

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Саратовский государственный технический университет имени
Гагарина Ю.А.»

Филиал федерального государственного бюджетного образовательного
учреждения высшего образования
«Саратовский государственный технический университет имени
Гагарина Ю.А.» в г. Петровске

УТВЕРЖДАЮ
Директор филиала СГТУ
имени Гагарина Ю.А. в г. Петровске

Е.А. Бессапошникова
«06» 06 2024 г.


МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по дисциплине
ОП.11 «Компьютерные сети»
специальности
«Информационные системы и программирование»

Методические указания рассмотрены
на заседании предметной (цикловой) комиссии
общепрофессиональных дисциплин,
профессиональных модулей специальностей
технического профиля
«14» июня 2024 года, протокол №12

Председатель ПЦК  /Ю.А. Табарова/

Петровск 2024

Пояснительная записка

Методические указания по выполнению практических работ подготовлены на основе рабочей программы учебной дисциплины ОП.11 «Компьютерные сети», разработанной на основе ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование» и соответствующих общих (ОК) и профессиональных (ПК) 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 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 09 - Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 4.1. Осуществлять установку, настройку и обслуживание программного обеспечения компьютерных систем.

ПК 4.3. Выполнять работы по модификации отдельных компонент программного обеспечения в соответствии с потребностями заказчика.

ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

ПК 6.1. Разрабатывать техническое задание на сопровождение информационной системы.

ПК 6.5. Осуществлять техническое сопровождение, обновление и восстановление данных информационной системы в соответствии с техническим заданием.

ПК 7.1. Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов.

ПК 7.2. Осуществлять администрирование отдельных компонент серверов.

ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов.

ПК 9.4. Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием.

ПК 9.6. Размещать веб-приложения в сети в соответствии с техническим заданием.

ПК 9.10. Реализовывать мероприятия по продвижению веб-приложений в информационно-телекоммуникационной сети "Интернет".

При выполнении практических работ студент должен **знать**:

- основные понятия компьютерных сетей: типы, топологии, методы доступа к среде передачи;
 - аппаратные компоненты компьютерных сетей;
 - принципы пакетной передачи данных;
 - понятие сетевой модели;
 - сетевую модель OSI и другие сетевые модели;
 - протоколы: основные понятия, принципы взаимодействия, различия и особенности распространенных протоколов, установка протоколов в операционных системах;
 - адресацию в сетях, организацию межсетевого воздействия.
- При выполнении практических работ студент должен **уметь:**
- организовывать и конфигурировать компьютерные сети;
 - строить и анализировать модели компьютерных сетей;
 - эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач;
 - выполнять схемы и чертежи по специальности с использованием прикладных программных средств;
 - работать с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP, IPX/SPX и т.д.);
 - устанавливать и настраивать параметры протоколов;
 - проверять правильность передачи данных;
 - обнаруживать и устранять ошибки при передаче данных.

Содержание практических занятий определено рабочей программой и тематическим планированием, соответствует теоретическому материалу изучаемых разделов учебной дисциплины.

Объем практических занятий по дисциплине определяется учебным планом по данной специальности.

Продолжительность практического занятия – 2 академических часа. Перед проведением практического занятия преподавателем организуется инструктаж, а по его окончании – обсуждение итогов.

Комплект методических указаний по выполнению практических работ по дисциплине ОП.11 «Компьютерные сети» содержит 9 практических занятий.

**Перечень практических работ
по дисциплине ОП.11 «Компьютерные сети»**

ПРАКТИЧЕСКАЯ РАБОТА № 1.

Тема: Построение схемы компьютерной сети

ПРАКТИЧЕСКАЯ РАБОТА № 2.

Тема: Построение одноранговой сети

ПРАКТИЧЕСКАЯ РАБОТА № 3.

Тема: Работа в локальной сети

ПРАКТИЧЕСКАЯ РАБОТА № 4.

Тема: Настройка протоколов TCP/IP в операционных системах.

ПРАКТИЧЕСКАЯ РАБОТА № 5.

Тема: Работа с диагностическими утилитами протокола TCP/IP.

ПРАКТИЧЕСКАЯ РАБОТА № 6.

Тема: Решение проблем с TCP/IP.

ПРАКТИЧЕСКАЯ РАБОТА № 7.

Тема: Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети

ПРАКТИЧЕСКАЯ РАБОТА № 8.

Тема: Монтаж кабельных сред технологий Ethernet.

ПРАКТИЧЕСКАЯ РАБОТА № 9.

Тема: Настройка удаленного доступа к компьютеру

ИНСТРУКЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

Прежде чем приступить к выполнению заданий, внимательно прочитайте данные рекомендации. Практические работы включают в себя задания следующих видов.

1. Работа за компьютером

В ходе выполнения практических работ студент должен:

- выполнять требования по охране труда
- соблюдать инструкцию по правилам и мерам безопасности в кабинете информационных технологий
- строго выполнять весь объем работы, указанный в задании
- соблюдать требования эксплуатации компьютерной техники (правила включения и выключения)
- предоставить отчет о проделанной работе по окончании выполненной работы, который должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.
4. Вывод о проделанной работе.

Текст отчета по практической работе должен быть набран на компьютере шрифтом Times New Roman размером 14 пт. (при оформлении текста используется текстовый редактор MS Word). Шрифт, используемый в иллюстративном материале (таблицы и рисунки), рекомендуется уменьшить до 12 пт. Межстрочный интервал в основном тексте - полуторный. В иллюстративном материале межстрочный интервал рекомендуется сделать одинарным. Поля страницы должны быть: левое поле - 30 мм; правое поле – 15 мм; верхнее и нижнее поле - 20 мм.

Каждый абзац должен начинаться с красной строки. Отступ абзаца – 1,25 см от левой границы текста.

Студент должен выполнить практическую работу самостоятельно (или в группе, если это предусмотрено заданием). Практическая работа выполняется согласно заданию и методическим рекомендациям. После выполнения практической работы обучающийся самостоятельно себя контролирует путем ответов на вопросы. Результат работы представляется преподавателю в виде файла (файлов) в личном каталоге, защищается обучающимися.

По ходу выполнения работы при возникновении вопросов обучающийся может получить консультацию у преподавателя или самостоятельно воспользоваться лекционным материалом, рекомендуемой литературой.

2. Поиск информации в сети – использование web-браузеров, баз данных, пользование информационно-поисковыми и информационно-справочными системами, автоматизированными библиотечными системами, электронными журналами. Поиск и обработка информации включает подготовку фрагмента практического занятия.

ПРАКТИЧЕСКАЯ РАБОТА № 1

Тема: Построение схемы компьютерной сети

Цель работы: научиться создавать схемы сетей с помощью программ 10-Strike LANState, EDraw Network Diagrammer.

Оборудование: ПК, программное обеспечение – 10-Strike LANState, EDraw Network Diagrammer, инструкции по выполнению работы.

Справочный материал:

Программа 10-Strike LANState , позволяет осуществлять мониторинг сетевых служб и устройств, устранять неполадки в их работе, и сокращать простои. Внезапные сбои в работе ответственных служб и протоколов сервера или активного сетевого оборудования часто оборачивается для компании немалыми убытками и подорванным доверием клиентов. В обязанности системного администратора входит задача своевременного обнаружения таких неполадок и их быстрого устранения. Но справиться с этой задачей без специальных программных инструментов подчас очень нелегко, и, можно сказать, невозможно. Решением проблемы автоматического мониторинга сети является программа 10-Strike LANState. Из под ее контроля не уйдет ни один сбой в работе сетевой службы или протокола. Программа вовремя обнаружит неполадку и сообщит о ней системному администратору.

В основе работы программы лежит механизм периодического выполнения заданных проверок контролируемых служб и протоколов на серверах и другом сетевом оборудовании. О результате проверок системный администратор оповещается несколькими альтернативными способами: электронной почтой, SMS, звуковым сигналом. Кроме этого, программой ведется фиксация всех событий в журналах с подробной расшифровкой неполадок и временем их происхождения.

10-Strike LANState обладает возможностями мониторинга работы серверов баз данных, систем управления базами данных, значений некоторых параметров производительности сетевого оборудования (например, трафик на коммутаторах), а также оперативного доведения информации до системного администратора о достижении критических значений этих параметров. Для устранения неполадок программа может автоматически выполнить заданные администратором действия: перезагрузку служб и компьютеров, запустить программу или скрипт. Кроме этого, отличительной особенностью 10-Strike LANState является то, что она наглядно отображает контролируемые устройства в виде графической карты сети со связями и условными обозначениями.

Системный администратор будет оповещен о фактах установки пользователями новых программ и удаления старых.

При проектировании сетей иногда используется **EDraw Network Diagrammer** – программа создания диаграмм сети с большим количеством примеров и шаблонов.

Основные диаграммы:

1. Топологические схемы сети
2. Проектирование сетей Cisco

3. Диаграммы кабельных сетей
4. Диаграммы LAN (локальная компьютерная сеть)
5. Диаграммы сетей WAN (глобальная сеть)

Сетевая диаграмма (граф сети) - графическое отображение работ проекта сети и их взаимосвязей. Отличием от блок-схемы является то, что сетевая диаграмма моделирует только логические зависимости между элементарными работами. Она не отображает входы, процессы и выходы.

