Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
Владимирский государственный университет имени
Александра Григорьевича и Николая Григорьевича Столетовых
Кафедра управления и информатики
в технических и экономических системах

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Лабораторный практикум для студентов,
обучающихся по направлению 230700 – Прикладная информатика.
(электронный ресурс)

Составитель
В.П Галас

Владимир 2013

УДК 681.32

Сети и телекоммуникации. Лабораторный практикум для студентов, обучающихся по направлению 230700 – Прикладная информатика.- (электронный ресурс)/ В.П.Галас, Владимир, 2013. 95 с.

Приведены описания лабораторных работ по дисциплине «Вычислительные системы, сети и телекоммуникации», в которых изучаются основные принципы построения современных вычислительных машин. Часть работ представляет собой программные модели, работа с которыми осуществляется в интерактивном режиме. Остальные работы выполнены в виде виртуальной электронной лаборатории на персональном компьютере с использованием пакета программ Electronic Workbench (Multisim), позволяющего производить необходимые экспериментальные исследования.

Предназначены для студентов специальности 23070000 - прикладная информатика дневной и дистанционной форм обучения.

Лабораторная работа № 1
ПРОВОДНЫЕ СОЕДИНЕНИЯ ЛВС

Обжим кабеля UTP5/STP5 (витая пара CAT5)

1. Цель работы

Научиться обжимать кабель «витая пара» 5-й категории и тестировать полученные соединения.

2. Приборы и материалы:

Кабель «витая пара» 5-й категории, устройство для обжимки кабеля HT-2008AR, коннекторы RJ-45, кабельный тестер (Lan Tester LT200).

3. Краткие теоретические сведения

Для построения компьютерных сетей применяются линии связи, использующие различную физическую среду. В качестве физической среды в коммуникациях используются металлы (в основном медь), сверхпрозрачное стекло (кварц) или пластик и эфир. Физическая среда передачи данных может представлять собой кабель "витая пара", коаксиальные кабель, волоконно-оптический кабель и окружающее пространство.

Линии связи, или линии передачи, данных - это промежуточная аппаратура и физическая среда, по которой передаются информационные сигналы (данные).

В одной линии связи можно образовать несколько каналов связи (виртуальных или логических каналов), например путем частотного или временного разделения каналов. Канал связи - это средство односторонней передачи данных. Если линия связи монопольно используется каналом связи, то в этом случае линию связи называют каналом связи.

Канал передачи данных - это средства двухстороннего обмена данными, которые включают в себя линии связи и аппаратуру передачи (приема) данных. Каналы передачи данных связывают между собой источники информации и приемники информации.

В качестве линий связи могут быть применены коаксиальный кабель или кабель "витая пара".

Витая пара (англ. twisted pair) — вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных

между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой. Свивание проводников производится с целью повышения связи проводников одной пары (электромагнитная помеха одинаково влияет на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара - один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и компьютерных сетях в качестве сетевого носителя во многих технологиях, таких как Ethernet, ARCNet и Token ring. В настоящее время благодаря своей дешевизне и лёгкости в установке является самым распространённым решением для построения локальных сетей.

Кабель подключается к сетевым устройствам при помощи соединителя 8P8C (RJ45 или RJ-45), немного большего, чем телефонный соединитель RJ11.

В зависимости от наличия защиты — электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар - определяют разновидности данной технологии.

Незащищенная витая пара

Неэкранированная витая пара (UTP — Unscreened twisted pair)

— экранирование полностью отсутствует;

Фольгированная витая пара (FTP — Foiled twisted pair) — также известна как S/UTP [1] присутствует один общий внешний экран;

Фольгированная экранированная витая пара (SFTP — Shielded Foiled twisted pair) — отличается от FTP наличием дополнительного внешнего экрана из медной оплетки;

Виды защищенной витой пары:

Стандартная (STP — Shielded twisted pair) присутствет экран для каждой пары;

Экранированная витая пара (S/STP — Screened shielded twisted pair) отличается от STP наличием дополнительного общего внешнего экрана.

Экранирование обеспечивает лучшую защиту от электромагнитных наводок как внешних, так и внутренних, и т. д. Экран по всей длине соеди-

нен с неизолированным дренажным проводом, который объединяет экран в случае разделения на секции при излишнем изгибе или растяжении кабеля. В зависимости от структуры проводников кабель применяется одно- и многожильный. В первом случае каждый провод состоит из одной медной жилы, а во втором — из нескольких.

Одножильный кабель не предполагает прямых контактов с подключаемой периферией. То есть, как правило, его применяют для прокладки в коробах, стенах и так далее с последующим оконечива нием розетками. Связано это с тем, что медные жилы довольно толстые и при частых изгибах быстро ломаются. Однако для «врезания» в разъемы панелей розеток такие жилы подходят как нельзя лучше.

В свою очередь, многожильный кабель плохо переносит «врезание» в разъёмы панелей розеток (тонкие жилы разрезаются), но замечательно ведет себя при изгибах и скручиваниях. Кроме того, многожильный провод обладает большим затуханием сигнала. Поэтому многожильный кабель используют в основном для изготовления патчкордов (PatchCord), соединяющих периферию с розетками.

Конструкция кабеля

Кабель обычно состоит из четырёх пар. Проводники в парах изготовлены из монолитной медной проволоки толщиной 0,5 - 0,65 мм. Кроме метрической, применяется система AWG, в которой эти величины составляют 24 или 22 соответственно. Толщина изоляции около

0,2 мм, материал обычно поливинилхлорид (английское сокращение PVC), для более качественных образцов 5-й категории - полипропилен (PP), полиэтилен (PE). Особенно высококачественные кабели имеют изоляцию из вспененного (ячеистого) полиэтилена, который обеспечивает низкие диэлектрические потери, или тефлона, обеспечивающего уникальный рабочий диапазон температур.

Также внутри кабеля встречается так называемая «разрывная нить» (обычно капрон), которая используется для облегчения разделки внешней оболочки: при вытягивании она делает на оболочке продольный разрез, который открывает доступ к кабельному сердечнику, гарантированно не повреждая изоляцию проводников.

Внешняя оболочка имеет толщину 0,5 - 0,6 мм и обычно изготавливается из привычного поливинилхлорида с добавлением мела, кото-

рый повышает хрупкость. Это необходимо для точного облома по месту надреза лезвием отрезного инструмента. Кроме этого начинают применяться так называемые «молодые полимеры», которые не поддерживают горения и не выделяют при нагреве галогенов (такие кабели маркируются как LSZH - Low Smoke Zero Halogen и обычно имеют яркую окраску внешней оболочки).

Самый распространенный цвет оболочки - серый. Оранжевая окраска, как правило, указывает на негорючий материал оболочки, который позволяет прокладывать линии в закрытых областях. В общем случае цвета не обозначают особых свойств, но их применение позволяет легко отличать коммуникации с разным функциональным назначением как при монтаже, так и обслуживании.

Отдельно нужно отметить маркировку. Кроме данных о производителе и типе кабеля она обязательно включает в себя метровые или футовые метки.

Форма внешней оболочки также может быть различна. Чаще других применяется самая простая - круглая. Только для прокладки под половым покрытием по очевидной причине используется плоский кабель.

Кабели для наружной прокладки обязательно имеют влагостойкую оболочку из полиэтилена, которая наносится (как правило) вторым слоем поверх обычной, поливинилхлоридной. Кроме этого возможны заполнение пустот в кабеле водоотталкивающим гелем и бронирование с помощью гофрированной ленты или стальной проволоки.

Категории кабеля

Существует несколько категорий кабеля „витая пара”, которые нумеруются от CAT1 до CAT7 и определяют эффективный пропускаемый частотный диапазон. Кабель более высокой категории обычно содержит больше пар проводов и каждая пара имеет больше витков на единицу длины. Категории неэкранированной витой пары описываются в стандарте EIA/TIA 568 (Американский стандарт проводки в коммерческих зданиях).

CAT1 (полоса частот 0.1 МГц) - телефонный кабель, всего одна пара (в России применялся кабель без скруток — «лапша», у него характеристики не хуже, но больше влияние помех). В США использовался ранее только в «скрученном» виде. Применяется только для передачи голоса или данных при помощи модема.

CAT2 (полоса частот 1 МГц) - старый тип кабеля, 2 пары про-

водников, поддерживал передачу данных на скоростях до 4 Мбит/с, использовался в сетях token ring и ARCNet. Сейчас иногда встречается в телефонных сетях.

CAT3 (полоса частот 16 МГц) - 4-парный кабель, использовался при построении локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных до 10 или 100 Мбит/с по технологии 100BASE-T4. В отличие от предыдущих двух отвечает требованиям стандарта IEEE 802.3. Также до сих пор встречается в телефонных сетях.

CAT4 (полоса частот 20 МГц). Кабель состоит из 4 скрученных пар, использовался в сетях token ring, 10BASE-T, 100BASE-T4, скорость передачи данных не превышает 16 Мбит/с по одной паре, сейчас не используется.

CAT5 (полоса частот 100 МГц) - 4- парный кабель, это и есть то, что обычно называют кабель «витая пара» (рис. 8.19). Благодаря высокой скорости передачи до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар, является самым распространённым сетевым носителем, использующимся в компьютерных сетях до сих пор. При прокладке новых сетей пользуются несколько усовершенствованным кабелем CAT5e (полоса частот 125 МГц), который лучше пропускает высокочастотные сигналы. Ограничение на длину кабеля между устройствами (компьютер-свитч, свитч- компьютер, свитч-свитч) 100 м. Ограничение хаб-хаб 5 м.

CAT6 (полоса частот 250 МГц) применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 1000 Мбит/с. Добавлен в стандарт в июне 2002 года. Существует категория CAT6a, в которой увеличена частота пропускаемого сигнала до 500 МГц. По данным IEEE, в 70 % установленных сетей в 2004 году применялся кабель категории CAT6.

CAT7. Спецификация на данный тип кабеля пока не утверждена, скорость передачи данных до 100 Гбит/с, частота пропускаемого сигнала до 600-700 МГц. Кабель этой категории экранирован. Седьмая категория витой пары не UTP, а S/FTP (Screened Fully shielded Twisted Pair). Благодаря двойному экрану длина кабеля может превышать 100 м.

Схемы обжима витой пары

Для обжима витой пары UTP используются разъемы стандарта RJ-45 (рис. 1), которые в зависимости от вида кабеля «витой пары» бывают:

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

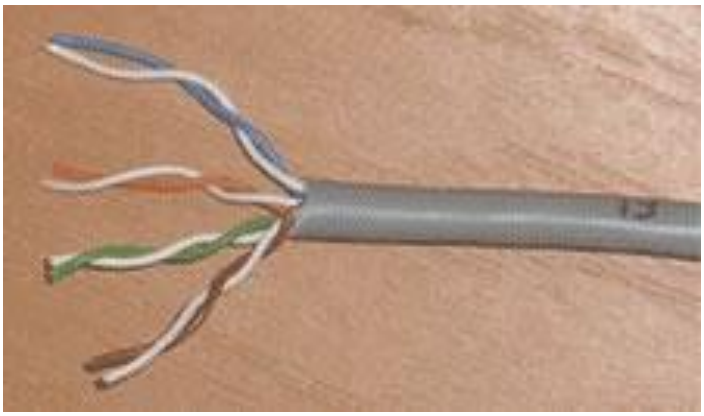


Рис. 1. Кабель из 4 неэкранированных витых пар

Для обжимки «витых пар» используют специальный инструмент, который имеет три рабочие области и соответственно выполняет три функции:

1. Ближе всего к рукояткам устройства располагается область, в которой установлен нож для обрезания проводников «витой пары». Также в этой области есть специальная выемка для снятия внешней изоляции с круглого кабеля (рис. 1).

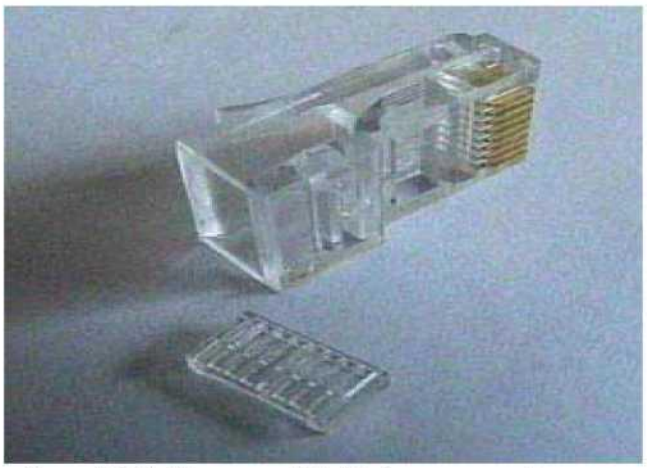


Рис. 8.20. Разъем RJ-45 для «витой пары» + вставка

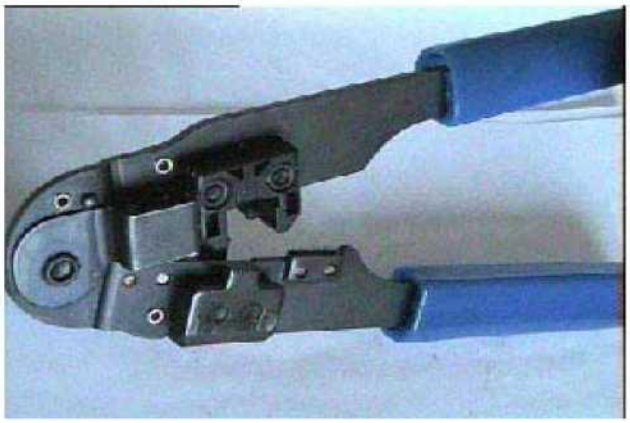


Рис. 2. Устройство для зачистки и обжима сетевого кабеля

2. В центре находится гнездо для обжима разъема RJ-45.
3. В верхней части устройства, область для зачистки наружной изоляции витой пары UTP (внутренняя изоляция проводников не зачищается, а прорезается контактами разъема).

Существует две схемы обжимки кабеля: прямой кабель и перекрёстный (Cross-over) кабель (рис. 2).

а)

Рис. 3. Схемы обжимки кабеля: а - прямой кабель

б)

Рис. 4. Схемы обжимки кабеля: б - перекрёстный (кросс-овер) кабель

Первая схема используется для соединения компьютера со свитчем/хабом, вторая для соединения двух компьютеров напрямую.

Кабельный тестер (Lan Tester)

Проверить качество выполненных соединений можно с помощью кабель тестера. В работе используется устройство LT200 представляющее собой простой кабельный тестер (Lan Tester) для экранированных (STP/FTP) и неэкранированных (UTP) кабелей витая пара. Тестер LT200 состоит из двух модулей - приемника и передатчика

Рис. 5

Приемник имеет один экранированный порт RJ-45 и один блок из 9 светодиодных индикаторов. Модуль приемника используется совместно с передатчиком при тестировании линии на удаленном конце. С помощью модуля приемника можно тестировать кабельные сегменты длиной до 305 метров. Светодиоды блока индикаторов приемника (9 шт.) имеют цифры от 1 до 8 обозначающие номер проводника, и символ G (Ground) - обозначающий экран кабеля. Приемник не имеет батареи, так как получает питание из линии от передатчика.

В отличии от приемника, модуль передатчика имеет уже два экранированных порта RJ-45 и два блока по 10 светодиодных индикаторов.

Модуль передатчика используется совместно с приемником при тестировании линии, а также без приемника при тестировании патч-кордов. При тестировании патч-кордов, обе вилки патч-корда подключаются к соответствующим портам RJ-45 модуля передатчика. Светодиоды блока индикаторов передатчика (10 шт.) имеют цифры от 1 до 8 обозначающие номер проводника, символ G (Ground) - обозначающий экран кабеля и символ P (Power) - питание. Питание передатчика осуществляется от 9В батареи типа "Крона".

Также передатчик имеет: батарейный отсек для установки 9В батарейки типа "Крона", кнопку ON/OF, колесико-регулятор скорости тестирования.

С помощью кабельного тестера LT200 можно выявить следующие ошибки, возникающие при монтаже:

- закороченные пары проводов (Shorted);
- открытые пары проводов (Open);
- перекрестные пары проводов (Crossed);
- реверсивные пары проводов (Reversed);
- перемещенные пары проводов (*перестановленные*-Transposed);

- расщепленные пары проводов (Split)

splitted pair - расщепленная пара. Наиболее трудно обнаруживаемая ошибка при монтаже витой пары, у которой один провод смонтирован правильно, а второй подключен к контакту другой пары);

- Non-Pair (*не пара*) Wiring.

Визуальный контроль в процессе тестирования может проводиться на любом из 2-х модулей. Также прибор позволяет проверить целостность экрана кабеля.

Если кабель не подключен, мигает только один ряд светодиодов. А когда кабель вставлен в оба модуля, светодиоды под номерами с 1 до 8 поочередно загораются и на приемнике, и на передатчике – по крайней мере, если жилы кабеля целы, а концы обжаты правильно. Светодиод же, обозначенный буквой G, будет светиться только при наличии заземления.

Если один из светодиодов не загорается, значит, сигнал не проходит по жиле с этим номером. Допустим, если не горит светодиод 2 на передатчике, сигнал обрывается на втором слева проводнике в коннекторе, вставленном в передатчик. При замыкании жил на передатчике светодиоды загораются, как положено, а на приемнике не горят два (три, четыре) светодиода либо при загорании одного индикатора на передатчике на приемнике вспыхивают два. Эти проблемы чаще всего решаются переобжатием концов витой пары. Если оно не помогает, возможно, поврежден сам провод – в таком случае его придется заменить, так как данный тестер примитивен и не может указать, насколько далеко от конца кабеля разрыв (а бывают девайсы, которые могут и это, – они дороже и сложнее в обращении).

В современных сетях чаще всего используется схема обжатия без перекрещивания – порядок жил витой пары на концах кабеля совпадает. Если светодиоды на передатчике загораются строго по очереди, а на приемнике – в неправильном порядке, значит, проводники перепутаны местами. Например, если после шестого загорается сначала восьмой, а потом седьмой светодиод, значит, жилы 7 и 8 заняли места друг друга. Необходимо отрезать штепсель и обжать конец кабеля, внимательно проследив за корректным порядком жил – для этого на них сделана разноцветная изоляция (бело-оранжевая, оранжевая, бело-зеленая, синяя, бело-синяя, зеленая, бело-коричневая, коричневая). При проверке телефонных кабелей тестер используется точно так же, как с витой парой, только в таком проводе шесть жил, и гореть будут первые шесть светодиодов.

Тестер LT200 нельзя подключать в активную цепь, т.е. на концах тестируемой линии не должно быть работающего активного оборудования, в противном случае тестер выйдет из строя.

4. Ход лабораторной работы

1. Изучить теоретический материал, записав основные моменты лабораторной работы.
2. Обжать кабель «витая пара» по схеме кросс-овер.
3. Вначале проводят зачистку наружной изоляции кабеля. При зачистке плоского кабеля его упирают в специальный выступ на устройстве, расположенный в области зачистки, чтобы получить глубину зачистки под стандартный разъем, зажимают кабель и рывком производят зачистку. Немного более сложным выглядит процесс зачистки круглых кабелей витых пар. Наружную изоляцию круглого кабеля лучше только слегка надрезать, осторожно поворачивая его в области зачистки, а затем снять кусочек изоляции по кольцевому надрезу вручную. На многих обжимных устройствах есть специальная область для снятия внешней изоляции с круглого кабеля.
4. После зачистки разводят провода сетевого кабеля в одной плоскости в необходимом порядке, выравнивают длину всех проводов и еще раз ровно подрезают (рис. 6).

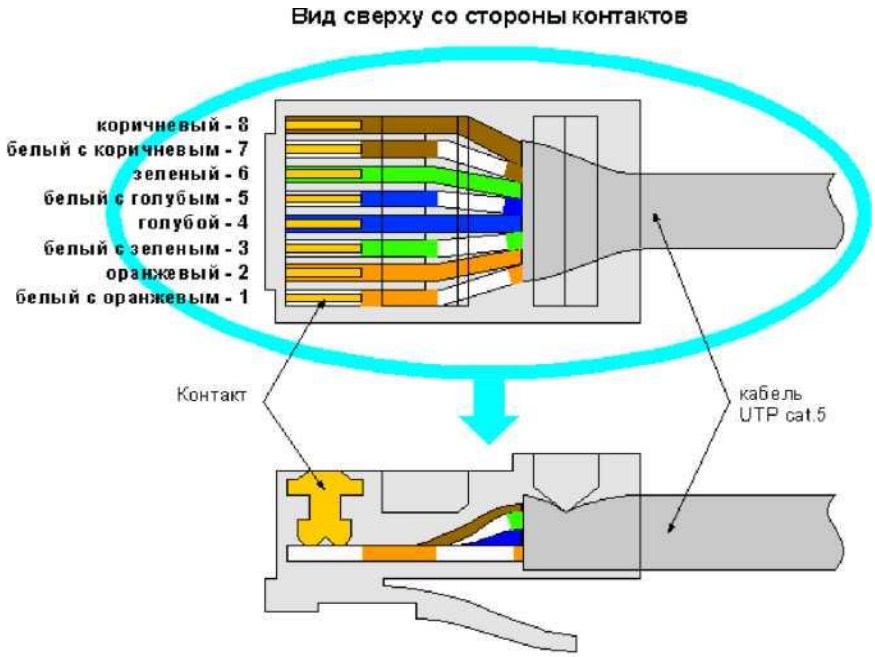


Рис. 6. Схема разводки кабеля

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

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

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

5. Проверить качество выполненных соединений с помощью кабель тестера.

6. Содержание отчета

1. Титульный лист.
2. Цель работы.
3. Краткое описание кабеля «витая пара».
4. Схемы обжима кабеля «витая пара».
5. Результаты тестирования
6. Выводы по работе.

7. Контрольные вопросы

1. Строение кабеля «витая пара».
2. Чем отличаются кабели «витая пара» различных категорий?
3. Каковы ограничения на применение «витой пары»?
4. Чем различаются схемы соединения „прямой кабель” и „перекрёстный кабель”?

Лабораторная работа № 2
ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

1.Цель работы

Изучить существующие способы оценки производительности вычислительных машин и получить базовые навыки сравнения их производительности.

2. Приборы и материалы

ПК на базе Intel Core 2 Duo 2,3 ГГц, ОЗУ 2048 Mb, HDD Seagate 80Gb 7200 rpm, ОС Windows XP SP3.

Тестовый пакет SiSoft Sandra Lite.

3. Краткие теоретические сведения

Основу для сравнения различных типов компьютеров между собой дают стандартные методики измерения производительности. В процессе развития вычислительной техники появилось несколько таких стандартных методик. Они позволяют разработчикам и пользователям осуществлять выбор между альтернативами на основе количественных показателей,

что дает возможность постоянного прогресса в данной области.

Единицей измерения производительности компьютера является время: компьютер, выполняющий определённый объем работы за меньшее время, является более быстрым. Время выполнения любой программы измеряется в секундах. Часто производительность измеряется как скорость появления некоторого числа событий в секунду, так что меньшее время подразумевает большую производительность.

MIPS

Одной из альтернативных единиц измерения производительности процессора (по отношению к времени выполнения) является MIPS - (миллион целочисленных команд в секунду). Имеется несколько различных вариантов интерпретации определения MIPS.

В общем случае MIPS есть скорость операций с целыми числами в единицу времени, т. е. для любой данной программы MIPS есть просто отношение количества команд в программе к времени ее выполнения. Таким образом, производительность может быть определена как обратная к времени выполнения величина, причем более быстрые машины при этом будут иметь более высокий рейтинг MIPS.

Положительными сторонами MIPS является то, что эту характеристику легко понять, особенно покупателю, и что более быстрая машина характеризуется большим числом MIPS, что соответствует нашим интуитивным представлениям. Однако использование MIPS в качестве метрики для сравнения наталкивается на три проблемы. Во- первых, MIPS зависит от набора команд процессора, что затрудняет сравнение по MIPS компьютеров, имеющих разные системы команд. Во-вторых, MIPS даже на одном и том же компьютере меняется от программы к программе. В-третьих, MIPS может меняться по отношению к производительности в противоположенную сторону.

MFLOPS

Измерение производительности компьютеров при решении научно-технических задач, в которых существенно используется арифметика с плавающей точкой, всегда вызывало особый интерес. Именно для таких вычислений впервые встал вопрос об измерении производительности, а по достигнутым показателям часто делались выводы об общем уровне разра-

боток компьютеров. Обычно для научно-технических задач производительность процессора оценивается в MFLOPS (миллионах чисел-результатов вычислений с плавающей точкой в секунду, или миллионах элементарных арифметических операций над числами с плавающей точкой, выполненных в секунду).

Как единица измерения, MFLOPS предназначена для оценки производительности только операций с плавающей точкой и поэтому не применима вне этой ограниченной области. Например, программыкомпиляторов имеют рейтинг MFLOPS, близкий к нулю, вне зависимости от того, насколько быстра машина, поскольку компиляторы редко используют арифметику с плавающей точкой.

SPECint92, SPECfp92

Важность создания пакетов тестов, базирующихся на реальных прикладных программах широкого круга пользователей и обеспечивающих эффективную оценку производительности процессоров, была осознана большинством крупнейших производителей компьютерного оборудования, которые в 1988 году учредили бесприбыльную корпорацию SPEC (Standard Performance Evaluation Corporation). Основной целью этой организации является разработка и поддержка стандартизованного набора специально подобранных тестовых программ для оценки производительности новейших поколений высокопроизводительных компьютеров. Членом SPEC может стать любая организация, уплатившая вступительный взнос.

Основным результатом работы SPEC являются наборы тестов, которые разрабатываются SPEC с использованием кодов, поступающих из разных источников. SPEC работает над импортированием этих кодов на разные платформы, а также создает инструментальные средства для формирования из кодов, выбранных в качестве тестов, осмысленных рабочих нагрузок. Поэтому тесты SPEC отличаются от свободно распространяемых программ. Хотя они могут существовать под похожими или теми же самыми именами, время их выполнения в общем случае будет отличаться.

В настоящее время имеется два базовых набора тестов SPEC, ориентированных на интенсивные расчеты и измеряющих производительность процессора, системы памяти, а также эффективность генерации кода компилятором. Как правило, эти тесты ориентированы на операционную систему UNIX, но они также импортированы и на другие платформы. Про-

цент времени, расходуемого на работу операционной системы и функции ввода/вывода, в общем случае ничтожно мал.

TPC-A, TPC-B, TPC-C

По мере расширения использования компьютеров при обработке транзакций в сфере бизнеса все более важной становится возможность справедливого сравнения систем между собой. С этой целью в 1988 году был создан Совет по оценке производительности обработки транзакций (TPC - Transaction Processing Performance Council), который представляет собой бесприбыльную организацию. Любая компания или организация может стать членом TPC после уплаты соответствующего взноса. На сегодня членами TPC являются практически все крупнейшие производители аппаратных платформ и программного обеспечения для автоматизации коммерческой деятельности. К настоящему времени TPC создал три тестовых пакета для обеспечения объективного сравнения различных систем обработки транзакций и планирует создать новые оценочные тесты.

