МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ

Государственное бюджетное профессиональное образовательное учреждение

«БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»

(ГБПОУ «БРИЭТ»)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для реализации

программы подготовки специалистов среднего звена

по специальности

09.02.02 Компьютерные сети

Проектирование сетевой инфраструктуры

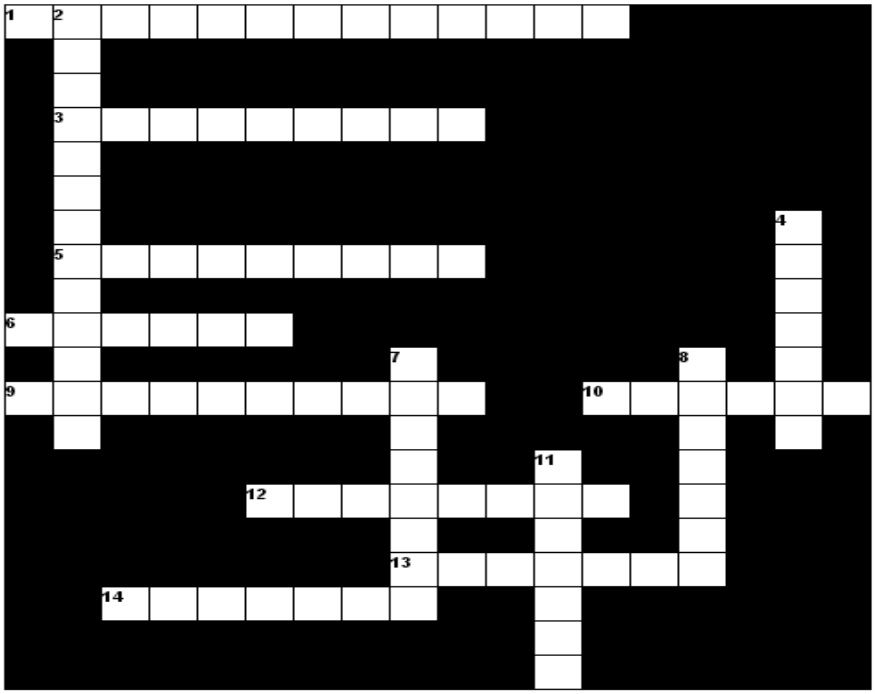
г. Улан-Удэ

2022

2.1. Оценочные средства для осуществления текущего контроля

ВХОДНОЙ КОНТРОЛЬ

Кроссворд «Компьютерные сети»



По горизонтали

1. Специализированный сетевой компьютер или устройство, имеющее минимум два сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором

3. Любые данные, которые компьютер отправляет в сеть или получает из сети проходят через сетевой ...

По вертикали

2. Учетная запись пользователя, позволяющая производить настройку операционной системы

4. Компьютерная программа, с помощью которой другие программы (обычно операционная система) получают доступ к аппаратному обеспечению некоторого устройства.

7. Групповая ... — это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды Windows

8. Программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц (преимущественно из Сети), их обработки, вывода и перехода от одной страницы к другой. Многие современные браузеры также могут загружать файлы с FTP-серверов.

5. Сетевая .... - способ описания конфигурации сети, схема расположения и соединения сетевых устройств

6. Сеть хранения .... — представляет собой архитектурное решение для подключения внешних устройств хранения данных, таких как дисковые массивы, ленточные библиотеки, оптические приводы к серверам таким образом, чтобы операционная система распознала подключённые ресурсы как локальные.

9. Switch – он же ....

10. Компьютер (или специальное компьютерное оборудование), выделенный и/или специализированный для выполнения определенных сервисных функций.

12. Набор правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

13. Группа компьютеров, объединённых высокоскоростными каналами связи и представляющая с точки зрения пользователя единый аппаратный ресурс.

14. Вспомогательная компьютерная программа в составе общего программного обеспечения для выполнения специализированных типовых задач, связанных с работой оборудования и операционной системы (ОС)

11. Окно для вывода системных сообщений и приёма команд

Критерии оценивания

Кроссворд разгадан на:
100%- «5»
75% - «4»
60% -«3»

ОПЕРАТИВНЫЙ КОНТРОЛЬ

МДК 01.01

Организация, принципы построения и функционирования компьютерных сетей

Тема 1.1 Общие принципы построения сетей

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 1 «Исследование топологии сети»

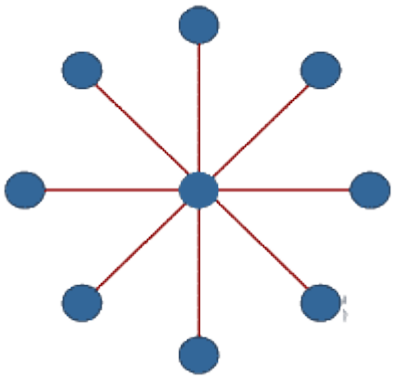
Цель работы: Изучить основы топологии и разработать сеть для конкретного учреждения

В процессе занятия решаются следующие задачи:

1. приобретение навыков исследования топологии сети;
2. разработка сети для конкретного учреждения;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Топология «звезда»



В сетях, использующих топологию "звезда", сетевой носитель соединяет центральный концентратор с каждым устройством, подключенным к сети. Физический вид топологии "звезда" напоминает радиальные спицы, исходящие из центра колеса. В этой топологии используется управление из центральной точки, а связь между устройствами, подключенными к сети, осуществляется посредством двухточечных линий между каждым устройством и центральным каналом или концентратором. Весь сетевой трафик в звездообразной топологии проходит через концентратор. Вначале данные посылаются концентратору, а затем концентратор переправляет их устройству в соответствии с адресом, содержащимся в данных. В сетях с топологией "звезда" концентратор может быть активным или пассивным. Активный концентратор не только соединяет участки среды передачи, но и регенерирует сигнал, т.е. работает как многопортовый повторитель. Благодаря выполнению регенерации сигналов, активный концентратор позволяет данным перемещаться на более значительные расстояния. В отличие от активного концентратора, пассивный концентратор только соединяет участки сетевой среды передачи данных.

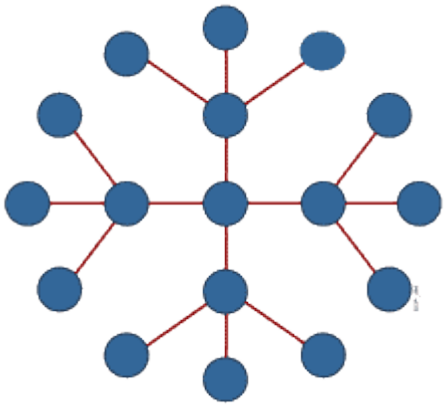
Преимущества и недостатки топологии «звезда»

Большинство проектировщиков сетей считают топологию "звезда" самой простой с точки зрения проектирования и установки. Это объясняется тем, что сетевая среда выходит непосредственно из концентратора и прокладывается к месту установки рабочей станции. Другим достоинством этой топологии является простота обслуживания: единственной областью концентрации является центр сети. Также топология "звезда" позволяет легко диагностировать проблемы и изменять схему прокладки. Кроме того, к сети, использующей топологию "звезда", легко добавлять рабочие станции. Если один из участков сетевой среды передачи данных обрывается или закорачивается, то теряет связь только устройство, подключенное к этой точке. Остальная часть сети будет функционировать нормально. Короче говоря, топология "звезда" считается наиболее надежной. В некотором смысле достоинства топологии "звезда" могут считаться и ее недостатками. Например, наличие отдельного отрезка кабеля для каждого устройства позволяет легко диагностировать отказы, однако, это же приводит и к увеличению количества отрезков. В результате повышается стоимость установки сети с топологией "звезда". Другой пример: концентратор может упростить обслуживание, поскольку все данные проходят через эту центральную точку; однако, если концентратор выходит из строя, то перестает работать вся сеть.

Область покрытия сети с топологией «звезда»

Максимально допустимая длина отрезков сетевого кабеля между концентратором и любой рабочей станцией (их еще называют горизонтальной кабельной системой) составляет 100 метров. Величина максимальной протяженности горизонтальной кабельной системы устанавливается Ассоциацией электронной промышленности (Electronic Industries Association, EIA) и Ассоциацией телекоммуникационной промышленности (Telecommunications Industry Association, TIA). Эти две организации совместно создают стандарты, которые часто называют стандартами EIA/TIA. В частности, для технического выполнения горизонтальной кабельной системы был и остается наиболее широко используемым стандарт EIA/T1A-568B. В топологии "звезда" каждый отрезок горизонтальной кабельной системы выходит из концентратора, во многом напоминая спицу колеса. Следовательно, локальная сеть, использующая этот тип топологии, может покрывать область 200x200 метров. Понятно, бывают случаи, когда область, которая должна быть покрыта сетью, превышает размеры, допускаемые простой топологией "звезда". Представим себе здание размером 250x250 метров. Сеть с простой звездообразной топологией, отвечающая требованиям к горизонтальной кабельной системе, устанавливаемым стандартом **EIA/TIA-568B,** не может полностью покрыть здание с такими размерами. Рабочие станции находятся за пределами области, которая может быть накрыта простой звездообразной топологией, и, как и изображено, они не являются частью этой сети. Когда сигнал покидает передающую станцию, он чистый и легко различимый. Однако по мере движения в среде передачи данных сигнал ухудшается и ослабевает — чем длиннее кабель, тем хуже сигнал; это явление называется ***аттенюацией.*** Поэтому, если сигнал проходит расстояние, которое превышает максимально допустимое, нет гарантии, что сетевой адаптер сможет этот сигнал прочитать.

Топология "расширенная звезда"



Если простая звездообразная топология не может покрыть предполагаемую область сети, то ее можно расширить путем использования межсетевых устройств, которые не дают проявляться эффекту аттенюации; результирующая топология называется топологией ***"расширенная звезда".*** Еще раз представим себе здание размером 250x250 метров. Для того чтобы звездообразная топология могла эффективно использоваться в этом здании, ее необходимо расширить. За счет увеличения длины кабелей горизонтальной кабельной системы это делать нельзя, поскольку нельзя превышать рекомендуемую максимальную длину кабеля. Вместо этого можно использовать сетевые устройства, которые препятствуют деградации сигнала. Чтобы сигналы могли распознаваться принимающими устройствами, используются повторители, которые берут ослабленный сигнал, очищают его, усиливают и отправляют дальше по сети. С помощью повторителей можно увеличить расстояние, на которое может простираться сеть. Повторители работают в тандеме с сетевыми носителями и, следовательно, относятся к физическому уровню эталонной модели **OSI.**

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. На плане здания (сооружения) прилагаемого к практический работе. Постройте сеть с топологией звезда, с отражением необходимых параметров, таких как:
    a. Прокладка кабеля;
    b. Расположения серверов;
    c. Расположение телефонных аппаратов;
    d. Расположение рабочих станций;

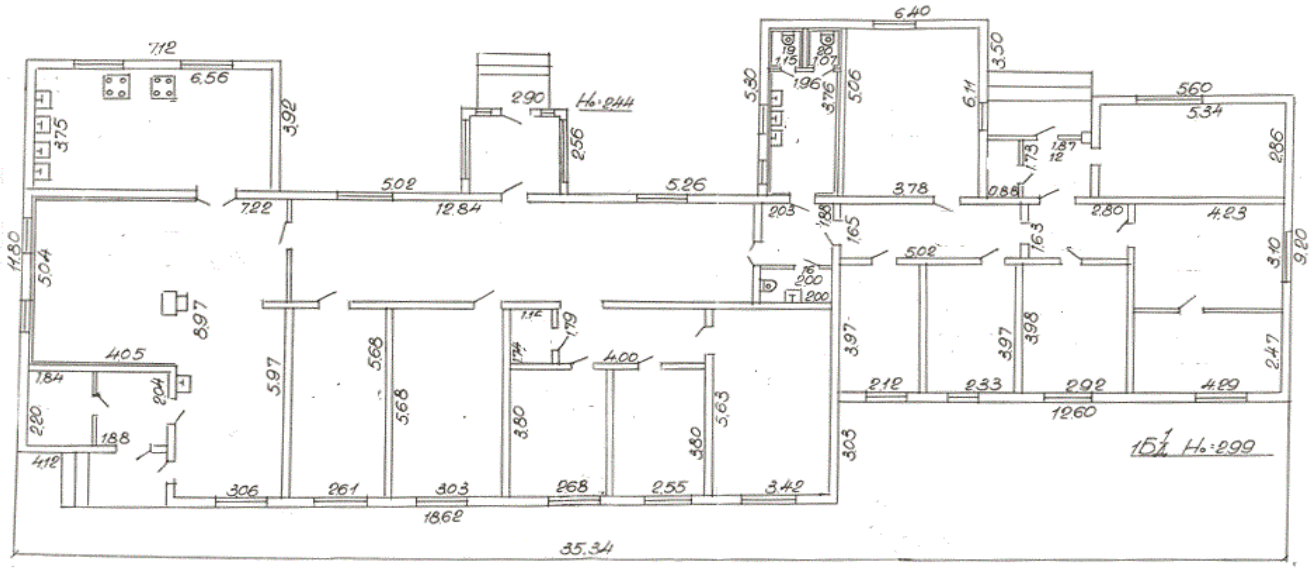
    Для выполнения работы необходимо обратиться к примеру прокладки сети.
3. По завершению работы необходимо сдать тетрадь для практических работ с отчетом о проделанной работе. Отчет должен содержать этапы построения сети, обоснование основных решений в процессе прокладки сети и вывод по практической работе.

ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Ниже на примере представлен план здания с указанной прокладкой сети.

Условие задачи: проложить сеть в организации «Н». Сеть должна содержать не мение десяти рабочих станций, с выделенным сервером. Каждый рабочий кабинет должен иметь по одному рабочему телефону.

Приложение1



Время выполнения работы 90 мин;

Контрольные вопросы

1. Основные достоинства топологии звезда?
2. Какой кабель рекомендуют использовать для реализации сетевой топологии звезда?

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если не выполнена одна часть задания, выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 2 «Выполнение монтажных работ с коаксиальным кабелем и витой парой»

Цель работы: получить навыки работы с сетевыми кабелями: «витая пара».
В процессе занятия решаются следующие задачи:

- Научиться работать с «тонким» коаксиальным кабелем и кабелем «витая пара» категории 5 (или более высокой);
- Научиться устанавливать на концах кабелей (*заделывать*) коннекторы RJ-45;
- Научиться проверять качество заделки коннекторов;
- Научиться использовать прямые и перекрестные кабели на основе «витой пары» для связи компьютеров, концентраторов и коммутаторов

Краткие теоретические и справочно-информационные материалы по теме занятия.

От выбора кабельной инфраструктуры и способа объединения компьютеров в сеть во многом зависят такие параметры сети, как ее надежность и расширяемость.

В этой лабораторной работе рассматриваются такие типы кабеля, как «тонкий» коаксиальный и «витая пара», описываются процедуры монтажа соответствующих коннекторов и демонстрируется применение различных кабелей на основе «витой пары» для объединения сетевых устройств.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Задание 1.
   Работа с «тонким» коаксиальным кабелем и с кабелем «витая пара»

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

Изучение тонкого коаксиального кабеля

1. Возьмите отрезок коаксиального кабеля и исследуйте его строение.
2. Аккуратно удалите часть внешней оболочки и обрежьте экранирующую оплетку. Затем надрежьте, чуть надломите и снимите внутреннюю изоляцию, не повредив центральную жилу.

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.

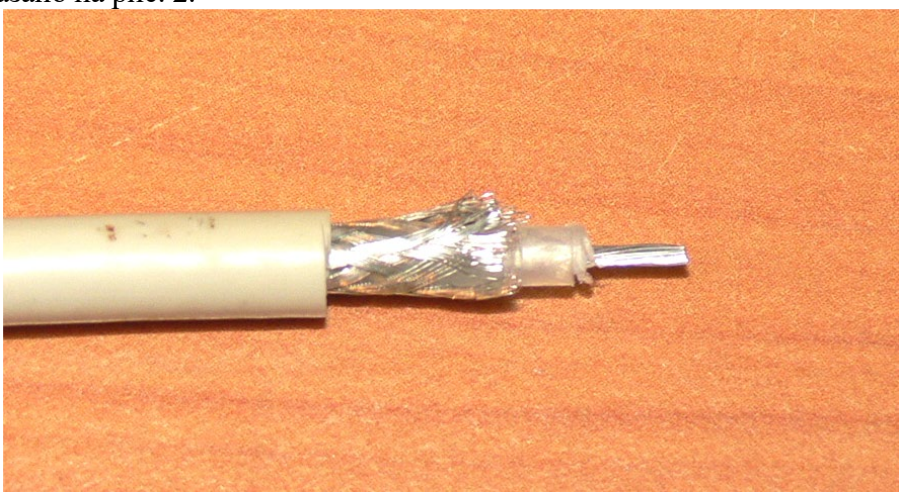


Рис. 2. Коаксиальный кабель RG-58 после зачистки

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.

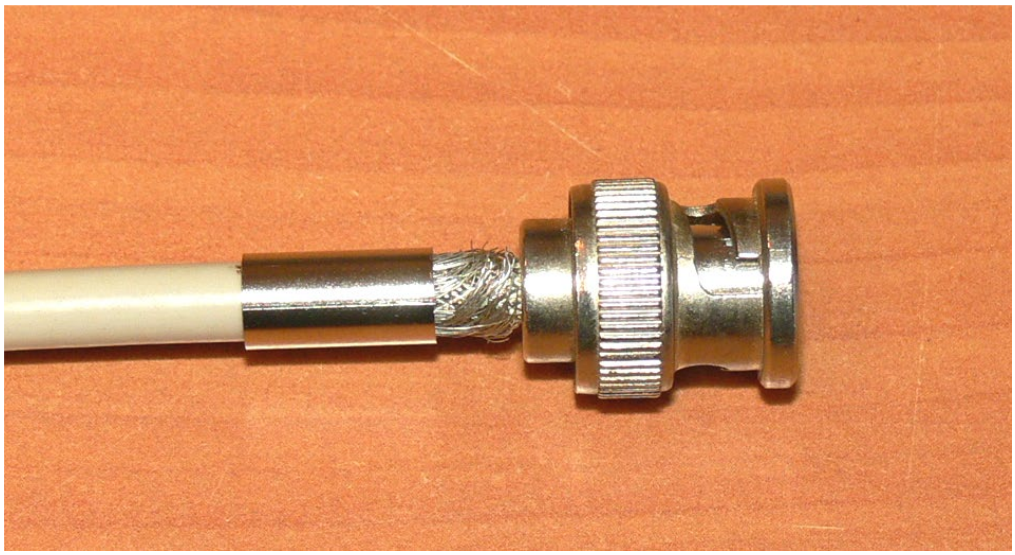


Рис. 4. Коаксиальный кабель с установленной основной частью коннектора
и не полностью надетой обжимной трубочкой

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

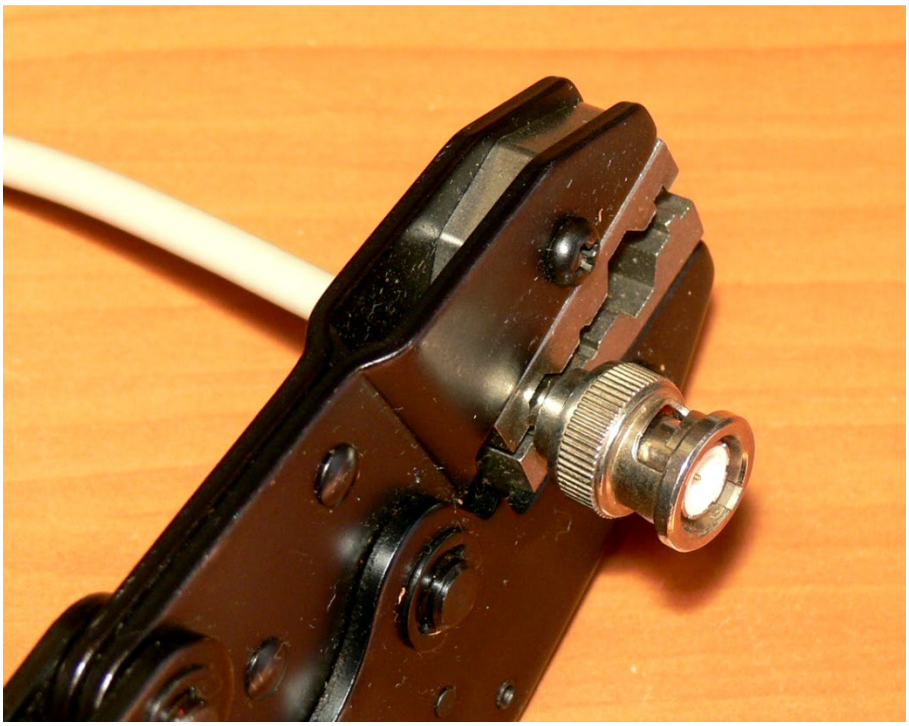


Рис.5. Коннектор BNC в обжимном инструменте

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).

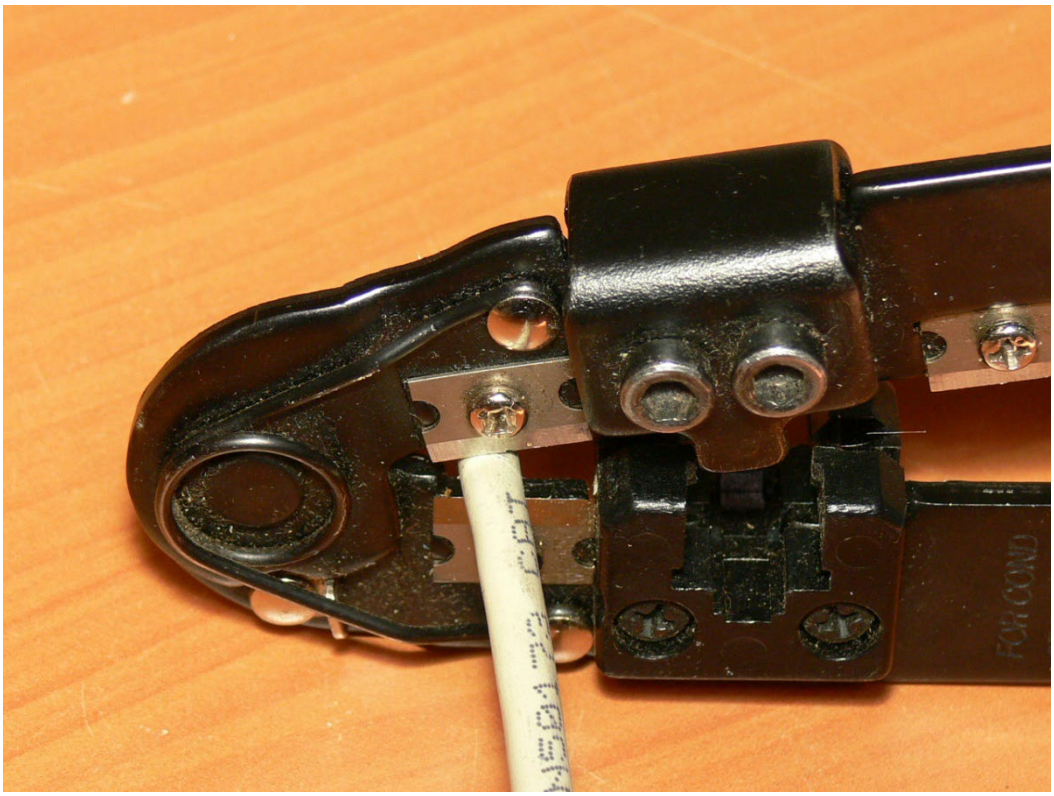


Рис.6. Обрезка внешней изоляции на кабеле «витая пара»

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.

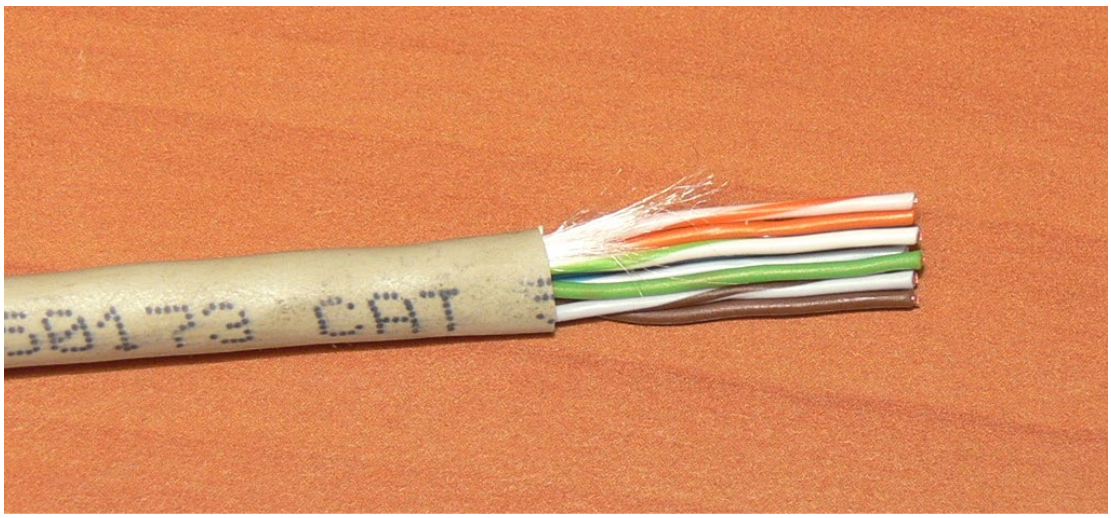


Рис. 7. Кабель «витая пара» с расплетенными и выпрямленными проводниками

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).

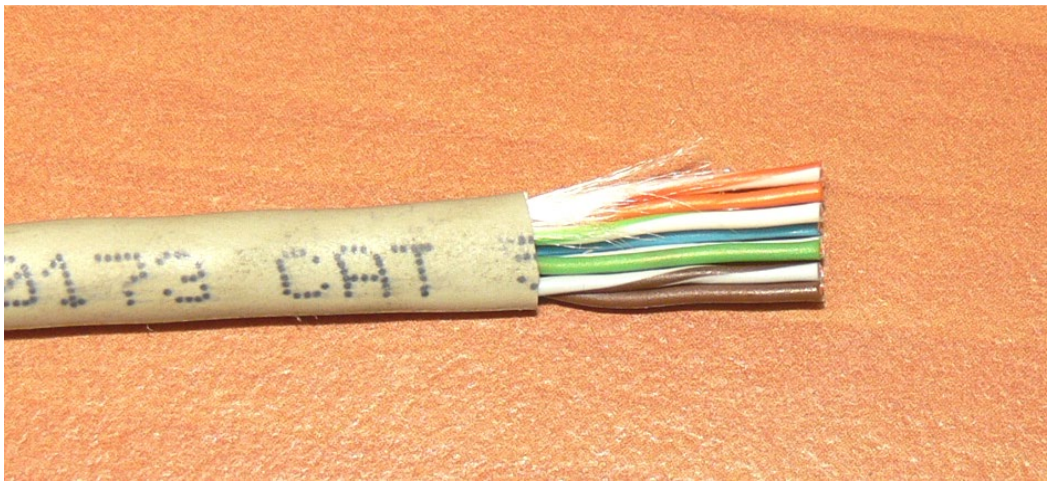


Рис. 8. Кабель «витая пара» с подготовленными к монтажу в коннектор проводниками

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*.
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. 4.10), 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

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

Примечание. Показанное на рис. 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.*

Задание 2.
Использование кабелей на базе «витой пары»

Для успешного выполнения этого задания необходимо, чтобы вы настроили компьютеры для работы в сети, как описано в задании 1 лабораторной работы 1, а также изготовили прямые и перекрестные кабели, как описано в задании 1 данной лабораторной работы.

Объединение двух компьютеров с помощью перекрестного кабеля

1. Возьмите только что изготовленный *прямой кабель*.
2. Соедините ваш компьютер с компьютером вашего партнера с помощью прямого кабеля (для этого коннекторы на обоих концах кабеля должны быть вставлены непосредственно в разъемы RJ-45 сетевых адаптеров). Включите оба компьютера.
3. Войдите в систему с учетной записью, входящей в локальную группу «Администраторы» (например, как пользователь User1 с паролем P@ssw0rd).
4. В меню **Пуск** выберите пункт **Мой компьютер**.
5. В поле **Открыть** окна **Запуск программы** введите строку \\Comp*x*, где Comp*x* — имя компьютера вашего партнера (например, Comp2). Щелкните мышью на кнопке **ОК**.

Удалось ли вам увидеть общие ресурсы на компьютере вашего партнера?