Программа имеет как сходство с программой 10 Страйк: Схема Сети, так и принципиальные отличия. Например, в ней можно нарисовать не только изображение сети, но и изображение помещения, где эту сеть планируется установить.

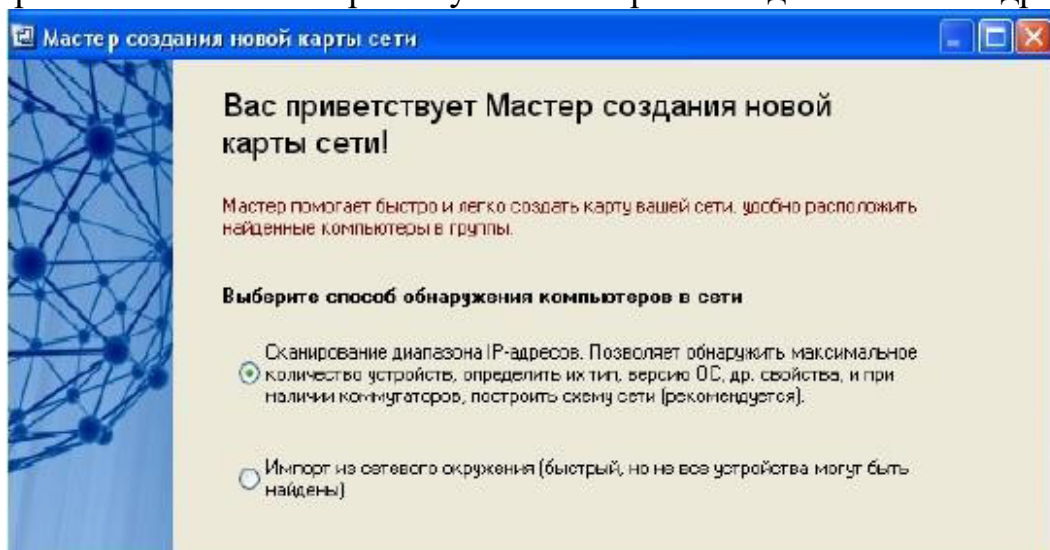
Содержание работы:

Задание 1. Построение схемы сети

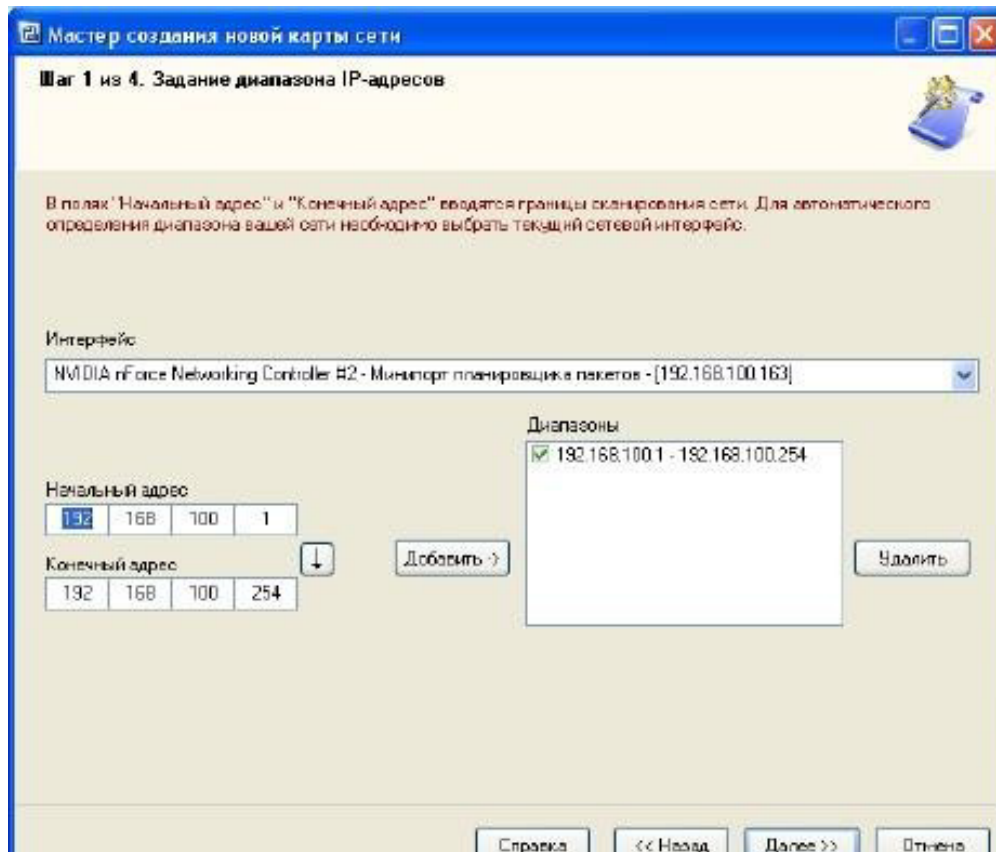
1. Запустите программу LANState
2. Создание схемы сети автоматически

Задание. Построить схему сети автоматически:

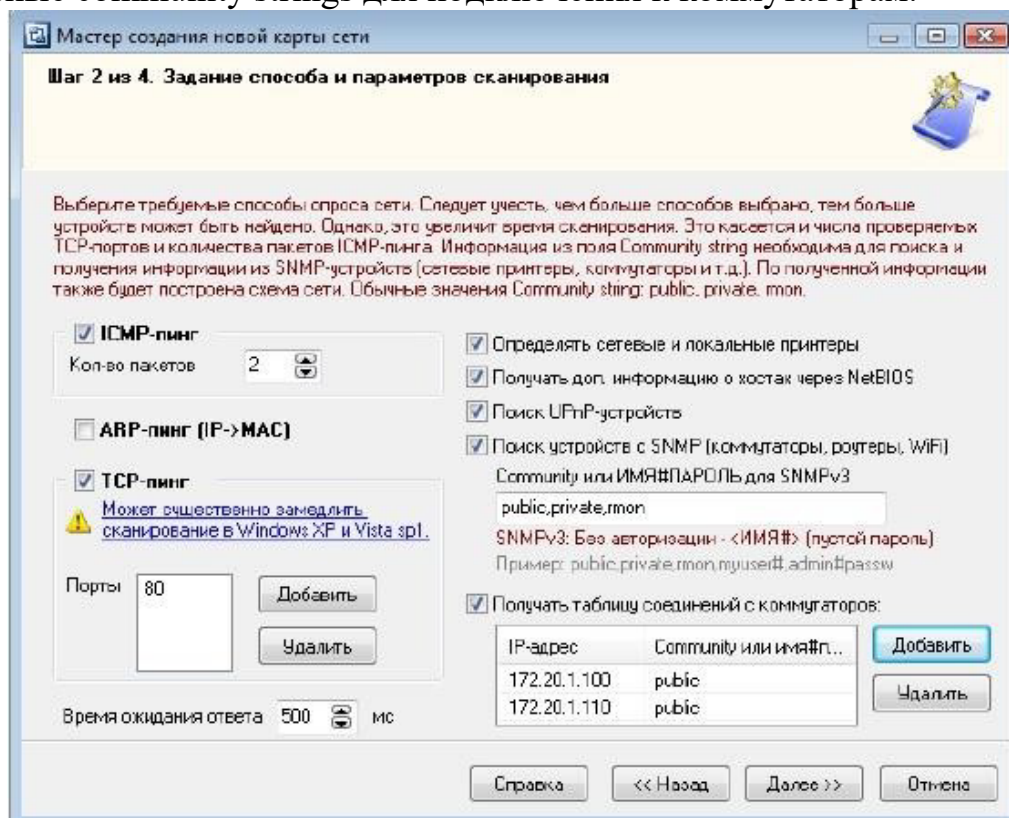
1. SNMP должен быть включен на коммутаторах. Программа должна быть разрешена в брандмауэре для успешной работы по протоколу SNMP.
2. Запустите Мастер Создания Карты Сети (Файл – Мастер создания карты).
3. В открывшемся окне выберите пункт Сканирование диапазона IP-адресов



4. Выберите сканирование сети по диапазону IP-адресов. Укажите диапазоны (от 192.168.1.1 до 192.168.1.254) Устройства с SNMP должны находиться внутри указанных диапазонов.



5. Выберите методы сканирования и настройте их параметры. Не забудьте поставить галочку рядом с опцией "Поиск устройств с SNMP..." и укажите правильные community strings для подключения к коммутаторам.



6. После сканирования программа должна нарисовать схему сети. Если сканирование SNMP прошло успешно, соединения между сетевыми

[illegible]

Задание 2. Построение диаграмм сети

1. Для выбора компьютеров и мониторов из библиотеки (Libraries) нужно выбрать команду **Network – Basic Network Diagram**, затем вкладки **Computers and Monitors** и **Server**, а для выбора кабелей – вкладку **Network and Peripherals**.

Б) Нарисуйте схему расположения компьютеров по топологиям «звезда», «кольцо».

В) В программе EDraw Network Diagrammer повторите схему, показанную на рис.2. Поясните, что за устройства присутствуют в данной сети и как они работают.

