ГБПОУ «Пермский политехнический колледж имени Н.Г. Славянова»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

для реализации Программы подготовки специалистов среднего звена
по специальности
09.02.01 Компьютерные системы и комплексы
(технологический профиль профессионального образования)

Рассмотрено и одобрено на заседании
Предметной цикловой комиссией
«Информационные технологии»
Протокол №14
от 29 августа 2022г.
Председатель ПЦК
_____ Н.В. Кадочникова

2022

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Практические занятия относятся к основным видам учебных занятий и составляют важную часть теоретической и профессиональной практической подготовки, являются формой организации учебного процесса, направленной на выработку у обучающихся практических умений для изучения последующих учебных дисциплин, профессиональных модулей и для решения профессиональных задач.

Выполнение обучающимся практических работ направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам учебных дисциплин профессиональных модулей;

- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;

- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;

- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Практические занятия проводятся в учебных кабинетах лабораториях, мастерских. Необходимыми структурными элементами практического занятия, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также анализ и оценка выполненных работ и степени овладения студентами запланированными умениями.

Наряду с формированием умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать теоретические знания на практике.

Содержание практического занятия определяется перечнем профессиональных умений по конкретной учебной дисциплине

(профессиональному модулю), а также характеристикой профессиональной деятельности выпускников, требованиями к результатам освоения основной профессиональной образовательной программы.

По каждой учебной дисциплине и междисциплинарному курсу для обучающихся разработаны методические указания по выполнению практических работ.

Работы, носящие репродуктивный характер, отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Работы, носящие частично поисковый характер, отличаются тем, что при их проведении студенты не пользуются подробными инструкциями, им не дан порядок выполнения необходимых действий, и требуют от студентов самостоятельного подбора оборудования, выбора способов выполнения работы в инструктивной и справочной литературе и др.

Работы, носящие поисковый характер, характеризуются тем, что студенты должны решить новую для них проблему, опираясь на имеющиеся у них теоретические знания.

Формы организации студентов на практических занятиях: фронтальная, групповая и индивидуальная.

При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.

При групповой форме организации занятий одна и та же работа выполняется микро-группами по 2—5 человек.

При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.

Оценки за выполнение практических работ являются показателями текущей успеваемости студентов по учебной дисциплине.

ПРИЛОЖЕНИЕ

Методические указания для обучающихся по выполнению практических работ по учебным дисциплинам и междисциплинарным курсам

Код	Наименование учебной дисциплины, профессионального модуля, междисциплинарного курса	№ Приложения
ОУД.01	Русский язык	1
ОУД.02	Литература	2
ОУД.03	Иностранный язык	3
ОУД.04	Математика	4
ОУД.05	История	5
ОУД.06	Физическая культура	6
ОУД.07	Основы безопасности жизнедеятельности	7
ОУД.08	Астрономия	8
ОУД.09	Информатика	9
ОУД.10	Физика	10
ОУД.11	Родная литература	11
ИУК.01	Основы профессиональной деятельности	12
СГ.01	История России	13
СГ.02	Иностранный язык в профессиональной деятельности	14
СГ.03	Безопасность жизнедеятельности	15
СГ.04	Физическая культура	16
СГ.04	Адаптивная физическая культура	17
СГ.05	Основы финансовой грамотности	18
СГ.06	Экологические основы природопользования	19
СГ.07	Психология общения	20
ОП.01	Элементы высшей математики	21
ОП.02	Дискретная математика	22
ОП.03	Инженерная компьютерная графика	23
ОП.04	Основы электротехники и электронной техники	24
ОП.05	Операционные системы и среды	25
ОП.06	Основы алгоритмизации и программирования	26
ОП.07	Метрология и электротехнические измерения	27
ОП.08	Информационные технологии	28
ОП.09	Сетевые технологии	29
МДК.01.01	Основы проектирования цифровой техники	33
МДК.01.02	Разработка и прототипирование цифровых систем	34
МДК.02.01	Микропроцессорные системы	35
МДК.02.02	Программирование микроконтроллеров	36
МДК.02.03	Системы управления базами данных	37
МДК.02.04	Разработка прикладных приложений	38

МДК.03.01	Техническое обслуживание и ремонт аппаратной части компьютерных систем и комплексов	39
МДК.03.02	Настройка и обеспечение функционирования программных средств компьютерных систем и комплексов	40
МДК.04.01	Проектирование и наладка беспроводных сетей	41
МДК.05.01	Веб-программирование	42

ПРИЛОЖЕНИЕ 29

Методические указания для выполнения практических работ по учебной дисциплине ОП.09 Сетевые технологии

Автор: Баранов Сергей Юрьевич,
ГБПОУ «Пермский политехнический колледж имени Н.Г. Славянова» преподаватель высшей квалификационной категории

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по выполнению практических занятий обучающимися по дисциплине **ОП.09 Сетевые технологии** предназначены для студентов специальности 09.02.01 «Компьютерные системы и комплексы».

Цель методических указаний: оказание помощи обучающимся в выполнении практических работ по ОП.09 Сетевые технологии

Настоящие методические указания содержат работы, которые позволят обучающимся закрепить теоретические знания, сформировать необходимые умения и навыки деятельности по профессии, направлены на формирование следующих компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.

ОК 04 Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 4.1. Осуществлять монтаж кабельной сети и оборудования локальных сетей различной топологии;

ПК 4.2. Выполнять работы по эксплуатации и обслуживанию сетевого оборудования

В результате изучения дисциплины ОП.09 Сетевые технологии, обучающийся должен

уметь:

- Анализировать структурную организацию ЭВМ и ВС;
- использовать программное обеспечение ЛВС;
- оценивать эффективность функционирования ТВС;
- выбирать необходимое сетевое оборудование локальных сетей и конфигурировать локальные сети;
- выбирать наборы сетевых протоколов для различных приложений;
- работать с конкретными программными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС.

знать:

- элементную базу ЭВМ;
- устройства ЭВМ и управление ими;
- программное обеспечение компьютерных сетей;
- классификацию вычислительных сетей;
- эталонную модель взаимосвязи открытых систем;
- построение, методы доступа, протоколы локальных вычислительных сетей;

- технологии корпоративных сетей, включая протоколы TCP/IP.
- физические принципы передачи информации в сетях;
- основы информационной безопасности на уровне сетей;
- тенденции и перспективы развития современных средств телекоммуникаций и сетевых технологий

Описание каждого практического занятия содержит: раздел, тему, количество часов, цели работы, что должен знать и уметь обучающийся, теоретическую часть, порядок выполнения работы, контрольные вопросы, учебно-методическое и информационное обеспечение.

На выполнение практических работ по ОП.09 Сетевые технологии отводится 36 *часов.*

Практическая работа №1

Тема: Программы для моделирования СКС

Цель: Научиться создавать проект локальной сети с учетом предлагаемых требований.

Методические указания и задания к лабораторной работе

В настоящее время довольно часто бывает необходимым проявить знания и умения выполнения проектов локальной сети. Обычно, для проектирования сети в крупных фирмах и организациях приглашают сотрудников фирм, занимающихся проектированием и монтажом сетей. Если фирма небольшая, то иногда целесообразно проводить проектирование и монтаж сети «своими» силами. Поэтому, рассмотрим основные этапы проектирования локальной сети для небольшой фирмы, состоящей из определенного количества сотрудников, которая занимает определенное количество комнат и этажей.

Основные этапы проектирования локальной сети:

1 Определение количества сотрудников, использующих PC.

2 Определение планируемого расширения штата фирмы (при проектировании локальной сети необходимо предусмотреть планируемое расширение фирмы, чтобы в дальнейшем была возможность подключения дополнительных узлов к сети).

3 Определение количества комнат и этажей, занимаемых фирмой с возможностью дальнейшего расширения.

4 Выбор физической топологии сети.

5 Выбор оптимального сетевого оборудования (коммутаторов, концентраторов) с учетом планируемого расширения и бюджета фирмы.

6 Выбор сетевого кабеля и предварительный подсчет метража в соответствии с метражом комнат.

7 Возможность использования сетевых коробов, пач-панелей, пачкортов, розеток, коммуникационных шкафов для размещения свичей, управляемых свичей, серверов, если необходимо обеспечить физический доступ к оборудованию сотрудников фирмы.

8 Выбор типа сети – одноранговая сеть, сеть на основе сервера, комбинированная сеть.

9 Определение типов серверов для сети на основе сервера и комбинированной сети (файловый сервер, сервер приложений, сервер-маршрутизатор, почтовый сервер, принт-сервер). Возможность совмещения услуг, предоставляемых серверами (например, можно объединить почтовый сервер и сервер-маршрутизатор, или файловый сервер и принт-сервер).

10 Определить уровень безопасности, необходимый для нормального функционирования фирмы и хранения коммерческой информации, исходя из этого выбрать, под какой операционной системой будут работать рабочие станции локальной сети и сервера.

11 Выбрав коммуникационное оборудование и дополнительное оборудование для монтажа сети, произвести с учетом текущих цен на сетевое оборудование расчет сметы расходов проекта локальной сети фирмы.

Задание к работе (часть 1)

Небольшую фирму, состоящую из «A» сотрудников, занимающую «B» этажей в одном здании, размещающуюся в «C» комнатах (количество комнат на этажах выбрать самостоятельно из указанного количества, приведенного в таблице), необходимо обеспечить локальной сетью.

Последнее время увеличился объем работы и в будущем планируется расширение штата (D человек).

У каждого сотрудника есть компьютер. Информация строго конфиденциальна. Одновременно с установкой сети планируется установка лазерного принтера (выбрать оптимальное количество принтеров для нормальной работы фирмы). Планируется, что будет использоваться сетевая база данных, необходим сервер для хранения информации.

Предложите проект локальной сети для этой фирмы. Необходимо привести примерный план размещения сотрудников по комнатам, перечислить сетевое оборудование, обосновать выбор данного сетевого оборудования, необходимого для нормальной работы сети, описать топологию, которой Вы будете придерживаться, проектируя сеть, обосновать выбор. Описать обязанности сотрудников по отношению к сети (будет ли ими производиться настройка адаптеров и т.д.). Какие меры безопасности Вы бы предложили для сохранения конфиденциальности информации. Посчитать стоимость проекта с учетом выбранного сетевого оборудования.

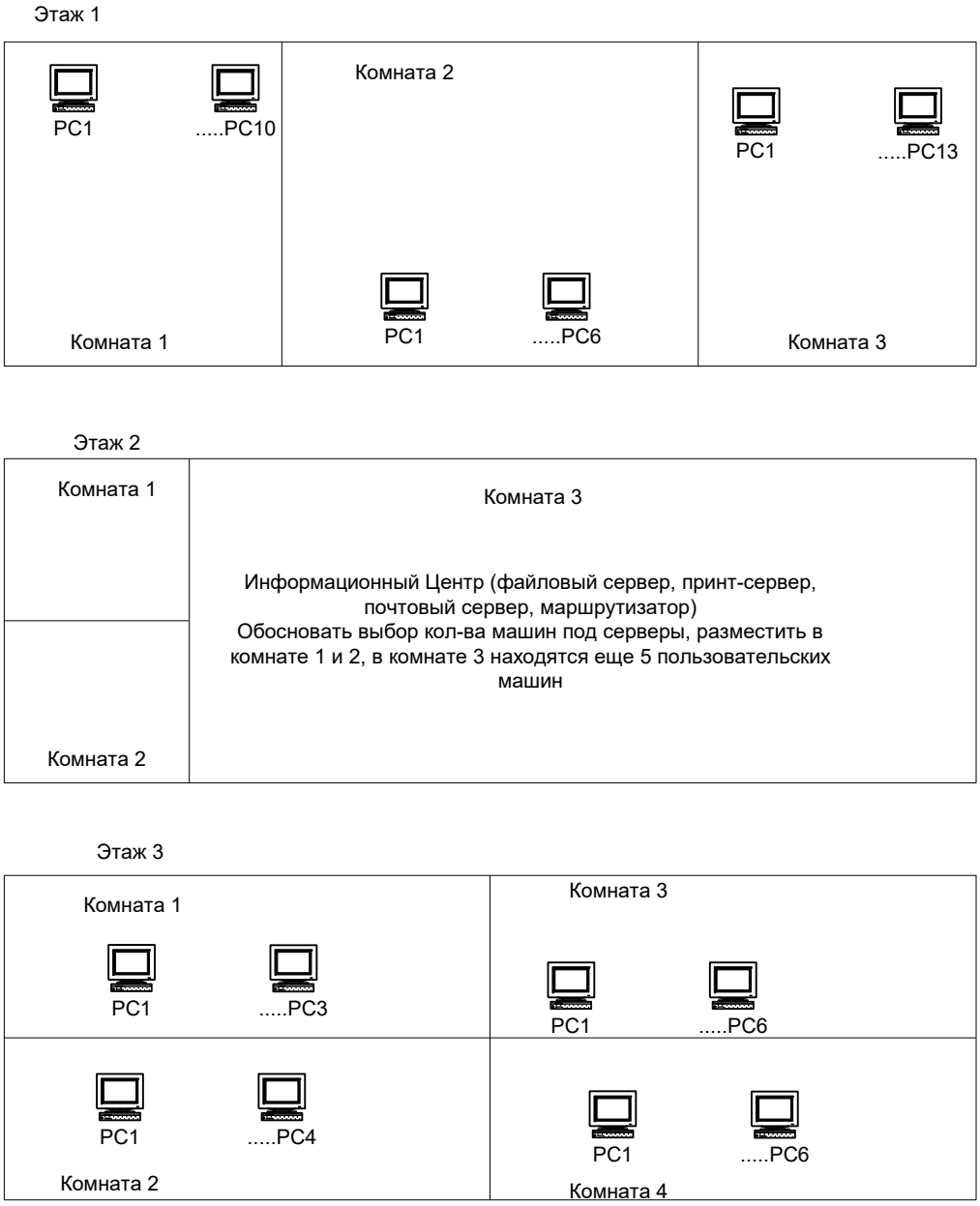
Варианты работы приведены таблице 1.

Таблица 1 – Варианты заданий

№ варианта	«A» сотрудники	«B» этажи	«C» комнаты	«Д» расширение
1	10	2	3	5
2	12	1	4	5
3	12	2	3	8
4	10	1	2	5
5	7	1	2	3
6	8	1	4	5
7	9	1	3	7
8	10	2	2	5
9	12	2	5	5
10	12	1	2	8
11	10	1	4	5
12	7	1	2	3
13	8	1	2	5
14	9	1	2	7
15	15	2	4	8
16	15	2	4	10
17	17	2	4	12
18	20	3	5	12
19	20	3	5	10
20	17	2	3	12
21	16	1	4	5
22	16	2	5	6
23	18	1	4	7
24	22	2	5	8
25	22	1	4	9
26	17	2	3	10
27	30	2	4	5
28	31	2	5	5
29	32	2	4	7
30	33	1	2	8

Задание к работе (часть 2, вариант для всех один)

Предложите проект локальной сети для этой фирмы, план размещения сотрудников которой приведен на рисунке 1. Необходимо перечислить сетевое оборудование, обосновать выбор данного сетевого оборудования, необходимого для нормальной работы сети, описать топологию, которой Вы будете придерживаться, проектируя сеть, обосновать выбор. Описать обязанности сотрудников по отношению к сети (будет ли ими производиться настройка адаптеров и т.д.). Какие меры безопасности Вы бы предложили для сохранения конфиденциальности информации.



Исходные данные взять из рисунка 1.
Рисунок 1– План размещения PC для проектирования ЛВС (задача 2)

Требования к отчету:
Отчет по лабораторной работе должен содержать:
Задание, описание проекта (в соответствии с требованиями к заданию по лабораторной работе).

Контрольные вопросы:
1. Что такое ЛВС. Типы ЛВС.
2. Что такое топология сети. Какие основные топологии сетей Вы знаете?
3. Какие коммутирующие устройства необходимы для функционирования ЛВС.
4. Какие типы кабеля вы знаете? Принципиальные отличия?
5. Обоснование выбора сетевого адаптера. Каким требованиям он должен удовлетворять?
6. Каким образом в Вашем проекте выполняется обеспечение защиты информации на серверах и на рабочих станциях.

Практическая работа №2

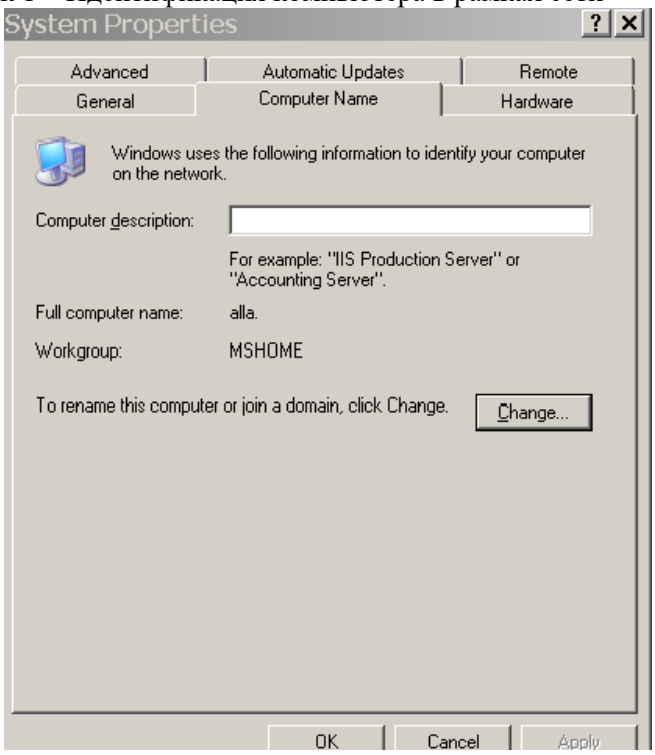
Тема: Оформление технического задания на проектирование СКС

Цель работы: Освоить принципы настройки сетевых параметров ОС Windows на остове полученного технического задания.

Методические указания к выполнению работы

Для настройки сети машины, подключенной к локальной сети, необходимо обратиться к «Свойствам» «Сетевого окружения» (рисунок 1)

Рисунок 1 – Идентификация компьютера в рамках сети



Здесь необходимо указать имя компьютера в сети, к какой группе принадлежит (например, PMI), и заполнить «Описание компьютера» (иногда совпадает с именем компьютера).

Теперь следует обратиться к вкладке «Конфигурации» (Рисунок 2)

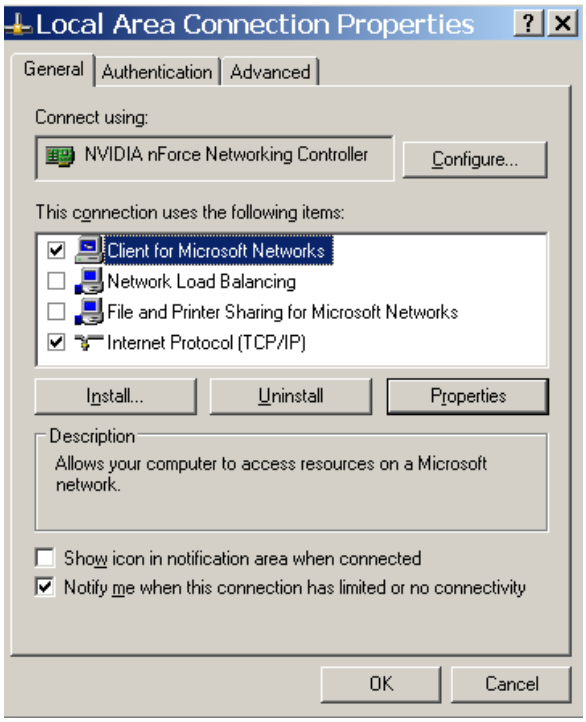


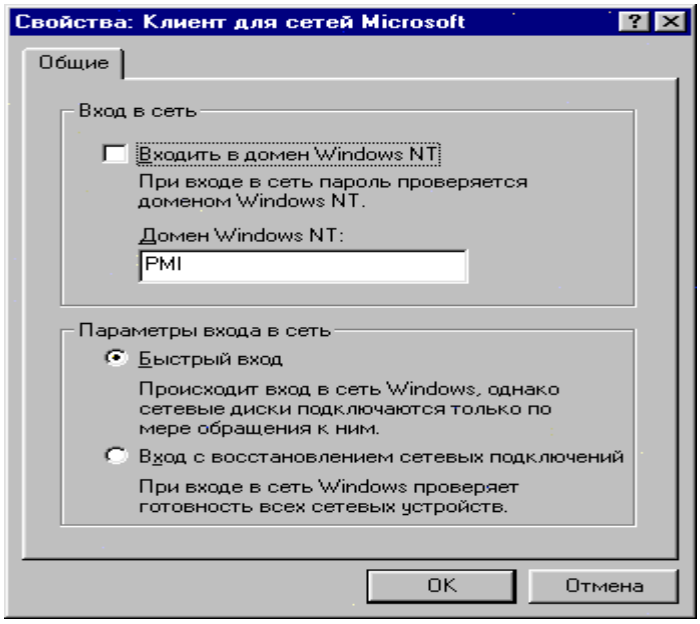
Рисунок 2 – Просмотр установленных компонентов

Для установления сети на локальном компьютере необходимо установить ряд протоколов и служб. На рисунке 2 показано, какие компоненты могут быть установлены для определенного компьютера (могут быть некоторые изменения в зависимости от типа сети).

Например, служба доступа к файлам и принтерам устанавливается в том случае, если необходимо организовывать доступ к локальным ресурсам узла для других пользователей или иметь доступ к ресурсам, предоставляемыми другими узлами сети.

Способ входа в сеть может быть или «Клиент для сетей Microsoft» или «Обычный вход в Windows». Выбор того или иного способа связан также с особенностями сети. Пользователи, объединенные в группы (например, PMI) для входа в сеть обычно используют способ входа в сеть - «Клиент для сетей Microsoft». При таком входе при загрузке компьютера предлагается ввести логин и пароль, после чего будут доступны ресурсы сети, разрешенные для использования данной рабочей группы и, непосредственно, вошедшему под определенным логином и паролем пользователю.

Рисунок 3 – «Свойства Клиент для сетей Microsoft»



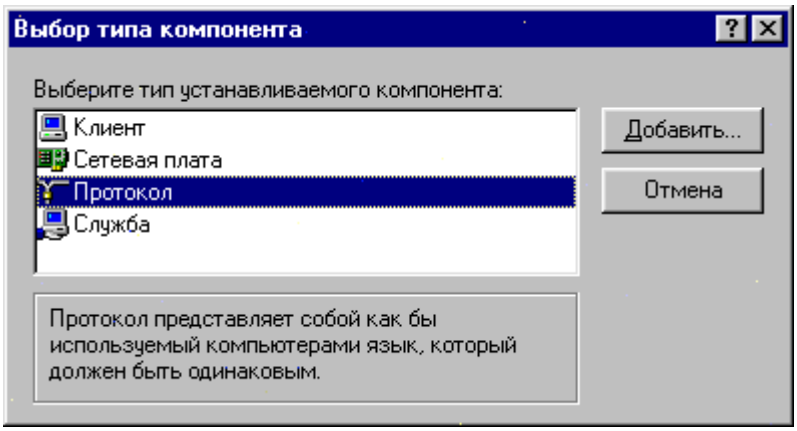
«Клиент для сетей Microsoft» обеспечивает связь с другими компьютерами и серверами, работающими в среде Microsoft Windows, а также доступ к общим файлам и принтерам. Нажав на «Свойства», можно просмотреть следующую информацию (рисунок 3)

Далее следует установить протоколы, необходимые для осуществления доступа в сеть. Чтобы добавить новый протокол необходимо выполнить «Добавить…» и из предложенного списка выбрать протоколы.

С помощью «Добавить», можно также выбрать и другие типы устанавливаемых компонент (служба, клиент, сетевая плата) (рисунок 4)

Рисунок 4 – Выбор типа устанавливаемого компонента

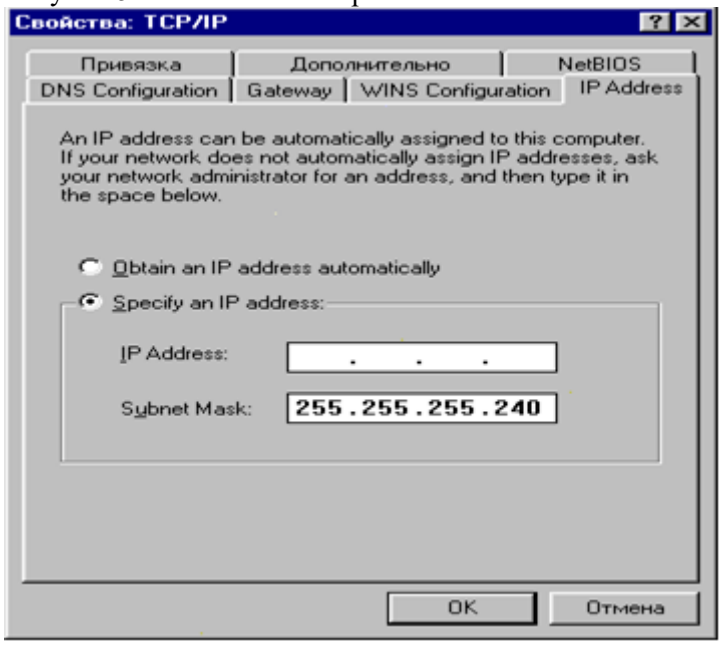
Следует особое внимание обратить на настройку «TCP/IP» - стек протоколов, используемый для подключения к Internet.



Настройка TCP/IP включает в себя набор вкладок. На каждой вкладке предложено ввести основные свойства TCP/IP. К таким свойствам относятся IP-адрес, маска подсети, сервер DNS, шлюз, привязка.

Установка IP-Address (рисунок 5). IP- Address конкретного узла можно узнать у администратора сети.

Рисунок 5 «Свойства» Настройка TCP/IP



Маска подсети может быть различной, значение маски подсети связано с особенностями организации сегментов сети и назначается также администратором сети.

«Gateway» или шлюз – устройство, которое обеспечивает выход в другую сеть, назначается администратором сети.

Сервер DNS осуществляет соответствие между IP-адресами и именами узлов. В DNS прописывается адрес этого сервера.
Для конкретной сети маска подсети, Gateway, DNS Server свои. При настройке сети на Вашем компьютере и незнанию вышеперечисленной информации, следует обратиться к системному администратору.
Следует помнить о том, что вся перечисленная выше информация, прописываемая в свойствах TCP/IP, может устанавливаться автоматически, без непосредственного участия пользователя. Автоматическое назначение IP-адресов, DNS-сервера, шлюза, маски подсети выполняется с помощью DHCP-сервера. DHCP-сервер настраивается в сети, и как только производится включение компьютера, узел посылает DHCP-запрос на получение основных параметров конфигурации, а DHCP – сервер назначает все перечисленные свойства TCP/IP автоматически. При этом значительно упрощается процесс настройки сети на локальном узле.
Одной из особенностей работы DHCP-сервера является то, что IP-адрес узла может назначаться по-разному. Первый вариант, когда IP-адреса выделяются динамически из пула свободных адресов. Второй вариант, когда в целях безопасности и разграничения доступа к ресурсам по IP-адресам, IP-адреса назначаются статически, т.е. происходит привязка IP-адреса к MAC-адресу сетевой карты. Если в первом варианте у клиента, подключающегося к сети, каждый раз может быть разный IP-адрес из пула свободных, то во втором случае, каждому клиенту IP-адрес устанавливается жестко на все время.
Для быстрого просмотра настроек сети Вашего компьютера в ОС Windows воспользуйтесь командой ipconfig, запущенной из командной строки. Вызов командной строки – команда cmd.
Информация по команде ipconfig:

ipconfig [/? | /all | /release [адаптер] | /renew [адаптер]| /flushdns | /registerdns | /showclassid адаптер | /setclassid адаптер [устанавливаемый_код_класса_dhcp]] адаптер

Полное имя или имя, содержащие подстановочные знаки "*" и "?" из допустимого множества:

* - любое количество символов, ? - один любой символ.

ключи:

/?	Отобразить это справочное сообщение.
/all	Отобразить полную информацию о настройке параметров.
/release	Освободить IP-адрес для указанного адаптера.
/renew	Обновить IP-адрес для указанного адаптера.
/flushdns	Очистить кэш разрешений DNS.
/registerdns	Обновить все DHCP-аренды и перерегистрировать DNS-имена
/displaydns	Отобразить содержимое кэша разрешений DNS.
/showclassid	Отобразить все допустимые для этого адаптера коды (IDs) классов DHCP.
/setclassid	Изменить код класса DHCP (ID).

По умолчанию отображается только IP-адрес, маска подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.
Для ключей /Release и /Renew, если не указано имя адаптера, то будет освобожден или обновлен IP-адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.
Для ключа SetClassID, если не указан код класса (ID), то существующий код класса будет удален.
Примеры:

> ipconfig - Отображает краткую информацию.
> ipconfig /all - Отображает полную информацию.
> ipconfig /renew - Обновляет сведения для всех адаптеров.
> ipconfig /renew EL* - Обновляет сведения для адаптеров, начинающихся с EL....
> ipconfig /release *ELINK?21* - Освобождает IP-адреса для всех адаптеров, удовлетворяющих запросу, например, ELINK-21, myELELINKi21adapter.