6. Отрицательный ответ на приведенный выше вопрос означает, что использовать прямой кабель для непосредственной связи компьютеров друг с другом нельзя.
7. Замените кабель на *перекрестный* и повторите описанные выше действия.

Удалось ли вам увидеть общие ресурсы на компьютере вашего партнера?

8. Открывшееся окно с общими ресурсами компьютера вашего партнера означает, что сетевое взаимодействие между компьютерами установлено. Закройте все окна.

Подключение компьютера к концентратору (коммутатору)

1. Отключите перекрестный кабель от компьютера вашего партнера и подключите его к концентратору (или коммутатору).
2. Убедитесь, что ваш партнер также подключился к концентратору с помощью *перекрестного* кабеля. Включите питание концентратора (коммутатора).
3. В меню **Пуск** выберите пункт **Мой компьютер**.
4. В поле **Открыть** окна **Запуск программы** введите строку \\Comp*x*, где Comp*x* — имя компьютера вашего партнера (например, Comp2). Щелкните мышью на кнопке **ОК**.

Удалось ли вам увидеть общие ресурсы на компьютере вашего партнера?

5. Отрицательный ответ на приведенный выше вопрос означает, что использовать перекрестный кабель для связи компьютеров с такими устройствами, как концентраторы и коммутаторы, нельзя.

Примечание. Многие современные коммутаторы достаточно «интеллектуальны», оснащены функцией авто определения типа кабеля и способны не только распознавать нестандартный тип кабеля, но и переключать порт в противоположный режим работы. При этом те контакты порта, которые обычно используются для передачи данных, начинают работать на их прием, и наоборот. Если при использовании перекрестного кабеля для подключения компьютера к коммутатору взаимодействие в сети обеспечено, это значит, что ваш коммутатор оснащен такой функцией.

6. Замените кабель на *прямой* (ваш партнер также должен проделать это) и повторите операцию.

Удалось ли вам увидеть общие ресурсы на компьютере вашего партнера?

7. Открывшееся окно с общими ресурсами компьютера вашего партнера означает, что сетевое взаимодействие между компьютерами установлено. Следовательно, для связи компьютеров с концентраторами и коммутаторами нужно использовать *прямой* кабель «витая пара».

8. Закройте все окна.

Подключение концентраторов или коммутаторов друг к другу (каскадирование)

1. Возьмите второй концентратор (коммутатор).
2. Переключите свой кабель с первого концентратора (коммутатора) на второй, а кабель вашего партнера оставьте подключенным к первому концентратору (коммутатору).
3. Соедините два концентратора (коммутатора) между собой с помощью *прямого* кабеля (обязательно используйте при этом порты со средними номерами, например, под номером 3).
4. В меню **Пуск** выберите пункт **Мой компьютер**.
5. В поле **Открыть** окна **Запуск программы** введите строку \\Comp*x*, где Comp*x* — имя компьютера вашего партнера (например, Comp2). Щелкните мышью на кнопке **ОК**.

Удалось ли вам увидеть общие ресурсы на компьютере вашего партнера?

6. Отрицательный ответ на приведенный выше вопрос означает, что просто использовать прямой кабель для связи концентраторов и коммутаторов между собой нельзя.

Примечание. Если увидеть общие ресурсы все же удалось, это значит, что ваш коммутатор поддерживает функцию определения типа кабеля на каждом из портов.

7. Найдите на одном из концентраторов (коммутаторов) порт с названием **Uplink**, **Crossover** или **MDI-X** и переключите туда коннектор кабеля, соединяющего концентраторы друг с другом (это нужно сделать только на одном устройстве). Повторите операцию обращения к сетевым ресурсам.

Удалось ли вам увидеть общие ресурсы на компьютере вашего партнера?

8. Открывшееся окно с общими ресурсами компьютера вашего партнера означает, что сетевое взаимодействие между концентраторами установлено. Обратите внимание, что связь между концентраторами или коммутаторами с помощью прямого кабеля работает только тогда, когда на одном из устройств используется так называемый *перекрестный* (**Uplink**, **Crossover** или **MDI-X**) *порт.*
9. Закройте все окна.
10. Замените кабель, связывающий концентраторы (коммутаторы), на *перекрестный*, но *не используйте* порт **Uplink** (например, вставьте оба коннектора в порты с номером 3). Повторите операцию обращения.

Удалось ли вам увидеть общие ресурсы на компьютере вашего партнера?

11. Открывшееся окно с общими ресурсами компьютера вашего партнера означает, что объединение концентраторов и коммутаторов друг с другом без использования перекрестного порта (**Uplink**) возможно благодаря применению *перекрестного* кабеля на основе «витой пары».
12. Закройте все окна и завершите работу с компьютером.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Сколько проводников используется для передачи сигнала по коаксиальному кабелю? Какие это проводники?
2. Из какого металла (меди или алюминия) изготовлен центральный проводник вашего кабеля? Одножильный он или многожильный?
3. Какие устройства соединяются с помощью прямого кабеля?
4. Все ли индикаторы на удаленной («REMOTE») части прибора загораются с соответствии с индикаторами на основной его части?
5. Какие устройства можно соединять с помощью перекрестного кабеля?

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ

Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 3 «Выполнение монтажных работ с оптоволоконным кабелем»

Цель работы: изучить конструкцию волоконно-оптических кабелей, аппаратуру и оборудование для монтажа волоконно-оптических кабелей, научиться сращивать волокна оптического кабеля;

В процессе занятия решаются следующие задачи:

1. формирование навыков монтажа опто-волоконных кабелей;

Краткие теоретические и справочно-информационные материалы по теме занятия.

В волоконно-оптических системах передачи информационные сигналы распространяются по оптическим кабелям. Основным элементом оптического кабеля является оптический волновод – круглый стержень из оптически прозрачного диэлектрика, структура которого обеспечивает распространение вдоль него световых сигналов. Оптические волноводы из-за малых размеров поперечного сечения обычно бывают волоконными световодами (ВС) или

оптическими волокнами (ОВ). Первый термин обычно применяется при исследовании вопросов передачи информации с помощью законов оптики, тогда как второму отдается предпочтение при рассмотрении конструктивных и технологических особенностей оптических кабелей.

Для связи по оптическому волокну (рис. 1) используются видимые лучи (0,4…0,75 мкм) и ближний диапазон инфракрасных лучей (0,85;1,3;1,55…6 мкм). При этом возможна передача большого числа различных типов волн – мод (m). Исходя из двойственной природы света (лучевой и волновой) различным типам волн (модам) соответствует различное число лучей. Одномодовой передаче соответствует один луч (рис. 2, *а*), а многомодовой – два и более (рис. 2, *б*)

Рис 1. Оптическое волокно

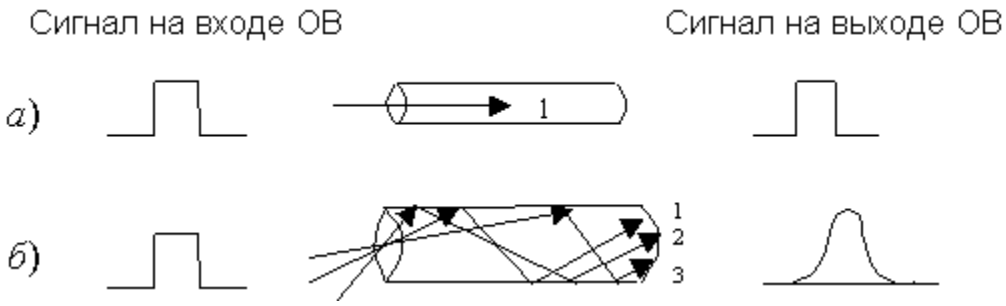


Рис 2. Одномодовая (*а*) и многомодовая (*б*) передачи

Одномодовый режим возможен при $l \gg d$, $l < d$.

Достоинства одномодовых систем:

- малая дисперсия (искажение сигналов);
- большая пропускная способность;
- большая дальность передачи;
- отсутствие модовых искажений.

Свойства оптического кабеля (ОК) определяются, главным образом, двумя характеристиками: затуханием и дисперсией. Затухание ограничивает длину регенерационных участков и дальность передачи по кабелю. Дисперсия приводит к искажению передаваемых сигналов и определяет частотную ширину тракта и пропускную способность кабеля.
Затухание ОК на волне 0,85 мкм – 3–5 дБ/км;
1,3 мкм – 1 дБ/км;
1,55 мкм – 0,5 дБ/км.
Полоса пропускания для многомодового ОК – 300 МГц км;
градиентного – 800 МГц км;
одномодового – 5000 МГц км.

2. Материалы для изготовления волоконных световодов

В настоящее время волоконные световоды изготовляют из кварцевого стекла (волокно “кварц–кварц”) с добавлением компонентов. В некоторых случаях применяют полимерные волокна.

Иногда сердцевины ОВ выполняют из кварцевого или многокомпонентного стекла, а оболочку из полимера (например, волокна “кварц – полимер”). Из кварцевого стекла изготовляют волокна высокого качества, достоинства которого перед другими видами оптически прозрачных диэлектриков состоит в том, что оно обладает наименьшими потерями на поглощение. Для создания необходимой разности показателей преломления сердцевины и оболочки волокна кварцевое стекло легируют соответствующими веществами, например оксидами германия, фосфора, бора и др. Так для увеличения показателя преломления сердцевины двухслойного волокна в состав SiO_2 входят легирующие добавки. Требуемую разность показателей преломления сердцевины и оболочки можно получить, уменьшая показатель преломления кварца путем легирования его веществами, понижающими показатель преломления, например, двуокисью бора B_2O_3. Другая возможность понижения показателя преломления заключается в добавлении фтора в плавленный кварц. Полимерные волокна имеют более высокие потери, чем стеклянные. Например, в лучших волокнах из полиметилнетокрита затухание составляет около 20 дБ/км. Однако полимерные волокна очень дешевы и отличаются высокими механическими характеристиками. Это позволяет широко использовать полимерные волокна в оптических линиях малой протяженности.

3. Конструкция оптических кабелей связи

Оптические кабели по назначению подразделяется на междугородные, городские, объектовые и монтажные.

Междугородные кабели предназначены для передачи информации на большие расстояния и поэтому должны обладать малым затуханием, дисперсией и большой широкополосностью.

Городские кабели используются в качестве соединительных линий между городскими АТС и узлами связи.

Объектовые кабели существуют для передачи различной информации внутри объекта. К ним относятся кабели как для отдельных объектов (самолет, корабль и т.д.), так и для организации различных видов учережденческой связи.

Монтажные оптические кабели предназначены для внутри- и межблочного монтажа аппаратуры.

В зависимости от условий прокладки и эксплуатации кабели разделяются на подземные и подводные, а также подвесные. В соответствии с условиями подземной прокладки и эксплуатации оптические кабели подразделяются на четыре типа:

1. с допустимым растягивающим усилием не менее 80 кН для прокладки через водные преграды (судоходные реки, водохранилища), болота и в районах вечной мерзлоты;
2. с допустимым растягивающим усилием 20 кН для прокладки в скальных и тяжелых грунтах при наличии опасности механического повреждения;

3. с допустимым растягивающим усилием не менее 7кН для прокладки в гравийно-песчаных грунтах, наносных песках и тяжелых глинистых грунтах;
4. с допустимым растягивающим усилием не менее 2,7 кН для прокладки в кабельной канализации и защитных пластиковых трубах.

По конструкции оптические кабели подразделяются на повивные с профилированным пластмассовым сердечником, жгутовые и ленточные.

Типовой повивной кабель имеет центральный элемент жесткости, на который навивают оптические волокна. При необходимости увеличения числа волокон накладывают второй повив. Оптические волокна защищают покрытиями, на которые накладывают армирующую полимерную оболочку. В качестве примера на рис. 3 показан семиволоконный кабель правильной повивной структуры в полиэтиленовой оболочке с армирующими силовыми элементами, расположенными по периферии.

В жгутовых конструкциях кабелей с числом волокон от 20 до 80 первоначально оптические волокна скручивают в группы и покрывают буферным слоем с внешним диаметром порядка 1 мм. Затем группы компонуют в модули, которые повивают на центральный силовой элемент, при этом модули могут чередоваться друг с другом и с элементами жесткости.

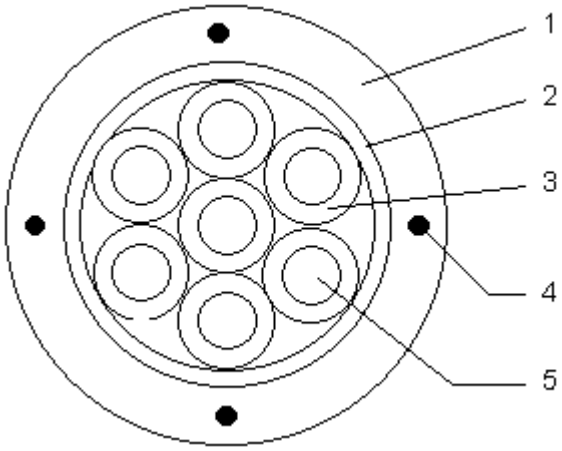


Рис. 3. Оптический кабель связи правильной повивной скрутки:
1 – внешняя полиэтиленовая оболочка; 2 – внутренняя пористая оболочка; 3 – защитное покрытие; 4 – армирующий элемент; 5 – модуль

На рис. 4 показан кабель, содержащий модуль в виде профилированного сердечника, в канавках которого расположены шесть волокон. Структуру кабеля завершает защитная оболочка с внешними элементами жесткости.

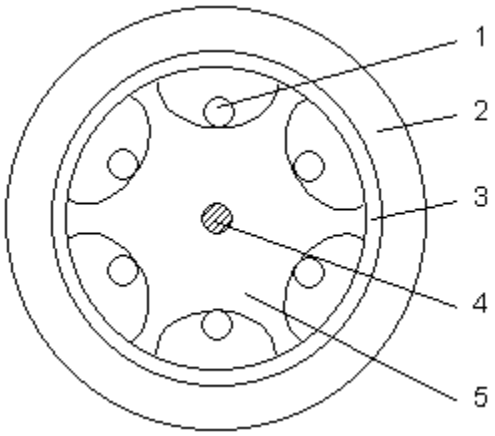


Рис.4. Оптический кабель связи с фигурным пластмассовым стержнем: 1 – ОВ; 2 – внешняя оболочка; 3 – алюминиевая оболочка; 4 – силовой элемент; 5 – профильный стержень

Далее рассмотрим марки оптических кабелей, выпускаемых российской промышленностью:

- ОМЗКГ-10-0 и ОМЗКГ-50-0 предназначены для прокладки в грунтах всех категорий. Кабели эксплуатируются при температуре от –40 до +50 ° С.
- Самонесущие кабели типа ДОН-0,4 (-0,6;-0,8) используются для прокладки на опорах ЛЭП, контактной сети железных дорог, по мостам и в тоннелях;
- ОКВО-М8 Т-10-0,4-8 – внутриобъектовый кабель, предназначен для прокладки внутри аппаратуры станций, зданий и сооружений;
- ОКП-10-01(рис. 5) предназначен для подвески на опорах;
- ОКЗК предназначен для прокладки в грунте и кабельной канализации, а кабель ОКЛ-01, ОКЛ-02 – для прокладки в кабельной канализации, трубах, а также внутри зданий (рис. 6);

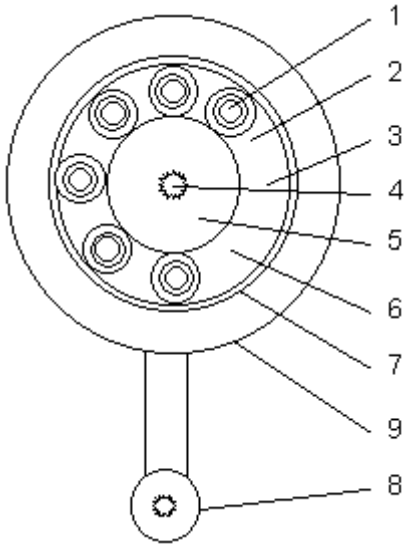


Рис.5. Оптический кабель для подвески на опорах (марки ОКП-10-01 производства ЗАО "Оптика-кабель"): 1– оптическое волокно; 2 – гидрофобный заполнитель; 3 – полимерная трубка; 4 – стеклопластик; 5 – полимерная трубка; 6 – гидрофобный заполнитель; 7 – скрепляющая лента; 8 – синтетическая нить; 9 – полимерная защитная оболочка

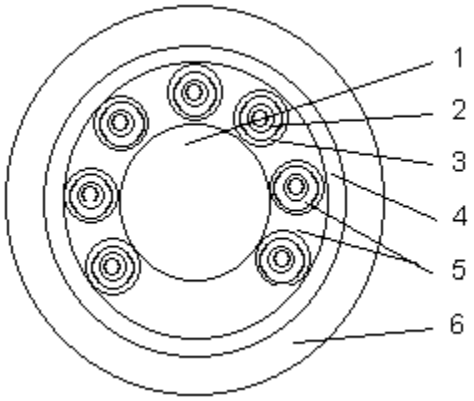


Рис. 6. Оптический кабель для прокладки в трубах: 1 – центральный элемент (стеклопластиковый пруток или стальной трос); 2 – оптическое волокно (от 1 до 10); 3 – оптический модуль (от 1 до 8); 4 – водоблокирующая обмотка; 5 – гидрофобный компаунд; 6 – наружная оболочка

ОКЛЖ-01-5 – несущий оптический кабель связи, предназначен для подвески на опорах линии связи, контактной сети железных дорог, линий электропередач напряжением 110 кВ.

4. Оборудование и аппаратура для монтажа волоконно-оптических кабелей

Одной из важнейших операций, определяющих параметры и качество ВОЛС, является сращивание оптических кабелей. На трассах сращивание производится с использованием оптических муфт. При монтаже ОК на оконечных участках ВОЛС используются коммутационно-распределительные устройства. Монтаж муфты проводится после завершения прокладки двух строительных длин кабеля (около 6 км).

В настоящее время для сращивания оптических кабелей в основном используется два способа: сварка оптических волокон и механическое соединение.

Сварка оптических волокон производится путем нагрева их до расплавления с помощью электрической дуги. При сварке предварительно подготовленные волокна подводят друг к другу, юстируют до минимальных зазоров между ними и минимальных (оптических) смещений оптических осей, а затем нагревают. При этом силы поверхностного натяжения волокна уменьшают смещения осей свариваемых волокон.

Аппараты для сварки многомодовых волокон обеспечивают ручную юстировку волокон с просмотром в двух плоскостях с помощью микроскопа и сварку в ручном и автономном режимах: электронное устройство позволяет регулировать ток и время оплавления торцов и сварки, скорость сдвига волокон при сварке. В современных сварочных устройствах предусмотрена автоматическая юстировка. Она осуществляется двумя методами:

- минимизацией потерь в стыке, т.е. в месте изгиба волокна в одно из соединяемых волокон вводят, а в другом выводят оптический сигнал, и юстировка проводится пьезоподвижками по максимуму прошедшего сигнала;
- анализом изображения стыков соединяемых волокон в параллельном пучке света: свет падает перпендикулярно оптической оси волокон и изображения стыков получают с помощью телекамеры, необходимая юстировка проводится путем анализа сигнала телекамеры.

Первый способ юстировки относительно прост и обеспечивает потери в сварке не более 0,1 дБ.

Рис. 7. Аппарат для сварки 0В FSM-30S

Автоматический аппарат для сварки оптических волокон FSH-30S (рис. 6.7) фирмы FUJIKURA (Япония) предназначен для соединения оптических волокон. В аппарате производится автоматическая юстировка по трем направлениям при сведении световодов, автоматический контроль мощности дугового разряда, компенсация изменения давления, температуры и влажности, запись режимов и результатов сварки.

В отечественном аппарате для сварки одномодовых и многомодовых волокон СОВА-11 и 12 используются ручные методы юстировки по наружному диаметру. Автоматическая юстировка волокон по максимуму оптического сигнала применяется в аппаратах СОВА-20, СОВА-20К.

5. Коммутационно-распределительные устройства и муфты

К коммутационно-распределительным устройствам относятся настенные соединительные коробки, соединительные модули, шкафы. Оптические муфты предназначены для сращивания оптических кабелей. Широкое применение получили муфты отечественного производства следующих марок: ММ30К, МОГ/МОГр, МТОК, МОМ3, МОГу.

Муфты МОГу (проходные / распределительные) предназначены для сращивания оптических кабелей с диаметром внешней оболочки от 9 до 25 мм.

Муфты МОМ3 (проходные / распределительные) – для сращивания оптических кабелей с наружным диаметром от 9 до 25 мм.

Шкафы кроссовые предназначены для соединения оптического кабеля с приемопередающей аппаратурой. Шкаф ШКО-Н-М1-РС (рис. 8, *а*) предназначен для применения совместно с кабелем марки ОКВО-М8(1,2)Т или ОКВО-М12(0,9)Т. Шкафы ШКО-С-СК (рис. 8, *б*), ШКО-С-СК1, ШКО-С-СК2 предназначены для установки в стойки СКУ и позволяют организовать оптическую кроссовую стойку с количеством портов до 352.

а) *б*)

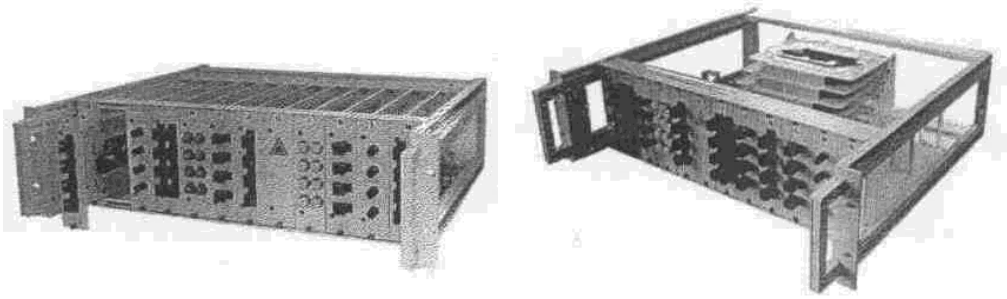


Рис. 6.8. Шкафы кроссовые

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Выполнение задания

Сращивание в муфте строительных длин оптических кабелей связи выполняется в следующем порядке.

1. Установить в пролете между двумя консолями нижней половины металлический желобок и выложить на нем нахлест сращиваемых концов кабелей.

2. Обрезать концы сращиваемых кабелей по размерам.

3. Надвинуть на концы кабелей полиэтиленовые конусы, цилиндры, опорные стальные кольца, отрезки термоусаживаемых трубок. Произвести сварку полиэтиленовых конусов с оболочкой кабелей методом наплавления полиэтиленовой ленты под стеклолентой (рис. 9).

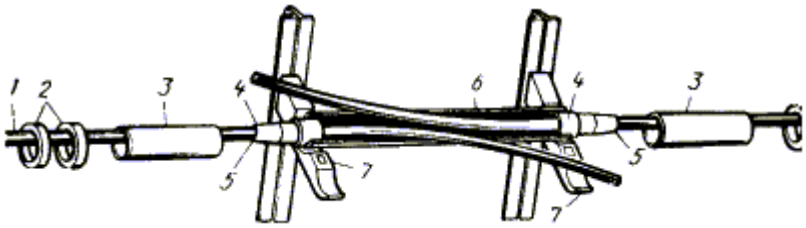


Рис. 9. Надвигание на сращиваемые концы кабелей термоусаживаемых трубок: 1 – сращиваемые кабели; *2* – отрезки термоусаживаемых трубок ТУТ 80/40; 3 – полиэтиленовые цилиндры; 4 – полиэтиленовые конуса с опорными стальными кольцами; 5 – приварка конусов к оболочке методом наплавления полиэтиленовой ленты под стеклолентой; 6 – нижняя половина металлического желобка; 7 – кабельные консоли

4. Надвинуть на сращиваемые концы кабелей конусы, цилиндры, отрезки термоусаживаемых трубок, приварить конусы к оболочке.

5. Снять оболочки с концов кабелей ножом или с помощью специального приспособления, один из возможных вариантов которого приведен на рис. 10.

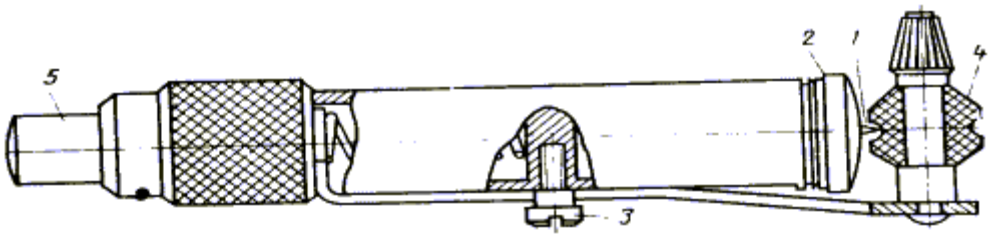


Рис. 10. Вариант конструкции инструмента для продольного и радиального прорезания оболочки кабеля: 1 – режущее лезвие; 2 – регулятор глубины реза; 3 – рычаг перевода лезвия с продольной на радиальную резку; 4 – ролик подачи кабеля; 5 – нажимная подпружиненная кнопка

6. Протереть сердечники кабелей ветошью, смоченной бензином Б-70, для удаления гидрофобного заполнения.

7. Надвинуть на центральный упрочняющий элемент одного из концов кабелей металлическую обжимную втулку и удалить поливинилхлоридную оболочку с обоих упрочняющих элементов от центра муфты до конца.

8. Обжать металлическую втулку на концах упрочняющих элементов с выводом оголенных прядей на поверхность втулки и связкой их двойным узлом (рис. 11).

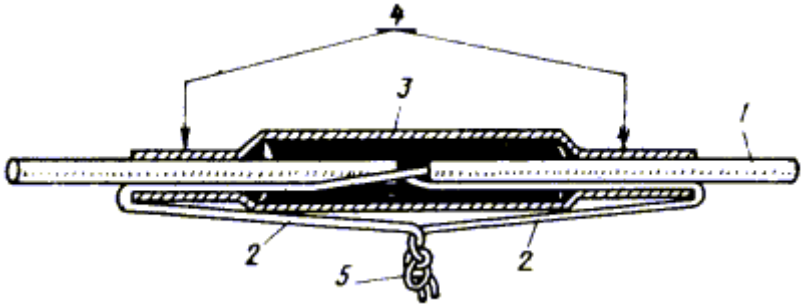


Рис. 11. Сращивание в металлической втулке центральных упрочняющих элементов: 1 – центральный упрочняющий элемент в поливинилхлоридной оболочке; 2 – оголенные пряди упрочняющего элемента; 3 – металлическая обжимная втулка; 4 – обжимаемые шейки втулки; 5 – концы, закрепляемые вязкой двойным узлом

9. Выложить оптические модули петлями запаса (рис.12) и обрезать лишнюю длину.

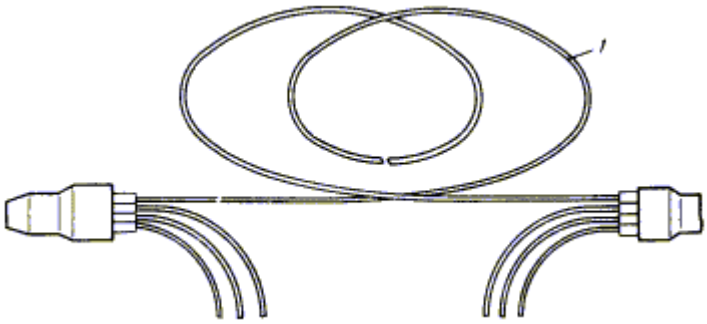


Рис. 12. Выкладка оптических модулей петлями запаса (1) и обрезка излишней длины

10. Удалить оболочки оптических модулей (рис. 13).

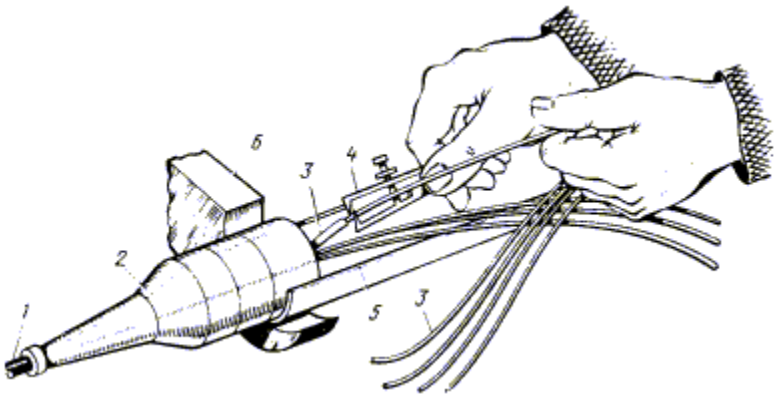


Рис. 13. Удаление оболочки оптических модулей с помощью специального приспособления: 1 – оптический кабель; *2* – полиэтиленовый конус; .3 – оптические модули в оболочке; 4 – приспособление для удаления оболочки; 5 – нижняя половина опорного металлического желобка; 6 – кабельная консоль

11. Надвинуть на оптические волокна кабеля с одной стороны термоусаживаемые гильзы с герметизирующим заполнителем.