Тесты TPC

TPC определяет и управляет форматом нескольких тестов для оценки производительности OLTP (On-Line Transaction Processing), включая тесты TPC-A, TPC-B и TPC-C. Как уже отмечалось, создание оценочного теста является ответственностью организации, выполняющей этот тест. TPC требует только, чтобы при создании оценочного теста выполнялись определенные условия. Хотя упомянутые тесты TPC не являются характерными тестами для оценки производительности баз данных, системы реляционных баз данных являются ключевыми компонентами любой системы обработки транзакций.

Следует отметить, что как и любой другой тест, ни один тест TPC не может измерить производительность системы, которая применима для всех возможных сред обработки транзакций, но эти тесты действительно могут помочь пользователю справедливо сравнивать похожие системы. Однако, когда пользователь делает покупку или планирует решение о покупке, он должен понимать, что никакой тест не может заменить его конкретную прикладную задачу.

Тест TPC-A

Выпущенный в ноябре 1989 года тест TCP-A предназначался для оценки производительности систем, работающих в среде интенсивно обновляемых баз данных, типичной для приложений интерактивной обработки данных (OLDP - on-line data processing). Такая среда характеризуется:

- множеством терминальных сессий в режиме on-line;
- значительным объемом ввода/вывода при работе с дисками;
- умеренным временем работы системы и приложений;
- целостностью транзакций.

Тест TPC-A определяет пропускную способность системы, измеряемую количеством транзакций в секунду (tps A), которые система может выполнить при работе с множеством терминалов. Хотя спецификация TPC-A не определяет точное количество терминалов, компании-поставщики систем должны увеличивать или уменьшать их количество в соответствии с нормой пропускной способности. Тест TPC-A может выполняться в локальных или региональных вычислительных сетях. В этом случае его результаты определяют либо “локальную” пропускную способность (TPC-A-local Throughput), либо “региональную” пропускную способность (TPC-A wide Throughput). Очевидно, эти два тестовых показателя нельзя непосредственно сравнивать. Спецификация теста TPC-A требует, чтобы все компании полностью раскрывали детали работы своего теста, свою конфигурацию системы и ее стоимость (с учетом пятилетнего срока обслуживания). Это позволяет определить нормализованную стоимость системы ($/tpsA).

Тест TPC-B

В августе 1990 года TPC одобрил TPC-B - интенсивный тест базы данных, характеризующийся следующими элементами:

- значительным объемом дискового ввода/вывода;
- умеренным временем работы системы и приложений;
- целостностью транзакций.

TPC-B измеряет пропускную способность системы в транзакциях в секунду (tpsB). Поскольку имеются существенные различия между двумя тестами -TPC-A и TPC-B - (в частности, в TPC-B не выполняется эмуляция терминалов и линий связи), их нельзя прямо сравнивать.

Тест TPC-C

Тестовый пакет TPC-C моделирует прикладную задачу обработки заказов, а также достаточно сложную систему OLTP, которая должна управлять приемом заказов, управлением учетом товаров и распространением товаров и услуг. Тест TPC-C осуществляет тестирование всех основных компонентов системы: терминалов, линий связи, ЦП, дискового ввода/вывода и базы данных.

TPC-C требует, чтобы выполнялись пять типов транзакций:

- новый заказ, вводимый с помощью сложной экранной формы;
- простое обновление базы данных, связанное с платежом;
- простое обновление базы данных, связанное с поставкой;
- справка о состоянии заказов;
- справка по учету товаров.

Обычно публикуются два результата. Один из них, tpm-C, представляет пиковую скорость выполнения транзакций (выражается в количестве транзакций в минуту). Второй результат, $/tpm-C, представляет собой нормализованную стоимость системы. Стоимость системы включает все аппаратные средства и программное обеспечение, используемые в тесте, плюс стоимость обслуживания в течение пяти лет.

AIM

Одной из независимых организаций, осуществляющей оценку производительности вычислительных систем, является частная компания AIM Technology, которая была основана в 1981 году. Компания разрабатывает и поставляет программное обеспечение для измерения производительности систем, а также оказывает услуги по тестированию систем конечным пользователям и поставщикам вычислительных систем и сетей, которые используют промышленные стандартные операционные системы.

Генератор тестовых пакетов представляет собой программную систему, которая обеспечивает одновременное выполнение множества программ. Он содержит большое число отдельных тестов, которые потребляют определенные ресурсы системы и тем самым акцентируют внимание на определенных компонентах, из которых складывается ее общая производительность. При каждом запуске генератора могут выполняться любые отдельные или все доступные тесты в любом порядке и при любом количестве проходов, позволяя тем самым создавать для системы практически

любую необходимую рабочую нагрузку. Все это дает возможность тестовому пакету моделировать любой тип смеси при постоянной смене акцентов (для лучшего представления реальной окружающей обстановки) и при обеспечении высокой степени конфигурирования.

Для оценки и сравнения систем в AIM Performance Report II используются следующие критерии:

1. Пиковая производительность (рейтинг производительности по AIM).
2. Максимальная пользовательская нагрузка.
3. Индекс производительности утилит.
4. Пропускная способность системы.

Рейтинг производительности по AIM - стандартная единица измерения пиковой производительности, установленная AIM Technology. Этот рейтинг определяет наивысший уровень производительности системы, который достигается при оптимальном использовании ЦП, операций с плавающей точкой и кэширования диска. Рейтинг вездесущей машины VAX 11/780 обычно составляет 1 AIM. В отчетах AIM представлен широкий ряд UNIX-систем, которые можно сравнивать по этому параметру.

Максимальная пользовательская нагрузка определяет “емкость” (capacity) системы, т. е. такую точку, начиная с которой производительность системы падает ниже приемлемого уровня для N-го пользователя (меньше чем одно задание в минуту на одного пользователя).

Индекс производительности утилит определяет количество пользовательских нагрузок пакета Milestone, которые данная система выполняет в течение одного часа. Набор тестов Milestone многократно выполняет выбранные утилиты UNIX в качестве основных и фоновых заданий при умеренных пользовательских нагрузках. Этот параметр показывает возможности системы по выполнению универсальных утилит UNIX.

Максимальная пропускная способность определяет пиковую производительность мультипрограммной системы, измеряемую количеством выполненных заданий в минуту. Приводящийся в отчете график пропускной способности системы показывает, как она работает при различных нагрузках.

4. Ход лабораторной работы

1. Изучить теоретический материал, записав основные положения

работы.

2. Установить на ПК бесплатную версию пакета SiSoft Sandra Lite http://www.softportal.com/software-223-sisoftware-sandra-lite.html (рис. 1).

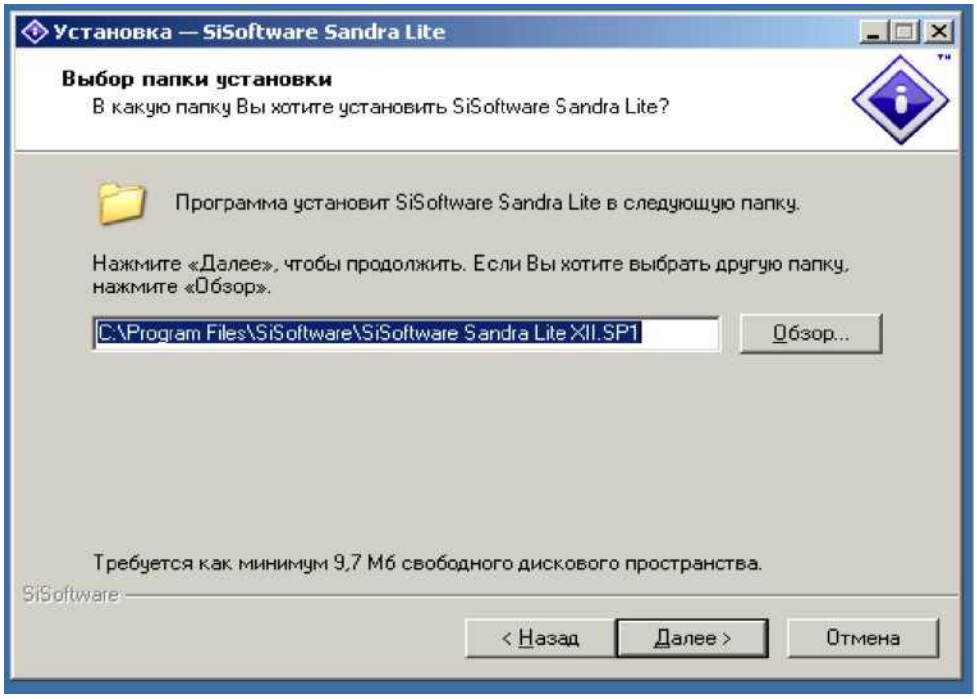


Рис. 1. Окно установки пакета SiSoft Sandra Lite

3. Настроить программный пакет в соответствии с требованиями операционной системы (рис. 2).

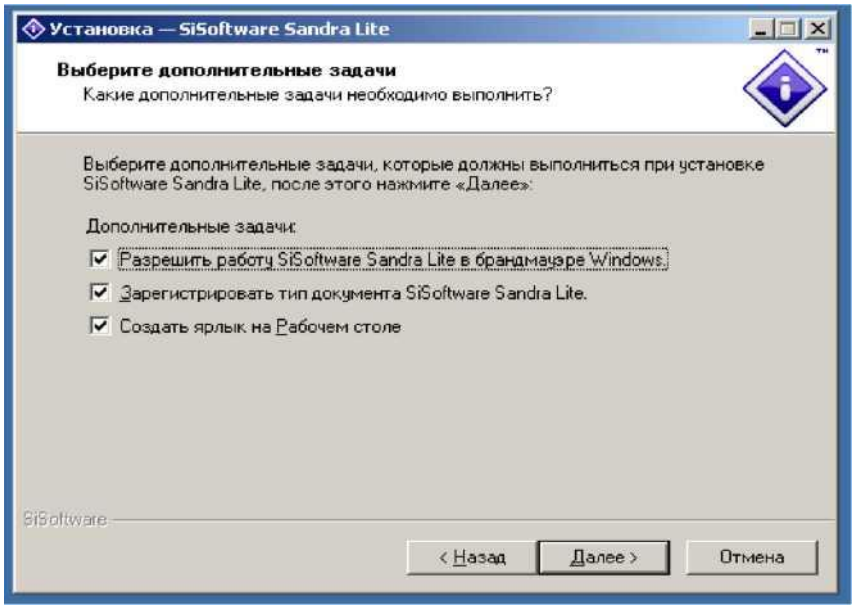


Рис. 2. Окно настройки дополнительных задач пакета SiSoft Sandra Lite

4. Получить сводную информацию о конфигурации Вашей системы (рис. 3).

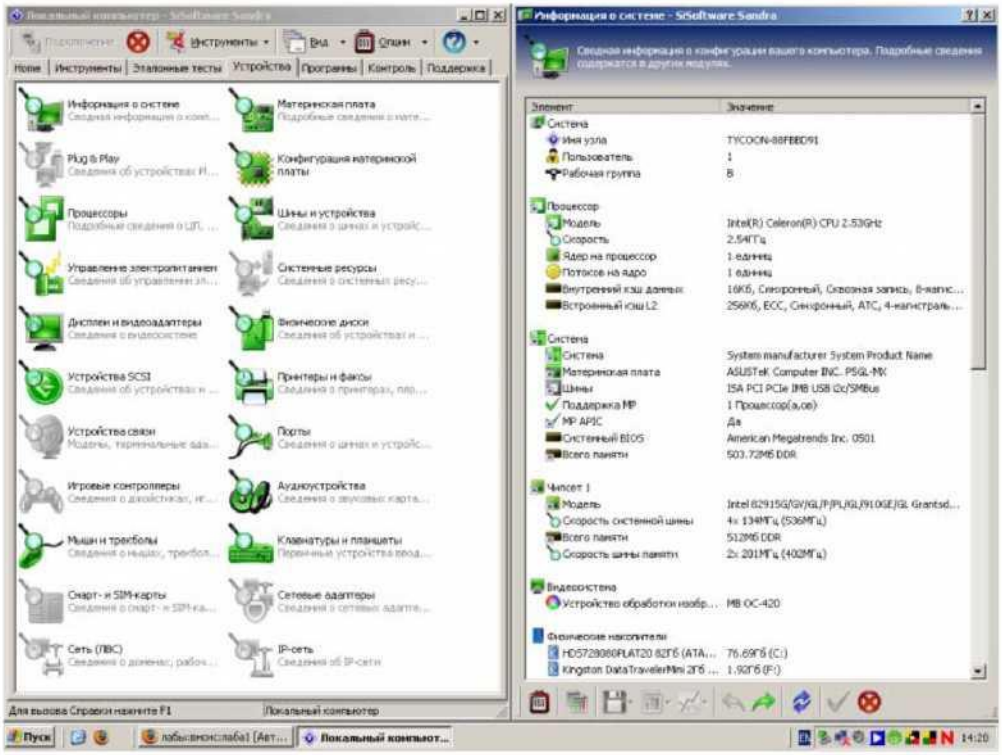


Рис. 3. Окно конфигурации системы

5. Провести тестирование производительности вычислительной системы по следующим пунктам:

- арифметический тест процессора;
- многоядерная эффективность;
- арифметика .net;
- файловые системы;
- съёмные диски;
- латентность памяти;
- пропускная способность сети;
- мультимедийный тест процессора;
- мультимедиа .net;
- физические диски;
- cd-rom и dvd;
- пропускная способность памяти;
- кэш и память;
- скорость интернет-соединения.

Получившиеся результаты необходимо представить в отчёте в качестве изображений с монитора ПК.

5. Содержание отчета

1. Титульный лист.
2. Цель работы.
3. Обзор и анализ способов оценки производительности вычислительных машин.
4. Описание лабораторных устройств.
5. Результаты экспериментальных исследований.
6. Выводы по работе.

6. Контрольные вопросы

1. Назовите основные факторы, влияющие на производительность ВМ.
2. Какие существуют тесты для оценки производительности, в чем их различие?
3. Как связана тактовая частота микропроцессора и производительность ВМ?

Лабораторная работа №3
РАБОТА С ПРОГРАММНЫМИ СРЕДСТВАМИ INTERNET. УТИЛИТЫ PING И TRACEROUTE

1. Цель работы

Исследование вероятностно-временных характеристик сети с использованием утилиты ping, исследование топологии фрагментов Internet с использованием утилиты traceroute.

2. Приборы и материалы:

ПК на базе Intel Core 2 Duo 2,3 ГГц, ОЗУ 2048 Mb, HDD Seagate 80Gb 7200 rpm, ОС Windows XP SP3.

3. Краткие теоретические сведения

3.1. Утилита ping

Утилита ping (Packet Internet Groper) является одним из главных средств, используемых для отладки сетей, и служит для принудительного вызова ответа конкретной машины. Она позволяет проверять работу программ TCP/IP на удаленных машинах, адреса устройств в локальной сети, адрес и маршрут для удаленного сетевого устройства. В выполнении команды ping участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы. Это утилита низкого уровня, которая не требует наличия серверных процессов на зондируемой машине, поэтому успешный результат при прохождении запроса вовсе не означает, что выполняются какие-либо сервисные программы высокого уровня, а говорит о том, что сеть находится в рабочем состоянии, питание зондируемой машины включено и машина не отказала ("не висит").

Утилита ping имеется не только в UNIX, но и в большинстве реализаций TCP/IP для других операционных систем. В Windows утилита ping имеется в комплекте поставки, но представляет собой программу, выполняющуюся в сеансе DOS из командной строки.

Запросы утилиты ping передаются по протоколу ICMP (Internet Control Message Protocol). Получив такой запрос, программное обеспечение, реализующее протокол IP у адресата, немедленно посылает эхо-ответ. Эхо-запросы посылаются заданное количество раз (ключ -n) или по умолчанию до тех пор, пока пользователь не введет команду прерывания (Ctrl+C или Del), после чего выводятся статистические данные.

Обратите внимание: *поскольку с утилиты ping начинается хакерская атака, некоторые серверы в целях безопасности могут не посылать эхо-ответы (например, www.microsoft.com). Не ждите напрасно, введите команду прерывания.*

Утилита ping (Packet Internet Groper) является одним из главных средств, используемых для отладки сетей, и служит для принудительного вызова ответа конкретной машины. Она позволяет проверять работу программ TCP/IP на удаленных машинах, адреса устройств в локальной сети, адрес и маршрут для удаленного сетевого устройства. В выполнении команды ping участвуют система маршрутизации, схемы разрешения адресов

и сетевые шлюзы. Это утилита низкого уровня, которая не требует наличия серверных процессов на зондируемой машине, поэтому успешный результат при прохождении запроса вовсе не означает, что выполняются какие-либо сервисные программы высокого уровня, а говорит о том, что сеть находится в рабочем состоянии, питание зондируемой машины включено и машина не отказала ("не висит").

Утилита ping имеется не только в UNIX, но и в большинстве реализаций TCP/IP для других операционных систем. В Windows утилита ping имеется в комплекте поставки, но представляет собой программу, выполняющуюся в сеансе DOS из командной строки.

Запросы утилиты ping передаются по протоколу ICMP (Internet Control Message Protocol). Получив такой запрос, программное обеспечение, реализующее протокол IP у адресата, немедленно посылает эхо-ответ. Эхо-запросы посылаются заданное количество раз (ключ -n) или по умолчанию до тех пор, пока пользователь не введет команду прерывания (Ctrl+C или Del), после чего выводятся статистические данные.

Поскольку с утилиты ping начинается хакерская атака, некоторые серверы в целях безопасности могут не посылать эхо-ответы (например, www.microsoft.com).

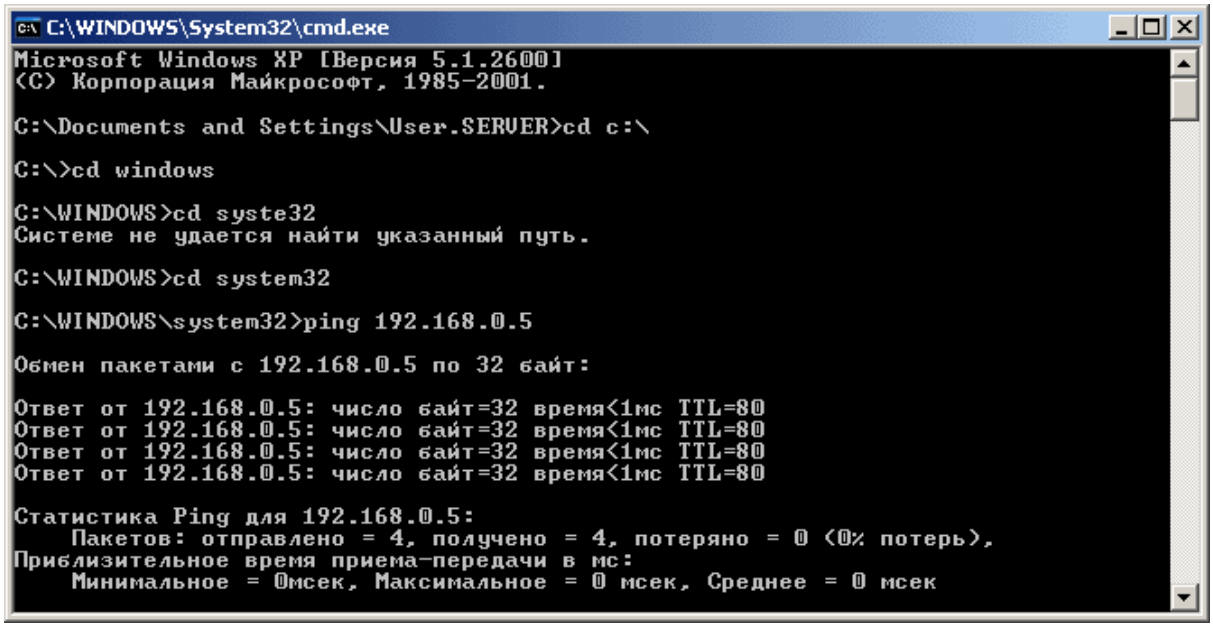
Формат команды: ping [-t][-a][-n][-l][-f][-i TTL][-v TOS] [-г][][имя машины][[- списокУзлов]|[-к списокУзловШ-w] (см. таблицу).

```
Использование: ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS]
               [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]]
               [-w таймаут] конечноеИмя

Параметры:
    -t              Отправка пакетов на указанный узел до команды прерывания.
                    Для вывода статистики и продолжения нажмите
                    <Ctrl>+<Break>, для прекращения - <Ctrl>+<C>.
    -a              Определение адресов по именам узлов.
    -n число        Число отправляемых запросов.
    -l размер       Размер буфера отправки.
    -f              Установка флага, запрещающего фрагментацию пакета.
    -i TTL          Задание срока жизни пакета (поле "Time To Live").
    -v TOS          Задание типа службы (поле "Type Of Service").
    -r число        Запись маршрута для указанного числа переходов.
    -s число        Штамп времени для указанного числа переходов.
    -j списокУзлов  Свободный выбор маршрута по списку узлов.
    -k списокУзлов  Жесткий выбор маршрута по списку узлов.
    -w таймаут      Таймаут каждого ответа в миллисекундах.
```

В составе Windows XP\2000 есть команда "Ping" она позволяет оправлять пакеты информации заданной длины и фиксировать время отклика удаленной системы, а так же целостность информации. Тестовая

служба Ping взаимодействует напрямую с сетевой картой на уровне протокола TCP/IP, поэтому вне зависимости от того, настроены ли параметры доступа и дополнительные службы, Ping систему увидит. Запустите командную строку "Пуск" -> "Выполнить -> "cmd" Появиться окно консольного сеанса, по сути, старый добрый MS DOS. Затем с помощью команд CD (Change Directory) перейдите в папку system32 вашей копии Windows XP как показано на рисунке. Если запустить ping из Windows с помощью bat\cmd файла или раздела "выполнить", сразу после выполнения задачи окно программы закроется и вы не успеете увидеть результаты.



Формат команды: Ping "IP адрес удаленной системы" Например "Ping 192.168.0.1". По умолчанию программа передает 4 пакета по 32 байт каждый, что недостаточно для объективного тестирования сети, так как система бодро отчитается об успешном результате даже при очень низком качестве сигнала. Данная команда подойдет только для того, чтобы определить, есть ли вообще связь с тем или иным узлом. Для тестирования качества связи запустите Ping со следующими параметрами. ping.exe -l 16384 -w 5000 -n 100 192.168.0.XX Это обеспечит отправку 100 запросов по 16 килобайт на заданный IP адрес с интервалом ожидания в 0,5 секунды.
1. Если по результатам тестирования дошли все пакеты и потери составили не более 3%, ваша сеть работает нормально.
2. От 3-10% - сеть по-прежнему работает, благодаря алгоритмам коррекции

ошибок, однако из-за значительного числа потерянных пакетов и необходимости их повторной доставки снижается эффективная скорость сети. 3. Если число потерянных пакетов превышает 10-15%, необходимо принять меры по устранению неисправности, вызвавшей ухудшения качества связи.

Для получения более объективных результатов можно увеличить размер пакетов и\или их число, однако это увеличит и время тестирования. Дополнительные настройки программы ping вы сможете узнать, если запустить её с привычным справочным ключом ping /?

Причины слабого сигнала в линии и потери пакетов данных:

- Физические повреждения сетевого кабеля или его изоляции
- Некачественный обжим
- Ошибки в разводке витой пары
- Превышение стандартной длины сегмента
- Наличие мощных источников помех по ходу кабеля
- Некачественное восстановление поврежденных участков
- Более 5 коммутаторов в цепи.

Вызов утилиты Ping в командной строке Windows: C:\Documents and Settings\<имя пользователя^^ www.mail.ru Обмен пакетами с 207.227.119.10 по 32 байт:

Ответ от 207.227.119.10: число байт=32 время=196мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=198мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=193мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=195мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=199мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=196мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=192мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=197мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=197мс TTL=237 Время ожидания запроса истекло.

Ответ от 207.227.119.10: число байт=32 время=202мс TTL=237

Ответ от 207.227.119.10: число байт=32 время=192мс TTL=237 228

Ответ от 207.227.119.10: число байт=32 время=191мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=193мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=200мс TTL=237 Ответ от

207.227.119.10: число байт=32 время=196мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=196мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=199мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=196мс TTL=237 Ответ от 207.227.119.10: число байт=32 время=193мс TTL=237 Статистика Ping для 207.227.119.10: Пакетов: послано = 20, получено = 19, потеряно = 1 (5% потерь).

Приблизительное время передачи и приема: наименьшее = 191 мс, наибольшее = 202 мс, среднее = 186 мс. Максимальное значение TTL по умолчанию принимается равным 255 узлам.

Следовательно, чтобы определить количество узлов, через которые прошел пакет, надо от 255 отнять полученное значение TTL.

Практическое использование

• Можно узнать IP-адрес по доменному имени.

• Можно узнать, работает ли сервер. Например, системный администратор может узнать, „завис” ли только веб-сервер или на сервере глобальные проблемы.

• Можно узнать, есть ли связь с сервером. Например, проблемы с настройкой DNS-серверов на машине можно узнать, задав в ping сначала доменное имя, а потом IP-адрес.

• Также можно узнать качество канала, посмотрев, сколько ответов не пришло.

Формат команды:

ping [-t][-a][-n][-l][-f][-i TTL][-v TOS] [-r][][имя машины][[-j списокУзлов]|[-k списокУзлов]][-w]

Параметры утилиты ping

Ключи	Функции
-t	Отправка пакетов на указанный узел до команды прерывания
-a	Определение адресов по именам узлов
-n	Число отправляемых запросов
-l	Размер буфера отправки

-f	Установка флага, запрещающего фрагментацию пакета
-i TTL	Задание времени жизни пакета (поле "Time To Live")
-v TOS	Задание типа службы (поле "Type Of Service")
-r	Запись маршрута для указанного числа переходов
-s	Штамп времени для указанного числа переходов
-j список узлов	Свободный выбор маршрута по списку узлов
-k список узлов	Жесткий выбор маршрута по списку узлов
-w интервал	Интервал ожидания каждого ответа в миллисекундах

На практике большинство опций в формате команды можно опустить, тогда в командной строке может быть: ping имя узла.

ping newslink.org

Обмен пакетами с 207.227.119.10 по 32 байт:

Ответ от 207.227.119.10: число байт=32 время=196мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=198мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=193мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=195мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=199мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=196мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=192мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=197мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=197мс TTL=237
Время ожидания запроса истекло.

Ответ от 207.227.119.10: число байт=32 время=202мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=192мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=191мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=193мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=200мс TTL=237
Ответ от 207.227.119.10: число байт=32 время=196мс TTL=237

Ответ	от	207.227.119.10:	число	байт=32	время=196мс	TTL=237
Ответ	от	207.227.119.10:	число	байт=32	время=199мс	TTL=237
Ответ	от	207.227.119.10:	число	байт=32	время=196мс	TTL=237
Ответ	от	207.227.119.10:	число	байт=32	время=193мс	TTL=237

Статистика Ping для 207.227.119.10: Пакетов: послано = 20, получено = 19, потеряно = 1 (5% потерь)

Приблизительное время передачи и приема:

наименьшее = 191 мс, наибольшее = 202 мс, среднее = 186 мс

Обратите внимание: *максимальное значение TTL по умолчанию принимается равным 255 узлов. Следовательно, чтобы определить количество узлов, через которые прошел пакет, надо от 255 отнять полученное значение TTL. (На практике это бывает не всегда.)*

3.2. Утилита traceroute

Программа traceroute позволяет выявлять последовательность шлюзов, через которые проходит IP-пакет на пути к пункту своего назначения. У этой команды есть очень много опций, большинство из которых применяются системными администраторами крайне редко. Traceroute - это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Traceroute основана на протоколе ICMP.