В разнородной сети (в сети, где используются различные операционные системы) бывает затруднительно настроить локальную сеть таким образом, чтобы ресурсы одного узла с операционной системой, например, ОС Windows были доступны для узлов с ОС Windows Чтобы избежать подобных проблем, и для быстрого поиска узла по его NetBIOS-имени, можно использовать дополнительные возможности сетевых настроек, в частности использование файла lmhosts.sam. Этот файл содержит таблицу соответствия IP-адресов и обычных (NetBIOS) имен компьютеров. Каждый элемент должен располагаться в отдельной строке. IP-адрес должен начинаться с первой позиции строки, а за ним следует соответствующее имя компьютера. IP-адрес

и имя компьютера должны быть отделены друг от друга хотя бы одним пробелом или символом табуляции. Знак "#" используется обычно для указания на начало комментария.
Для быстрого доступа к ресурсам узлов, находящихся в других подсетях, можно прописать соответствии IP-адресов полным именам узлов.
Этот файл называется hosts и содержит сопоставления IP-адресов именам узлов. Каждый элемент должен располагаться в отдельной строке. IP-адрес должен находиться в первом столбце, за ним должно следовать соответствующее имя. IP-адрес и имя узла должны разделяться хотя бы одним пробелом. Кроме того, в некоторых строках могут быть вставлены комментарии, они должны следовать за именем узла и отделяться от него символом '#'.
Например:
194.44.183.17 donntu.edu.ua # узел клиента x
127.0.0.1 localhost

Следует обратить внимание на то, что использование файлов hosts и lmhosts.sam целесообразно использовать в том случае, если узлы, к которым Вы хотите получить более быстрый доступ, получают один и тот же IP-адрес (статический) при настроенном DHCP-сервере.
Установка дополнительных протоколов зависит от конфигурации сети, необходимость установки тех или иных протоколов можно узнать у сетевого администратора.

Задание к лабораторной работе:

В соответствии с изложенным теоретическим материалом, выполнить ряд действий по установке сетевых компонентов. Посмотреть сетевые настройки на локальном компьютере, уметь объяснить использование соответствующих протоколов и их свойств, ответить на контрольные вопросы.

Контрольные вопросы:

1. Какие сетевые протоколы Вы знаете?
2. Какие транспортные протоколы Вы знаете?
3. Что такое привязка?
4. Объяснить основные настройки TCP/IP.
5. Функции DHCP.
6. Что такое шлюз?
7. Назначение маски подсети?
8. Какие параметры сети могут назначаться сервером DHCP.
9. Назначение файлов hosts и lmhosts.sam.
10. Что такое MAC-адрес.
11. Какую информацию позволяет увидеть команда ipconfig?

Практическая работа №3

Тема: Построение схемы компьютерной сети

Цель работы: Ознакомиться с основными построения СКС и командами для проверки сети в OS Windows и OS Linux.

После того, как выполнены все сетевые настройки, необходимо проверить, есть ли сеть. Это можно сделать с помощью следующих команд:
Ping – проверяет соединение с удаленным хостом;
Использование: ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]] [-w интервал] списокРассылки
Параметры:

-t Отправка пакетов на указанный узел до команды прерывания.
-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 времени 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 интервал Интервал ожидания каждого ответа в миллисекундах.

Web-сервер кафедры ПМиИ имеет IP Address 194.44.183.180. Если передачи данных нет, то возможны ошибки в сетевых настройках, либо Web-сервер кафедры выключен. Для проверки наличия сетевого подключения можно в качестве тестируемого адреса выбрать адрес прокси-сервера ДонНТУ – 194.44.183.17.

Для определения участка сети, где прерывается передача данных можно использовать команду:

tracert – определяет маршрут, фактически выбранный к узлу назначения.

Использование: tracert [-d] [-h максЧисло] [-j списокУзлов] [-w интервал] имя

Параметры:

-d Без определения адресов по именам узлов.
-h максЧисло Максимальное число переходов при поиске узла.
-j списокУзлов Свободный выбор маршрута по списку узлов.
-w интервал Интервал ожидания каждого ответа в миллисекундах.

В Windows есть еще несколько полезных команд:

netstat – показывает статистику протоколов и TCP соединений;

NETSTAT [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]

-a Отображение всех подключений и ожидающих портов.

-e Отображение статистики Ethernet. Этот ключ может применяться вместе с ключом -s.

-n Отображение адресов и номеров портов в числовом формате.

-p имя Отображение подключений для протокола "имя": tcp или udp. Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip.

-r Отображение содержимого таблицы маршрутов.

-s Отображение статистики по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ -p позволяет указать подмножество выводящихся данных.

- интервал Повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

nbtstat – показывает статистику протоколов и TCP/IP – соединений при работе через NetBIOS.

NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-s] [S] [interval]]

Route – ручное управление маршрутными таблицами;

ARP – показывает и модифицирует таблицы трансляции IP-to-Ethernet адресов.

-a Вывод текущих записей таблицы ARP путем опроса текущих данных протокола. Если указан адрес inet_addr, то адреса IP и физические выводятся только для указанного компьютера. Если протокол ARP используется несколькими сетевыми интерфейсами, то выводятся записи из каждой таблицы ARP.

-g Аналог -a.

inet_addr Задание адреса IP.

-N if_addr Вывод текущих записей таблицы ARP для сетевого интерфейса, определяемого параметром if_addr.

-d Удаление узла, определяемого параметром inet_addr.

-s Добавление узла и связывание адреса IP inet_addr с физическим адресом eth_addr. Физический адрес задается с помощью 6 шестнадцатеричных чисел, разделяемых дефисами. Запись является постоянной.

eth_addr Задание физического адреса.

if_addr Необязательный параметр, указывающий адрес IP интерфейса, для которого следует изменить таблицу адресов. Если параметр не задан, используется первый доступный интерфейс.

Образец::

> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Добавляет статическую запись.
> arp -a .... Выводит таблицу arp.

FTP – передает и принимает файлы для узла, имеющего FTP-сервис.

Обмен файлами с компьютером, на котором запущена служба сервера FTP. Ftp может использоваться интерактивно.

FTP [-v] [-d] [-i] [-n] [-g] [-s:имя_файла] [-a] [-w:буфер] [узел]

-v Отключение вывода на экран ответов с удаленного сервера.

-n Отключение автоматического входа при начальном подключении.

-i Отключение интерактивных запросов при передаче нескольких файлов.

-d Включение отладочного режима.

-g Отключение глобализации имен файлов (см. команду GLOB).

-s: имя_файла Задание текстового файла, содержащего команды FTP, которые будут выполняться автоматически при запуске FTP.

-a Использование локального интерфейса для привязки соединения.

-w:буфер Переопределение стандартного размера буфера передачи (4096).

узел Задание имени или адреса IP удаленного узла, к которому необходимо выполнить подключение.

Команды для работы с сетью в OS Linux

Команды, предназначенные для установления соединения с удаленной системой и проведения сеанса работы после установления соединения.

host – выводит IP-адрес указанной системы, используя службу DNS. Можно указать IP-адрес, и он будет преобразован в имя системы.

Параметры: -d – отладочный режим;

-C – вывод списка всех систем в зоне;

-dd - аналогично d, но в более подробной форме.

hostname – выводит имя локальной системы.

-d – выводит имя DNS-сервера;

-f – вывод полного имени системы;

-s – краткого имени системы;

ping – отправляет пакеты на указанную систему для определения пропускной способности сети. Для получения более подробной информации см. man ping.

rlogin – позволяет провести сеанс работы на удаленной системе. Для получения более подробной информации см. man rlogin.

rwall <система> – отправляет сообщение всем пользователям, подключенным к указанной системе.

talk пользователь [терминал] – позволяет 2-м пользователям вели интерактивный разговор.

finger – выводит информацию об указанном пользователе.

- l – выводит информацию в подробном формате

Задание к лабораторной работе:

Изучить команды для тестирования сети в ОС Windows и ОС Linux.

Проанализировать работу утилит для проверки работоспособности сети. Результаты работы всех команд по проверке сети представить в виде отчета. Уметь прокомментировать результаты работы сетевых утилит.

Контрольные вопросы:

1) Что такое FTP? Какие команды для работы с FTP Вы знаете?
2) Назначение протокола ARP и RARP.
3) Выполнить сравнительный анализ работы 2-х протоколов транспортного уровня – TCP и UDP.
4) Что такое DNS.
5) Если на компьютере есть локальная сеть, но нет выхода в Internet, в чем может быть проблема? Объясните все возможные причины отсутствия выхода в Internet.

Практическая работа № 4

Тема: Оформление технического задания на проектирование СКС.

Цель: Оформление ТЗ на проектирование СКС Установка и настройка программы NetView. Изучение основных возможностей программы NetView.

Программа NetView распространяется свободно.

Методические указания к работе

Программа NetView предназначена для анализа сетевого окружения, сбора данных о доступных сетевых ресурсах. В качестве основных возможностей можно выделить следующие:

- получение доступа к рабочим станциям;
- получение доступа к HTTP и FTP серверам;
- получение детальной информации о рабочей станции - IP и MAC адреса, тип установленной ОС, список работающих на компьютере сетевых сервисов, список пользователей в системе, список подключенных к доступным ресурсам компьютеров, время на удаленной машине, какие порты открыты на машине;
- возможность выполнения поиска файлов в сети;
- мониторинг активных сетевых подключений, с возможностью создания «черного» и «белого» списков;
- отслеживание соединения с заданными портами (полезно для обнаружения IP-адресов, с которых проводятся попытки установить соединения на “троянские” порты или выполнение попытки сканирования портов). Имеет функцию «Scan chaser», при включении которой удаленный сканер портов показывает открытыми практически все порты. Имеется поддержка скриптов, позволяющая в простейшем случае эмулировать серверные службы;
- встроенный «Terminal», основанный на скриптах, позволяющий подключаться к любому выбранному порту либо его прослушивать. Также может использоваться IRC, telnet, pop3 или любым другим текстовым протоколом;
- «NetMessenger» - позволяет слать сообщения Windows Messenger. Аналог NET SEND с возможностью посылки сообщений от произвольного имени. Под Win'9x есть возможность принимать сообщения (WinPopup).
- «TraceRoute» - аналог утилиты tracert. Отображение машин либо в виде списка, либо в виде дерева сегментов (используется traceroute). Карта составляется и обновляется практически автоматически. Также возможно отображение в виде визуальной карты, с возможностью задания произвольных иконок для компьютеров.
- «Traffic Redirector» - позволяет прослушивать входящие соединения на заданный (свободный) порт и перенаправлять их на другой порт другого IP.

Огромным достоинством данной программы является ее доступность. Программа является абсолютно бесплатной, также доступны и исходные коды почти всех модулей.

Рассмотрим интерфейс программы. Главное окно программы NetView представлено на рисунке 1.

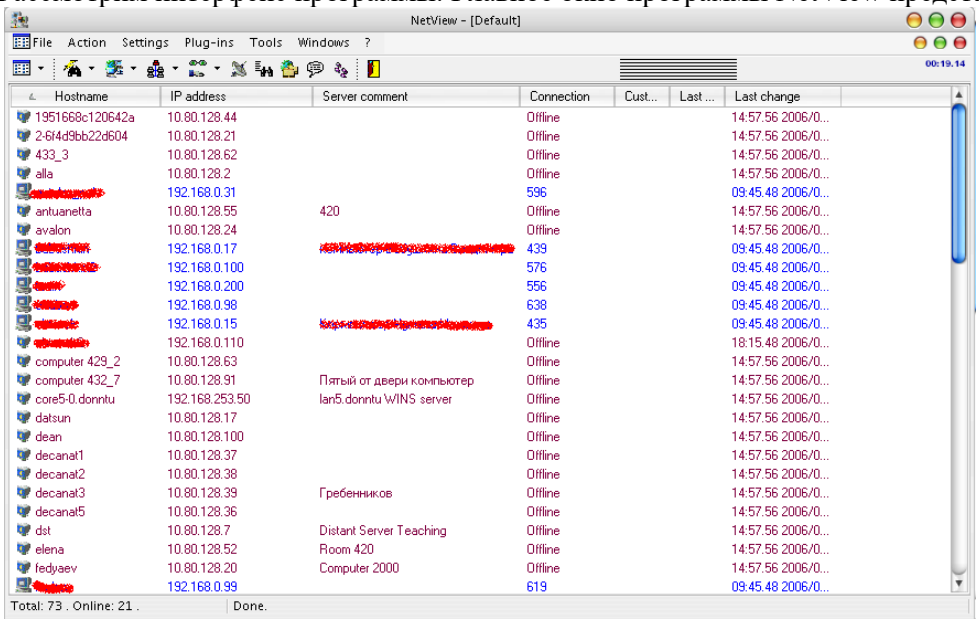


Рисунок 1 - Основное окно программы

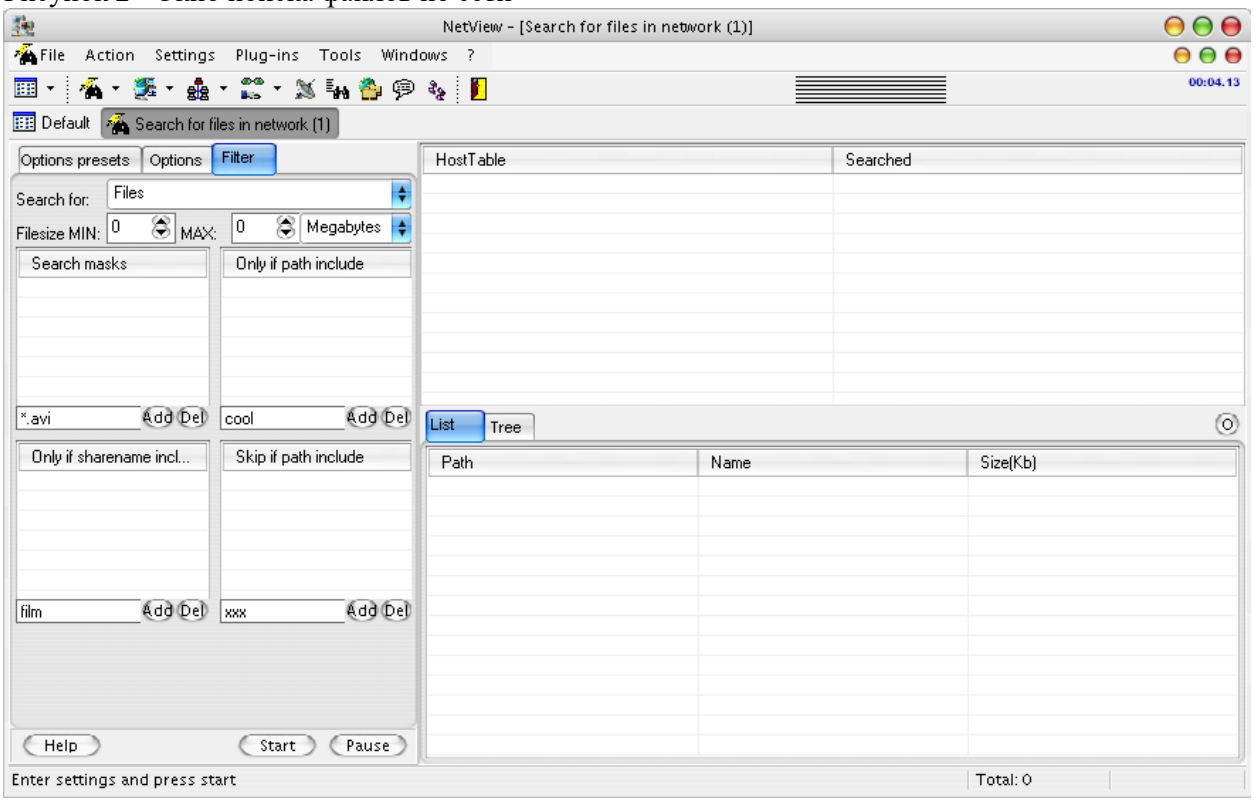
Основное окно программы содержит список всех компьютеров в сети (имя, IP-адрес, комментарии, наличие соединения)

Хост-лист (рис. 1) – это объект, содержащий узлы, линии и области визуальной карты. Хосты могут отображаться различными цветами в зависимости от текущего состояния offline, online, opened и

alarm. Узел находится в состоянии «Opened», если он открывался хотя бы один раз в текущем сеансе работы. Узел находится в состоянии «Alarm», если для него выполнено оповещение, например, о том, что он выключился. При этом он будет находиться в таком состоянии до тех пор, пока пользователь не щелкнет по записи мышью. Узлы можно переносить из одного хост-листа в другой, указав нужный хост-лист в поле Hostlist окна редактирования свойств компьютера. Можно включить автоматическую группировку узлов по имени рабочей группы, либо по первым трем цифрам их IP-адреса. Это задается в главном меню-> «Settings»-> «Autosplit». Там же можно отключить автогруппировку или перенести все узлы в основной хост-лист. В настройках можно включить пункт Delete empty lists для того, чтобы автоматически удалялись пустые хост-листы. Данные всех хост-листов NetView хранит в файле (по умолчанию default.nvh, либо default.sam). Информация хост-листа может представляться в четырех видах, которые можно переключать из контекстного меню-> «Current sublist»-> «View as»:
1 – Список. В этом случае отображаются только иконки, соответствующие состояниям хостов и их названия. Дополнительная информация, такая как IP, рабочая группа, состояние, заметки отображаются во всплывающей подсказке при наведении мышки на хост.
2 – Детально. Информация отображается в виде списка со столбцами (столбец имен, IP адресов и тд). Столбцы можно менять в окне редактирования хост-листа. Ширину столбцов и сортировку также можно менять, она сохраняется в файле хост-листа и восстанавливается при следующем запуске. Если хост-лист не сохранить перед выходом, и если выключено «Autosave hostlist» в настройках, то эта информация также не сохранится.
Колонки:
- «Hostname» – имя узла, собственное, либо DNS.
- «IP address» – IP-адрес.
Следующие столбцы включены и настроены по умолчанию, но их можно изменить в окне редактирования хост-листа:
- «Server comment» - комментарий сервера. Устанавливается на самом сервере. Виден только если при обновлении списка машин хост был включен.
- «Connection» - значение в миллисекундах задержки ICMP эхо-ответа, при включенной проверке PINGами, задержка установления соединения, при включенной проверке соединением на заданный порт, либо количество ресурсов на хосте, если включен «Enum shares on host».
- «Custom» - редактируемый Вами комментарий к хосту.
- «Last time» - время последнего открытия компьютера, с момента запуска NetView.
- «Last change» - время/дата последнего изменения online/offline состояния хоста.
3 – Визуальный план. Уменьшенная в 2 раза визуальная карта без возможности редактирования.
4 – Визуальная карта. Этот режим предназначен для визуализации компьютерной сети. Вы можете ставить компьютеры в любое место на карте, соединять их различными линиями, задавать им различные картинки, зависящие от состояния узла. Хосты можно также объединять в прямоугольные области, и щелкнув правой кнопкой мыши в любое место области, можно перепроверить все узлы в ней, выбрав пункт меню «Recheck area». Для того чтобы изменить название области и цвет ее границ нужно щелкнуть правой кнопкой в любое место внутри ее и выбрать «Edit area label». После изменения текста и цвета, нужно нажать Enter, либо Esc для отмены. Линии на карте рисуются с помощью пункта контекстного меню «Start line». Начните рисовать линию, левым щелчком добавляется узел, правым рисование линии завершается, и она закрепится на карте. Для удаления любой линии просто щелкните на ней правой кнопкой и выберите «Delete line». Линии могут быть различной толщины, цветов и стиля. Редактируются эти параметры из контекстного меню -> «Edit line». При этом Вы попадете в окно конфигурации хост-листа, все параметры, касающиеся линий, будут задавать только выделенную линию. Картинки, изображающие устройства, задаются при их редактировании. Размеры карты и фоновую текстуру можно также менять, для этого надо щелкнуть правой кнопкой по карте и выбрать «Current sublist»-> «Settings». Объекты можно произвольно таскать по карте. Можно выделить сразу несколько узлов линий, узлов и областей и переносить их вместе. Можно нажав левой кнопкой на заголовок какой-нибудь области выделить ее и все находящиеся в ней объекты, чтобы затем переносить все вместе. Можно менять размер областей.
5 – Карта маршрута
На карте маршрутов показана схема соединения узлов сети. Составляется она путем выбора пункта меню «Retrace all» главного меню либо путем трассирования выделенных хостов или текущего хост-листа через контекстное меню хост-листа. При этом следует учесть, что некоторые серверы

могут ограничивать количество ICMP-запросов с Вашего компьютера, что может привести к трассировке не всех узлов. В этом случае следует пользоваться пунктом «Trace all» главного меню - он трассирует только те узлы, маршрут до которых еще не был успешно найден. Просто нажимайте его несколько раз, пока количество узлов на карте не перестанет добавляться. Информация этой карты сохраняется с хост-листом в .nvh файл и может экспортироваться в файл формата .txt через подменю «File» главного меню. Карта также имеет контекстное меню с основными функциями - открыть хост, перепроверить, трассировать, редактировать, удалить из хост-листа, посмотреть свойства. Пункт меню «Delete from map» удаляет узел вместе со всеми дочерними из карты маршрутов, сохраняя их в хост-листе. «Clear route map» очищает карту маршрутов.
Довольно часто бывает необходимым произвести поиск каких-либо файлов, которые могут находиться на различных узлах сети, например, поиск технической литературы, музыки. В рассматриваемой программе имеется возможность выполнения поиска файлов среди всех узлов сети. На рисунке 2 представлено окно поиска файлов (NetSearcher)

Рисунок 2 - Окно поиска файлов по сети

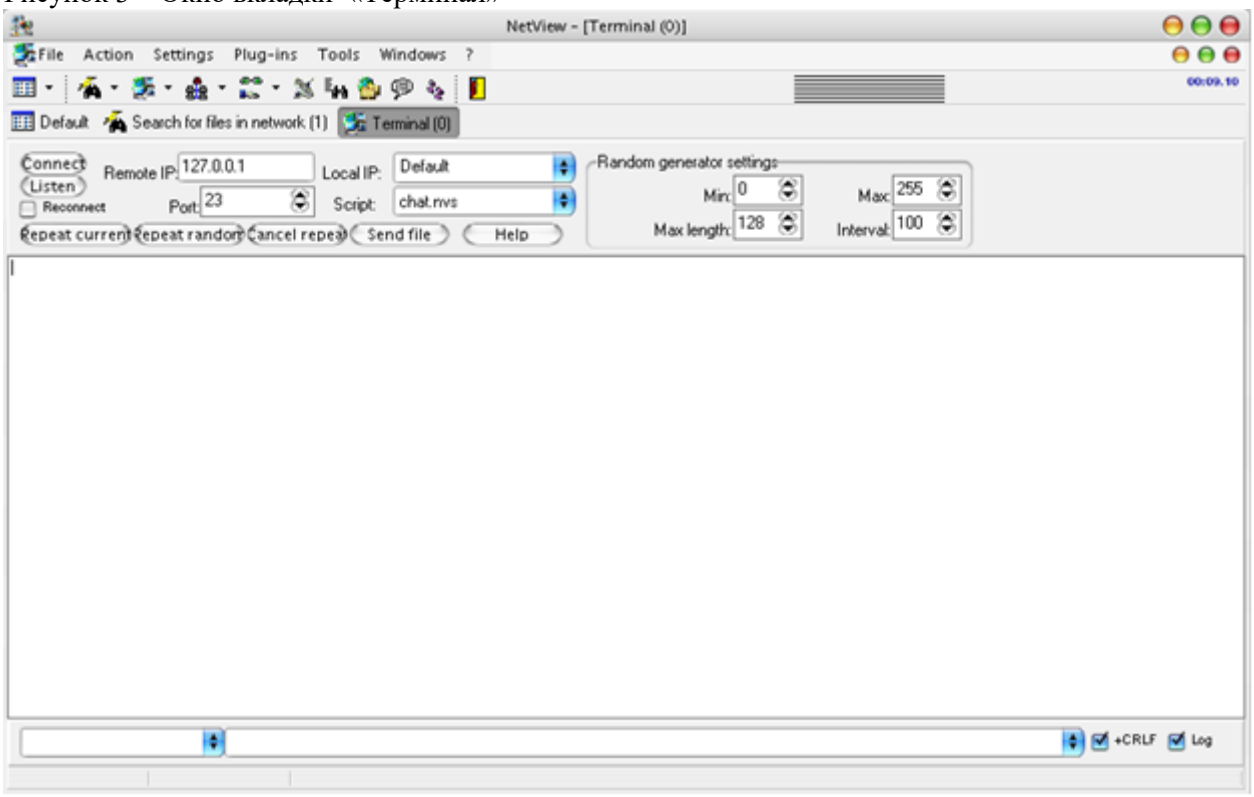


Это поисковик файлов в сети, позволяющий искать файлы и каталоги по заданным маскам (нескольким одновременно), размеру файла. Есть возможность выполнять поиск файлов как по NETBIOS, так и по FTP протоколам. Можно редактировать список машин, подлежащих поиску, сохранять результаты поиска в текстовый файл либо в .html виде с ссылками. Поиск может вестись в циклическом режиме, пока не будет выполнено сканирование всех машин списка. Используется многопотоковый механизм поиска, значительно ускоряющий поиск. Найденные файлы можно автоматически скачать во время или в конце поиска. Настройки поиска можно сохранять. Поиск файлов может работать в режиме обновления списка - периодически начиная поиск, добавляя в список новые файлы и удаляя те, которые он не видел больше указанного количества часов.
Рассмотрим настройки:
«Time limit» - ограничение времени на сканирование одного хоста. Если какой-то хост сканируется время большее, чем здесь указано - он автоматически пропускается (в поле «Searched» ставится "yes").
«Cycled searching» - режим циклического поиска, при котором поиск проводится циклически, пока для всех хостов не будет Searched="yes" или пока поиск не будет прерван вручную нажатием кнопки "Stop";
«Save filelist on finish» - при включенном флажке список файлов будет сохранен автоматически после окончания процесса поиска. При щелчке по этому флажку открывается окно, в котором указываются опции сохранения списка файлов.

«Recheck hosts» - перепроверять хост перед тем, как искать файлы. Экономит время, если в списке много выключенных машин.
«Autosearch on» – автоматическое начало сканирования по таймеру. В Формат задания времени начала автоматического сканирования: "08:10;10:45;16:30" или "06:30".
«Threads count» - максимально количество потоков одновременного поиска (каждый поток сканирует отдельный хост одновременно с другими, что ускоряет поиск, но на слабых машинах с установленной Win 9x большое количество потоков может значительно замедлить работу системы).
«Priority» - приоритет потоков. Малое значение замедляет поиск при одновременном выполнении других программ, большое - замедляет другие программы.
«Use script» - позволяет задать скрипт из каталога \Scripts\Searcher, который может обрабатывать результаты поиска файлов.
«Enable list-update mode» - включает режим обновления списка файлов, при котором поисковая система при сохранении списка файлов в файл автоматически сохраняет состояние списка во временный .sfl файл в каталоге NetView, при следующем поиске NetView загрузит этот файл и будет добавлять туда лишь новые файлы.
«Delete if not found on searched» - после завершения поиска «NetSearcher» проходит по созданному списку файлов, удаляет из него те файлы, которые были удалены с хостов, на которых был успешно проведен поиск
«Display files as new for» - здесь можно указать в течение скольких часов после первого нахождения поисковик будет считать файлы новыми. Новые файлы выделяются в html списке цветом.
«Delete files not refreshed for» - если нужно, чтобы старые файлы, которых поисковик не видел в течение определенного периода времени, удалялись автоматически - включите эту опцию и укажите, по истечении скольких часов после последнего обнаружения файлы будут удаляться.

Терминал (Terminal) - средство, позволяющее подключаться к удаленному IP/порту и работать в терминальном режиме.

Рисунок 3 – Окно вкладки «Терминал»



Если в системе установлено несколько IP, можно выбрать локальный адрес, с которого устанавливается подключение. Кнопкой «Send file» можно послать небольшой файл. Терминал также можно использовать для ожидания входящих соединений (server). Для этого надо выбрать локальный порт и адрес и нажать «Listen». Обработкой поступающего потока информации и выводом на экран занимаются скрипты терминала.

TCP мост (Traffic redirector) – «слушает» соединения на указанный порт, и при запросе на соединение устанавливает соединение с удаленным сервером на любой порт, и в дальнейшем перенаправляет траффик между ними.

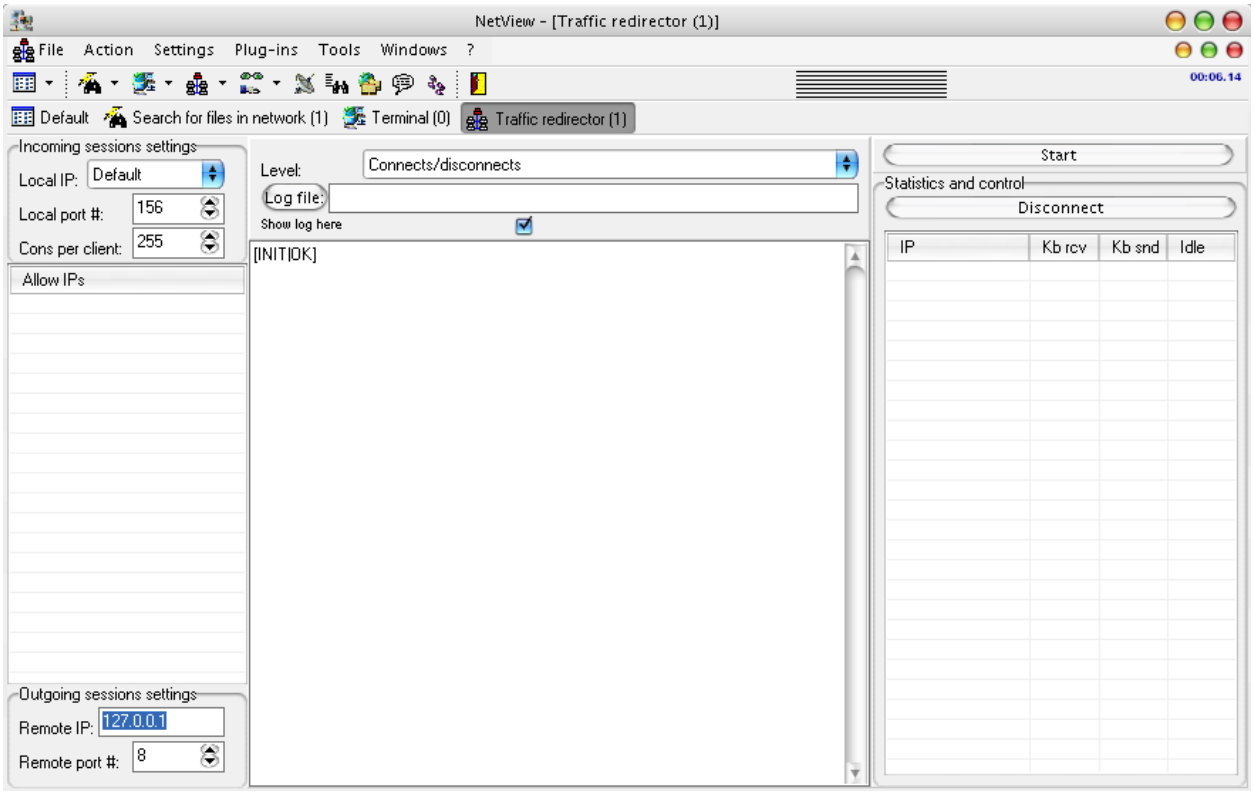


Рисунок 4 - Окно вкладки «Traffic redirector»

Traffic redirector позволяет задавать разрешенные IP адреса, отключать любое соединение принудительно, ведет лог (3 уровня детализации). Полезно, например, если Вы хотите, чтобы через Вас кто-то мог подключиться к сервису на другом компьютере, к которому Вы имеете доступ, а этот кто-то нет.