12. Удалить с оптического волокна внешнее защитное покрытие (рис. 14).

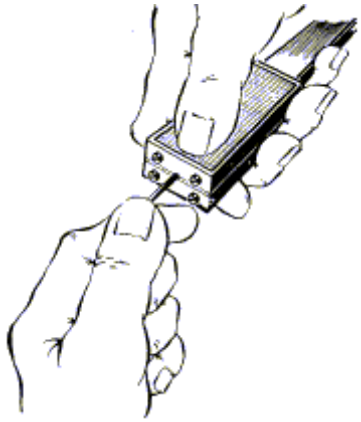


Рис. 14. Удаление с оптических волокон внешнего защитного покрытия

13. Удалить с оптического волокна внутреннее защитное покрытие (рис. 15). Один из вариантов комбинированного приспособления для удаления с оптических волокон защитных покрытий приведен на рис.16.

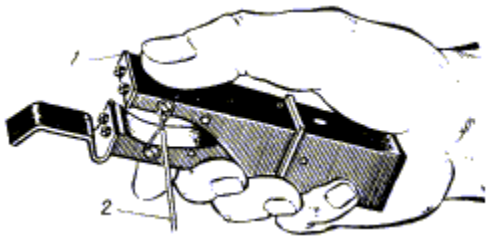


Рис. 15. Удаление с оптических волокон внутреннего защитного покрытия: 1 – приспособление для удаления покрытий; 2 – оптическое волокно с внутренним покрытием

-

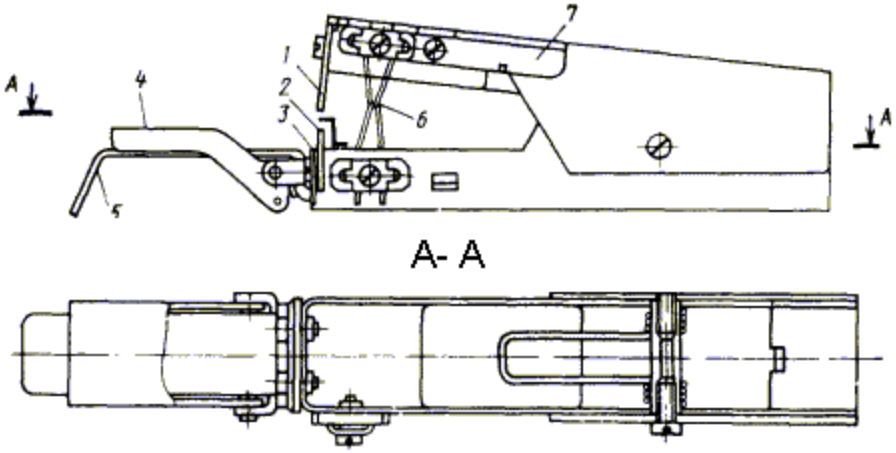


Рис.16. Приспособление для удаления с оптических волокон защитных покрытий: 1 – верхний нож; 2 – направляющая пластина; 3 – нижний нож; 4 – крышка выдвижной планки; 5 – выдвижная планка; 6 – две лески; 7 – рычаг натяжения лесок

14. Сколоть волокна на обоих сращиваемых концах модулей (рис.17) с помощью приспособления, приведенного на рис.18.

Рис. 17. Скол оптического волокна

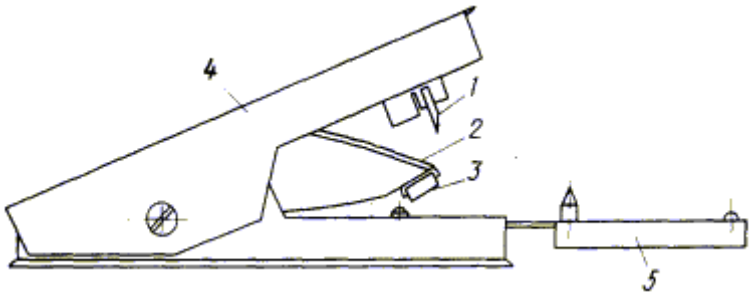


Рис.18. Приспособление для скола волокон: 1 – лезвие ножа; 2 – держатель; 3 – лапка держателя; 4 – верхний рычаг; 5 – пластина

15. Заложить сращиваемые пары оптических волокон в сварочный аппарат УСВ (рис. 19).

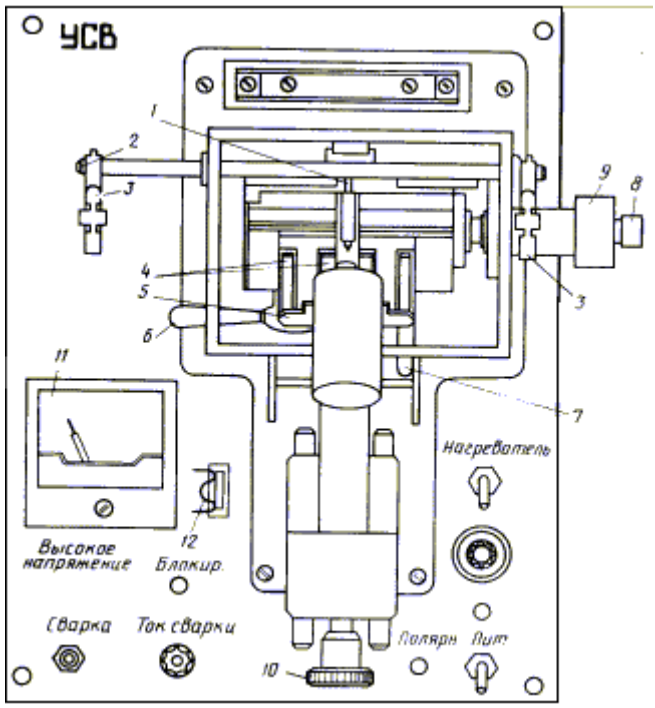


Рис. 19. Общий вид панели устройства для сварки волокон оптических кабелей (УСВ): 1 – электрод; 2 – держатель; 3 – зажимы держателя; 4 – зажимы блоков узла крепления и перемещения волокон; 5 – кнопки с фиксаторами для отжатия зажимов блоков; 6 – ручка горизонтального перемещения волокон; 7 – ручка вертикального перемещения волокон; 8 – ручка перемещения одного волокна; 9 – ручка перемещения двух волокон; 10 – ручка крепления микроскопа; 11 – миллиамперметр; 12 – гнездо включения освещения места сварки

16. Подогнать в горизонтальной и вертикальной плоскостях (юстировка) торец стороны *b* к торцу стороны *a* под контролем микроскопа, вмонтированного в устройство УСВ.

17. Подать высокое напряжение на соответствующие электроды устройства УСВ и сварить торцы волокон в электрической дуге.

18. Надвинуть на сросток волокон термоусаживаемую гильзу с герметизирующим заполнителем.

19. Прогреть и усадить гильзы над нагревательной электроспиралью устройства УСВ.

20. Подготовить и сварить аналогичным способом все оптические волокна кабеля.

21. Выложить все сращенные оптические волокна в муфте петлями; скрепить общей вязкой все волокна в муфте (рис 20).

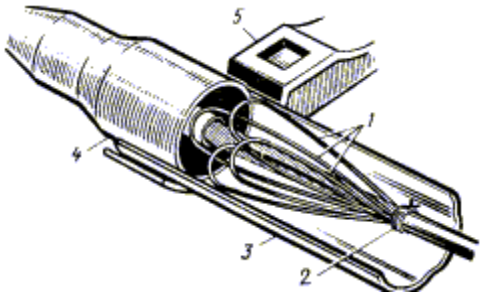


Рис. 6.20. Скрепление волокон в муфте общей вязкой:
1 – петли сращенных волокон; 2 – общая вязка; 3 – металлический желобок; 4 – полиэтиленовый корпус муфты; 5 – кабельная консоль

22. Наложить на муфту верхнюю половину металлического желобка.

23. Надвинуть на желобки и конусы два полиэтиленовых цилиндра.

24. Надвинуть на муфту три отрезка термоусаживаемых трубок с подклеивающим составом.

25. Прогреть и усадить три отрезка термоусаживаемых трубок на стыках муфты.

26. Выложить и закрепить муфты на консолях колодца. Общий вид готовой муфты показан на рис. 21.

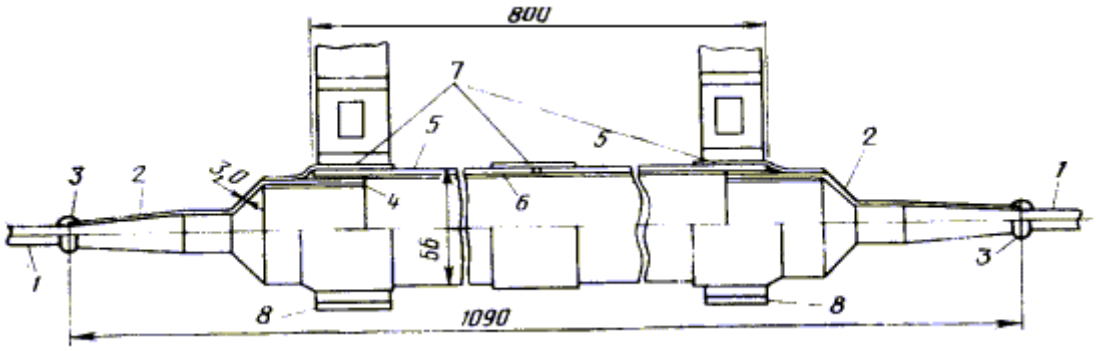


Рис. 21. Готовая муфта: 1 – оптический кабель; 2 – полиэтиленовые конусы; 3 – приварка конусов к оболочке кабелей методом наплавления полиэтиленовой ленты под стеклолентой; 4 – опорные стальные втулки; 5 – полиэтиленовые цилиндры; 6 – металлический желобок; 7 – пояски из отрезков термоусаживаемых трубок 80/40; 8 – кабельные консоли

В ходе монтажа осуществляются оперативные и контрольные измерения. Основными измерительными приборами служат оптические тестеры и рефлектометры, которыми контролируется затухание светового потока в сростке волокон.

Время выполнения работы 90 мин;
Контрольные вопросы

1. Приведите классификацию оптических кабелей связи.

2. Почему длины волн излучением l =1,3 мкм, l = 1,55 мкм считается наиболее перспективными в ВОСП?
3. Какие материалы используются для изготовления оптических волокон?
4. Какой режим работы волоконного световода называется одномодовым и какой многомодовым?
5. Перечислите методы соединения оптических волокон между собой.
6. Какие узлы входят в состав волоконно-оптической системы передачи?
7. Приведите порядок выполнения операций при сращивании оптических волокон.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*
1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ

Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 4 «Исследование типов интерфейсов данных»

Цель работы исследование возможных типов интерфейсов;

В процессе занятия решаются следующие задачи:

1. изучение типов пользовательских интерфейсов, моделей пользовательского интерфейса, приобретение практических навыков построения моделей интерфейсов.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Пользовательский интерфейс. *Пользовательский интерфейс* представляет собой совокупность программных и аппаратных средств, обеспечивающих взаимодействие пользователя с компьютером.

Различают процедурно-ориентированный и объектно-ориентированный подходы к разработке интерфейсов.

Процедурно-ориентированные интерфейсы используют традиционную модель взаимодействия с пользователем, основанную на понятиях «процедура» и «операция». В рамках этой модели программное обеспечение предоставляет пользователю возможность выполнения некоторых *действий,* для которых пользователь определяет соответствующие данные и следствием выполнения которых является получение желаемых результатов. Различают процедурно-ориентированные интерфейсы трех типов: *примитивные*, *меню* и *со свободной навигацией*.

Объектно-ориентированные интерфейсы используют модель взаимодействия с пользователем, ориентированную на манипулирование *объектами* предметной области. В рамках этой модели пользователю предоставляется возможность напрямую взаимодействовать с каждым объектом и инициировать выполнение операций, в процессе которых взаимодействуют несколько объектов. Задача пользователя формулируется как целенаправленное изменение некоторого объекта, имеющего внутреннюю структуру, определенное содержание и внешнее символьное или графическое представление. Пользователю предоставляется возможность создавать объекты, изменять их параметры и связи с другими объектами, а также инициировать взаимодействие этих объектов. Объектно-ориентированные интерфейсы пока представлены только интерфейсом *прямого манипулирования.*

Примитивный интерфейс. *Примитивным* называют интерфейс, который организует взаимодействие с пользователем в консольном режиме. Обычно такой интерфейс реализует конкретный сценарий работы программного обеспечения, например: ввод данных - решение задачи - вывод результата. Единственное отклонение от последовательного процесса, которое обеспечивается данным интерфейсом, заключается в организации цикла для обработки нескольких наборов данных. В настоящее время подобные интерфейсы используют только в процессе обучения программированию или в тех случаях, когда вся программа реализует одну функцию (например, в некоторых системных утилитах).

Интерфейс-меню. *Интерфейс-меню*, в отличие от примитивного интерфейса, позволяет выбирать пользователю необходимые операции из специального списка, выводимого программой. Эти интерфейсы предполагают реализацию множества сценариев работы, последовательность действий в которых определяется пользователем.

Различают одноуровневые и иерархические меню. Первые используют для сравнительно простого управления вычислительным процессом, когда вариантов немного (не более 5–7), и они включают операции одного типа, например, **Создать**, **Открыть**, **Закрыть** и т. п. Вторые используют при большом количестве вариантов или их очевидных различиях, например, операции с файлами и операции с данными, хранящимися в этих файлах.

В настоящее время интерфейсы-меню также используют редко и только для сравнительно простого программного обеспечения или в разработках, которые должны быть выполнены по структурной технологии и без использования специальных библиотек.

Интерфейс со свободной навигацией. *Интерфейс со свободной навигацией* также называют *графическим пользовательским интерфейсом* (Graphic User Interface – GUI) или *интерфейсомWYSIWYG* (What You See Is What You Get – что видишь, то и получишь, т. е. что пользователь видит на экране, то он и получит при печати).

Интерфейс со свободной навигацией обеспечивает возможность осуществления любых допустимых в конкретном состоянии операций, доступ к которым возможен через различные интерфейсные компоненты. Существенной особенностью интерфейсов данного типа является способность изменяться в процессе взаимодействия с пользователем, предлагая выбор только тех операций, которые имеют смысл в конкретной ситуации.

Интерфейс прямого манипулирования. Этот тип интерфейса предполагает, что взаимодействие пользователя с программным обеспечением осуществляется посредством выбора и перемещения*пиктограмм,* соответствующих объектам предметной области. При этом слово «объект» означает модель реальной системы или процесса, базу данных, текст и т. п.

Элементы интерфейса данного типа включены в пользовательский интерфейс Windows. Например, пользователь может «взять» файл и «переместить» его в другую папку. Таким образом, он инициирует выполнение операции перемещения файла.

Модели интерфейса. Существует три различные модели пользовательского интерфейса: модель программиста, модель пользователя и программная модель.

Программист, разрабатывая пользовательский интерфейс, исходит из того, управление какими операциями ему необходимо реализовать в пользовательском интерфейсе и как это осуществить. В модель программиста входят:

– платформа;

– операционная система;

– подход к разработке;

– методы разработки;

– среда и язык разработки;

– спецификации и т.п.

Пользовательская модель интерфейса – это совокупность обобщенных представлений конкретного пользователя или некоторой группы пользователей о процессах, происходящих во время работы программы или программной системы. Эта модель базируется на *особенностях* опыта конкретных пользователей. Для изучения этих особенностей используют опросы, тесты и даже фиксируют последовательность действий, осуществляемых в процессе выполнения некоторых операций, на пленку. В модель пользователя входят:

– интуитивные модели;

– формальные модели;

– задачи;

– процессы;

– инструменты;

– результаты и т.п.

Приведение в соответствие моделей пользователя и программиста, а также построение на их базе программной модели интерфейса – задача не тривиальная. В программную модель входят:

– модель программиста;

– модель пользователя;

– тип интерфейса;

– метафоры;

– символы и т.п.

Интуитивные модели выполнения операций в предметной области должны стать основой для разработки интерфейса, а потому в большинстве случаев их необходимо уточнять и совершенствовать. Именно нежелание или невозможность следования интуитивным моделям выполнения операций приводит к созданию искусственных надуманных интерфейсов, которые негативно воспринимаются пользователями.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Используя информационные источники, укажите основные характеристики интерфейсов:

1.V.24	**12. RS-485**
2. V.35	**13. Fast ATA-2**
3. V.36	**14. Ultra DMA/33**
4. X.21	**15. AT-BUS**
5. G.703	**16.LAPI**
6. FXS	**17.SSI**
7. FXO	**18.SATA**
8. E&M	**19.MIDI**
9. X20	**20.ISA**
10. PS/2	**21.AGP**
11. FireWire EEE1394b	

Создать презентацию, с указанием основных характеристик стандартов.

Время выполнения работы 90 мин;

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

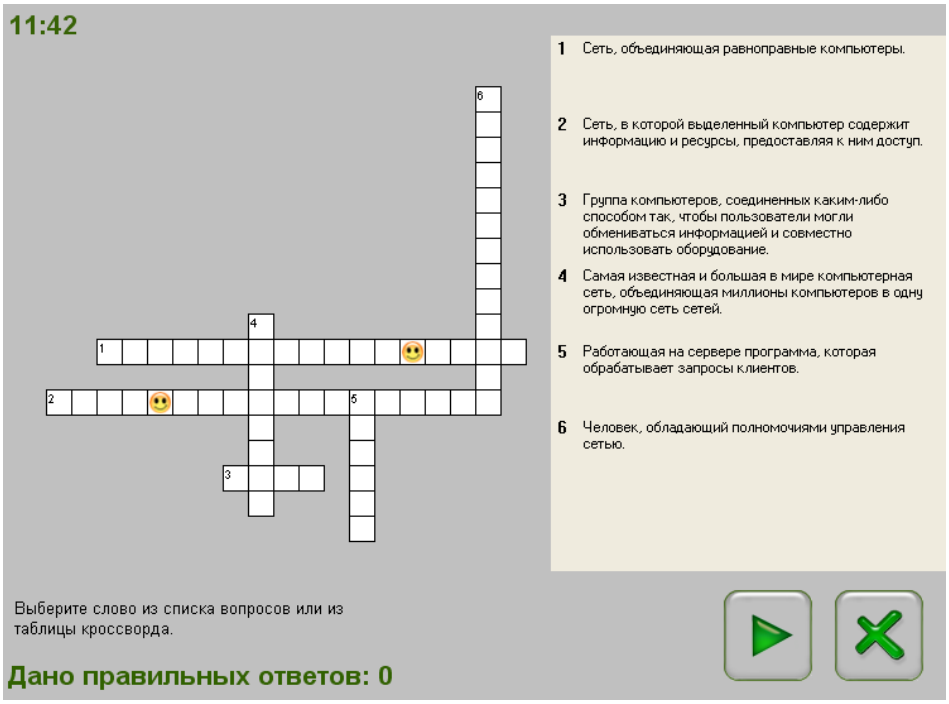
Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Кроссворд



Критерии оценивания

Кроссворд разгадан на:

100%- «5»

75% - «4»

60% -«3»

Кроссворд

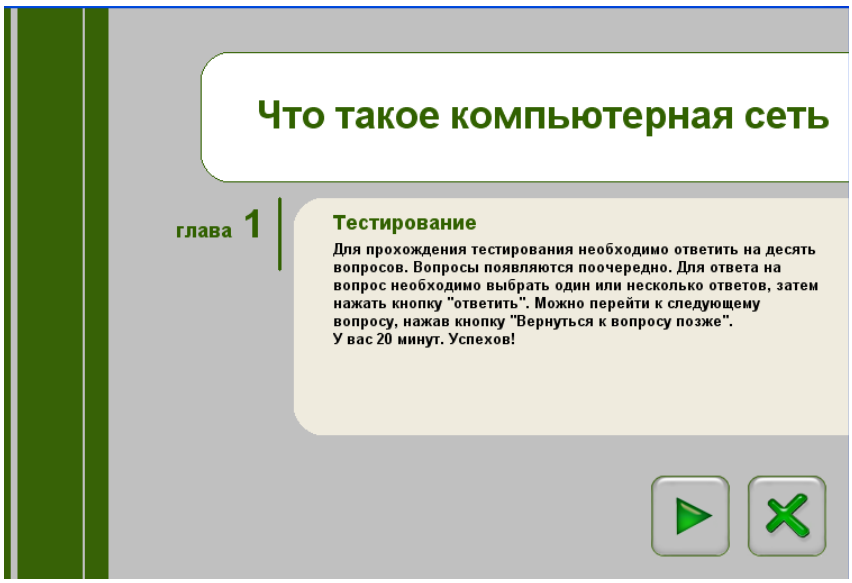
Критерии оценивания

Кроссворд разгадан на:
100%- «5»
75% - «4»
60% -«3»

Кроссворд

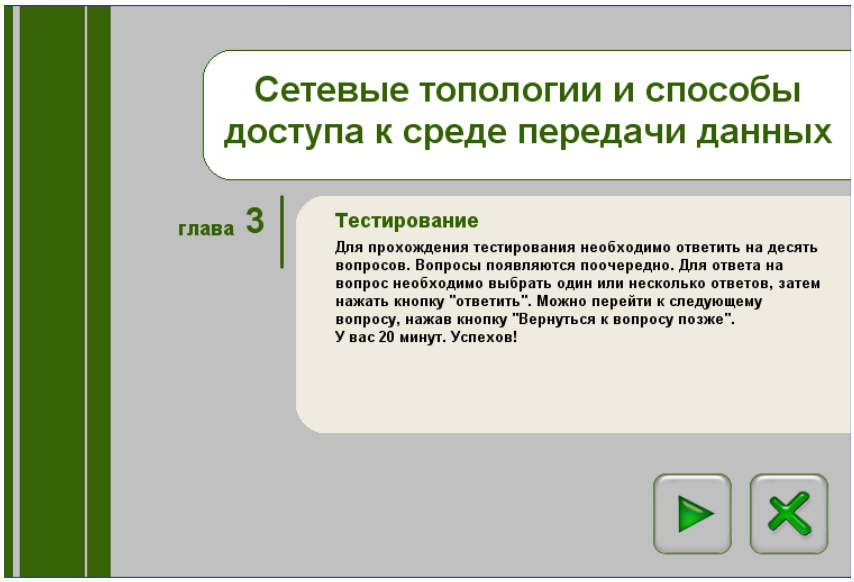
Критерии оценивания
Кроссворд разгадан на:
100%- «5»
75% - «4»
60% -«3»

Тест



Критерии оценивания
Работа выполнена на:
100%- «5»
75% - «4»
60% -«3»

Тест



Критерии оценивания
Работа выполнена на:
100%- «5»
75% - «4»
60% -«3»

Тема 1.2.

Сетевое передающее оборудование

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 5 «Изучение протокола IP»

Цель работы: Изучить способы адресации в IP сетях.

В процессе занятия решаются следующие задачи:

1. формирование навыков определения адресов подсетей;
2. формирование навыков структурирования сетей с использованием масок.

Краткие теоретические и справочно-информационные материалы по теме занятия.
Связь с проектом

Для успешного решения задач администрирования необходимо хорошо разбираться в системе IP-адресации. Знание принципов использования масок и структуризации сетей поможет грамотно решать многие вопросы настройки локальной сети.

Задание 1. Определить, находятся ли два узла А и В в одной подсети или в разных подсетях, если адреса компьютера А и компьютера В соответственно равны: 26.219.123.6 и 26.218.102.31, маска подсети 255.192.0.0.

Указания к выполнению

1. Переведите адреса компьютеров и маску в двоичный вид.
2. Для получения двоичного представления номеров подсетей обоих узлов выполните операцию логического умножения AND над IP-адресом и маской каждого компьютера.
3. Двоичный результат переведите в десятичный вид.
4. Сделайте вывод.

Процесс решения можно записать следующим образом:

Компьютер А:

IP-адрес: 26.219.123.6 = 00011010. 11011011. 01111011. 00000110

Маска подсети: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Компьютер В:

IP-адрес: 26.218.102.31 = 00011010. 11011010. 01100110. 00011111

Маска подсети: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Получаем номер подсети, выполняя операцию AND над IP-адресом и маской подсети.

Компьютер А:

AND	00011010. 11011011. 01111011. 00000110 11111111. 11000000. 00000000. 00000000 00011010. 11000000. 00000000. 00000000 26 192 0 0

Компьютер В:

AND	00011010. 11011010. 01100110. 00011111 11111111. 11000000. 00000000. 00000000 00011010. 11000000. 00000000. 00000000 26 192 0 0

Ответ: номера подсетей двух IP-адресов совпадают, значит компьютеры А и В находятся в одной подсети. Следовательно, между ними возможно установить прямое соединение без применения шлюзов.

Задание 2. Определить количество и диапазон IP-адресов в подсети, если известны номер подсети и маска подсети.

Номер подсети – 26.219.128.0, маска подсети – 255.255.192.0.

Указания к выполнению

1. Переведите номер и маску подсети в двоичный вид.

Номер подсети: 26.219.128.0 = 00011010. 11011011. 10000000. 00000000
Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

2. По маске определите количество бит, предназначенных для адресации узлов (их значение равно нулю). Обозначим их буквой К.
3. Общее количество адресов равно $2^К$. Но из этого числа следует исключить комбинации, состоящие из всех нулей или всех единиц, так как данные адреса являются особыми. Следовательно, общее количество узлов подсети будет равно $2^К – 2$.
   В рассматриваемом примере К = 14, $2^К – 2$ = 16 382 адресов.
4. Чтобы найти диапазон IP-адресов нужно найти начальный и конечный IP-адреса подсети. Для этого выделите в номере подсети те биты, которые в маске подсети равны единице.
   Это разряды, отвечающие за номер подсети. Они будут совпадать для всех узлов данной подсети, включая начальный и конечный:

Номер подсети: 26.219.128.0 = **00011010. 11011011. 10**000000. 00000000
Маска подсети: 255.255.192.0 = **11111111. 11111111. 11**000000. 00000000

5. Чтобы получить начальный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить *нулями*, за исключением крайнего правого бита, который должен быть равен единице. Полученный адрес будет первым из допустимых адресов данной подсети:
Начальный адрес: 26.219.128.1 = **00011010. 11011011. 10**000000. 00000001
Маска подсети: 255.255.192.0 = **11111111. 11111111. 11**000000. 00000000

6. Чтобы получить конечный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить *единицами*, за исключением крайнего правого бита, который должен быть равен нулю. Полученный адрес будет последним из допустимых адресов данной подсети:
Конечный адрес: 26.219.191.254 = **00011010. 11011011. 10**111111. 11111110
Маска подсети: 255.255.192.0 = **11111111. 11111111. 11**000000. 00000000

Ответ: Для подсети 26.219.128.0 с маской 255.255.192.0: количество возможных адресов: 16 382,
диапазон возможных адресов: 26.219.128.1 – 26.219.191.254.

Задание 3. Организации выделена сеть класса С: 212.100.54.0/24.
Требуется разделить данную сеть на 4 подсети с количеством узлов в каждой не менее 50.
Определить маски и количество возможных адресов новых подсетей.

Указания к выполнению

1. В сетях класса С (маска содержит 24 единицы – 255.255.255.0) под номер узла отводится 8 бит, т. е. сеть может включать 28 – 2 = 254 узла.
2. Требование деления на 4 подсети по 50 узлов в каждой может быть выполнено: 4·50 = 200 < 254. Однако число узлов в подсети должно быть кратно степени двойки. Относительно 50 ближайшая б*о*льшая степень – 26 = 64. Следовательно, для номера узла нужно отвести 6 бит, вместо 8, а маску расширить на 2 бита – до 26 бит (см. рис. 3).
3. В этом случае вместо одной сети с маской 255.255.255.0 образуется 4 подсети с маской 255.255.255.192 и количеством возможных адресов в каждой – 62 (не забывайте про два особых адреса).
4. Номера новых подсетей отличаются друг от друга значениями двух битов, отведенных под номер подсети. Эти биты равны 00, 01, 10, 11.

Ответ: маска подсети – 255.255.255.192, количество возможных адресов – 62.