Формат команды:

traceoute имя_машины

Как обычно, имя_машины может быть задано в символической или числовой форме. Выходная информация представляет собой список машин, начиная с первого шлюза и кончая пунктом назначения. Кроме того, показано полное время прохождения каждого шлюза.

Пример:

st1@pds:~ > traceroute www.newslink.org

traceroute to www.newslink.org (207.227.119.10),30 hops max,40 byte packets

18 lgw.ccs.sut.ru (195.19.219.129)1 ms 1 ms 1 ms

18 ing-e0.nw.ru (195.19.194.68)5 ms 2 ms 2 ms

```
18      StPetersburg-LE-4.Relcom.EU.net (193.125.189.189)4 ms 2 ms 6 ms
18      cwrussia-relcom.SPB.cwrussia.ru (213.152.128.249)29 ms 33 ms 19
ms
18      bar2-serial6-1-0-0.NewYorknyr.cw.net(206.24.205.153)166 ms 168 ms
170 ms
18      acr2-loopback.NewYorknyr.cw.net(206.24.194.62)166 ms 163 ms 167
ms
18      p4-2.nycmny1-ba1.bbnplanet.net (4.24.7.69)177 ms 175 ms 172 ms
18      p7-0.nycmny1-br1.bbnplanet.net (4.24.6.229)174 ms 176 ms 170 ms
18      p4-0.nycmny1-br2.bbnplanet.net (4.24.6.226)170 ms 175 ms 171 ms
18      so-4-0-0.chcgil2-br1.bbnplanet.net (4.24.9.65)184 ms 184 ms 183 ms
18      p6-0.chcgil1-br1.bbnplanet.net (4.24.9.70)181 ms 182 ms 185 ms
18      p4-0.chcgil1-br2.bbnplanet.net (4.24.5.226)181 ms 189 ms 184 ms
18      p2-0.nchicago2-br1.bbnplanet.net (4.0.5.210)184 ms 183 ms 182 ms
18      p1-0.nchicago2-br2.bbnplanet.net (4.0.1.146)187 ms 188 ms 194 ms
18      p8-0-0.nchicago2-core0.bbnplanet.net (4.0.6.2)482 ms 343 ms 331 ms
18      chi2-eth.cyberlynk.net (207.112.240.102)190 ms 183 ms 193 ms
18      core0-fe0.rac.cyberlynk.net (206.54.254.20)222 ms 217 ms 239 ms
18      www.newslink.org (207.227.119.10)254 ms 218 ms 229 ms
```

Команда traceroute работает путем установки поля времени жизни (числа переходов) исходящего пакета таким образом, чтобы это время истекало до достижения пакетом пункта назначения. Когда время жизни истечет, текущий шлюз отправит сообщение об ошибке на машину-источник. Каждое приращение поля времени жизни позволяет пакету пройти на один шлюз дальше.

Команда traceroute посылает для каждого значения поля времени жизни три пакета. Если промежуточный шлюз распределяет трафик по нескольким маршрутам, то эти пакеты могут возвращаться разными машинами. В этом случае на печать выводятся они все. Некоторые системы не посылают уведомлений о пакетах, время жизни которых истекло, а некоторые посылают уведомления, которые поступают обратно на машину-источник только после того, как истекло время их ожидания командой traceroute. Эти шлюзы обозначаются рядом звездочек. Даже если конкретный шлюз определить нельзя, traceroute чаще всего сможет увидеть следующие за ним узлы маршрута.

Программа traceroute выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки. Здесь хочется отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети. В силу особенностей работы протоколов маршрутизации в сети Интернет обратные маршруты часто не совпадают с прямыми, причем это справедливо для всех промежуточных узлов в трейсе. Поэтому ICMP-ответ от каждого промежуточного узла может идти своим собственным маршрутом, затеряться или прийти с большой задержкой, хотя в реальности с пакетами, которые адресованы конечному узлу, этого не происходит. Кроме того, на промежуточных маршрутизаторах часто стоит ограничение числа ответов ICMP в единицу времени, что приводит к появлению ложных потерь.

Traceroute входит в поставку большинства современных сетевых операционных систем. В системах Microsoft Windows эта программа носит название tracert, а в системах GNU/Linux, Cisco IOS и Mac OS

— traceroute.

Так как же работает утилита tracert?

Для того чтобы ответить на этот вопрос, нужно вспомнить структуру IP пакета, а точнее вспомнить про одно из его полей - TTL (Число переходов):

0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Версия				IHL				Тип обслуживания								Длина пакета															
Идентификатор																Флаги				Смещение фрагмента											
Число переходов (TTL)								Протокол								Контрольная сумма заголовка															
IP-адрес отправителя (32 бита)																															
IP-адрес получателя (32 бита)																															
Параметры (до 320 бит)																Данные (до 65535 байт минус заголовок)															

При отправке пакета это поле выставляется в 255 и затем, каждый маршрутизатор, через который пройдёт данный пакет уменьшает это зна-

чение на 1 т.е. **TTL=TTL-1**. Маршрутизатор, который получает пакет с значением TTL=1, уменьшает его на единицу, а затем удаляет пакет, т.к. значение поля TTL у пакета стало равно 0. После того как пакет был отброшен маршрутизатором, отправителю пакета отправляется ICMP-сообщение с кодом 11: "Превышение временного интервала". В заголовке IP-пакета с ICMP сообщением *источником* является IP-адрес маршрутизатора, дропнувшего пакет, а *назначением* - IP-адрес компьютера, отправившего отброшенный пакет.

Теперь не сложно догадаться как работает **Tracert**:

- Отправляется IP-пакет на указанный узел (в нашем примере yandex.ru) со значением поля TTL=1
- первый маршрутизатор на пути пакета уменьшает TTL и дропает(уничтожает) пакет
- Маршрутизатор отправляет ICMP уведомление что пакетик умер
- Утилита **Tracert** извлекает из ICMP пакета IP-адрес маршрутизатора измеряет потраченное время на прохождение пакета до маршрутизатора
- Если не указано иное в параметрах запуска **Tracert**, то посылается запрос DNS-серверу и определяется доменное имя маршрутизатора, если такое имеется
- В консоль выводится IP-адрес (или доменное имя) первого маршрутизатора
- Снова отправляется IP пакет на указанный узел, но с TTL=2
- Пакет дропается на втором промежуточном маршрутизаторе
- Процедура повторяется до тех пор, пока не придёт ответ от узла назначения (yandex.ru) либо число промежуточных узлов не привысит максимального значения для **tracert** - 30 узлов.

Для определения промежуточных маршрутизаторов traceroute отправляет серию (обычно три) пакетов данных целевому узлу, при этом каждый раз увеличивая на 1 значение поля TTL («время жизни»). Это поле обычно указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно сообщение ICMP, указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и

получением ответа (эти сведения выводятся на монитор компьютера). Затем traceroute повторяет отправку серии пакетов, но уже с TTL, равным 2, что позволяет первому маршрутизатору пропустить их дальше.

Процесс повторяется до тех пор, пока при определённом значении TTL пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

На оконечном хосте IP-дейтаграмма с TTL = 1 не отбрасывается и не вызывает ICMP-сообщения типа „Срок истёк”, а должна быть отдана приложению. Достижение пункта назначения определяется следующим образом: отсылаемые traceroute дейтаграммы содержат UDP- пакет с таким номером UDP-порта адресата (превышающим 30 000), что он заведомо не используется на адресуемом хосте. В пункте назначения UDP-модуль, получая подобные дейтаграммы, возвращает ICMP-сообщения об ошибке «порт недоступен». Таким образом, чтобы узнать о завершении работы, программе traceroute достаточно обнаружить, что поступило ICMP-сообщение об ошибке этого типа.

Вызов утилиты traceroute в командной строке Windows:

C:\Documents and Settings\<имя пользователя>tracert www.mail.ru

Трассировка маршрута к www.mail.ru [91.198.174.2] с максимальным числом прыжков 30:

1 1 ms <1 ms <1 ms vpn4.kras.gldn [10.10.1.14]

2 2 ms <1 ms <1 ms C7604-BRAS4-FTTB.ranetka.ru [80.255.150.41]

3 1 ms 1 ms 4 ms C76-External.ranetka.ru [80.255.128.162]

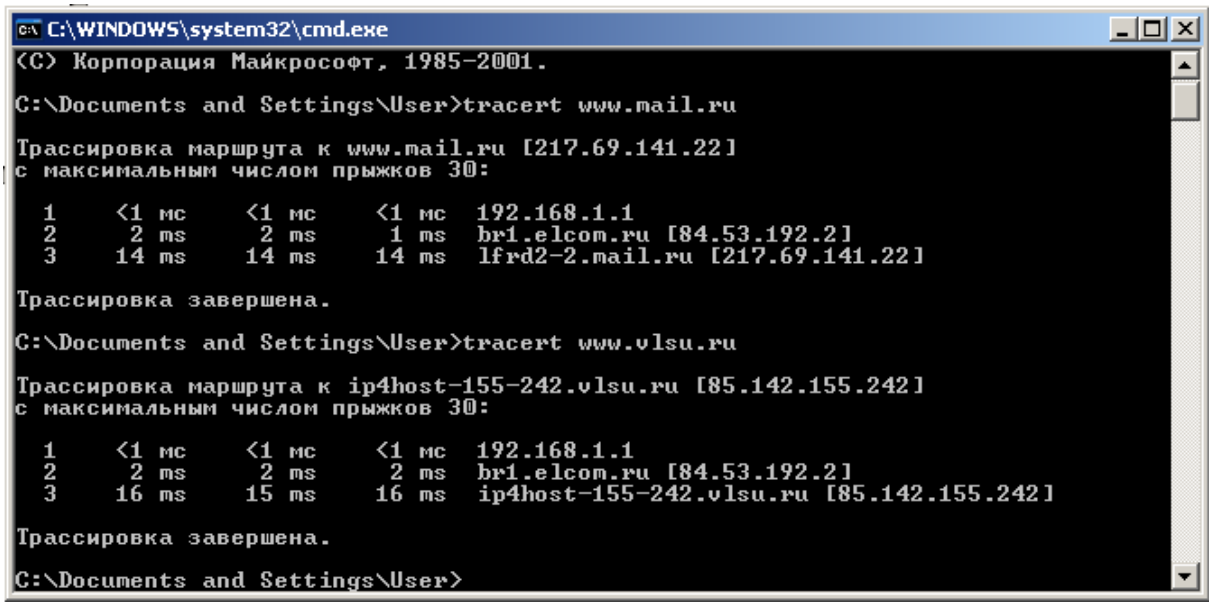
4 1 ms <1 ms <1 ms pe-l.Krasnoyarsk.gldn.net [195.239.173.37]

5 79 ms 79 ms 98 ms cat01.Stockholm.gldn.net [194.186.157.62]

6 131 ms 131 ms 132 ms ams-ix.2ge-2-1.br1-knams.mail.org [195.69.145.176]

7 131 ms 131 ms 131 ms te-8-2.csw1-esams.mail.org [91.198.174.254]

8 133 ms 134 ms 133 ms mail.org [91.198.174.2]



Как обычно, имя машины может быть задано в символической или числовой формах. Выходная информация представляет собой список машин, начиная с первого шлюза и кончая пунктом назначения. Кроме того, показано полное время прохождения каждого шлюза.

Команда traceroute работает путем установки поля времени жизни (числа переходов) исходящего пакета таким образом, чтобы это время истекало до достижения пакетом пункта назначения. Когда время жизни истечет, текущий шлюз отправит сообщение об ошибке на машину-источник. Каждое приращение поля времени жизни позволяет пакету пройти на один шлюз дальше.

Команда traceroute посылает для каждого значения поля времени жизни три пакета. Если промежуточный шлюз распределяет трафик по нескольким маршрутам, то эти пакеты могут возвращаться разны

ми машинами. В этом случае на печать выводятся они все. Некоторые системы не посылают уведомлений о пакетах, время жизни которых истекло, а некоторые посылают уведомления, которые поступают обратно на машину-источник только после того, как истекло время их ожидания командой traceroute. Эти шлюзы обозначаются рядом звездочек. Даже если конкретный шлюз определить нельзя, traceroute чаще всего сможет увидеть следующие за ним узлы маршрута.

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Изучить утилиту ping.

2. Произвести трассировку узлов www.mail.ru, www.rome- guide.it, www.novol.pl,www.newslink.org или любых других по желанию, но не менее 7 узлов.

3 С помощью команды ping проверить состояние связи с узлами pds.sut.ru (каф. ОПДС), www.sut.ru (ГУТ), www.spb.ru (С-Петербург), www.mail.ru (Москва) - обязательно; www.romeguide.it (Италия), www.novol.pl (Польша), www.newslink.org (США) или другими по желанию, но не менее 7-и узлов. Число отправляемых запросов рекомендуется взять равным 20.

Результаты исследований представить в таблице:

Доменное имя	IP-адрес	Страна	Число потерянных запросов, %	Среднее время прохождения запроса, мс	255 - TTL

4 Представить графики статистической информации.

5 Произвести трассировку узлов www.mail.ru, www.romeguide.it, www.novol.pl, www.newslink.org или любых других по желанию, но не менее 7-и узлов. Результаты протоколировать в файл st.log.

6 Описать маршрут прохождения для двух выбранных узлов (страна, город, сеть).

7 Представить графики времени прохождения шлюзов для каждого узла (для 3-х пакетов), указать наиболее узкие места в сети.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Результаты тестирования.
2. Таблица с результатами исследований согласно п.3
3. Графики статистической информации согласно п.4.
4. Листинг произведенной трассировки узлов
5. Описание маршрута прохождения трассировки.
6. Графики времени прохождения шлюзов (по количеству узлов) с анализом узких мест сети.

6. Контрольные вопросы

1. Для чего применяется утилита ping?
2. Каков формат команды ping?
3. Что можно определить с помощью утилиты ping?
4. Для чего применяется утилита traceroute?
5. Каков формат команды traceroute?
6. Что можно определить с помощью утилиты traceroute?

Литература

1. Карлинг М., Деглер С., Деннис Дж. Системное администрирование Linux.: Пер. с англ.: Уч. пос. – М.: Издательский дом "Вильямс", 2000
2. Немет Э., Снайдер Г., Сибасс С., Хейн Т. Р. UNIX: руководство системного администратора: Пер. с англ. – К.: BHV, 1997.
3. Кирх О. Linux для профессионалов. Руководство администратора сети. – СПб: Издательство "Питер", 2000.
4. Ping и Traceroute // CITFORUM.RU Форум высоких технологий.
5. Вопросы о ping-е // CITFORUM.RU : Форум высоких технологий. 2011. URL: http://citforum.ru/internet/articles/ping/ (дата обращения: 20.05.2012).
6. Ping и Traceroute // CITFORUM.RU Форум высоких технологий. 2011. URL: http://citforum.ru/nets/semenov/4/45/ping_451.shtml (дата обращения: 20.05.2012).
7. Фигурнов, В.Э. IBM PC для пользователя / В.Э. Фигурнов. - Изд. 5-е, испр. и доп. - СПб. : Коруна : Информатика и компьютеры, 1994. - 352 с. - ISBN 5-87672-002-X. 2011. URL: http://citforum.ru/nets/semenov/4/45/ping_451.shtml (дата обращения: 20.05.2012).
8. Фигурнов, В.Э. IBM PC для пользователя / В.Э. Фигурнов. - Изд. 5-е, испр. и доп. - СПб. : Коруна : Информатика и компьютеры, 1994. - 352 с. - ISBN 5-87672-002-X.
9. Кушнир, А.Н. Новейшая энциклопедия компьютера / А.Н. Кушнир. - М. : Эксмо, 2008. - 975 с. - (Новейшая энциклопедия). -ISBN 978-5-699-24136-1.

Лабораторная работа № 4

ДИНАМИЧЕСКАЯ РАЗДАЧА IP АДРЕСОВ ШИРОКОПОЛОСНЫМ МАРШРУТИЗАТОРОМ

Цель работы: Перевод компьютеров со статических IP адресов на динамическую раздачу IP адресов. Получение работы с широкополосным маршрутизатором.

Аппаратура: ПК, роутер Dlink DIR-120

Программное обеспечение: ОС Windows

Общие сведения

Широкополосный маршрутизатор (роутер) D-Link DIR-120 разработан для совместного доступа группы пользователей к широкополосному Интернет-соединению через выделенную линию, DSL или кабельный модем. Маршрутизатор оснащен одним USB-портом и 4-мя портами 10/100 Мбит/с, обеспечивая готовое подключение для рабочей группы посредством сетевых кабелей Ethernet. DIR-120 успешно сочетает в себе функции коммутатора Ethernet и принт-сервера, что обеспечивает сохранение инвестиций пользователя. К тому же, установить и обслуживать одно устройство, как правило, гораздо проще. Работа с DIR-120 проста и удобна, благодаря чему этот маршрутизатор идеально подходит для использования как домашними и офисными пользователями, создающими свою первую сеть, так и более продвинутыми пользователями.

TCP/IP должен быть правильно настроен у каждого компьютера в сети. Это означает, что на каждом компьютере должны быть настроены IP-адрес, сетевая маска, адрес сетевого шлюза, адрес DNS-сервера и т.д. Если специалисту необходимо настроить вручную большое количество компьютеров в сети, тяжело избежать ошибок, например использования одного адреса дважды, что может вызывать коллизии и зачастую нарушать работу сети в целом.

Для облегчения задачи был создан протокол динамического конфигурирования хоста (Dynamic Host Configuration Protocol, DHCP), используемый для динамической настройки протокола TCP/ip на клиентских машинах. Во время загрузки компьютера с DHCP-клиентом, посылается запрос. При его получении DHCP-сервером он выбирает параметры настройки TCP/IP для клиента, такие как IP-адрес, сетевая маска, шлюз, адрес DNS-сервера, имя домена клиента и т.п. Используя эти параметры, сервер формирует ответ и отсылает его клиенту. Конфигурация, назначенная клинету сервером, действует ограниченное время (так называемое "время аренды"). Сервер всегда назначает IP-адрес, не совпадающий с другими адресами, использованными DHCP-сервером другим клиентам.

Порядок выполнения работы

Вход в WEB-интерфейс обеспечивается по средствам браузера. Для входа в него, требуется запустить любой установленный на компьютере

браузер и в окне ввода адреса сайта, ввести IP-адрес маршрутизатора (по умолчанию 192.168.0.1). Имя пользователя стандартное (admin), пароль отсутствует (рис.1).

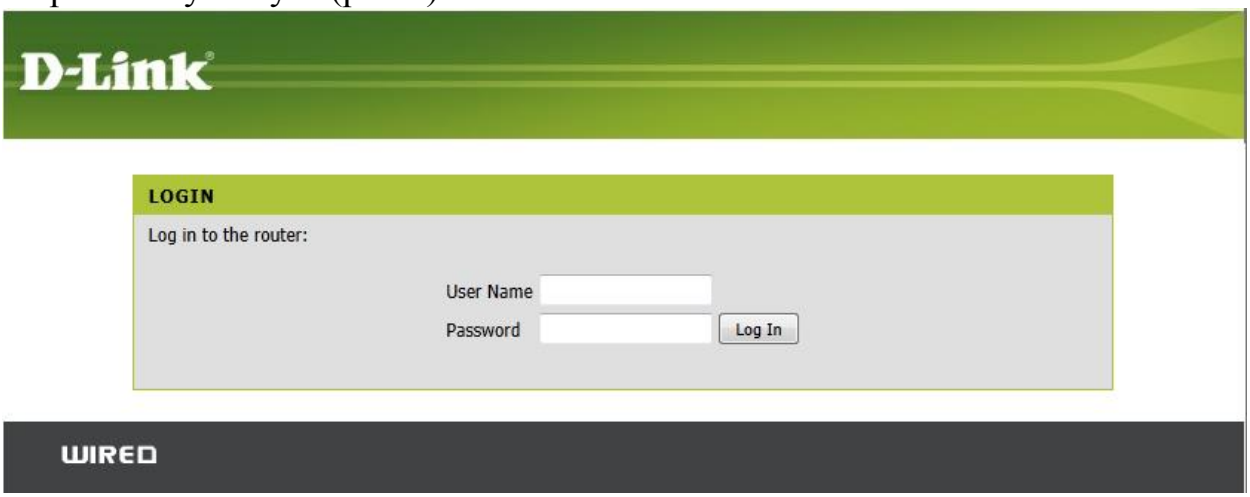


Рис.1

Для сохранения конфигурации через WEB-интерфейс необходимо нажать кнопку «Save Settings» (рис.2).

Настройка IP-адреса роутера производится в меню SETUP | LAN SETUP | Router settings. Необходимо задать IP-адрес и маску из диапазона IP-адресов сети аудитории. Маска подсети должна соответствовать маске подсети коммутатора второго уровня. Для работы DHCP сервера необходимо активировать функцию «Enable DHCP Server» (Рис.4). Маска подсети указывается в поле «Default Subnet Mask» (Рис.2). IP-адрес роутера указывается в поле «Router IP Adress» (Рис.2)

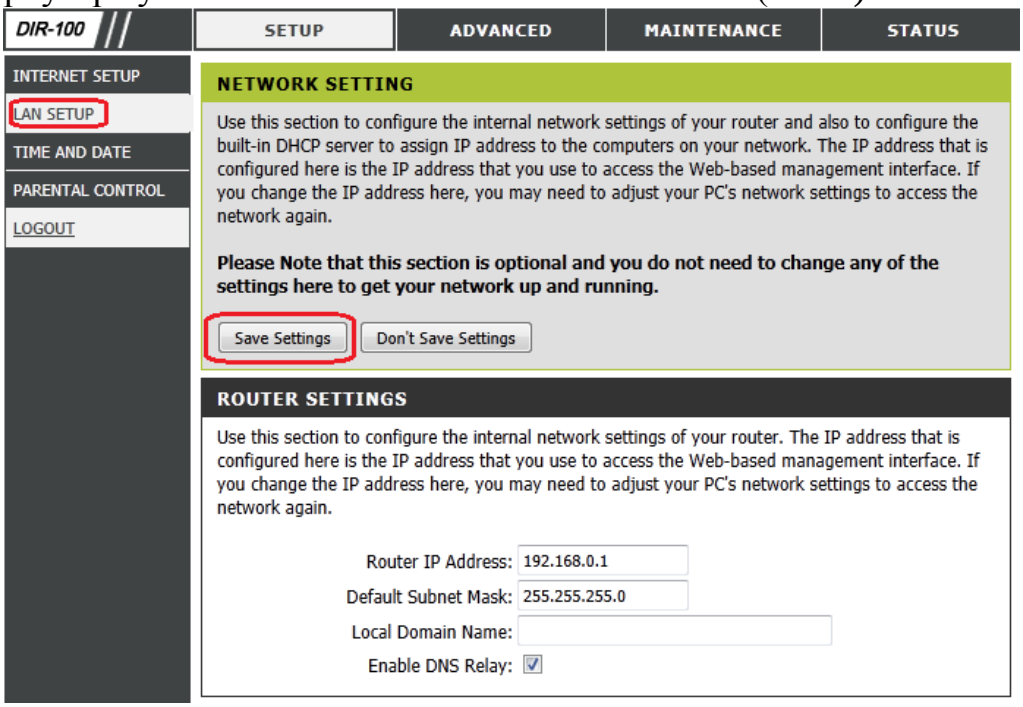


Рис.2

Что бы указать диапазон IP-адресов, необходимо ввести диапазон последнего байта IP-адреса в поля «DHCP IP Address Range» (Рис.4). Этот диапазон, должен быть строго больше последнего байта IP-адреса роутера.

Пример: IP-адрес роутера 192.168.1.70, тогда диапазон допустимых IP-адресов будет 192.168.1.71 – 192.168.1.255. Если указать диапазон 71-100, то IP-адреса будут находиться в диапазоне 192.168.1.71 – 192.168.1.100.

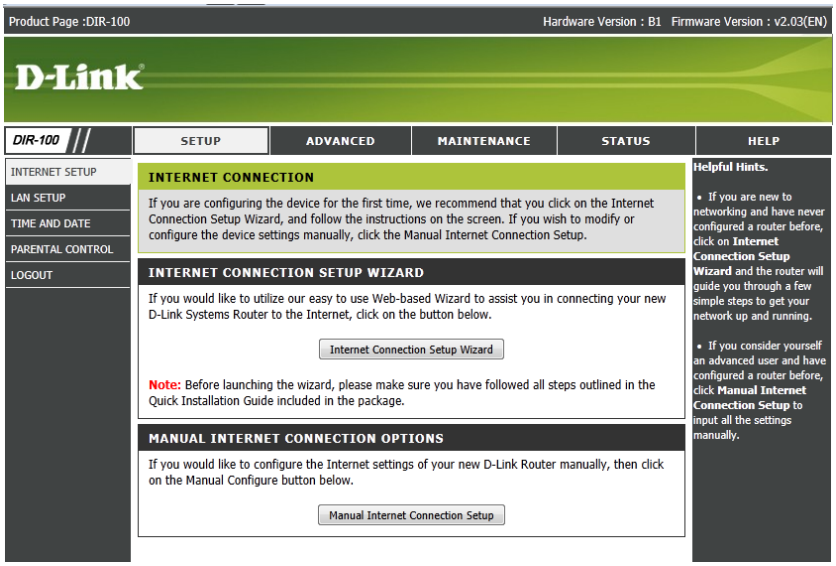


Рис.3

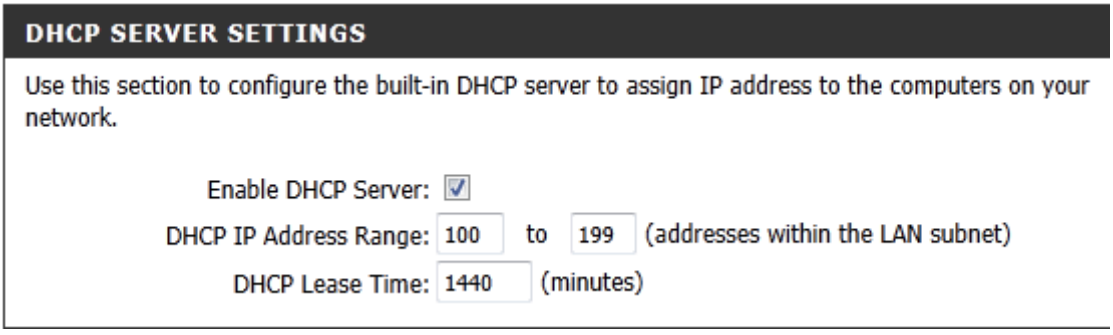


Рис.4

ОБЖИМ СЕТЕВОГО КАБЕЛЯ.

Для обжима сетевого кабеля используются стандартные разъемы RJ-45, которые в зависимости от вида "витой пары" бывают экранированными и неэкранированными, так же различают разъёмы для одножильных или многожильных "витых пар". Конструктивно можно выделить составные разъёмные, выполненные со вставками и монолитные. Вставки являются направляющими, для проводников и упрощают заправку кабеля, но с точ-

ки зрения надёжности они уступают монолитным вариантам. Пример разъема RJ-45 b и **обжимного устройства** UTP.