Монитор подключений (NetWatcher) - монитор активных сетевых соединений.

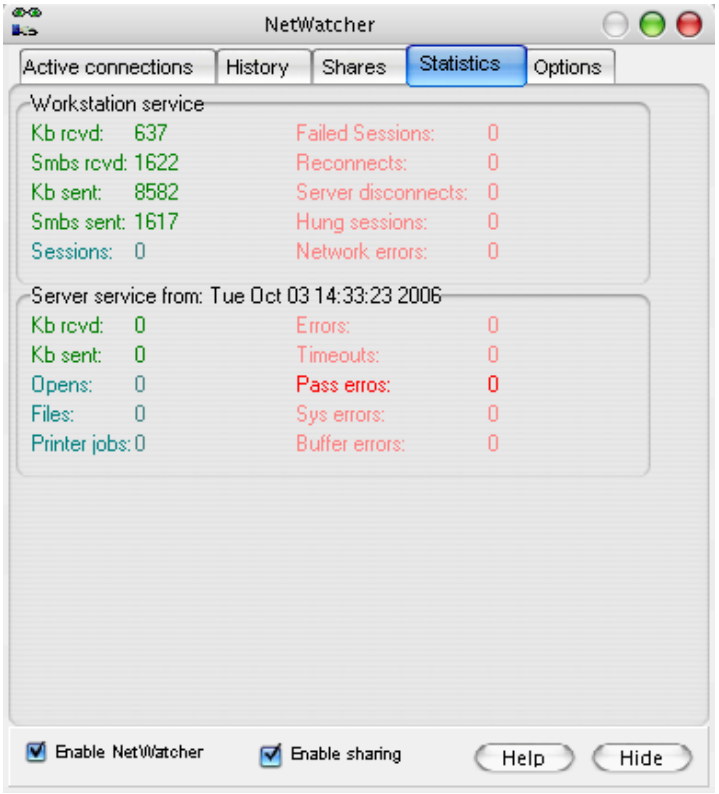


Рисунок 5 - Монитор подключений (NetWatcher) (вкладка Статистика)

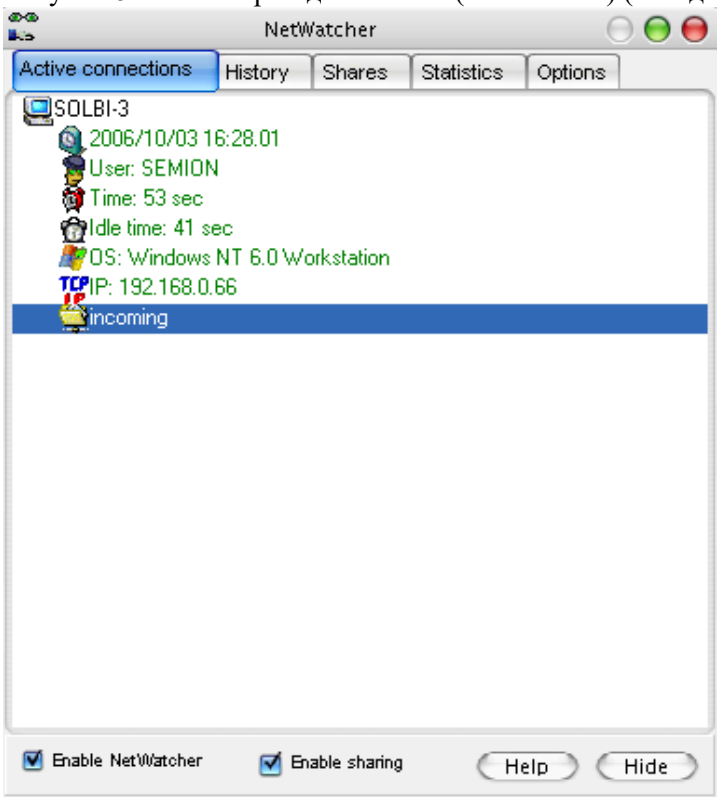


Рисунок 6 - Монитор подключений (NetWatcher)
(вкладка Активные соединения)

«NetWatcher» - Позволяет видеть, что скачивается с Вашего компьютера в данный момент и в недалеком прошлом. Можно прервать любую сессию. Ведется лог соединений, в котором пишется имя и IP-адрес компьютера, имя пользователя, установившего сессию, тип используемой ОС и все открытые за сессию файлы. Файлы, открытые для чтения, рисуются зеленым цветом, для записи - фиолетовым, а созданные - красным. Есть функция «черного» и «белого» списков. По умолчанию любой пользователь из «черного» списка отключается автоматически. Можно поставить

отключение всех пользователей, кроме «белого» списка. Также выводится статистика по службам SERVER и WORKSTATION в системе.
Вкладка «Active connections» – просмотр всех текущих подключений и открытых файлов. Как только файл закрывается, он автоматически переносится в «History». Файлы, открытые для чтения, отмечены синим, для записи - фиолетовым, созданные - красным цветами. Ресурсы, открытые в сессии, также отображаются здесь, но коричневым цветом.
Вкладка «History» - история всех соединений. Хранится в лог-файле. Размер ее для удобства чтения может быть ограничен максимальным количеством клиентов.
Вкладка «Shares» - список доступных ресурсов на Вашем компьютере.
Вкладка «Options» - здесь находятся все настройки «NetWatcher» и kick/keep/popup/skip списки пользователей. В списки можно вносить либо просто пользователей, либо делать ограничения различным пользователям на различные ресурсы. «Skip-лист» - это список компьютеров, которые не будут вноситься в лог.
Здесь же задаются горячие клавиши для вызова окна «NetWatcher» и отключения всех подключенных на данный момент пользователей.

IP монитор (IP logger) - Выводит список текущих TCP/UDP соединений.

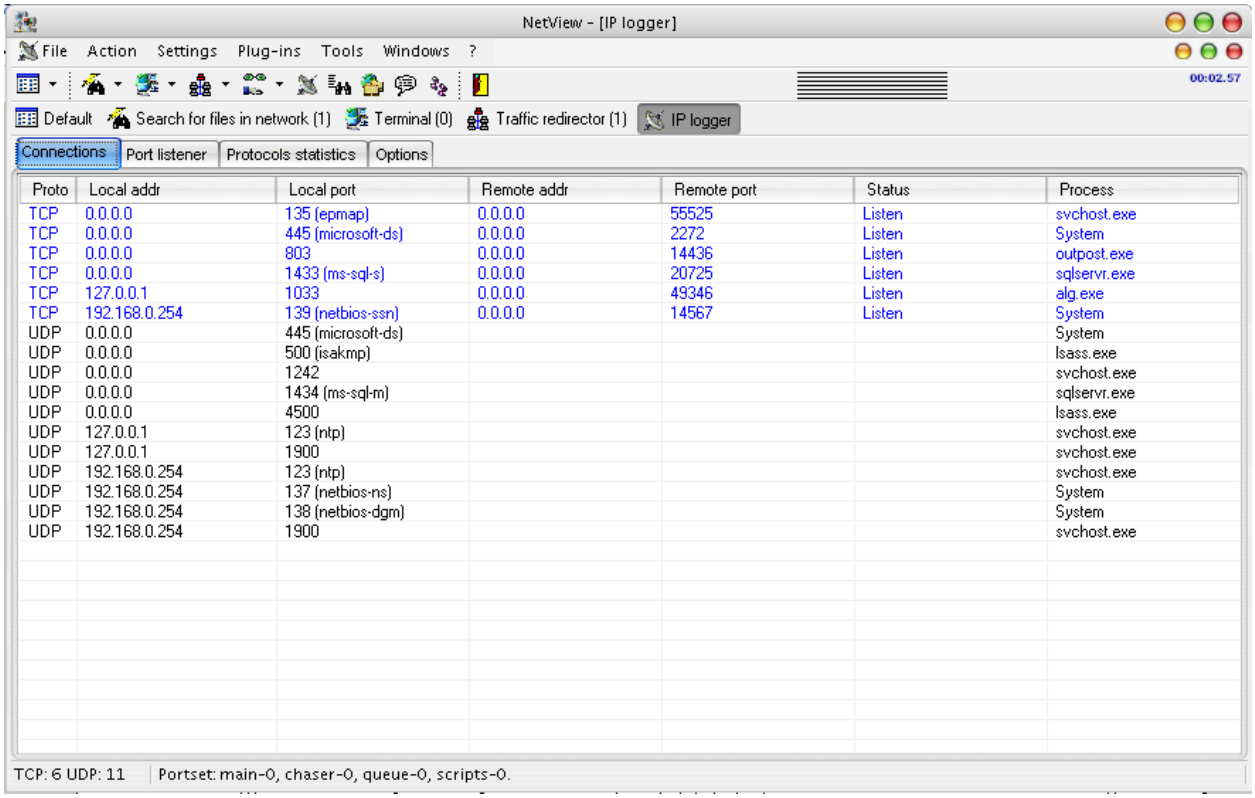


Рисунок 7 - IP монитор (IP logger)

«IP logger» выводит имя процесса, который использует открытый порт. Работает только на Win XP, выводит также статистику по протоколам TCP, IP, ICMP. Имеет функцию предупреждения о сетевых DOS атаках типа SYN, UDP и ICMP flood. Для этого необходимо установить порог срабатывания оповещения. Для ICMP и SYN пакетов можно установить ~100 запросов в секунду. Если количество запросов будет превышать это число, прозвучит сигнал оповещения. С помощью IP logger можно вести логи установленных соединений, причем можно использовать фильтрацию лога.

Сканер сети (Network scaner) - Сканер, позволяющий находить открытые порты на одном, либо диапазоне IP адресов.

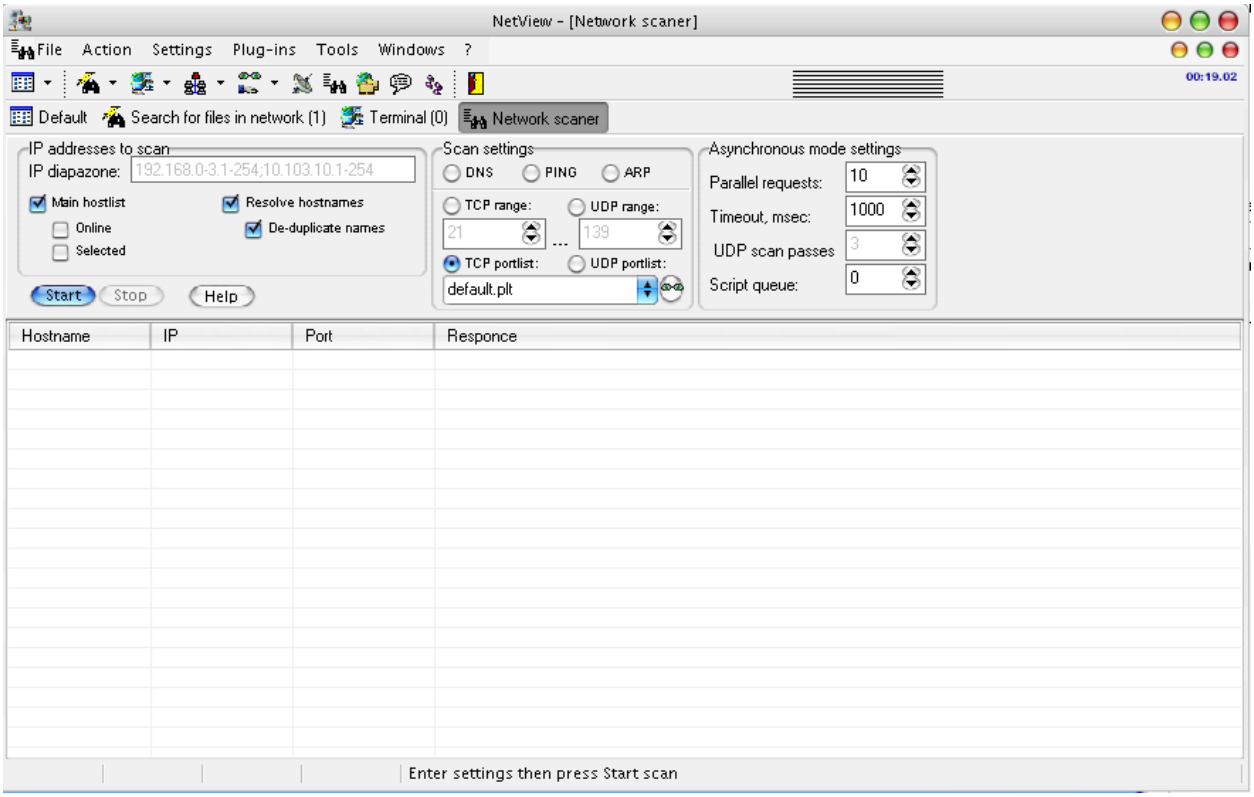


Рисунок 8 - Сканер сети (Network scaner)

Порты можно сканировать также в каком-то диапазоне, либо по списку в файле. При нахождении IP-адреса автоматически определяется соответствующее имя компьютера, которое тут же можно внести в общий список. Если удаленный компьютер сразу после соединения посылает какую-либо строку, она выводится в столбце «Responce». Есть возможность перебирать IP-адреса, находя те, которые прописаны в DNS, или пинговать диапазон, или составленный список IP адресов. Также можно сканировать узлы из хост-листов - для этого включите «Main hostlist». Если включить «Online» сканер, будет сканировать только включенные узлы, что ускорит процесс сканирования. Можно выделить несколько узлов в списке и включив «Selected» просканировать только их. Опция «Parallel requests» регулирует максимально число одновременных запросов. «Timeout» - время ожидания ответа на каждый запрос, не работает для DNS и ARP сканирования.
Описание типов сканирования:

- DNS - сканер последовательно пытается определить имена у всех IP-адресов. Если имя определяется - то адрес и имя вносятся в список найденных.
- PING - сканер последовательно пингует все адреса, в список найденных добавляются те, которые ответили на запрос. В «Responce» пишется задержка эхо-ответа в миллисекундах.
- ARP - сканер последовательно шлет ARP-запросы на определение MAC-адреса каждого IP. Работает только в пределах сегмента (до маршрутизатора). В поле «Responce» записываются найденные MAC адреса.
- TCP - сканер сканирует IP адреса, пытаясь подключиться к портам из диапазона или файла - списка портов. Возможно исполнение скриптов при нахождении открытых портов. Скрипты могут подробно исследовать удаленные системы. В столбце «Responce» пишется либо результат исследования скрипта, либо, если скрипта для найденного порта нет, - строка, которую шлет удаленный хост сразу при подключении.
- UDP - сканер сканирует UDP порты на указанных адресах следующим методом: вначале NetView посылает на указанные порты пакет с данными размером 1 байт. Затем, через указанный интервал времени проверяет, на какой из портов пришел отклик ICMP «Destination port unreachable» и исключает их из списка открытых портов. Затем повторно обходит те же порты и делает это столько раз, сколько указано в UDP «scan passes» каждый раз, исключая закрытые порты. Отсюда и особенность сканирования - при сканировании, например выключенного или заблокированного файерволом IP, сканер покажет открытыми все UDP-порты. В столбце «Responce» или ничего не пишется или пишется результат исследования скриптом.

Сканер ресурсов (Resources scaner) - Отображает все доступные сетевые ресурсы.

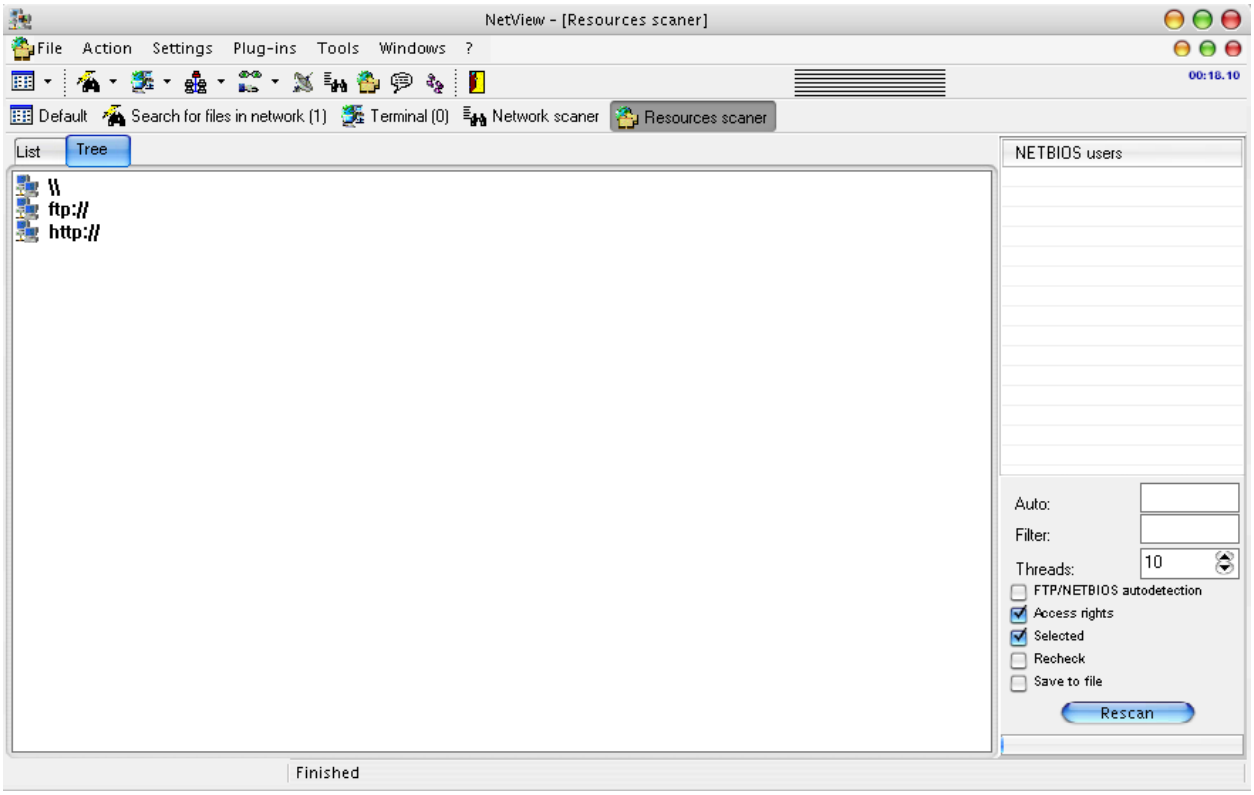


Рисунок 9 – Окно сканера ресурсов

Этот модуль может использоваться для 2-х целей:

- Составляет список доступных по FTP/NETBIOS ресурсов на всех компьютерах сети, с указанием прав доступа для различных пользователей. Можно задать имена пользователей, от которых проводится подключение, также проводится попытка перечисления пользователей удаленного узла (работает применительно к WIN'NT/2000). Нажав правой кнопкой, можно открыть сетевой ресурс, либо подключить сетевой диск (для NETBIOS). Опция «Selected» позволяет сканировать только выделенные во всех хост-листах узлы. Результат можно сохранить в текстовый файл SHARELIST.TXT в каталоге NetView. Либо включив опцию «Save to file» - в этом случае NetView автоматически сохранит этот файл после завершения сканирования. Включив опцию «Recheck» можно ускорить сканирование за счет того, что не будут производиться попытки подключиться к отключенным узлам.
- По умолчанию сканер ресурсов ищет FTP и NETBIOS ресурсы на узлах в зависимости от их настроек. При включении опции FTP/NETBIOS autodetection, сканер ресурсов будет определять наличие таких ресурсов автоматически (путем сканирования портов 139, 445 и 21) и при необходимости менять настройки узлов хост-листе.

Задание к лабораторной работе

1 Исследовать все возможности программы NetView, установив программу на рабочей станции.

2 Сохранить скриншоты работы основных модулей программы и поместить их в отчет по лабораторной работе.

3 Оценить достоинства и недостатки данной программы, если пользовались другой подобной программой провести анализ программы NetView относительно других известных Вам программ, позволяющих выполнять мониторинг сетевых подключений.

Содержание отчета:

1 Задание к лабораторной работе.

2 Скриншоты работы основных модулей программы NetView, установленной и запущенной с рабочей станции в локальной сети.

3 Оценка статистики по сетевым подключениям.

4 Достоинства и недостатки программы NetView.

Контрольные вопросы:

1 Перечислите основные модули программы NetView.

2 Что такое UDP протокол, к какому уровню он относится, его назначение.

3 Протокол TCP, его назначение, отличие от UDP-протокола.

4 Протокол ARP, назначение.

5 Что такое ICMP протокол, какую информацию можно посмотреть благодаря программе NetView по ICMP-пакетам.

6 Что такое DOS-атака, какие средства встроены в программу NetView для контроля за DOS-атакой.

Практическая работа №5

Тема: Управление рисками в СКС. Типовые неисправности в СКС. «Сетевой шторм»

Цель работы: Изучить типовые неисправности в СКС. Изучение основных возможностей и использование в сети программы «Friendly Pinger».

Методические указания к лабораторной работе

Friendly Pinger - это мощное приложение для администрирования, мониторинга и инвентаризации компьютерной сети.

Общие возможности программы:

- визуализация компьютерной сети в красивой анимационной форме;
- отображение, какие компьютеры включены, а какие нет;
- пингование всех устройств;
- оповещение в случае остановки/запуска серверов;
- инвентаризация программного и аппаратного обеспечения всех компьютеров в сети;
- слежение, кто имеет доступ к Вашему компьютеру и какие файлы качает;
- назначение внешних команд (например, telnet, tracert) устройствам;
- поиск HTTP, FTP, e-mail и других служб, которые присутствуют в Вашей сети;
- отображение состояния сети на рабочем столе или Web странице;
- графический TraceRoute;
- открытие компьютеров в проводнике или Total Commander;

На рисунке 1 представлен интерфейс программы Friendly Pinger (Основное окно программы).

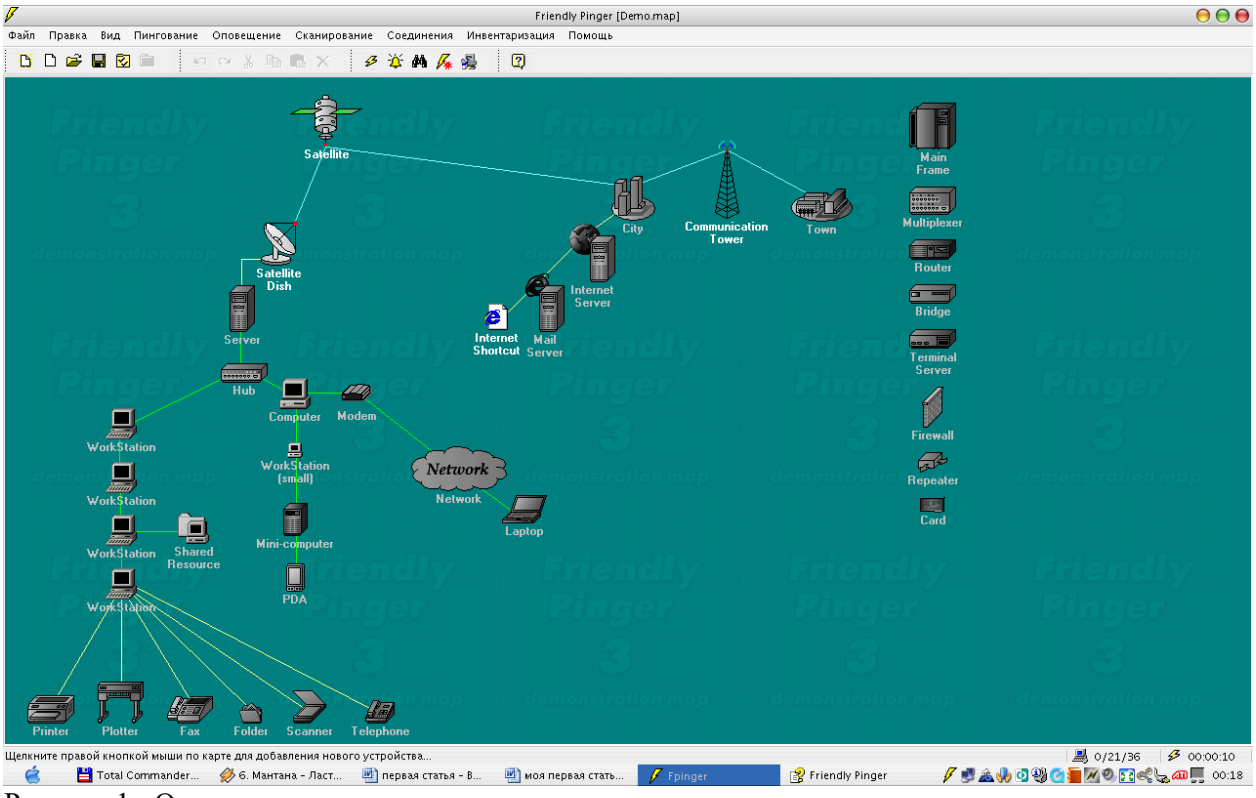


Рисунок 1 - Основное окно программы

Прежде чем начать работать непосредственно с программой и использовать все возможности, которые она предлагает, необходимо создать начальную карту. Вы подключены к сети, которая

включает в себя ряд рабочих станций, серверов, дополнительных коммутационных устройств. Создайте простую карту сети, включающую рабочие станции текущей комнаты, если Вы затрудняетесь составить подробную карту всех подключений.
Вы можете создать начальную карту, используя «Wizard», или создать карту вручную.
Карта занимает основную часть окна. Щелкните по ней правой кнопкой мыши. В появившемся меню выберите "Добавить" и затем "Workstation". Появится окно «Свойства устройства». Укажите запрашиваемые параметры: имя устройства, адрес, описание, картинку.
Аналогично, можно добавить другие устройства, которые присутствуют в вашей сети. После создания устройства будут автоматически пинговаться., т.е. в зависимости от того, включено устройство или нет, вы будете получать информацию о состоянии устройства в сети. Это может быть крайне удобным при администрировании небольшой сети и, когда администратор должен видеть текущее состояние устройств в сети.
Устройство будет отображаться в виде анимационной картинки, если оно пингуется, или в виде черно-белой картинки, если оно не пингуется.
Щелкните дважды по устройству для открытия его в проводнике. Вы можете обозначить сегменты Вашей сети в виде линий. Нажмите CTRL+I для получения подробной информации о созданной карте. В появившемся диалоге введите свое имя в качестве автора.
В меню "Файл" выберите "Настройки..." и настройте Friendly Pinger по своему желанию.
Рассмотрим основные возможности программы.
1) «Wizard» - позволяет создать начальную карту.
Friendly Pinger будет сканировать указанный диапазон IP-адресов и получать DNS-информацию о каждом адресе. Устройство будет добавлено, если DNS-сервер знает о нем.
Для запуска Wizard выберите пункт "Wizard" в меню "Файл".