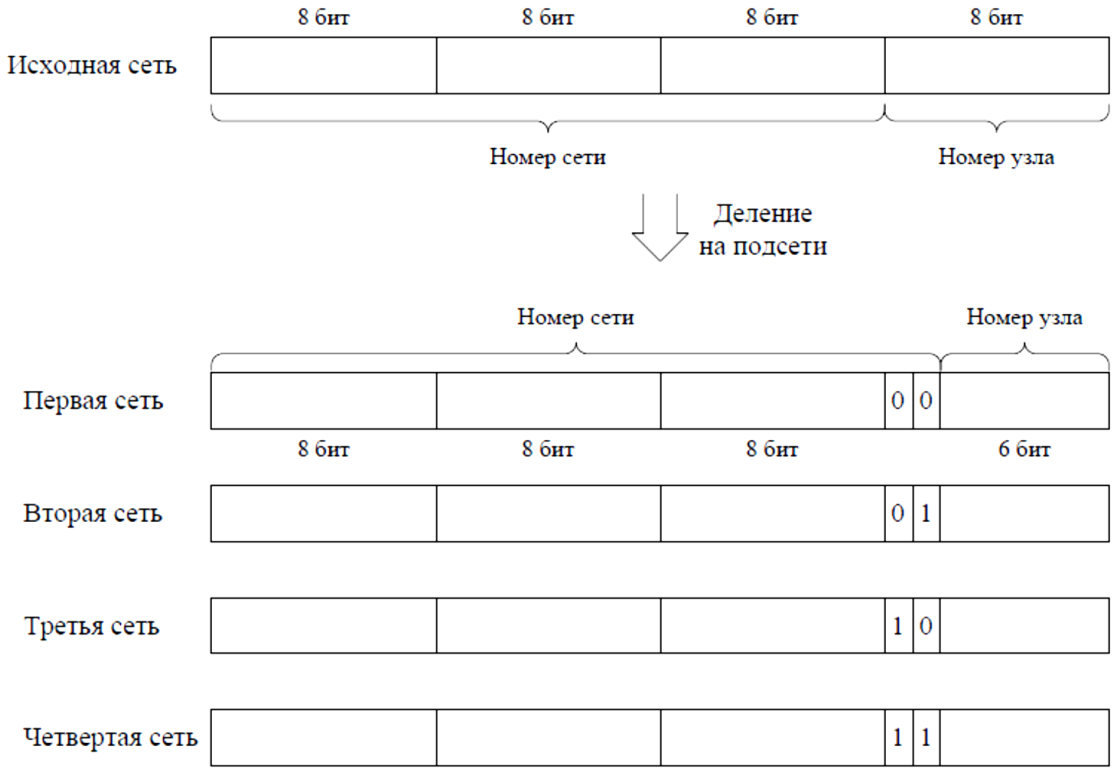


Рис. 3. Адреса подсетей после деления

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Самостоятельная работа

Задание 1. Определить, находятся ли два узла A и B в одной подсети или в разных подсетях.

1. IP-адрес компьютера A: 94.235.16.59;
IP-адрес компьютера B: 94.235.23.240;
Маска подсети: 255.255.240.0.
2. IP-адрес компьютера A: 131.189.15.6;
IP-адрес компьютера B: 131.173.216.56;
Маска подсети: 255.248.0.0.
3. IP-адрес компьютера A: 215.125.159.36;
IP-адрес компьютера B: 215.125.153.56;
Маска подсети: 255.255.224.0.

Задание 2. Определить количество и диапазон адресов узлов в подсети, если известны номер подсети и маска подсети.

1. Номер подсети: 192.168.1.0, маска подсети: 255.255.255.0.
2. Номер подсети: 110.56.0.0, маска подсети: 255.248.0.0.
3. Номер подсети: 88.217.0.0, маска подсети: 255.255.128.0.

Задание 3. Определить маску подсети, соответствующую указанному диапазону IP-адресов.

1. 119.38.0.1 – 119.38.255.254.
2. 75.96.0.1 – 75.103.255.254.
3. 48.192.0.1 – 48.255.255.254.

Задание 4. Организации выделена сеть класса B: 185.210.0.0/16.

Определить маски и количество возможных адресов новых подсетей в каждом из следующих вариантов разделения на подсети:

1. Число подсетей – 256, число узлов – не менее 250.
2. Число подсетей – 16, число узлов – не менее 4000.

3. Число подсетей – 5, число узлов – не менее 4000. В этом варианте укажите не менее двух способов решения.

Время выполнения работы 180 мин;

Контрольные вопросы

1. Может ли быть IP-адрес узла таким? Укажите неверные варианты IP-адрес. Ответ обоснуйте.
• 192.168.255.0
• 167.234.56.13
• 224.0.5.3
• 172.34.267.34
• 230.0.0.7
• 160.54.255.255
2. Может ли маска подсети быть такой? Укажите неверные варианты. Ответ обоснуйте.
• 255.254.128.0
• 255.255.252.0
• 240.0.0.0
• 255.255.194.0
• 255.255.128.0
• 255.255.255.244
• 255.255.255.255
3. Можно ли следующие подсети разделить на N подсетей. Если это возможно, то укажите варианты разбиения с максимально возможным количеством подсетей или узлов в каждой подсети. Ответ обоснуйте.
• 165.45.67.0, маска 255.255.255.224, N=3
• 235.162.56.0, маска 255.255.255.224, N=6
• 234.49.32.0, маска 255.255.255.192, N=3

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.

6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ
Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 6 «Разложение IP по подсетям»

Цель работы: изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети

В процессе занятия решаются следующие задачи:
1. Формирование разложения IP по подсетям.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Сетевой уровень отвечает за возможность доставки пакетов по сети передачи данных – совокупности сегментов сети, объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети.

IP - адреса представляют собой 32-х разрядные двоичные числа. Для удобства их записывают в виде четырех десятичных чисел, разделенных точками. Каждое число является десятичным эквивалентом соответствующего байта адреса (для удобства будем записывать точки и в двоичном изображении).

Например, IP–адрес 192.168.200.47 является десятичным эквивалентом двоичного адреса 11000000.10101000.11001000.00101111

Иногда применяют десятичное значение IP-адреса. Его легко вычислить: $192*256^3+168*256^2+200*256+47=3232286767$

Существует несколько правил об особенностях IP-адресов:

- если IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;
- если в поле номера сети стоят 0, то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет;

- если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);
- если в поле адреса назначения стоят сплошные 1, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast);

адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback

Адрес получателя должен содержать в себе:

1. адрес (номер) подсети;
2. адрес (номер) хоста (узла) внутри подсети

Часто (например, маршрутизация осуществляется на основании номера сети) возникает необходимость разделить IP - адрес на эти две части: номер подсети и номер узла. Для разделения IP – адреса используют один из способов:

1. использование фиксированной границы – (не нашел применения; весь адрес делится на 2 части фиксированной длины, в одной из них всегда размещается номер сети, в другой – номер узла)
2. использование маски, которая позволяет максимально гибко установить границу между номером сети и номером узла.
3. использование классов адресации (самый распространенный, компромисс между первым и вторым способом). Вводится 5 классов: A,B,C,D,E. A,B,C – используют для адресации сетей; D,E – имеют специальное назначение. Для каждого класса определены границы между номером сети и номером узлов, которые хранятся в таблицах:

Диапазоны адресов для всех классов сетей:

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число машин в сети
A	0	1.0.0.0	126.0.0.0	$2^{24} = 16\,777\,216$
B	10	128.0.0.0	191.255.0.0	$2^{16} = 65\,536$
C	110	192.0.1.0	223.255.255.0	$2^{8} = 256$
D	1110	224.0.0.0	239.255.255.255	Групповые адреса
E	11110	240.0.0.0	247.255.255.255	Зарезервировано для будущих применений

Диапазон адресов сетей и хостов классов A и C:

Класс	Диапазон номера сети	Диапазон номеров узлов
A	1 – 126	0.0.1 – 255.255.254
B	128.0 – 191.255	0.1 – 255.254
C	192.0.0 – 223.255.255	1-254

Чтобы получить из IP-адреса номер сети и номер узла надо разбить адрес на 2 соответствующие части (см. таблицу) и дополнить каждую из них нулями до полных 4 байт.

Пример:

Дан IP-адрес класса B: 129.64.134.5. Так как для класса B IP-адрес разбивается пополам, то номер сети равен 129.64.0.0; номер узла равен 0.0.134.5.

Использование масок в IP-адресации

Маска - это 4-байтное число, которое используется в паре с IP-адресом. Двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресах использоваться как номер сети.

Маска - это число, применяемое в паре с IP – адресом, причем двоичная запись маски содержит непрерывную последовательность единиц в тех разрядах, которые должны в IP – адресе интерпретироваться как номер сети, а остальные - нули.

Поэтому маску часто записывают в виде числа единиц в ней содержащихся.
255.255.248.0 (11111111.11111111.11111000.00000000) – является правильной маской подсети (/21), а 255.255.250.0 (11111111.11111111.11111010.00000000) – является неправильной, недопустимой.

Если маску «наложить» на IP – адрес, то граница между единицами и нулями в маске станет границей номер сети и номер узла IP – адреса.

Для стандартных классов сетей маски имеют следующие значения:

255.0.0.0 - маска для сети класса A, 255.255.0.0 - маска для сети класса B, 255.255.255.0 - маска для сети класса C.

В масках, которые использует администратор для увеличения числа подсетей, количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты.

Пример1: IP-адрес - 194.110.345.185, маска - 255.255.255.192. Если не учитывать маску подсети: номер сети - 194.110.245.0, а номер узла - 0.0.0.185. С учетом маски - номер сети - 194.110.345.128, а номер узла 0.0.0.57 Пример2: маска имеет значение 255.255.192.0 (11111111 11111111 11000000 00000000). И пусть сеть имеет номер 129.44.0.0 (10000001 00101100 00000000 00000000), из которого видно, что она относится к классу B. После наложения маски на этот адрес число разрядов, интерпретируемых как номер сети, увеличилось с 16 до 18, то есть администратор получил возможность использовать вместо одного, централизованно заданного ему номера сети, четыре:
129.44.0.0 (10000001 00101100 00000000 00000000)
129.44.64.0 (10000001 00101100 01000000 00000000)
129.44.128.0 (10000001 00101100 10000000 00000000)
129.44.192.0 (10000001 00101100 11000000 00000000)

Пример3: IP-адрес 129.44.141.15 (10000001 00101100 10001101 00001111), который по стандартам IP задает номер сети 129.44.0.0 и номер узла 0.0.141.15, теперь, при использовании маски, будет интерпретироваться как пара:

129.44.128.0 - номер сети,
0.0. 13.15 - номер узла.

Таким образом, установив новое значение маски, можно заставить маршрутизатор по-другому интерпретировать IP-адрес.

Пример4: пусть ваша сеть относится к классу B. В одной сети циркулирует единый трафик. Но среди всех станций сети есть некоторые, слабо взаимодействующие между собой. Эти станции желательно бы изолировать в разных сетях. Пусть это будут узел

129.34.17.15 и узел 129.34.20.01, которые в исходной ситуации относятся к одной сети класса B с номером 129.34. Если задать в качестве маски число 255. 255.255.0, то адреса этих двух узлов будут интерпретироваться маршрутизаторами как адреса узла 15 сети класса C с номером
129.34.17 и узла 01 сети класса C с номером 129.34.20. Извне сеть по-прежнему будет выглядеть как единая сеть класса B, а на местном уровне это будет несколько отдельных сетей класса C.

Нетрудно увидеть, что максимальный размер подсети может быть только степенью двойки (двойку надо возвести в степень, равную количеству нулей в маске).

При передаче пакетов используются правила маршрутизации, главное из которых звучит так: «Пакеты участникам своей подсети доставляются напрямую, а остальным – по другим правилам маршрутизации».

Таким образом, требуется определить, является ли получатель членом нашей подсети или нет.

Алгоритм определения диапазона адресов подсети (из определения маски).

1. Перевести и записать IP-адрес в двоичной системе счисления.
2. Перевести маску и записать ее в двоичной системе счисления.
3. «Наложить» маску на IP-адрес и записать диапазон номеров подсети в двоичной системе счисления.
4. Перевести и записать диапазон из двоичной системы счисления в десятичную.

Задача. Дан IP-адрес 192.168.200.47 /20 (маска подсети 20). Определить диапазон номеров (адресов) подсети.

Решение.

1. 192.168.200.47 переведем в двоичную систему счисления:

* Алгоритм перевода числа из десятичной системы счисления в двоичную:

1. Делим число на 2, остаток от деления может быть 1 или 0, значение остатка присваивается младшему (самому правому) знаку искомой двоичной записи.
2. Полученное число вновь делим на 2, остаток равен значению следующего по старшинству знака.
3. Повторить п.2 пока частное не станет меньше двух, частное от последнего деления равно значению старшего знака, остаток – второму по старшинству знаку.

Перевод числа 192 из десятичной записи в двоичную:

Пояснения:

192	96	48	24	12	6	3	1
0	0	0	0	0	0	1	1

192 – четное, значит, пишем – 0; 192/2=96 – четное, пишем – 0; 96/2=48 – четное, пишем – 0;

Результат записываем из таблицы слева направо: 11000000.

24/2=12 – четное, пишем – 0; 12/2=6 – четное, пишем – 0; 6/2=3 – нечетное, пишем 1; 3/2=1 – нечетное, пишем 1.

Аналогично переводим 168 в двоичную систему счисления и получаем: 10101000. Аналогично переводим 200 в двоичную систему счисления и получаем: 11001000

Аналогично переводим 47 в двоичную систему счисления и получаем: 00101111 (впереди недостающие разряды дописываем нулями до 4 байт)

Записываем 192.168.200.47 в двоичной форме: **11000000.10101000.11001000.00101111 – IP-адрес**

2. Записываем маску 20 в двоичной форме. Для этого пишем 20 нулей с разделением на 4 байта, оставшиеся 12 знаков дописываем нулями:

11111111.11111111.11110000.00000
000 – маска 20.

3. «Накладываем» маску на IP-адрес и выявляем диапазон номеров подсети:

11000000.10101000.11001000.00101111
11111111.11111111.11110000.00000000

Граница единиц и нулей попадает на середину третьего числа; все что оказалось под единицами остается без изменений, значит первые два числа в IP-адресе останутся без изменений и надо получить только третье число и четвертое.

Для того чтобы определить начало диапазона надо в IP-адресе все числа от границы заполнить нулями, для того, чтобы определить конец диапазона надо в IP-адресе все числа от границы заполнить единицами, то есть:

Диапазон адресов подсети будет такой:

от 11000000.10101000.11000000.00000000

до 11000000.10101000.11001111.11111111

4. Переведем и запишем полученный диапазон номеров подсети из двоичной системы счисления в десятичную:

$11000000 = 1*2^7+1*2^6+0*2^5+0*2^4+0*2^3+0*2^2+0*2^1+0*2^0=2^7+2^6=192$

$00000000 = 0$

$11001111 = 1*2^7+1*2^6+0*2^5+0*2^4+1*2^3+1*2^2+1*2^1+1*2^0=2^7+2^6+2^3+2^2+2^1+2^0=207$

$11111111 = 1$

Значит, диапазон адресов подсети будет такой: от 192.168.192.0 до 192.168.207.255

Порядок работы

Задания для выполнения:

1. Какие адреса из приведенного ниже списка являются допустимыми адресами хостов и почему: 0.10.10.10
   10.0.10.10

   10.10.0.10

   10.10.10.10

127.0.127.127

127.0.127.0

255.0.200.1

1.255.0.0

2. Перечислите все допустимые маски, по какому принципу они получаются.
3. Определите диапазоны адресов подсетей (даны адрес хоста и маска подсети): 10.212.157.12/24
27.31.12.254/31

192.168.0.217/28

10.7.14.14/16

4. Какие из адресов
241.253.169.212

243.253.169.212

242.252.169.212

242.254.168.212

242.254.178.212

242.254.170.212

242.254.169.211

242.254.179.213

будут достигнуты напрямую с хоста 242.254.169.212/21. Определите диапазон адресов в его подсети.

5. Посмотрите параметры IP на своем компьютере с помощью команды ipconfig. Команда ipconfig отображает краткую информацию, т.е. только IP-адрес, маску подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.
Определите диапазон адресов и размер подсети, в которой Вы находитесь. Попробуйте объяснить, почему выбраны такие сетевые параметры, и какие сетевые параметры выбрали бы Вы.

6. Определить к какому классу относятся IP – адреса:

1.	102.54.94.97	8. 203.23.106.33
2.	109.26.17.100	9. 128.10.2.30
3.	130.37.120.25	10. 129.64.134.5
4.	128.10.2.30	11. 132.13.34.15
5.	192.45.66.17	12. 127.255.255.255 - зарезервирован для обозначения обратной связи
6	14.0.0.6	
7	201.22.100.33	

Результаты представить в виде таблицы (все расчеты ниже таблицы)

№ примера	Десятичная форма IP - адреса	Двоичная форма IP - адреса	Принадлежность к классу IP – адресов	Диапазон IP–адресов этого класса	Максимальное количество ПК в сети этого класса

7. Выделить номер подсети и номер узла по заданному IP – адресу и маске подсети: IP – адрес: 129. 64. 134. 5
Маска подсети: 255. 255. 128. 0

8. Дан IP-адрес 198.65.12.67 и маска этой подсети – 255.255.255.240. Определить номер подсети и максимальное число узлов этой подсети.

9. Какие из приведенных ниже адресов не могут быть использованы для узлов Интернета? Ответ обоснуйте. Для верных адресов определите их класс: A,B,C,D,E. Результат представить в виде таблицы.

1. 127.0.0.1
2. 201.13.123.245
3. 226.4.37.105
4. 103.24.254.0
5. 10.234.17.25
6. 154.12.255.255
7. 193.256.1.16
8. 194.87.45.0
9. 195.34.116.255
10. 161.23.45.305
11. 13.13.13.13
12. 204.0.3.1

10.* Какое максимальное количество подсетей теоретически можно иметь, если в вашем распоряжении имеется сеть класса С? Какое значение при этом может иметь маска? Ответ обосновать.

Примечание:

Следует учитывать, что некоторые адреса являются запрещенными или служебными и их нельзя использовать для адресов хостов или подсетей. Это адреса, содержащие:

0 в первом или последнем байте,

255 в любом байте (это широковещательные адреса),

127 в первом байте (внутренняя петля – этот адрес имеется в каждом хосте и служит для связывания компонентов сетевого уровня).

Поэтому доступный диапазон адресов будет несколько меньше.
Диапазон адресов:

10.X.X.X – для больших локальных сетей;

172.16.X.X – для больших локальных сетей, но применяется реже,
192.168.X.X – для маленьких (небольших) локальных сетей,

не может быть использован в сети Internet, т.к. эти адреса отданы для использования в сетях непосредственно не подключенных к глобальной сети.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Какой адрес называется неопределенным IP – адресом?
2. Что обозначает неопределенный IP – адрес?
3. Какой адрес может быть использован **только** в качестве адреса отправителя?
4. Какой адрес называется ограниченным широковещательным?
5. Какой адрес называется широковещательным?
6. Чем отличается ограниченный широковещательный адрес от широковещательного?
7. Какой адрес является внутренним адресом стека протоколов ПК?
8. Для чего он используется?
9. Какая операция называется разделением на подсети?
10. Какая операция называется объединением подсетей?
11. Какой класс IP – адресов используется для корпоративных внутренних сетей предприятия?
12. Чем занимается сетевой уровень?
13. Какие требования предъявляются к сетевой адресации?
14. Можно ли использовать в качестве сетевого MAC-адрес?
15. Что такое маска подсети?
16. Какова структура IP-адреса?
17. Чем определяется размер подсети?
18. Как определить диапазон адресов в подсети?
19. Как определить размер подсети?

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил

9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 7 «FTP-протокол»

Цель работы: ознакомиться с принципами работы текстовых протоколов высших уровней на примере протоколов электронной почты.

В процессе занятия решаются следующие задачи:

1. Изучить основные протоколы высших уровней.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Большинство протоколов высших уровней – текстовые – запросы и ответы передаются в виде текста, т.е. в запросах и ответах могут присутствовать только печатные символы.

Во многих протоколах ответы начинаются со специальной строки, состоящей из трехзначного числа и, возможно, текстового описания типа ответа. Трехзначное число разделяется на две части: 1-ый символ рассматривается как код класса сообщения; два последние – как тип сообщения данной важности.

Коды классов следующие:

1 – информационное сообщение. Обычно игнорируется программными клиентами.

2 – удачное завершение запроса. Рассматривается программами-клиентами как успех обработки запроса и обычно игнорируется.

Часто программы-серверы не различают сообщения первого и второго типа, т.е. информационное сообщение проходит по второй категории.

3 – сообщение об удачной обработке запроса, но требующее дополнительных действий клиента.

4 – ошибка со стороны клиента, т.е. клиент послал запрос, который не может обработать сервер вследствие ошибочности или недостаточности данных.

5 – ошибка со стороны сервера. Клиент послал правильный запрос, но сервер не смог его выполнить в силу каких-то причин.

Трехзначные коды ответов очень удобны для программного распознавания, нет необходимости распознавать текст ответа, который, в общем случае, может прийти на разных языках, достаточно распознать только 3 цифры.

2 Программа TELNET

Для работы с текстовыми протоколами воспользуемся программой TELNET, входящей в состав Windows. Эта программа предназначена для работы с протоколом TELNET, задачей которого является обмен информацией между клиентом и сервером без каких либо преобразований, т.е. организация прозрачного канала между клиентом и сервером.

Синтаксис команды TELNET следующий:

TELNET адрес_сервера [порт]

Если порт не указан, используется 23 - стандартный порт протокола TELNET.

3 Протокол SMTP

Для начала попробуем поработать с протоколом SMTP. Обычно он работает, используя порт 25.

Для наглядности команды пользователя выделены *курсивом*, а ответы сервера – подчеркиванием.

Даем команду на подключение:

telnet 192.168.1.2 25

Получаем ответ

220 home VPOP3 SMTP Server Ready

Работает! Обратите внимание на число 220 в начале строки ответа. Это нормальный ответ, сервер ответил на наш запрос на подключение.

Многие серверы, работающие по текстовым протоколам, поддерживают команду HELP. Проверим.

Help

Дадим серверу неправильный запрос

abrakadabra

500 Command Unrecognised

Как ни странно, но код ответа 5 – ошибка на стороне сервера!

Попробуем написать письмо

Поздороваемся

helo home

250 home VPOP3 SMTP Server - Hello home, pleased to meet you

Укажем отправителя письма

mail from: user1

250 <user1>... Sender ok

Укажем получателя письма

rcpt to: user2

250 <user2>... Recipient ok

Перейдем в режим ввода письма

data

354 Start Mail input, end with <CRLF>.<CRLF>

Обратите внимание на код ответа 354.

Это нормальное завершение, но требуются дополнительные данные – само письмо, которое, как видно, должно заканчиваться строкой, состоящей из одной точки «.».

А теперь само письмо. Формат письма описан стандартами. Их изучение не входит в нашу задачу, но наиболее важные служебные строки вкратце рассмотрим:

Date: Tue, 22 Nov 2005 19:55:07 +0200

Дата создания по GMT и часовой пояс

From: User user1@home.my

От кого

Reply-To: User user1@home.my

Кому отвечать

To: user2@home.my

Кому

Subject: Test

Тема письма

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Информация почтовой программе, как закодировано письмо – с помощью этих строк почтовая программа клиент сможет реализовать шестой уровень – представить информацию пользователю в читабельном виде

Hello user2,

It's a test message.

Best regards,

User mailto:user1@home.my

Само письмо

.

250 OK
Письмо принято!
Теперь выходим
quit
221 home VPOP3 Server Closing Connection

Протокол SMTP (Simple Mail Transfer Protocol) используется для передачи электронной почты от клиента серверу или между серверами. Не содержит встроенных средств идентификации и преобразования.

4 Протокол POP3

Теперь поработаем с протоколом POP3. Обычно он работает, используя порт 110.
Даем команду на подключение:
telnet 192.168.1.2 25
Получаем ответ
+OK VPOP3 Server Ready <1.7b0.435a37>
Работает, но трехсимвольного кода ответа нет!
Попробуем help
help
-ERR Unrecognised command
Видим, что помощи нет, заодно и посмотрели, как сервер отвечает на ошибочный для него запрос.
Как мы знаем, POP3 требует аутентификации, поэтому представимся:
user user2
+OK User Accepted, PASSword required
А теперь пароль.
pass 2
+OK user2 has 1 message(s) (580 octets)
Нам есть почта! Посмотрим.
list
+OK 1 messages (580 octets)
1 580
.
Одно письмо 580 символов. Если бы было несколько писем, было бы несколько строк с указанием номеров и размеров писем. Точка в последней строке показывает, что это окончание ответа.
Теперь прочитаем (получим) первое письмо.
retr 1
+OK 580 octets
Received: from 192.168.200.1 by home ([192.168.200.1] running VPOP3) with SMTP
or <user2>; Tue, 22 Nov 2005 20:31:07 +0200
Date: Tue, 22 Nov 2005 19:55:07 +0200
From: User <user1@home.my>
Reply-To: User <user1@home.my>
To: user2@home.my
Subject: Test
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <VPOP31.3.0c.20051122203134.814.e.1.40132205@home>
X-Server: VPOP3 V1.3.0c - Registered to: Collega

Hello user2,
It's a test message.

Best regards,

User mailto:user1@home.my

.
Служебных полей стало больше – их добавил сервер.
Обратите внимание на последнюю строку ответа
Теперь удалим письмо с сервера, ведь оно уже прочитано:
dele 1
+OK message 1 deleted
Проверим, есть ли что еще
list
+OK 0 messages (0 octets)
.
Ничего нет. А можно и так, для программы это будет более удобным
list 1
-ERR Invalid Message Number
Ну, и теперь выходим
quit
+OK VPOP3 Server Closing Connection

В приведенном выше примере было отправлено письмо от пользователя «user1» пользователю «user2» и получена почта пользователя «user2» с помощью утилиты TELNET, т.е. без использования почтового клиента.

Протокол POP3 (Post Office Protocol) предназначен для получения электронной почты от сервера к клиенту. Содержит средства идентификации клиента, использует факультативные средства преобразования.

5 Протокол FTP

Протокол FTP (File Transfer Protocol) – протокол передачи файлов.

Он использует 20-ый порт для установления соединений и 21-ый порт для установления соединений и передачи файлов. Этот протокол содержит встроенные средства идентификации клиента. Все распознаваемые им команды состоят из 3-х или 4-х символов, являющихся сокращениями или аббревиатурами выполняемых действий.

6 Протокол HTTP

Протокол HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста, т.е. данных разного представления (текст, изображения, видео, звук). Обычно этот протокол работает на 80-ом порту. Он содержит средства идентификации и перекодирования передаваемой информации.

Как видим работа с текстовыми протоколами не представляет особых трудностей. Правда некоторые протоколысодержат большое число команд и чтобы узнать их формат требуется использовать их стандарт и описания RFC.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Во всех заданиях адрес сервера:192.168.1.2
Где необходимо требуется пояснить трехсимвольные коды ответов, например, при первом появлении такого кода.
В пятом и шестом заданиях, после аутентификации (если она необходима) рекомендуется в первую очередь вызвать помощь командой help и посмотреть информацию о других командах, поддерживаемых данным протоколом.

1. Получить у преподавателя адрес сервера электронной почты, имена и пароли пользователей. Отправить и получить почту без использования почтового клиента (для аутентификации использовать

имя пользователя типа: user№, тогда паролем будет №, в качестве номера № использовать номер Вашей подгруппы).

2. Поработать с POP3 без аутентификации. Сделать соответствующие выводы.
3. Определить, является ли протокол FTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.
4. Подключиться к HTTP серверу и определить, является ли протокол HTTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.
5. Получить у преподавателя адрес и порт неизвестного для вас протокола и сервера. Получите список его команд, объясните, что делает каждая команда. Попробовать некоторые из них и проанализировать результаты.(использовать 1000-ый порт, при аутентификации имя пользователя и пароль: admin).
6. Поработайте с FTP-сервером с помощью TELNET и программы FTP. Объясните и подтвердите на конкретном примере разницу между ними (при аутентификации имя пользователя: anonymous и пароль: a). Для запуска программы FTP в командной строке вызвать ftp>open (узел) 10.203.0.120)

Время выполнения работы 180мин;

Контрольные вопросы

1. Почему протоколы называются протоколами высших уровней?
2. Почему прием и передача электронной почты производятся по разным протоколам?
3. Почему POP3требует обязательной аутентификации, а SMTP нет?
4. Как определить окончание письма?
5. Почему для проверки наличия писем удобнее использовать list 1 по сравнению с list без параметра?
6. Для чего предназначен данный вам сервер?
7. Является ли его протокол текст-ориентированным?
8. Поддерживает ли он трехсимвольные коды ответов?
9. Почему для работы со стандартными протоколами используют специальные программы?