Рис.5

Вначале осуществляется зачистка наружной изоляции кабеля, можно использовать или специальные клещи или аккуратно снять изоляцию обычными ножницами. Необходимый уровень зачистки кабеля – 1,2-1,5 см. При этом зачищать оплетку необходимо таким образом, что бы она была прижата зажимом коннектора, при этом провода должны упираться в торец коннектора. Если витая пара экранирована, то заземление не срезается, а укладывается с разворотом в 180 градусов по направлению кабеля. После зачистки необходимо развести жилы "витой пары" в одной плоскости и выравнить их по длине. После данной подготовки производят заправку жил в разъем и их прессовку. После изготовления сетевого шнурка, его нужно прозвонить тестером или опробовать на оборудовании.

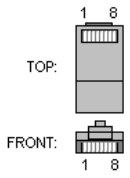
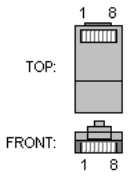
При организации сети по каналу 100 Мбит/сек используются 2 пары витой пары и используются жилы 1, 2 , 3 и 6. При организации гигабитной сети используются 4 пары, т.е. все 8 жил витой пары.

Рис.6

Рис.7

В сети Ethernet существует два типа кабелей. Первый тип используется для прямых соединений (хаб-свитч, компьютер-хаб) и кроссовер, который используется в локальных компьютерных сетях для прямого соединения двух компьютеров, без хаба. Тип кабеля для соединения разных портов можно выбрать по нижеприведённой таблице:

1.При соединении Computer-Hub/Switch (карта-хаб/свитч) используется следующая схема:

С одной стороны	С другой стороны
 **1: Бело-оранжевый** **2: Оранжевый** **3: Бело-зелёный** **4: Синий** **5: Бело-синий** **6: Зелёный** **7: Бело-коричневый** **8: Коричневый**	 **1: Бело-оранжевый** **2: Оранжевый** **3: Бело-зелёный** **4: Синий** **5: Бело-синий** **6: Зелёный** **7: Бело-коричневый** **8: Коричневый**

2. При соединении двух компьютеров crossover (карта-карта) используется следующая схема обжима:

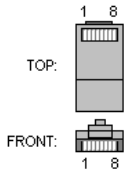
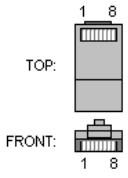
С одной стороны	С другой стороны
 **1: Бело-оранжевый** **2: Оранжевый** **3: Бело-зелёный** **4: Синий** **5: Бело-синий** **6: Зелёный** **7: Бело-коричневый** **8: Коричневый**	 **1: Бело-зеленый** **2: Зеленый** **3: Бело-оранжевый** **4: Синий** **5: Бело-синий** **6: Оранжевый** **7: Бело-коричневый** **8: Коричневый**

Рис.8

Для проверки работоспособности обжатого кабеля следует воспользоваться специальным прибором. Пример такого устройства изображен на рисунке 9. Перед использованием прибора необходимо ознакомиться с инструкцией данного прибора.

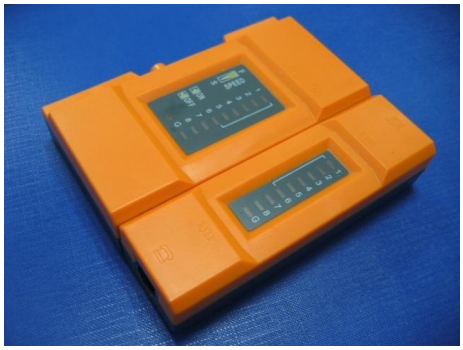


Рис.9

Рабочее задание

1. Обжать кабели для соединения компьютера с роутером. (По возможности протестировать специальным тестером).
2. Подключить роутер к локально сети и подключить к нему компьютер (порт WAN не используется).
3. Визуально убедиться в том, что необходимый кабель подключен к коммутатору и роутеру;
4. Настроить компьютер на работу с динамическим IP адресом (см. лаб1);
5. Попытаться зайти в WEB-интерфейс роутера;
6. Произвести настройку IP-адреса роутера, маску подсети и диапазон IP адресов сервера (DHCP);
7. Выполнить команду PING до роутера, до коммутатора и до компьютера в сети (например компьютера преводавателя). Оценить время PING-а;
8. Основываясь на лабораторной работе по настройке WI-FI (лаб.2), настроить фильтр по MAC адресам.

Лабораторная работа №5

НАСТРОЙКА ВЕБ-СЕРВЕРА

Цель работы: Изучение настройка веб-сервера, на примере утилиты HFS (HTTP File Server) и устройств Allied Telesis AT-8000S и Allied Telesis AT-8624T.

Аппаратура: ПК, коммутаторы Allied Telesis AT-8000S и Allied Telesis AT-8624T.

Программное обеспечение: тилита HFS (HTTP File Server)

Общие сведения

Веб-сервер — это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными. Веб-серверы — основа Всемирной паутины.

В данной работе, будет изучаться настройка веб-сервера, на примере утилиты HFS (HTTP File Server) и устройств Allied Telesis AT-8000S и Allied Telesis AT-8624T.

Эти устройства являются управляемыми коммутаторами 2-го и 3-го уровня соответственно. Настройка первого была детально рассмотрена в лабораторной работе №1. Настройка второго не составляет большого труда.

HTTP File Server — бесплатная программа, разработанная итальянским программистом Массимо Мелина (Rejetto), позволяющая очень быстро организовать файловый HTTP веб-сервер в ОС Windows.

Изначально программа разрабатывалась для публикации пользователем файлов во всемирной сети. Благодаря широким возможностям настройки, программу можно использовать как полноценный веб-сервер для Windows.

HTTP File Server даёт возможность выбора папки (или папок), доступной из сети или из Интернета. Можно установить доступ как для всех, так и только для избранных — в этом случае доступ к файлам будет открыт только после ввода пароля. Кроме этого, можно устанавливать ограничения на тип доступных для скачивания файлов (zip, rar и т. п.). Наконец, для дополнительной безопасности допускается размещать общедоступные папки на виртуальной файловой системе. Из дополнительных удобств следует отметить допустимость написания к каждой из расшаренной папке комментария, который будет видеть пользователь, решивший в нее заглянуть. Работает без инсталляции, поддерживает докачку файлов, есть неплохая статистика (в том числе работающая в реальном времени), при использовании нескольких сетевых карт из них можно выбрать ту, на которой будет работать HTTP File Server.

Основные достоинства HFS:

- Не требуется установка программы (инсталляция)
- Небольшой размер запускаемого файла
- Учётные записи пользователей,
- Разграничение прав

- Ограничение скорости трафика
- Возможность скачивания/загрузки файлов

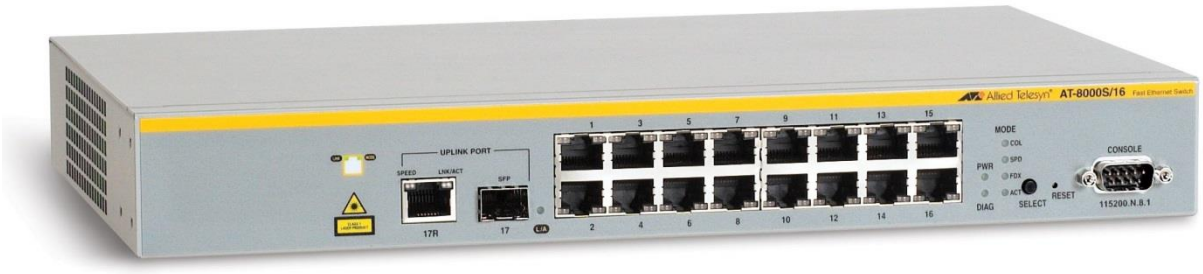


Рис.1

Перед началом работы, необходимо убедиться, что коммутаторы находятся во включенном состоянии (у обоих горят или мигают зеленые светодиоды на передней панели). Фотография коммутатора второго уровня приведена на рис.1, третьего уровня на рис.2. На рис.2 находятся модули, которые могут отсутствовать, т.к. не требуются в данной работе.

Рис.2

Компьютеры, должны быть ОБЯЗАТЕЛЬНО подключены по Ethernet к четным розеткам. Необходимо убедиться, что кабель с соответствующим (четным) номером подключен к коммутатору 3-го уровня (Рис.2). Коммутатор 3-го уровня должен быть соединенным сетевым кабелем с коммутатором 2-го уровня. Коммутатор 2-го уровня должен быть настроен согласно лабораторной работе №1.

Далее следует убедиться, что на двух компьютерах есть программа HFS. При распаковке/установке, ярлык программы в Windows 7 появляется в «Пуск → Все программы → Утилиты». Внешний вид ярлыка приведен на рис.3.

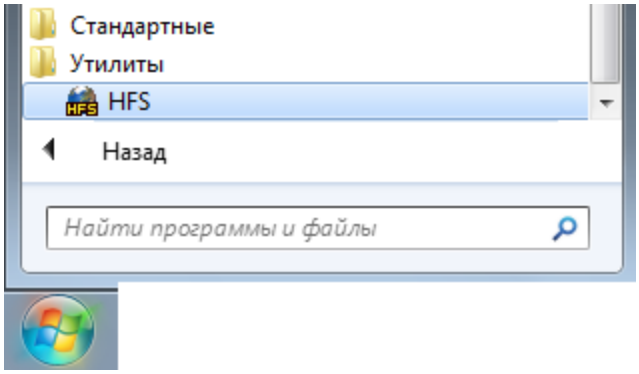


Рис.3

Один из компьютеров будет выступать в роли сервера, другой в роли клиента. Рассмотрим настройку компьютера-сервера.

Если приложение запускается впервые, то оно предложит создать файл файловой системы. Этот файл служебный, в нем хранятся различные пути к файлам и описания. Его лучше сохранить на диске. Эта операция представлена на рис.4 и рис.5.

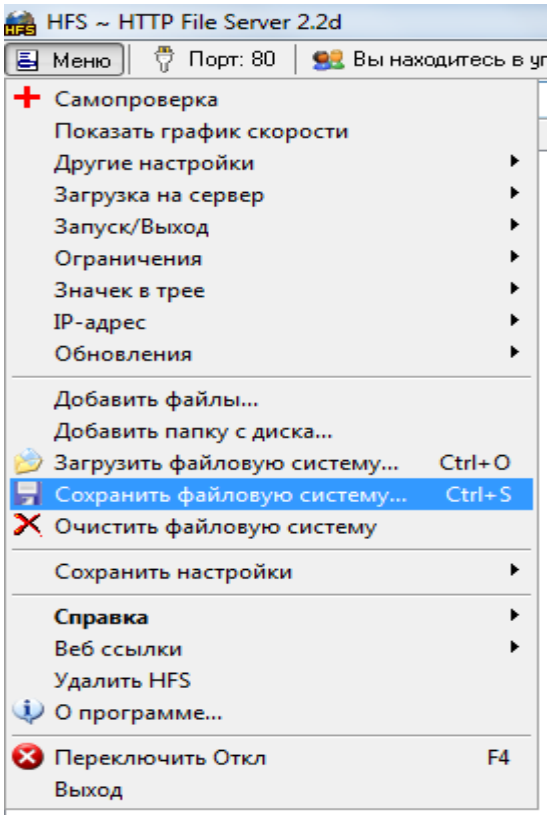


Рис.4

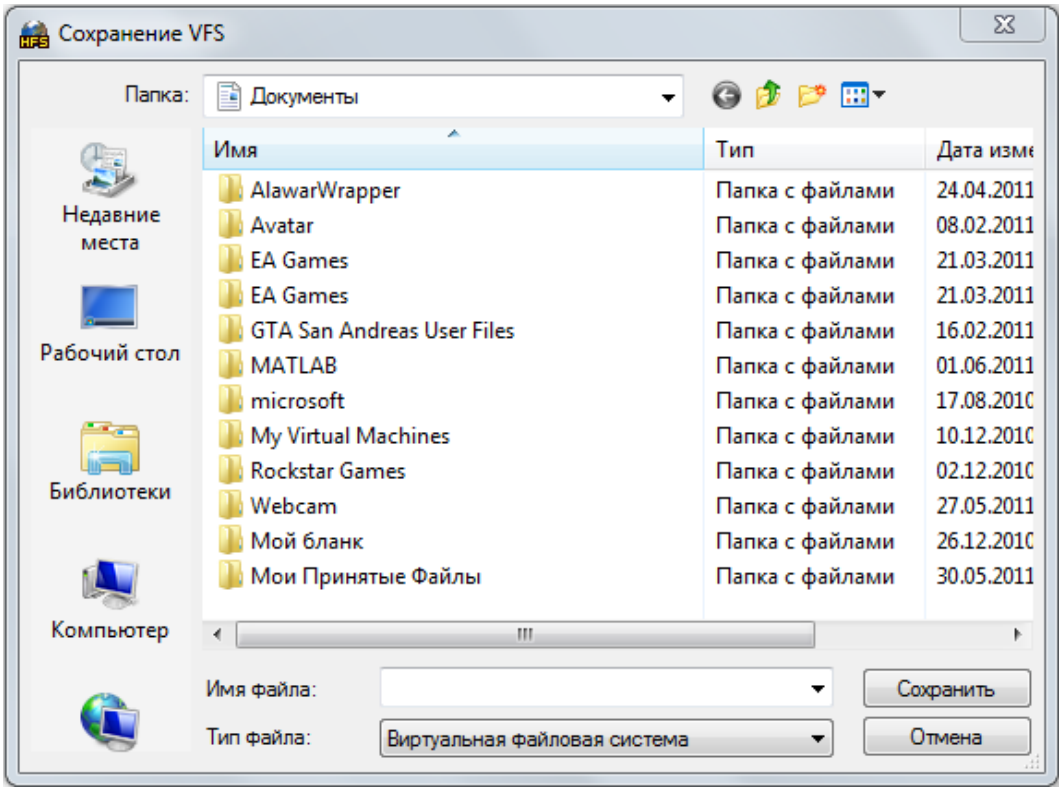


Рис.5

В поле «Имя файла» указать имя файла виртуальной файловой системы (лучше латиницей) и сохранить.

Если приложение запускается не впервые, то оно по умолчанию будет обращаться к ранее созданному файлу. По умолчанию этот файл сохраняется в «Документах».

Далее следует выбрать внутрисетевой IP-адрес. Для этого нужно нажать по кнопке «Меню» в верхнем левом углу. Выбрать курсором «IP-адрес» и поставить галочку напротив заданного ранее (см. лаб. работу №1).

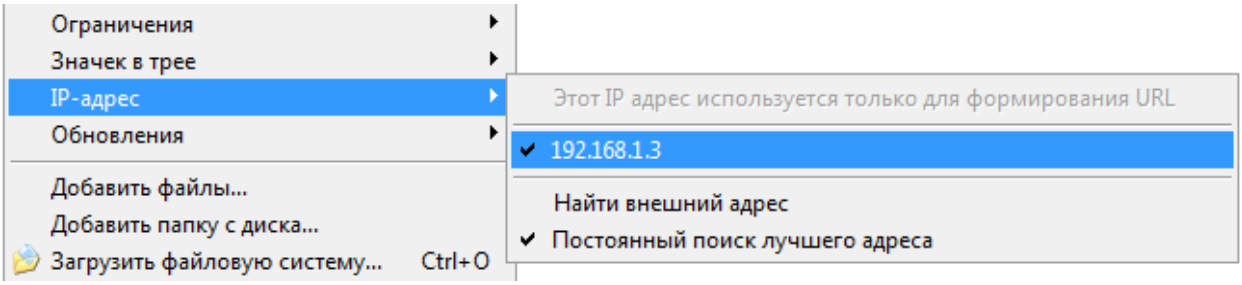


Рис.6

Также следует указать порт, по которому будет происходить обращение к серверу. Порт для подключения представляет собой цифру (по умолчанию 80). Эта функция нужна, например, в том случае, когда на сервере стоит утилита Apache выводящая по стандартному (80) порту веб-сайт. Порт может содержать до 4 цифр.

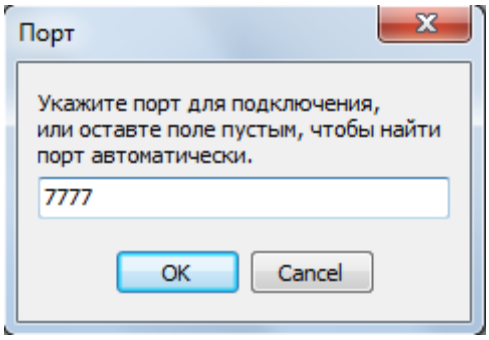


Рис.7

Уже после этого можно выкладывать файлы и целые папки в общий доступ. Для этого нужно в том же «Меню» выбрать «Добавить файлы…» или «Добавить папку с диска…» и следовать указанием утилиты. При добавлении папки программа предложит выбрать тип этой папки (Рис.8)

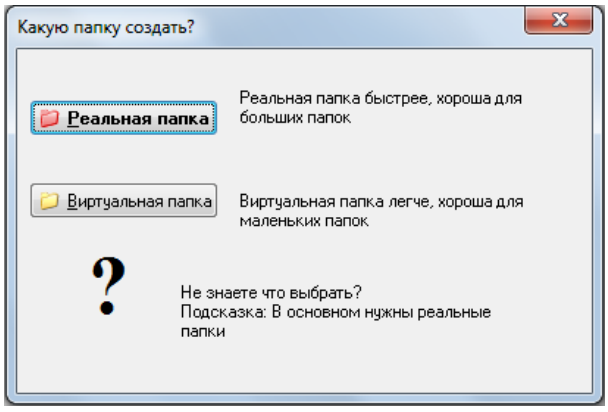


Рис.8

После добавления файлов и папок они должны появиться в столбике «Виртуальная файловая система» (Рис.9).

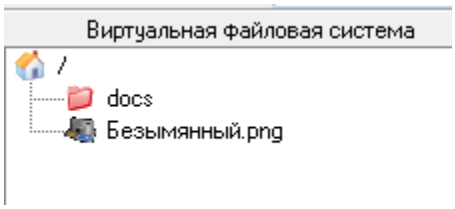


Рис.9

Для того, чтобы просмотреть веб-интерфейс HTTP File Server нужно нажать на клавишу «Открыть в браузере». Она находится в левом верхнем углу рядом со строкой адреса. Если вы все правильно сделали, то у вас автоматически откроется браузер, в котором вы увидите примерно следующую картину:

Рассмотрим различные ограничения, позволяющие пользователя сервера обезопасить себя от некоторых неприятностей. Например, ограничение по скорости и запрет загрузок в несколько каналов. Ограничение по скорости вызывается из «Меню → Ограничения → Ограничение по скорости», которое записывается в Кб/с. Ограничение «Не допускать личеров (акселераторы загрузки)» позволяет обезопасить сервер от закачек в несколько потоков. Скачивание в несколько потоков сильно забивает канал связи, и в некоторых условиях является неприемлемым для сервера. Если же требуется побыстрей передать файл – то это ограничение можно снять. И тогда пользователь компьютера-клиента, посредством специальных программ (Download Master, Flash Get) может быть ограничен в скорости только плотностью своего канала.

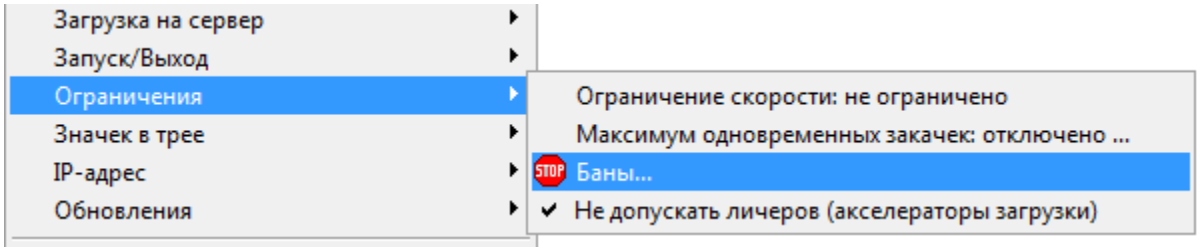


Рис.10

Также в ограничениях есть функция «Баны…» (Рис.10). Бан — один из принятых в Интернете способов контроля за действиями пользователей. Как правило, бан заключается в лишении или ограничении каких-либо прав пользователя. В данном случае бан запрещает скачивание и

загрузку файлов. Бан представляет из себя список IP-адресов и масок, которым запрещено скачивать и закачивать файлы на сервер. В этой же форме можно и убрать адреса.

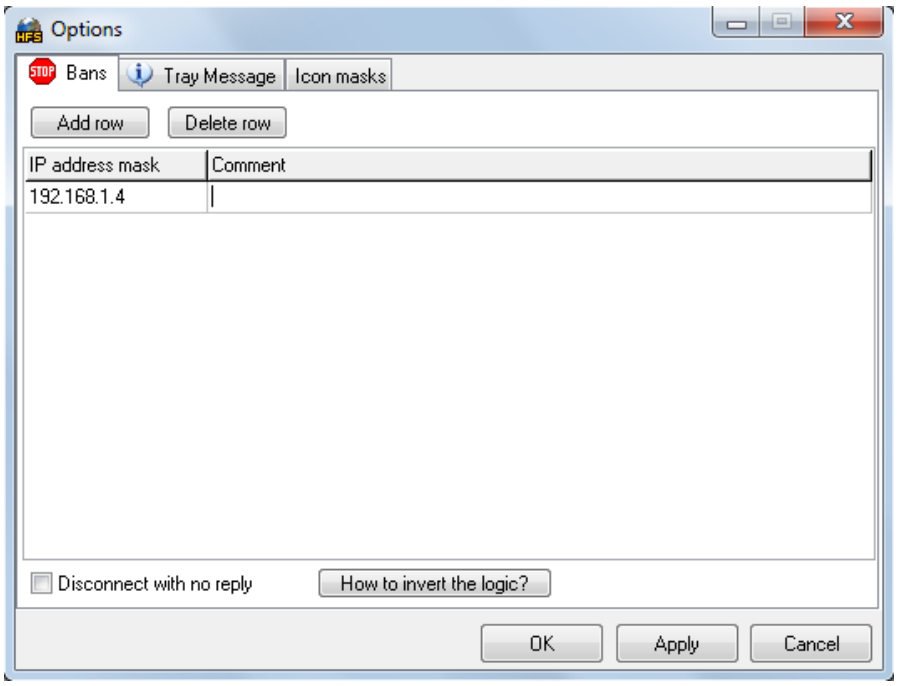


Рис.11

Помимо скачивания файлов, HFS позволяет клиентам закачивать файлы на сервер в расшаренную папку по сети (Правой кнопкой мыши по выбранной папке «Загрузка → Загрузка для учетной записи» и поставить галочку напротив «Любой»). Можно установить эту функцию для каждой из папок на сервере. Также в утилите есть возможность создавать виртуальную папку (В том же контекстном меню выбрать «Новая папка»).

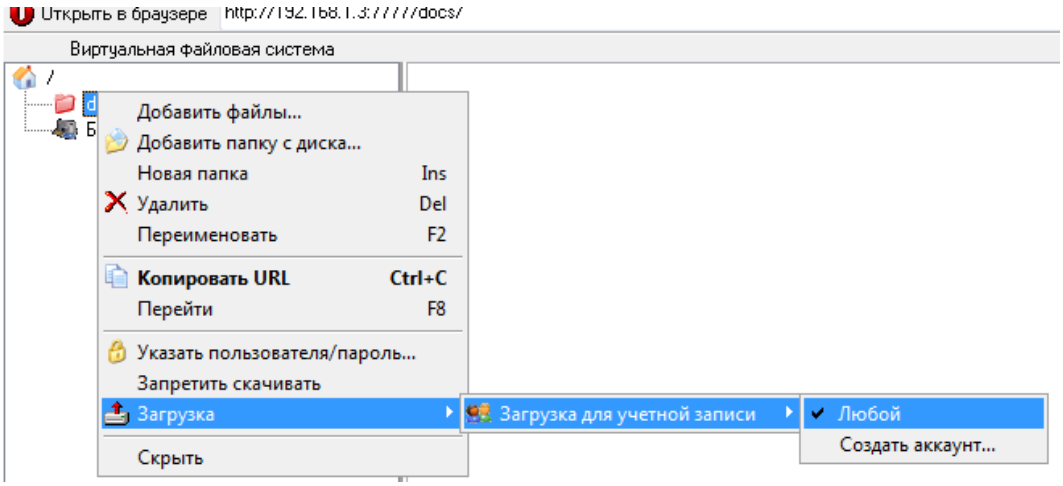


Рис.12

В целях безопасности в HTTP File Server есть функция создания учетных записей. Нужно задать имя и пароль, и выставить различные ограничения, такие как: запрет на скачивание файлов и папок (В контектсном меню на рис.12 «Запретить скачивать → Загрузка для учетной записи» и поставить галочку); запрет на закачку файлов незарегистрированным пользователям (В контектсном меню на рис.12 «Загрузка → Загрузка для учетной записи», убрав галочку напротив «Любой» и поставив её на «Создать аккаунт…»); ограничения по скорости и бан.

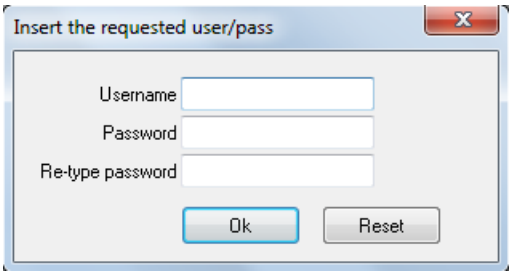


Рис.13

Рассмотрим теперь какие функции предоставляет HFS для компьютера-клиента.

Для этого на другой машине откроем веб-браузер. В адресную строку вставим следующее:

Указание правильного IP-адреса и номера порта обязательно для корректной работы приложений. Далее попробуем скачать файлы с сервера на компьютер клиента. В журнале сервера отображаются все опе-

рации извне. По нему стоит убедиться, что файл действительно скачался.

Скачивать можно и сразу целую папку, используя встроенную в HFS функцию архивации данных.

Попытаемся закачать файлы с клиента на сервер, для этого нужно зайти в папку «upload», созданную ранее, и нажать кнопку «Upload». На открывшейся странице есть поля с кнопками, которыми можно выбрать пути к файлам, которые будем закачивать. Эти закачки также отображаются в журнале и на диаграмме сервера.

Зайдем на сервер под зарегистрированной ранее учетной записью. Для этого нужно нажать кнопку «LOGIN». И ввести нужные значения в поля.

Установив на сервере ограничение: скачивание и закачку файлов только для созданной учетной записи, попытаемся скачать/закачать файлы с компьютера-клиента на сервер.

После окончания работы с HFS нужно сохранять настройки и файловую систему.

Рабочее задание

1. Подключить сетевые кабели к компьютеру таким образом, чтобы они оказались подключенными к коммутатору третьего уровня;
2. Визуально убедиться в том, что необходимый кабель подключен к коммутатору;
3. Узнать IP-адреса компьютеров, за которыми вы работаете;
4. Убедиться, что они статические;
5. Запустить утилиту HFS;
6. Настроить IP-адрес в HFS
7. Выставить порт, например 7777.
8. Сохранить файл виртуальной файловой системы, в указанный преподавателем раздел и папку;
9. Добавить несколько файлов и папок в общий доступ
10. Выставить ограничение по скорости, например в 8 Кб/с.

11.Поставить «Бан» компьютеру-клиенту.