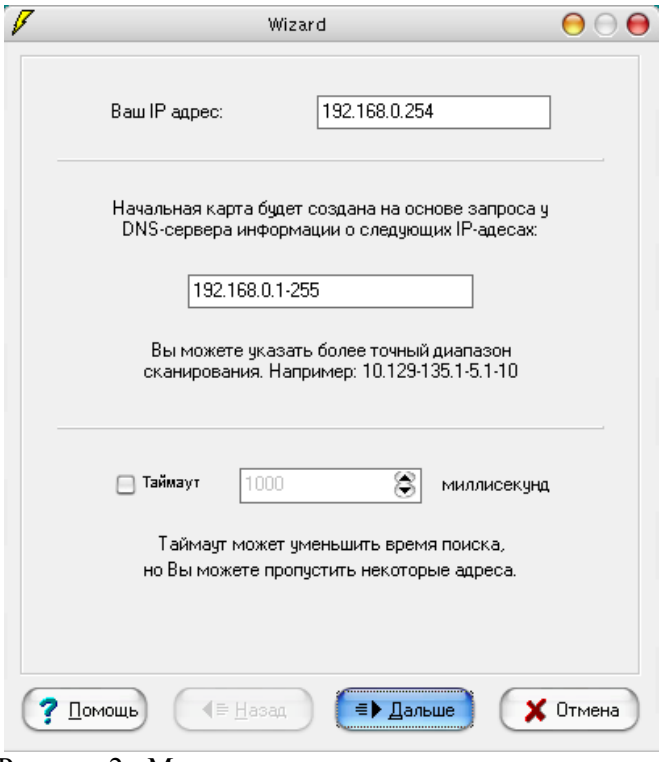


Рисунок 2 - Мастер создания карты

Wizard состоит из трех шагов:
1. Указание диапазона адресов, которые Вы хотите просканировать;
Friendly Pinger покажет IP-адрес Вашего компьютера и предложит начальный диапазон адресов для сканирования. Вы можете указать другой IP-адрес для изменения начального диапазона или указать диапазон вручную. Например: "10.129-135.1-9.1-9". Если некоторые адреса из диапазона в Вашей сети не существуют, их обработка может занять довольно длительное время. Вы можете ускорить ее, задав timeout. Нажмите кнопку "Далее" для начала сканирования.
2. Сканирование;

Friendly Pinger начнет сканирование Вашей сети. Каждый IP адрес будет запрашиваться у Вашего DNS-сервера для получения имени узла, ассоциированного с этим адресом.
Если DNS-сервер знает очередной IP-адрес, он будет добавлен в список найденных устройств.
Удалите галочку с тех устройств, которые Вы не хотите добавлять на карту. Галочка показывает, что устройство будет добавлено на карту. По умолчанию она ставится только на те устройства, которых нет на карте.
После поиска, нажмите "Далее" для задания дополнительных параметров или нажмите "Назад" для поиска в следующем диапазоне.
3. Добавление устройств.
Для добавления найденных устройств на карту Вы должны указать следующие параметры:
- Тип найденного устройства;
- Что использовать в качестве адреса: DNS-имя или IP-адрес;
- Если в Вашей сети присутствует DNS-суффикс, Вы можете удалить его из имени устройств;
- Выберите, где Вы хотите добавлять устройства, на новой карте или текущей.
После нажатия кнопки "Далее" устройство будет добавлено на карту.
Основное меню программы содержит следующие пункты:
- Файл;
- Правка;
- Вид;
- Пингование;
- Оповещение;
- Сканирование;
- Соединения;
- Инвентаризация;
- Помощь.

При наведении на любой пункт в меню, в статусной строке показывается его описание.
Рассмотрим Меню "Файл". Меню «Файл» содержит следующие пункты:
- Wizard - создать начальную карту.
- Новый - создать новую карту.
- Открыть - открыть существующую карту - Вы можете запустить FPinger с указанной картой, передав ее в качестве параметра. Например: fpinger.exe mymap.map
- Переоткрыть - открыть ранее используемую карту. Список открытых ранее карт запоминается и сохраняется в "Переоткрыть". Данный пункт недоступен, если история открытия карт пуста. Для переоткрытия карты:

1. Выберите "Файл Переоткрыть";
2. Выберите карту, которую Вы хотите переоткрыть.

Для возврата на предыдущую карту используйте клавишу BackSpace.
- Сохранить - сохранить карту.
- Сохранить как - сохранить карту в новый файл.
- Экспорт - сохранить карту в графический файл - поддерживаются два формата: Windows Bitmap Files (BMP), CompuServe Graphics Interchange (GIF).
- Печать - печать карты.
- Блокировать / Разблокировать - блокирование приложения. Вы можете заблокировать приложение паролем для предотвращения изменений другими пользователями.

Существуют три способа блокировки:
1. Блокировка всего приложения;
2. Блокировка изменений;
3. Запрещение только перемещения объектов на карте.

После блокирования этот пункт меню заменяется командой "Разблокировать", для того чтобы можно было разблокировать приложение.
Примечание: Если Вы забыли пароль, то закройте приложение и удалите строчку "Lock=1" в FPinger.ini файле.
- Создать дистрибутив

Создать дистрибутив Friendly Pinger'a (как FPinger3.exe) с Вашими картами и настройками. Затем Вы сможете раздать его другим пользователям Вашей сети. Вы можете создать дистрибутив "Friendly Pinger" или "Friendly Pinger Lite". Friendly Pinger Lite - это бесплатная облегченная версия Friendly Pinger'a, в которой запрещены следующие возможности:

- Создание и редактирование карт;
- Экспорт в GIF-файл;
- TraceRoute;
- Некоторые способы оповещения: журнал; e-mail и выполнение;
- Просмотр инвентаризации (работает только сбор, согласно настройкам "inventory.ini" файла).

Вы можете указать, какие конфигурационные файлы Вы хотите включить в дистрибутив. Например, Вы можете настроить инвентаризацию для сбора информации на Ваш компьютер, создать дистрибутив, включить в него inventory.ini файл, затем раздать и установить его другим пользователям Вашей сети, после этого Вы будете получать информацию о программном и аппаратном обеспечении Вашей сети для проведения инвентаризации.

- Настройки - Настроить программу.
- Выход - Закрыть программу.

FPinger можно также закрыть щелчком правой кнопкой мыши по иконке в трее и выбором "Выход":

Меню "Пингование" содержит следующие пункты:

- Пинговать все - Пинговать все устройства. Пингование также может быть начато нажатием клавиши F5 или щелчком правой кнопкой мыши на иконке программы и выбором "Пингование все":
- Пауза - Приостановить пингование устройств. После этого данный пункт меню заменится на "Продолжить". Пингование также может быть приостановлено нажатием клавиши F4 или щелчком правой кнопкой мыши на иконке программы и выбором "Пауза":
- Продолжить - Продолжить пингование устройств. После этого данный пункт меню заменится на "Пауза". Пингование так же может быть продолжить нажатием клавиши F4 или щелчком правой кнопкой мыши на иконке программы и выбором "Продолжить":
- Очистить кэш - Сбросить кэш IP адресов.
- FPinger запоминает, какой IP адрес соответствует каждому DNS имени. Это позволяет избежать постоянных запросов к DNS серверу, что увеличивает скорость работы приложения и экономит сетевой трафик. С другой стороны, после переконфигурирования DNS сервера, FPinger будет использовать старые IP-адреса. Чтобы избежать этого, воспользуйтесь этой опцией, либо перезапустите FPinger.
- Параметры пингования - Настроить параметры пингования.

Меню "Оповещение" содержит следующие пункты:

- Оповещение - настроить "службу оповещения".
- Отчет. Просмотр отчета оповещения. FPinger может показывать события на Вашей Web-странице. Для того чтобы изменить стиль отчета, правьте файл-шаблон "Events.htm".
- Очистить log-файл - Очистить Notification.log файл в каталоге приложения.
- Параметры оповещения. Настроить log-файл, HTML-файл и другие параметры оповещения.

Работа с объектами

Для того чтобы выделить устройство на карте воспользуйтесь одним из следующих способов:

- Если требуется выделить только один объект, щелкните по нему.
- Если требуется выделить на один объект больше, щелкните по нему, удерживая клавишу SHIFT.
- Если требуется снять выделение с одного из выделенных объектов, щелкните по нему, удерживая клавишу SHIFT.
- Если требуется снять выделение со всех объектов, щелкните в пустое место на карте.
- Если требуется выделить несколько объектов в одной прямоугольной области, выделите ее мышкой.
- Если требуется выделить несколько объектов в одной прямоугольной области, выделите ее мышкой, удерживая клавишу SHIFT. В этом случае, те объекты в области, которые были не выделены, станут выделенными и наоборот.
- Для выделения всех объектов нажмите Ctrl+A или выберите пункт "Выделить все" в меню "Правка" или щелкните правой кнопкой мыши по карте и выберите "Выделить все".

- Для перемещения выделенных объектов воспользуйтесь одним из следующих способов:

- Перетащите выделенные устройства мышкой;

- Перетащите мышкой за один из центров выделенной линии;
- Воспользуйтесь курсором клавиатуры, удерживая клавишу SHIFT;
В этом случае объекты будут перемещаться попиксельно;
- Воспользуйтесь курсором клавиатуры, удерживая клавишу CTRL;
В этом случае объекты будут перемещаться по 10 пикселей;
Если при перемещении какой-либо объект выйдет за правую или нижнюю границу карты, то автоматически появятся полосы прокрутки.
Специальные возможности:
- Если перетаскивать объекты мышкой, удерживая клавишу SHIFT, то они будут перемещаться только по горизонтали или только по вертикали, в зависимости от того, в какую сторону Вы перетаскиваете объекты;
- Если перетаскивать объекты мышкой, удерживая клавишу CTRL, то они будут перемещаться по сетке (т.е. по 10 пикселей);
- Оба этих способа можно совместить, удерживая одновременно CTRL и SHIFT.
Для выравнивания выделенных устройств, щелкните по ним правой кнопкой мыши, выберите "Выровнять" и затем:
- По левому краю - все выделенные устройства будут выровнены по самому левому краю их картинок.
- По правому краю - все выделенные устройства будут выровнены по самому правому краю их картинок.
- По верхнему краю - все выделенные устройства будут выровнены по самому верхнему краю их картинок.
- По нижнему краю -все выделенные устройства будут выровнены по самому нижнему краю их картинок.
- По центру - все выделенные устройства будут выровнены по вертикали, по центру их картинок.
- По сетке - все выделенные устройства будут выровнены по сетке. Сетка представляет собой ячейки 10x10 пикселей. Т.е. координаты всех объектов будут округлены до десятых.
- По горизонтали - все выделенные устройства будут выстроены по горизонтали на равном расстоянии друг от друга.
- По вертикали - все выделенные устройства будут выстроены по вертикали на равном расстоянии друг от друга.
- Центрировать вершины линий - для каждой линии будет проверено, есть ли у нее вершины под устройствами. И если есть, то эти вершины будут перемещены в центры соответствующих устройств.
Выравнивать по надписям - если выбрана эта опция, то все операции выравнивания будут учитывать позицию и размеры надписей устройств. Иначе выравнивание будет происходить только по картинкам устройств.
Привязка линий - если выбрана эта опция, то при перемещении устройств, линии, которые под ними, тоже будут перемещены.

Устройства
Создание - для добавления нового устройства, щелкните по карте правой кнопкой мыши и выберите элемент в пункте "Добавить", в зависимости от того, устройство какого типа Вы хотите добавить на карту. Появится окно свойства устройства. Укажите все необходимые параметры и нажмите кнопку OK.
Удаление - для того чтобы удалить устройство, выделите его и: нажмите клавишу Del; или выберите "Удалить" в меню "Edit";
Пингование - Для того чтобы принудительно пинговать устройство, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Пинговать выделенные устройства".
Открытие в проводнике - для того чтобы открыть устройство в проводнике, щелкните по нему правой кнопкой мыши и выберите "Открыть". Данная команда эквивалентна выполнению команды Windows "\\адрес_устройства" или "адрес_устройства", если это internet-адрес.
Открытие в Total Commander - для того чтобы открыть устройство в Total Commander, щелкните по нему правой кнопкой мыши и выберите "Открыть в TotalCmd". Этот пункт отсутствует, если Total Commander не установлен на Вашем компьютере.
Оповещение - оповещать, когда устройство остановится или запустится.

Инвентаризация - просмотр списка программного обеспечения и аппаратных средств компьютера.

Выполнение внешних команд - для выполнения внешней команды, щелкните по устройству правой кнопкой мыши и выберите соответствующую команду. Внешние команды для устройств каждого типа регистрируются в настройках для типа устройств.

Конфигурирование - для конфигурирования устройства, щелкните по нему правой кнопкой мыши и выберите "Параметры". Появится окно "Свойства устройства". Для изменения параметров типа устройства, щелкните по устройству правой кнопкой мыши и выберите "Настроить тип устройства...". Появится диалог "Параметры типа устройства". Для изменения типа устройства, щелкните по устройству правой кнопкой мыши и выберите "Установить тип устройства". Затем выберите требуемый тип из списка.

Остановка пингования - для того чтобы приостановить пингование устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Приостановить пингование выделенных устройств". Для того чтобы продолжить пингование устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Продолжить пингование выделенных устройств".

TraceRoute - для получения пути до устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "TraceRoute".

Соединение - для того чтобы соединиться с FP-сервером, запущенном на устройстве, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Соединиться". Для того чтобы отсоединиться от FP-Server, запущенном на устройстве, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Рассоединиться". "Рассоединиться" доступно только после соединения.

Свойства устройств - для того чтобы настроить параметры выделенного объекта, щелкните по нему правой кнопкой мыши и выберите "Параметры". В появившемся окне Вы можете изменять следующие параметры: Имя - имя устройства, которое отображается под устройством. Допускается вводить несколько имен построчно. Текст в подсказке - описание устройства, которое отображается при наведении на него мышкой. Картинка в подсказке - картинка, ассоциированная с устройством, которая отображается при наведении на него мышкой. Тип - тип устройства. Типы устройств регистрируются в настройках программы. Они показывают, каким образом отображать те или иные устройства на карте, так же они задают способ опроса устройства, его внешние команды и т.д. Адрес - Адрес устройства. Адрес устройства используется для пингования и для выполнения внешних команд. В качестве адреса можно указывать IP адрес или DNS имя устройства. Вы можете назначить адрес, только если для типа данного устройства установлен режим опроса "Пинговать" или "Всегда включено".
Дополнительные адреса - вы можете указать дополнительные адреса для устройства. Они будут пинговаться и отображаться на карте в виде кружочков. Если дополнительный адрес пингуется, то он будет показан в виде кружочка зеленого цвета, иначе красного. Адрес будет показываться при наведении мышкой на кружок.
Обычно дополнительные адреса обозначают присутствие нескольких сетевых карт на сервере. Активно используются для TraceRoute.
Вы можете назначать дополнительные адреса, только если для типа данного устройства установлен режим опроса "Пинговать" или "Всегда включено".
Файл с картой - файл с картой, которая будет открываться по двойному щелчку на устройстве. Вы можете назначить карту, только если для типа данного устройства установлен параметр "Открывать другую карту"
Привязать к другим устройствам - Привязать данное устройство к другим устройствам - если одно из них пингуется, то это устройство будет показываться включенным.
Для того чтобы привязать устройство к другим устройствам, например, хаб к компьютерам, выделите хаб на карте, нажмите клавишу ALT и щелкайте по компьютерам, которые Вы хотите привязать к хабу, или с которых Вы хотите снять привязку.
Устройства, которые привязаны к данному устройству, показываются в красных прямоугольниках.

Вы можете привязать устройство к другим, только если для типа данного устройства установлен режим опроса "Привязывать к другим устройствам".
Тип устройства - для того чтобы настроить параметры типа устройства, щелкните по нему правой кнопкой мыши и выберите "Настроить тип устройства...".
В появившемся диалоге Вам доступны следующие параметры: имя - имя типа устройств.
Способ опроса - существуют три способа опроса состояния устройств:
Всегда включено - устройство не будет пинговаться и будет отображаться на карте всегда включенным.
Пинговать - устройство будет пинговаться.
Привязывать - устройство будет привязано к другим устройствам и отображаться включенным, только если хотя бы одно из них включено.

Внешние команды - вы можете назначить устройствам внешние команды, такие как telnet, ping.exe, tracert.exe, net.exe и т.д. Они будут показываться в контекстном меню устройства (при щелчке на нем правой кнопкой мыши).
В настройках можно навешать двойной щелчок на запуск первой внешней команды.
Допускается использовать следующие ключи в параметрах внешних команд:
%Address - адрес устройства;
%IP - IP адрес устройства;
Каждый ключ при выполнении внешней команды будет заменен на его соответствующее значение.
Допускается использовать произвольные ключи. Их значения будут запрашиваться перед запуском внешней команды. Например, для реализации NetSend добавьте следующую внешнюю команду:
Приложение: "net.exe";
Параметры: "send %Address %Text".
%Text будет предварительно запрашиваться.
Для ввода пароля используйте ключ %Password. Он позволить вводить текст секретно. Если требуется указать несколько разных паролей, используйте ключи, начинающие со слова %Password, например, %Password1, %Password2 и т.д.
Рекомендуем установить Windows Resource Kit, он содержит довольно много полезных команд для удаленного управления другими компьютерами, например, для их удаленной перезагрузки, запуска приложений и т.д. Все их можно успешно вызывать из FPinger'a.
Групповые операции - групповые операции позволяют выравнивать и изменять параметры сразу нескольких устройств на карте. Для того чтобы выполнить групповую операцию, выберите "Правка Групповые операции".
В появившемся окне Вам предложат выполнить одну из следующих операций:
- Выстроить устройства;
- Изменить тип устройств;
- Установить имена устройств значениями их адресов;
- Установить значения адресов значениями их IP адресов.

Выберите требуемую операцию и нажмите "Далее".
В зависимости от выбранной операции Вас попросят указать следующие данные:
- Выстроить устройства: направление выравнивания объектов: слева направо, сверху вниз, или наоборот. Так же можете выбрать "Отображать имена справа", если хотите поменять позицию отображения имен устройств.
- Изменить тип устройств: новый тип устройств.

Далее, для любой выбранной операции Вы должны указать, для каких устройств ее осуществить:
- Для всех устройств на карте;
- Только для выделенных устройств (недоступно, если ни одно устройство на карте не выделено);
- Только для устройств определенного типа (нужно указать для какого);
- Только для устройств неизвестного типа - если Вы удалите какой-либо тип устройств, то сами устройства останутся на карте, но будут показываться без иконок.

С помощью групповых операций Вы можете задать тип сразу для всех неизвестных устройств. Данная опция недоступна, если устройств неизвестного типа нет на карте. Для завершения групповой операции, нажмите "Закончить".
Линии - линии на карте обычно обозначают сегменты. Если линия выделена, то красно-желтые квадраты показывают ее вершины, а красно-голубой - центр (для перемещения).

Пингование

Для того чтобы начать пингование устройств, воспользуйтесь одним из следующих способов: нажмите клавишу F5; выберите пункт "Пинговать все" в меню "Пингование"; щелкните по иконке программы в системном трее и выберите "Пинговать все". Для пингования только выделенных устройств, щелкните по ним правой кнопкой мыши и выберите "Пинговать выделенные". Для того чтобы временно прекратить пингование устройств, воспользуйтесь одним из следующих способов: нажмите клавишу F4; выберите пункт "Пауза" в меню "Ping"; щелкните по иконке программы в системном трее и выберите "Пауза".

Для того чтобы продолжить пингование устройств, воспользуйтесь одним из следующих способов: нажмите клавишу F4; выберите пункт "Продолжить" в меню "Ping"; щелкните по иконке программы в системном трее и выберите "Продолжить".

TraceRoute

TraceRoute - это средство для просмотра маршрута до указанного адреса.

Как использовать TraceRoute в FPinger'e: Для просмотра маршрута до устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "TraceRoute". В нижней части карты появится окно TraceRoute.

В процессе определения промежуточных адресов они будут добавляться в этом окне и отображаться на карте в виде стрелок. Каждая строчка в окне TraceRoute имеет popup-меню, которое активизируется щелчком правой кнопкой мыши. С помощью него Вы можете скопировать текст, IP-адрес или имя хоста из этой строчки в буфер обмена, найти устройство на карте или закрыть окно TraceRoute.

Примечание:

- Промежуточные адреса, которые не найдены на карте, пропускаются при графическом представлении маршрута;
- Вы можете задавать дополнительные адреса для устройств, если они не найдены на карте.

FPinger может оповещать Вас если какой-либо компьютер остановится или запустится. Присутствуют 7 способов оповещения:

- Сохранение события в log-файл;
- Анимация иконки в системном трее;
- Показ сообщения на экране;
- Отправление e-mail сообщения;
- Проигрывание звукового файла;
- Запуск внешнего приложения;
- Отображение события на Вашей Web странице.

Для использования оповещения на устройство, щелкните по нему правой кнопкой мыши, выберите "Оповещение" и затем один из следующих пунктов:

- Когда "имя устройства" запустится;
- Когда "имя устройства" остановится;
- Когда любой "тип устройства" запустится;
- Когда любой "тип устройства" остановится.
- В окне "Оповещение" вы можете устанавливать следующие параметры:
- Перепроверять - перепроверять, что устройство действительно остановилось или запустилось; Так же Вы можете указать, сколько раз требуется перепроверить событие.
- Оповестить только один раз - выключить это оповещение после первого срабатывания;
- Сохранить в log-файл - сохранить событие в log-файл. Требуется для отчетов;
- Анимация в трее - анимировать иконку в трее после срабатывания события;
- Показать сообщение - показать сообщение на экране после срабатывания события;
- Отправить письмо - отправить письмо по электронной почте указанным получателям после срабатывания события. Многие провайдеры сотовой и пейджинговой связи предоставляют возможность отправлять сообщения своим клиентам с помощью электронной почты. Вы можете воспользоваться этой услугой и получать сообщения об остановке или запуске серверов напрямую на Ваш сотовый или пейджер. Дополнительную информацию Вы можете получить у Вашего провайдера сотовой или пейджинговой связи.

 Проиграть звуковой файл - проиграть звуковой файл после срабатывания события. Вы можете записать свой файл, используя микрофон;
 Выполнить - выполнить внешнее приложение после срабатывания события. Вы можете передать адрес устройства в качестве параметра, используя ключ %Address. Для передачи IP адреса устройства используйте ключ %IP.

Программа FP-сервер. FP-сервер - это бесплатное приложение, с открытым текстом программ, разработанное специально для FPinger'a, написанное для Windows и Linux.
FPinger может соединяться с FP-сервером, который запущен на другом компьютере. После соединения, все Ping и TraceRoute операции будут происходить с удаленного компьютера, где запущен FP-сервер, а результат будет показываться на Вашем компьютере. С помощью FP-сервера Вы можете смотреть как пингуется сеть с серверов, или смотреть TraceRoute между любыми компьютерами.
Чтобы соединиться с FP-сервером, необходимо запустить FP-сервер на удаленном компьютере. Щелкните правой кнопкой мыши по тому устройству на карте, на котором запущен FP-сервер, выберите "Ping, Trace" и затем "Connect". Для рассоединения с FP-сервер, запущенном на компьютере, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Disconnect".
Примечания:
FP-сервер сейчас находится в стадии разработки. Доступна только тестовая версия.

Дабораторная работа №1
Тема: Концентраторы, мосты, коммутирующие мосты, маршрутизаторы, шлюзы, их назначение, основные функции и параметры.
Цель работы: Изучение состава аппаратного и программного обеспечения сетей ЭВМ. Получение практических навыков базовой настройки сетевой системы.

Задание 1: Охарактеризовать назначение, маркировку, функции и параметры следующего коммуникационного оборудования:
→ Повторитель
→ Концентратор
→ Коммутатор
→ Кабельная система «Витая пара»
→ Оптоволоконный кабель
→ Маршрутизатор
→ Брандмауэр
→ Сетевая плата
→ Модем
→ Мост

Повторитель - устройство для соединения сегментов одной сети, обеспечивающее усиление и формирования сигналов. Оперирует на физическом уровне модели OSI. Позволяет расширять сеть по расстоянию и количеству подключенных узлов.
Концентратор - это сетевое устройство, предназначенное для объединения нескольких устройств в общий сигнал.
Функции концентраторов:
1. Объединение сегментов с разными физическими средами в один локальный сегмент.
2. Автосегментация портов.
3. Совместно используют периферийное устройства.

Коммутатор – многопортовое устройство, обеспечивающее высокоскоростную коммутацию пакетов между портами.

Функции концентраторов:
1. Объединяет различные сетевые устройства такие, как компьютеры, серверы, подключенные к ним, в единый сегмент сети.
2. Анализ MAC- адреса порта-отправителя и отправка данных на другой порт, а так же этом формирование таблиц.

Кабельная система «Витая пара» используется в телефонных системах, локальных сетях, в передачи данных на дальние расстояния телефонных и телевизионных сигналов.
Существуют 2 вида «Витай пары»: экранизированная витая пара и неэкранизированная витая пара.
Неэкранизированная витая пара широко используется в ЛВС, максимальная длина сегмента составляет 100 м. Неэкранизированная витая пара состоит из двух изолированных медных провода. Разделяются на категории 1-5, 5е, 6, 6а и 7.
Экранизированная витая пара имеет медную обмотку, обеспечивающая большую защиту, так же проводы перемотаны фольгой. Экранизированная витая пара обладает прекрасной изоляцией, защищающий данные от внешних помех. Кабели разделяются на типы (Type1-Type9).

Оптоволоконный кабель.
Информация передаются с помощью световых сигналов.
Каждое стеклянное оптоволокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон с отдельными коннекторами.

Маршрутизатор - устройство, предназначенное для построения компьютерной сети и обеспечения стабильной ее работы, транслирующее пакеты данных между различными элементами сети.
Функции маршрутизатора:
1. Подключение локальных сетей (LAN) к территориально-распределенным сетям (WAN).
2. Соединение нескольких локальных сетей.

Маршрутизаторы работают на третьем или седьмом уровне модели OSI.

Брандмауэр - средство, с помощью которого осуществляется процесс разграничения доступа к компьютеру через интернет. Различают два типа брандмауэров: программные и аппаратные.
Функции брандмауэров:
1. Обеспечивает безопасность компьютера.
2. Осуществляет взаимодействие с какими-либо сетевыми программами, которые установлены на компьютер.

Сетевая плата - специализированный компонент компьютера, обеспечивающий связь и передачу данных между несколькими компьютерами в сети.

Модем - коммуникационное устройство, позволяющее передавать бинарные (цифровые) данные по аналоговой телефонной линии.
Он осуществляет преобразование данных с компьютера в последовательность дискретных (разнотипных) сигналов и их отправку по аналоговой телефонной линии. На другом конце они расшифровываются принимающим модемом путем аналого-цифрового преобразования.
Мост - средство передачи кадров между двумя (или больше) сегментами. Мост анализирует заглавие кадра – его интересуют MAC-адрес источника и получателя. Мост прослушивает кадры, которые приходят, и составляет таблицы MACC-адресов узлов, подключенных к этим портам.

Задание 2: Охарактеризовать сетевые операционные системы согласно вариантам по следующей схеме:
1) платность,
2) доступ к исходному коду,
3) многоплатформенность,
4) мультизадачность,
5) количество пользователей,
6) функции управления сетью,
7) интерфейс работы,
8) потребляемые ресурсы

MS DOS.
- Бесплатная;
- Закрытый исходный код;
- Одноплатформенная;
- Однозадачная с элементами многозадачности

– Однопользовательская;
– Несетевая;

Window XP.

– Платная;
– Закрытый исходный код;
– Многоплатформенная;
– Мультизадачная;
– Многопользовательская;
– Общий доступ к подключению Интернет;
– Интерес работы: рабочий стол, меню, панели инструментов, программные окна, диалоговые окна, вторичные окна;
– Потребляемые ресурсы: тактовая частота ЦП – 233 МГц, объем ОП – 128 Мбайт, разрешение видеокарты 600x800, свободное место на диске для установки Windows XP – от 1536 Мбайт, столько же для программного обеспечения.

Windows 7.

– Платная;
– Закрытый исходный код;
– Многоплатформенная;
– Мультизадачная;
– Многопользовательская;
– Общий доступ к подключению Интернет;
– Интерес работы: рабочий стол, меню, панели инструментов, программные окна, диалоговые окна, вторичные окна;
– Потребляемые ресурсы: тактовая частота ЦП – 1ГГц и выше, 1Гб или 2Гб ОЗУ, 16 Гб или 20 Гб свободного места на жестком диске.

Windows 8.1.

– Платная;
– Закрытый исходный код;
– Многоплатформенная;
– Мультизадачная;
– Многопользовательская;
– Общий доступ к подключению Интернет;
– Интерес работы: введена «чудо-кнопка», возможность открыть рабочий стол сразу же после входа в систему;
– Потребляемые ресурсы: тактовая частота ЦП – 1ГГц и выше, 1Гб или 2Гб ОЗУ, 16 Гб или 20 Гб свободного места на жестком диске.

Ответы на контрольные вопрос:

1. Что такое компьютерная сеть?

Компьютерная сеть - совокупность узлов (компьютеров, терминалов, периферийных устройств), имеющих возможность информационного взаимодействия друг с другом с помощью специального коммуникационного оборудования и программного обеспечения.

2. Что входит в аппаратное обеспечение сетей?

– компьютеров;
– коммуникационного оборудования;
– операционных систем;
– сетевых приложений.

3. Функции и характеристики коммуникационного оборудования?

– средства линий передачи данных
– средства соединения линий передачи с сетевым оборудованием узлов
– средства увеличения дистанции передачи данных - репитеры, модемы и пр.

– средства повышения емкости линий передачи (мультиплексирования)
– средства управления информационными потоками в сети

4. Что такое активное оборудование сетей?
Активное оборудование сети – устройство, которому необходимо подача энергии для генерации сигналов.
К активному оборудованию относят интерфейсные карты, повторители, концентраторы.

5. Что такое пассивное оборудование сетей?
Пассивное оборудование сети – устройство, которому не требуется подача энергии.
К пассивному оборудованию относят кабели, соединительные разъемы, коммутационные панели.

6. Что такое вспомогательное оборудование сетей?
Вспомогательное оборудование - устройства бесперебойного питания, кондиционирования воздуха и аксессуары - монтажные стойки, шкафы, кабелепроводы различного вида.

7. Что называют операционной системой?
Сетевая ОС - ОС, которая обеспечивают пользователям распределенный доступ к сетям ЭВМ.

8. Что входит в группу прикладного программного обеспечения?
В группу прикладного ПО входят: сетевые операционные системы; сетевые драйвера, протоколы, службы и другое дополнительное программное обеспечение сетевых интерфейсов; прикладное сетевое программное обеспечение.

9. По каким критериям можно охарактеризовать сетевую операционную систему?
1) платность,
2) доступ к исходному коду,
3) многоплатформенность,
4) мультизадачность,
5) количество пользователей,
6) функции управления сетью,
7) интерфейс работы,
8) потребляемые ресурсы

10. Что такое технология «клиент-сервер»?
«Клиент – сервер» - топология, обеспечивающая совместный доступ пользователей к определенному типу ресурсов.

11. Что такое виртуальная машина? Ее назначение?
Виртуальная машина - программная и/или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы и исполняющая программы для target-платформы на host-платформе.
При помощи виртуальной машины можно установить любую систему на любую платформу. При этом получим полнофункциональную систему с доступом в локальную сеть и интернет.
Виртуальная машина имеет свой жесткий диск, процессор, выделенную оперативную память, графический адаптер и т.д. Всеми этими ресурсами делится с ней физическая машина.