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.

4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 8 «Изучение и настройка маршрутизаторов»

Цель работы: Научиться настраивать соединение между сегментами сети.

В процессе занятия решаются следующие задачи:

1. Решить задачи сетевого администратора связанные с настройкой сетевого оборудования;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Маршрутиза́тор (от англ. *router*) — специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

Маршрутизатор работает на более высоком «сетевом» уровне 3 сетевой модели OSI, нежели коммутатор (или сетевой мост) и концентратор (хаб), которые работают соответственно на уровне 2 и уровне 1 модели OSI.

Принцип работы

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

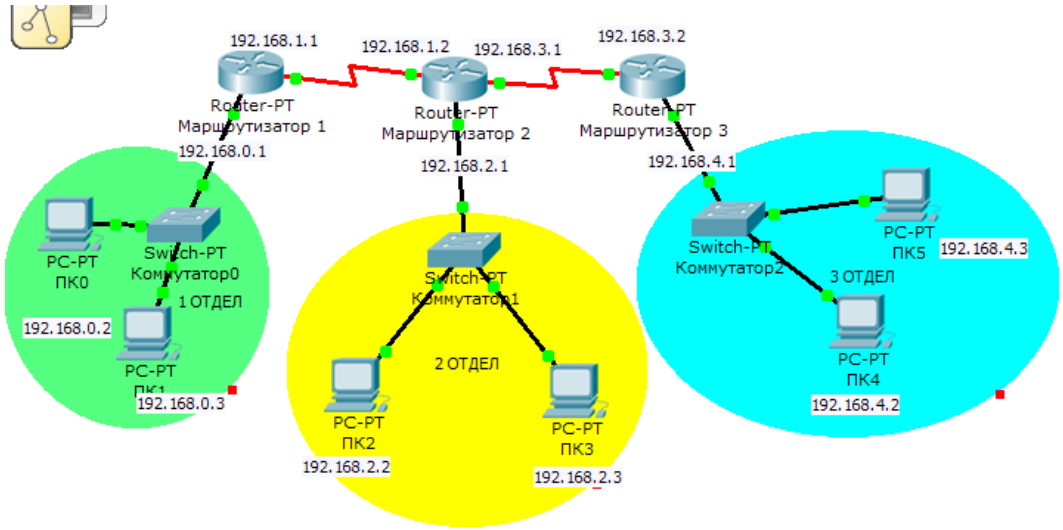
Существуют и другие способы определения маршрута пересылки пакетов, когда, например, используется адрес отправителя, используемые протоколы верхних уровней и другая информация, содержащаяся в заголовках пакетов сетевого уровня. Нередко маршрутизаторы могут осуществлять трансляцию адресов отправителя и получателя, фильтрацию транзитного потока данных на основе определённых правил с целью ограничения доступа, шифрование/расшифрование передаваемых данных и т. д.

Применение

Маршрутизаторы помогают уменьшить загрузку сети, благодаря её разделению на домены коллизий или широковещательные домены, а также благодаря фильтрации пакетов. В основном их применяют для объединения сетей разных типов, зачастую несовместимых по архитектуре и протоколам, например для объединения локальных сетей Ethernet и WAN-соединений, использующих протоколы xDSL, PPP, ATM, Frame relay и т. д. Нередко маршрутизатор используется для обеспечения доступа из локальной сети в глобальную сеть Интернет, осуществляя функции трансляции адресов и межсетевого экрана.

В качестве маршрутизатора может выступать как специализированное (аппаратное) устройство, так и обычный компьютер, выполняющий функции маршрутизатора. Существует несколько пакетов программного обеспечения (на основе ядра Linux, на основе операционных систем BSD) с помощью которого можно превратить ПК в высокопроизводительный и многофункциональный маршрутизатор, например, Quagga, IPFW или простой в применении PF.

Пример настройки маршрутизатора



Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Необходимо настроить маршрутизаторы для объединения сегментов локальной сети

Выполнение задания

1. Соберите схему, изображенную на рисунке в программе Cisco Packet Tracer;
2. Настройте сетевые интерфейсы ПК, согласно рисунку;
3. Компьютеры в каждой подсети должны быть доступны друг другу;
4. Настройте сетевые интерфейсы первого маршрутизатора (Маршрутизатор 1). Для этого выполните сл. действия:
   a. Настройте сетевой интерфейс, «смотрящий» в сторону ПК первого отдела. Пропишите сл. данные: IP адрес 192.168.0.1, Маска 255.255.255.0
   b. Настройте сетевой интерфейс, «смотрящий» в сторону второго маршрутизатора (Маршрутизатор 2). Пропишите сл. данные: IP адрес 192.168.1.1, Маска 255.255.255.252
5. Аналогичным образом настройте ПК из двух других отделов и маршрутизаторы этих отделов. Примечание. У второго маршрутизатора настраиваются три сетевых интерфейса. Очень внимательно смотрите на рисунок.
6. После того как настроили сетевые интерфейсы на оборудовании, переходим к настройке маршрутизаторов для пропуска пакетов из одного сегмента сети в другой. Для этого
   a. Откройте конфигурацию маршрутизатора. Перейдите в пункт меню *Статическая*
   b. В разделе *Статическая маршрутизация* в пункты *СЕТЬ* и *МАСКА* введите 0.0.0.0 (позволяет пропускать пакеты из всех подсетей с любыми масками)

с. В пункт *СЛЕДУЮЩИЙ ПЕРЕХОД* введите номер сетевого интерфейса последующего маршрутизатора. Нажмите кнопку ДОБАВИТЬ. Например, для маршрутизатора 1 данные будут выглядеть так:

0.0.0.0
0.0.0.0
192.168.3.1

0.0.0.0
0.0.0.0
192.168.3.2

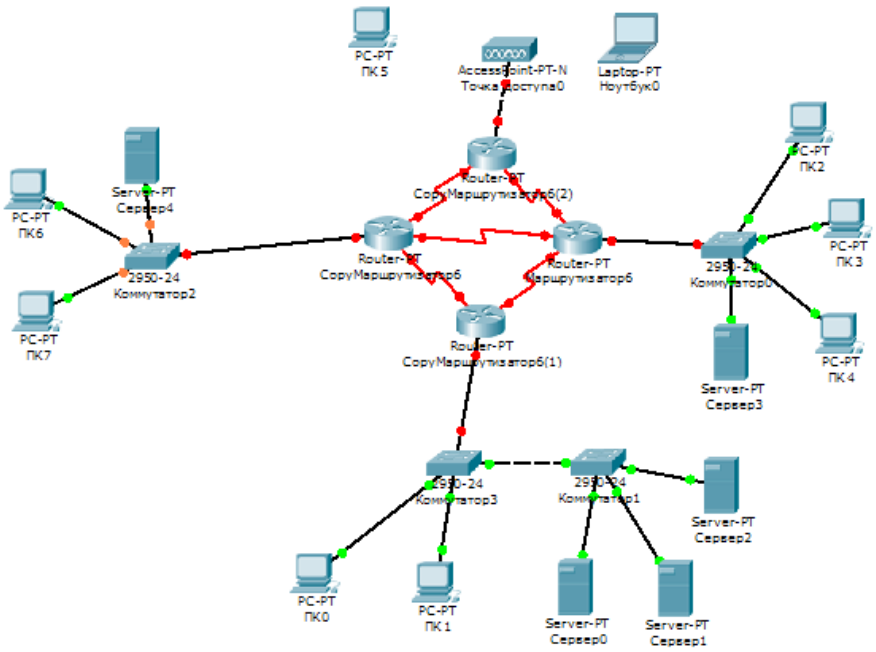
0.0.0.0
0.0.0.0
192.168.2.1

0.0.0.0
0.0.0.0
192.168.1.2
---

7. Аналогичным образом настройте оставшиеся маршрутизаторы.
8. Проверьте доступность всех ПК из разных подсетей.

Контрольное задание

Настройте сетевое оборудование и ПК , для объединения сегментов сетей.



Результат продемонстрируйте преподавателю.

Время выполнения работы 180мин;
Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки*:*
1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.- 1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 9 «Изучение и настройка коммутаторов сетей»

Цель работы: Научиться настраивать коммутаторы Cisco для получения настроек VLAN по сети.

В процессе занятия решаются следующие задачи:

1. Формирование умения настройки коммутаторов;.

Краткие теоретические и справочно-информационные материалы по теме занятия.

VLAN (аббр. от англ. *Virtual Local Area Network*) — логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

В устройствах Cisco, протокол VTP (VLAN Trunking Protocol) предусматривает VLAN-домены для упрощения администрирования. VTP также выполняет «чистку» трафика, направляя VLAN трафик только на те коммутаторы, которые имеют целевые VLAN-порты (функция VTP pruning). Коммутаторы Cisco в основном используют протокол 802.1Q Trunk вместо устаревшего проприетарного ISL (Inter-Switch Link) для обеспечения совместимости информации.

По умолчанию на каждом порту коммутатора имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Native VLAN — это параметр каждого порта, который определяет номер VLAN, который получают все непомеченные (untagged) пакеты.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Зачем делать так, чтобы настройки VLAN передавались по сети? Все просто, когда в сети становится больше десятка коммутаторов и маршрутизаторов, то следить и управлять ими становится все сложней, не говоря уже о настройке. В этой лабораторной работе вы научитесь создавать VLAN и распределять их на устройства в сети по средствам протокола VTP.

Настройка VLAN database

В данной лабораторной работе на будет рассматриваться разбиение сети на подсети с помощью VLAN. Будет рассмотрен вопрос настройки головного устройство и распределение VLAN на остальные. Топология для примера очень проста, один головной коммутатор и два клиента(VLAN10 и VLAN11).

Настройки главного коммутатора findotvet:

```
Switch>en
Switch#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname findotvet
```

Настройка домена:

```
findotvet(config)#vtp domain FIND
Changing VTP domain name from NULL to FIND
findotvet(config)#vtp password 123456789
Setting device VLAN database password to 123456789
findotvet(config)#vtp mode server
Device mode already VTP SERVER.
```

Настройка VLAN:

```
findotvet(config)#vlan 10
findotvet(config-vlan)#name FI1
findotvet(config-vlan)#exit
findotvet(config)#vlan 11
findotvet(config-vlan)#name FI2
findotvet(config-vlan)#exit
```