12.Убрать адрес клиента из списка банов.

13.Скачать файлы с сервера на компьютере клиенте

14.Скачать сразу целую папку с сервера на компьютере клиенте

15.Создать новую папку для закачивания файлов на сервер, назвать её именем «upload».

16.Закачать несколько файлов на сервер

17.Создать новую учетную запись и задать пароль для клиента.

18.Разрешить скачивание и закачку файлов на сервер только зарегистрированным пользователям

19.Введя логин и пароль на компьютере клиенте скачать несколько файлов с сервера

20.Введя логин и пароль на компьютере клиенте закачать несколько файлов на сервер

21.Нажать выход из программы, на просьбу «сохранить виртуальную файловую систему» нажать «да».

22.Сохранить настройки в файл.

23.Составить отчет и сделать выводы о проделанной работе.

Лабораторная работа №6

КОНФИГУРИРОВАНИЕ VLAN НА КОММУТАТОРЕ AT-8000S

Цель работы: Ознакомление с принципами и режимами работы коммутатора. Получение навыков конфигурирования портов и VLAN коммутатора.

Аппаратура: ПК, коммутатор Allied Telesis AT-8000S/16

Программное обеспечение: ОС Windows, HyperTerminal

Прежде, чем выполнять работу необходимо сконфигурировать коммутатор таким образом, чтобы выполнялась схема, представленная на рисунке 1.

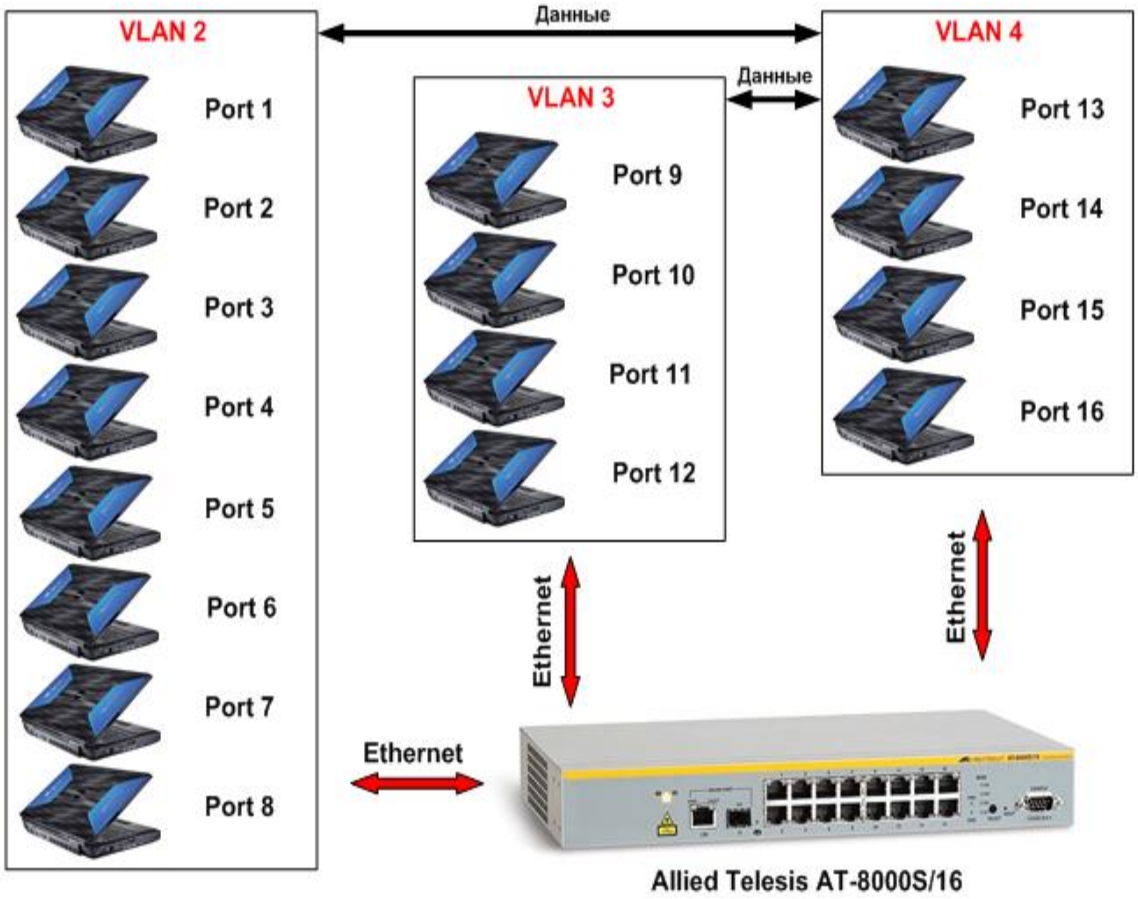


Рис.1 – Схема конфигурирования VLAN на AT-8000S/16

Настроить коммутатор таким образом, чтобы компьютеры, подключенные к портам VLAN 2 и VLAN 3 не могли «видеть» друг друга, а подключенные к портам VLAN 4 могли вести обмен и с портами VLAN 2, и с портами VLAN 3.

Порядок выполнения работы:

1. Настроить программу HyperTerminal

Для этого необходимо выполнить пункт 2 лабораторной работы №3

2. Конфигурирование VLAN на коммутаторе

Для реализации данной схемы необходимо:

1. Создать три VLAN: VLAN 2, VLAN 3, VLAN 4 (VLAN 1 используется для управления коммутатором, поэтому его не используем)

2. Включить порты с 1 по 8 порт во VLAN 2 с возможностью обмена данными с портами VLAN 4

3. Включить порты с 9 по 12 порт во VLAN 3 с возможностью обмена данными с портами VLAN 4

4. Включить порты с 13 по 16 порт во VLAN 4 с возможностью обмена данными с портами VLAN 2 и портами VLAN 3

Для реализации пукта 1 необходимо последовательно ввести следующие команды в HyperTerminal:

```
config
vlan database
vlan 2-4
exit
```

Для реализации пукта 2 необходимо последовательно ввести следующие команды в HyperTerminal:

```
interface range ethernet e(1-8)
switchport mode general
switchport general allowed vlan add 2,4 untagged
switchport general pvid 2
exit
```

Результатом выполненных действий будет набор команд, представленных на рисунке 29.

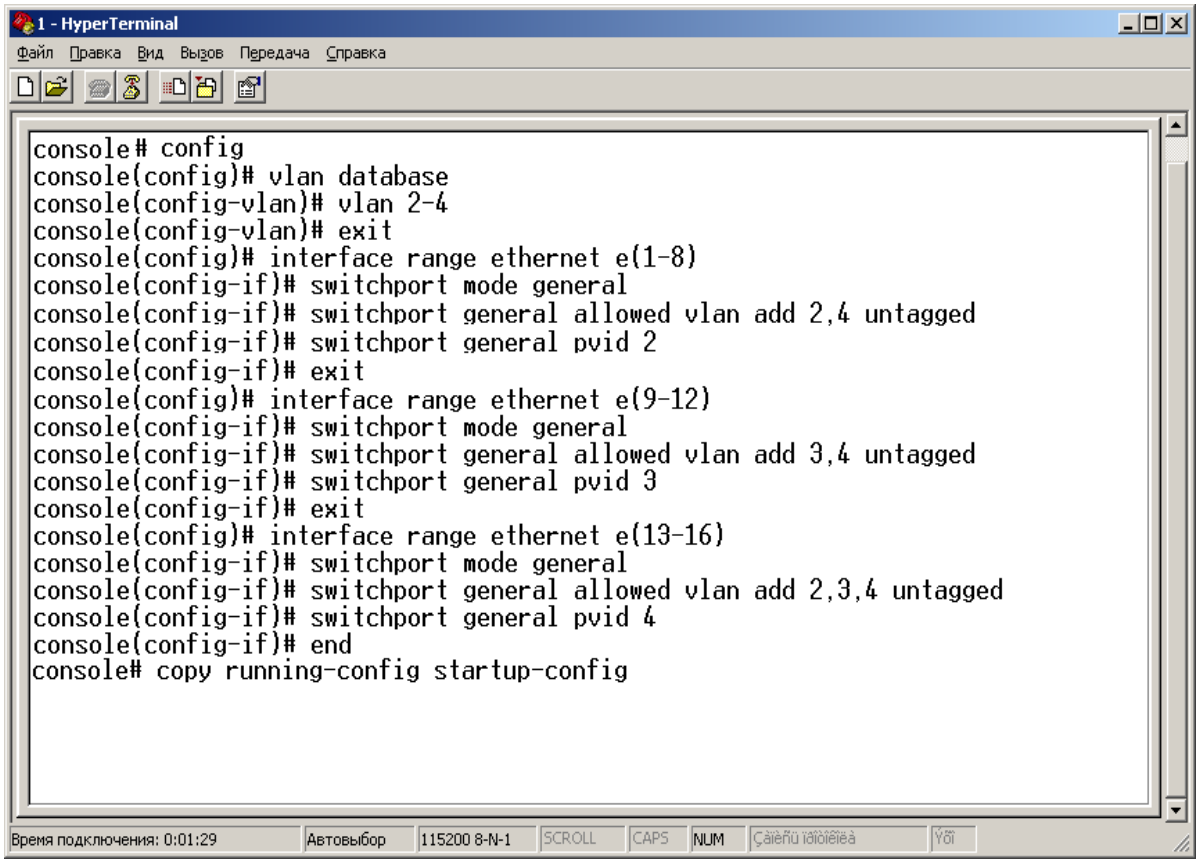


Рис. 2 – Команды конфигурирования в HyperTerminal

Студентам для самостоятельной работы необходимо реализовать на практике пункты 3 и 4, а так же сконфигурировать данную схему через Web-интерфейс Allied Telesis. Для начала работы с Web-интерфейсом необходимо выполнить следующие действия:

1. Подключиться к web-интерфейсу коммутатора

Для этого необходимо:

а) выбрать «Пуск» => «Программы» => «Internet Explorer»

б) в web-браузере прописать в поле адреса внутренний IP-адрес маршрутизатора 100.1.1.1 и нажать «Enter»

Результат выполненных действий представлен на рисунке 30.

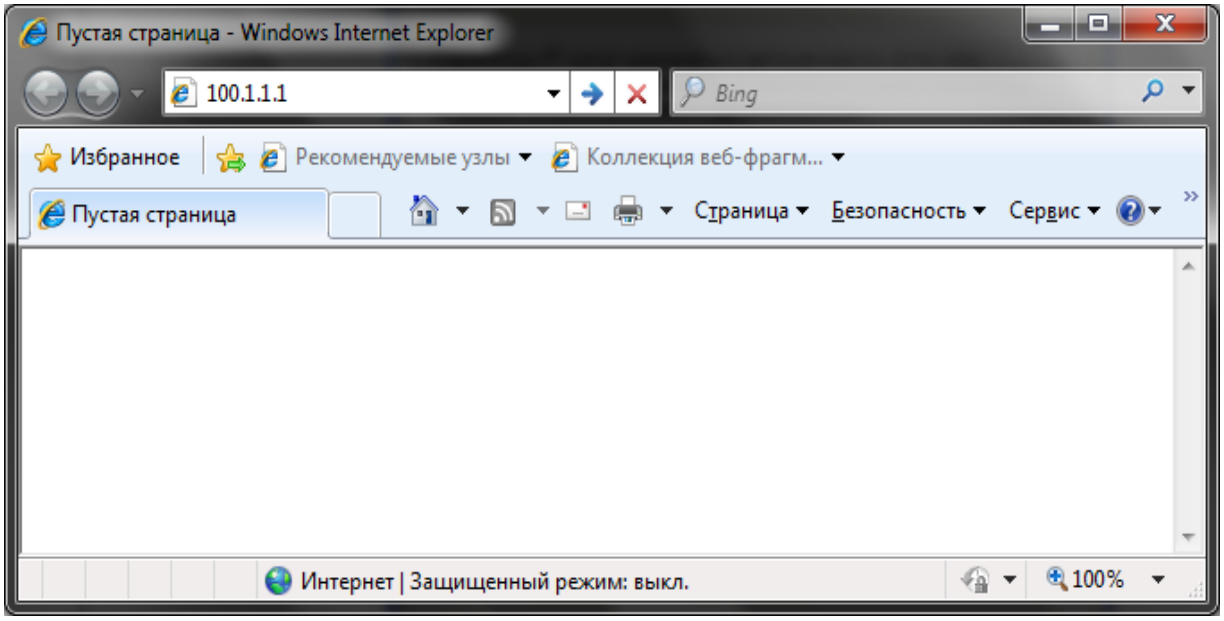


Рис. 3 - Web-браузер Internet Explorer

в) вводим в появившемся окне user name: «manager», password «friend»

Результат выполненных действий представлен на рисунке 31.

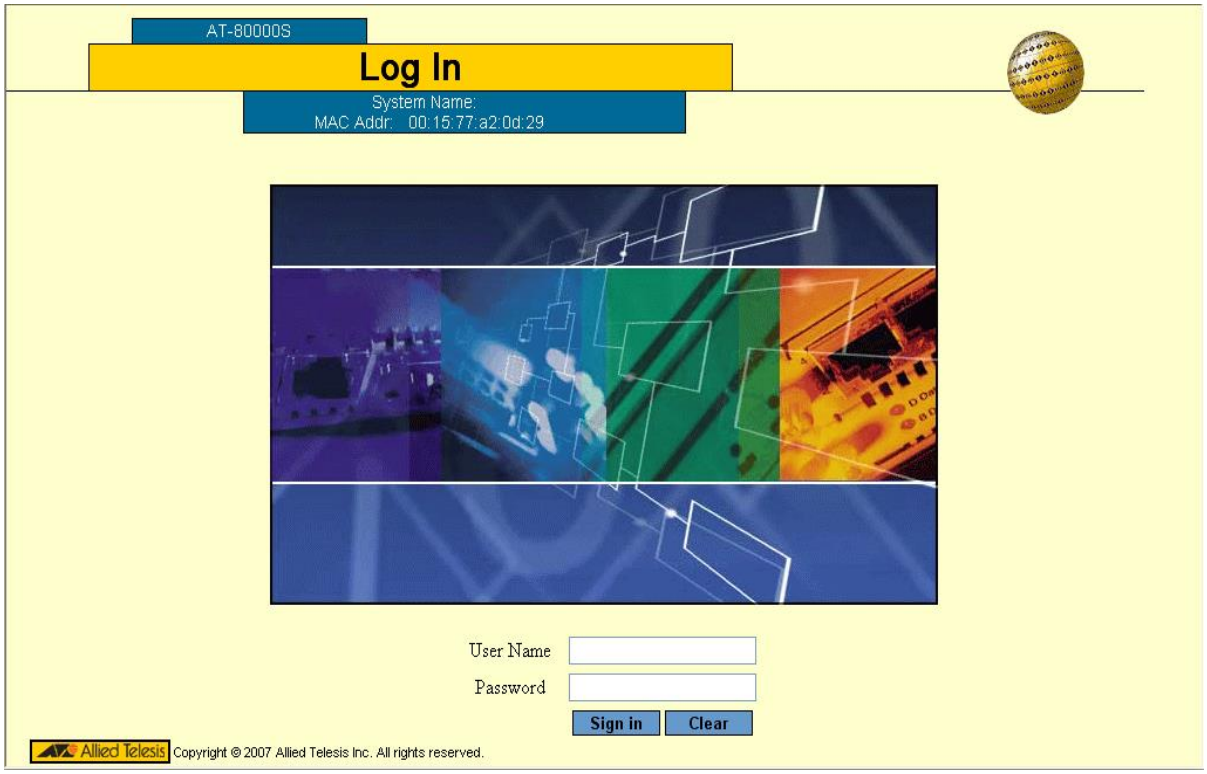


Рис. 4 – Окно входа в web-интерфейс

г) нажать кнопку «Layer 2»

д) на вкладках «VLAN» (рисунок 32) и «VLAN Interface» (рисунок 33) произвести необходимые настройки самостоятельно, согласно заданной схеме, учитывая команды, вводимые в HyperTerminal

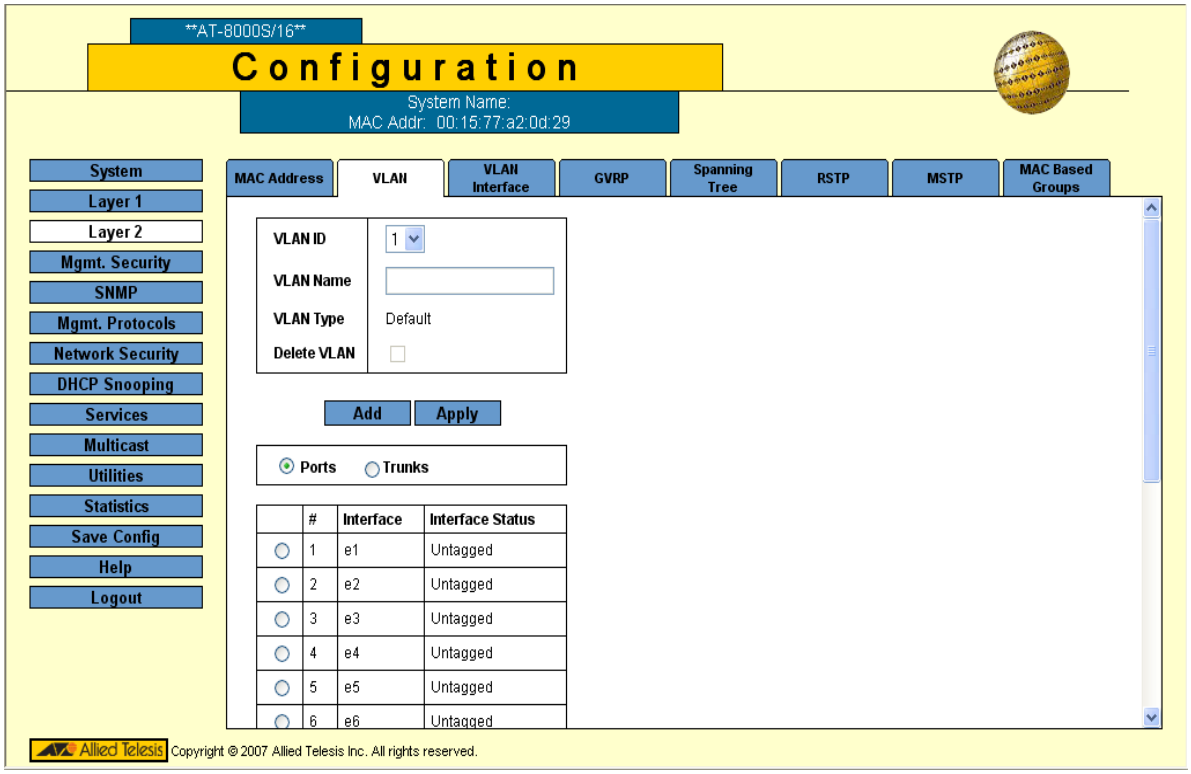


Рис. 5 – Вкладка VLAN

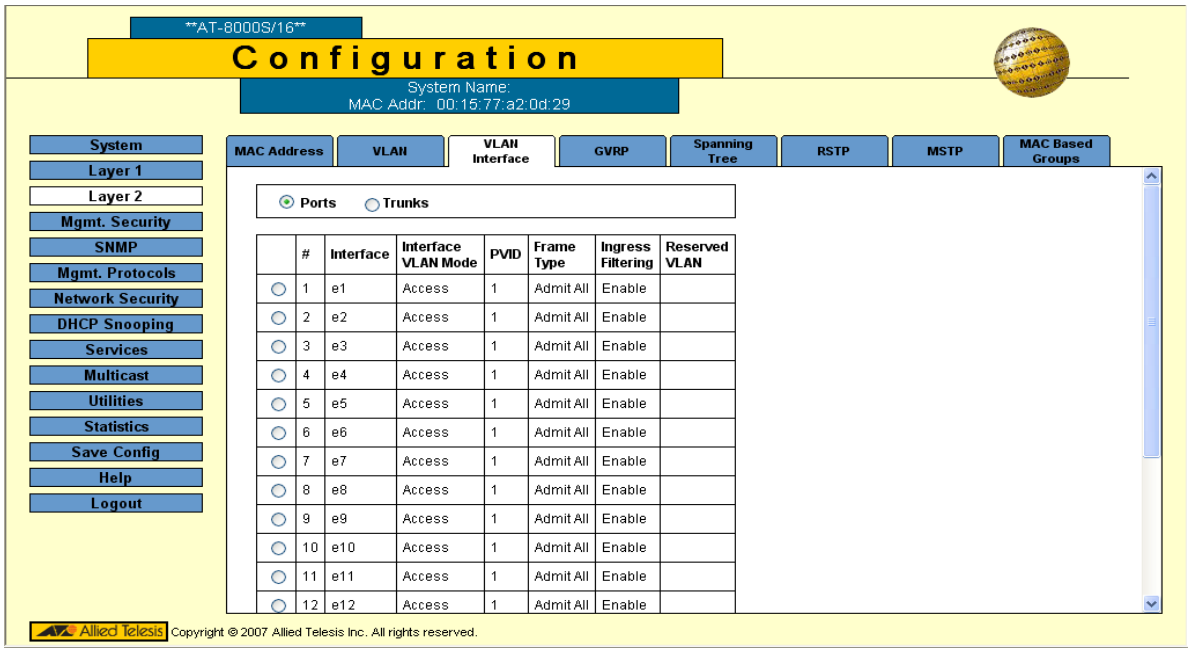


Рис. 6 – Вкладка VLAN Interface

Содержание отчета:

1. Цель работы
2. Краткие теоретические сведения
3. Описание возможностей коммутатора
4. Результат выполненных действий в виде скриншотов с пояснениями
5. Вывод по выполненной работе

Контрольные вопросы

1. Что такое коммутатор?
2. Какие способы коммутации существуют?
3. Что такое таблица коммутации?
4. Для чего нужна программа HyperTerminal?
5. Что такое VLAN?
6. Какие порты называют нетегированные?
7. Какие порты называют тегированные?
8. Назовите основные команды HyperTerminal

Лабораторная работа №7

НАСТРОЙКА ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ VLAN

Цель работы: Ознакомление с принципами и режимами работы сетей, получение навыков настройки виртуальных локальных сетей VLAN.

Аппаратура: ПК, коммутатор Allied Telesis AT-8000S/16
Программное обеспечение: ОС Windows, HyperTerminal

1. Теоретические сведения

VLAN (от англ. *Virtual Local Area Network*), *VLAN* могут являться частью большего *LAN*, имея определенные правила взаимодействия с другими *VLAN*, либо быть полностью изолированными от них.

Наиболее простой вариант использования *VLAN* заключается в отнесении каждого порта одного коммутатора к конкретному *VLAN*, что позволяет разделить физический коммутатор на несколько логических. (Например, порты 1-5,7 — это *VLAN* № 3, порты 6,9-12 — *VLAN* № 2). При этом пакеты из одного *VLAN* не передаются в другой *VLAN*.

Однако мы будем рассматривать более сложный способ создания подсетей – VLAN на базе меток (стандарт 802.1q).

Для начала нужно определиться с некоторыми основными понятиями:

- **Тег** – дополнительное поле, вставляемое в пакет *Ethernet*. Тег состоит из нескольких частей, однако нам важна лишь одна – идентификатор подсети (**VID**). Изначально (на выходе сетевой карты компьютера), тег – отсутствует, т.е. **VID не определен;**
- **Метка порта**. У каждого порта коммутатора, для каждой *VLAN* имеется специальная метка, она может принимать три значения: **U**, **T**, **N**. Метки используются в двух случаях.
    - Если на вход коммутатора пришел тегированный пакет. В таком случае коммутатор проверяет свою таблицу меток и принимает решение:
        - Если для *VID* пакета, установлена метка **N**, то пакет игнорируется;
        - В остальных случаях (установлена метка **U** или **T**), пакет заходит в коммутатор.
    - На выходе коммутатора принимается одно из трех решений:
        - Если для соответствующего *VID* пакета, у данного порта коммутатора стоит **N** (*note*), то пакет игнорируется;
        - Если **U** (*untagged*) , то на выходе из коммутатора, *VID* пакета становится неопределенным (отсутствует);

- Если **T** (*tagged*), то на выходе из коммутатора, *VID* пакета сохраняется.

- **PVID порта**. Это идентификатор подсети имеется у каждого порта коммутатора. Он используется лишь в том случае, если на коммутатор поступил пакет с неопределенным *VID*. При заходе в коммутатор такого пакета, его *VID* становится **равен** *PVID* порта.

Для лучшего понимания, рассмотрим несколько примеров (рисунок.1).

Важное замечание! Для удобства объяснения, некоторые компьютеры могут формировать тегированные пакеты. В учебной аудитории – это невозможно.

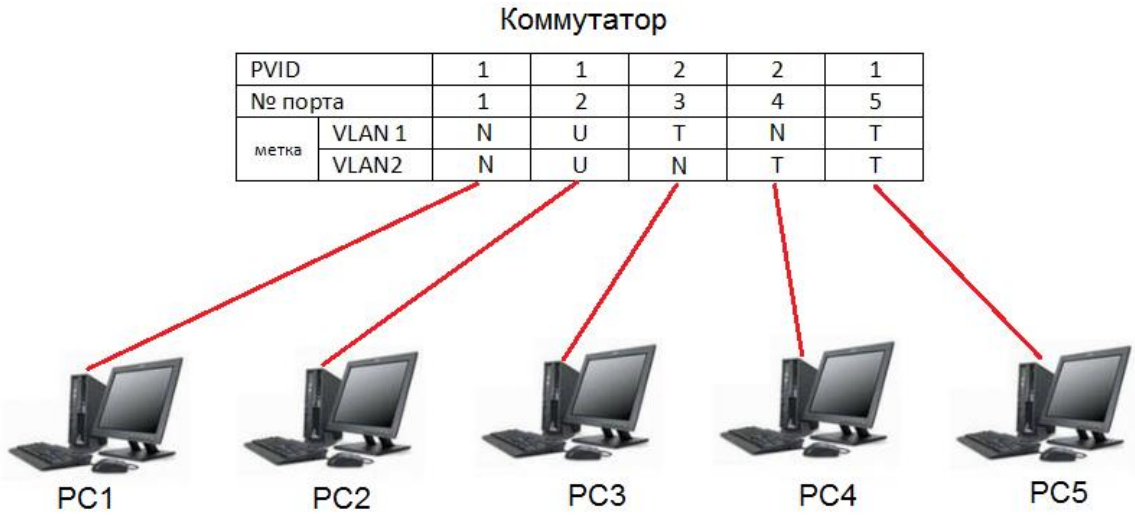


Рис.1

1. Тегированный пакет (*VID*=1) идет от *PC*1 к *PC*5. Данный пакет, поступая в порт, отбрасывается, т.к. для *VLAN* 1, доступ к порту запрещен (стоит метка *N*).
2. Не тегированный пакет идет от *PC*1 к *PC*2. На входе в коммутатор, пакет *VID* соответствует *PVID* порта (т.е. *VID* = 1). На выходе коммутатора (порт №2), *VID* пакета становится неопределенным и в таком виде поступает на *PC*2 (это происходит, т.к. метка *VLAN* 1 = *U*).
3. Не тегированный пакет идет от *PC*1 к *PC*3. На входе в коммутатор, пакет *VID* соответствует *PVID* порта (т.е. *VID* = 1). На выходе коммутатора, пакет сохранит свой *VID* (т.к. метка *VLAN* 1 = *T*) и в таком виде поступит на *PC*3.