Практическая работа №3

Тема: Монтаж кабельных сетей на основе UTP/STP

Цель работы: **В этом задании вы должны познакомиться с различными типами кабелей и освоить процедуры монтажа коннекторов BNC и RJ-45.**

Задание: Работа с «тонким» коаксиальным кабелем
и с кабелем «витая пара»

Задание 1.
Работа с «тонким» коаксиальным кабелем
и с кабелем «витая пара»

Цель работы В этом задании вы должны познакомиться с различными типами кабелей и освоить процедуры монтажа коннекторов BNC и RJ-45.

Изучение тонкого коаксиального кабеля

1. Возьмите отрезок коаксиального кабеля и исследуйте его строение.

Сколько проводников используется для передачи сигнала по коаксиальному кабелю? Какие это проводники?

2. Аккуратно удалите часть внешней оболочки и обрежьте экранирующую оплетку. Затем надрежьте, чуть надломите и снимите внутреннюю изоляцию, не повредив центральную жилу.

Из какого металла (меди или алюминия) изготовлен центральный проводник вашего кабеля? Одножильный он или многожильный?

Монтаж BNC-коннектора на коаксиальном кабеле

1. Возьмите отрезок коаксиального кабеля длиной 2–3 метра.
2. Отрежьте на конце кабеля небольшой кусок в 2–3 см, чтобы удалить поврежденную или окислившуюся часть кабеля.
3. Наденьте на кабель трубочку, используемую для обжима экранирующей оплетки, и сдвиньте ее немного вниз, чтобы она не мешала дальнейшей работе.
4. Возьмите устройство для зачистки кабеля RG-58, заложите конец кабеля в подпружиненную часть (как показано на рис. .1) и проверните инструмент один-два раза вокруг кабеля, следя за тем, чтобы устройство все время оставалось перпендикулярным кабелю.

Рис. .1. Коаксиальный кабель RG-58 в устройстве для его зачистки

Внимание! В устройстве для зачистки кабеля используются острые ножи. Поэтому не пытайтесь использовать это устройство для зачистки чего-либо другого, кроме «тонкого» коаксиального кабеля, и ни в коем случае не пытайтесь зажимать в этом устройстве, например, палец: такие действия могут привести к серьезной травме.

5. В результате кабель должен оказаться надрезанным в нескольких местах на разную глубину:

- первый нож должен надрезать только внешнюю оболочку;
- второй — должен надрезать внешнюю оболочку и экранирующую оплетку;
- третий — внешнюю оболочку, экранирующую оплетку и внутреннюю изоляцию.

Примечание. Лучше, если ножи чуть не дорезают указанные оболочки кабеля, чем перерезают их глубже необходимого.

6. Аккуратно удалите надрезанные части — после этого конец кабеля должен выглядеть, как показано на рис. .2.

Рис. .2. Коаксиальный кабель RG-58 после зачистки

7. Возьмите центральный контакт и наденьте на внутреннюю жилу кабеля, причем эта жила должна полностью уместиться в отверстии контакта, а сам контакт должен прилегать краем к внутренней изоляции.

8. Поместите центральный контакт со вставленной жилой в маленький штамп обжимного устройства и сожмите ручки клещей до упора. После этого конец кабеля должен выглядеть, как показано на рис. .3.

Рис. 3. Коаксиальный кабель RG-58 после установки и обжима центрального контакта

Внимание! В обжимном устройстве используется блокировочный механизм, препятствующий разжиманию инструмента до полного обжима. Поэтому не пытайтесь сжимать что-либо, кроме частей коннектора BNC, и ни в коем случае не пытайтесь зажать в нем, например, палец: такие действия могут привести к серьезной травме.

9. Расправьте экранирующую оплетку — это легко сделать с помощью иглы или распрямленной канцелярской скрепки.

10. Возьмите основную часть коннектора (корпус) и аккуратно, но с усилием вставьте центральный контакт в отверстие внутри корпуса до слабо слышного щелчка (проследите, чтобы экранирующая оплетка при этом оказалась снаружи).

11. Равномерно обмотайте экранирующую оплетку вокруг хвостовой части корпуса коннектора, как показано на рис. 4. и наденьте трубочку на обмотанный оплеткой хвостовик.

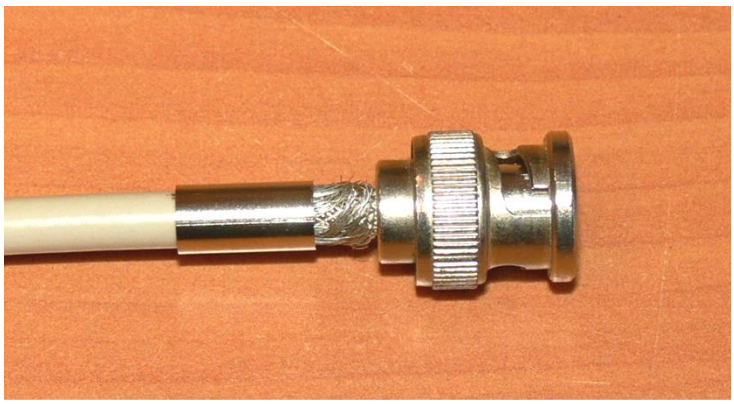


Рис. 4. Коаксиальный кабель с установленной основной частью коннектора
и не полностью надетой обжимной трубочкой

12. Наконец, следует поместить хвостовую часть коннектора в обжимное устройство (рис. 5) и одним движением обжать ее.

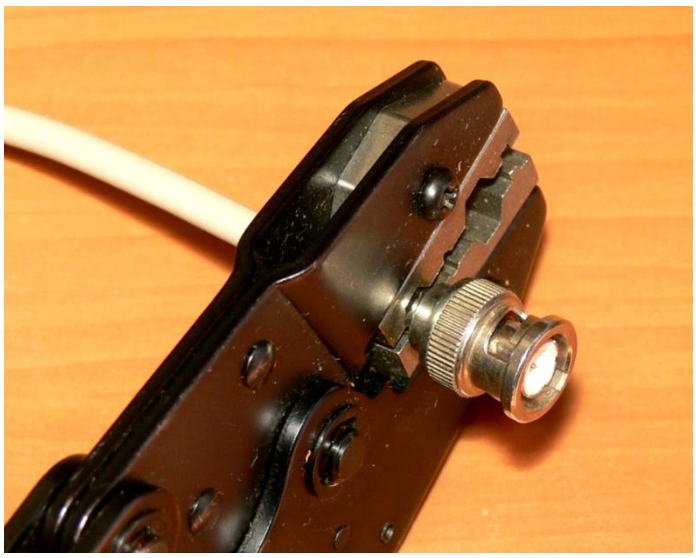


Рис. 5. Коннектор BNC в обжимном инструменте

Изучение кабеля «витая пара»

1. Возьмите отрезок кабеля «витая пара» и исследуйте его строение.

Сколько проводников используется для передачи сигнала по кабелю витая пара? Какие это проводники?

2. Аккуратно удалите часть внешней оболочки, расплетите одну из пар и снимите с нее изоляцию, не повредив проводники.

Из какого металла изготовлены проводники вашего кабеля? Одножильные они или многожильные?

Монтаж коннектора RJ-45 на кабеле «витая пара»

1. Возьмите отрезок кабеля «витая пара» длиной 2–3 метра.
2. Отрежьте на конце кабеля небольшой кусок в 2–3 см, чтобы удалить поврежденную или окислившуюся часть кабеля.
3. Возьмите устройство для обжима коннекторов RJ-45 и найдите в нем ножи для обрезания внешней оплетки. Заложите конец кабеля между ножами, как показано на рис. .6, слегка сожмите ручки и вращающим движением надрежьте внешнюю оплетку кабеля (аккуратно, чтобы не разрезать проводники).

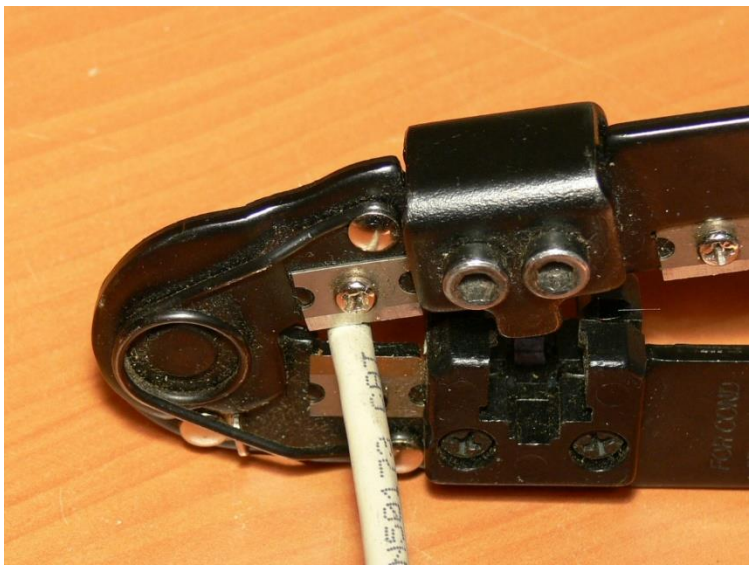


Рис..6. Обрезка внешней изоляции на кабеле «витая пара»

Внимание! В устройстве для обрезки кабеля используются острые ножи. Поэтому не пытайтесь использовать это устройство для зачистки чего-либо другого, кроме кабеля «витая пара» или телефонного кабеля, и ни в коем случае не пытайтесь зажимать в устройстве, например, палец: такие действия могут привести к серьезной травме.

4. Удалите надрезанный кусок внешней оплетки кабеля, расплетите и выпрямите все проводники. После этого конец кабеля должен выглядеть, как показано на рис. 7.

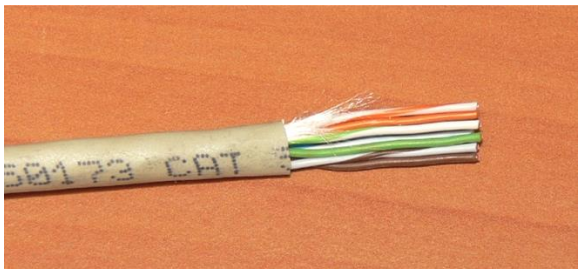


Рис. 7. Кабель «витая пара» с расплетенными и выпрямленными проводниками

5. Расположите проводники в соответствии с выбранным вами стандартом заделки (наиболее распространенным является стандарт 568B) и, срезав на их концах кусочки по 2–4 миллиметра, аккуратно подровняйте их (как показано на рис. 8).

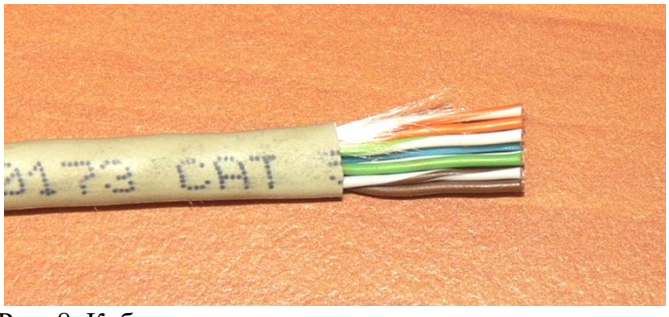


Рис. 8. Кабель «витая пара» с подготовленными к монтажу в коннектор проводниками

6. Вставьте проводники в коннектор, следя за тем, чтобы расположение проводников не нарушилось, затем поместите коннектор в обжимное устройство до фиксации защелкой (рис. 9) и обожмите разъем.

Рис. 9. Коннектор RJ-45 в обжимном инструменте

Изготовление прямого кабеля на базе «витой пары» и проверка качества заделки коннекторов

1. Возьмите отрезок кабеля, на одном конце которого вы только что смонтировали коннектор RJ-45.
2. Повторите операции 2–6 из предыдущей части задания, чтобы установить и обжать коннектор на втором конце кабеля. Проследите, чтобы разводка проводников в точности совпадала с разводкой проводников в коннекторе на другом конце кабеля.
3. Полученный таким образом кабель называется прямым.

Какие устройства соединяются с помощью прямого кабеля?

4. Возьмите прибор для проверки кабелей.
5. Используя разъемы для коннекторов RJ-45, соедините обе части прибора: основную («MASTER») и удаленную («REMOTE») с помощью только что изготовленного кабеля (рис. 10), после чего нажмите кнопку включения питания на основной («MASTER») части прибора. Обратите внимание на мигающие светодиодные индикаторы.

Рис. 10. Проверка качества заделки коннекторов RJ-45 с помощью специального тестера

Все ли индикаторы на удаленной («REMOTE») части прибора загораются с соответствии с индикаторами на основной его части?

6. Если все индикаторы загораются, значит, ваш кабель прошел простейшую проверку.

Примечание. Показанное на рис. 4.10 устройство является достаточно примитивным — оно позволяет обнаруживать только нарушения электрического контакта в коннекторах и кабеле, но не дает информации о качестве самого кабеля и коннекторов. Для получения таких данных используются профессиональные тестеры.

Изготовление перекрестного кабеля на базе «витой пары»

1. Возьмите отрезок кабеля и, используя разводку по стандарту 568B, смонтируйте на его конце коннектор RJ-45.
2. На обратном конце кабеля коннектор следует заделать, поменяв расположение проводников следующим образом: зеленую пару нужно поменять местами с оранжевой, а голубую — с коричневой.
3. Полученный таким образом кабель называется перекрестным.

Какие устройства можно соединять с помощью перекрестного кабеля?

Практическая работа №4

Тема: Сравнение топологий ЛВС

Цель работы: Изучить структуру сети Ethernet.

Теоретические основы

Наибольшее распространение среди стандартных сетей получила сеть *Ethernet*. Впервые она появилась в 1972 году (разработчиком выступила известная фирма Xerox). Сеть оказалась довольно удачной, и вследствие этого ее в 1980 году поддержали такие крупнейшие компании, как DEC и Intel (объединение этих компаний назвали DIX по первым буквам их названий). Их стараниями в 1985 году сеть *Ethernet* стала международным стандартом, ее приняли крупнейшие международные организации по стандартам: комитет 802 IEEE (Institute of Electrical and Electronic Engineers) и ECMA (European Computer Manufacturers Association).

Стандарт получил название IEEE 802.3 (по-английски читается как "eight oh two dot three"). Он определяет множественный доступ к моноканалу типа шина с обнаружением конфликтов и контролем передачи, то есть с уже упоминавшимся методом доступа CSMA/CD. Этому стандарту удовлетворяли и некоторые другие сети, так как уровень его детализации невысок. В результате сети стандарта IEEE 802.3 нередко были несовместимы между собой как по конструктивным, так и по электрическим характеристикам. Однако в последнее время стандарт IEEE 802.3 считается стандартом именно сети *Ethernet*.

Основные характеристики первоначального стандарта IEEE 802.3:

- топология – шина;
- *среда передачи* – коаксиальный кабель;
- скорость передачи – 10 Мбит/с;
- максимальная длина сети – 5 км;
- максимальное количество абонентов – до 1024;
- длина сегмента сети – до 500 м;
- количество абонентов на одном сегменте – до 100;
- метод доступа – CSMA/CD;
- передача узкополосная, то есть без модуляции (моноканал).

Строго говоря, между стандартами IEEE 802.3 и *Ethernet* существуют незначительные отличия, но о них обычно предпочитают не вспоминать.

Сеть *Ethernet* сейчас наиболее популярна в мире (более 90% рынка), предположительно таковой она и останется в ближайшие годы. Этому в немалой степени способствовало то, что с самого начала характеристики, параметры, протоколы сети были открыты, в результате чего огромное число производителей во всем мире стали выпускать аппаратуру *Ethernet*, полностью совместимую между собой.

В классической сети *Ethernet* применялся 50-омный коаксиальный кабель двух видов (толстый и тонкий). Однако в последнее время (с начала 90-х годов) наибольшее распространение получила версия *Ethernet*, использующая в качестве *среды передачи* витые пары. Определен также стандарт для применения в сети оптоволоконного кабеля. Для учета этих изменений в изначальный стандарт IEEE 802.3 были сделаны соответствующие добавления. В 1995 году появился дополнительный стандарт на более быструю версию *Ethernet*, работающую на скорости 100 Мбит/с (так называемый *Fast Ethernet*, стандарт IEEE 802.3u), использующую в качестве *среды передачи* витую пару или оптоволоконный кабель. В 1997 году появилась и версия на скорость 1000 Мбит/с (Gigabit Ethernet, стандарт IEEE 802.3z).

Помимо стандартной топологии шина все шире применяются топологии типа пассивная звезда и пассивное дерево. При этом предполагается использование репитеров и репитерных концентраторов, соединяющих между собой различные части (сегменты) сети. В результате может сформироваться древовидная структура на сегментах разных типов (рис 1).

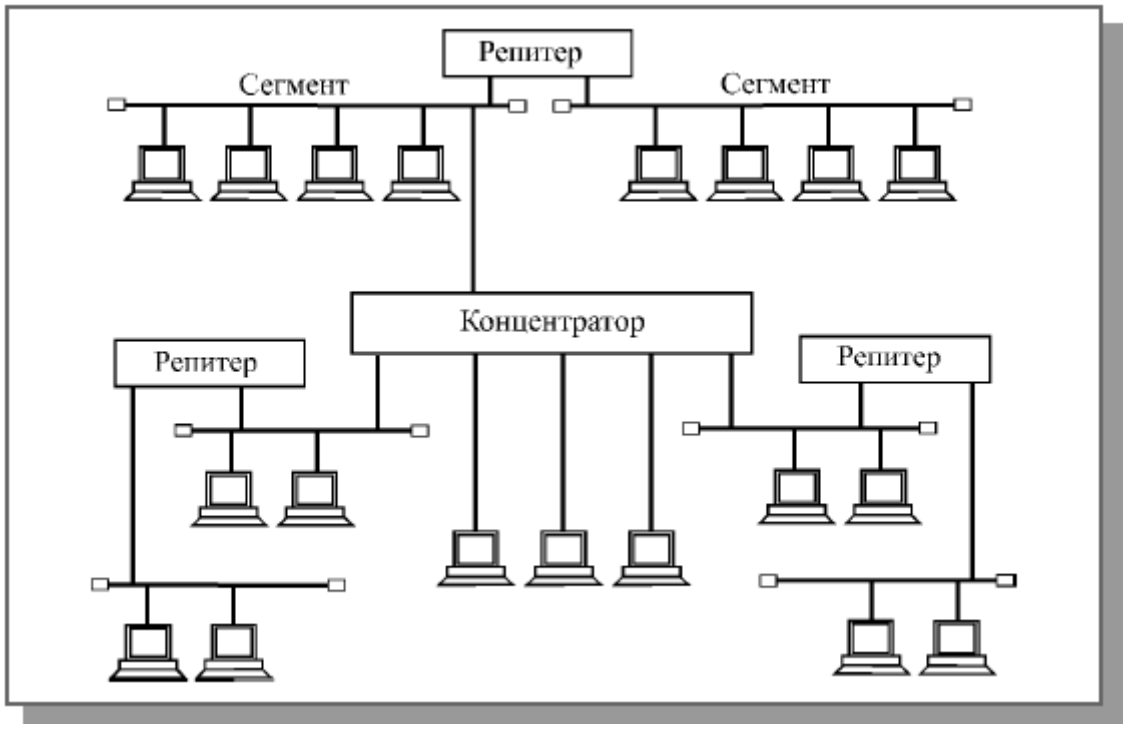


Рис. 1. Классическая топология сети Ethernet

В качестве сегмента (части сети) может выступать классическая шина или единичный абонент. Для шинных сегментов используется коаксиальный кабель, а для лучей пассивной звезды (для присоединения к концентратору одиночных компьютеров) – витая пара и оптоволоконный кабель. Главное требование к полученной в результате топологии – чтобы в ней не было замкнутых путей (петель). Фактически получается, что все абоненты соединены в физическую шину, так как сигнал от каждого из них распространяется сразу во все стороны и не возвращается назад (как в кольце).

Максимальная длина кабеля сети в целом (максимальный путь сигнала) теоретически может достигать 6,5 километров, но практически не превышает 3,5 километров.

В сети *Fast Ethernet* не предусмотрена физическая топология шина, используется только пассивная звезда или пассивное дерево. К тому же в *Fast Ethernet* гораздо более жесткие требования к предельной длине сети. Ведь при увеличении в 10 раз скорости передачи и сохранении *формата пакета* его минимальная длина становится в десять раз короче. Таким образом в 10 раз уменьшается допустимая величина двойного времени прохождения сигнала по сети (5,12 мкс против 51,2 мкс в *Ethernet*).

Для передачи информации в сети *Ethernet* применяется стандартный манчестерский код.

Доступ к сети *Ethernet* осуществляется по случайному методу CSMA/CD, обеспечивающему равноправие абонентов. В сети используются пакеты переменной длины со структурой, представленной на рис.2. (цифры показывают количество байт)

Рис 2. Структура пакета сети Ethernet

Длина кадра *Ethernet* (то есть пакета без преамбулы) должна быть не менее 512 битовых интервалов или 51,2 мкс (именно такова предельная величина двойного времени прохождения в сети). Предусмотрена индивидуальная, групповая и широковещательная адресация.

В пакет *Ethernet* входят следующие поля:

- Преамбула состоит из 8 байт, первые семь представляют собой код 10101010, а последний байт – код 10101011. В стандарте IEEE 802.3 восьмой байт называется признаком начала кадра (SFD – Start of Frame Delimiter) и образует отдельное поле пакета.
- Адреса получателя (приемника) и отправителя (передатчика) включают по 6 байт и строятся по стандарту, описанному в разделе "Адресация пакетов" лекции 4. Эти адресные поля обрабатываются аппаратурой абонентов.
- Поле управления (L/T – Length/Type) содержит информацию о длине поля данных. Оно может также определять тип используемого протокола. Принято считать, что если значение этого поля не больше 1500, то оно указывает на длину поля данных. Если же его значение больше 1500, то оно определяет тип кадра. Поле управления обрабатывается программно.
- Поле данных должно включать в себя от 46 до 1500 байт данных. Если пакет должен содержать менее 46 байт данных, то поле данных дополняется байтами заполнения. Согласно стандарту IEEE 802.3, в структуре пакета выделяется специальное поле заполнения (pad data – незначащие данные), которое может иметь нулевую длину, когда данных достаточно (больше 46 байт).
- Поле контрольной суммы (FCS – Frame Check Sequence) содержит 32-разрядную циклическую контрольную сумму пакета (CRC) и служит для проверки правильности передачи пакета.

Таким образом, минимальная длина кадра (пакета без преамбулы) составляет 64 байта (512 бит). Именно эта величина определяет максимально допустимую двойную задержку распространения сигнала по сети в 512 битовых интервалов (51,2 мкс для *Ethernet* или 5,12 мкс для *Fast Ethernet*). Стандарт предполагает, что преамбула может уменьшаться при прохождении пакета через различные сетевые устройства, поэтому она не учитывается. Максимальная длина кадра равна 1518 байтам (12144 бита, то есть 1214,4 мкс для *Ethernet*, 121,44 мкс для *Fast Ethernet*). Это важно для выбора размера буферной памяти сетевого оборудования и для оценки общей загруженности сети.

Выбор формата преамбулы не случаен. Дело в том, что последовательность чередующихся единиц и нулей (101010...10) в манчестерском коде характеризуется тем, что имеет переходы только в середине битовых интервалов (см. раздел 2.6.3), то есть только информационные переходы. Безусловно, приемнику просто настроиться (синхронизоваться) при такой последовательности, даже если она по какой-то причине укорачивается на несколько бит. Последние два единичные бита преамбулы (11) существенно отличаются от последовательности 101010...10 (появляются переходы еще и на границе битовых интервалов). Поэтому уже настроившийся приемник легко может выделить их и детектировать тем самым начало полезной информации (начало кадра).

Для сети *Ethernet*, работающей на скорости 10 Мбит/с, стандарт определяет четыре основных типа сегментов сети, ориентированных на различные *среды передачи* информации:

- 10BASE5 (толстый коаксиальный кабель);
- 10BASE2 (тонкий коаксиальный кабель);
- 10BASE-T (витая пара);
- 10BASE-FL (оптоволоконный кабель).

Наименование сегмента включает в себя три элемента: цифра "10" означает скорость передачи 10 Мбит/с, слово BASE – передачу в основной полосе частот (то есть без модуляции высокочастотного сигнала), а последний элемент – допустимую длину сегмента: "5" – 500 метров, "2" – 200 метров (точнее, 185 метров) или тип линии связи: "T" – витая пара (от английского "twisted-pair"), "F" – оптоволоконный кабель (от английского "fiber optic").

Точно так же для сети *Ethernet*, работающей на скорости 100 Мбит/с (*Fast Ethernet*) стандарт определяет три типа сегментов, отличающихся типами *среды передачи*:

- 100BASE-T4 (счетверенная витая пара);
- 100BASE-TX (сдвоенная витая пара);
- 100BASE-FX (оптоволоконный кабель).

Здесь цифра "100" означает скорость передачи 100 Мбит/с, буква "T" – витую пару, буква "F" – оптоволоконный кабель. Типы 100BASE-TX и 100BASE-FX иногда объединяют под именем 100BASE-X, а 100BASE-T4 и 100BASE-TX – под именем 100BASE-T.

Подробнее особенности аппаратуры *Ethernet*, а также алгоритма управления обменом CSMA/CD и алгоритма вычисления циклической контрольной суммы (CRC) будут рассмотрены далее в специальных разделах курса. Здесь следует отметить только то, что сеть *Ethernet* не отличается ни рекордными характеристиками, ни оптимальными алгоритмами, она уступает по ряду параметров

другим стандартным сетям. Но благодаря мощной поддержке, высочайшему уровню стандартизации, огромным объемам выпуска технических средств, *Ethernet* выгодно выделяется среди других стандартных сетей, и поэтому любую другую сетевую технологию принято сравнивать именно с *Ethernet*.

Развитие технологии *Ethernet* идет по пути все большего отхода от первоначального стандарта. Применение новых *сред передачи* и коммутаторов позволяет существенно увеличить размер сети. Отказ от манчестерского кода (в сети *Fast Ethernet* и Gigabit Ethernet) обеспечивает увеличение скорости передачи данных и снижение требований к кабелю. Отказ от *метода управления* CSMA/CD (при полнодуплексном режиме обмена) дает возможность резко повысить эффективность работы и снять ограничения с длины сети. Тем не менее, все новые разновидности сети также называются сетью *Ethernet*.

Расчет PDV

Для упрощения расчетов обычно используются справочные данные IEEE, содержащие значения задержек распространения сигналов в повторителях, приемопередатчиках и различных физических средах. В табл. 1 приведены данные, необходимые для расчета значения PDV для всех физических стандартов сетей Ethernet. Битовый интервал обозначен как bt.

Таблица 1. Данные для расчета значения PDV

Тип сегмента	База левого сегмента, bt	База промежуточного сегмента, bt	База правого сегмента, bt	Задержка среды на 1 м, bt	Максимальная длина сегмента, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	—	24,0	—	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000
AUI (> 2 м)	0	0	0	0,1026	2+48

Комитет 802.3 старался максимально упростить выполнение расчетов, поэтому данные, приведенные в таблице, включают сразу несколько этапов прохождения сигнала. Например, задержки, вносимые повторителем, состоят из задержки входного трансивера, задержки блока повторения и задержки выходного трансивера. Тем не менее в таблице все эти задержки представлены одной величиной, названной базой сегмента. Чтобы не нужно было два раза складывать задержки, вносимые кабелем, в таблице даются удвоенные величины задержек для каждого типа кабеля.

В таблице используются также такие понятия, как левый сегмент, правый сегмент и промежуточный сегмент. Поясним эти термины на примере сети, приведенной на рис. 3. Левым сегментом называется сегмент, в котором начинается путь сигнала от выхода передатчика конечного узла. На примере это сегмент *1*. Затем сигнал проходит через промежуточные сегменты *2-5* и доходит до приемника наиболее удаленного узла наиболее удаленного сегмента 6, который называется правым. Именно здесь в худшем случае происходит столкновение кадров и возникает коллизия, что, и подразумевается в таблице.

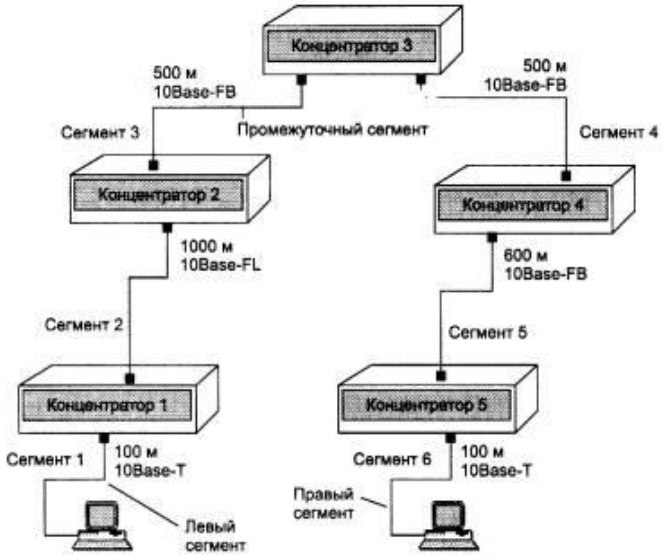


Рис. 3. Пример сети Ethernet, состоящей из сегментов различных физических стандартов

С каждым сегментом связана постоянная задержка, названная базой, которая зависит только от типа сегмента и от положения сегмента на пути сигнала (левый, промежуточный или правый). База правого сегмента, в котором возникает коллизия, намного превышает базу левого и промежуточных сегментов.