Настройка транк портов:

```
findotvet(config)#int fastEthernet 0/1
findotvet(config-if)#switchport trunk encapsulation dot1q
findotvet(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
findotvet(config-if)#exit
findotvet(config)#int fastEthernet 0/2
findotvet(config-if)#switchport trunk encapsulation dot1q
findotvet(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

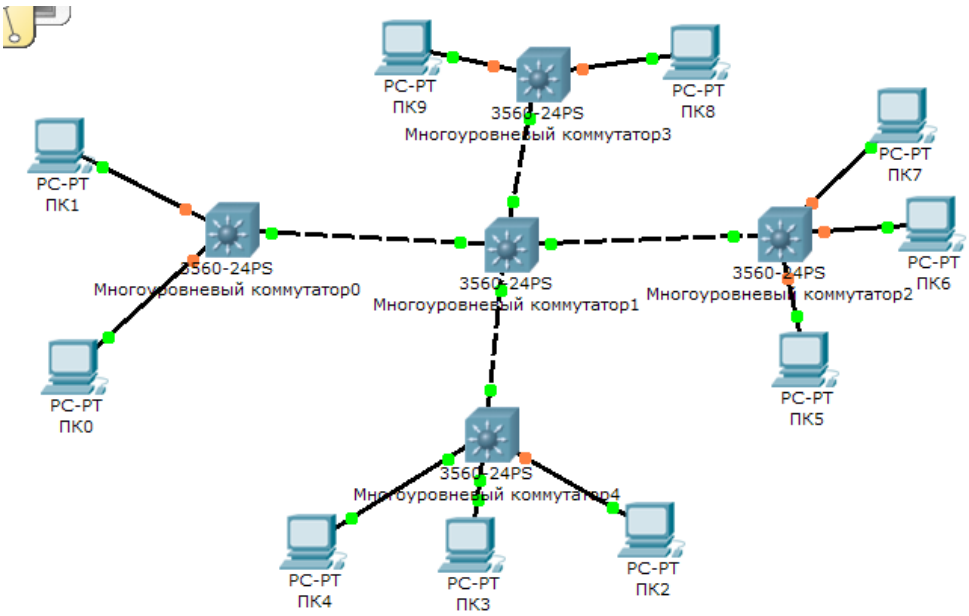
На этом настройка головного устройства завершена.

Настройка Switch10

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

Switch(config)#hostname Switch10
Switch10(config)#vtp domain FIND
Switch10(config)#vtp password 123456789
Setting device VLAN database password to 123456789
Switch10(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch10(config)#exit
Switch10#
%SYS-5-CONFIG_I: Configured from console by console
Проверяем настройки:
Switch10#sh vlan brief
VLAN Name Status Ports
—- ——————————— ——— ——————————-
1 default active Fa0/1, Fa0/3, Fa0/4
10 FI1 active
11 FI2 active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch10#
Как видно коммутатор получил настройки VLAN от головного, значит все настроено правильно. Аналогичным образом настраиваем второй коммутатор.
Настройки Switch11
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch11
Switch11(config)#vtp domain FIND
Domain name already set to FIND.
Switch11(config)#vtp password 123456789
Setting device VLAN database password to 123456789
Switch11(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch11(config)#ex
Switch11#
Switch11#sh vlan brief
VLAN Name Status Ports
—- ——————————— ——— ——————————-
1 default active Fa0/2, Fa0/3, Fa0/4
10 FI1 active
11 FI2 active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch11#

Контрольное задание
Спроектируйте и произведите настройку сети, состоящей из четырех сегментов посредством VLAN



Время выполнения работы 180мин;
Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки:
1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ

Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 10 «Принципы организации VPN»

Цель работы: изучить принцип организации работы VPN;

В процессе занятия решаются следующие задачи:

1. формированиея умения организации VPN сети.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Протокол L2TP является более предпочтительным для построения VPN-сетей, нежели PPTP, в основном это касается безопасности и более высокой доступности, благодаря тому, что для для каналов данных и управления используется одна UDP-сессия. Сегодня мы рассмотрим настройку L2TP VPN-сервера на платформе Windows.

Несмотря на простоту развертывания и подключения самых различных клиентов протокол PPTP имеет ряд существенных недостатков. Самый существенный - это однофакторная аутентификация при помощи пары логин / пароль, а так как логин пользователя чаще всего известен (или не составляет труда его выяснить), то по факту для аутентификации используется только пароль, будучи скомпрометированным он позволяет третьим лицам получить полный доступ к корпоративной сети.

Второй недостаток, вытекающий из первого - невозможность проверить подлинность подключающегося хоста, т.е. администратор не может с уверенностью сказать, что данное подключение выполнено пользователем Иванов со служебного ноутбука, а не злоумышленником, получившим доступ к учетным данным.

И наконец, третий недостаток связан с тем, что PPTP использует для работы два соединения: канал данных и канал управления. Это создает сложности с подключением, так как не все провайдеры, особенно при мобильном или гостевом доступе, обеспечивают нормальное прохождение GRE-пакетов, что делает подключение к VPN-серверу невозможным.

L2TP не имеет указанного недостатка, так как использует только одну UDP-сессию для передачи данных и управления, что облегчает подключение клиентов и администрирование сетевой инфраструктуры.

Вторым достоинством L2TP является двухфакторная аутентификация. Перед установлением соединения узлы проверяют подлинность друг друга на основании сертификата или предварительного ключа и только после этого приступают к соединению. Аутентификация с использованием сертификатов требует развернутой в сети инфраструктуры PKI, при ее отсутствии можно использовать аутентификацию по предварительному ключу. Мы будем рассматривать именно этот вариант.

Аутентификация по предварительному ключу менее надежна, чем по сертификату, но тем не менее позволяет организовать более высокий уровень безопасности VPN-сети нежели с использованием протокола PPTP. Предварительный ключ указывается один раз, при создании VPN-подключения на клиенте и может быть неизвестен пользователю (настройку производит администратор), в этом случае можно быть уверенным в подлинности подключающегося хоста и компрометация пароля в этом случае не позволит подключится к сети предприятия, так как предварительный ключ неизвестен.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Для развертывания VPN L2TP-сервера мы будем использовать Windows Server 2008 R2 SP1, однако все сказанное, с небольшими поправками, будет справедливо и для иных версий Windows Server.

Нам потребуется установленная роль **Службы политики сети и доступа**, которая должна содержать **Службы маршрутизации и удаленного доступа**.

Дальнейшая настройка производится через оснастку **Маршрутизация и удаленный доступ**, доступной в меню **Пуск - Администрирование**. При первом обращении будет запущен мастер, который поможет вам быстро настроить необходимые службы. Если вы планируете использовать это сервер как роутер, для обеспечения доступа в интернет компьютеров локальной сети, то следует выбрать **Доступ к виртуальной частной сети (VPN) и NAT**, если вам нужен только VPN-сервер, то**Удаленный доступ (VPN или модем)**.

Также довольно часто встречается ситуация, когда службы NAT уже развернуты, в этом случае нужно включить службы VPN вручную. Для этого в оснастке **Маршрутизация и удаленный доступ** щелкните

правой кнопкой мыши на имени сервера и выберите **Свойства**. В открывшемся окне на вкладке**Общие** поставьте переключатель **IPv4-маршрутизатор** в положение **локальной сети и вызова по требованию**, а также установите галочку **IPv4-сервер удаленного доступа**.

На вкладке **Безопасность** введите предварительный ключ.

Применяем изменения, перезапускам службу.

Затем переходим в раздел **Порты** и в свойствах L2TP устанавливаем обе галочки**Подключения удаленного доступа** и **Подключения по требованию**, максимальное число портов должно соответствовать или превышать предполагаемое количество клиентов. Неиспользуемые протоколы лучше отключить, убрав с свойствах обе галочки.

В итоге в списке портов должны остаться только L2TP порты в указанном вами количестве.

Настройка L2TP подключения на клиенте производится стандартными методами, на вкладке **Безопасность** выберите тип VPN как **L2TP с IPsec** и нажмите кнопку**Дополнительные свойства**, в открывшемся окне укажите использование предварительного ключа и введите сам ключ.

Также не забудьте включить использование **протокола расширенной проверки подлинности EAP**.

В остальном никаких отличий от создания PPTP подключения нет, пользователи могут подключаться к нашему серверу используя свои учетные данные.

Время выполнения работы 90 мин;

Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки*:*
1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ

11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 1 «Настройка протокола TCP/IP»

Цель работы: В результате выполнения лабораторной работы обучающиеся изучат способы диагностики настроек стека протоколов TCP/ IP; получить сведения о настройке TCP/IP для работы с DHCP сервером.

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками протокола TCP/ IP для работы с DHCP;
2. научить учащихся основным способам настройки TCP/IP;

Краткие теоретические и справочно-информационные материалы по теме занятия.

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***.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Запишите в тетрадь для лабораторных работ основные команды для работы с протоколом TCP/IP;
3. Выполните задания

3.1. **Задание 1. Подготовьте компьютер для выполнения лабораторной работы:**

3.1.1. Запустите компьютер

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

3.2.1. Запустите консоль ***(Пуск/Программы/Стандартные/Командная строка).***

3.2.2. В командной строке введите ipconfig /all | more.

3.2.3. Используя приведенную ниже информацию, создайте в своей папке текстовый документ 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.

3.2.4. 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);
- отправьте эхо-запрос по другому ***IP***-адресу, например ***192.168.10.100***.

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

3.3.1. Откройте окно Сетевые подключения (**Пуск/Панель управления/ Сетевые подключения).**

3.3.2. Вызовите свойства Подключения по локальной сети. Для этого можно воспользоваться контекстным меню.

3.3.3. В появившемся диалоговом окне на вкладке Общие откройте свойства Протокол Интернета TCP/IP.

3.3.4. Щелкните переключатель Использовать следующий IP-адрес и введите в соответствующие поля данные: IP_адрес (192.168.1.2)**;** Маску подсети (255.255.255.0)**;** Основной шлюз (192.168.1.1)**;** Предпочитаемый DNS (10.0.1.1)**.**

3.3.5. Примените параметры кнопкой ОК.

3.3.6. Закройте окно свойств подключения кнопкой ОК (если потребуется, то согласитесь на перезагрузку компьютера).

3.3.7. Проверьте работоспособность стека протоколов ***TCP/IP.***

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

3.4.1. Откройте окно Сетевые подключения.

3.4.2. Вызовите свойства Подключения по локальной сети.

3.4.3. Откройте свойства Протокол Интернета TCP/IP.

3.4.4. Установите переключатель Получить IP-адрес автоматически.

3.4.5. Закройте диалоговое окно Свойства: Протокол Интернета ***TCP/IP*** кнопкой ***ОК***.

3.4.6. Примените параметры кнопкой ОК.

3.4.7. Проверьте настройку стека протоколов ***TCP/IP.***

3.4.8. 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;

3.4.9. Проверьте работоспособность стека протоколов ***TCP/IP.***

Время выполнения работы 90 мин;

Контрольные вопросы

1. Какую информацию выводит команда ipconfig/all?
2. С помощью какой команды можно проверить доступность хоста?
3. С помощью какой команды можно узнать маршрут до хоста?
4. Служба DHCP предназначена для ….?

Сделайте выводы:

Возможности консольных команд для диагностики состояния сети.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 2 «Использование прикладного протокола Telnet»

Цель работы: В результате выполнения лабораторной работы обучающиеся познакомится с принципами работы текстовых протоколов высших уровней на примере протоколов электронной почты.

В процессе занятия решаются следующие задачи:

1. познакомить с основными принципами работы текстовых протоколов;
2. научить учащихся основным способам работы с прикладным протоколом Telnet;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Большинство протоколов высших уровней – текстовые – запросы и ответы передаются в виде текста, т.е. в запросах и ответах могут присутствовать только печатные символы.

Во многих протоколах ответы начинаются со специальной строки, состоящей из трехзначного числа и, возможно, текстового описания типа ответа. Трехзначное число разделяется на две части: 1-ый символ рассматривается как код класса сообщения; два последние – как тип сообщения данной важности.

Коды классов следующие:

1 – информационное сообщение. Обычно игнорируется программными клиентами.

2 – удачное завершение запроса. Рассматривается программами-клиентами как успех обработки запроса и обычно игнорируется.

Часто программы-серверы не различают сообщения первого и второго типа, т.е. информационное сообщение проходит по второй категории.

3 – сообщение об удачной обработке запроса, но требующее дополнительных действий клиента.

4 – ошибка со стороны клиента, т.е. клиент послал запрос, который не может обработать сервер вследствие ошибочности или недостаточности данных.

5 – ошибка со стороны сервера. Клиент послал правильный запрос, но сервер не смог его выполнить в силу каких-то причин.

Трехзначные коды ответов очень удобны для программного распознавания, нет необходимости распознавать текст ответа, который, в общем случае, может прийти на разных языках, достаточно распознать только 3 цифры.

2. Программа TELNET

Для работы с текстовыми протоколами воспользуемся программой TELNET, входящей в состав Windows. Эта программа предназначена для работы с протоколом TELNET, задачей которого является обмен информацией между клиентом и сервером без каких либо преобразований, т.е. организация прозрачного канала между клиентом и сервером.

Синтаксис команды TELNET следующий:

TELNET адрес_сервера [порт]

Если порт не указан, используется 23 - стандартный порт протокола TELNET.

3. Протокол SMTP

Для начала попробуем поработать с протоколом SMTP. Обычно он работает, используя порт 25.

Для наглядности команды пользователя выделены *курсивом*, а ответы сервера – подчеркиванием.

Даем команду на подключение:

telnet 192.168.1.2 25

Получаем ответ

220 home VPOP3 SMTP Server Ready

Работает! Обратите внимание на число 220 в начале строки ответа. Это нормальный ответ, сервер ответил на наш запрос на подключение.

Многие серверы, работающие по текстовым протоколам, поддерживают команду HELP. Проверим.

Help

Дадим серверу неправильный запрос

abrakadabra

500 Command Unrecognised

Как ни странно, но код ответа 5 – ошибка на стороне сервера!

Попробуем написать письмо

Поздороваемся

helo home

250 home VPOP3 SMTP Server - Hello home, pleased to meet you
Укажем отправителя письма
mail from: user1
250 <user1>... Sender ok
Укажем получателя письма
rcpt to: user2
250 <user2>... Recipient ok
Перейдем в режим ввода письма
data
354 Start Mail input, end with <CRLF>.<CRLF>
Обратите внимание на код ответа 354.

Это нормальное завершение, но требуются дополнительные данные – само письмо, которое, как видно, должно заканчиваться строкой, состоящей из одной точки «.».

А теперь само письмо. Формат письма описан стандартами. Их изучение не входит в нашу задачу, но наиболее важные служебные строки вкратце рассмотрим:

Date: Tue, 22 Nov 2005 19:55:07 +0200
Дата создания по GMT и часовой пояс
From: User user1@home.my
От кого
Reply-To: User user1@home.my
Кому отвечать
To: user2@home.my
Кому
Subject: Test
Тема письма
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

Информация почтовой программе, как закодировано письмо – с помощью этих строк почтовая программа клиент сможет реализовать шестой уровень – представить информацию пользователю в читабельном виде

Hello user2,
It's a test message.
Best regards,
User mailto:user1@home.my

Само письмо
.250 OK
Письмо принято!
Теперь выходим
quit
221 home VPOP3 Server Closing Connection

Протокол SMTP (Simple Mail Transfer Protocol) используется для передачи электронной почты от клиента серверу или между серверами. Не содержит встроенных средств идентификации и преобразования.

4. Протокол POP3

Теперь поработаем с протоколом POP3. Обычно он работает, используя порт 110.
Даем команду на подключение:
telnet 192.168.1.2 25
Получаем ответ
+OK VPOP3 Server Ready <1.7b0.435a37>
Работает, но трехсимвольного кода ответа нет!
Попробуем help
help

-ERR Unrecognised command

Видим, что помощи нет, заодно и посмотрели, как сервер отвечает на ошибочный для него запрос.

Как мы знаем, POP3 требует аутентификации, поэтому представимся:

user user2

+OK User Accepted, PASSword required

А теперь пароль.

pass 2

+OK user2 has 1 message(s) (580 octets)

Нам есть почта! Посмотрим.

list

+OK 1 messages (580 octets)

1 580

.

Одно письмо 580 символов. Если бы было несколько писем, было бы несколько строк с указанием номеров и размеров писем. Точка в последней строке показывает, что это окончание ответа.

Теперь прочитаем (получим) первое письмо.

retr 1

+OK 580 octets

Received: from 192.168.200.1 by home ([192.168.200.1] running VPOP3) with SMTP
or <user2>; Tue, 22 Nov 2005 20:31:07 +0200

Date: Tue, 22 Nov 2005 19:55:07 +0200

From: User <user1@home.my>

Reply-To: User <user1@home.my>

To: user2@home.my

Subject: Test

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Message-Id: <VPOP31.3.0c.20051122203134.814.e.1.40132205@home>

X-Server: VPOP3 V1.3.0c - Registered to: Collega

Hello user2,

It's a test message.

Best regards,

User mailto:user1@home.my

.

Служебных полей стало больше – их добавил сервер.

Обратите внимание на последнюю строку ответа

Теперь удалим письмо с сервера, ведь оно уже прочитано:

dele 1

+OK message 1 deleted

Проверим, есть ли что еще

list

+OK 0 messages (0 octets)

.

Ничего нет. А можно и так, для программы это будет более удобным

list 1

-ERR Invalid Message Number

Ну, и теперь выходим

quit

+OK VPOP3 Server Closing Connection

В приведенном выше примере было отправлено письмо от пользователя «user1» пользователю «user2» и получена почта пользователя «user2» с помощью утилиты TELNET, т.е. без использования почтового клиента.

Протокол POP3 (Post Office Protocol) предназначен для получения электронной почты от сервера к клиенту. Содержит средства идентификации клиента, использует факультативные средства преобразования.

3. Протокол FTP

Протокол FTP (File Transfer Protocol) – протокол передачи файлов.

Он использует 20-ый порт для установления соединений и 21-ый порт для установления соединений и передачи файлов. Этот протокол содержит встроенные средства идентификации клиента. Все распознаваемые им команды состоят из 3-х или 4-х символов, являющихся сокращениями или аббревиатурами выполняемых действий.

6. Протокол HTTP

Протокол HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста, т.е. данных разного представления (текст, изображения, видео, звук). Обычно этот протокол работает на 80-ом порту. Он содержит средства идентификации и перекодирования передаваемой информации.

Как видим работа с текстовыми протоколами не представляет особых трудностей. Правда некоторые протоколысодержат большое число команд и чтобы узнать их формат требуется использовать их стандарт и описания RFC.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Запишите в тетрадь для лабораторных работ основные команды для работы с протоколом TCP/IP;
3. **Выполните задания**

Во всех заданиях адрес сервера:**192.168.1.2**

В пятом и шестом заданиях, после аутентификации (если она необходима) рекомендуется в первую очередь вызвать помощь командой help и посмотреть информацию о других командах, поддерживаемых данным протоколом.

1. Используйте адрес сервера электронной почты, установленного на VirtualBox (если почтовый сервер не установлен установите его), имена и пароли пользователей. Отправить и получить почту без использования почтового клиента.
2. Поработать с POP3 без аутентификации. Сделать соответствующие выводы.
3. Определить, является ли протокол FTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.
4. Подключиться к HTTP серверу и определить, является ли протокол HTTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.
5. Использовать адрес и порт неизвестного для вас протокола и сервера. Получите список его команд, объясните, что делает каждая команда. Попробовать некоторые из них и проанализировать результаты.(использовать 1000-ый порт, при аутентификации имя пользователя и пароль: admin).
6. Поработайте с FTP-сервером с помощью TELNET и программы FTP. Объясните и подтвердите на конкретном примере разницу между ними. Для запуска программы FTP в командной строке вызвать ftp>open (узел)……)

Время выполнения работы 180 мин;

Контрольные вопросы

1. Почему протоколы называются протоколами высших уровней?
2. Почему прием и передача электронной почты производятся по разным протоколам?

3. Почему POP3требует обязательной аутентификации, а SMTP нет?

4. Как определить окончание письма?

5. Почему для проверки наличия писем удобнее использовать list 1 по сравнению с list без параметра?

6. Для чего предназначен данный вам сервер?

7. Является ли его протокол текст-ориентированным?

8. Поддерживает ли он трехсимвольные коды ответов?

9. Почему для работы со стандартными протоколами используют специальные программы?

Сделайте выводы:

Возможности и список консольных команд для работы через Telnet .

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 3 «Дистанционное управление компьютером»

Цель работы: В результате выполнения лабораторной работы обучающиеся научится включать на сервере программу Удаленный рабочий стол для администрирования; включать пользователей в соответствующую группу, чтобы разрешить им удаленно администрировать сервер; подключаться к серверу с помощью программы Удаленный рабочий стол для администрирования.

В процессе занятия решаются следующие задачи:

1. познакомить с основными принципами работы с удаленным рабочим столом;
2. научить учащихся проводить администрирование сервера;

Краткие теоретические и справочно-информационные материалы по теме занятия.

В семействе Windows Server был впервые реализован тесно интегрированный набор программных средств и технологий, позволяющих выполнять удаленное администрирование и совместно использовать приложения с помощью ***Служб терминалов*** *(Terminal Services)*. Эволюция продолжилась: отныне службы терминалов — неотъемлемый компонент семейства Windows Server 2003, а инструмент ***Дистанционное управление рабочим столом*** *(Remote Desktop)* усовершенствован и позиционируется как стандартная функция. Так что теперь достаточно одного щелчка мыши, и компьютер с Windows Server 2003 будет параллельно обрабатывать до двух подключений удаленного администрирования. Добавив компонент ***Сервер терминалов*** *(Terminal Server)* и настроив соответствующую лицензию, администратор добьется еще большего эффекта: множество пользователей смогут запускать приложения на сервере. На этом занятии вы научитесь работать со служебной программой ***Удаленный рабочий стол для администрирования*** *(Remote Desktop for Administration).*

Включение и конфигурирование программы *Удаленный рабочий стол для администрирования.*

Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как *Дистанционное управление рабочим столом* (Remote Desktop), *Удаленный помощник* (Remote Assistance) и *Сервер терминалов* (Terminal Server). По умолчанию служба устанавливается вместе с Windows Server 2003 и настраивается в программе *Дистанционное управление рабочим столом* для работы в режиме удаленного администрирования: допускает только два параллельных удаленных подключения и не содержит компоненты для совместного использования приложений из состава *Сервера терминалов.* Следовательно, *Дистанционное управление рабочим столом* создает очень небольшую дополнительную нагрузку на систему, причем не требует дополнительного лицензирования.

Примечание Поскольку *Службы терминалов* и *Дистанционное управление рабочим столом* являются стандартными компонентами Windows Server 2003, каждый сервер способен поддерживать удаленные подключения к своей консоли. Термин «сервер терминалов», таким образом, теперь по праву можно применить к любому компьютеру под управлением Windows Server 2003, обеспечивающему совместное использование приложений несколькими клиентами за счет добавления компонента *Службы терминалов.*

Другие компоненты — *Сервер терминалов* и службу *Лицензирование сервера терминалов* (Terminal Server Licensing) — нужно добавлять с помощью функции *Установка и удаление программ* (Add Or Remove Programs). Тем не менее, все средства администрирования для настройки и поддержки клиентских подключений и управления сервером терминалов устанавливаются по умолчанию на все компьютеры с Windows Server 2003. Эти средства и их функции описаны в таблице 1.

Таблица 1. Стандартные компоненты *Сервер терминалов* и *Подключение к удаленному рабочему столу*

Установленное ПО	Назначение
Настройка служб терминалов (Terminal Services Configuration)	Настройка свойств сервера терминалов, в том числе параметров сеанса, сети, клиентского рабочего стола и удаленного управления клиентом
Диспетчер служб терминалов (Terminal Services Manager)	Отправка сообщений клиентам, подключенным к серверу терминалов, отключение или завершение сеансов, а также инициирование удаленного управления или маскировки сеансов
*Подключение к удаленному рабочему столу (*Установочные файлы клиента Remote Desktop Connection)	Установка клиентского приложения *Дистанционное управление рабочим столом* (Remote Desktop) для Windows Server 2003 или Windows XP. 32_разрядное клиентское ПО *Дистанционное управление рабочим столом* устанавливается в папку %Systemroot%\System32\ Clients\Tsclient\Win32 на сервере терминалов
Лицензирование служб терминалов (Terminal Services Licensing)	Настройка лицензий для клиентских подключений к серверу терминалов. Это средство не подходит для сред, где используется только *Удаленный рабочий стол для администрирования*

Чтобы разрешить подключения *Дистанционное управление рабочим столом* (Remote Desktop) на компьютере под управлением Windows Server 2003, в *Панели управления* выберите Система (System Properties). На вкладке Удаленное использование (Remote) выберите ***Разрешить удаленный доступ к этому компьютеру*** **(Allow Users To Connect Remotely To This Computer)**.

Примечание Если сервер терминалов является контроллером домена, необходимо также настроить групповую политику контроллера, чтобы разрешить группе *Пользователи удаленного рабочего стола* (Remote Desktop Users) подключение посредством служб терминалов. На серверах, не являющихся контроллерами домена, подключение через службы терминалов пользователям из этой группы разрешено по умолчанию.

Подключение к удаленному рабочему столу.

Подключение к удаленному рабочему столу *(Remote Desktop Connection)* — это клиентское приложение, используемое для подключения к серверу в контексте режима *Дистанционное управление рабочим столом* (Remote Desktop) или *Сервер терминалов* (Terminal Server). Для клиента нет функциональных различий между этими двумя конфигурациями сервера.