4. Не тегированный пакет идет от *PC*1 к *PC*4. На входе в коммутатор, пакет *VID* соответствует *PVID* порта (т.е. *VID* = 1). На выходе коммутатора, пакет игнорируется, т.к. метка *VLAN* 1 = *N*.
5. Тегированный пакет (*VID*=2) идет от *PC*2 к *PC*5. Пакет заходит в коммутатор, т.к. для *VLAN* 2 установлена метка *U*. На выходе коммутатора, пакет сохранит свой *VID* (т.к. метка *VLAN* 2 = *T*) и в таком виде поступит на *PC*3.
6. Тегированный пакет (*VID*=2) идет от *PC*5 к *PC*2. Пакет заходит в коммутатор, т.к. для *VLAN* 2 установлена метка *T*. На выходе коммутатора (порт №2), *VID* пакета становится неопределенным и в таком виде поступает на *PC*2 (это происходит, т.к. метка *VLAN* 2 = *U*).

2. Настройка коммутатора AT-8000S/16

1. Необходимо настроить возможность входа в веб-интерфейс коммутатора и настроить статические *ip*, на все необходимые компьютеры (минимум – четыре). Данный процесс был подробно описан в ЛР1. *ip*-адрес коммутатора должен быть настроен следующим образом: *ip*-коммутатора 192.168.1.1, макса подсети 255.255.255.0. Также необходимо подключить компьютеры в розетки с четными номерами.

2. Выполнить вход в веб-интерфейс коммутатора (см. ЛР1). Далее перейти в меню настройку «*Layer*-2» и выбрать вкладку «*VLAN*».

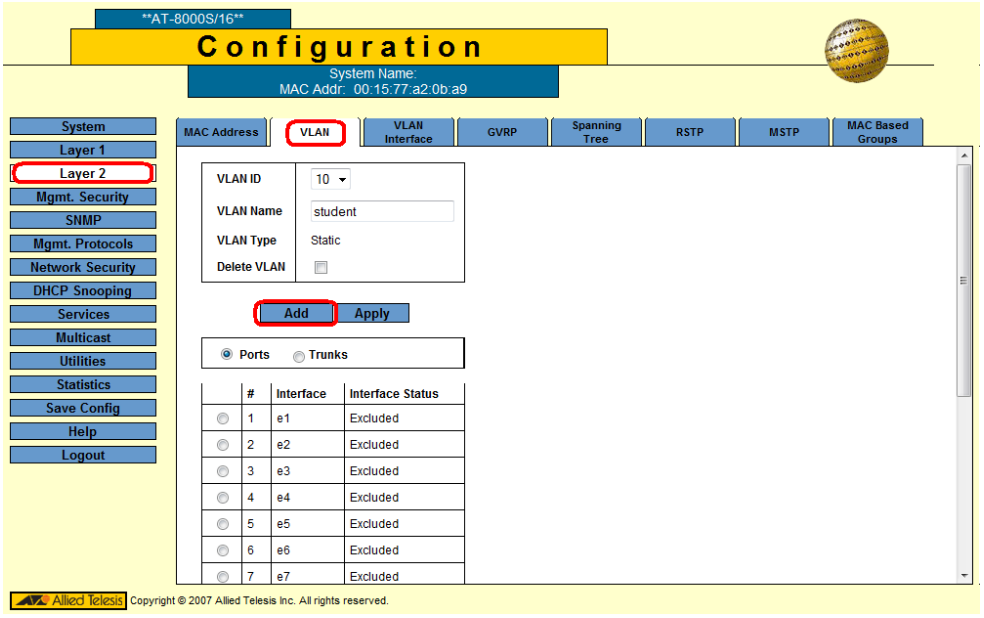


Рис.2

3. В данном меню (Рисунок.2), вы можете создать необходимое количество VLAN (до 4096 штук). Для этого следует нажать на кнопку «Add», после чего откроется меню создания новой *VLAN* (Рисунок.3).

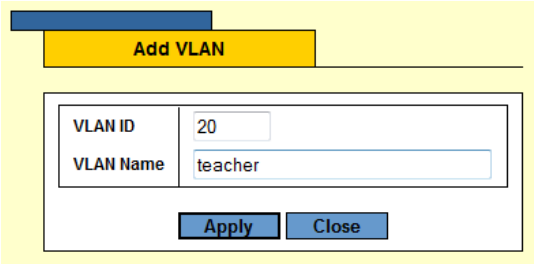


Рис.3

В данном меню необходимо указать идентификатор *VLAN* (*VLAN ID*) и имя новой подсети (*VLAN Name*). В данном примере, мы создаем новую *VLAN*, для преподавателей. Завершить создание можно нажав на кнопку «*Apply*».

В данной ЛР, необходимо создать 2-3 подсети.

4. Теперь, создав необходимое количество *VLAN*, можем переходить к конфигурации портов. Для этого перейдем на вкладку «*VLAN Interface*» (Рисунок.4). Здесь Вы можете присвоить *VPID* для всех необходимых портов.

Внимание! Не выполняйте действия описанные в этом шаге для компьютера на котором производится конфигурирование, иначе вы не сможете больше получить доступ к веб-интерфейсу, т.к. эти действия сделают невозможным ваше пребывание в сервисной «*Vlan*1», в которой находится сам коммутатор. Эту проблему можно обойти различными способами, однако это уже выходит за рамки данной ЛР.

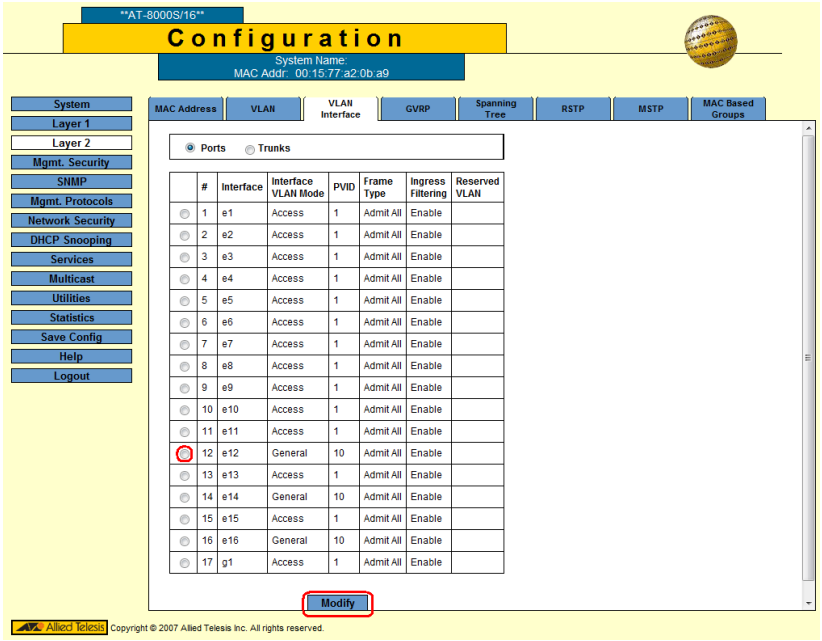


Рис.4

Для перехода к редактированию *PVID*, необходимо выделить нужный порт из списка (радиокнопкой) и начать «*Modify*», после чего вы перейдете в меню настройки порта. Здесь в пункте «*Port VLAN Mode*», нужно выбрать пункт «*General*», а в качестве *PVID*, указать *ID* необходимой подсети (Рисунок.5).

Примечание: номер порта, соответствует номеру розетки, к которой подключен компьютер (например, розетке №2, соответствует интерфейс *e*2).

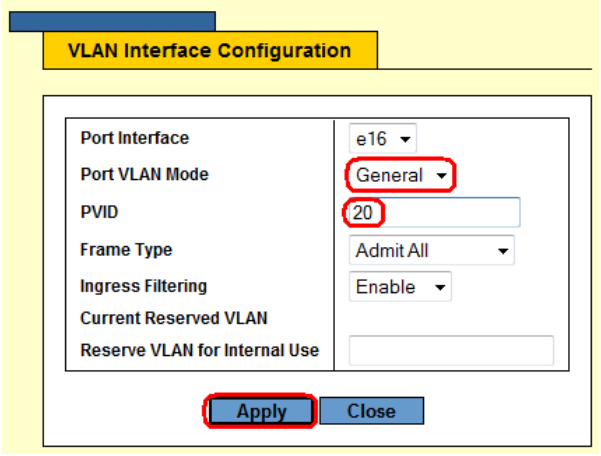


Рис.5

5. Вернемся к вкладке «*VLAN*» (Рисунок.6). Теперь здесь мы можем установить необходимые маркеры для каждой подсети каждого порта. Для этого нужно сначала выбрать необходимую подсеть (*VLAN ID*), далее с помощью радиокнопки выбрать необходимый порт и наконец, нажать на кнопку «*Modify*». Откроется окно редактирования маркера (Рисунок.7).

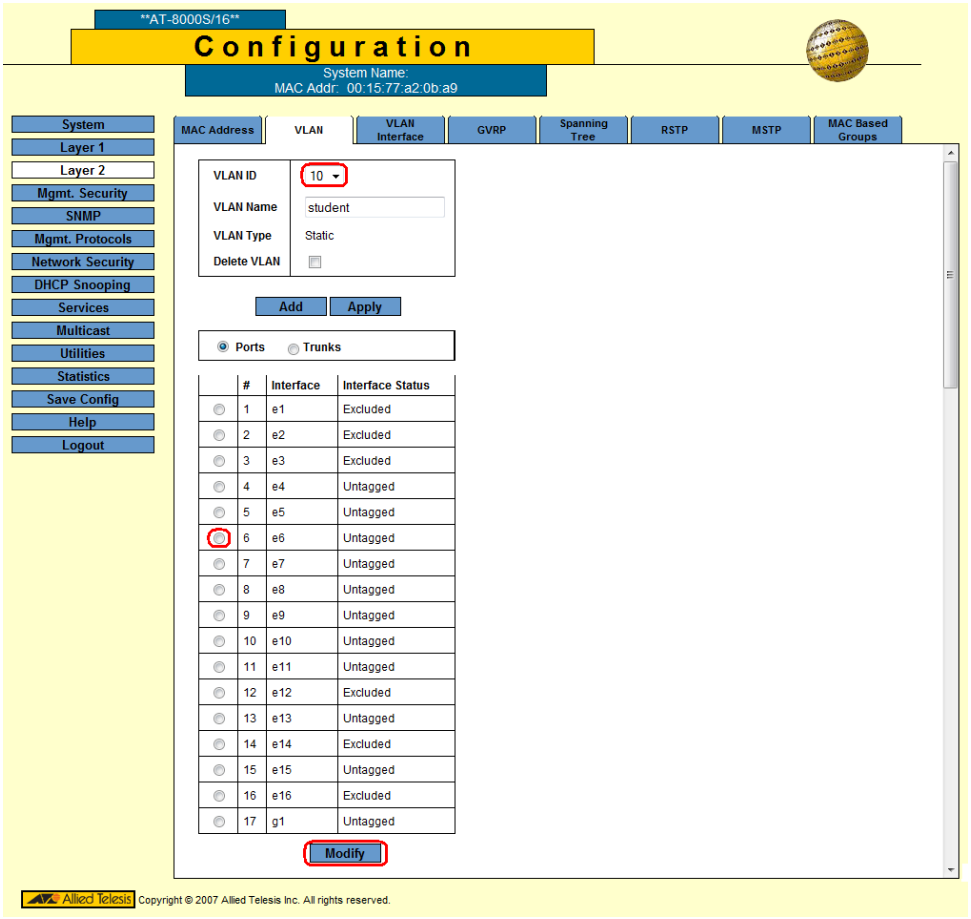


Рис.6

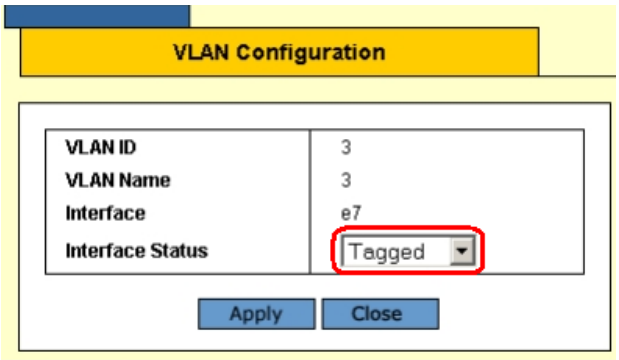


Рис.7

В этом окне, необходимо выбрать метку (Interface Status):

- *Tagged* – тегированный (*T*);
- *Untagged* – не тегированный (*U*);
- *Excluded* – исключенный из *VLAN* (*N*);
- *Forbidden* – указывает, что порт не может быть включен в *VLAN*.

Для сохранения, необходимо нажать на кнопку «Apply».

Замечание: как было сказано в ЛР1, для того, чтобы настройки оставались без изменения, даже после выключения питания, необходимо выполнить их сохранение. Однако, если вы хотите, чтобы в следующий раз все произведенные вами настройки исчезли, не следует производить сохранение. Подробно об это, см. ЛР1.

6. Для того, чтобы убедиться, что сеть настроена верно, можно воспользоваться программой *ping* (она рассмотрена в ЛР1). Если компьютеры настроены так, как показано на Рисунке.8, то команда ping будет корректно работать между компьютерами *PC*1-*PC*2, *PC*3-*PC*4. Однако *ping* не будет работать между *PC*1-*PC*3, *PC*1-*PC*4, *PC*2-*PC*3 и *PC*2-*PC*4, что свидетельствует, о том, что *PC*1 и *PC*2 находятся в подсети *VLAN* 1, а компьютеры *PC*3 и *PC*4 – в подсети *VLAN* 2.

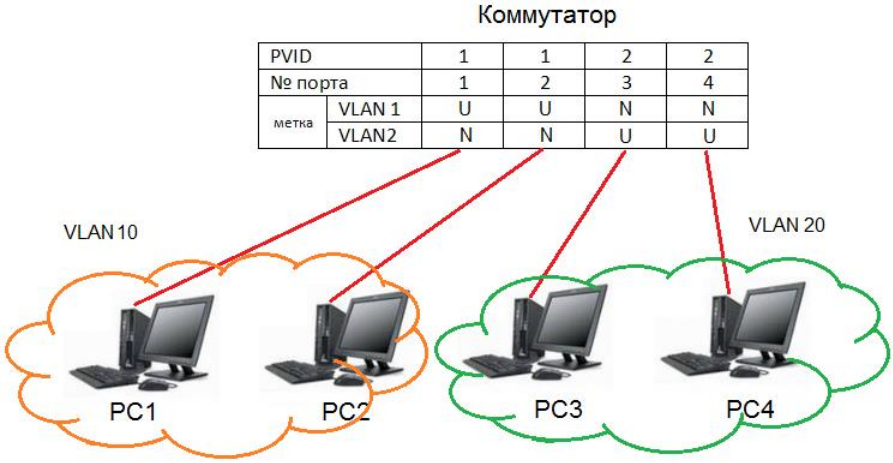


Рис.8

Рабочее задание

1. Подключить сетевые кабели к компьютерам таким образом, чтобы они оказался подключенным к учебному коммутатору;
2. Визуально убедиться в том, что необходимый кабель подключен к коммутатору;
3. Настроить компьютер на работу со статическим *IP* адресом;
4. Настроить коммутатор на работу с *WEB*-интерфейсом;
5. Зайти на коммутатор через *WEB*-интерфейс;
6. Настроить подсети так, как показано на рисунке.8.
7. Произвести ping между всеми участвующими в ЛР компьютерами;
8. Создать еще одну *VLAN* и произвести настройку коммутатора таким образом, чтоб *PC*2 и *PC*3 могли обмениваться пакетами, а *PC*1-*PC*4 – нет;
9. Сделать любой из компьютеров недоступным для всех остальных

Расчетное задание

1) Представим, что в нашей сети имеется два коммутатора. У нас имеется 10 компьютеров. Необходимо настроить коммутаторы так, чтобы часть компьютеров находилась в одной подсети, а часть в другой;
2) Настроить дополнительную подсеть так, чтобы по одному компьютеру из каждой подсети имели доступ к интернету (кабель интернета подключен к *VLAN* 3).

Вопросы для самопроверки

1) Что такое *VLAN*?
2) Какие бывают метки?
3) Не тегированный пакет от *PC*3 входит в коммутатор. Куда пакет может пойти дальше? (см. Рисунок.1)
4) По аналогии с предыдущим вопросом, куда может пойти пакет, если он имеет *VID*=1 и поступает на *PC*3?

5) Если все порты коммутатора были настроены в соответствии с п.4-5 то, как можно будет восстановить настройки, ведь мы больше не имеем доступ к коммутатору по *Ethernet*?
6) К какой подсети относится сам коммутатор?

Вопросы для самопроверки

Лабораторная работа №8
СОЗДАНИЕ VPN-ТУННЕЛЯ НА ОСНОВЕ МАРШРУТИЗАТОРОВ

Цель работы: Ознакомление с принципами и режимами работы маршрутизатора. Получение навыков конфигурирования оборудования

Аппаратура: ПК, маршрутизаторы D-Link DI-804HV

***Программное обеспечение*:** ОС Windows 7, web-браузер Internet Explorer

Общие сведения

Маршрутизатор (router - роутер) — сетевое устройство, на основании информации о топологии сети и определенных правил принимающее решения о пересылке пакетов сетевого уровня между различными сегментами сети. Работает на более высоком уровне, нежели коммутатор и сетевой мост.

Обычно маршрутизатор использует адрес получателя, указанный в пакетах данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Таблица состоит из некоторого числа записей — маршрутов, в каждой из которых содержится адрес сети получателя, адрес следующего узла, которому следует передавать пакеты и некоторый вес записи — метрика. Метрики записей в таблице играют роль в вычислении кратчайших маршрутов к различным получателям.

VPN (виртуальные частные сети) и туннелирование являются методами, позволяющими шифровать информационное соединение между вашим компьютером и другим компьютером сети. Другой компьютер

может принадлежать вашей организации, доверенному лицу или коммерческому VPN сервису. Туннелирование скрывает информацию отдельных информационных потоков внутри зашифрованного протокола, таким образом, превращая весь проходящий через туннель трафик нечитабельным для посторонних, на всем своем пути.

Виртуальные частные сети очень часто используются корпорациями для обеспечения сотрудников, которым необходим доступ к конфиденциальной финансовой или другой информации, подключением к компьютерным сетям компании из дома или других отдаленных мест через сеть Интернет.

Использование VPN соединения или других разновидностей туннелирования с целью шифрования вашей информации может быть очень хорошим способом обеспечения её закрытости для всех, кроме вас и тех людей, которым вы доверяете.

Эти методы создают туннель от вашего компьютера до другого компьютера в сети Интернет. Ваша информация может сначала проходить через этот туннель, а затем продолжить путь до пункта назначения во всемирной паутине. Сохранность и конфиденциальность трафика внутри туннеля защищаются шифрованием.

Важно заметить, что данные шифруются только до конца туннеля и затем перемещаются в незашифрованном виде до пункта назначения.

Главным различием между VPN соединением и туннелем является то, что система VPN подразумевает шифрование всех данных между вашим компьютером и Интернетом, в то время как при использовании туннеля кодируется только трафик, обрабатываемый отдельными приложениями. Шифрование при этом основывается либо на номерах портов, используемых этими приложениями, либо программа запрашивает у вас информацию о том, какой туннель использовать для каждого приложения. В отличие от VPN, при использовании туннелей требуется отдельно настраивать все приложения, которые должны использовать шифрованный туннель (веб браузер, клиент электронной почты или программа службы обмена мгновенными сообщениями) на работу через него.

После создания туннеля и настройки приложений, коммуникация этих приложений с сетью Интернет будет проходить через шифрованный туннель, идущий до компьютера с установленным программным

обеспечением туннелирования, который напрямую передает запросы пользователей и ответы серверов сети.

В отличие от туннелей системы VPN передают все данные через шифрованную сеть, включая Voice over IP (VoIP) и информационный обмен с приложениями, не поддерживающими SOCKS. Установленные VPN системы являются более разносторонними инструментами, чем туннели, но их установка и настройка является более сложной по сравнению с большинством приложений туннелирования.

Существует несколько различных стандартов установки VPN сетей, включая IPSec, SSL/TLS и PPTP, которые различаются по своей сложности, по обеспечиваемому уровню безопасности и по совместимости с отдельными операционными системами. Естественно существует также множество различий в реализации каждого стандарта на уровне программного обеспечения, которое имеет различные свойства.

На сегодняшний день одним из самых проработанных и совершенных Интернет-протоколов для построения VPN является протокол IPSec (IP Security). Он обеспечивает аутентификацию, проверку целостности и шифрование сообщений на уровне каждого пакета. Для управления криптографическими ключами IPSec использует протокол IKE. Пожалуй, самым основным преимуществом IPSec является то, что это протокол сетевого уровня. VPN, построенные на его базе, работают абсолютно прозрачно для всех приложений, сетевых сервисов, а также для сетей передачи данных канального уровня. IPSec позволяет маршрутизировать зашифрованные пакеты сетям без дополнительной настройки промежуточных маршрутизаторов, поскольку он сохраняет, принятый в IPv4, стандартный IP-заголовок. IPSec является более гибким инструментом, так как он может быть использован для защиты всех остальных протоколов, находящихся на более высоких уровнях. Кроме того, приложения не должны быть разработаны специально для использования IPSec, в то время как функции SSL/TLS или других протоколов высокого уровня должны быть встроены в приложение.

Маршрутизатор D-Link DI-804HV полностью поддерживает протокол IPSec. При помощи этого маршрутизатора возможно организовать до 40 туннелей IPSec. Включена поддержка Dynamic VPN, позволяющая осуществлять VPN подключение к корпоративной сети мобильным хостам с непостоянными IP-адресами. DI-804HV

предоставляет гибкую и недорогую реализацию VPN для обеспечения сохранности корпоративных данных.

Допустим, есть две офисных сети, одна главная, другая – удаленная. Нужно объединить при помощи VPN-туннеля сети главного и удаленного офисов, с тем, чтобы обеспечить безопасный обмен корпоративными данными, а также прозрачный защищенный доступ к Intranet-ресурсам сети главного офиса пользователям сети удаленного офиса через небезопасный Интернет. Оба офиса имеют выделенное подключение к Интернет с реальными статическими IP-адресами. Для осуществления задачи есть два маршрутизатора D-Link DI-804HV.

На рисунке 10 изображена схема, которую необходимо реализовать.

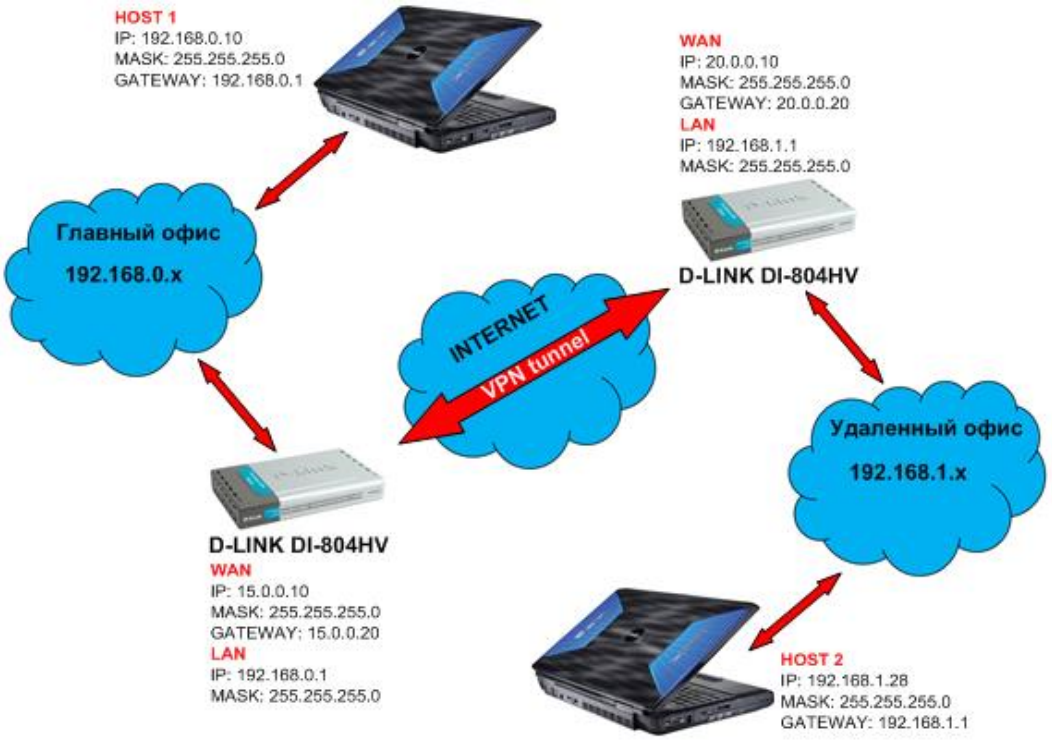


Рис .10 - Схема VPN-туннеля

Порядок выполнения работы:

1. Установить на компьютере IP-адрес и маску подсети

Для этого необходимо:

а) выбрать «Пуск» => «Панель управления» => «Сеть и интернет» => «Центр управления сетями и общим доступом» => «Изменение параметров адаптера»

б) выбрать подключение по локальной сети и нажать «Свойства»

в) на вкладке «Сеть» выбрать «Протокол интернета версии 4 (TCP/IPv4)» и нажать на кнопку «Свойства»

г) на вкладке «Общие» выбираем пункт «Использовать следующий IP-адрес» и прописываем:

IP-адрес 192.168.0.2

маска подсети 255.255.255.0

Результат выполненных действий представлен на рисунке 11.

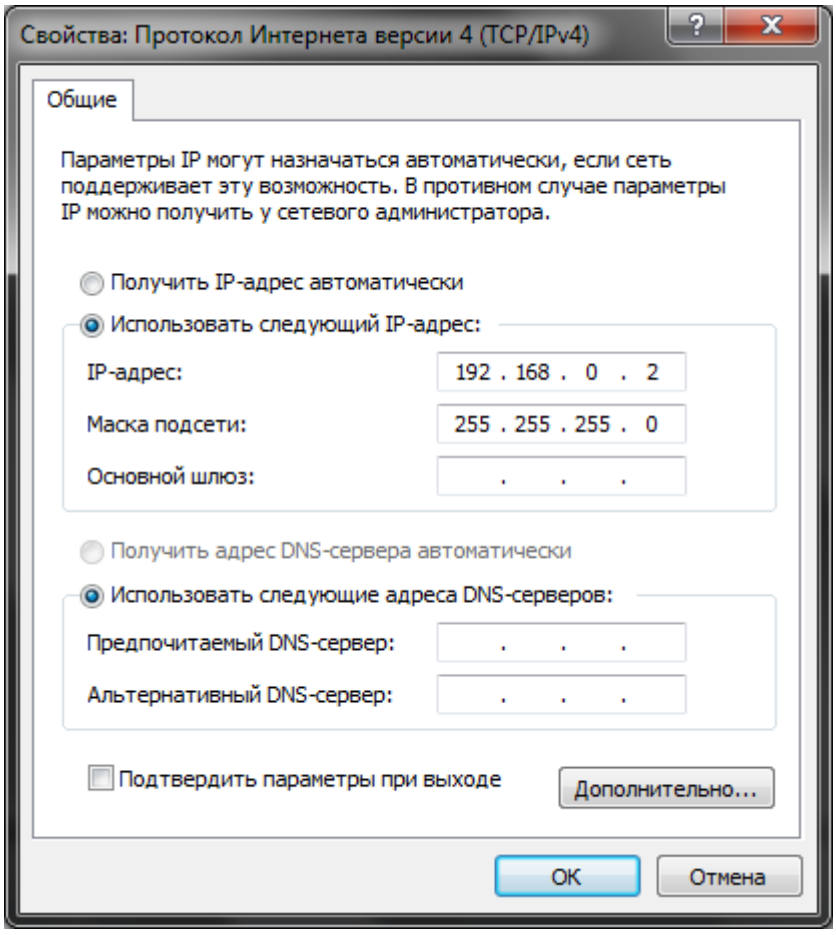


Рис. 11 – Окно свойств протокола TCP/IP

2. Подключиться к web-интерфейсу маршрутизатора

Для этого необходимо:

а) выбрать «Пуск» => «Программы» => «Internet Explorer»

Результат выполненных действий представлен на рисунке 12.