Кроме этого, с каждым сегментом связана задержка распространения сигнала вдоль кабеля сегмента, которая зависит от длины сегмента и вычисляется путем умножения времени распространения сигнала по одному метру кабеля (в битовых интервалах) на длину кабеля в метрах. Расчет заключается в вычислении задержек, вносимых каждым отрезком кабеля (приведенная в таблице задержка сигнала на 1 м кабеля умножается на длину сегмента), а затем суммировании этих задержек с базами левого, промежуточных и правого сегментов. Общее значение PDV не должно превышать 575.

Так как левый и правый сегменты имеют различные величины базовой задержки, то в случае различных типов сегментов на удаленных краях сети необходимо выполнить расчеты дважды: один раз принять в качестве левого сегмента сегмент одного типа, а во второй - сегмент другого типа. Результатом можно считать максимальное значение PDV. В нашем примере крайние сегменты сети принадлежат к одному типу - стандарту 10Base-T, поэтому двойной расчет не требуется, но если бы они были сегментами разного типа, то в первом случае нужно было бы принять в качестве левого сегмент между станцией и концентратором *1*, а во втором считать левым сегмент между станцией и концентратором *5*.

Приведенная на рисунке сеть в соответствии с правилом 4-х хабов не является корректной - в сети между узлами сегментов *1 и 6* имеется 5 хабов, хотя не все сегменты являются сегментами lOBase-FB. Кроме того, общая длина сети равна 2800 м, что нарушает правило 2500 м.

Расчетная формула PDV:

(Т зад. баз. лев.+L1*Т зад. среды) + … + (Т зад. баз. прав.+ L6*Т зад. среды) = PDV <575bt

Для расчетов вам понадобится данные комитета IEEE 802.3 о задержках сигналов в повторителях и кабельных сегментах (табл. 1,2):

Рассчитаем значение PDV для нашего примера.

Левый сегмент *1*/ 15,3 (база) + 100 * 0,113= 26,6.

Промежуточный сегмент *2*/33,5 + 1000 * 0,1 = 133,5.

Промежуточный сегмент *3*/ 24 + 500 * 0,1 = 74,0.

Промежуточный сегмент *4*/24 + 500 * 0,1 = 74,0.

Промежуточный сегмент *5*/ 24 + 600 * 0,1 = 84,0.

Правый сегмент *6*/165 + 100 * 0,113 = 176,3.

Сумма всех составляющих дает значение PDV, равное 568,4.

Так как значение PDV меньше максимально допустимой величины 575, то эта сеть проходит по критерию времени двойного оборота сигнала, несмотря на то, что ее общая длина составляет больше 2500 м, а количество повторителей - больше 4-х.

Расчет PVV

Чтобы признать конфигурацию сети корректной, нужно рассчитать также уменьшение межкадрового интервала повторителями, то есть величину PVV.

Для расчета PW также можно воспользоваться значениями максимальных величин уменьшения межкадрового интервала при прохождении повторителей различных физических сред, рекомендованными IEEE и приведенными в табл. 2.

Таблица 2. Сокращение межкадрового интервала повторителями

Тип сегмента	Передающий сегмент, bt	Промежуточный сегмент, bt
10Base-5 или 10Base-2	16	11
10Base-FB	—	2
10Base-FL	10,5	8
10Base-T	10,5	8

В соответствии с этими данными рассчитаем значение PVV для нашего примера.

Левый сегмент *1* 10Base-T: сокращение в 10,5 bt.

Промежуточный сегмент *2* 10Base-FL: 8.

Промежуточный сегмент *3* 10Base-FB: 2.

Промежуточный сегмент *4* 10Base-FB: 2.

Промежуточный сегмент *5* 10Base-FB: 2.

Сумма этих величин дает значение PW, равное 24,5, что меньше предельного значения в 49 битовых интервала.

Лабораторная работа №5

Тема: Программирование маршрутизаторов

Цель: Изучение основ программирования маршрутизаторов ЛВС в программе Packet Tracer

Задание:

1. Изучить общий вид программы Packet Tracer;

2. Научиться добавлять, заменять и удалять платы из устройства;

3. Собрать схему локальной сети;

4. Назначить IP адреса;

5. Протестировать сеть на работоспособность.

Методика выполнения:

По приложению к лабораторной работе изучите общий вид программы Packet Tracer.

Практическая часть

1. Добавим на рабочую область программы 2 коммутатора Switch-PT. По умолчанию они имеют имена – Switch0 и Switch1.
2. Добавим на рабочее поле четыре компъютера с именами по умолчанию PC0, PC1, PC2, PC3.
3. Соединим устройства в сеть Ethernet , как показано на рис.1
4. Сохраним созданную топологию, нажав кнопку Save (в меню File -> Save).
5. Откроем свойства устройства PC0 нажав на его изображение. Перейдем к вкладке Desktop и симулируем работу run нажав Command Prompt.
6. IP адрес и маску сети будем вводить в удобном графическом инерфейсе устройства (см. рис.2). Поле DEFAULT GATEWAY – адреса шлюза не важно, так как создаваемая сеть не требует маршрутизации.

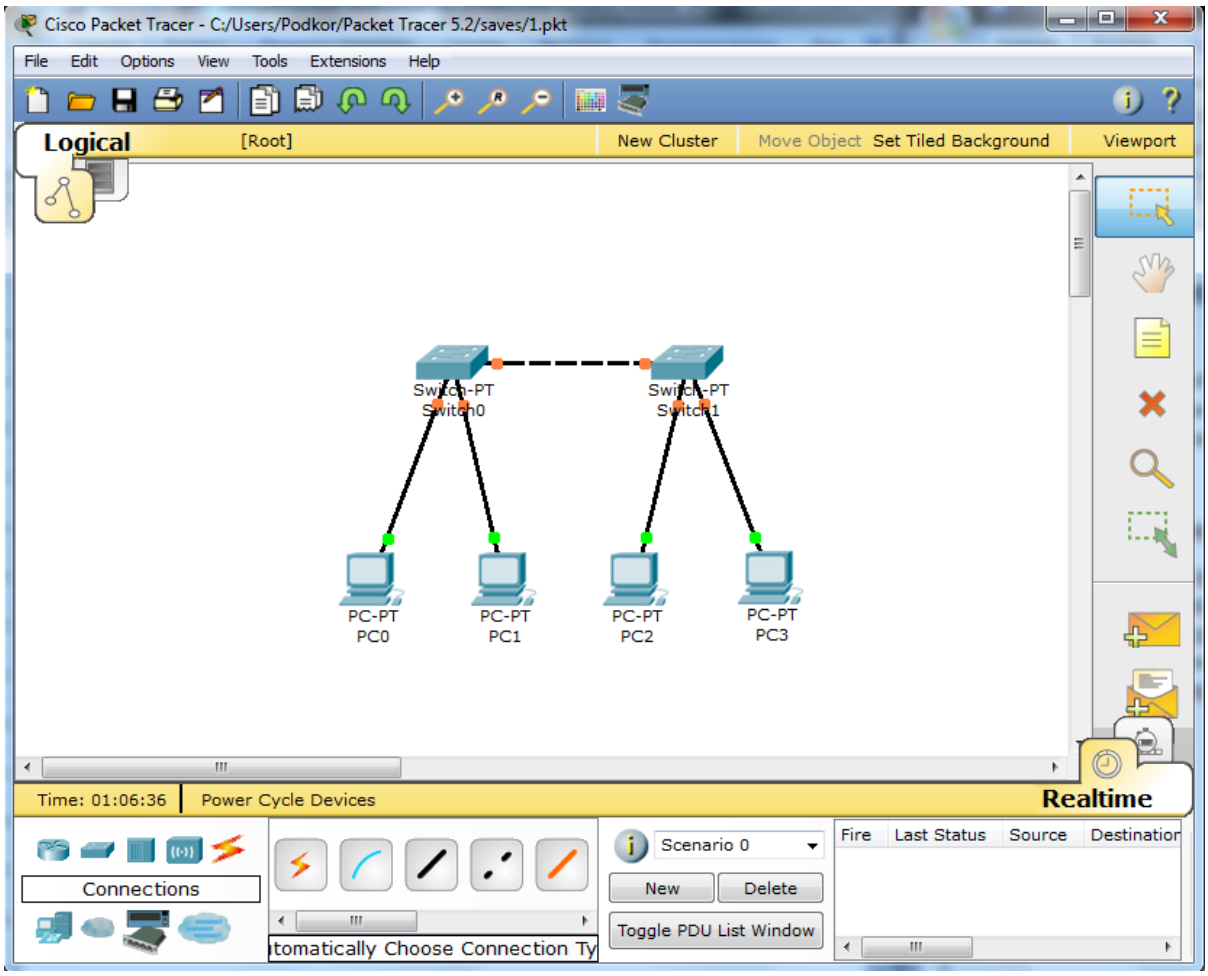


Рис.1

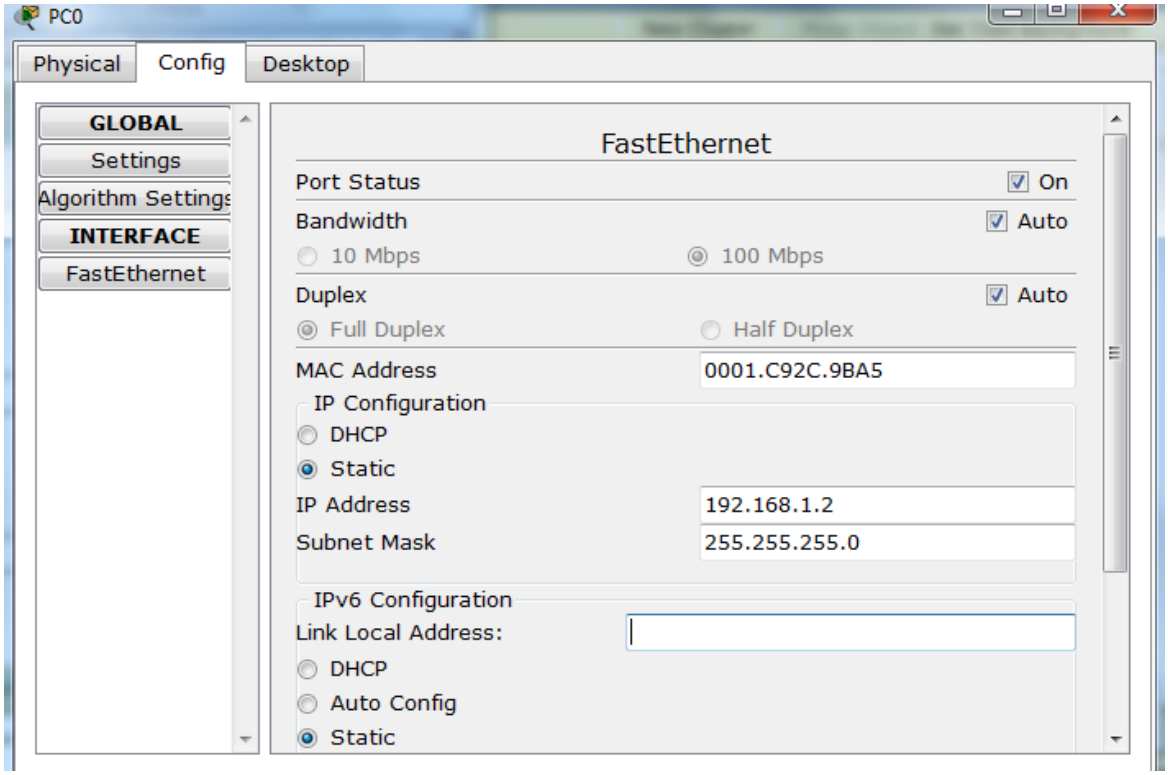


Рис.2

Таким же путем настроим каждый компьютер.

Устройство	IP ADRESS	SUBNET MASK

PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

7. На каждом компъютере посмотрим назначеные адресса командой **ipconfig** без параметров.
8. Если все сделано правильно мы сможем пропинговать любой из любого компъютера. Например, зайдем на компъютер PC3 и пропингуем компъютер PC0. Мы должны увидеть отчет о пинге подобный рисунку 3.

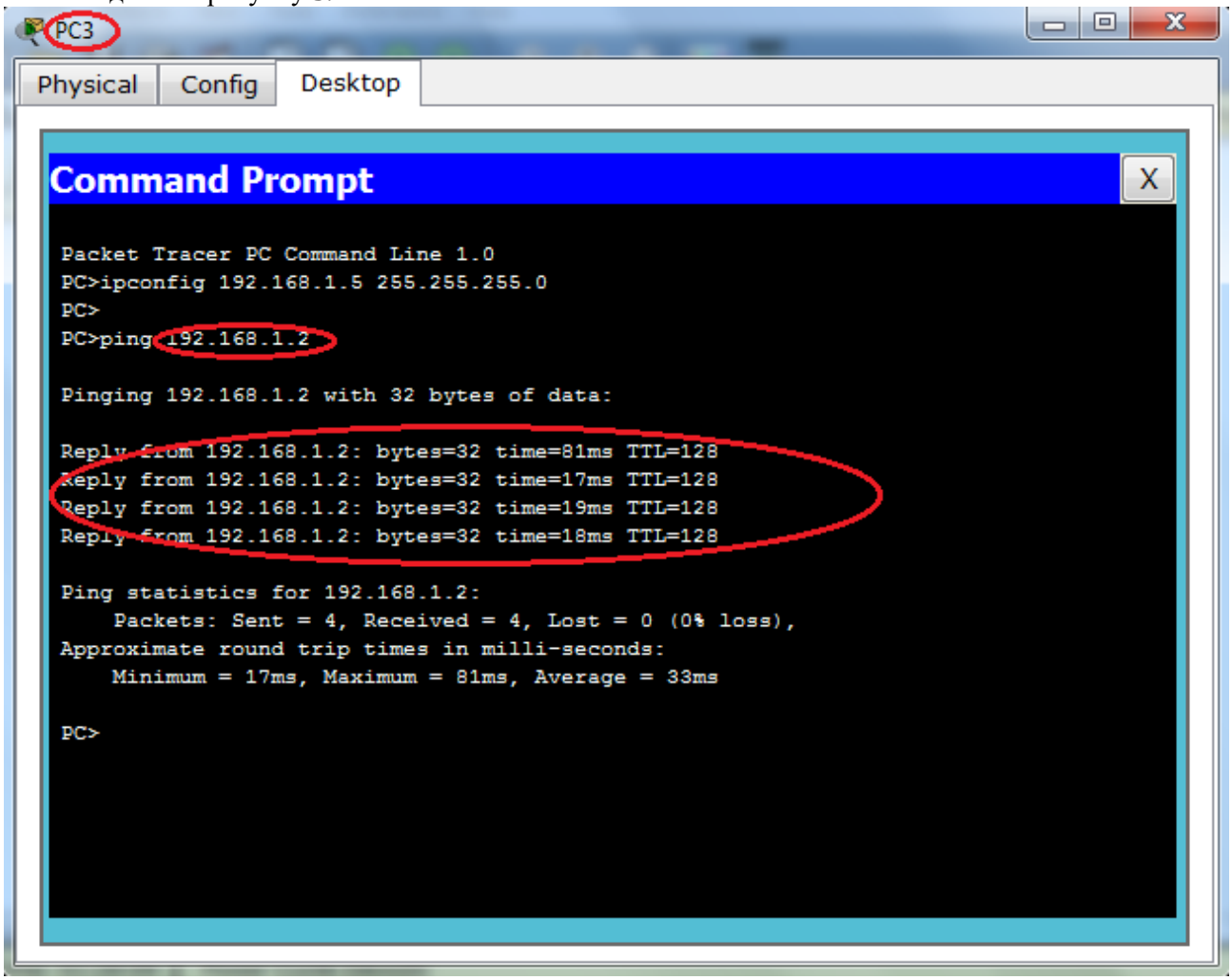


Рис.3

Контрольные вопросы:
1 Классификация сетей связи.
2 Основные компоненты информационных сетей.
3 Топологии физических связей.
4 Сетевые протоколы.
5 IP-адрес, что он из себя представляет.

1. Описание программы Packet Tracer 5.1
1.1 Общий вид программы Packet Tracer 5.1
Для начала работы выполните следующие действия:
Запустите ярлык программы на рабочем столе. Перед Вами представлено главное окно программы (см. рис. 4.).

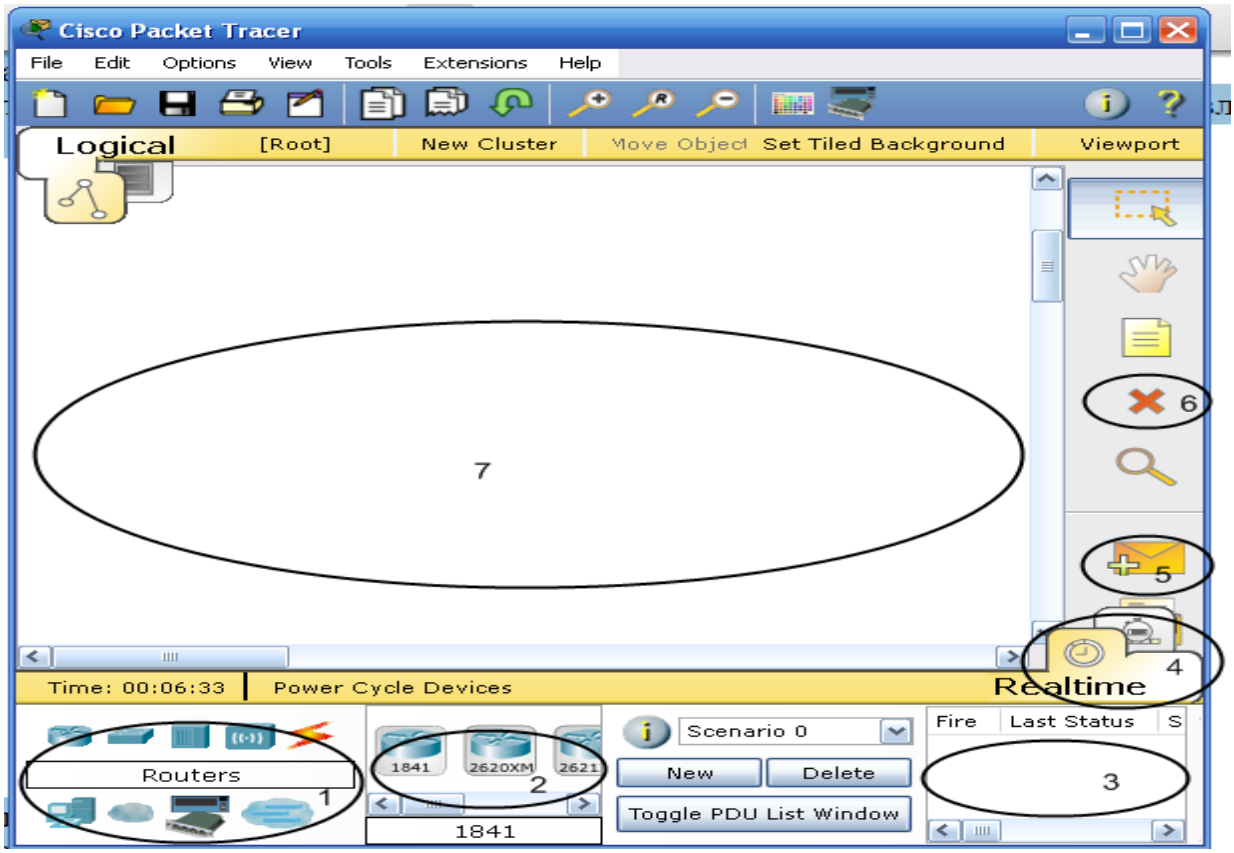


Рис. 4. Общий вид главного окна программы Packet Tracer

На рисунке 4 цифрами обозначены:

1: Область выбора типа сетевого оборудования.
2: Область выбора определенного устройства заданного типа.
3: Область управления созданными пакетами.
4: Область переключения между режимом реального времени и режимом симуляции.
5: Кнопка создания пакета “ping”.
6: Кнопка удаления объекта.
7: Рабочая область.

Добавленные элементы связываются с помощью соединительных связей. Для этого необходимо выбрать вкладку **Connections** в области выбора сетевого устройства. Мы увидим все возможные типы соединений между устройствами. Выберем подходящий тип кабеля. Выберем и нажмем на каждом из устройств, которые нужно соединить. Между устройствами появится кабельное соединение, а индикаторы на каждом конце покажут статус соединения (для интерфейсов которые имеют индикатор).

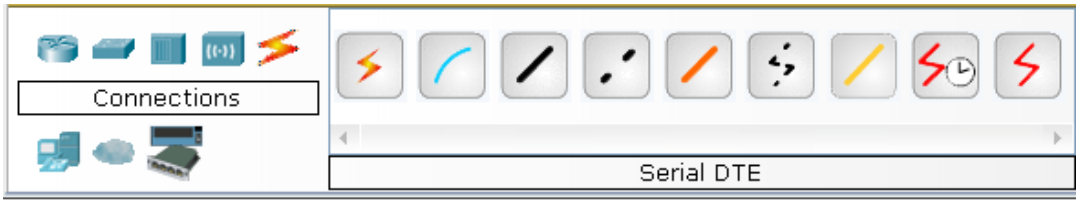


Рис. 5 Поддерживаемые в Packet Tracer типы кабелей.

Packet Tracer поддерживает широкий диапазон сетевых соединений (см. табл. 1). Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов.

Тип кабеля	Описание
Console	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами.
Copper Straight-through	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, который функционирует на разных уровнях

	OSI. Он должен быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).
Copper Cross-over	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).
Fiber	Оптоволоконная среда используется для соединения между оптическими портами (100 Мбит/с или 1000 Мбит/с).
Phone	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты.
Coaxial	Коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельный модем, соединенный с облаком Packet Tracer.
Serial DCE and DTE	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становиться DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

Таблица 1. Типы соединений в Packet Tracer

1.2 Добавление, замена и удаление плат из устройства

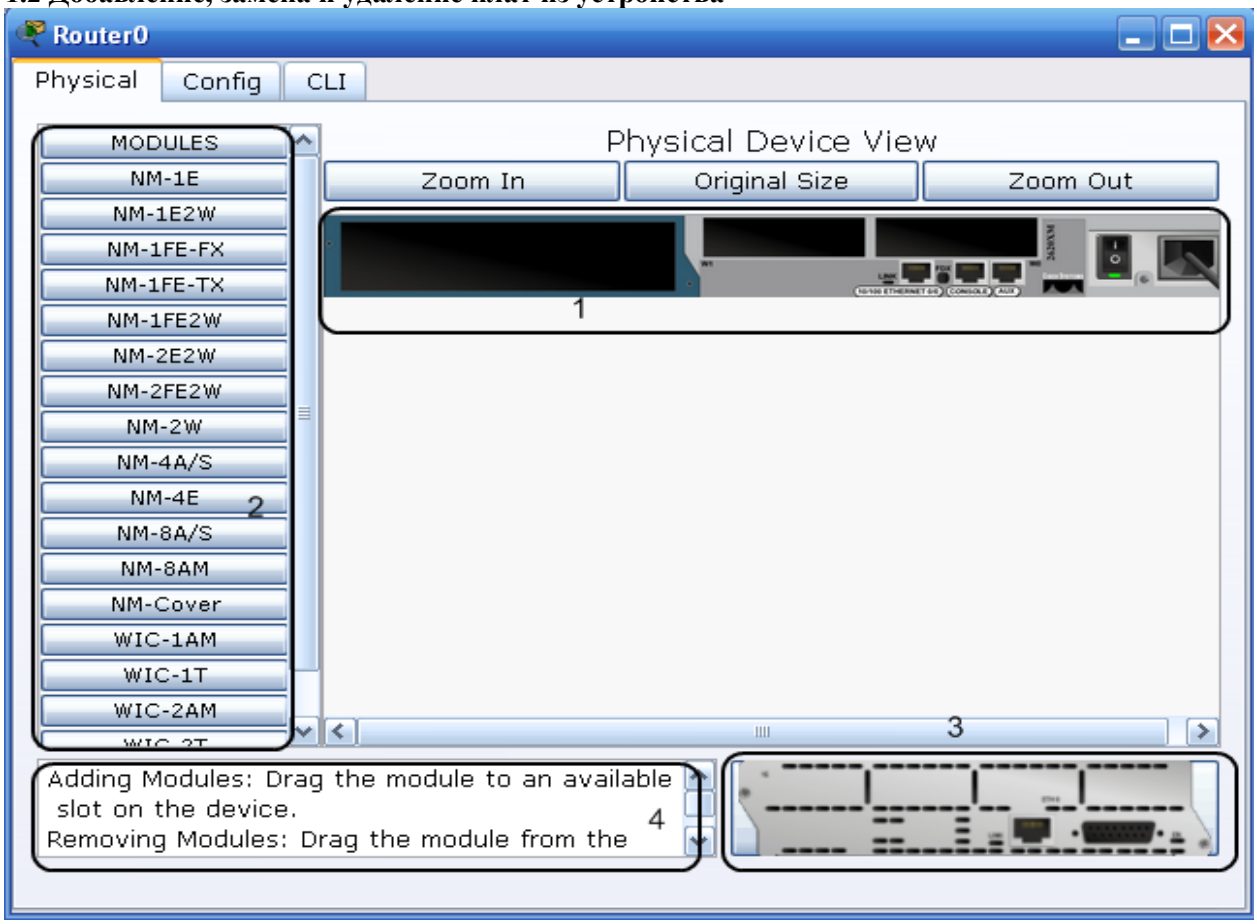


Рис. 6. Вид окна настроек оборудования

На рисунке 6 цифрами обозначены:

1: Внешний вид выбранного устройства.
2: Поле выбора платы, которую можно установить в устройство.
3: Внешний вид выбранной платы.
4: Описание выбранной платы.

Порядок выполнения действий

1. Перетащите выбранное сетевое устройство на рабочую область.
2. Левой кнопкой мыши щелкните по нему. Перед вами появится окно, представленное на рисунке 6.
3. Отключите питание устройства тумблером.
4. Чтобы удалить одну из плат перетащите ее из устройства в поле 2 или 3.
5. Чтобы добавить плату в устройство перетащите ее изображение из поля 3 в соответствующий слот поля 1.
6. Включите питание тумблером.

1.3 Использование пакета “ping” в режиме симуляции для проверки работоспособности сети

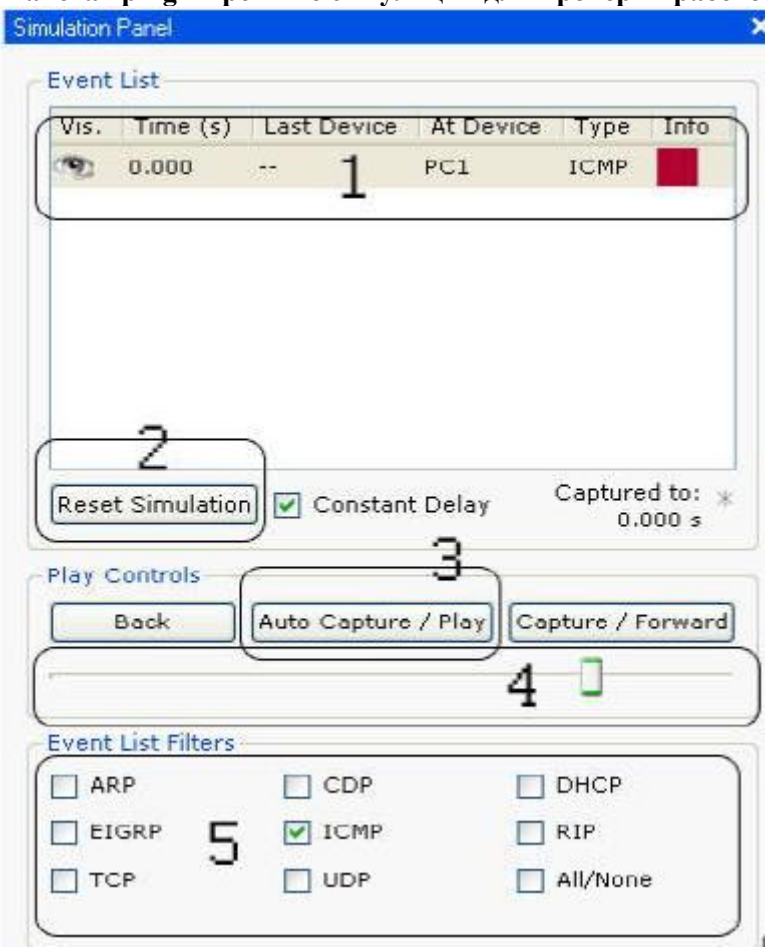


Рис. 7. Окно режима симуляции

На рисунке 7 цифрами обозначены:
1: Список пакетов.
2: Кнопка сброса симуляции в начало.
3: Кнопка запуска / останова симуляции.
4: Бегунок регулирования скорости симуляции.
5: Поле выбора типа пакетов, движение которых будет отслеживаться.

Порядок выполнения действий

1. В режиме симуляции нажмите на значок “Add Simple PDU” -  в правой части главного окна программы (см. рис. 4).
2. Нажмите на устройство, с которого вы хотите послать пакет “ping”.
3. Нажмите на устройство, на которое вы хотите послать пакет “ping”.