На компьютерах с Windows XP и Windows Server 2003 программа *Подключение к удаленному рабочему столу* установлена по умолчанию, но глубоко запрятана:

Пуск (Start)\Все программы (All Programs)\ Стандартные (Accessories)\Связь (Communications)\Подключение к удаленному рабочему столу (Remote Desktop Connection).

На других платформах программу *Подключение к удаленному рабочему столу* можно установить с компакт_диска Windows Server 2003 либо из установочной папки клиента (%Systemroot%\System32\Clients \Tsclient\Win32) на любом из компьютеров под управлением Windows Server 2003. Установочный пакет MSI можно распространять на системы Windows 2000 с помощью групповой политики или средствами SMS (Systems Management Server).

Совет Рекомендуется обновить предыдущие версии клиента *Служб терминалов,* установив последнюю версию *Подключение к удаленному рабочему столу,* чтобы обеспечить наиболее оптимальную, безопасную и стабильную среду, поскольку в этом случае будет доступен улучшенный пользовательский интерфейс, 128_битное шифрование и выбор альтернативных портов.

Настройка клиента удаленного подключения к рабочему столу.

Вы можете управлять множеством аспектов дистанционного подключения как со стороны клиента, так и со стороны сервера. В таблице 2 перечислены конфигурационные параметры и их назначение.

Таблица 2. Параметры программы *Удаленное подключение к рабочему столу*

Параметры	**Назначение**
Параметры клиента	
Общие (General)	Параметры выбора компьютера, к которому необходимо подключаться, настройка статических реквизитов для входа в систему, а также сохранение параметров для данного подключения
Экран (Display)	Задает размер окна клиента, глубину цвета, а также доступность панели подключений при работе в полноэкранном режиме
Локальные ресурсы (Local Resources)	Параметры передачи звуковых событий на локальный компьютер, помимо стандартных выходных сигналов мыши, клавиатуры и экрана. Также параметры на этой вкладке определяют, как удаленный компьютер интерпретирует комбинации клавиш Windows (например Alt+Tab), и доступны ли в сеансе удаленного доступа такие устройства, как локальные диски, принтеры и последовательные порты
Программы (Programs)	Задает путь и папки расположения для любых программ, которые необходимо запустить после установки соединения
Дополнительно (Experience)	Категории функций экрана можно включать или отключать в зависимости от пропускной способности канала связи между локальным и удаленными компьютерами. Предусмотрены параметры для отображения фона рабочего стола, содержимого окна при перетаскивании, визуальных эффектов при прорисовке меню и окон, тем рабочего стола; также вы можете активировать режим кэширования растровой графики, при котором после каждого интервала обновления передаются только изменения, а не весь экран целиком
Параметры сервера	
Параметры входа (Logon Settings)	Позволяет задать статические реквизиты для подключения вместо реквизитов, предоставляемых клиентом

Сеансы (Sessions)	Чтобы перекрыть настройки клиента, задайте здесь параметры завершения прерванного сеанса, ограничения длительности сеанса и времени его простоя, а также допустимость повторного подключения
Среда (Environment)	Перекрывает настройки из профиля пользователя для данного подключения в отношении запуска программы: здесь вы можете переопределить запускаемую при подключении программу. Заданный здесь путь и папка запуска приоритетнее настроек, сделанных программой *Подключение к удаленному рабочему столу*
Разрешения (Permissions)	Позволяет задавать дополнительные разрешения для данного подключения
Удаленное управление (Remote Control)	Указывает, можно ли удаленно управлять сеансом *Подключение к удаленному рабочему столу,* и если так, то должен ли пользователь выдавать разрешение на инициализацию сеанса удаленного управления. Дополнительные параметры позволяют ограничить сеанс удаленного управления только функцией просмотра либо разрешить полную интерактивность с сеансом клиента *Дистанционное управление рабочим столом*
Параметры клиента (Client Settings)	Позволяют перекрыть параметры из конфигурации клиента, изменить глубину цвета и отключить различные коммуникационные порты (порты ввода-вывода)
Сетевой адаптер (Network Adapters)	Указывает, какие сетевые платы на сервере будут принимать удаленные подключения для администрирования
Общие (General)	Задает уровень шифрования и механизм проверки подлинности для подключений к этому серверу

Устранение неполадок при работе со службами терминалов.

При использовании программы *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration) создается подключение к консоли сервера. Есть несколько потенциальных причин неудачных подключений или сеансов с ошибками.

• **Сбои сети.** Ошибки в работе стандартной TCP/IP_сети могут вызывать сбои или разрывы подключений *Дистанционное подключение к рабочему столу* (Remote Desktop). Если не функционирует служба DNS, клиент не сможет найти сервер по имени. Если не функционирует маршрутизация либо неверно настроен порт *Служб терминалов* (Terminal Services) (по умолчанию это порт 3389) на клиенте или сервере, соединение установить не удастся.

• **Реквизиты входа.** Для успешного подключения к серверу средствами программы *Удаленный рабочий стол для администрирования* пользователи должны быть включены в группу *Администраторы* (Administrators) или *Пользователи удаленного рабочего стола* (Remote Desktop Users).

Подготовка к экзамену Если подключиться через *Удаленный рабочий стол для администрирования* не удается из_за запрета доступа, проанализируйте членство в группах. В предыдущих версиях *Сервера терминалов* (Terminal Server) для подключения к серверу требовалось быть участником группы *Администраторы* (Administrators), хотя специальные разрешения можно было выдать вручную. Сервер терминалов поддерживает только два удаленных подключения.

• **Политика.** Только администраторам разрешено подключаться средствами программы *Дистанционное подключение к рабочему столу* (Remote Desktop) к контроллерам доменов. Чтобы разрешить подключаться остальным пользователям, нужно настроить политику безопасности на контроллере домена.

• **Слишком много** параллельных **подключений.** Если сеансы прерывались без выхода из системы, сервер может посчитать, что достигнут предел, одновременно обрабатываемых подключений, даже если в данный момент к серверу не подключены два пользователя. Например, администратор может завершить сеанс без выхода из системы. Если еще два администратора попытаются подключиться к серверу, это удастся только одному из них.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Запишите в тетрадь для лабораторных работ основные команды для работы с протоколом TCP/IP;

4. Выполните задания

На этой лабораторной работе вы настроите на сервере Server01 подключения через *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration). Затем вы оптимизируете Server01, чтобы обеспечить доступность неиспользуемого подключения и разрешить лишь одно подключение в любой момент времени. После этого вы установите сеанс удаленного администрирования с ПК 2 (либо с другого удаленного компьютера).

Если в вашем распоряжении только один компьютер, можно использовать клиент программы *Дистанционное подключение к рабочему столу* (Remote Desktop) для подключения к службам терминалов на том же компьютере. В этом случае ссылки на удаленный компьютер на этой лабораторной работе будут относится к локальному компьютеру.

Упражнение 1. Настройка удаленного подключения к рабочему столу

В этом упражнении вы активируете удаленное подключение к рабочему столу, измените число разрешенных одновременных подключений на сервере и настроите параметры завершения подключения.

1. Войдите на Server01 как *Администратор* (Administrator).
2. В Панели управления выберите **Система (System Properties).**
3. На вкладке **Remote** включите **Remote Desktop.** Закройте окно **Система (System Properties).**
4. Откройте консоль *Настройка служб терминалов* (Terminal Services Configuration) из группы программ *Администрирование* (Administrative Tools).
5. В консоли tscc (Terminal Services Configuration\Connections) на правой панели щелкните правой кнопкой подключение **RDP_tcp** и выберите **Свойства (Properties).**
6. На вкладке **Сетевой адаптер (Network Adapter)** установите значение параметра **Максимальное число подключений (Maximum Connections)** равным 1.
7. На вкладке **Сеансы (Sessions)** установите оба флажка **Заменить параметры пользователя (Override User Settings)** и измените настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия.

• **Завершение отключенного сеанса (End a disconnected session):** 15 минут,
• **Ограничение активного сеанса (Active session limit): никогда (never),**
• **Ограничение активного сеанса (Active session limit):** 15 минут.
• **При превышении ограничений или разрыве подключения (When session limit is reached or connection is broken): Отключить сеанс (Disconnect from session).**

Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через 15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).

Упражнение 2. Подключение к серверу с помощью клиента удаленного подключения к рабочему столу

1. На ПК 2 (или на другом удаленном компьютере либо прямо с ServerOl, если удаленного компьютера нет) в группе Стандартные\Связь (Accessories\Communications) щелкните **Подключение к удаленному рабочему столу (Remote Desktop Connection),** подключитесь к Server01 и войдите в его систему.
2. На сервере Server01 откройте консоль tscc.msc: **Администрирование (Administrative tools)\Настройка служб терминалов (Terminal Services Configuration).** В открывшейся консоли выберите **Подключения (Connections).** Вы должны увидеть сведения о сеансе удаленного подключения к Server01.
3. Не выполняйте никаких действий в этом сеансе 15 минут либо закройте клиент программы *Удаленное*

подключение к рабочему столу (Remote Desktop), не завершив сеанс *Сервера терминалов* (Terminal Server) явно: сеанс должен будет завершиться автоматически через 15 минут.
В данный момент вы подключены к ServerOl удаленно и можете выполнять на нем любые задачи, допустимые в интерактивном режиме на консоли.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования? Почему?

2. Как оптимальным образом предоставить администраторам возможность удаленного управления сервером через службы терминалов?

a. Не выполнять никаких действий; они уже имеют доступ, поскольку являются администраторами.

b. Удалить группу *Администраторы* (Administrators) из списка разрешений в подключении к серверу терминалов и поместить их административную учетную запись в группу *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).

c. Создать отдельную пользовательскую учетную запись с более низким уровнем авторизации для повседневного использования группой *Администраторы* и поместить ее в группу *Удаленный рабочий стол для администрирования.*

3. Какое программное средство используется на сервере для включения удаленного подключения к рабочему столу?

a. *Диспетчер служб терминалов* (Terminal Services Manager).

b. *Настройка служб терминалов* (Terminal Services Configuration).

c. *Система* (System Properties) из Панели управления.

d. *Лицензирование служб терминалов* (Terminal Services Licensing).

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 4 «Дистанционная настройка локальной сети»

Цель работы: В результате выполнения лабораторной работы обучающиеся научится использовать специализированные программы для дистанционной настройки и управления сетью .

В процессе занятия решаются следующие задачи:

1. познакомить с основными программами дистанционного управления и настройки сети;
2. научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Remote Administrator (сокращенно Radmin).

Данная программа позволяет администрировать все рабочие станции и серверы вашей локальной сети прямо со своего рабочего места Вы будете видеть экран администрируемого компьютера в окне на своем Рабочем столе или в полноэкранном режиме. Кроме того, вы сможете управлять данным компьютером с помощью своей клавиатуры и мыши (впрочем, вы можете просто наблюдать за действиями пользователя).

Radmin способна работать с соединениями по локальной сети, а также через коммутируемое соединение, так как высокая скорость соединения не является основным требованием программы. При использовании соединения через модем частота обновления экрана составит около 5-10 кадров в секунду, чего достаточно для работы. Если вы используете локальную сеть, то экран будет обновляться в реальном времени (около 100-500 кадров в секунду).

Данная программа предоставляет следующие возможности

- Поддержку нескольких режимов просмотра экрана удаленного компьютера (оконный, полноэкранный, оконный масштабируемый).
- Radmin-сервер способен выступать в виде службы Windows NT/2000/XP и Windows 95/98/Me (таким образом, можно выйти и войти в систему удаленно). □ Radmin-сервер может устанавливать несколько соединений с удаленными компьютерами одновременно.
- Присутствует возможность передачи файлов удаленному компьютеру и наоборот,
- Доступна возможность управления питанием удаленного компьютера,
- Возможность использования TELNET-сервера.
- Реализована поддержка системы безопасности Windows NT. Возможно также предоставление прав на удаленное управление, слежение за информацией и обмен ею. TELNET-доступ определенным пользователям или группам пользователей Windows. Если конкретная рабочая станция входит в домен, то программа будет использовать активную учетную запись, чтобы организовать доступ к Radmin-серверу. Если же система безопасности Windows отключена, то на доступ будет установлен пароль с 128-битным ключом.
- 128-битное шифрование всех потоков данных.
- Применение специального IP-фильтра позволяет разрешать доступ к Radmin-серверу ограниченному количеству определенных IP-адресов и подсетей.
- Remote Administrator состоит из клиентской и серверной частей.
- Серверная часть захватывает изображение на экране и передает его по сети клиентской части, а также исполняет инструкции, полученные от нее.
- Клиентская часть отображает экран удаленного компьютера и предоставляет возможность управления удаленным компьютером.

Network Assistant (Nassi, для краткости) - это программа для общения и эффективного взаимодействия в локальной сети, не требующая работы выделенного сервера.

Основные возможности: **многоканальный чат**, общая**доска для рисования**, мгновенные **сообщения**,**передача файлов**, **управление процессами** на удаленном компьютере, **просмотр копии экрана/буфера обмена** удаленного компьютера, статистика использования, сигнализаторы удаленных событий и др.

Network Assistant поддерживает пять стандартных состояний и позволяет создавать до десяти пользовательских.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

5. Выполните задания

Установим *сервер* и клиент на машины Win Server 2003 и Windows XP. При этом *права* пользователей на сервере пока настраивать не будем (сделаем это позднее).

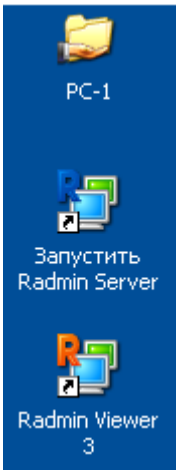


Рис. 1. Сервер и клиент установлены на Windows Server

Запустим на Windows Server программу **Настройки Radmin Server** и в правах доступа установим *переключатель* в положение **Radmin** (рис. 2 и рис. 3).

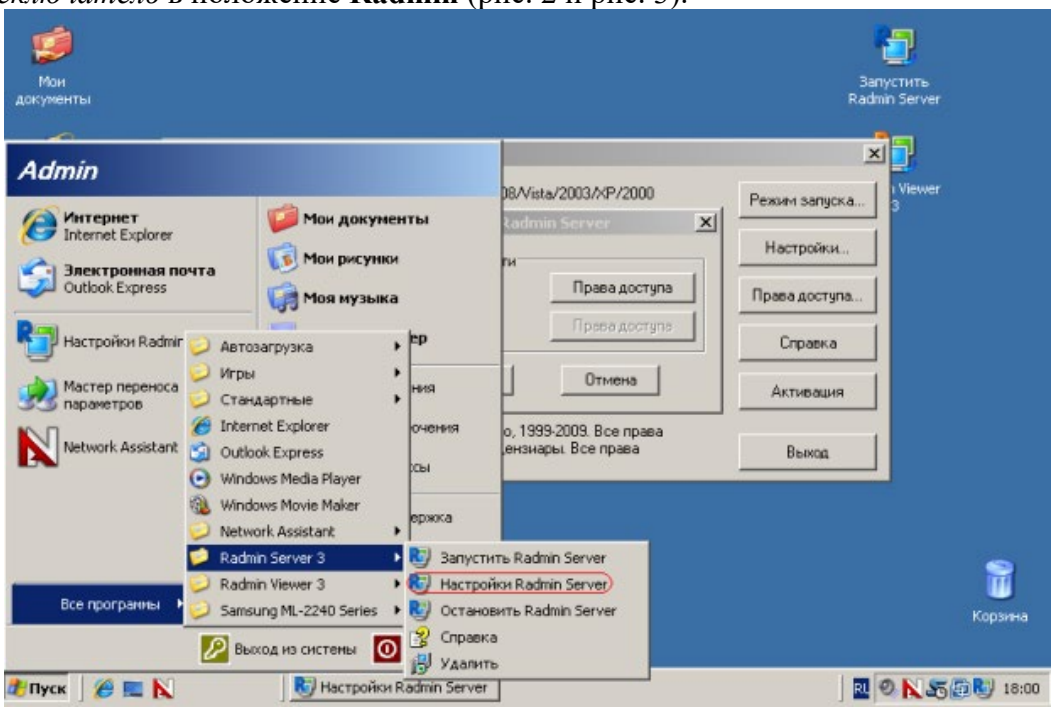


Рис. 2. Запускаем команду Настройки Radmin Server

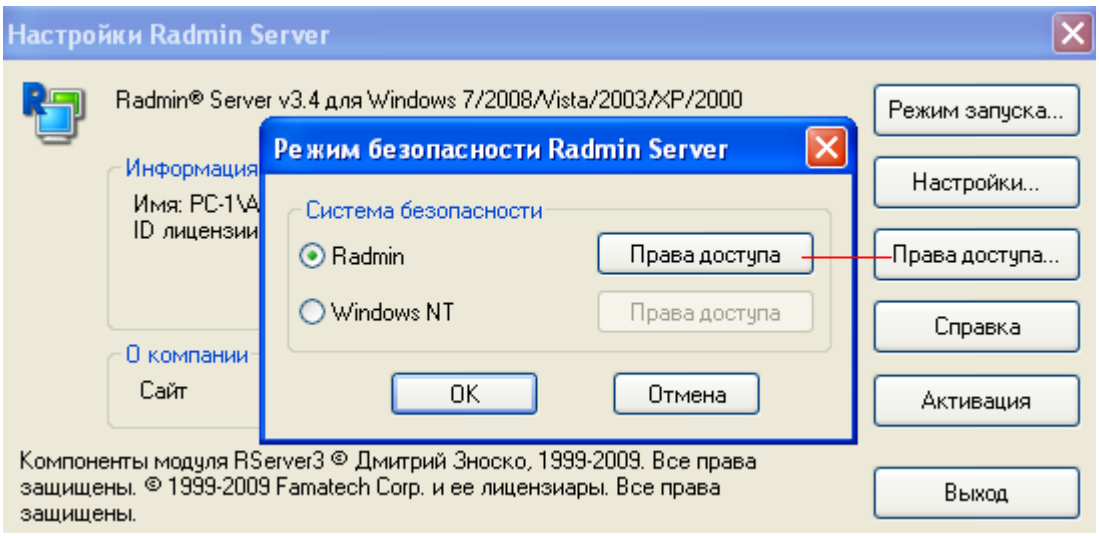


Рис. 3. Выставляем режим безопасности Radmin Server

Нажмем на кнопку **Права доступа** и создадим пользователя серверной частью программы Radmin на ПК Windows Server , т.е. организуем пользователя User-1 с паролем 123456 (рис. 4).

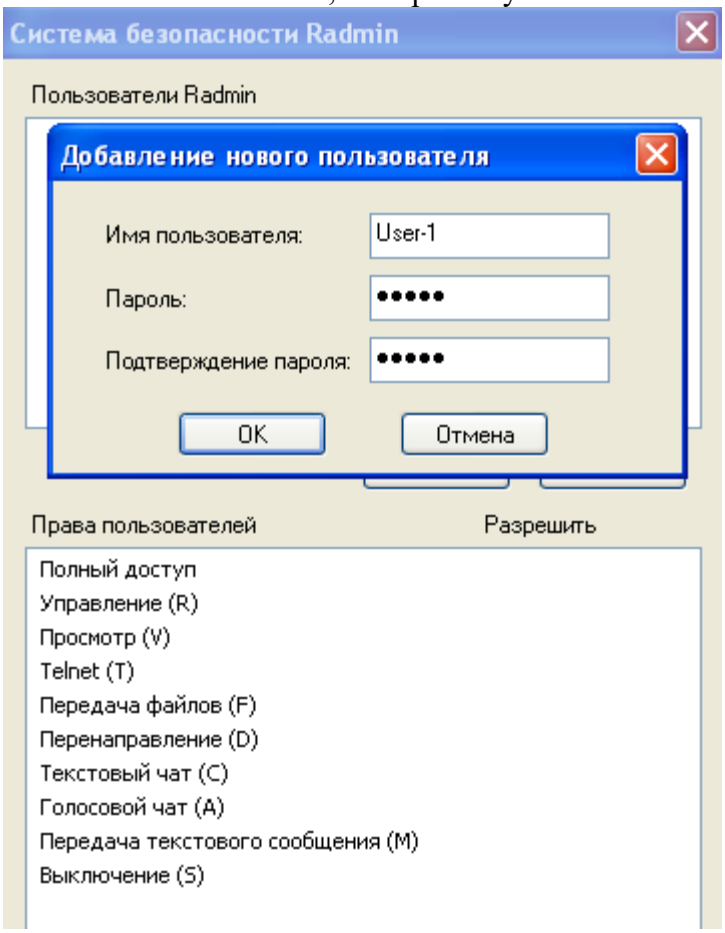


Рис. 4. Добавление нового пользователя

Этому пользователю дадим все *права* (рис. 5).

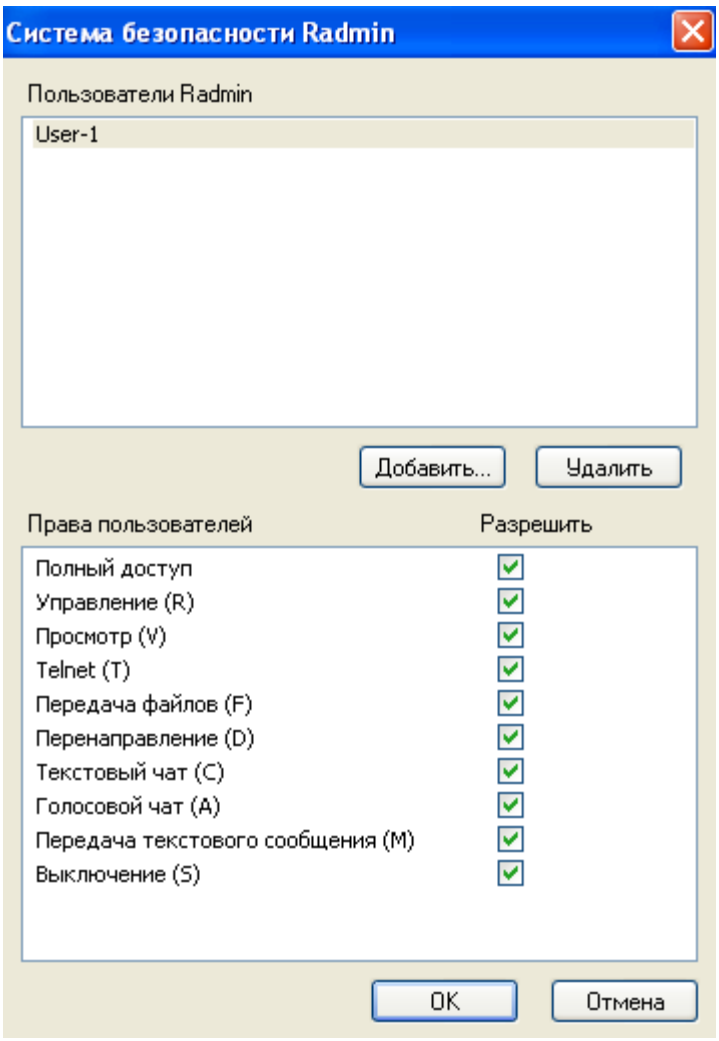


Рис. 5. Права пользователя User-1 на ПК 110-1

Теперь на ПК Windows XP запускаем Radmin *Viewer*, выполняем команду **Соединение-Соединиться с- Windows Server** (рис. 6).

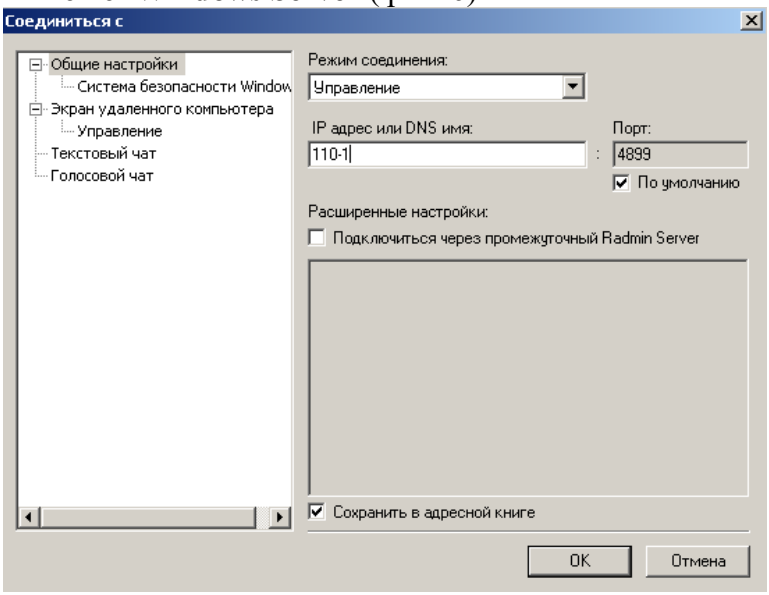


Рис. 6. Окно соединения клиента Windows XP с сервером Windows Server

Теперь следует ввести имя User-1 с паролем 123456 и нажать OK (рис. 7).

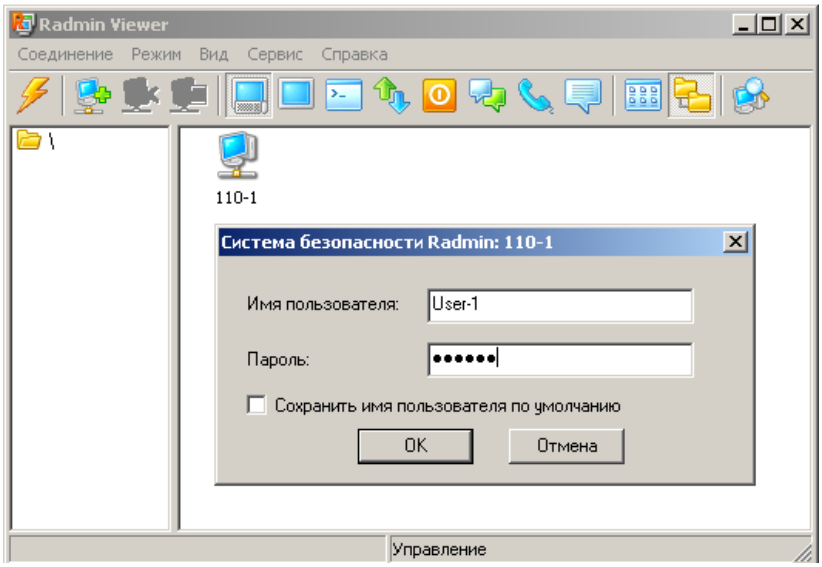


Рис. 7. После нажатия ОК вы увидите рабочий стол ПК Windows Server

Теперь мы полностью можем управлять с ПК Windows XP компьютером Windows Server , как будто вы физически сидите не на ПК Windows XP, а на ПК Windows Server. Иначе говоря, с помощью Radmin, вы можете администрировать удаленный ПК удаленно.

Примечание

Полезной особенностью Radmin является возможность подключения к удаленному компьютеру в **режиме Telnet**. Это позволит осуществлять перенос текстовых команд на удаленный компьютер с помощью командной строки. Это практически терминальный доступ, только ограниченный режимом командной строки. Положительной стороной этого метода является экономия и уменьшение расхода трафика в тысячи раз по сравнению с графическим режимом.

Nassi - система общения пользователей в локальной сети

Для обмена сообщениями и файлами в локальной сети удобно использовать чат под названием **Net Work Assistant** (Nassi). Установим эту программу на Windows Server и Windows XP и запустим ее (рис. 8).

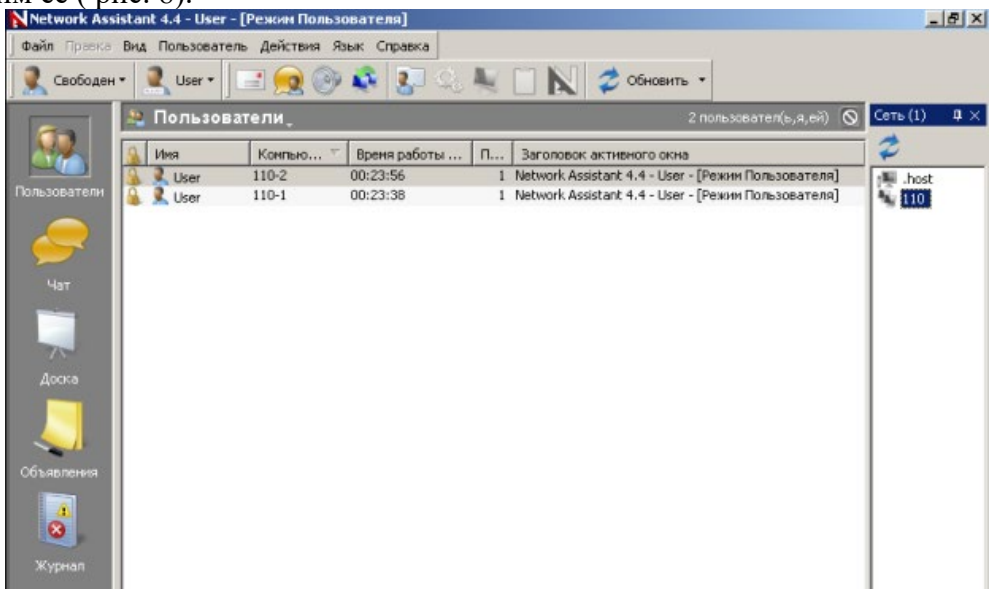


Рис. 8. Network Assistant (интерфейс)

Теперь вы можете отправлять с одного ПК на другой сообщения, файлы, разобраться в этой простой программе совсем не сложно. Например, вы можете на удаленный ПК послать звуковой сигнал (типа телефонного звонка), который сигнализирует ему "Подойди к ПК, поговорим".

Основные возможности Nassi:

- Многоканальный чат

- Общая доска для рисования
- Мгновенные сообщения
- Передача файлов
- Управление процессами на удаленном компьютере
- Сигнализаторы удаленных событий
- И другое...

Задание 1. Групповая работа в чате и на доске для рисования

Войдите в **Чат** и попробуйте пообщаться с другими ПК. Для этого внизу есть *поле* ввода, в которое можно набрать нужное сообщение и нажать /Enter/. Для отправки личного сообщения, щелкните по нику пользователя в списке справа и в появившееся окно вводите ваше сообщение. Если же хотите, чтобы личное сообщение было отправлено всем, то вызовите контекстное *меню*(правым щелчком мыши) на списке пользователей главного окна, и выберите "сообщение всем". Перейдите на пиктограмму **Доска**. Здесь все пользователи могут вместе (одновременно) рисовать общий рисунок. Изучите другие возможности программы самостоятельно.

Примечание

Если брандмауэр не выключен, то программа **Nassi** должна быть включена в его исключения.

Команда отправки текстовых сообщений Net send

Текстовые сообщения по локальной сети можно отправлять не только в специальных программах (Radmin, Nassi), но и из командной строки *Windows* XP. *Команда* **Net send** служит для отправки текстовых сообщений другому компьютеру, доступному в сети. Однако, для того, чтобы *команда* работала, первоначально необходимо включить службу доставки сообщений. Для этого зайдите в **Панель управления**. Откройте папку **Администрирование, Службы**. Найдите в списке службу сообщений (рис. 9).

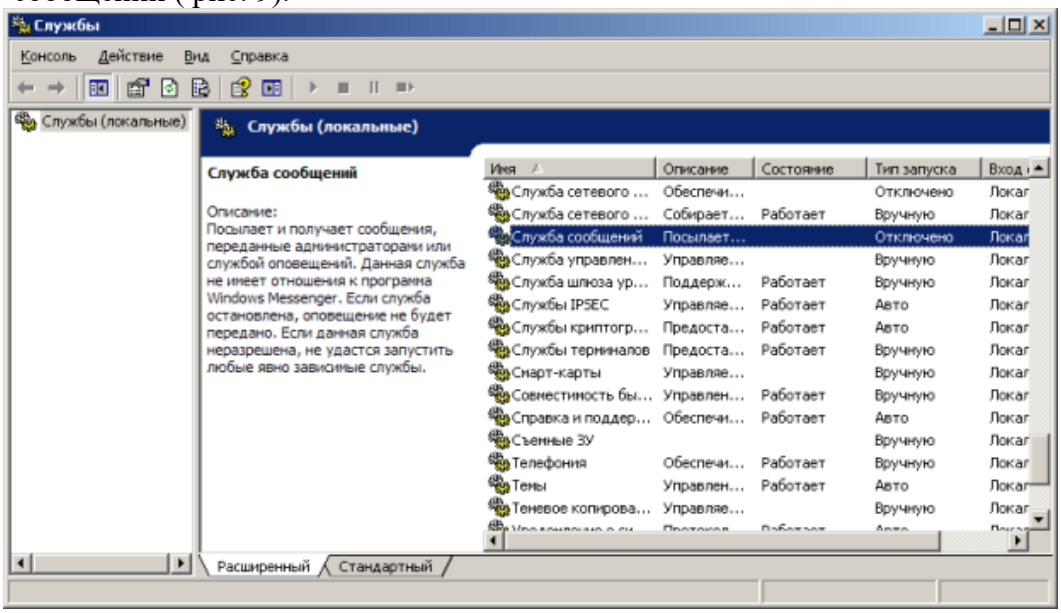


Рис. 9. Служба сообщений отключена

Откройте ее свойства. Выберите *значение* **Авто** из списка **Тип запуска,** если вы хотите, чтобы служба автоматически запускалась при загрузке *Windows*. Затем нажмите на кнопку **Пуск** и **ОК** (рис. 10 и рис. 11).

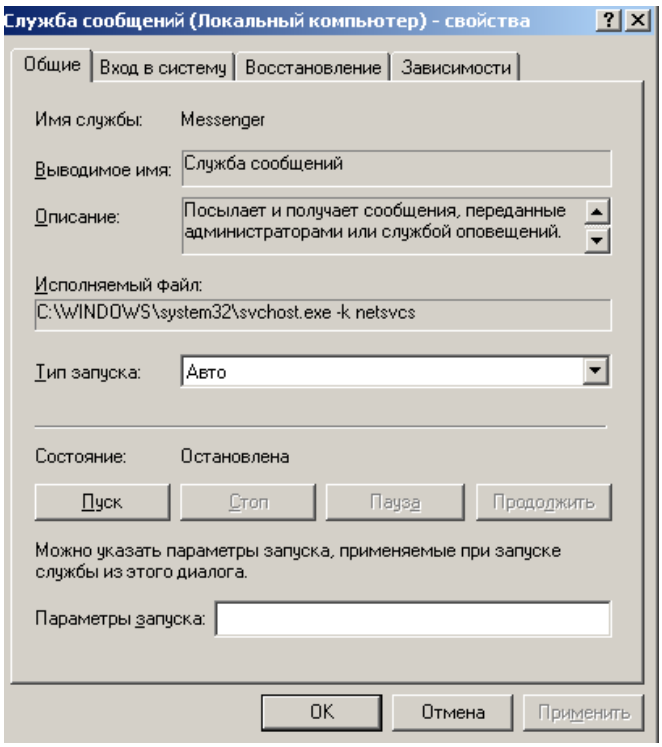


Рис. 10. Окно Служба сообщений

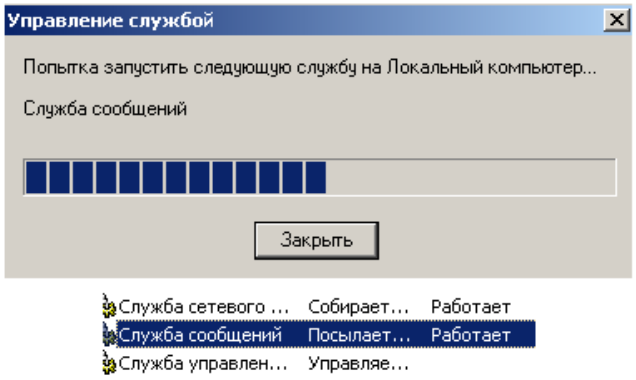
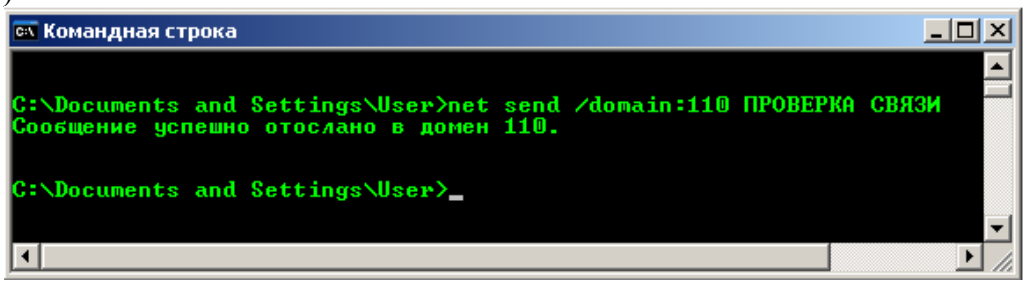


Рис. 11. Служба сообщений работает

Давайте рассмотрим примеры использования команды **net send** при отправке сообщений в рабочей группе (домене) 110. Чтобы отправить сообщение всем пользователям в рабочей группе 110 введите: **net send /domain:110 ПРОВЕРКА СВЯЗИ.** Другой вариант подобной команды: чтобы отправить сообщение всем пользователям в вашем домене введите: **net send * проверка связи** (рис. 12 и 13)



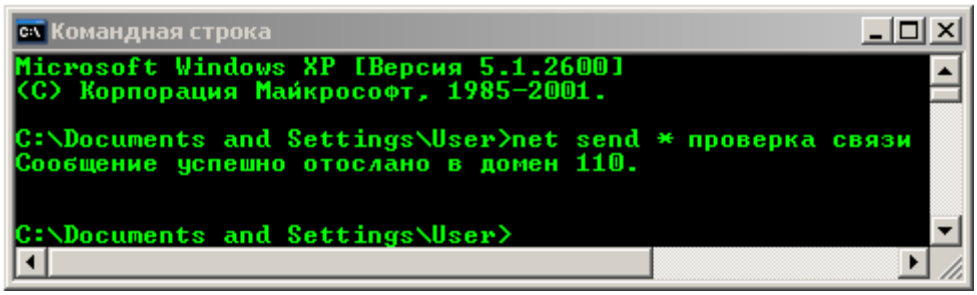


Рис. 12. Пример успешной отправки сообщения всем пользователям домена 110

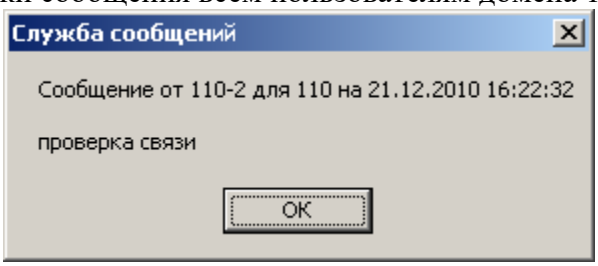


Рис. 13. Пример успешного получения сообщения от ПК 110-2 в рабочую группу 110

Чтобы отправить сообщение конкретному пользователю, например, 110-1, введите: **net send 110-1 ПРИВЕТ!** (рис. 14).

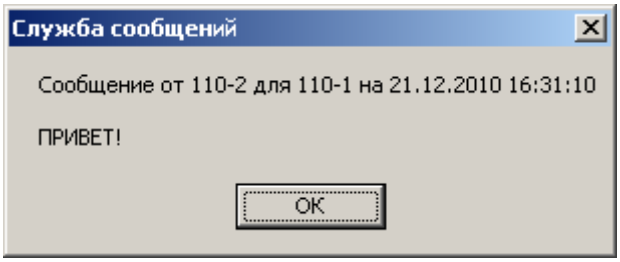


Рис. 14. Сообщение пользователю 110-1 доставлено

В *Windows* XP есть еще одна возможность отправки сообщений по сети. Выполните команды **Панель управления-Администрирование-Управление компьютером**. Дальше: **Действие-Все задачи-Отправка сообщения консоли**. Далее выбираете ПК и отправляете ему текст (рис. 15).

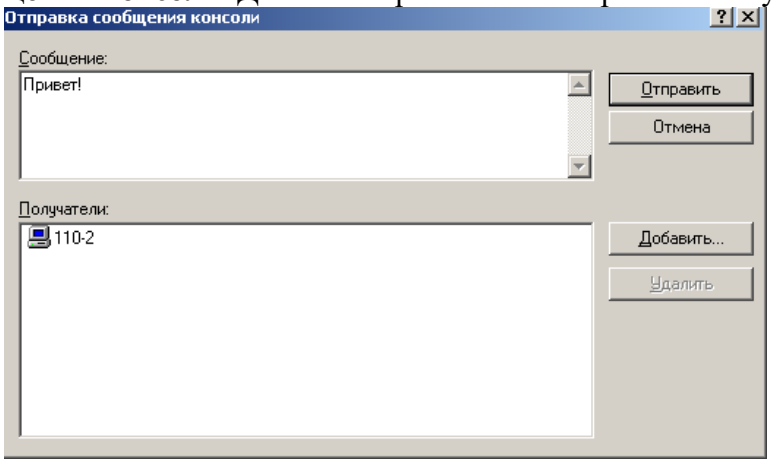


Рис. 15. Вариант отправки сообщения по сети без команды >net send

Примечание

Команда **net send** может блокироваться брандмауэром, поэтому его необходимо настроить или отключить (не желательно).

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.
Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 5 «Использование прикладного протокола FTP»

Цель работы: В результате выполнения лабораторной работы обучающиеся научится использовать протокол прикладного уровня FTP..

В процессе занятия решаются следующие задачи:

1. Изучить принцип устройства протоколов прикладного уровня на примере протокола FTP;
2. научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

FTP (англ. *File Transfer Protocol* — протокол передачи файлов) — стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). FTP часто используется для загрузки сетевых страниц и других документов с частного устройства разработки на открытые сервера хостинга.

Протокол построен на архитектуре "клиент-сервер" и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. Пользователи FTP могут пройти аутентификацию, передавая логин и пароль открытым текстом, или же, если это разрешено на сервере, они могут подключиться анонимно. Можно использовать протокол SSH для безопасной передачи, скрывающей (шифрующей) логин и пароль, а также шифрующей содержимое.

Первые клиентские FTP-приложения были интерактивными инструментами командной строки, реализующими стандартные команды и синтаксис. Графические пользовательские интерфейсы с тех пор были разработаны для многих используемых по сей день операционных систем. Среди этих интерфейсов как программы общего веб-дизайна вроде Microsoft Expression Web, так и специализированные FTP-клиенты (например, FileZilla).

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, и даже до TCP/IP, в 1971 году. В первое время он работал поверх протокола NCP. Он и сегодня широко используется для распространения ПО и доступа к удалённым хостам.

TELNET (англ. TErminaL NETwork) — сетевой протокол для реализации текстового интерфейса по сети (в современной форме — при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Современный стандарт протокола описан в RFC 854. Выполняет функции протокола прикладного уровня модели OSI.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Говоря «протокол» подразумеваем договорённость о стандарте взаимодействия, установленную между участниками этого взаимодействия. Попробуем на примере понять как же устроены протоколы изнутри.

Протоколы низких уровней сложны в восприятии хотя бы потому, что их использование часто сопряжено с построением специальных битовых последовательностей. Кроме того, для того чтобы посмотреть и построить пакет (или сообщение) какого-нибудь протокола сетевого или транспортного уровня нам не обойтись без специальных средств.

Однако среди протоколов прикладного уровня часто встречаются текстовые (text based) протоколы. Взаимодействие с использованием таких протоколов не сильно отличается от общения двух собеседников в чате. Одним из таких текстовых протоколов прикладного уровня является FTP.

Протокол текстовый, значит мы можем соединиться с FTP-сервером и, зная правила, сыграть роль клиента. Но! Все программы-FTP-клиенты знают как устроен протокол, общаются с сервером, а пользователю показывают результат этого общения (списки файлов, папок и т.п.). Мы же хотим сами посылать команды, получать на них ответы и обрабатывать их лично. Значит нам потребуется необычный FTP-клиент.

Для реализации передачи любых (почти любых) текстовых сообщений по сети был разработан протокол telnet. По своим свойствам он похож на телеграф. Используя клиент этого протокола, мы сможем соединиться к FTP-серверу, при этом telnet-клиент не будет сам слать какие-либо команды (ведь он не знает как устроен FTP), но позволит нам набрать и отправить по установленному соединению любую текстовую команды.

Теперь нужно определить как же соединиться с FTP-сервером. Узнать это подробно можно из спецификации протокола FTP. Но это изучение вы проделаете самостоятельно. Сейчас же узнаем некоторые важные для выполнения практики сведения.

FTP использует два канала для связи. Один канал называется управляющим — по нему передаются только команды, а второй канал называется каналом данных — по нему передаются данные, например, содержимое файла, закачиваемого на сервер или скачиваемого с него.

Другой нужный нам для практики факт — *FTP* ***может работать в двух режимах*****: активном и пассивном**. В активном режиме FTP-сервер сам инициирует соединение (образование канала данных) с клиентом и посылает клиенту данные. В пассивном режиме сервер указывает клиенту номера портов, на которые нужно соединиться, чтобы оттуда получить данные, запрошенные командами через управляющий канал.

Поскольку мы будем использовать не программный FTP-клиент, работать в активном режиме не получится (объясните почему). Используем для практики пассивный FTP-режим.

Чтобы соединиться с FTP-сервером, вызовем из командной строки telnet-клиент, указав ему хост и порт 21 (FTP слушает 21 порт). Предлагается соединиться с файловым сервером техникума.