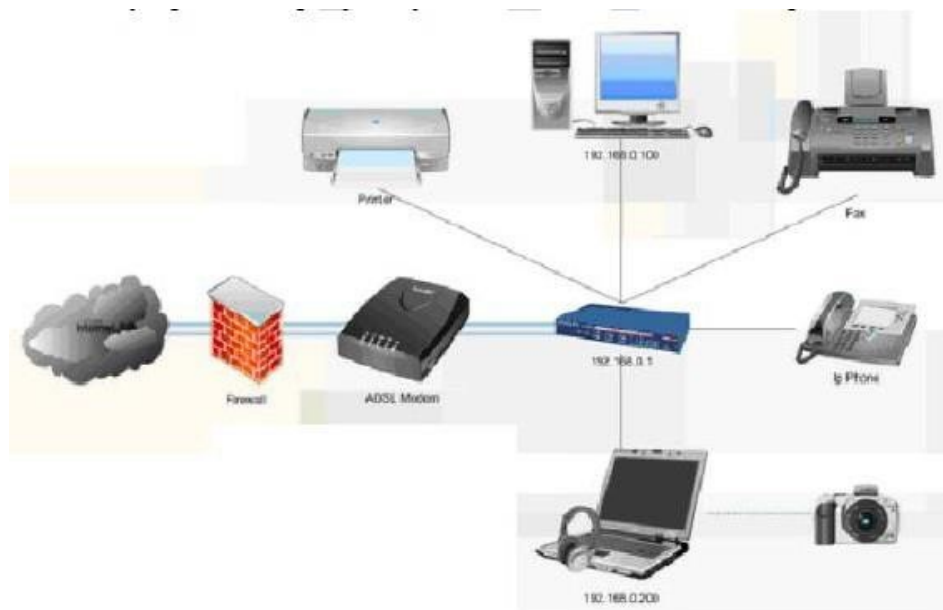


Рис 2. Схема сети небольшого офиса

Г) Используя возможности программы EDraw Network Diagrammer создайте схему помещения и расположения компьютерной техники в кабинете.

ПРАКТИЧЕСКАЯ РАБОТА № 2

Тема: Построение одноранговой сети

Цель работы: освоение умений по построению одноранговой локальной вычислительной сети

Оборудование (на 1 рабочее место): рабочая станция - 2 шт.; коммутатор DES-1100-16 1 шт.; витая пара – 2 шт. по 1м; комплект для обжима кабеля; сетевой тестер; разъемы RG – 45 - 4 шт., инструкции по выполнению работы.

Содержание работы:

1. Выполните практические задания 1, 2, делая промежуточные записи в карте - отчете.
2. Результаты выполнения каждого практического задания продемонстрируйте преподавателю.
3. После контроля выполнения последнего практического задания, восстановите исходные сетевые параметры на своем рабочем компьютере и проверьте работоспособность локальной и глобальной сети.
4. Приведите рабочее место в порядок.

Задание 1: Обожмите 2 отрезка UTP – кабеля с обеих сторон по стандарту EIA/TIA-568A или EIA/TIA-568B (прямой кабель).

Методические рекомендации: Вставляя проводники в разъем, следите за тем, чтобы они доходили до конца разъема, а внешняя изоляция кабеля выходила за фиксирующую защелку. Для проверки правильности обжима используйте сетевой тестер.

Инструкция по обжиму витой пары:

Для обжимки кабеля понадобится:

1. Кабель типа витая пара



2. Коннекторы RJ-45. Также для увеличения влаго- и пылезащиты контактной площадки коннектора можно использовать специальный пластиковый колпачок (но не обязательно):



3. Обжимной инструмент (его еще называют обжимные клещи или *кримпер*):



Внешний вид инструмента может отличаться лишь некоторыми деталями, но, как правило, с его помощью можно производить обжим, используя сетевой коннектор RJ-45 и телефонный коннектор RJ-11. Кроме того, в нем имеется площадка с резаками, с помощью которых можно обрезать кабель.

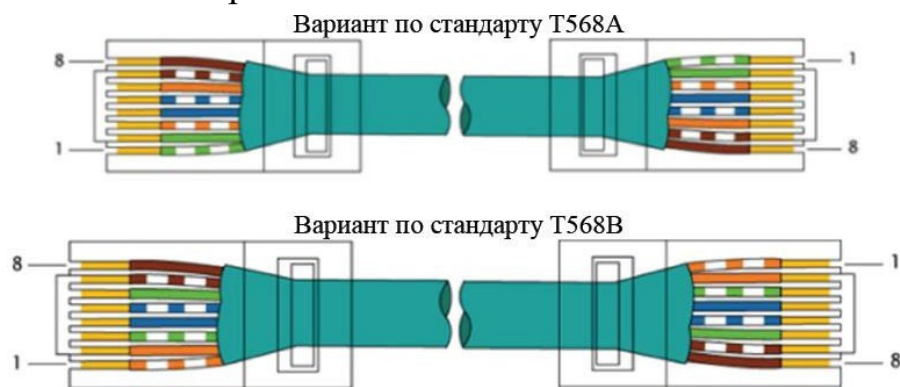
4. Инструмент для снятия внешней изоляции – *stripper*. Иметь его, конечно, желательно, но не обязательно, т.к. в большинстве кримперов уже есть встроенное лезвие для снятия изоляции:



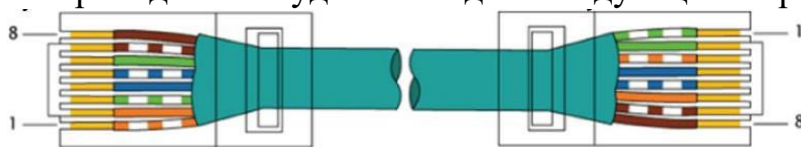
Теперь нам нужно определиться со схемой обжима. Существует два варианта обжима коннектора на кабеле “витая пара”:

- для создания прямого кабеля – используется для соединения компьютера с коммутатором;
- для создания перекрёстного кабеля (называемого *кроссовер*) – используется для соединения двух компьютеров напрямую без коммутатора, а также для соединения между собой некоторых старых моделей коммутаторов.

При создании *прямого* кабеля развести цвета по парам можно в соответствии с двумя стандартами: EIA/TIA-568A или EIA/TIA-568B. Оба эти стандарта используются при обжиге витой пары для соединения компьютера и коммутатора и абсолютно равнозначны.



При создании *перекрёстного* кабеля (*crossover*) цветовая последовательность проводников будет выглядеть следующим образом:

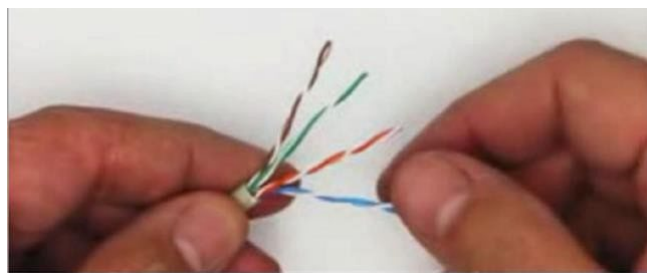


Необходимо выполнить следующую последовательность действий:

1. Аккуратно обрежьте конец кабеля. При этом лучше всего пользоваться резакон, встроенным в обжимные клещи.
2. Снимите с кабеля изоляцию. Это можно сделать с помощью все того же обжимного инструмента, либо с помощью стриппера:

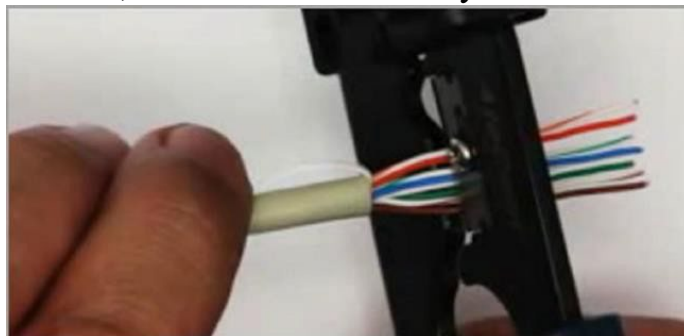


3. Разведите и расплетите проводки:

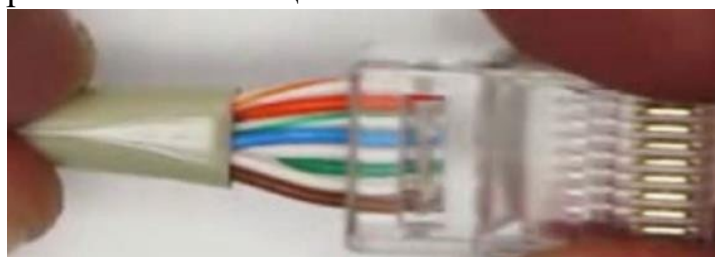


Затем выровняйте их в один ряд, при этом соблюдая цветовую последовательность. Вам необходимо разложить провода по цветам в соответствии с выбранным стандартом EIA/TIA-568A или EIA/TIA-568B

4. Обкусите проводки так, чтобы их осталось чуть больше сантиметра:



5. Вставьте проводки в разъем RJ-45. Помните, что коннектор вы должны расположить отверстием вниз и защелкой от себя:



6. Проверьте, правильно ли вы расположили проводки.