4. В поле выбора типа пакетов для отслеживания окна режима симуляции (см. рис.7) отметьте галочками те протоколы, пакеты которых вы хотите отслеживать. В рамках данной лабораторной работы будет отслеживаться только движение пакета “ping”, который относится к протоколу ICMP* и пакетов протокола ARP**. Только около этих протоколов должны стоять галочка, у остальных протоколов галочки должны быть сняты.
5. Запустите симуляцию.
6. Проследите путь прохождения пакета.
В случае если сеть настроена правильно и функционирует корректно, пакет вернется на устройство, с которого был послан пакет. Если пакет был отброшен одним из устройств, проверьте наличие и правильность записей в таблицах сетевых устройств. После установления причины сбоя в работе нажмите кнопку “Reset Simulation”, а затем снова запустите симуляцию.
Примечание:
* **ICMP -** протокол обмена управляющими сообщениями ICMP (Internet Control Message Protocol) позволяет маршрутизатору сообщить конечному узлу об ошибках, с которыми машрутизатор столкнулся при передаче какого-либо IP-пакета от данного конечного узла. Управляющие сообщения ICMP не могут направляться промежуточному маршрутизатору, который участвовал в передаче пакета, с которым возникли проблемы, так как для такой посылки нет адресной информации - пакет несет в себе только адрес источника и адрес назначения, не фиксируя адреса промежуточных маршрутизаторов.
Протокол ICMP - это протокол сообщения об ошибках, а не протокол коррекции ошибок. Конечный узел может предпринять некоторые действия для того, чтобы ошибка больше не возникала, но эти действия протоколом ICMP не регламентируются. Каждое сообщение протокола ICMP передается по сети внутри пакета IP. Пакеты IP с сообщениями ICMP маршрутизируются точно так же, как и любые другие пакеты, без приоритетов, поэтому они также могут теряться. Кроме того, в загруженной сети они могут вызывать дополнительную загрузку маршрутизаторов. Для того, чтобы не вызывать лавины сообщения об ошибках, потери пакетов IP, переносящие сообщения ICMP об ошибках, не могут порождать новые сообщения ICMP.
ARP – адресный протокол для отображения IP-адресов в Ethernet адреса используется протокол ARP (Address Resolution Protocol). Отображение выполняется только для отправляемых IP-пакетов, так как только в момент отправки создаются заголовки IP и Ethernet.

Практическая работа №5

Тема: Работа с диагностическими утилитами СКС

Цель работы: ознакомиться с основными диагостическими коммандами системы Cisco IOS

Теоретическая часть.

Для настройки сетевого оборудования в вашем распоряжении имеются разнообразные команды операционной системы Cisco IOS.

При входе в сетевое устройство командная строка имеет вид:

Switch>

Команды, доступные на пользовательском уровне являются подмножеством команд, доступных в привилегированном режиме. Эти команды позволяют выводить на экран информацию без смены установок сетевого устройства.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим.

Press ENTER to start.

Switch>

Switch> enable

Switch#

Выход из привилегированного режима:

Switch# disable

Switch>

О переходе в привилегированный режим будет свидетельствовать появление в командной строке приглашения в виде знака #.

Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, подъинтерфейса, линии, сетевого устройства, карты маршрутов и т.п.

Для выхода из системы IOS необходимо набрать на клавиатуре команду exit (выход):

Switch> exit

Возможна работа в следующих режимах:

- Пользовательский режим — это режим просмотра, в котором пользователь может только просматривать определённую информацию о сетевом устройстве, но не может ничего менять. В этом режиме приглашение имеет вид:

Switch>

- Привилегированный режим— поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид:

Switch#

- Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В том режиме приглашение имеет вид:

Switch(config)#

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии табуляции IOS сам дополнит команду до полного имени.

При вводе в командной строке любого режима имени команды и знака вопроса (?) на экран выводятся комментарии к команде. При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка - More -. Для продолжения следует нажать enter или пробел.

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования включают команды переходу в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима configure. При вводе этой команды следует указать источник команд конфигурирования:

- terminal (терминал),
- memory (энергонезависимая память или файл),
- network (сервер tftp (Trivial ftp -упрощённый ftp) в сети).

По умолчанию команды вводятся с терминала консоли, например:

Switch(config)#(commands)
Switch(config)#exit
Switch#
Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение
Switch(config-if)#
сначала вводится глобальная команда для определения типа интерфейса и номера его порта:
Switch#conf t
Switch(config)#interface type port
Switch(config-if)#(commands)
Switch(config-if)#exit
Switch(config)#exit
Практическая работа №3. Знакомство с командами IOS.
Основные команды сетевого устройства
1. Войдите сетевое устройство Router1
Router>
2. Мы хотим увидеть список всех доступных команд в этом режиме. Введите
команду, которая используется для просмотра всех доступных команд:
Router>?
Клавишу Enter нажимать не надо.
3. Теперь войдите в привилегированный режим
Router>enable
Router#
4. Просмотрите список доступных команд в привилегированном режиме
Router#?
5. Перейдём в режим конфигурации
Router#config terminal
Router(config)#
6. Имя хоста сетевого устройства используется для локальной идентификации.
Когда вы входите в сетевое устройство, вы видите Имя хоста перед символом режима (">" или "#"). Это имя может быть использовано для определения места нахождения.
Установите "Router1" как имя вашег сетевого устройства.
Router(config)#hostname Router1
Router1(config)#
7. Пароль доступа позволяет вам контролировать доступ в привилегированный
режим. Это очень важный пароль, потому что в привилегированном режиме можно вносить конфигурационные изменения. Установите пароль доступу "parol".
Router1(config)#enable password parol
1. Давайте испытаем этот пароль. Выйдите из сетевого устройства и попытайтесь зайти в привилегированный режим.
2.
Router1>en
Password:*****
Router1#
Здесь знаки: ***** - это ваш ввод пароля. Эти знаки на экране не видны.

Основные Show команды.
Перейдите в пользовательский режим командой disable. Введите команду для просмотра всех доступных show команд.
Router1>show ?
1. Команда show version используется для получения типа платформы сетевого устройства, версии операционной системы, имени файла образа операционной системы, время работы системы, объём памяти, количество интерфейсов и конфигурационный регистр.
2. Просмотр времени:
Router1>show clock
3. Во флеш-памяти сетевого устройства со аняется файл-образ операционной системы Cisco IOS. В

отличие от оперативной памяти, в реальных устройствах флеш память со аняет файл-образ даже при сбое питания.
Router1>show flash
4. ИКС сетевого устройства по умолчанию со аняет10 последних введенных команд
Router1>show history
5. Две команды позволят вам вернуться к командам, введённым ранее. Нажмите на стрелку вверх или <ctrl> P.
6. Две команды позволят вам перейти к следующей команде, со анённой в буфере.
Нажмите на стрелку вниз или <ctrl> N
7. Можно увидеть список хостов и IP-Адреса всех их интерфейсов
Router1>show hosts
8. Следующая команда выведет детальную информацию о каждом интерфейсе
Router1>show interfaces
9. Следующая команда выведет информацию о каждой telnet сессии:
Router1>show sessions
10. Следующая команда показывает конфигурационные параметры терминала:
Router1>show terminal
11. Можно увидеть список всех пользователей, подсоединённых к устройству по терминальным линиям:
Router1>show users
12. Команда
Router1>show controllers
показывает состояние контроллеров интерфейсов.
13. Перейдём в привилегированный режим.
Router1>en
14. Введите команду для просмотра всех доступных show команд.
Router1#show ?
Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых.
15. Посмотрим активную конфигурацию в памяти сетевого устройства. Необходим привилегированный режим. Активная конфигурация автоматически не со аняется и будет потеряна в случае сбоя электропитания. Чтобы со анить настройки роутера используйте следующие команды:
со анение текущей конфигурации:
Router# write memory
Или
Router# copy run start
Просмотр со аненной конфигурации:
Router# Show configuration
или
Router1#show running-config
В строке more, нажмите на клавишу пробел для просмотра следующей страницы информации.
16. Следующая команда позволит вам увидеть текущее состояние протоколов
третьего уровня:
Router#show protocols
Введение в конфигурацию интерфейсов.
Рассмотрим команды настройки интерфейсов сетевого устройства.
На сетевом устройстве Router1 войдём в режим конфигурации:

Router1#conf t
Router1(config)#

2. Теперь ми хотим настроить Ethernet интерфейс. Для этого мы должны зайти в режим конфигурации интерфейса:
Router1(config)#interface FastEthernet0/0
Router1(config-if)#
3. Посмотрим все доступные в этом режиме команды:
Router1(config-if)#?

Для выхода в режим глобальной конфигурации наберите exit. Снова войдите в режим конфигурации интерфейса:
Router1(config)#int fa0/0
Мы использовали сокращенное имя интерфейса.
4. Для каждой команды мы можем выполнить противоположную команду, поставивши перед ней слово no. Следующая команда включает этот интерфейс:
Router1(config-if)#no shutdown
5. Добавим к интерфейсу описание:
Router1(config-if)#description Ethernet interface on Router 1
Чтобы увидеть описание этого интерфейса, перейдите в привилегированный режим и выполните команду show interface :
Router1(config-if)#end
Router1#show interface
6. Теперь присоединитесь к сетевому устройству Router 2 и поменяйте имя его хоста на Router2:
Router#conf t
Router(config)#hostname Router2
Войдём на интерфейс FastEthernet 0/0:
Router2(config)#interface fa0/0
Включите интерфейс:
Router2(config-if)#no shutdown
Теперь, когда интерфейсы на двух концах нашего Ethernet соединения включены на экране появится сообщение о смене состояния интерфейса на активное.
7. Перейдём к конфигурации последовательных интерфейсов. Зайдём на Router1.
Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: оконечным устройством DTE (data terminal equipment), либо устройством связи DCE (data circuit):
Router1#show controllers fa0/1
Если видим сообщение:
DCE cable
то наш маршрутизатор является устройством связи и он должен задавать частоту син онизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.
Router1#conf t
Router1(config)#int fa0/1
Router1(config-if)#clock rate ?
Выберем частоту 64000
Router1(config-if)#clock rate 64000
и включаем интерфейс
Router1(config-if)#no shut
Контрольные вопросы.

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера.
3. Как просмотреть конфигурационные настройки коммутатора?
4. Как определить распределение вилланов по портам коммутатора?
5. Перечислите основные режимы конфигурации при настройке коммутатора.
6. Перечислите основные режимы конфигурации при настройке роутера.
7. Как посмотреть таблицу маршрутизации на роутере?
8. Какие команды формируют таблицу маршрутизации роутера?
9. Какими командами настраиваются вилланы на коммутаторе?
10. Какими командами настраивается взаимодействие между вилланами?

Практическая работа № 6

Тема Эскизное проектирование СКС.

Цель: научиться проектировать структурированную кабельную сеть.

Теоретические сведения

Структурированная кабельная система (СКС) — основа информационной инфраструктуры предприятия, позволяющая свести в единую систему множество информационных сервисов разного назначения: локальные вычислительные и телефонные сети, системы безопасности, видео наблюдения и т.д.

СКС представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. Она состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Термин ***«структурированная»*** означает, с одной стороны, способность системы поддерживать различные телекоммуникационные приложения (передачу речи, данных и видеоизображений), с другой — возможность применения различных компонентов и продукции различных производителей, и с третьей — способность к реализации так называемой мультимедийной среды, в которой используются несколько типов передающих сред — коаксиальный кабель, UTP, STP и оптическое волокно. Структуру кабельной системы определяет инфраструктура информационных технологий, IT (Information Technology), именно она диктует содержание конкретного проекта кабельной системы в соответствии с требованиями конечного пользователя, независимо от активного оборудования, которое может применяться впоследствии.

Типовые работы по монтажу СКС включают:

- установку кабельных каналов (коробах, лотках, гофротрубе, трубах и т.п.);
- пробивку отверстий в стенах;
- прокладку кабеля в кабельных каналах;
- установку розеток и заделку кабеля модули розетки;
- сборку и установку монтажного шкафа;
- установку и набивку патч-панелей и органайзеров.

Этапы монтажа СКС:

- Изучение объекта для монтажа СКС;
- Разработка технического проекта;
- Подбор необходимого оборудования и монтаж на объекте;
- Тестирование и сертификация, сдача работ заказчику;
- После установочная поддержка и обучение

Каждое рабочее место пользователя должно быть оборудовано розеткой электропитания с заземлением и информационными розетками. В небольших организациях обычно используют розетки существующей электропроводки. При этом следует учитывать, что расстояние между силовой и информационными розетками одного рабочего места по стандарту не должно превышать 1 м.

Выполнение работы

Задание 1. Учитывая исходную информацию (примерный план здания образовательного заведения, количество и специфику оборудования и применяемые технологии) спроектировать структурированную кабельную сеть (собрать исходные данные; выбрать оборудование, рассчитать примерную стоимость оборудования и материалов).

Описание задания

Необходимо спроектировать структурированную кабельную сеть для компьютерной сети школы.

Исходные данные

Здание школы 3-х этажное , кирпичное , перекрытия железобетонные, имеет два внутренних лестничных «стояка». Высота потолков – 2,7м . В горизонтальном разрезе имеет форму буквы «П». В школе имеются 45 учебных аудиторий, стандартного размера 12х6 м .

На удалении 120 м от основного здания находятся учебные школьные мастерские, где кроме всего прочего, располагается кабинет заместителя директора. Здание мастерских кирпичное, одно этажное, высота потолков 2,7м.

В школе уже существует две компьютерные сети:

- административная сеть, объединяющая компьютеры директора, секретаря и бухгалтерии – 5 рабочих мест, 1 этаж правое крыло здания;
- автономная ЛВС кабинета информатики -15 рабочих мест, 2-й этаж , правое крыло, окна выходят во внутренний двор здания;

Школа имеет доступ к сети ИНТЕРНЕТ, точка входа в комнате лаборантов компьютерного класса (2-й этаж, правое крыло здания) – отдельное рабочее место 1ПК.
Все компьютеры однотипные, ОС Windows XP, прикладное ПО однотипное, за исключением 3-х ПК бухгалтерии , на которых установлена кроме того ПО 1С.Бухгалтерия.
Кроме этого еще в 5-ти кабинетах имеются демонстрационные компьютеры с проекторами, и в библиотеке одно рабочее место, включающее в себя ПК и МФУ.

При создании компьютерной сети, планируется:

- развёртывание, дополнительно 3-х компьютерных классов (обозначено на схеме здания «1»);
- создание файл-сервера, для нужд школьной библиотеки (размещение сервера на усмотрение разработчика);
- организация 4-х рабочих мест для заместителей директора (обозначено на схеме здания «2»);
- организация 5-ти рабочих мест в учительской (обозначено на схеме здания «3»);
- организация видео наблюдения, по периметру основного здания (4 точки), внутри здания 12 точек, и 2 точки в здании школьных мастерских;
- в каждой учебной аудитории школы иметь минимум одно рабочее место;

Цели использования сети:

- Обучение школьников различным дисциплинам с использованием сетевых технологий.
- Доступ к информационным ресурсам (библиотека, Интернет).
- Демонстрация видео уроков (в том числе и через Интернет) .
- Голосовое общение по сети (в том числе и через Интернет)
- Одновременная трансляция видео и передача голосовых данных.

Требуемые характеристики сети:

- скорость передачи достаточная для поддержания видео и голосового трафика;
- возможность организации доступа в сеть Интернет;
- создание единого информационного пространства для структурных подразделений учреждения;
- логическое структурирование информационной сети, разграничение прав доступа для отдельных сегментов;
- возможность ограничения доступа пользователей к ресурсам сети;
- масштабируемость сети, то есть способность легко расширяться;
- обеспечение отказоустойчивости, надёжности, защиты и управляемости сети в целом.

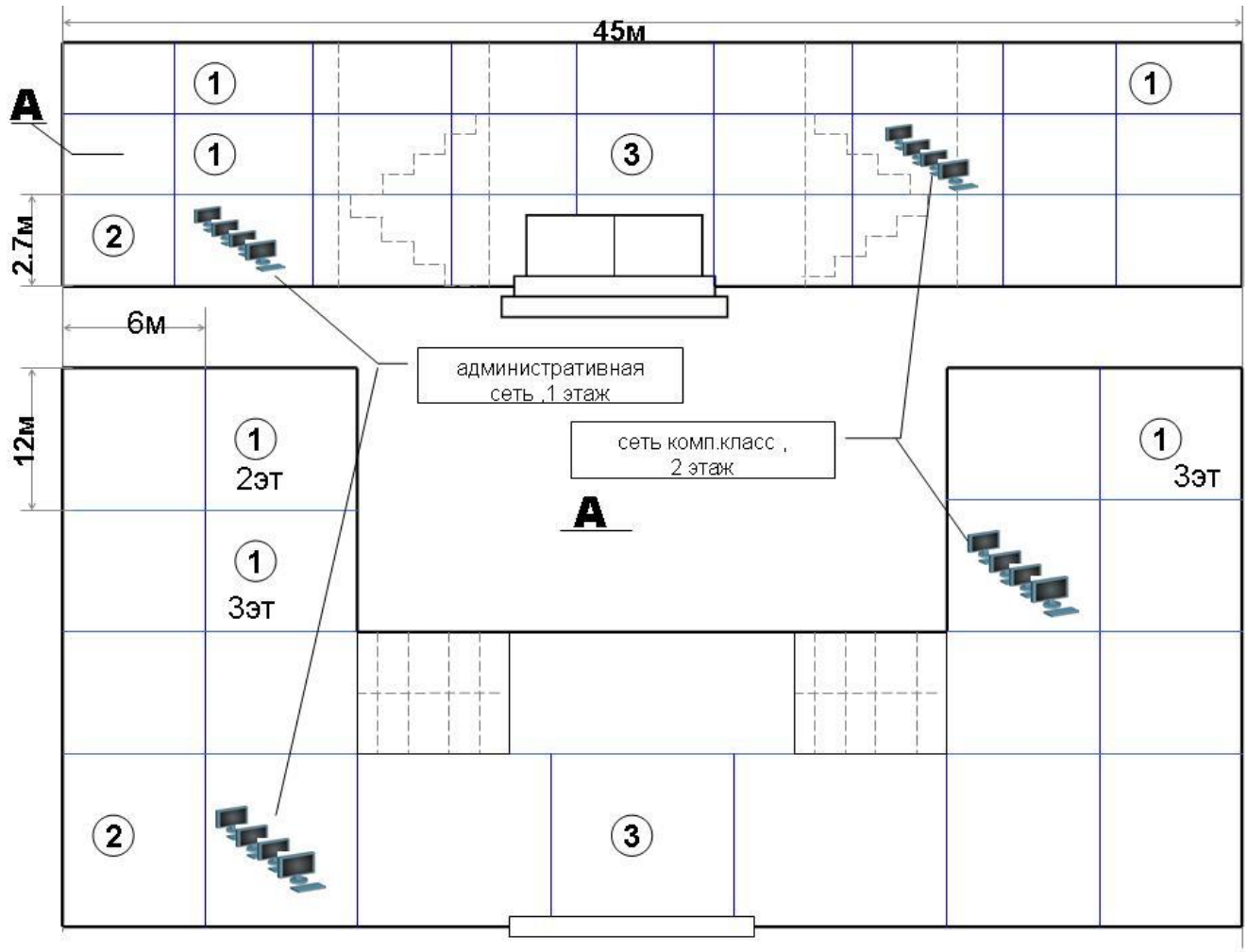


Рисунок 1. план основного здания школы с имеющимися ЛВС.

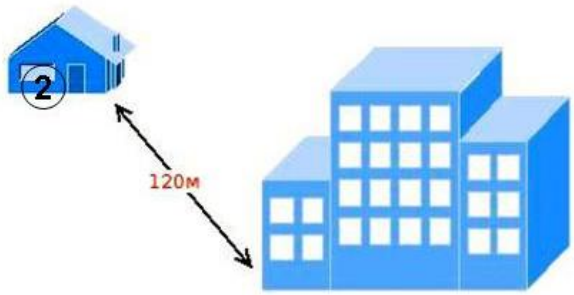


Рисунок 2. схема взаимного расположения основного и дополнительного зданий школы

Проектирование сети

Используя исходные данные определить:

способ сегментирования и объединения сегментов, используемые технологии ПД

порядок размещения сетевого активного оборудования

тип кабельной продукции, места «входа» в учебные аудитории, порядок монтажа

тип кабельной продукции, места «входа» в учебные аудитории, порядок монтажа

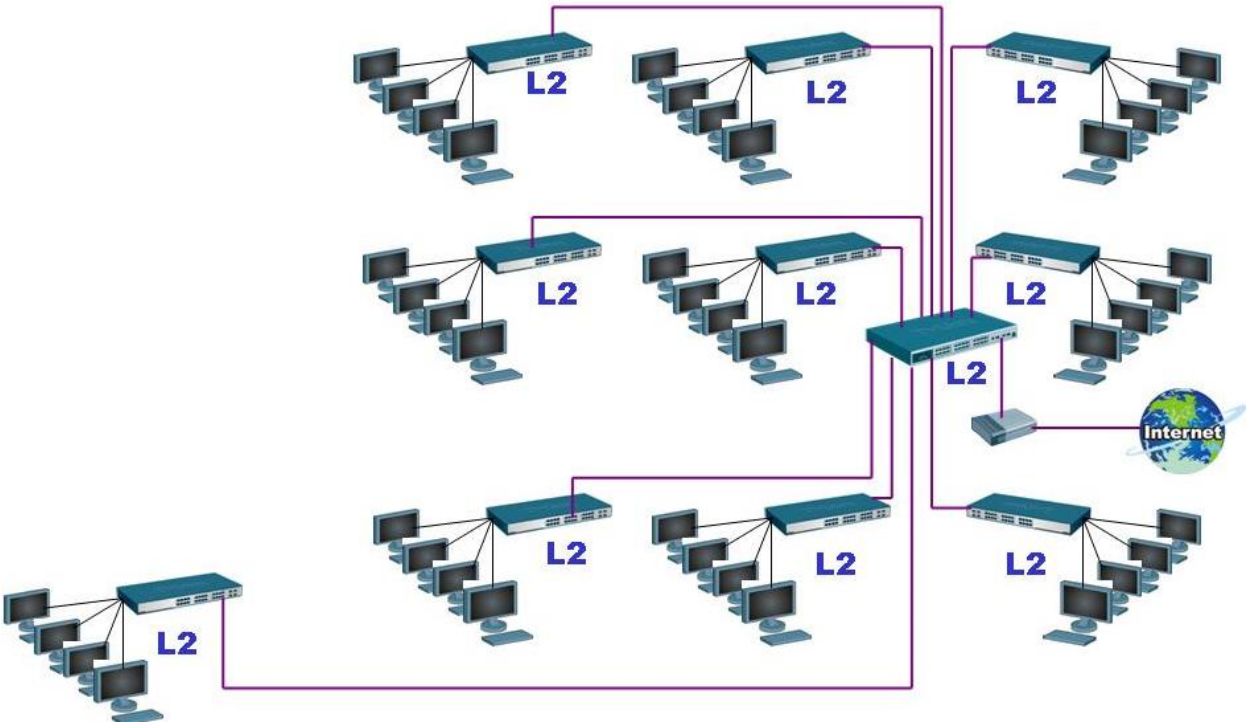


Рисунок 3. примерная схема распределения коммутаторов

Практическая работа №8
Тема: Распределение пула IP адресов
Цель работы: Получить знания о масках подсетей
Задачи работы:

1. **Научиться конвертировать различные представления маски**
2. **Приобрести навыки определения значений средних диапазонов подсетей**
3. **Подготовить отчет о проделанной работе.**

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Первейшая проблема стандартной IP-маршрутизации заключалась в том, что на фоне общего развития Интернета большое количество IP-адресов раздавалось, но оставалось неиспользованным. Что, в свою очередь, приводило к быстрому перерасходу адресного пространства. Вызвано это

большими различиями в количестве IP-адресов в разных классах. По своей сути, сеть в организации, как правило, представляет собой локальную сеть, подключенную через какую-либо точку – маршрутизатор или шлюз. Такая локальная сеть в Интернете и интерпретируется как подсеть. Снаружи, со стороны Интернета, обращение ведется лишь к одному устройству сети – маршрутизатору (шлюзу), и, совершенно все равно, сколько компьютеров и сетей стоит за этим маршрутизатором. При этом трафик направляется на него, а он сам занимается его последующим распределением. При этом, IP-адрес в подсети состоит из таких компонентов, как идентификатор сети и идентификатор узла. Идентификаторы сети и узла содержатся в идентификаторе узла исходного IP-адреса, при этом фактически забирается часть битов ID узла для ID сети. Осуществляется это путем использования специального псевдоадреса IP, называемого маской сети. И в этой лабораторной работе вы узнаете о компоненте, который определяет, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети и предоставляющем идентификатор сети – о **маске подсети**.

По сути, маска подсети предоставляет набор методов, которые можно использовать для эффективного разделения адресного пространства префикса адреса для распределения подсетей сети организации. Фиксированная часть префикса индивидуальных адресов включает в себя определенное количество бит и длину префикса, которые имеют определенное значение. Переменная часть префикса индивидуальных адресов включает в себя биты, расположенные за пределами длины префикса, которые могут равняться 0. Подсети предназначены для использования переменной части префикса индивидуальных адресов и создания префиксов, которые присваиваются в подсетях сети организации. Именно благодаря подсетям вы можете определить какие из 32 битов используются для идентификатора сети и для идентификатора узла в адресах класса A и класса B.

Например, вы наверняка часто видели записи IPv4 адресов вида: 192.168.23.245/24, где значение /24 является маской подсети и указывает на то, что в этом адресе первые 24 бита из 32 представляют идентификатор сети. А подсеть адреса 156.60.0.20/16 может поддерживать до 65534 узлов, что является приличным количеством и не требует перенастройки маршрутизаторов сети Интернет.

Обе указанные выше подсети (/24 и /16) легко интерпретируются. Обратим внимание на то, что значения обеих указанных выше масок подсети делятся на 8 и, соответственно, легко догадаться, что идентификатор сети состоит из первых трех и первых двух октетов IPv4 адреса. То есть, в узле с адресом 192.168.23.245/24 идентификатором сети является 192.168.23, поэтому сетевым адресом узла будет 192.168.23.0. А в узле с адресом 156.60.0.20 ID сети будет 156.60, и сетевой адрес узла будет 156.60.0.0.

Подсети IPv4 производят набор префиксов адресов подсетей и диапазонов, допустимых IPv4-адресов, предназначенных для назначения префиксов адресов подсетей, а также количество принимающих идентификаторов для физических и логических подсетей IPv4 сети организации, в связи с чем, организации сети могут использовать получившееся адресное пространство наиболее эффективным образом.

Перед проектированием подсетей организации необходимо обратить внимание на следующие моменты:

- Сколько подсетей включает сеть организации (включая физические, логические, а также подсети, предназначенные для WAN ссылок между сайтами);
- Количество идентификаторов узлов, которое необходимо для каждой подсети. Необходимо помнить, что каждому узлу или маршрутизатору необходимо иметь как минимум один IPv4 адрес.

На основании этих требований можно определить набор префиксов адресов подсетей с диапазоном допустимых адресов для каждого префикса подсети. Также подсети не должны иметь одинаковое количество узлов, так как большинство IPv4 сетей включают разные размеры подсетей.

Определение значений средних диапазонов подсетей

Маска сообщает конечным системам сети, какие именно биты IP-адреса следует интерпретировать как идентификатор сети. Такие биты называются расширенным сетевым префиксом. Общепринятым и самым распространенным представлением масок подсетей является представление префиксов сети или представлением бесклассовой междоменной маршрутизации CIDR (Classes Inter Domain Routing), т.е. представление с косыми чертами. Помимо этого

представления, вы также можете увидеть маски подсети в форме 32-битового представления с разделительными точками в десятеричной или в двоичной системах счисления. Например, маска подсети /16 в представлении с разделительными точками выглядит 255.255.0.0. Но маски подсети не всегда делятся на 8, так что для их интерпретации вначале вам нужно будет преобразовать представление с косыми чертами в двоичный формат.

Рассмотрим живой пример. Есть IPv4 адрес 192.168.207.47/22 с маской подсети, соответственно, /22. Нам нужно преобразовать маску подсети в представление с разделительными точками в десятеричную систему счисления и определить сетевой адрес узла. Для начала попробуем преобразовать маску подсети из представления с косой чертой в двоичный формат, затем узнаем десятеричное значение маски подсети, после этого определим адрес узла.

Для того чтобы быстро определить маску подсети, выполните следующие действия:

1. Разделите длину префикса, в нашем случае 22, как сумму из четырех цифр с последующим вычитанием из 8. В нашем примере получится 8+8+6+0;
2. Запишите слева направо единицы, где количество единиц будет соответствовать цифре в десятичной системе счисления: 11111111 11111111 11111100 00000000;
3. Преобразуйте маску подсети из двоичной системы счисления в десятеричную. Получится следующее: 255.255.252.0.

Для того чтобы быстро определить адрес узла, выполните следующие действия:

1. Запишите IPv4 адрес и полученные значения суммы длины маски подсети в таблицу с тремя строками и четырьмя колонками следующие образом:

192	168	207	47
8	8	6	0

2. Не меняем значения третьей строки для столбцов, в которых присутствуют цифры 8 и записываем значение 0 в третьей строке для тех столбцов, где во второй строке указан 0. Получится следующее:

192	168	207	47

3. Для октета, в котором значение не равняется 8 или 0, преобразовываем оба числа в двоичную систему счисления и выполняем вычитание. В нашем примере нужно преобразовать числа 207 и 6 в двоичный формат и отнять от 207 число 6. Преобразовываем число 207 в двоичную систему счисления, получается 128+64+8+4+2+1, что в двоичной системе счисления выглядит 11001111. Теперь вычитаем из получившегося октета 6 цифр и получаем значение 11001100, что равняется 204.

В итоге адресом сети для IPv4-адреса 192.168.207.47/22 будет 192.168.204.0/22, где маска подсети в представлении с разделительными точками выглядит 255.255.252.0

Для того чтобы постоянно не высчитывать представления масок подсетей, можно составить таблицу соответствия для всех вариантов записей масок через косую черту, двоичным значением записи и десятичных значений с разделенными точками. Однако гораздо важнее понимать принцип данного пересчета.

Количество адресов в подсетях

Используя число битов префикса подсети, вы можете определить максимальное количество подсетей, на которые можно разбить существующую подсеть, а также количество адресов, которые можно присвоить для существующей подсети. Обычно в организациях используют как общественные, так и частные адреса, и организации, которым необходимо иметь более одного публичного адреса приходится приобретать у Интернет-провайдера публичные адреса в виде блока. Блоком адресов называется готовая группа индивидуальных IP-адресов использующих один идентификатор сети и его размер определяется маской подсети.

