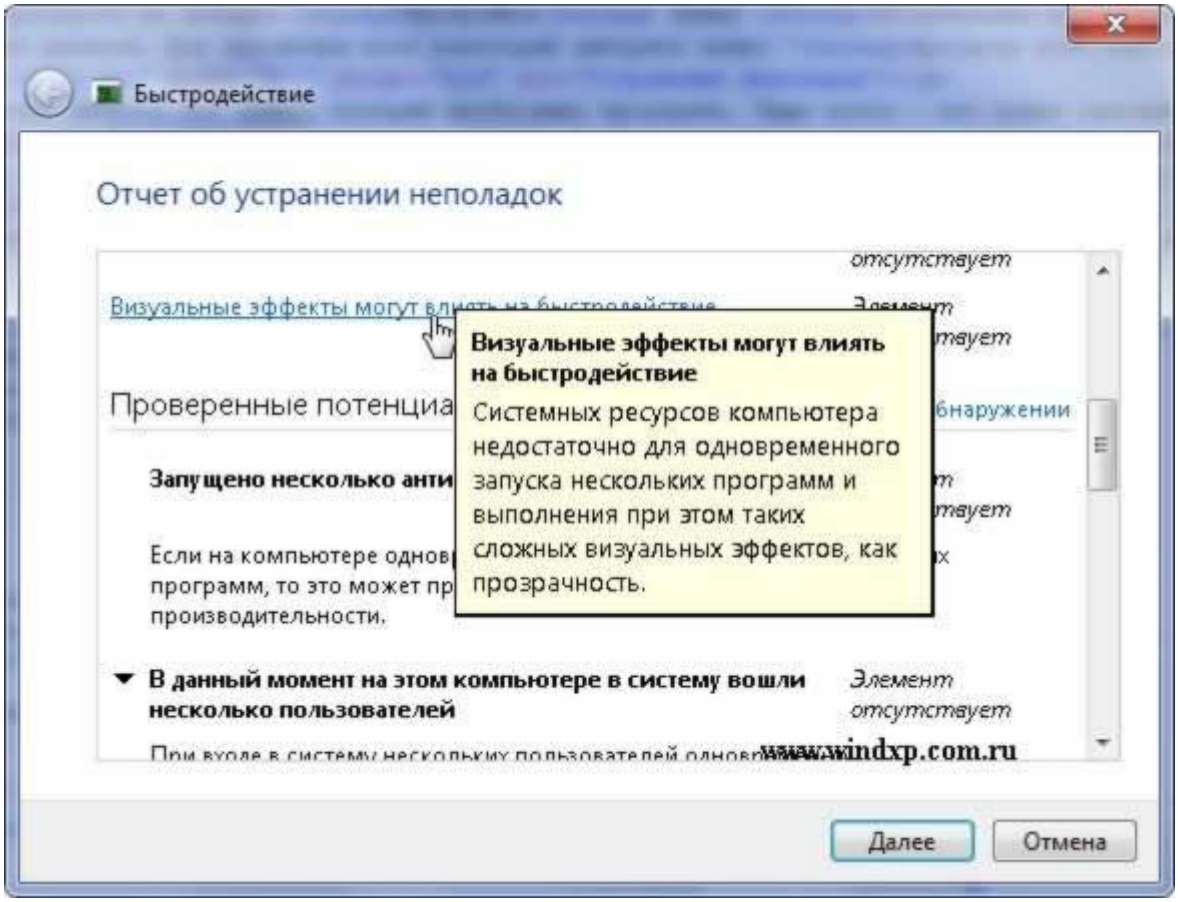


Теперь достаточно выбрать тот пункт, который необходимо проверить. Чаще всего - это пункт связанный с производительностью "Быстродействие". Если щелкнуть ссылку **Дополнительно** и снять флажок **Автоматически применять исправления**, то при обнаружении неполадки будет отображен список возможных путей ее устранения.