7. Убедитесь, чтобы все провода полностью вошли в разъем и уперлись в его переднюю стенку.

8. Поместите коннектор с установленной парой в обжимные клещи, затем плавно, но сильно произведите обжим:



На этом обжатие кабеля “витая пара” закончено.

Задание 2: Создайте подключение типа «компьютер-компьютер».

Методические рекомендации: Проверьте наличие физического соединения между компьютерами по индикации светодиодов на сетевых адаптерах ПК1 и ПК2. Перед тем как изменить параметры IP– адресации, запишите в тетрадь все сетевые параметры, установленные на вашем

компьютере(IP – адрес, маску подсети, основной шлюз) для последующего их восстановления. Осуществите настройку сетевых параметров и проверьте наличие соединения между ПК 1 и ПК 2.

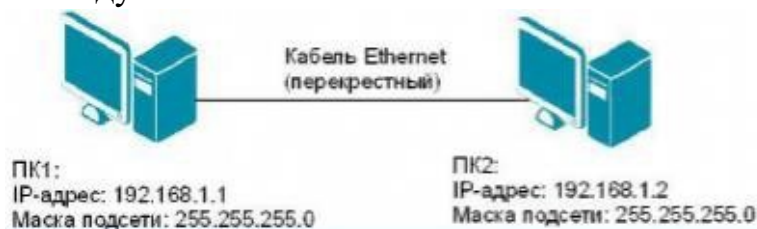


Рисунок 1 - Схема подключения типа «компьютер-компьютер»

1. Подключите ПК1 и ПК2 в соответствии со схемой прямым Ethernet -ткабелем (прямой кабель). (рис. 1).

2. Настройте статический IP-адрес на рабочих станциях ПК1 и ПК2.

Откройте Сетевые подключения (прямой кабель). Пуск - Панель управления - Сетевые подключения);

В контекстном меню пункта Подключение по локальной сети выберите Свойства;

В диалоговом окне выберите Протокол Интернета (TCP/IP) и нажмите Свойства;

Выберите Использовать следующий IP-адрес (см. рис. 2);

2.5 Задайте новые IP – адрес и маску подсети для ПК1или ПК 2 (см. рис. 1).

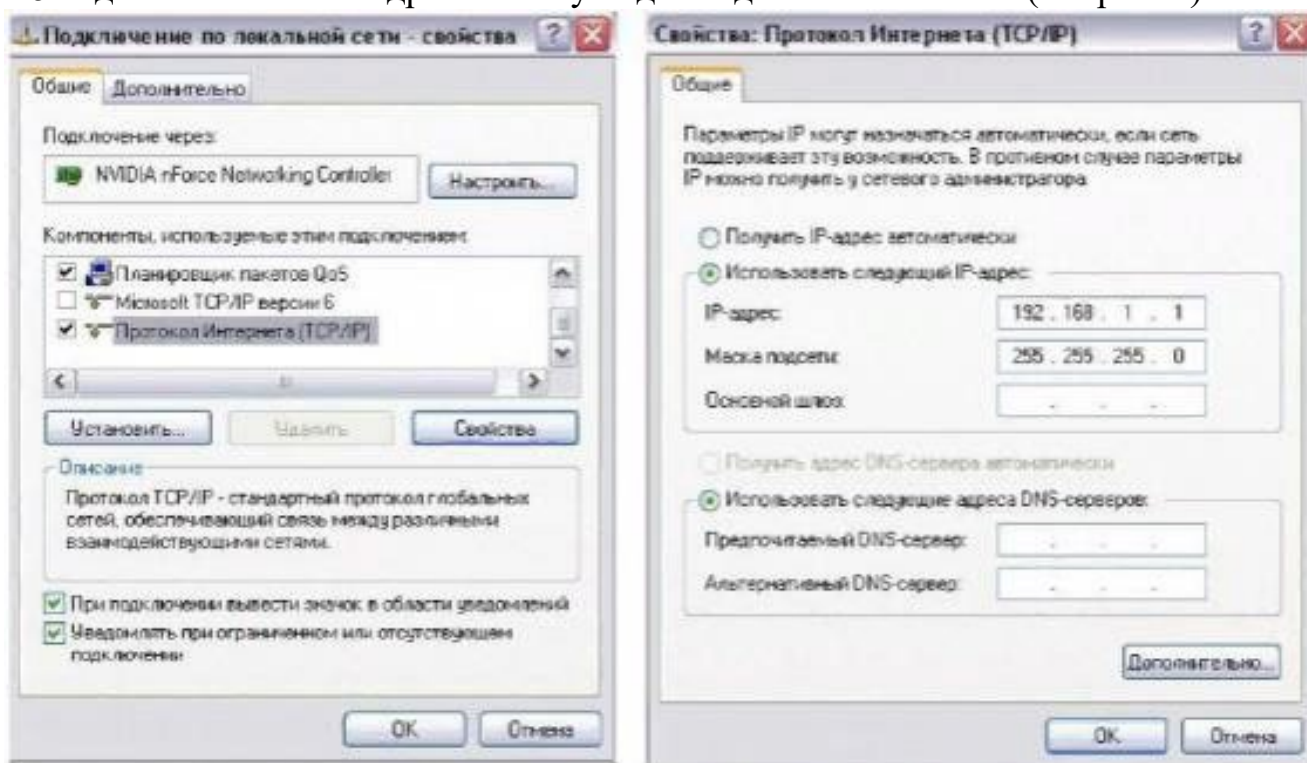


Рисунок 2 - Настройка статического IP-адреса

3. Проверьте конфигурацию сетевого адаптера ПК1 (или ПК 2) с помощью команды ipconfig.

4. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2 с помощью команды ping.

ПРАКТИЧЕСКАЯ РАБОТА № 3

Тема: Работа в локальной сети

Цель работы: Научиться работать в локальной компьютерной сети – создавать и использовать сетевые папки, подключать сетевой принтер и печатать на нём, устанавливать права доступа к ресурсам и предоставлять другим пользователям доступ к ресурсам своего компьютера, осуществлять поиск файлов в сети, ознакомиться с аппаратным обеспечением сети, с возможностями локальной сети.

Оборудование: ПК, программное обеспечение – операционная система Windows 7, инструкции по выполнению работы.

Содержание работы:

Задание 1. Работа в локальной сети

1. С разрешения преподавателя включите компьютер, дождитесь завершения загрузки операционной системы Windows 7.
2. Найдите в вашей сети сетевой адаптер, концентратор (HUB или Switch), модем, волоконно-оптический приёмопередатчик, Wi-Fi-роутер, интернет-сервер, файловый сервер, выделенный сервер, рабочую станцию (покажите преподавателю, что вы нашли).
3. Поместите на «Рабочий стол» значок «Сеть» (если его там нет), выполните двойной щелчок по этому значку и ознакомьтесь с содержимым вашей локальной компьютерной сети. Попробуйте определить, какая у вас локальная сеть (по способу взаимодействия компьютеров) – одноранговая или сеть с выделенным сервером?

Сделайте **Screenshot** (копию экрана) окна «Сетевое окружение» и вставьте его в ваш отчёт.

4. Открывая в окне «Сетевое окружение» папки подключенных к сети ПК, определите, какие ресурсы они предоставляют в совместное использование. Сделайте **Screenshot** окон 2-х папок и вставьте их в ваш отчёт.
5. Выясните, куда входят компьютеры (рабочая группа, домен), определите название рабочей группы или домена, определите имя своего компьютера. Запишите результаты в отчёт.

Свойства папки «Компьютер» - Имя компьютера.

6. Определите, есть ли на вашем компьютере сетевые диски и сетевые принтеры.

- **Сетевые диски** — это диски другого компьютера сети, которые данный компьютер воспринимает как своё дополнительное внешнее устройство.

- **Сетевые принтеры** — это принтеры другого компьютера сети, которые данный компьютер воспринимает как свои дополнительные устройства печати.

7. Подключите к своему компьютеру сетевой принтер. Какой вид имеет значок сетевого принтера?

– Найдите в сетевом окружении компьютер преподавателя, выполните двойной щелчок мышью по нему, а затем по значку принтера. Принтер подключится автоматически.