Перед тем как начать определять число адресов или, иначе говоря, **емкость узла адресного блока**, которые можно назначать маршрутизаторам, компьютерам и прочим устройствам нужно запомнить несколько моментов: в адресном блоке первый адрес в блоке обязательно должен быть зарезервирован для адреса сети (адрес, состоящий из нулей), а последний – для широковещательного сетевого адреса (адрес, состоящие из единиц). Широковещательный адрес —

это условный (не присвоенный никакому устройству в сети) адрес, который используется для передачи широковещательных пакетов в компьютерных сетях. Также нужно запомнить, что блок /24 всегда состоит из 256 адресов и для определения количества адресов нужно в другой подсети разделить или умножить на два значения 256 относительно этой маски подсети. Соответственно, сеть /23 содержит 512 адресов, а сеть /25 – 128 адресов.

Для примера возьмем подсеть 255.255.192.0. Для того чтобы определить емкость узла адресного блока, выполним следующие действия:

1. Определим представление маски подсети с использованием косой черты. Значение данной маски подсети /18
2. Определим количество адресов в блоке. Для этого умножим значение 256 шесть раз на два. Соответственно, получим 16384 адреса в данном блоке;
3. Определим емкость узла адресного блока, отняв от полученного значения два адреса - адрес сети и широковещательный адрес, и получим 16382.

Помимо этого, во многих крупных организациях, для повышения уровня безопасности сети путем ограничения неавторизованного трафика и упрощения администрирования принято разбивать существующую подсеть на несколько подсетей. **Разбиением на подсети** называется методика деления адресного блока путем расширения строки битов, которые используются в маске подсети.

Для примера можно взять школу, в которой на четырех этажах есть компьютерные классы с 25 компьютерами. Интернет провайдер выделил вам сеть 194.149.155.0/24, где вам нужно использовать только 100 узлов адреса, скажем, в диапазоне 194.149.155.1 – 194.149.155.254. Если вы сконфигурируете маску подсети с начальным значением 255.255.255.0, то все узлы в этом адресном пространстве будут "видеть" друг друга и принадлежать к одной подсети. Помимо этого все узлы этого адресного блока будут осуществлять коммуникации друг с другом. Если вы решите заменить существующую маску подсети маской /27, внутренние узлы будут читать адреса как адреса с разными идентификаторами сети. Для коммуникаций друг с другом адреса 194.149.155.1/27 и 194.149.155.33/27 пересылают пакеты на свои основные шлюзы, адреса которых располагаются в пределах своей подсети, причем, для коммуникаций за пределами данной организации узлы продолжат использовать маску подсети /24.

Для того чтобы определить количество логических подсетей, вы можете использовать следующую несложную формулу:

$$s=2n,$$

где s – это число подсетей, а n – количество бит в идентификаторе подсети. Для того чтобы вычислить количество битов в идентификаторе подсети, нужно воспользоваться следующей формулой:

$$n = nint – next,$$

где nint является длиной битов IDсети, предназначенной для внутреннего использования, а next, соответственно, длина исходного идентификатора сети.

В нашем случае ID сети с исходным адресным блоком равняется 24, а ID сети для внутреннего использования – 27. Соответственно, n = 27 -24 = 3, а количество подсетей будет равняться 8. Если значения масок подсети вам предоставляются в десятичном представлении, проще всего сначала перевести значение в представление с косой чертой, а затем уже просчитывать количество подсетей. В нашем случае в каждой из четырех нужных для нас подсетей (с маской подсети 255.255.255.224) можно использовать следующие блоки адресов:

194.149.155.1 – 194.149.155.30
194.149.155.33 – 194.149.155.62
194.149.155.65 – 194.149.155.94
194.149.155.97 – 194.149.155.126
194.149.155.129 – 194.149.155.158
194.149.155.161 – 194.149.155.190
194.149.155.193 – 194.149.155.222
194.149.155.225 – 194.149.155.255

Таким образом, в рамках лабораторной работы были рассмотрены основы масок подсетей, примеры конвертации представлений с косой чертой в двоичную систему счисления, а также в формат десятеричного значения с разделительными точками. Помимо этого было рассказано, как можно подсчитать количество адресов в блоках масок подсетей, а также определять число адресов,

которые можно назначать маршрутизаторам, компьютерам и прочим устройствам и разбивать существующие подсети постоянной длины (/8, /16 и /24) на подсети переменной длины.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ САМОПОДГОТОВКИ

1. Для чего используется маска подсети.
2. Какие существуют формы записей масок?
3. Опишите алгоритм, по которому можно определить адрес узла, зная Ipv4 адрес и маску.
4. Что подразумевается под понятием емкость адресного блока и как она рассчитывается?

Практическая работа №2. (2 часа)
Тема: Рабочий проект СКС
Цель работы: Научиться строить простую сеть по заданным параметрам

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы меж собой соединяются кроссоверным кабелем (рис.1).

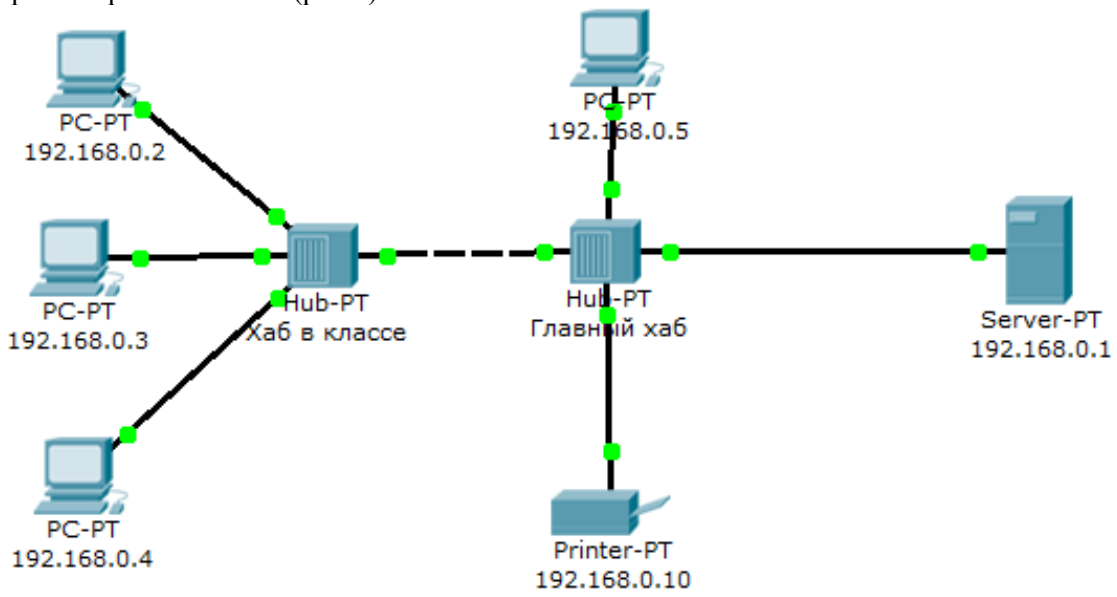


Рис.1. Схема сети.

Нужно перейти в режим симуляции (Shift+S), либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь мы видим окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но отфильтруем пока только ICMP, это исключит случайный трафик между узлами.

Для перехода к следующему событию используем кнопку "Вперёд", либо автоматика (рис.2).

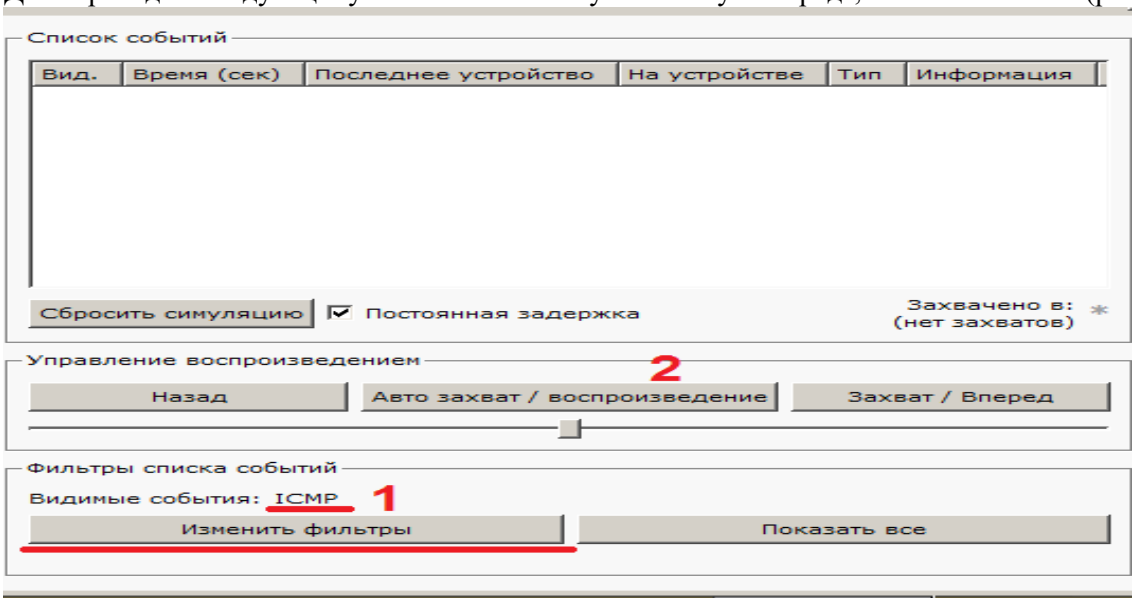


Рис2. Интерфейс симулятора.

Посылаем PING-запрос.

С одного из узлов попробуем пропинговать другой узел. Выбираем далеко расположенные узлы,

чтобы наглядней увидеть как будут проходить пакеты по сети в режиме симуляции. Итак, входим на узел .4 и пошлём пинг-запрос на узел 5.
С розового узла пингуем зелёный. На розовом узле образовался пакет (конвертик), который ждёт (иконка паузы на нём). Запустить пакет в сеть можно, нажав кнопку "Вперёд" в окне симуляции (рис.3).

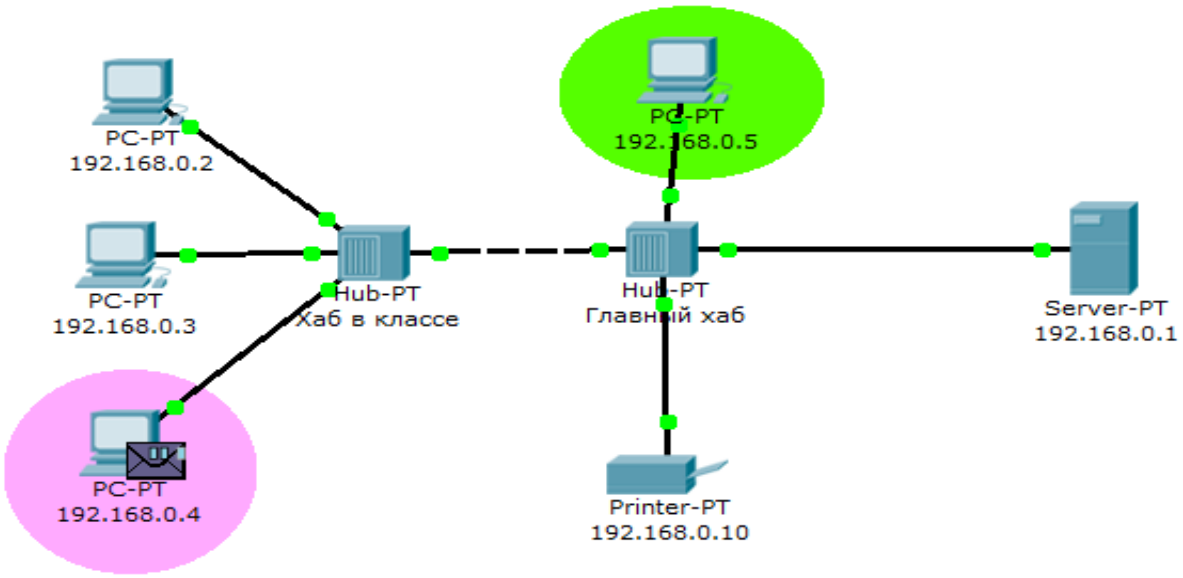


Рис. 3. Демонстрация работы симулятора.
Так же в окне симуляции мы увидим этот пакет, отметив его тип (ICMP) и источник (192.168.0.4) – рис. 4.

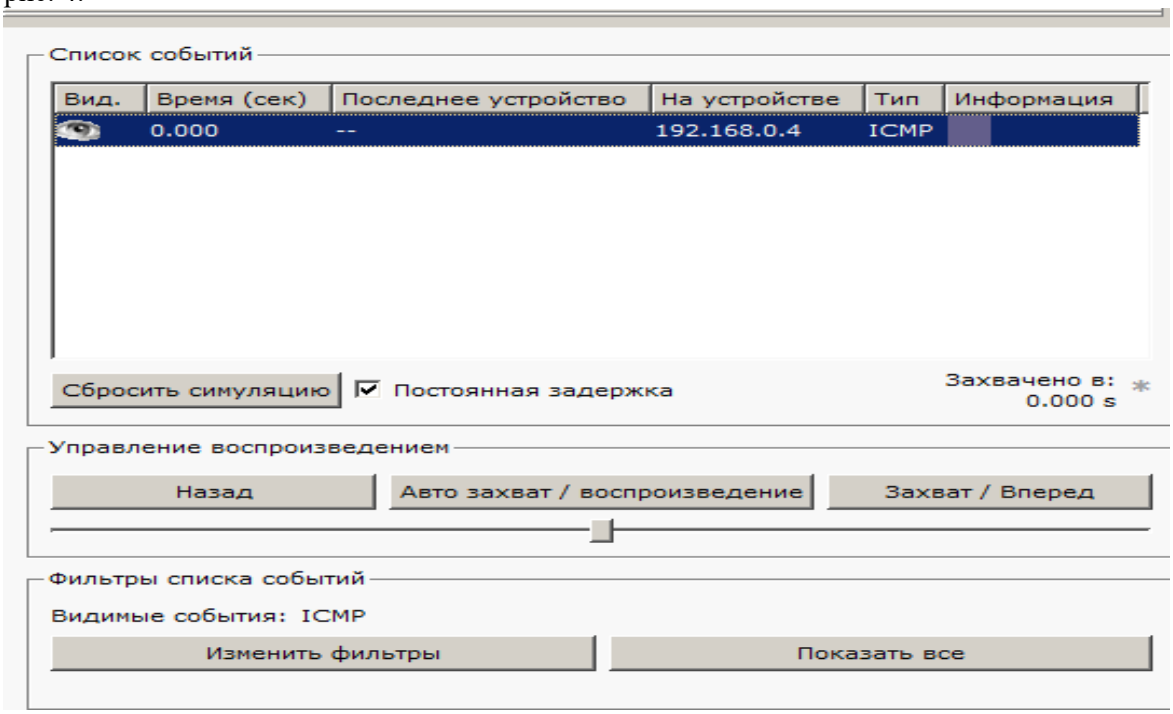


Рис. 4. Мониторинг работы протоколов.
Клик на пакете покажет нам подробную информацию. При этом мы увидим модель OSI. Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рис.2.5).

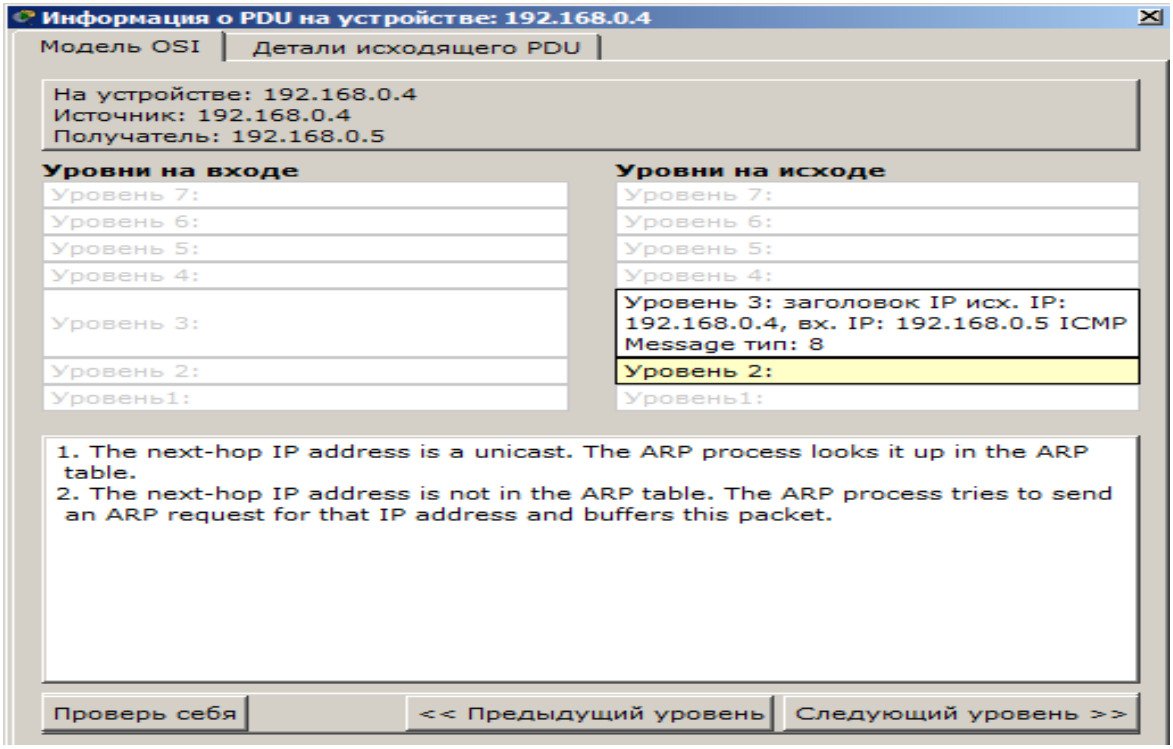


Рис. 5. Мониторинг работы на модели OSI.

А на другой вкладке можно посмотреть структуру пакета (рис.2.6).

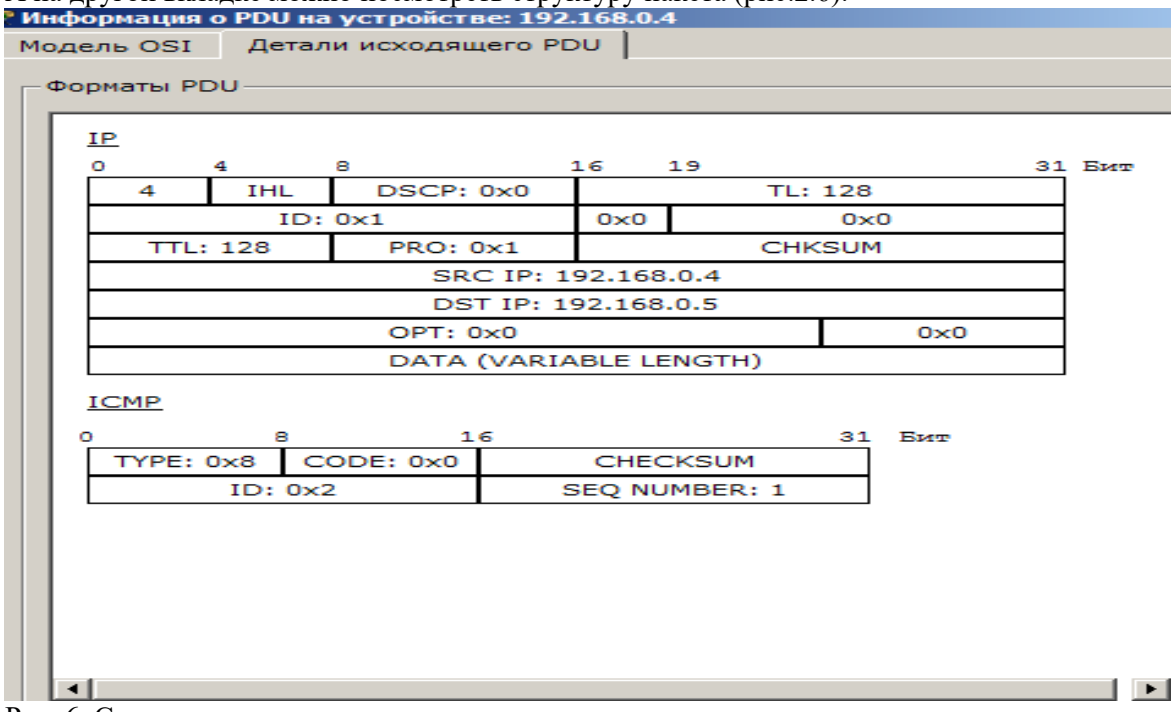


Рис. 6. Структура пакета.

Нажмём кнопку "Вперёд". И пакет тут же двинется к концентратору. Это единственное сетевое подключение с этой стороны (2.7).

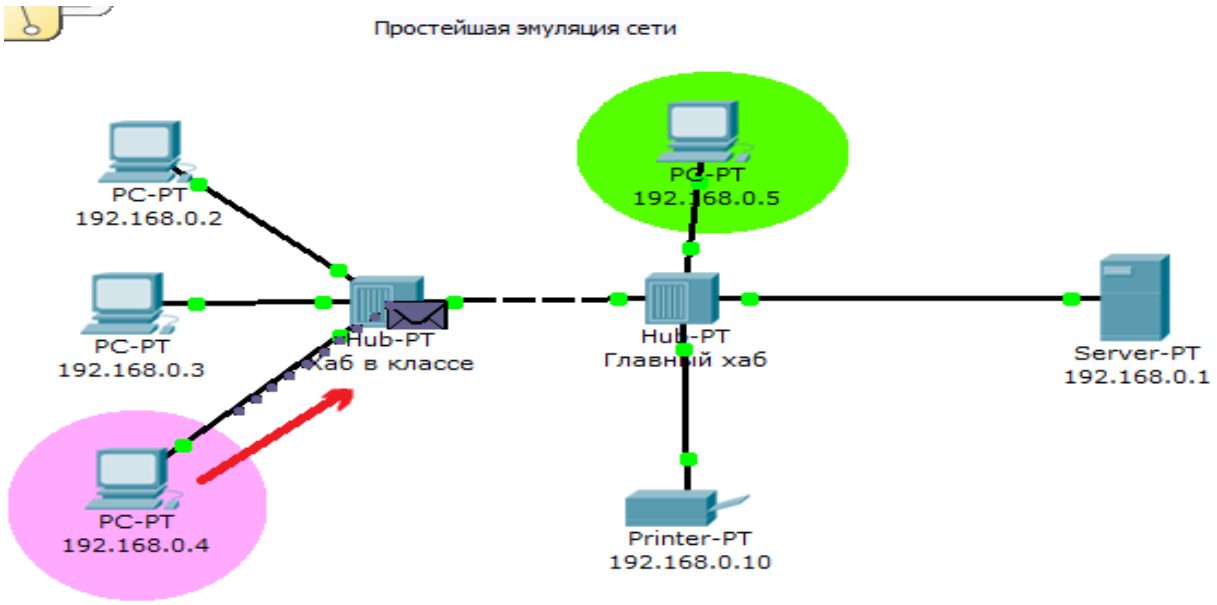


Рис. 7. Прохождение пакета. Первый этап.

Концентратор повторяет пакет на всех остальных портах в надежде, что на одном из них есть адресат (рис.2.8)

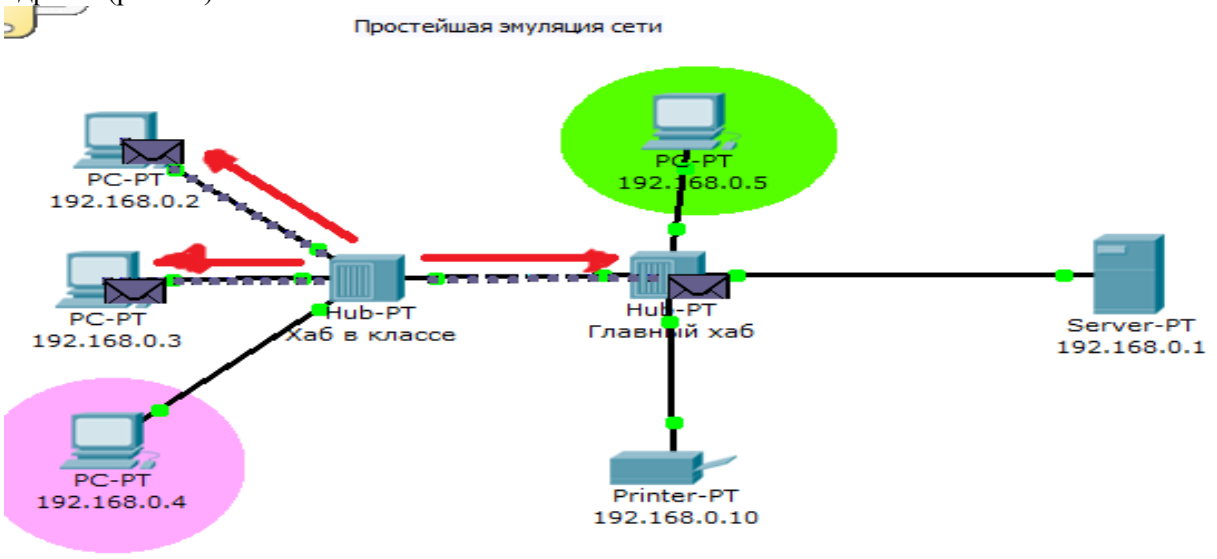


Рис. 8. Прохождение пакета. Второй этап.

Если пакеты каким-то узлам не предназначены, они игнорируют их (рис.2.9).

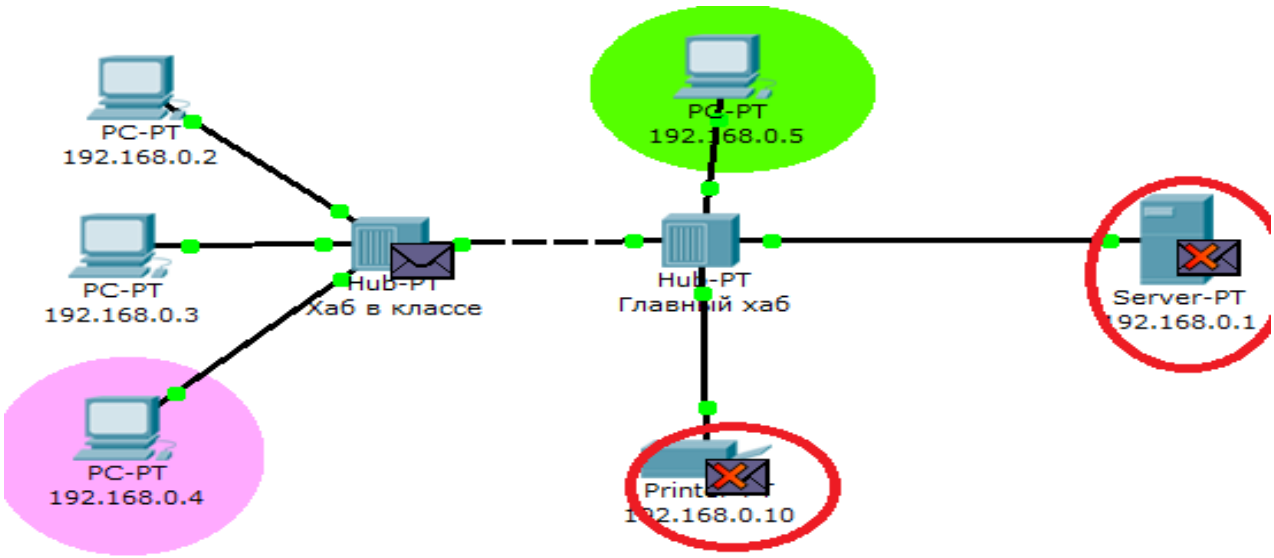


Рис. 9. Прохождение пакета. Третий этап.

Когда пакет вернётся обратно, увидим подтверждение соединения:

Контрольные вопросы.

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

Критерии оценки за практическую работу

Оценка «5» ставится, если:

• работа выполнена полностью;

• в логических рассуждениях и обоснованиях решения нет пробелов и ошибок;

• в решении нет математических ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

Оценка «4» ставится, если:

• работа выполнена полностью, но обоснования шагов решения недостаточны (если умение обосновывать рассуждения не являлось специальным объектом проверки);

• допущена одна ошибка или два-три недочета в выкладках, рисунках, чертежах или графиках (если эти виды работы не являлись специальным объектом проверки).

Оценка «3» ставится, если:

• допущены более одной ошибки или более двух-трех недочетов в выкладках, чертежах или графиках, но учащийся владеет обязательными умениями по проверяемой теме

Оценка «2» ставится, если допущены существенные ошибки, показавшие, что учащийся не владеет обязательными умениями по данной теме в полной мере.

Список источников и литературы

Основные печатные издания

1. Лифиц, И.М. Стандартизация, метрология и подтверждение соответствия: учебник и практику для среднего профессионального образования / И.М. Лифиц. – 14-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2021. – 423 с. – (Профессиональное образование)

2. Шишмарёв, В.Ю. Метрология, стандартизация, сертификация и техническое регулирование: учебник для студ. Учреждений сред. проф. образования / В.Ю. Шишмарёв. – 9-е изд., стер. – М.: Издательский центр «Академия», 2018. – 320 с.

Основные электронные издания

1. Золкин, А. Л., Проектирование цифровых экосистем окружающего интеллекта, сенсорных и компьютерных сетей : монография / А. Л. Золкин, В. Д. Мунистер. — Москва : Русайнс, 2022. — 147 с. — ISBN 978-5-4365-9267-1. — URL: https://book.ru/book/943754. — Текст : электронный..