Примечание: При запуске средство устранения неполадок может задать несколько вопросов или сбросить часто используемые параметры. Если средству устранения неполадок удалось решить проблему, можно закрыть его. В противном случае на экране будет отображен запрос с несколькими вариантами ответа для поиска решения по устранению неполадки в Интернете. В любом случае пользователь всегда сможет просмотреть полный список внесенных изменений

Рекомендуется запускать от имени Администратора. После проверки если нет проблем, можно просмотреть и дополнительные сведения, выбрав пункт "**Просмотреть дополнительные сведения**".



Практическая работа № 10

Тема: Программные средства диагностики компьютеров

Теоретические сведения

Процесс тестирования можно разделить на отдельные части, называемые элементарными проверками. Элементарная проверка состоит в подаче на объект тестового воздействия и в измерении (оценке) ответа объекта на это воздействие. Алгоритм тестирования определяется как совокупность и последовательность элементарных проверок вместе с определенными правилами анализа результатов последних с целью отыскания места в объекте, параметры которого не отвечают заданным значениям. Таким образом, диагностика — это тоже контроль, но контроль последовательный, направленный на отыскание неисправного места (элемента) в диагностируемом объекте.

Обычно тестирование начинается по сигналу ошибки, выработанному схемами контроля ПК. Диагностическое программное обеспечение чрезвычайно необходимо в том случае, если система начинает сбоить или если осуществляется модернизация системы, добавляя новые устройства. Диагностические программы можно разделить на три уровня:

- Тестовые средства ПК (тест POST)
- Системные средства (средства ОС)
- Дополнительные программы, которые либо поставляются вместе с компьютером, либо приобретаются у его изготовителя.

Дополнительные программы можно разделить на:

о Информационные программы — Которые тестируют компьютер или отдельные компоненты, и выдают подробную информацию о его состоянии, функциональности, и возможных программных и физических неполадках.

о Тестовые программы. — Которые работают по принципу максимальной загрузки различными операциями, эмулирующими работу пользователя за компьютером, и замеряют общую производительность системы или производительность отдельных компонентов на основе сравнения, с уже имеющейся базой данных. Выполняя тестирование отдельных элементов или системы в целом.

1. **Atomic Cpu Test** – Утилита для проверки производительности вашего процессора и отдельных его составляющих (кэш-память, арифметическо-логическое устройство).
2. **CPU-Z 1.59 –** Очень полезная программа, определяющая информацию о процессоре, чипсете материнской платы и памяти.
3. **AIDA64 (EVEREST)** является мощнейшим средством для анализа начинки компьютера (железо, софт, сеть), тестирования производительности и мониторинга состояния ключевых узлов системы.
4. **RightMark Memory Analyzer 3.5** — новая версия тестового пакета с новым тестом стабильности функционирования подсистемы памяти
5. **MemTest** — утилита предназначена для тестирования надежности работы оперативной памяти. При тестировании оценивается способность памяти записывать и считывать данные. Есть возможность задавать количество мегабайт для тестирования.
6. **TestVideoRAM** предназначен для тестирования видеопамяти на картах от nVidia! Полное описание работы можно найти на страничке программы.
7. **Victoria**,– предназначенна для глубокого тестирования состояния жесткого диска.
8. **MHDD–** предназначенна для тестирования жесткого диска.
9. **System Information for Windows** — программа для предоставления детальной информации о компьютере. Показывает информацию о материнской плате, BIOS, процессоре, жестких дисках, установленных устройствах.
10. **SiSoftware SANDRA–** нформационная и диагностическая программа, которая предоставляет подробнейшую информацию об аппаратном и

программном обеспечении компьютера. В процессе работы Sandra тестирует компьютер и сравнивает полученные результаты с эталонными данными.

11. **HDDSpeed v2.3.2** – Тестирование реальной скорости жестких дисков
12. **HDDScan –** Программа предназначена для проверки носителей информации на наличие сбойных блоков, просмотра S.M.A.R.T. атрибутов, изменения специальных настроек, таких как: управление питанием, старт/стоп шпинделя, регулировка акустического режима и др.

Постановка задачи:

- 1 Знакомство с ПО или утилитой согласно варианту, дать описание описание.
- 2 Опишите основные функции работы утилиты с пояснениями и скриншотами.
- 3 Выполните проверку устройства с пояснениями и скриншотами.
- 4 Опишите принцип работы заданной утилиты с пояснениями и скриншотами.