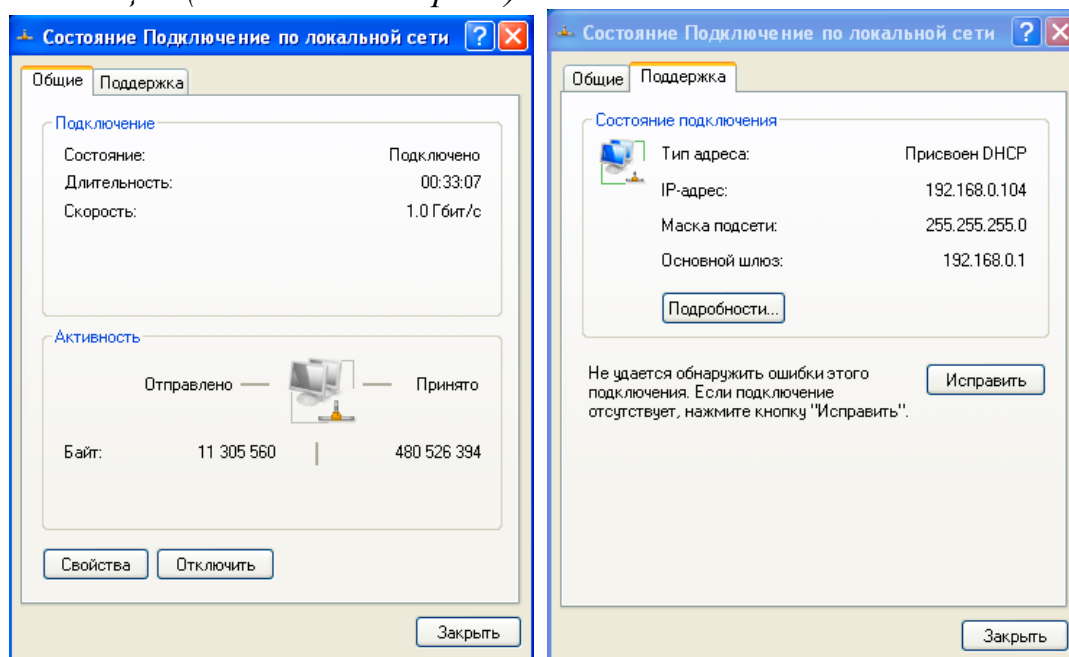
8. Создайте на сервере, в папке своей группы новую папку и назовите её своей фамилией с инициалами, например, Чумак А.А и подключите её к своему компьютеру как сетевой диск. Какой вид имеет значок сетевого диска?

Удалить сетевые диски и принтеры можно, воспользовавшись контекстным меню выбранного объекта.

9. Определите IP адрес вашего персонального компьютера.

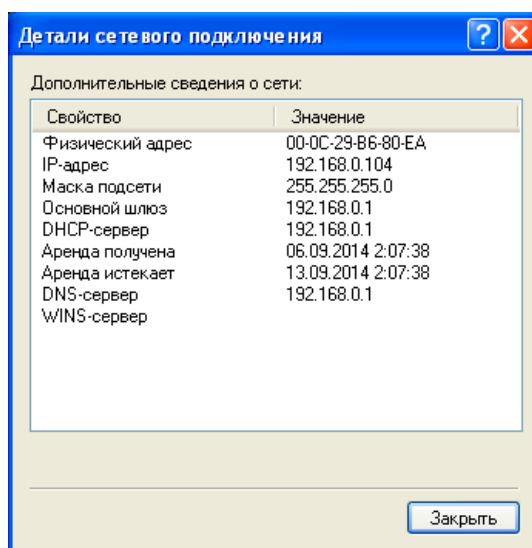
См. свойства папки Сетевое окружение - свойства параметра "Подключение по локальной сети" - свойства параметра "Протокол TCP/IP"). Результаты запишите в отчёт.

Можно выполнить двойной щелчок по значку «Сеть» на панели индикации («системный трэй»):

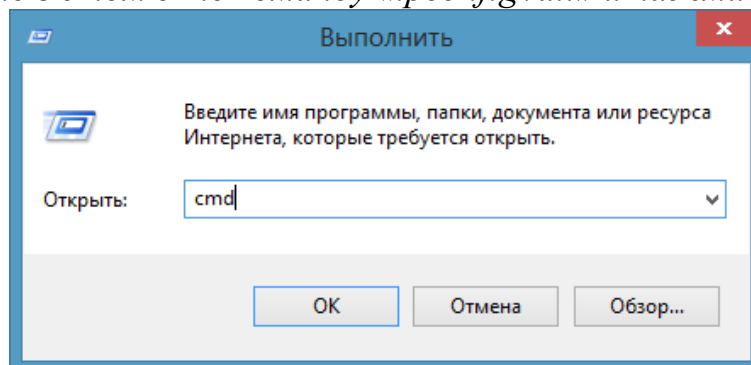


10. Определите физический адрес сетевой карты вашего компьютера

В окне «Состояние Подключение по локальной сети» нажмите кнопку «Подробности»:



Второй способ: в «Главном меню» найдите команду «Выполнить», введите «cmd». Откроется окно командного интерпретатора (режим «ДОС»). Введите в этом окне команду «ipconfig /all» и нажмите «Enter».



```
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\Igor>hostname
ivk-ultrabook

C:\Users\Igor>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : ivk-ultrabook
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Смешанный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : mytrinity.com.ua

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : mytrinity.com.ua
Описание . . . . . : Intel(R) Centrino(R) Wireless-N 2230
Физический адрес . . . . . : 84-A6-C8-D4-C1-E1
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::917f:157e:4fd9:ca9%4(Основной)
IPv4-адрес . . . . . : 192.168.0.100(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена . . . . . : 3 сентября 2014 г. 0:35:00
Срок аренды истекает . . . . . : 15 сентября 2014 г. 15:11:47
Основной шлюз . . . . . : 192.168.0.1
DHCP-сервер . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 75802312
DUID клиента DHCPv6 . . . . . : 00-01-00-01-19-FE-F0-C5-08-60-6E-04-6B-AB

DNS-серверы . . . . . : 192.168.0.1
NetBios через TCP/IP . . . . . : Включен

Ethernet adapter Ethernet:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : mshome.net
Описание . . . . . : Контроллер семейства Realtek PCIe GBE
Физический адрес . . . . . : 08-60-6E-04-6B-AB
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да
```

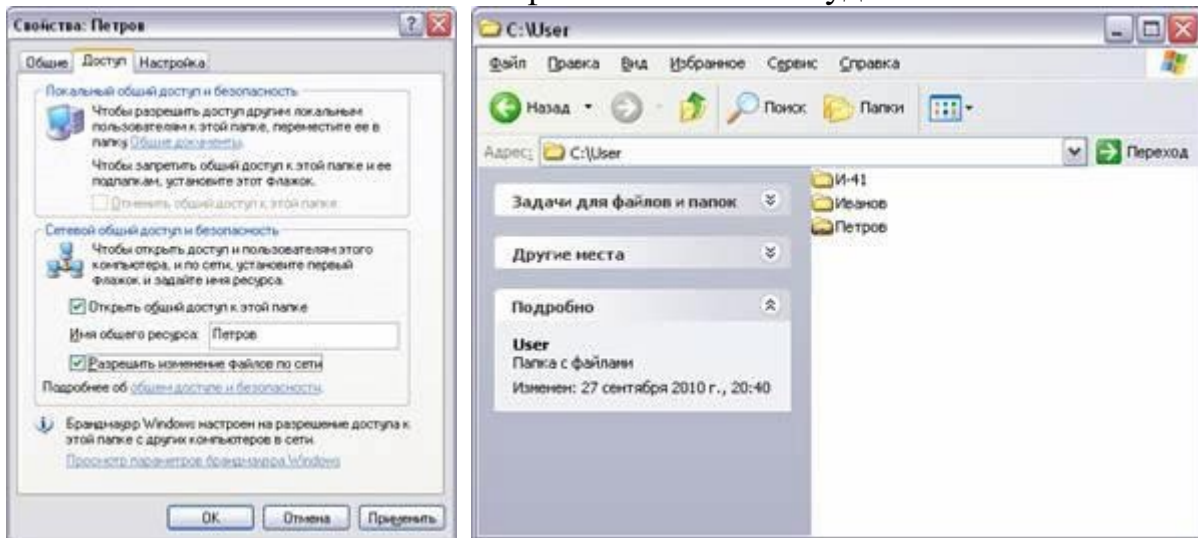
11. Предоставьте в совместное использование свои ресурсы - объявите свой каталог общим, выбрав команду «Доступ» в контекстном меню.

В папке «Мои документы» создайте каталог с именем, совпадающим с Вашей фамилией.

Задайте тип доступа Полный (команда «Разрешить изменение файлов по сети»).

Обратите внимание на изменение вида значка каталога.

Сделайте копию экрана и сохраните графический файл с этой копией в этой папке. Обменяйтесь этими файлами с кем-нибудь по сети.



12. Сохраните отчёт в своём каталоге на сервере и распечатайте его на сетевом принтере. Покажите преподавателю.

ПРАКТИЧЕСКАЯ РАБОТА № 4

Тема: Настройка протоколов TCP/IP в операционных системах

Цель работы: Изучить способы диагностики настроек стека протоколов TCP/IP; получить сведения о настройке TCP/IP для работы с DHCP-сервером.

Оборудование: компьютер, подключенный к ЛВС, программное обеспечение: ОС Windows 7; виртуальная машина (Microsoft Virtual PC) с установленной операционной системой MS Windows XP, инструкции по выполнению работы.

Справочный материал:

На концептуальной модели взаимодействия открытых систем OSI основан стек протоколов TCP/IP (Transmission Control Protocol — протокол управления передачей / Internet Protocol — Интернет-протокол), который предоставляет ряд стандартов для связи компьютеров и сетей.

Стек протоколов TCP/IP – промышленный стандарт, который позволяет организовать сеть масштаба предприятия и связывать компьютеры, работающие под управлением различных операционных систем.

Применение стека протоколов TCP/IP дает следующие преимущества:

- поддерживается почти всеми операционными системами; почти все большие сети основаны на TCP/IP;
- технология позволяет соединить разнородные системы;
- надежная, расширяемая интегрированная среда на основе модели «клиент — сервер»;
- получение доступа к ресурсам сети Интернет.