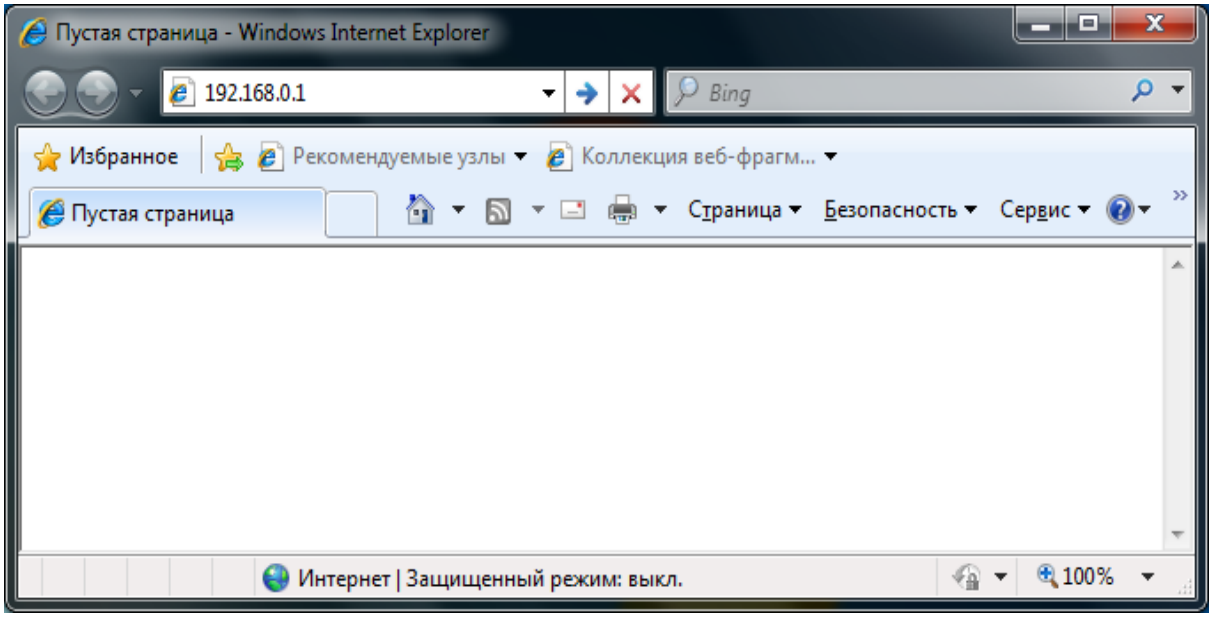


Рис. 12 - Web-браузер Internet Explorer

б) в web-браузере прописать в поле адреса внутренний IP-адрес маршрутизатора 192.168.0.1 и нажать «Enter»

в) вводим в появившемся окне login: «admin», password пустой

Результат выполненных действий представлен на рисунке 13.

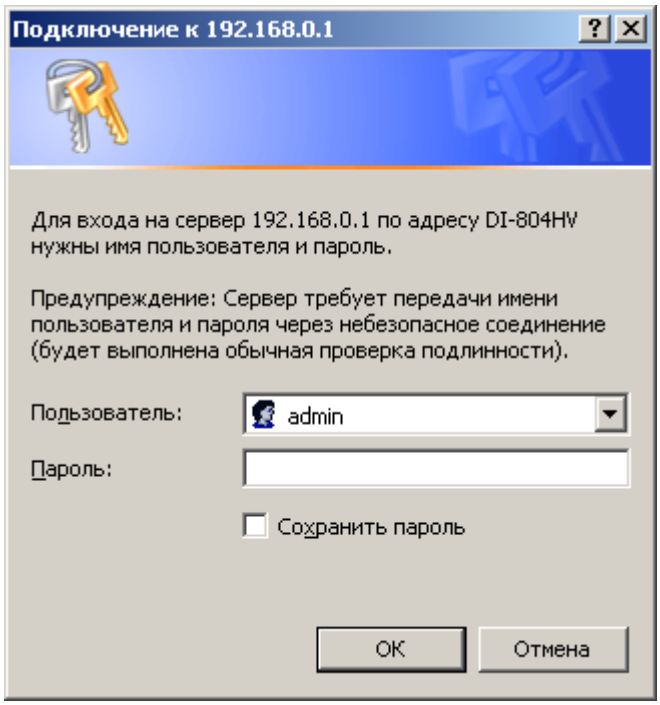


Рис. 13 – Окно входа в web-интерфейс

3. Настроить WAN (внешний IP) маршрутизатора через web-интерфейс

Для этого необходимо:

а) выбрать «Static IP address»

б) вводим следующие настройки:

IP Address: 20.0.0.10

Subnet mask: 255.255.255.0

ISP Gateway Address: 20.0.0.20

Primary DNS Address: 20.0.0.31

Secondary DNS Address: 20.0.0.32

MTU: 1500

WAN Keep-alive: Disabled

Change the TTL value: Enabled

Auto-backup: Disabled

в) нажать кнопку «Apply» и затем «Restart»

Результат выполненных действий представлен на рисунке 14.

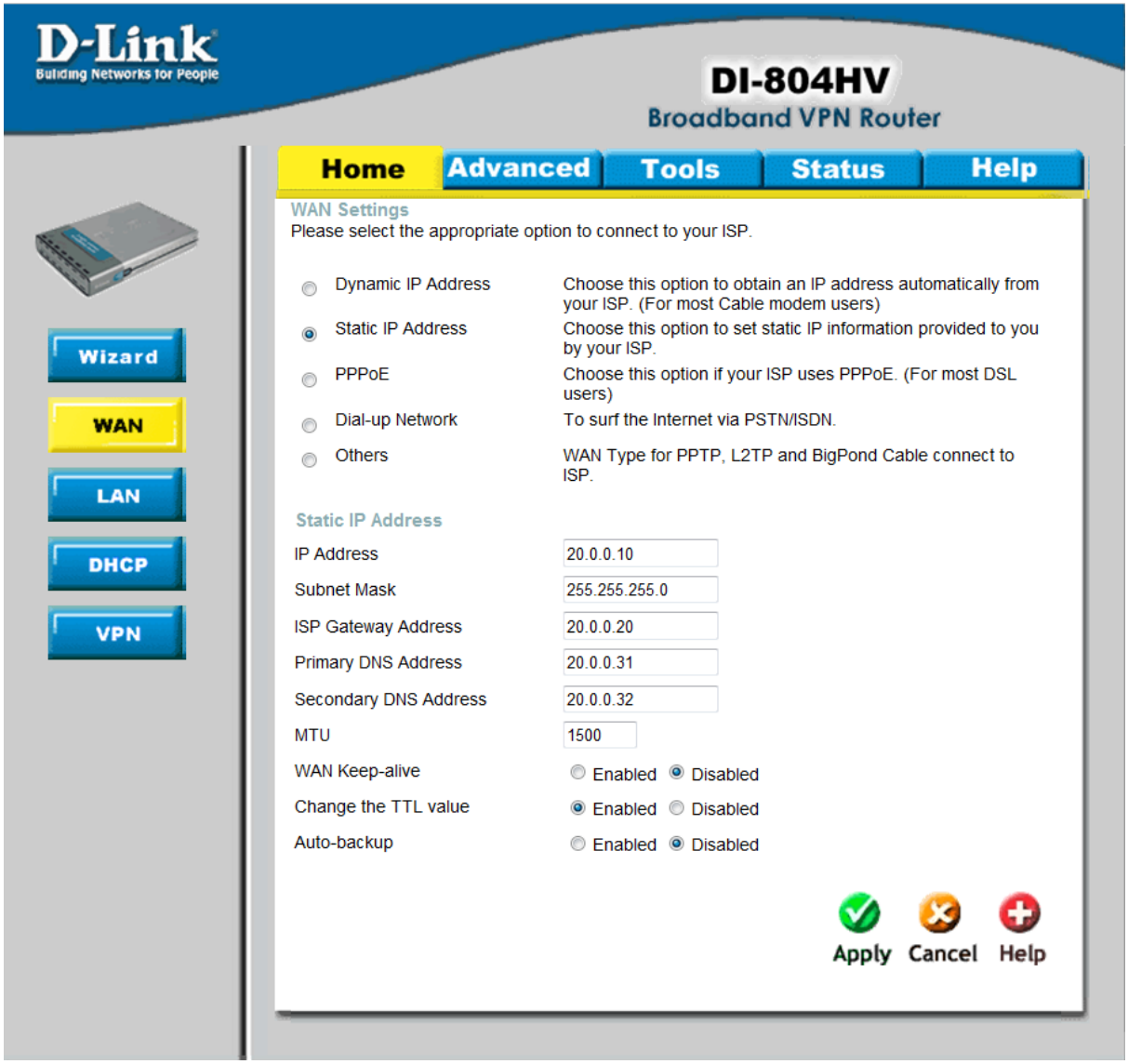


Рис. 14 – Настройка WAN маршрутизатора

4. Настроить LAN (внутренний IP) маршрутизатора через web-интерфейс

Для этого необходимо:

а) вводим следующие настройки:

IP Address: 192.168.0.1

Subnet mask: 255.255.255.0

б) нажать кнопку «Apply» и затем «Restart»

Результат выполненных действий представлен на рисунке 15.

Рис. 15 - Настройка LAN маршрутизатора

5. Настроить VPN маршрутизатора через web-интерфейс

Для этого необходимо:

а) вводим следующие настройки:

VPN: Enabled

Max. number of tunnels: 10

Tunnel Name: New-VPN

Method: IKE

б) нажать кнопку «More»

Результат выполненных действий представлен на рисунке 16.

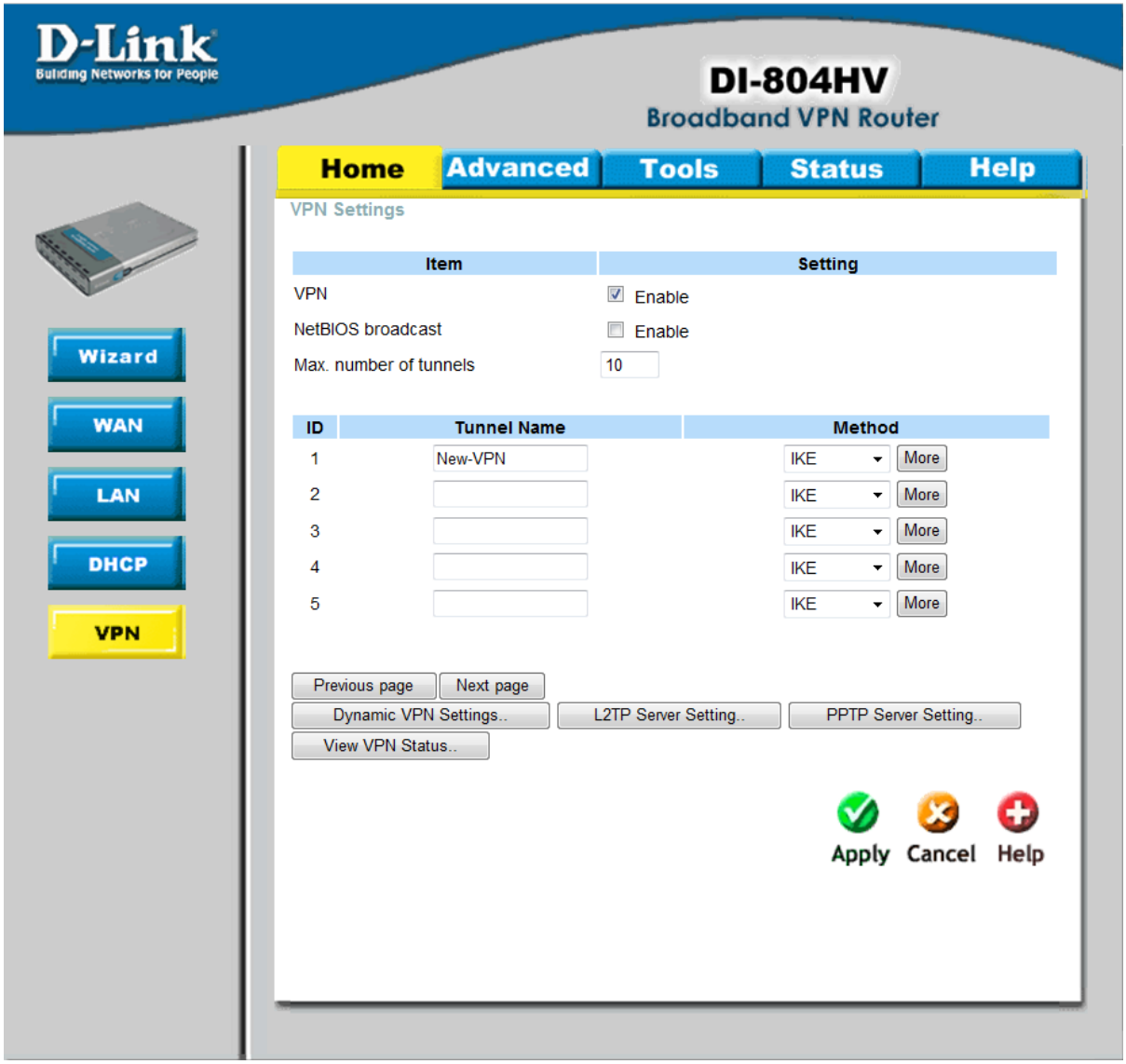


Рис. 16 - Настройка VPN маршрутизатора

в) в появившемся окне вводим следующие настройки:

Local Subnet: 192.168.0.0

Local Netmask: 255.255.255.0

Remote Subnet: 192.168.1.0

Remote Netmask: 255.255.255.0

Remote Gateway: 20.0.0.10

Preshare Key: произвольный (ключ должен быть одинаковым на обоих концах VPN-туннеля)

г) нажимаем кнопку «Select IKE Proposal …»

Результат выполненных действий представлен на рисунке 17.

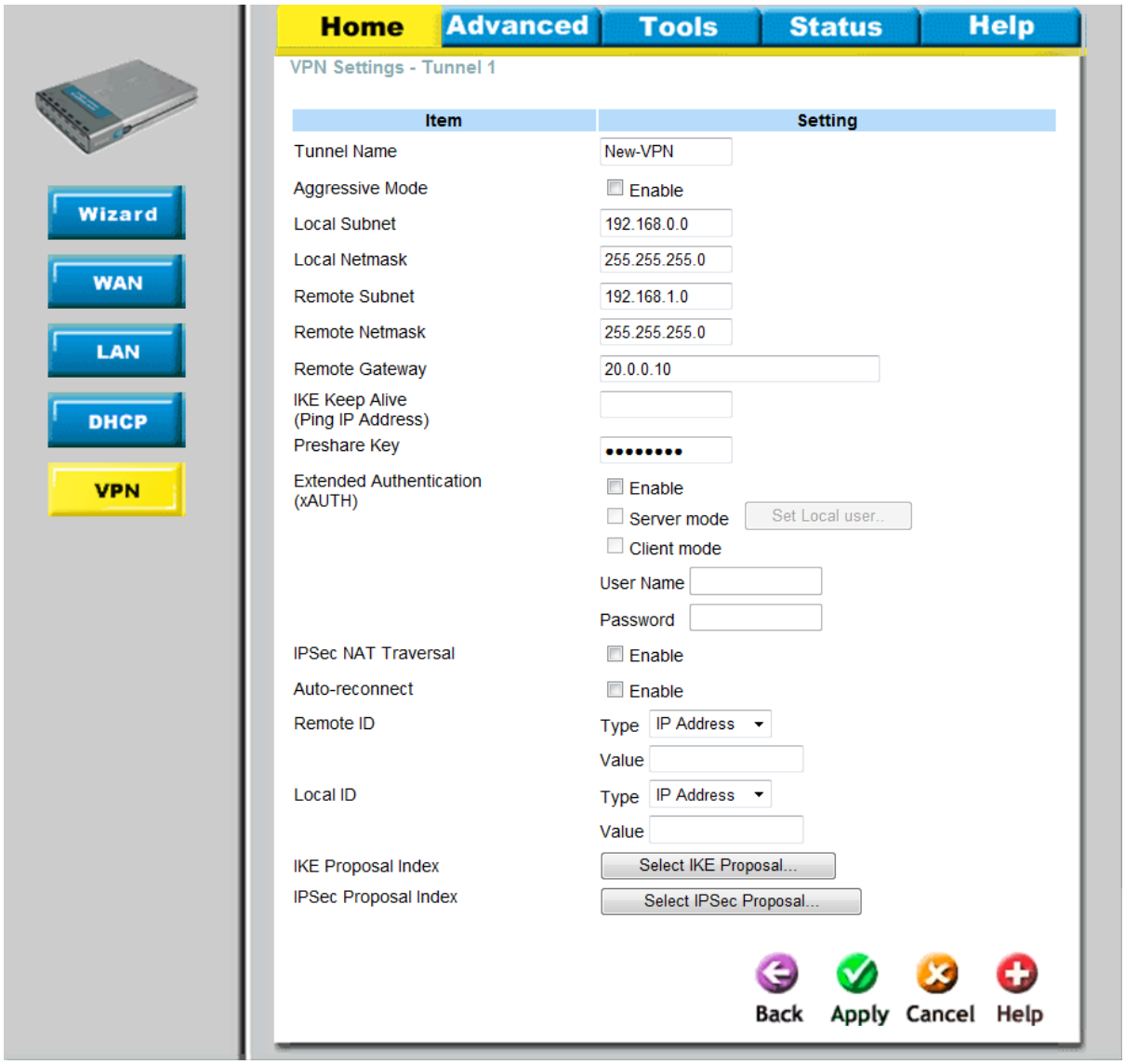


Рис. 17 - Настройка VPN-tunnel маршрутизатора

д) в появившемся окне вводим следующие настройки:
Proposal Name: IKE Proposal
DH Group: Group 1
Encrypt algorithm: 3DES
Auth algorithm: SHA1
Life Time: 28800
Life Time Unit: Sec
е) нажать кнопку «Add to»
ж) нажать кнопку «Apply» и затем «Restart»
Результат выполненных действий представлен на рисунке 18.

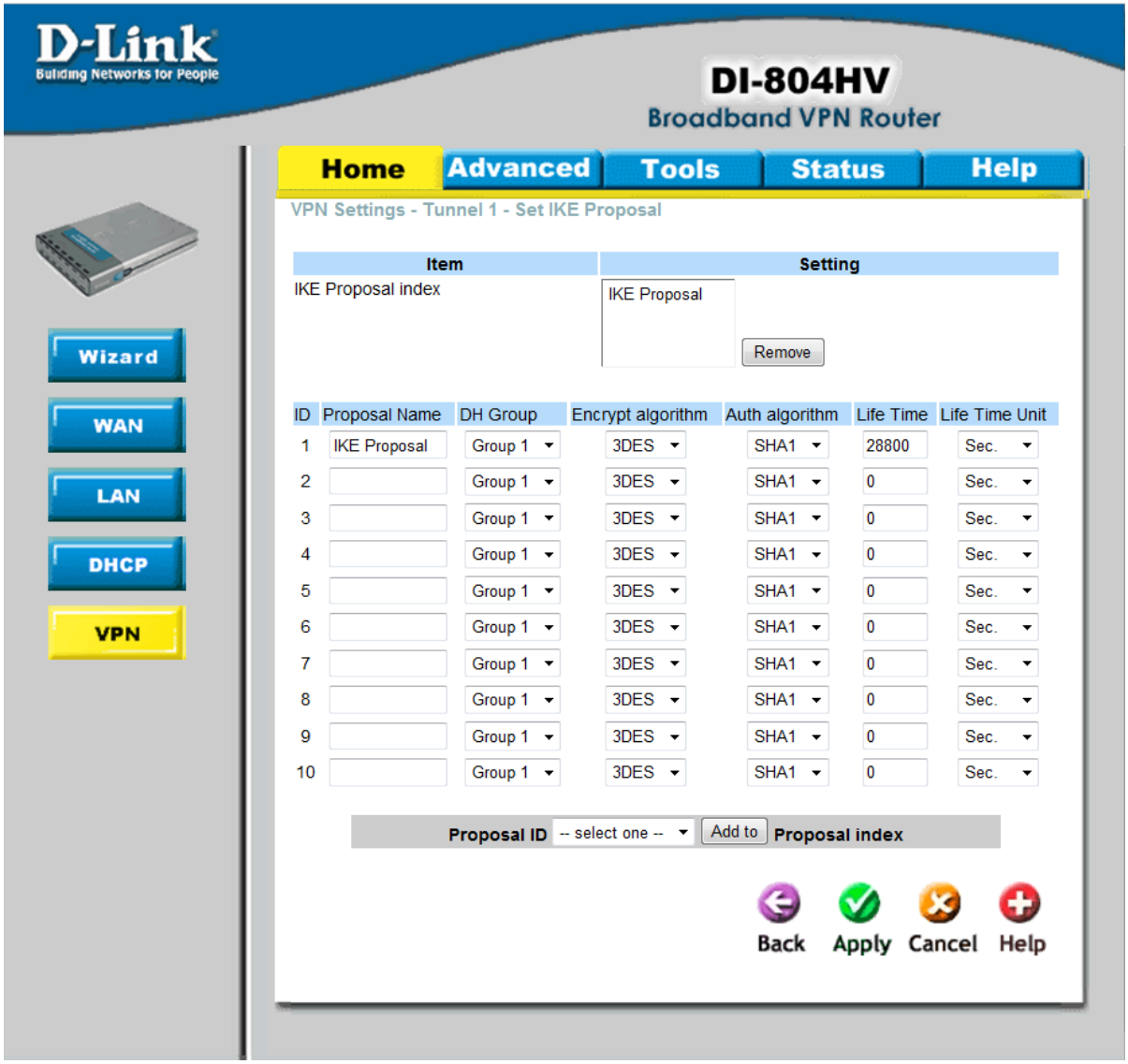


Рис. 18 - Настройка Set IKE Proposal маршрутизатора

з) зайти в меню «Set IPSEC Proposal» и ввести следующие настройки:

Proposal Name: IPSEC Proposal

DH Group: None

Encap protocol: ESP

Encrypt algorithm: 3DES

Auth algorithm: MD5

Life Time: 3800

Life Time Unit: Sec

и) нажать кнопку «Add to»

к) нажать кнопку «Apply» и затем «Restart»

Результат выполненных действий представлен на рисунке 19.

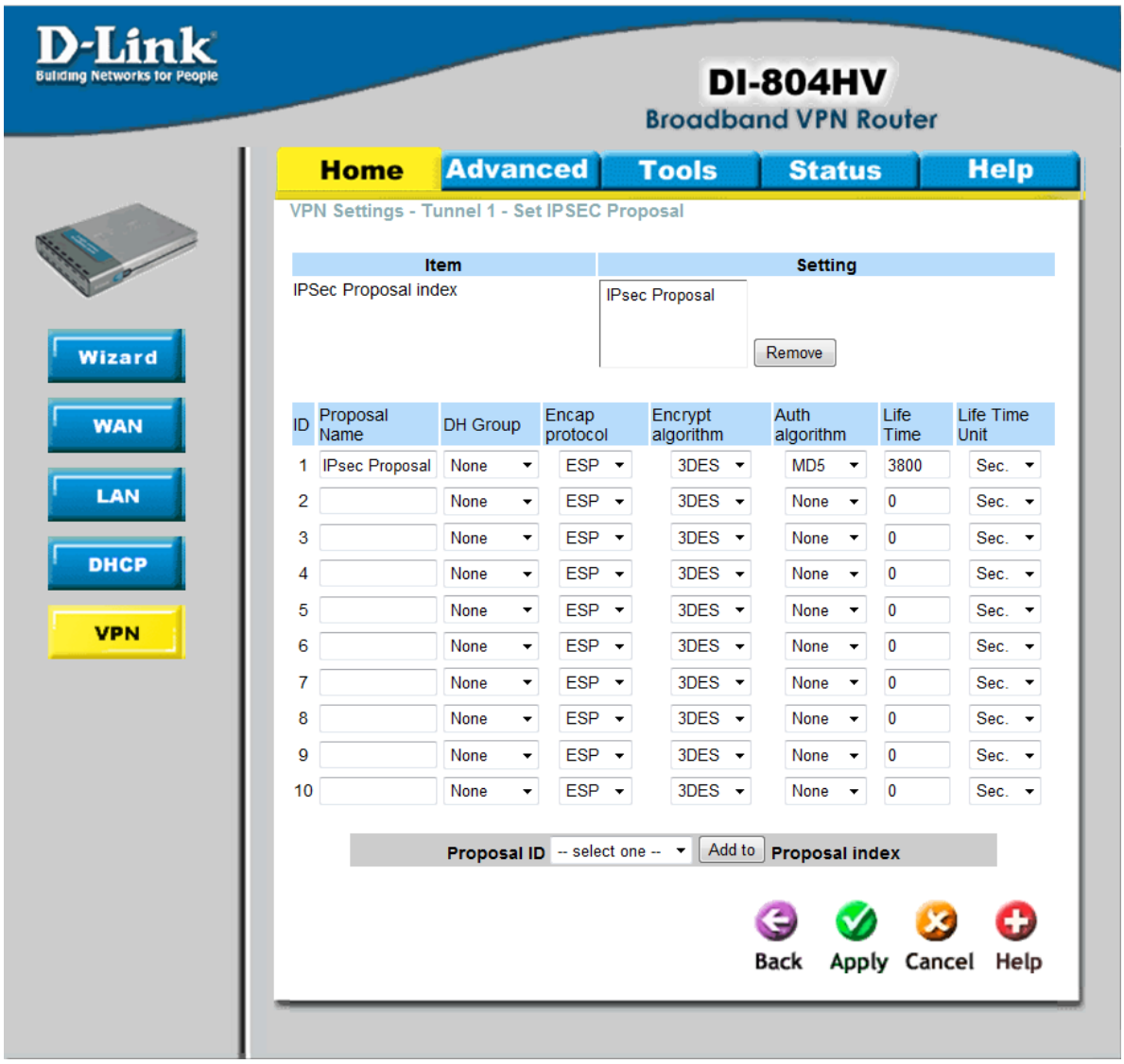


Рис. 19 - Настройка Set IKE Proposal маршрутизатора

6. Настроить второй маршрутизатор аналогичным образом

Для этого необходимо:

а) выполнить все пункты настройки как для первого маршрутизатора

б) при выполнении пункта 5 в) ввести следующие настройки:

Local Subnet: 192.168.0.1

Local Netmask: 255.255.255.0

Remote Subnet: 192.168.0.0

Remote Netmask: 255.255.255.0

Remote Gateway: 15.0.0.10

Preshare Key: такой же как и в настройках первого маршрутизатора

Результат выполненных действий представлен на рисунке 20.