Каждый узел TCP/IP идентифицирован своим логическим IP-адресом, который идентифицирует положение компьютера в сети почти таким же способом, как номер дома идентифицирует дом на улице. Реализация TCP/IP позволяет узлу TCP/IP использовать статический IP-адрес или получить IP-адрес автоматически с помощью DHCP-сервера (Dynamic Host Configuration Protocol — протокол динамической конфигурации хоста).

Для простых сетевых конфигураций, основанных на локальных сетях (LAN, Local Area Network), он поддерживает автоматическое назначение IP-адресов.

По умолчанию компьютеры клиентов, работающие под управлением ОС Windows или Linux, получают информацию о настройке протокола TCP/IP автоматически от службы DHCP.

Однако даже в том случае, если в сети доступен DHCP-сервер, необходимо назначить статический IP-адрес для отдельных компьютеров в сети. Например, компьютеры с запущенной службой DHCP не могут быть клиентами DHCP, поэтому они должны иметь статический IP-адрес.

Если служба DHCP недоступна, можно настроить TCP/IP для использования статического IP-адреса.

Для каждой платы сетевого адаптера в компьютере, которая использует TCP/IP, можно установить IP-адрес, маску подсети и шлюз по умолчанию.

Ниже описаны параметры, которые используются при настройке статического адреса TCP/IP.

Параметр	Описание
IP-адрес	Логический 32-битный адрес, который идентифицирует TCP/IP узел. Каждой плате сетевого адаптера в компьютере с запущенным протоколом TCP/IP необходим уникальный IP-адрес, такой, как 192.168.0.108. Каждый адрес имеет две части: ID сети, который идентифицирует все узлы в одной физической сети и ID узла, который идентифицирует узел в сети. В этом примере ID сети — 192.168.0, и ID узла — 108.
Маска подсети	Подсети делят большую сеть на множество физических сетей, соединенных маршрутизаторами. Маска подсети закрывает часть IP-адреса так, чтобы TCP/IP мог отличать ID сети от ID узла. При соединении узлов TCP/IP, маска подсети определяет, где находится узел получателя: в локальной или удаленной сети. Для связи в локальной сети компьютеры должны иметь одинаковую маску подсети.
Шлюз по умолчанию	Промежуточное устройство в локальной сети, на котором хранятся сетевые идентификаторы других сетей предприятия или Интернета. TCP/IP посылает пакеты в удаленную сеть через шлюз по умолчанию (если никакой другой маршрут не настроен), который затем пересылает пакеты другим шлюзам, пока пакет не достигнет шлюза, связанного с указанным адресатом.

Если сервер с запущенной службой *DHCP* доступен в сети, он автоматически предоставляет информацию о параметрах *TCP/IP* клиентам *DHCP*.

Содержание работы:

Задание 1. Подготовьте компьютер для выполнения практической работы:

1. Запустите виртуальную машину с помощью ярлыка Microsoft Virtual PC.
2. Загрузите в виртуальный компьютер ОС Windows XP.
3. Перейдите в полноэкранный режим работы.
4. Выполняйте задания практической работы в виртуальной машине.

Задание 2. Проверьте работоспособность стека протоколов *TCP/IP*:

1. Запустите консоль (*Пуск/Программы/Стандартные/Командная строка*).
2. В командной строке введите *ipconfig /all | more*.
3. Используя приведенную ниже информацию, создайте в своей папке (со своей фамилией) текстовый документ Word со следующими данными: имя компьютера; основной DNS-суффикс; описание DNS-суффикса для подключения; физический адрес; DHCP включен; Автоконфигурация включена; IP-адрес автоконфигурации; маска подсети; шлюз по умолчанию.
4. Убедитесь в работоспособности стека *TCP/IP*, отправив эхо-запросы на IP-адреса. Для этого воспользуйтесь командой *ping*:
 - отправьте эхо-запросы на локальный адрес компьютера (*loopback*) *ping 127.0.0.1* (на экране должны появиться сообщения о полученном ответе от узла 127.0.0.1) Скриншот окна поместите в отчет работы.
 - отправьте эхо-запрос по другому IP-адресу, например 85.95.185.75. Скриншот окна поместите в отчет лабораторной работы.

Задание 3. Настройте стек протоколов *TCP/IP* для использования статического IP-адреса:

1. Откройте окно *Сетевые подключения* (*Пуск/Панель управления/ Сетевые подключения*).
2. Вызовите свойства *Подключения по локальной сети*. Для этого можно воспользоваться контекстным меню.
3. В появившемся диалоговом окне на вкладке *Общие* откройте свойства *Протокол Интернета TCP/IP*.
4. Щелкните переключатель *Использовать следующий IP-адрес* и введите в соответствующие поля данные: *IP_адрес*; *Маску подсети*; *Основной шлюз*; *Предпочитаемый DNS*.
5. Примените параметры кнопкой *ОК*.
6. Закройте окно свойств подключения кнопкой *ОК* (если потребуется, то согласитесь на перезагрузку компьютера).
7. Проверьте работоспособность стека протоколов *TCP/IP*. (пункты 2 и 3 повторить)

Задание 4. Настройте *TCP/IP* для автоматического получения IP-адреса:

1. Откройте окно *Сетевые подключения*.
2. Вызовите свойства *Подключения по локальной сети*.
3. Откройте свойства *Протокол Интернета TCP/IP*.
4. Установите переключатель *Получить IP-адрес автоматически*.
5. Закройте диалоговое окно *Свойства: Протокол Интернета TCP/IP* кнопкой *ОК*.
6. Примените параметры кнопкой *ОК*.
7. Проверьте настройку стека протоколов *TCP/IP*.
8. Получите другой адрес для своего компьютера. Для этого:
 - запустите консоль (командную строку);

- введите команду для сброса назначенных адресов *ipconfig /release*;
 - введите команду для получения нового адреса *ipconfig /renew*;
9. Проверьте работоспособность стека протоколов TCP/IP.

Контрольные вопросы:

1. Опишите параметры, используемые при настройке статического адреса TCP/IP.
2. Какие преимущества дает применение стека протоколов TCP/IP .
3. Дайте определение понятию стек протоколов TCP/IP.

ПРАКТИЧЕСКАЯ РАБОТА № 5

Тема: Работа с диагностическими утилитами протокола TCP/IP

Цель работы: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Оборудование: ПК, программное обеспечение – операционная система Windows, утилиты, MS Word, инструкции по выполнению работы.

Содержание работы:

Задание 1. Получение справочной информации по командам.

1. Выведите на экран справочную информацию по всем рассмотренным утилитами. Для этого в командной строке введите имя утилиты без параметров и дополните /?.
2. Сохраните справочную информацию в отдельном файле.
3. Изучите ключи, используемые при запуске утилит.

Задание 2. Получение имени хоста.

1. Выведите на экран имя локального хоста с помощью команды hostname.
2. Сохраните результат в отдельном файле.

Задание 3. Изучение утилиты ipconfig.

1. Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

Задание 4. Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.

4. С помощью команды `ping` проверьте адреса (взять из списка локальных ресурсов на сайте `aspu.ru`) и для каждого из них отметьте время отклика.
5. Попробуйте изменить параметры команды `ping` таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

Задание 5. Определение пути IP-пакета.

С помощью команды `tracert` проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

- a) `aspu.ru`
- b) `mathmod.aspu.ru`
- c) `yarus.aspu.ru`

Задание 6: Просмотр ARP-кэша.

- 1. С помощью утилиты `arp` просмотрите ARP-таблицу локального компьютера.
- 2. Внести в кэш локального компьютера любую статическую запись.

Задание 7: Просмотр локальной таблицы маршрутизации.

С помощью утилиты `route` просмотреть локальную таблицу маршрутизации.

Задание 8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты `netstat` выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

- 1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.
- 2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
- 3. Каким образом команда `ping` проверяет соединение с удаленным хостом?
- 4. Каково назначение протокола ARP?
- 5. Как утилита `ping` разрешает имена узлов в ip-адреса (и наоборот)?
- 6. Какие могут быть причины неудачного завершения `ping` и `tracert`? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
- 7. Всегда ли можно узнать символьное имя узла по его ip-адресу?
- 8. Какой тип записи запрашивает у DNS-сервера простейшая форма `nslookup`?

ПРАКТИЧЕСКАЯ РАБОТА № 6

Тема: Решение проблем с TCP/IP

Цель работы: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Оборудование: ПК, программное обеспечение – операционная система Windows 7, MS Word, инструкции по выполнению работы.

Содержание работы:

1. Открыть окно командной строки, ввести команду `ping` с IP-адресом машины, при взаимодействии с которой возникают проблемы. Определить, использует ли проблемная машина конфигурацию статичного или динамичного IP адреса. Для этого откройте панель управления и выберите опцию Сетевые подключения. Теперь правой клавишей нажмите на подключении, которое собираетесь диагностировать, затем выберите опцию Свойства в появившемся меню быстрого доступа.
2. Перейдите по спискам элементов, используемых подключением, пока не дойдете до TCP/IP протокола. Выберите этот протокол, нажмите на кнопке Свойства, чтобы открыть страницу свойств для Internet Protocol (TCP/IP).
3. Запишите IP конфигурацию машины. Особенно важно сделать заметки следующих элементов:
 - Использует ли машина статичную или динамичную конфигурацию?
 - Если используется статичная конфигурация, запишите значение IP адреса, маски подсети и основного шлюза?
 - Получает ли машина адрес DNS сервера автоматически?
 - Если адрес DNS сервера вводится вручную, то какой адрес используется?
4. Если на компьютере установлено несколько сетевых адаптеров, то в панели управления будут перечислены несколько сетевых подключений.
5. Проверьте тип адаптера.
6. Определите, принимает ли Windows такую конфигурацию. Для этого откройте окно командной строки и введите следующую команду: `IPCONFIG /ALL`.
7. Определите правильный сетевой адаптер. В этом случае определение нужного адаптера довольно простое, поскольку в списке есть всего лишь один адаптер.
8. Отправьте `ping` запрос на адрес локального узла. Существует два различных способа того, как это сделать. Одним способом является ввод команды: `PING LOCALHOST`.
9. Введите команду `Nslookup`, за которой должно идти полное доменное имя удаленного узла. Команда `Nslookup` должна суметь разрешить полное доменное имя в IP адрес.
10. Необходимо просканировать клиентскую машину на предмет вредоносного ПО. Если на машине не обнаружено вредоносного ПО, сбросьте DNS кэш путем ввода следующей команды: `IPCONFIG /FLUSHDNS`.

Контрольные вопросы

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

ПРАКТИЧЕСКАЯ РАБОТА № 7

Тема: Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети

Цель работы: определение класса и расчет IP-адреса и маски подсети.

Оборудование: ПК, программное обеспечение – операционная система Windows 7, MS Word, инструкции по выполнению работы.

Справочный материал:

IP-адрес представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемых *октетами*.

Наиболее распространенной формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в *десятичной форме* и разделенных точками, например: 128.10.2.30

Этот же адрес может быть представлен в *двоичном формате*: 10000000 00001010 00000010 00011110.

А также в *шестнадцатеричном формате*: 80.0A.02.1D

Следует заметить, что максимальное значение октета равно 11111111 (двоичная система счисления), что соответствует в десятичной системе 255.

Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными. Пример: 172.16.123.1 – действительный адрес, 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона.

IP-адрес состоит из двух логических частей – *номера подсети (ID подсети)* и *номера узла (ID хоста)* в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом:

ID подсети: 172.16.0.0.

ID хоста: 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно N , то общее количество узлов равно $2^N - 2$. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях.

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно $2^{16} - 2 = 65534$ узла.

Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа:

- 1) с помощью классов
- 2) с помощью масок.

Общее правило: под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Признаком, на основании которого IP-адрес относят к тому или иному классу, являются значения нескольких первых битов адреса.

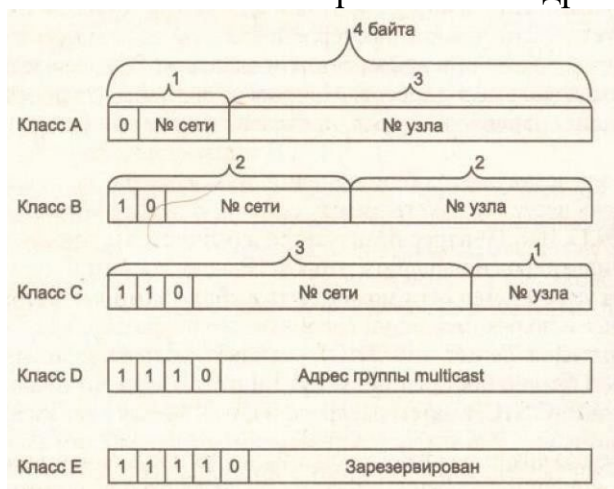


Таблица - Классы IP-адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Количество сетей	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	126	$2^{24} - 2 = 16777214$
B	10	128.0.0.0	191.255.0.0	16384	$2^{16} - 2 = 65534$
C	110	192.0.1.0	223.255.255.0	2097152	$2^8 - 2 = 254$
D	1110	224.0.0.0	239.255.255.255	Групповой адрес	
E	11110	240.0.0.0	247.255.255.255	Зарезервирован	

Адреса **класса А** предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов.

Адреса **класса В** используются в сетях среднего размера, например, сетях университетов и крупных компаний.

Адреса **класса С** используются в сетях с небольшим числом компьютеров.

Адреса **класса D** используются при обращениях к группам машин.

Адреса **класса E** зарезервированы на будущее.

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей:

- Если все биты IP-адреса равны нулю, адрес обозначает узел-отправитель и используется в некоторых сообщениях ICMP.

- Если все биты ID сети равны 1, адрес называется *ограниченным широковещательным (limited broadcast)*, пакеты, направленные по такому адресу, рассылаются всем узлам той подсети, в которой находится отправитель пакета.

- Если все биты ID хоста равны 1, адрес называется *широковещательным (broadcast)*, пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.

- Если все биты ID хоста равны 0, адрес считается идентификатором подсети (subnet ID).

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес является *внутренним адресом стека протоколов* компьютера (или маршрутизатора). Он используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере. Обе программные части данного приложения спроектированы в расчете на то, что они будут обмениваться сообщениями по сети. В IP-сети запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся со значения 127. Когда программа посылает данные по IP-адресу 127.x.x.x, то данные не передаются в сеть, а возвращаются модулям верхнего уровня того же компьютера, как только что принятые. Маршрут перемещения данных образует «петлю», поэтому этот адрес называется *адресом обратной петли* (loopback).

Форма *группового IP-адреса - multicast* - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Групповой адрес не делится на номера сети и узла и обрабатывается маршрутизатором особым образом. Основное назначение групповых адресов распространение информации по схеме «один ко многим». Основное назначение multicast-адресов - распространение информации по схеме «один-ко-многим». Хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Manageme Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом. Маршрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора. Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы. Групповая адресация предназначена для экономичного распространения в Internet или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей.

Маска - число, которое служит для выделения частей IP-адреса, чтобы TCP/IP мог отличать номер сети от номера хоста. Используя маску подсети, TCP/IP-хосты могут связаться и определить, где находится хост назначения: в локальной или удаленной сети. Пример маски подсети: 255.255.255.0.

Биты IP-адреса, определяющие номер IP-сети, в маске подсети должны быть равны 1, а биты, определяющие номер узла, в маске подсети должны быть равны 0. Для стандартных классов сетей маски имеют следующие значения:

- класс А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
- класс В - 11111111.11111111. 00000000. 00000000 (255.255.0.0);
- класс С-11111111.11111111.11111111. 00000000 (255.255.255.0).

Маски подсетей могут использоваться для маскирования тех частей адреса, которые согласно структуре класса, определяются как адреса сети. На практике разделение на подсети применяется в случае, когда конкретное сетевое адресное пространство разбивается дальше на отдельные подсети.

Подсети являются удобным средством структуризации сетей в рамках одной организации, когда все адресное пространство сети internet может быть разделено на непересекающиеся подпространства - "*подсети*", с каждой из которых можно работать как с обычной сетью TCP/IP. Таким образом единая IP-сеть организации может строиться как объединение подсетей. При этом организация должна получить один сетевой номер.

Содержание работы:

Задание 1. Изучить теоретические основы IP-адресации

1. Сколько октетов в IP — адресе?
2. Сколько битов в октете?
3. Сколько бит в маске подсети?

Задание 2. Определить IP адрес вашего ПК

1. Узнайте собственный *IP адрес* компьютера и определите, к какому классу он относится.
2. Узнать свой собственный *IP адрес* вы можете, если запустите на выполнение команду *Пуск – Программы – Стандартные – Командная Строка* и наберете в ней *ipconfig*.

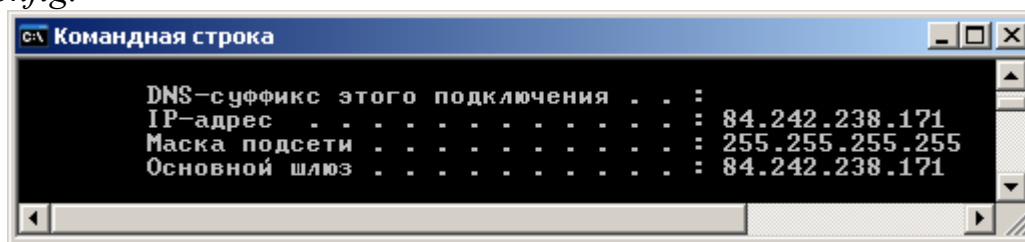


Рис.1. IP адрес вашего ПК в десятичной системе счисления

Задание 3. Переведите следующие двоичные числа в десятичные, а десятичные в двоичные

Двоичное значение	Десятичное значение	Десятичное значение	Двоичное значение
10101100.00101000.00000000.00000000		127.1.1.1	
01011110.01110111.10011111.00000000		109.128.255.254	
10010001.0110000.10000000.00011001		131.107.2.89	
01111111.00000000.00000000.00000001		129.46.78.0	

Задание 4. Определение частей IP- адресов.

Заполнить таблицу об идентификации различных классов IP-адресов.