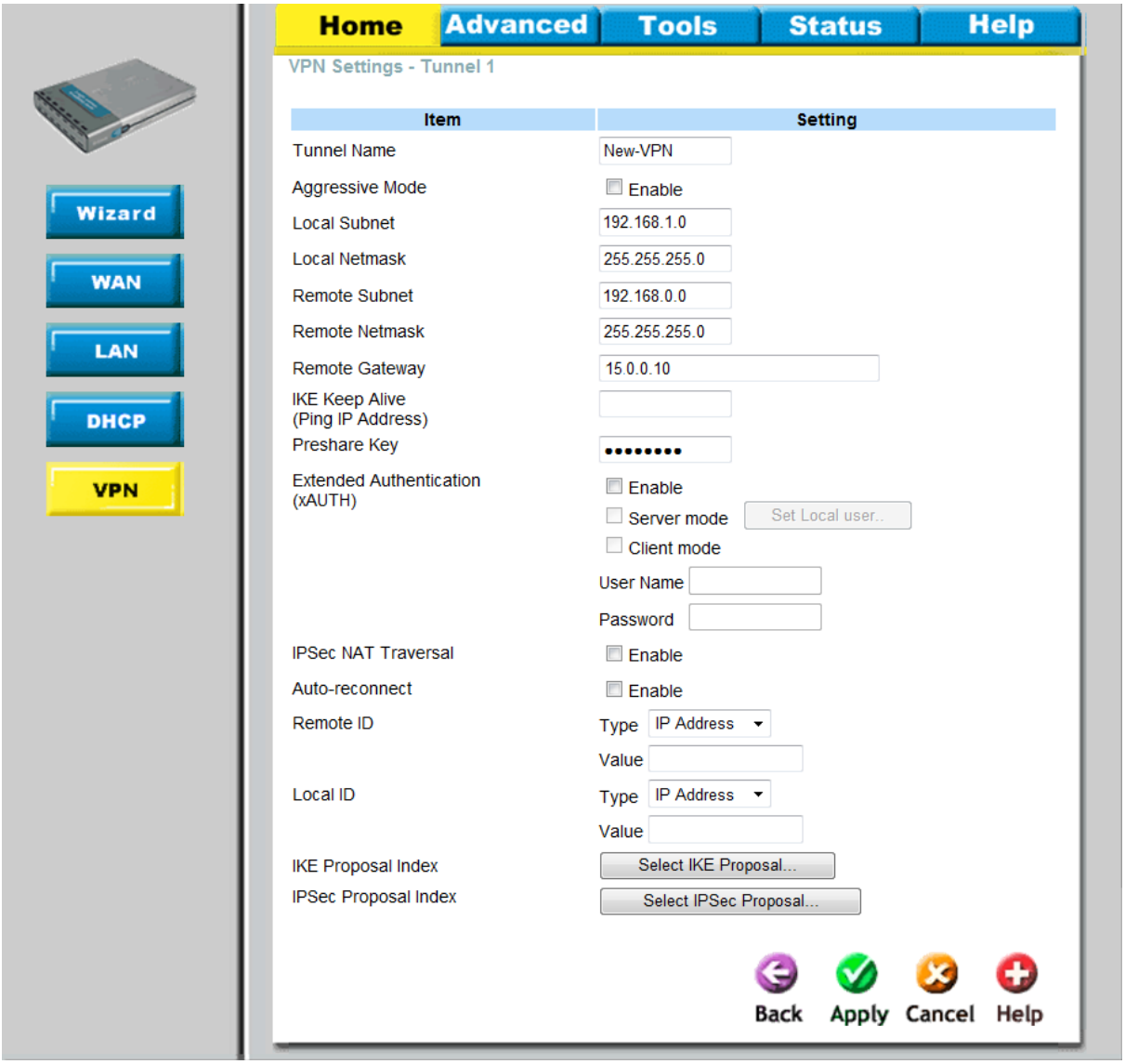


Рис. 20 - Настройка VPN-tunnel маршрутизатора

В результате выполненных действий настройка VPN-туннеля на маршрутизаторах D-Link DI-804HV успешно выполнена.

7. Проверить работу созданного соединения и текущую конфигурацию

Для этого необходимо на обоих компьютерах выполнить следующие действия:

а) выбрать «Пуск» => «Программы» => «Стандартные» => «Командная строка»

б) ввести команду ipconfig

(вывод диагностической информации о конфигурации сети, позволяет просмотреть текущую конфигурацию адресов TCP/IP для протокола DHCP)

в) ввести команду ping

(проверяет соединение на IP-уровне, отправляет эхо-запрос по протоколу ICMP на имя или IP-адрес целевого узла)

г) проверить соответствие полученных результатов скриншотам, представленных на рисунках 21, 22, 23.

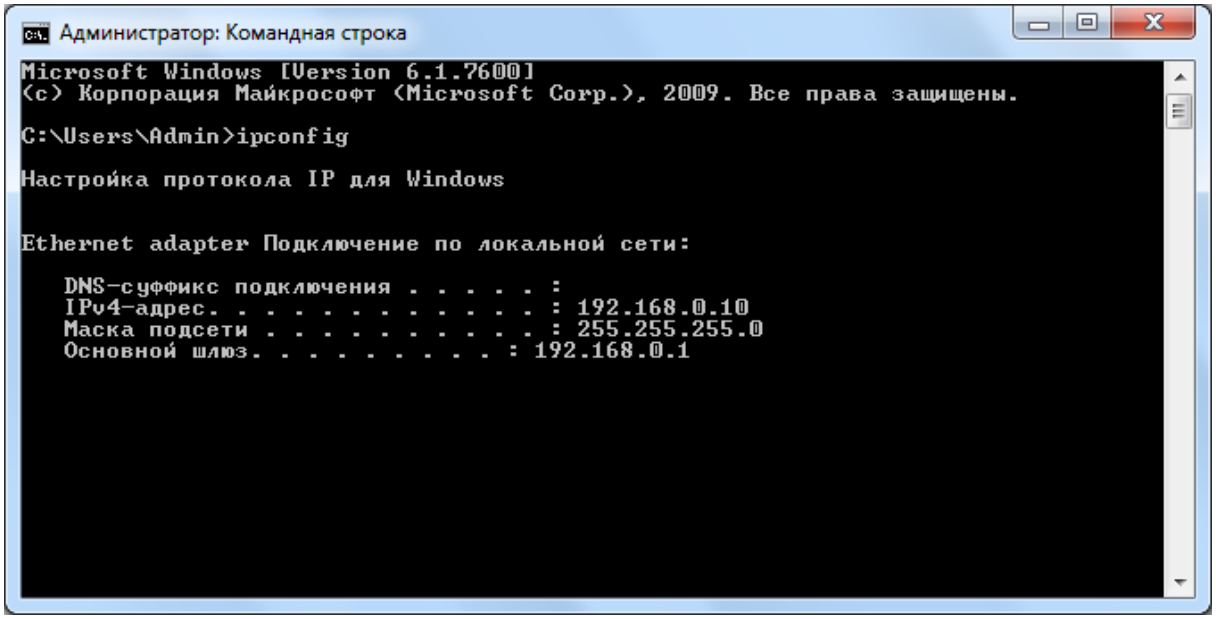


Рис. 21 – Настройки конфигурации сети первого компьютера

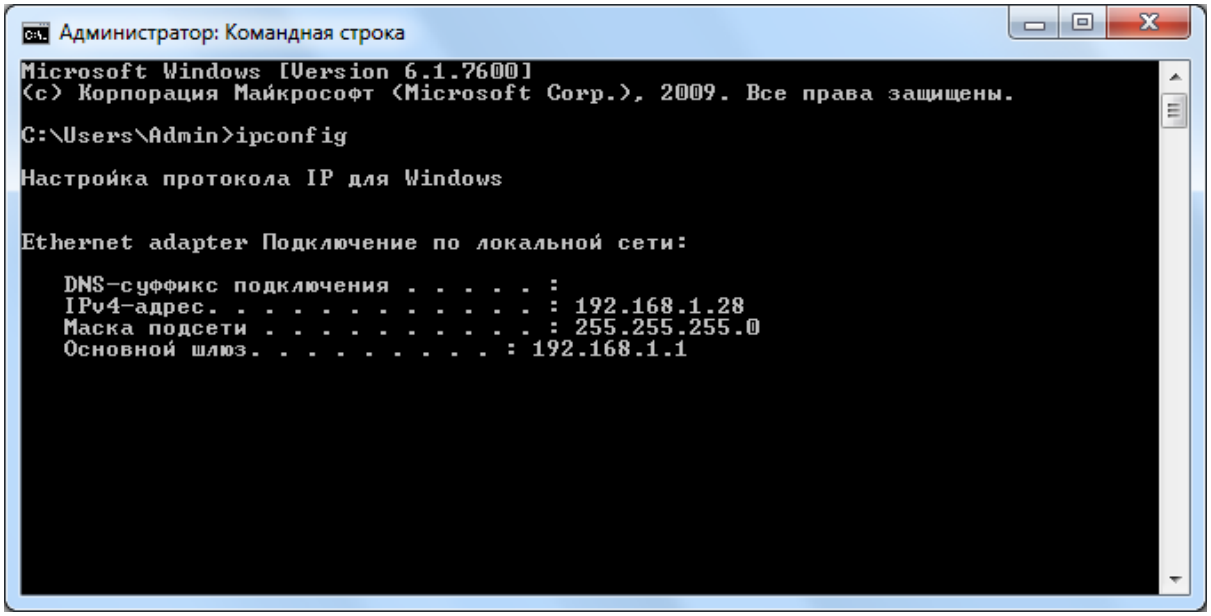


Рис. 22 – Настройки конфигурации сети второго компьютера

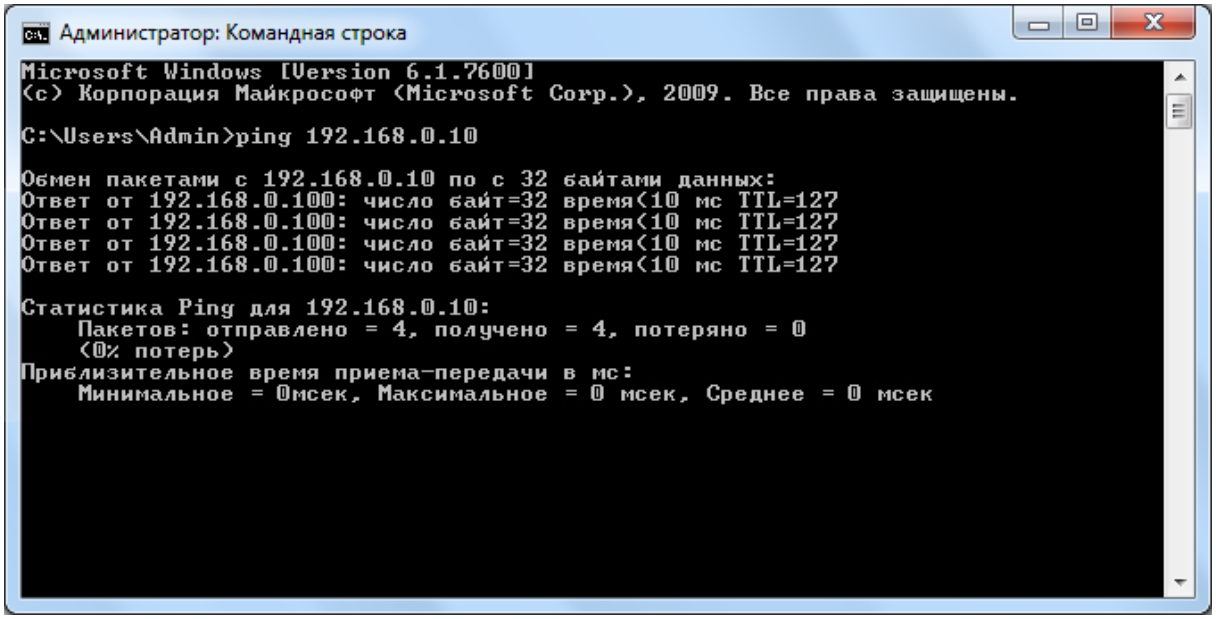


Рис. 23 – Результат выполнения команды ping

Как видно на рисунке 23, наличие между хостами VPN-туннеля, проходящего через Интернет, остаётся совершенно незамеченным для команды ping, также оно будет незаметно и для всех других сетевых приложений и служб. Это свойство протокола IPSec, обусловленное тем, что это протокол сетевого уровня, открывает огромные возможности перед системными администраторами компаний, имеющих более чем один офис. Поверх IPSec, например, можно развернуть доменную структуру, организовать работу почты, работу уже созданных систем внутреннего документооборота и других сетевых служб. Это избавляет от необходимости создания в каждом удалённом офисе своего отдельного почтового сервера, своего отдельного домена, избавляет от необходимости нанимать высококвалифицированный персонал для администрирования серверов и для модификации существующих систем документооборота. Всё это в значительной мере экономит средства компании, использующей VPN.

Содержание отчета:

1. Цель работы.
2. Краткие теоретические сведения.
3. Описание возможностей маршрутизатора.

4. Результат выполненных действий в виде скриншотов с пояснениями.

5. Вывод по выполненной работе.

Контрольные вопросы

1. В чем суть технологии VPN?
2. Что означает термин IPSec?
3. К протоколам какого уровня относится IPSec?
4. Каков принцип работы VPN-туннеля?
5. Чем отличается VPN от VPN-туннеля?
6. Что такое маршрутизатор?
7. В чем различие между коммутатором и маршрутизатором?
8. Для чего нужна таблица маршрутизации?

Лабораторная работа № 9
ИЗУЧЕНИЕ СИСТЕМЫ ОБМЕНА ДАННЫМИ МЕЖДУ УДАЛЕННЫМИ PC

***Цель работы*:** изучение способов обмена данными между удаленными PC и аппаратных средств, реализующих информационную связь. Освоение приемов работы, основных правил эксплуатации и обслуживания технических средств.

***Аппаратура*:** компьютер, V.92 56K Fax Modem, принтер.

***Программное обеспечение*:** стандартный телекоммуникационный пакет, входящий в комплект Windows.

Общие сведения

В простейшем случае передача данных может быть осуществлена посредством соединения двух PC через последовательный интерфейс. Связь в этом случае осуществляется без использования устройств усиления и преобразования передаваемых и полученных данных с помощью специального кабеля, называемого кабелем нуль-модема. Такой кабель может иметь длину 100 метров и более и исключает опасность потери данных. От других кабелей периферийных устройств кабель нуль-модема

отличается распайкой проводников, некоторые из которых включаются перекрестно.

Для организации обмена данными в этом случае необходимо соответствующее программное обеспечение. Можно использовать команды (например Interlnk) операционной системы MS DOS или программы из пакетов утилит (PC Tools, Norton commander, Windows и др.).

Устройство, позволяющее обмениваться информацией через PC (цифровыми устройствами), через аналоговые каналы (обыкновенные телефонные станции и сети), называется *модемом* (МОдулятор-ДЕМодулятор).

Назначение модема заключается в замене цифрового сигнала, поступающего из PC электрическим сигналом с частотой, соответствующей рабочему диапазону телефонной линии. Акустический канал этой линии модем разделяет на две полосы низкой и высокой частоты. Полоса низкой частоты применяется для передачи данных, а полоса высокой частоты - для приема. Используется два способа кодировки информации: метод FSK (частотный) для скорости передачи до 300 бод (бит/с) и метод PSK (фазовый) для более быстрых модемов - скорость передачи до 2400 бод. В данное время существуют модемы способные передавать со скоростью более 56 000 бод.

При частотном методе сигнал "1" передается на частоте большей, чем сигнал "0".

Метод PSK использует всего две частоты: для передачи данных - 2400 Гц и для приема - 1200 Гц. Данные передаются по два бита, при этом кодировка осуществляется посредством сдвига фазы сигнала (табл.2).

1. **Таблица 2**

2. Сочетание бит	3. Сдвиг фазы (градус)
00	0
01	90
10	180
11	270

Модем выполняется либо в виде внешнего устройства, которое одним выходом подсоединяется к телефонной линии, а другим - к PC через последовательный асинхронный адаптер, либо в виде платы (внутренний

модем), которая устанавливается на общую шину PC (в слот материнской платы). Внешний модем проще в установке и имеет больше возможностей для контроля и настройки благодаря расположению и наличию светодиодных индикаторов (LED). Преимущество внутреннего модема заключается в цене и в том, что на рабочем месте оператора нет дополнительного периферийного устройства.

Типичный модем содержит следующие компоненты: специализированный микропроцессор, управляющий работой модема, оперативную память, хранящую значения регистров модема и буферизующую входную/выходную информацию, постоянную память, динамик, позволяющий выполнять звуковой контроль связи, а также другие вспомогательные элементы (трансформатор, резисторы, конденсаторы, разъемы). Современные модемы дополнительно содержат электрически перепрограммируемую постоянную память, в которой может быть сохранена конфигурация модема даже при выключении питания и устройства, позволяющие организовывать прием/передачу факсов.

На плате отдельных модемов имеются конфигурационные переключатели (свитчи), которые позволяют устанавливать некоторые параметры модема. Как правило, свитчами устанавливается адрес порта модема, который использует DOS для обмена данными с ним. Это могут быть COM1- COM4.

Другие параметры модема могут устанавливаться также переключателями типа JAMPER (джампер), расположенными на его плате.

Для обмена информацией модемами надо, чтобы они использовали одинаковые способы передачи данных по телефонным линиям. Для разработки стандартов передачи данных был создан специальный международный консультативный комитет по телеграфии и телефонии (ССТГТ).

Различают следующие режимы работы модема:

1. Режим передачи данных, в котором модем передает и принимает данные.
2. Режим команд, с помощью которых можно программировать работу модема.

Для режима команд нормой признан так называемый набор команд Hayes (фирма Hayes), состоящий из АТ-команд и обеспечивающий всем модемам единую основу для осуществления связи друг с другом. Эти

команды (за некоторым исключением) начинаются с префикса AT (Attention - внимание), который дополняется собственно командой с параметрами. Например, команда ATDP8W095 означает вызов (команда DP) абонента из Москвы (код 8, ожидание гудка, 095) по номеру 100.

Существует также два режима передачи команд PC и ответов модема: асинхронный и синхронный.

В *асинхронном* режиме формат передаваемой команды состоит из стартового бита, 8 битов данных и стоп-бита. В состав битов данных входит 1 бит проверки на четность.

В *синхронном* режиме стартовый бит и стоп-бит не передаются. Передача информации осуществляется в виде так называемых кадров, в состав которых входят заголовок, поле информации и комбинация проверки. В настоящее время в модемах, как правило, используется синхронный режим.

Передача данных на большие расстояния, как правило, подвержена ошибкам. Для решения таких проблем разработаны методы коррекции ошибок, которые вместе с методами сжатия данных определяются соответствующими протоколами.

Протоколом организации сети PC является Microcom Networking Protocol- MNP. MNP- коррекция может быть реализована или аппаратно (все современные модемы имеют встроенные протоколы коррекции ошибок) или на программном уровне с помощью телекоммуникационного пакета (ТП), входящего в Windows .

Принцип работы MNP-модема заключается в использовании при передаче информации блоков переменной длины. Модем принимает от компьютера подлежащие передаче данные и собирает их в пакет (блок), который затем передается. При этом вычисляется контрольная сумма, которая передается в конце пакета. При ошибочной передаче, в случае несовпадения объема переданной информации и контрольной суммы, модем на принимающей стороне затребует повтора передачи неправильно переданного блока.

При передаче важных данных (исполняемого кода архивированных данных и т.п.) ошибка даже в одном бите может привести к полной потере информации. Поэтому для надежного обмена файлами созданы различные алгоритмы передачи данных, которые называются протоколами. Наиболее известны протоколы ASCII, Xmodem, Ymodem, Zmodem, Kermit и т.п. Их

поддерживает ТП. Необходимо, чтобы программа, работающая на удаленном модеме, поддерживала протокол передающего модема. Для этого осуществляется предварительная «договоренность» о типе используемого протокола.

Повышение производительности достигается применением сжатия передаваемых данных. При этом математические методы аналогичны применяемым в утилитах архиваторов.

Наиболее простым способом обмена сообщениями и файлами с помощью модема является использование электронной доски объявлений BBS (Bulletin Board System). BBS - это станция (компьютер), снабженная одним или несколькими модемами, на которой выполняется специальная программа, предоставляющая возможность удаленным пользователям связываться с BBS по телефонным линиям.

Большинство станций BBS объединены в сеть FidoNet, которая представляет собой международную некоммерческую сеть пользователей PC многих стран.

Управляющая программа BBS организует диалог с пользователем, позволяет пользователю получить адресованные ему сообщения (почту), отправить их другим пользователям станции BBS или сети FidoNet. Кроме того, пользователь BBS получает возможность просматривать архивы файлов BBS, обмениваться с BBS файлами.

Порядок выполнения работы

Выполнить инсталляцию ТП в соответствии с нижеприведенной инструкцией.

Осуществить прямое соединение двух PC и произвести обмен данными (по инструкции).

Установить связь с помощью модема.

Проверить и при необходимости сделать переустановку характеристик.

Установить необходимую конфигурацию PC.

Войти в «Каталог абонентов» ТП, внести собственные данные и данные вызываемого абонента (в соответствии с предложенным преподавателем вариантом задания).

Набрать в соответствии с вариантом задания требуемый номер абонента, войти в связь, передать абоненту из каталога передачи подготовленный заранее файл.

4. ИНСТРУКЦИЯ

1. Инсталляция ТП

В первую очередь следует проверить, установлен ТП на ваш компьютер или нет. Для этого нажмите кнопку «Пуск», войдите в папку «Программы», выберите опцию «Стандартные». Если ТП установлен, то должны присутствовать программы «Прямое кабельное соединение», «Удаленный доступ к сети» и «Сервер удаленного доступа».

Для установки ТП выполните следующее:

1. Нажмите кнопку «Пуск».
2. Войдите в режим «Настройки», «Панель управления» и выберите значок «Установка и удаление программ».
3. Выберите пункт «Установка Windows».
4. Выберите значок «Связь» и нажмите кнопку «Состав».
5. Далее отметьте недостающие элементы и нажмите кнопку «ОК».

2. Прямое соединение (кабелем нуль-модема)

1. Соедините кабелем два PC.
2. Включите оба PC. Запустите Windows 98 . Нажмите «Пуск». В программах выберите папку «Стандартные». Запустите программу «Связь»/«Прямое соединение».
3. Пункты 1 и 2 выполняются на обоих PC.
4. Один из компьютеров выберите ведущим (только с этого PC можно будет управлять переносом файлов), другой – ведомым.
5. Выберите порт, к которому подключен кабель (нуль-модема), то же самое проделайте на другом компьютере. Установите связь.
6. Скопируйте файлы в соответствии с заданием.

3. Соединение при помощи модема

1. В меню «Стандартные» запустите программу «Связь»/«Новое соединение».
2. Введите название соединения, установите нужные параметры, после этого наберите номер абонента.

3. В соответствии с заданием выберите нужный пункт меню, установите протокол передачи (приема), передайте или примите файл.

Содержание отчета

1. Краткое описание конструкции, принципа работы, характеристик и возможностей модемов.
2. Распечатка файла, подготовленного для передачи.
3. Выводы по работе.

5. Вопросы и задания для самопроверки

1. Каким образом может быть организована передача информации по линии связи в цифровом виде?
2. Как организуется передача информации через аналоговые каналы связи?
3. Каково назначение модема? На каком принципе основана его работа?
4. Какие частотные полосы используются для приема-передачи модема?
5. Какие методы передачи сигналов используются в модемах?
6. Как конструктивно выполнен типичный модем?
7. Какие режимы использует модем при приеме-передаче данных? Изложите их суть.
8. В чем суть работы MNP-модемов?
9. Каково назначение протоколов, используемых модемами?
10. Каково назначение электронной доски объявлений?
11. Как осуществляется программирование модемов?
12. Пояснить порядок прямого соединения при передаче информации.
13. Как осуществить соединение при помощи модема?
14. Назвать основные параметры и характеристики модемов.

Библиографический список

1. Вычислительные машины, системы, сети и телекоммуникации: Учебник/ А.П.Пятибратов, С.Н.Беляев и др.; Под ред. проф. А.П.Пятибратова.-М.: Финансы и статистика, 1998.- с.: ил.
2. Олифер, В. Г. Основы компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2009. - 305 с. - (Учебное пособие). - ISBN 978-549807-218-0.
3. Карлащук В.И. Электронная лаборатория на IBM PC. Программа Electronics Workbench и ее применение.- М.: «Солон-Р», 1999.- 512 с.
4. Панфилов Д.И. и др. Электротехника и электроника в экспериментах и упражнениях: Практикум на Electronics Workbench: В 2 т./Под общей ред. Д.И. Панфилова – М.: ДОДЭКА, 2000.
5. Фигурнов, В.Э. IBM PC для пользователя / В.Э. Фигурнов. - Изд. 5-е, испр. и доп. - СПб. : Коруна : Информатика и компьютеры, 1994. - 352 с. - ISBN 5-87672-002-X.
6. Колесниченко О.В., Шишигин И.В. Аппаратные средства PC.- 4-е изд., перераб. и доп. – Спб.: БХВ-Петербург, 2001. – 1024 с.: ил.
7. Кушнир, А.Н. Новейшая энциклопедия компьютера / А.Н. Кушнир. - М. : Эксмо, 2008. - 975 с. - (Новейшая энциклопедия). - ISBN 978-5-699-24136-1.
8. Обжим сетевого кабеля // OBZHIMKABELJA.RU : рук. по монтажу ЛВС. 2009. URL: http://obzhimkabelja/ru/
9. MIPS // CITFORUM.RU Форум высоких технологий. 2011. URL: http://citforum.ru/hardware/app_kis/glava_7.shtml (дата обращения: 20.05.2012).
10. MIPS // CITFORUM.RU Форум высоких технологий. 2011. URL: http://citforum.ru/hardware/app_kis/glava_11.shtml (дата обращения: 20.05.2012).
11. MIPS // CITFORUM.RU Форум высоких технологий. 2011. URL: http://citforum.ru/hardware/app_kis/glava_8.shtml (дата обращения: 20.05.2012).
12. Ping и Traceroute // CITFORUM.RU Форум высоких технологий.2011. URL: http://citforum.ru/nets/semenov/4/45/ping_451.shtml (дата обращения: 20.05.2012).

ОГЛАВЛЕНИЕ

Вычислительные системы. Лабораторный практикум для студентов, обучающихся по направлению 230700 – Прикладная информатика.- (электронный ресурс)/ В.П.Галас, Владимир, 2013. 95 с.

Составитель:
ГАЛАС Валерий Петрович

Редакционно-издательский комплекс
Владимирского государственного университета.
600000, Владимир, ул. Горького, 87.