IP- адреса хостов	Класс адреса	Адрес сети	Адреса хостов	Широковещательный (broadcast) адрес	Маска подсети по умолчанию
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Задание 5. Дан IP- адрес 142.226.0.15

1. Чему равен двоичный эквивалент второго октета?

2. Какому классу принадлежит этот адрес?
3. Чему равен адрес сети, в которой находится хост с этим адресом?
4. Является ли этот адрес хоста допустимым в классической схеме адресации?

Задание 6. Найти адрес сети, минимальный IP, максимальный IP и число хостов по IP-адресу и маске сети:

IP-адрес: 192.168.215.89 Маска: 255.255.255.0

Задание 7. Найти маску сети, минимальный IP, максимальный IP по IP-адресу и адресу сети:

IP-адрес: 124.165.101.45 Сеть: 124.128.0.0

Задание 8. Найти минимальный IP, максимальный IP по адресу сети и маске:

Маска: 255.255.192.0 Сеть: 92.151.0.0

Задание 9. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

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

ПРАКТИЧЕСКАЯ РАБОТА № 8

Тема: Монтаж кабельных сред технологий Ethernet

Цель работы: изучение назначения и способов монтажа разъемов для витой пары.

Оборудование: ПК, образец витой пары, обжимные клещи, 2 коннектора RJ-45, мультиметр, программное обеспечение – MS Word, инструкции по выполнению работы.

Содержание работы:

Задание: смонтировать разъемы на кабеле типа «витая пара».

При монтаже кабеля витой пары должен выдерживаться минимально допустимый радиус изгиба — сильный изгиб может привести к увеличению внешних наводок на сигнал или привести к разрушению оболочки кабеля.

При монтаже экранированной витой пары необходимо следить за целостностью экрана по всей длине кабеля. Растяжение или изгиб приводит к разрушению экрана, что влечёт уменьшение сопротивляемости наводкам. Дренажный провод должен быть соединен с экраном разъема.

1. Отрезать кусок витой пары нужной длины от бухты, при этом можно воспользоваться резаком, встроенным в обжимной инструмент.

2. Аккуратно снять изоляцию с кабеля. Для этого лучше использовать специальный инструмент для зачистки изоляции витой пары, его лезвие выступает ровно на толщину изоляции, чтобы не повредить проводники.

3. Расплести и развести проводники, выровнять их в один ряд, при этом соблюдая схему обжима витой пары.

4. Обкусить проводники таким образом, чтобы их длина от изоляции была чуть больше сантиметра. Для этого можно воспользоваться инструментом для обрезки витой пары, или ножами встроенными в обжимной инструмент.

5. Аккуратно вставить проводники в коннектор RJ-45. Обратите внимание, чтобы расположение проводов относительно коннектора при обжиге второго конца провода полностью совпадало с первым.

6. Проверить, не перепутались ли проводники и правильно ли они вошли в коннектор, при этом все провода должны упереться в переднюю стенку коннектора.

7. Поместить коннектор с расположенными в нем проводниками в клещи, затем плавно, но сильно произвести обжим витой пары. Обязательно следует проверить правильность обжима витой пары на предмет отсутствия контакта в отдельных проводниках. Это можно сделать при помощи мультиметра.

Подготовить отчет по выполненной работе

ПРАКТИЧЕСКАЯ РАБОТА № 9

Тема: Настройка удаленного доступа к компьютеру

Цель работы: формирование умений и навыков работы с удаленным компьютером

Оборудование: ПК, программное обеспечение – операционная система Windows 7, TeamViewer, инструкции по выполнению работы.

Справочный материал:

Нередко встречаются ситуации, когда появляется необходимость получить доступ к удаленному компьютеру - к его рабочему столу. Удаленный доступ бывает очень полезен, когда на компьютере, находящемся далеко, нужно установить или настроить какое-нибудь программное обеспечение. Да и к своему компьютеру иногда бывает нужен доступ на расстоянии.

В операционной системе Windows удаленный доступ можно осуществлять средствами самой системы. Откройте *Панель управления - Система - Удаленный доступ*. Там нужно включить опцию разрешения подключения удаленного помощника и удаленного рабочего стола.

Настройки удаленного доступа в Windows 7. Если на вашем и на удаленном компьютере установлена Windows 7, тогда среди опций удаленного рабочего стола выбирайте третий вариант - подключаться к удаленному рабочему столу с проверкой подлинности на уровне сети. Если планируется подключаться к Windows XP, тогда надо выбрать второй вариант.

Включение удаленного помощника в Windows 7 поддерживает два разных режима:

- подключение удаленного помощника;
- дистанционное управление рабочим столом.

Удаленный помощник работает во всех версиях Windows от XP до Windows 7. При этом вы будете видеть рабочий стол вашего абонента и сможете обмениваться с ним сообщениями в чате, также он может дать вам доступ к управлению компьютером: вы получите возможность своей мышью и клавиатурой совершать различные действия на его компьютере.

Дистанционное управление рабочим столом поддерживается только в Windows 7, причем кроме версий "Начальная", "Домашняя базовая" или "Домашняя расширенная". При дистанционном управлении ваш абонент будет видеть экран блокировки, а вы сможете зайти на его компьютер под определенным пользователем и работать так же, как будто вы сидите за этим компьютером.

Подключение удаленного помощника. На обоих компьютерах запустите программу "Удаленный помощник Windows". На вызываемом компьютере щелкните "Пригласить того, кому вы доверяете для оказания помощи". Далее может быть три варианта:

- Easy Connect - можно использовать только в локальной сети, при условии, что на локальном сервере Windows Server 2008 имеется протокол Peer Name Resolution Protocol, или для отправки запроса на помощь в Интернет (если ваш маршрутизатор поддерживает это).

- Пригласить по электронной почте - подойдет, если на компьютере установлена совместимая программа электронной почты (например Outlook).

- Сохранить приглашение как файл - наиболее универсальный способ, приглашение сохраняется в виде файла и ваша задача любыми способами передать его на второй компьютер (можно использовать - электронную почту, Skype, ftp сервер и т.д.).

Содержание работы:

1. С помощью сети Интернет проанализируйте те, программы, которые позволяют осуществлять подключение к удаленному компьютеру. Опишите, их.

2. Установите на свой компьютер программу для удаленного доступа через Интернет – TeamViewer.

3. Выполните соединение с удаленными компьютерами в вашей микрогруппе следуя алгоритму.

После того, как вы установили программу, запустите ее и вы увидите окошечко удаленного управления. В колонке «Разрешить управление» видно два поля – это «Ваш ID» и «Пароль».

Если вы хотите, чтобы какой-нибудь человек в данный момент подключился к вашему компьютеру, то сообщите ему ID и пароль, чтобы он смог зайти на ваш ПК.

Если нажать на кнопку «Компьютеры и контакты» в правом нижнем углу, то можно увидеть список компьютеров, которые сейчас подключены к сети.

Для того чтобы добавить еще один компьютер в список управляемых, необходимо на этом компьютере кликнуть по ссылке: «Настроить неконтролируемый доступ». В открывшемся окне введите имя компьютера и пароль доступа. Далее просто нажмите на кнопку «Готово».

Можно добавлять ПК в список только зарегистрированным пользователям, так что обязательно пройдите регистрацию.

Если вы хотите временно получить доступ к какому-нибудь компьютеру. Например, вашему другу требуется ваша помощь по настройке какой-нибудь программы. В этом случае уже он сообщает вам свой ID и временный пароль, а вы в колонке «Управлять компьютером» его указываете и попадаете на удаленную машину, которой можете управлять точно так же, как своей.

4. Отключить возможность удаленного доступа к вашему компьютеру

Кликнете правой кнопкой мыши по значку "Мой компьютер" - и откроется нужное окно, в котором выбирайте вкладку "Свойства".

Дальше Вам откроется окно "Свойства системы" - где вам необходимо выбрать вкладку меню "Удаленные сеансы"

Когда откроется окно, там Вы увидите два пункта "Удаленный помощник" и "Дистанционное удаление рабочим столом". Вот эти пункты и нужно отключить, если они включены, методом снятия "галочек" в чекбоксах.

Информационное обеспечение обучения

Печатные издания:

Основные учебные издания:

1. Ковган, Н. М. Компьютерные сети: учебное пособие / Н. М. Ковган. — Минск: Республиканский институт профессионального образования (РИПО), 2019. — 179 с. — ISBN 978-985-503-947-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/93384>

Дополнительные учебные издания:

2. Зиангирова, Л. Ф. Инфокоммуникационные системы и сети: учебное пособие для СПО / Л. Ф. Зиангирова. — Саратов: Профобразование, Ай Пи Ар Медиа, 2019. — 128 с. — ISBN 978-5-4488-0302-4, 978-5-4497-0183-1. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/85806>

3. Ракитин, Р. Ю. Компьютерные сети: учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул: Алтайский государственный педагогический университет, 2019. — 338 с. — ISBN 978-5-88210-942-3. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/102731>

4. Сергеев, М. Ю. Компьютерные сети: практикум / М. Ю. Сергеев, Т. И. Сергеева, С. А. Олейникова. — Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2019. — 154 с. — ISBN 978-5-7731-0739-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/93261>