```
1. telnet 192.168.10.1 21
```

TelNet-клиент напишет что-то подобное:

```
1. Trying 192.168.10.1...
2. Connected to 192.168.10.1.
3. Escape character is '^]'.
4. 220 FTP Server ready.
```

Это означает, что FTP-сервер готов и ждёт команд. Какие команды мы можем отправлять, указано в RFC. Например, можно использовать следующие команды:

1. SYST — возвращает тип системы
2. USER <имя пользователя> — отправка логина
3. PASS <пароль> — отправка пароля
4. PWD — получение имени текущей (рабочей) папки
5. CWD — смена текущей (рабочей) папки
6. QUIT — завершение соединения

7. PASV — переход в пассивный режим
8. LIST — получение списка файлов (список будет передан через канал данных)

Попробуйте соединиться с сервером 192.168.10.1. Используйте команду SYST, чтобы узнать тип системы. Затем аутентифицируйтесь, используя свои логин и пароль. Узнайте имя текущей папки. Затем завершите сеанс связи командой QUIT.

Только что вы сыграли роль клиента, взаимодействуя с файловым сервером по протоколу FTP.

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 6 «Создание виртуальной локальной сети»

Цель работы: В результате выполнения лабораторной работы научиться устанавливать VPN сервер и производить подключение к VPN серверу с клиентской машины.

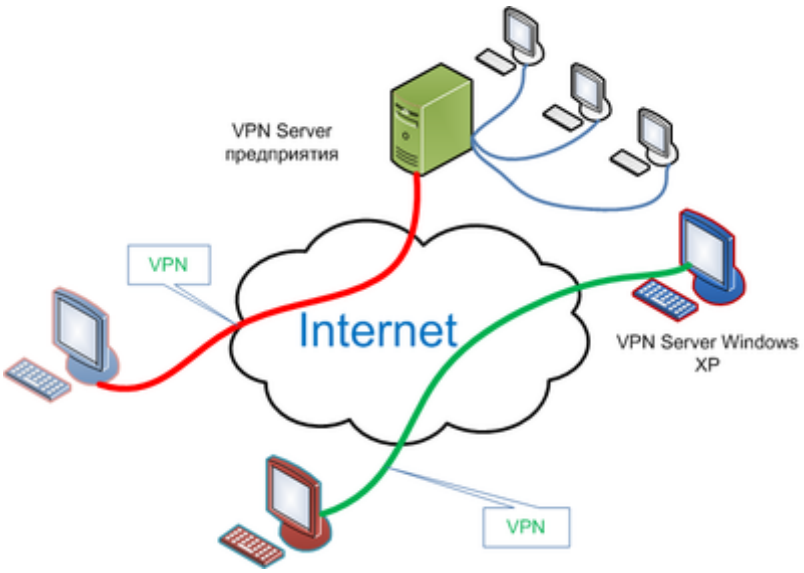
В процессе занятия решаются следующие задачи:

1. Изучить порядок установки настройки VPN сервер на Windows XP? Windows Server 2003;
2. Изучить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Технология виртуальных частных сетей (VPN) позволяет объединять сегменты одной сети, с помощью другой сети, например Интернета. Это достигается путем туннелирования, т. е. создания туннеля, по которому данные передаются через Интернет или другую публичную сеть. При этом обеспечивается безопасность и другие возможности частных сетей. Хотя данные по туннелям VPN

передаются по Интернету, с точки зрения пользователя это выглядит как передача данных между двумя сетями по выделенному частному каналу (VPN).



Общие сведения о VPN

Технология VPN предоставляет возможность подключения к частной сети (например, к офисной сети) с помощью ресурсов общедоступной сети (например, Интернета).

Она объединяет преимущества подключений удаленного доступа с простотой и гибкостью подключений к Интернету. Использование подключения к Интернету позволяет подключаться к ресурсам, расположенным по всему миру, а также подключаться к офисной сети, установив соединение по местной линии с любым поставщиком услуг Интернета. Если офисная сеть и домашний компьютер используют высокоскоростное подключение к Интернету (например, с помощью кабельного модема или технологии DSL), то между ними можно организовать канал обмена данными, пропускная способность которого будет многократно превышать пропускную способность соединения через аналоговый модем.

Виртуальные частные сети проводят шифрование данных и проверку подлинности, что гарантирует конфиденциальность пересылаемых через Интернет данных и позволяет подключаться к сети только пользователям, имеющим соответствующие права. Для обеспечения безопасности данных Windows XP использует протоколы туннелирования PPTP и L2TP. В процессе работы этих протоколов создаются туннели, обеспечивающие высокую защищенность данных при передаче между компьютерами через Интернет.

Технология VPN также позволяет использовать общедоступную сеть для создания защищенных каналов связи с различными компаниями или филиалами одной компании. С точки зрения пользователя VPN-подключение через Интернет работает как выделенный канал глобальной сети.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

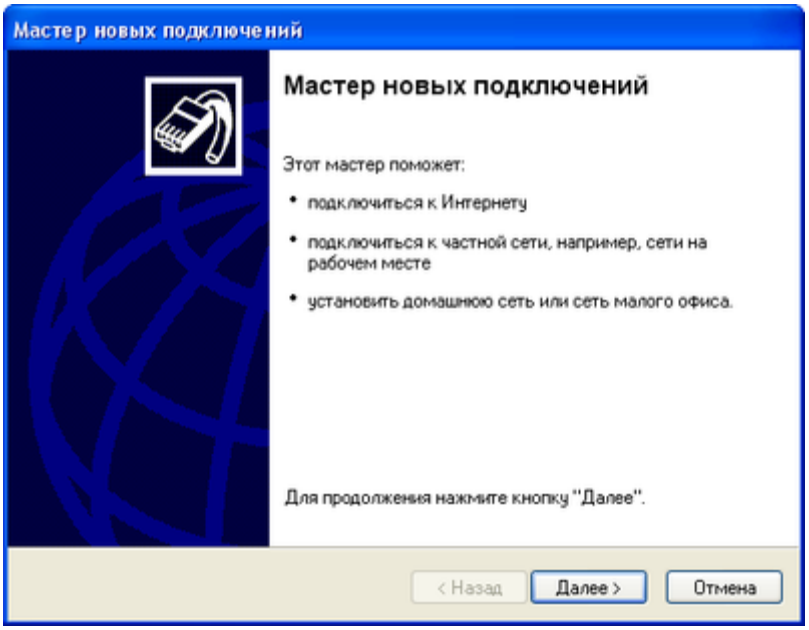
Настройка VPN сервера в Windows XP

Запуск мастера новых подключений

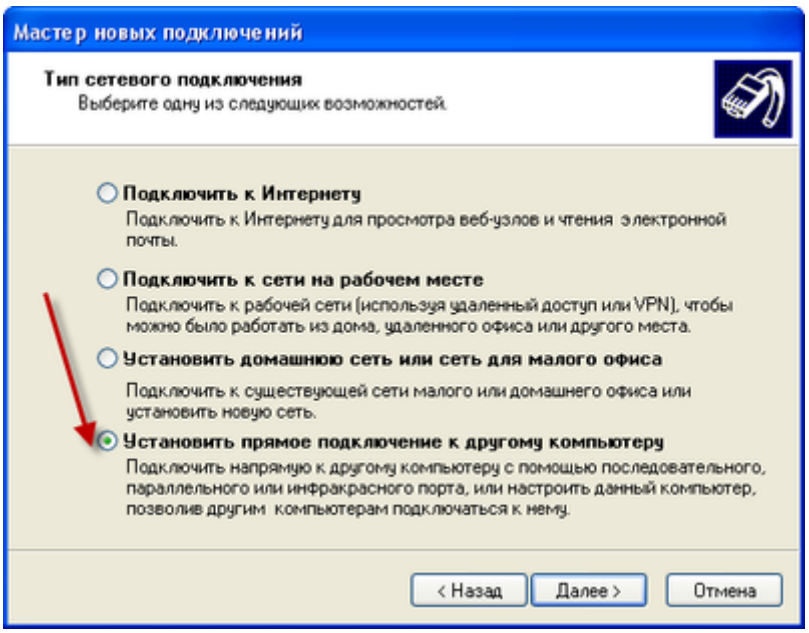
Пуск => Панель Управления => Сетевые Подключения

Файл => Новое Подключение

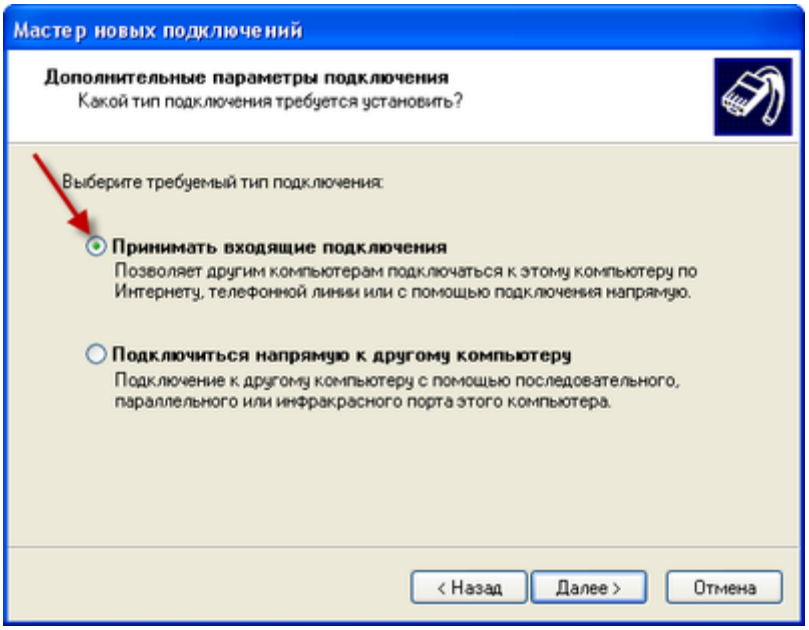
Нажимаем Далее



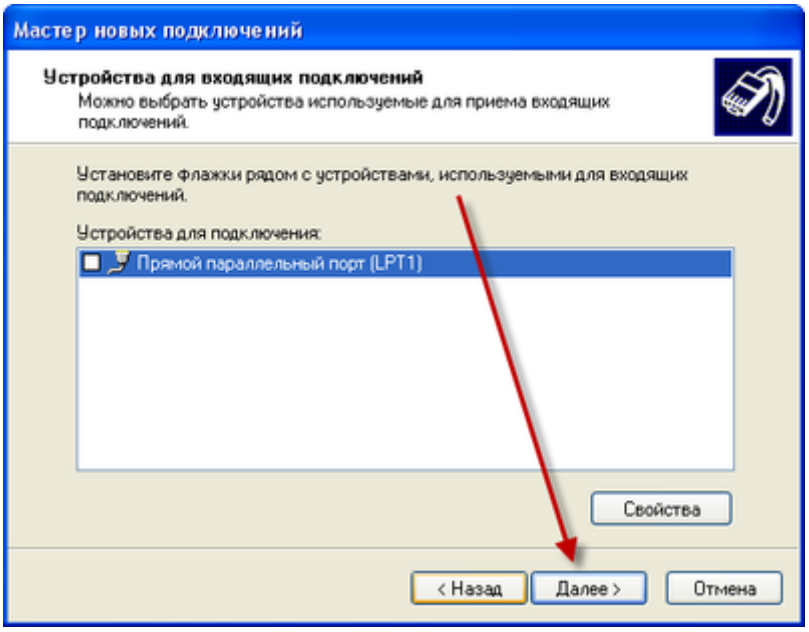
Выбор типа сетевого подключения
Выбираем *Установить прямое подключение к другому компьютеру*
Нажимаем *Далее*



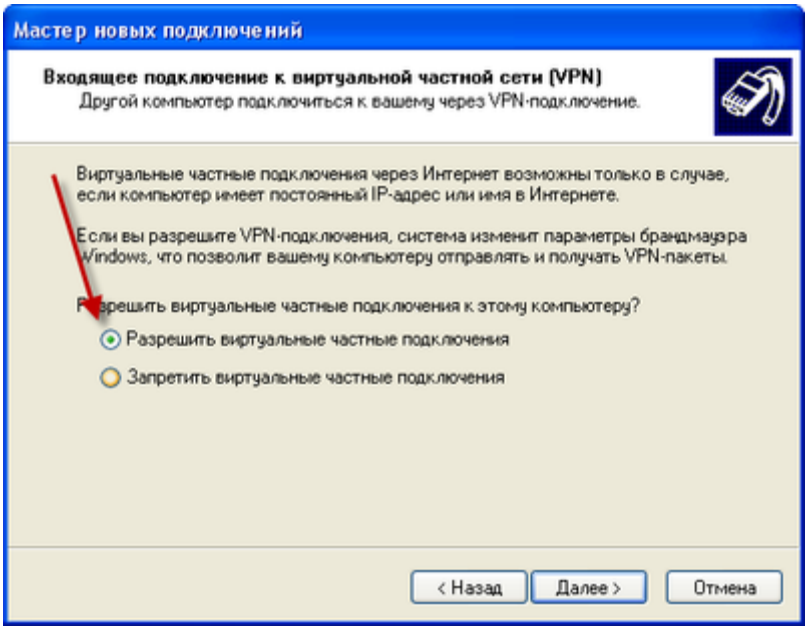
Установка дополнительных параметров подключения
Выбираем *Принимать входящие подключения*
Нажимаем *Далее*



Игнорирование устройств для входящих подключений
Если у вас есть модем или ЛПТ то проигнорируйте нажмите кнопку далее

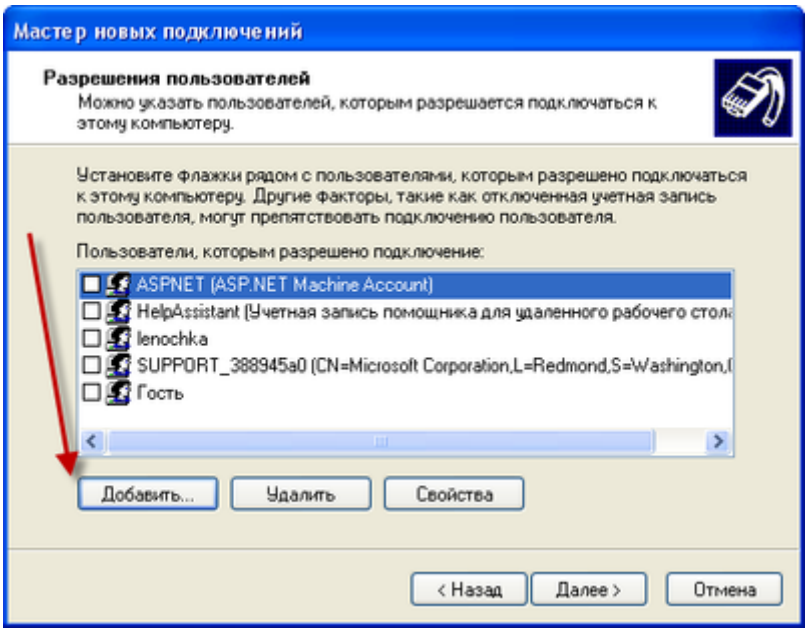


Настройка входящих подключения к виртуальной частной сети (VPN)
Выбираем *Разрешить виртуальный частные подключения!*
Нажимаем *Далее*



Разрешения пользователей VPN

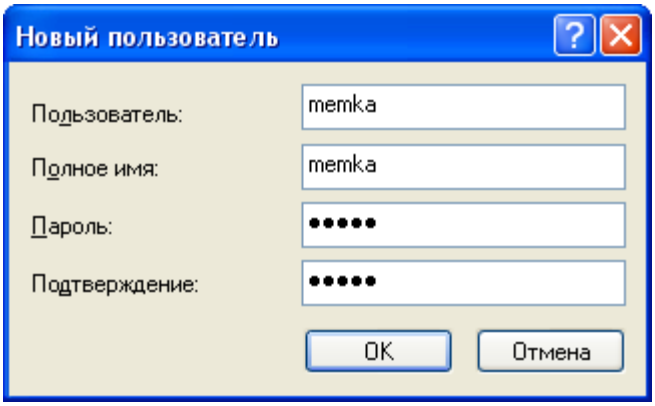
Нажимаем кнопочку *Добавить*



Добавление нового пользователя

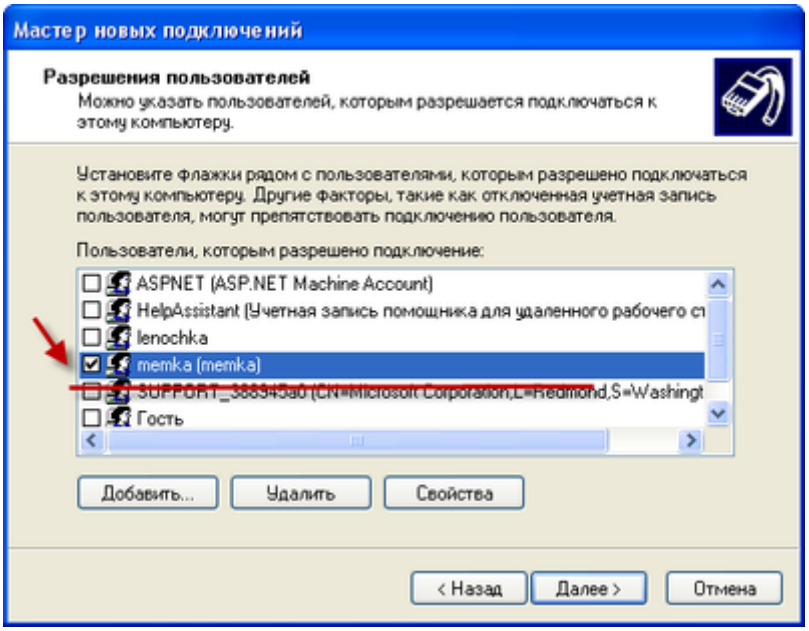
Заполняем все поля. *Новый пользователь является пользователем VPN*, зайти под этим логином на компьютер не получиться.

Пользователь созданный через это окно может только создать VPN соединение.



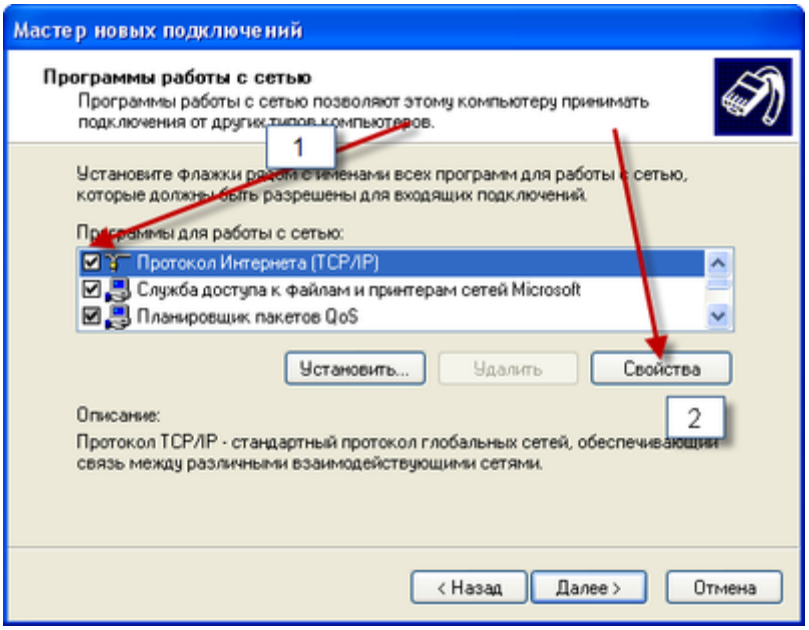
Выбор пользователей

Удостоверяемся что стоит галочка напротив нашего нового пользователя!!



Выбор программ работы с сетью

Выделяем "проток интернета TCP/IP" и нажимаем кнопку свойства

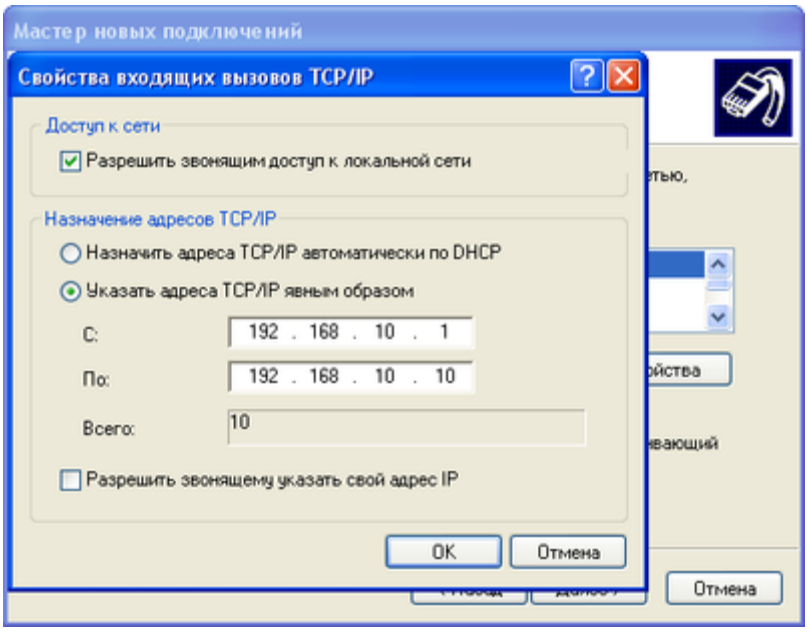


Настройка входящих вызовов TCP/IP

Ставим галочку "разрешить звонящим доступ к локальной сети!"

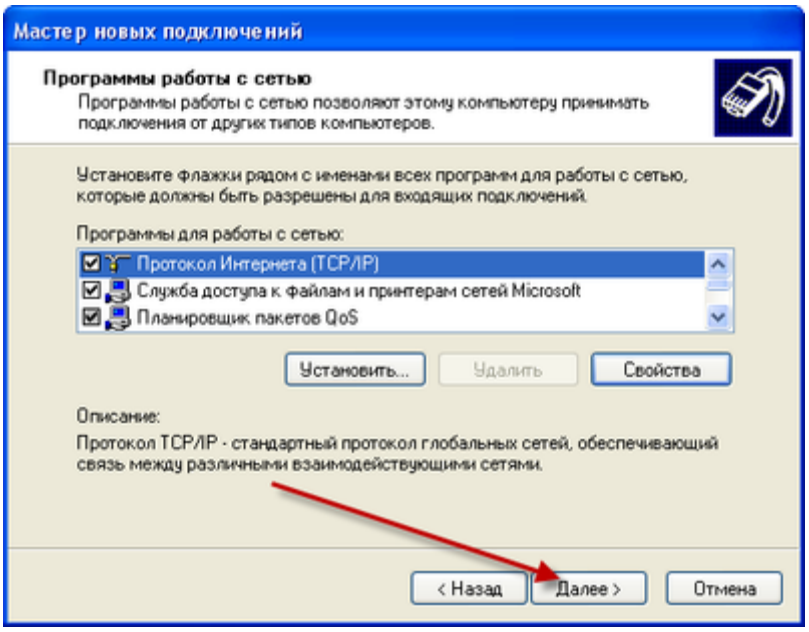
Ставим точку "указать адреса TCP/IP явным образом" и вписываем как на рисунке!

Проверяем количество доступных адресов, если нужно больше то увеличиваем последнюю цифру второго поля и нажимаем кнопку ОК

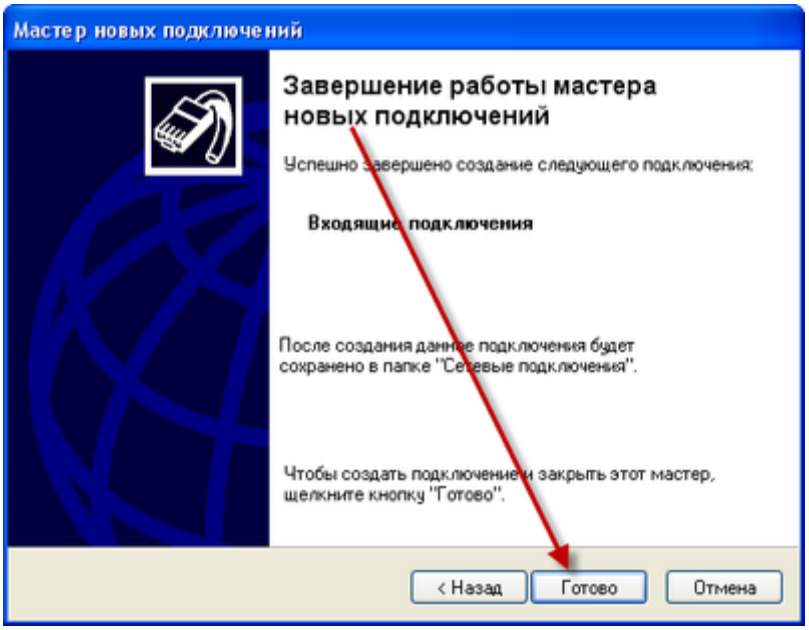


Завершение работы мастера новых подключений

Нажимаем *Далее*



Готово



Чтобы установить подключение, выполните следующие действия.

1. Используйте один из следующих способов.
   - Нажмите кнопку **Пуск**, выберите пункт **Подключение** и щелкните значок нового подключения.
   - Если ярлык подключения был добавлен на рабочий стол, дважды щелкните его.
2. Если подключение к Интернету в данный момент не установлено, система Windows предложит подключиться к Интернету.
3. После подключения к Интернету сервер VPN запросит имя и пароль. Введите имя пользователя и пароль, и нажмите кнопку **Подключиться**. К ресурсам удаленной сети после подключения можно будет обращаться как к ресурсам локальной сети.
4. Для отключения от сервера VPN щелкните значок подключения правой кнопкой мыши и выберите команду **Отключить**.

Примечание. Если получить доступ к общим ресурсам удаленной сети по имени компьютера не удается, используйте IP-адрес удаленного компьютера, чтобы установить подключение с помощью пути UNC (\\<IP-адрес>\ресурс). Добавьте в файл Windows\System32\Drivers\hosts запись, сопоставляющую имя удаленного сервера с его IP-адресом. После этого имя компьютера можно использовать в соединении UNC (\\имя_сервера\ресурс).

Время выполнения работы 90 мин;
Контрольные вопросы

Сделайте выводы.
Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература
Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 7 «Настройка фильтрации TCP/IP»

Цель работы: В результате выполнения лабораторной работы научиться производить настройку фильтрации TCP/IP на компьютерах под управлением Microsoft Windows .

В процессе занятия решаются следующие задачи:
1. Изучить порядок настройки фильтрации на Windows XP, Windows Server 2003;
2. Изучить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Windows XP поддерживает несколько методов контроля входящего доступа. Одним из наиболее простых и одновременно самых мощных является фильтрация TCP/IP. Фильтрация TCP/IP доступна на всех компьютерах под управлением Windows XP с установленным стеком протокола TCP/IP.

Фильтрация TCP/IP полезна с точки зрения безопасности, поскольку работает в режиме ядра. В противоположность этому другие методы контроля входящего доступа на компьютерах под управлением Windows XP (например, фильтры политики IPSec или сервер маршрутизации и удаленного доступа) зависят от процессов режима пользователя или службы рабочих станций и серверов.

Для контроля входящего доступа по протоколу TCP/IP может быть использована комбинированная схема с применением фильтрации TCP/IP, фильтров IPSec и фильтрации пакетов маршрутизации и удаленного доступа. Такой метод особенно эффективен, если требуется контролировать как входящие, так и исходящие пакеты протокола TCP/IP. Фильтрация TCP/IP позволяет следить только за входящим доступом.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Настройка безопасности протокола TCP/IP

Чтобы настроить безопасность протокола TCP/IP, выполните следующие действия:

1. Нажмите кнопку **Пуск**, выберите пункт **Настройка**, а затем **Панель управления** и дважды щелкните значок **Сеть и удаленный доступ к сети**.
2. Щелкните правой кнопкой мыши интерфейс, для которого будет настраиваться контроль входящего доступа, и выберите команду **Свойства**.
3. В списке **Отмеченные компоненты используются этим подключением** выберите элемент **Протокол Интернета (TCP/IP)** и нажмите кнопку **Свойства**.
4. В окне **Свойства протокола Интернета (TCP/IP)** нажмите кнопку **Дополнительно**.
5. Откройте вкладку **Параметры**.
6. Выберите параметр **Фильтрация TCP/IP** и нажмите кнопку **Свойства**.
7. Установите флажок **Задействовать фильтрацию TCP/IP (все адаптеры)**. Установка этого флажка приводит к включению фильтрации для всех адаптеров, однако настраивать фильтры необходимо отдельно для каждого адаптера. Одни и те же фильтры не применяются ко всем адаптерам.
8. В этом окне имеются три столбца:

TCP-порты
UDP-порты
IP-протоколы

В каждом столбце необходимо выбрать одно из следующих значений:

Можно все. Для разрешения всех пакетов трафика по протоколу TCP или UDP необходимо выбрать значение **Можно все**.

Только. Чтобы пропускать только определенный трафик по протоколу TCP или UDP, установите значение**Только**, нажмите кнопку **Добавить** и введите в диалоговом окне **Добавление фильтра** соответствующий порт.

Для блокировки всего трафика по протоколу UDP или TCP установите значение **Только**, но не добавляйте номера портов в столбце **UDP-порты** или **TCP-порты**. Нельзя заблокировать трафик по протоколу UDP или TCP, установив значение **Только** для столбца **IP-протоколы** и исключив IP-протоколы 6 и 17.

Нельзя заблокировать сообщения ICMP, даже если установить значение **Только** в столбце **IP-протоколы** и не включать IP-протокол 1.

С помощью фильтрации TCP/IP возможен контроль только входящих пакетов. Использование этой функции не оказывает влияния на исходящие пакеты и порты откликов, созданные для ответов на внешние запросы. Для осуществления контроля за исходящим доступом используются политики IPSec и фильтрация пакетов.

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

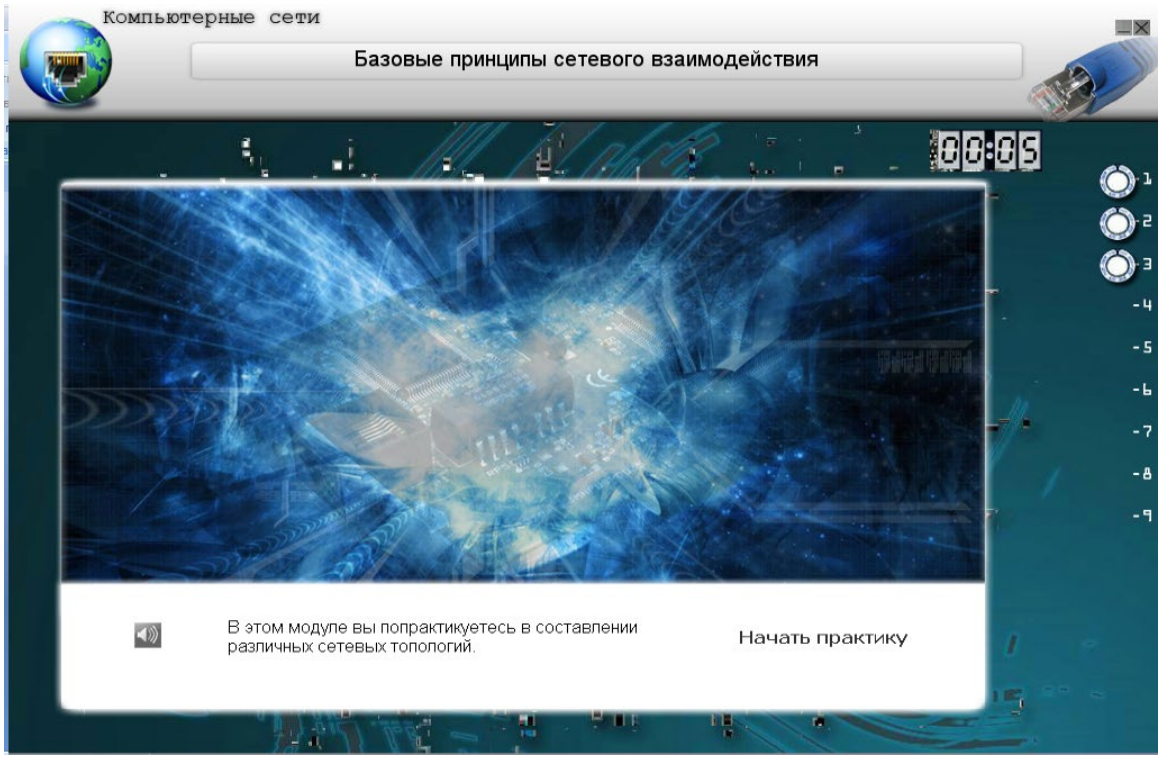
Рекомендуемая литература

Рекомендуемая литература

Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

ЭОР «Базовые принципы сетевого взаимодействия» (практическая работа)



Критерии оценивания

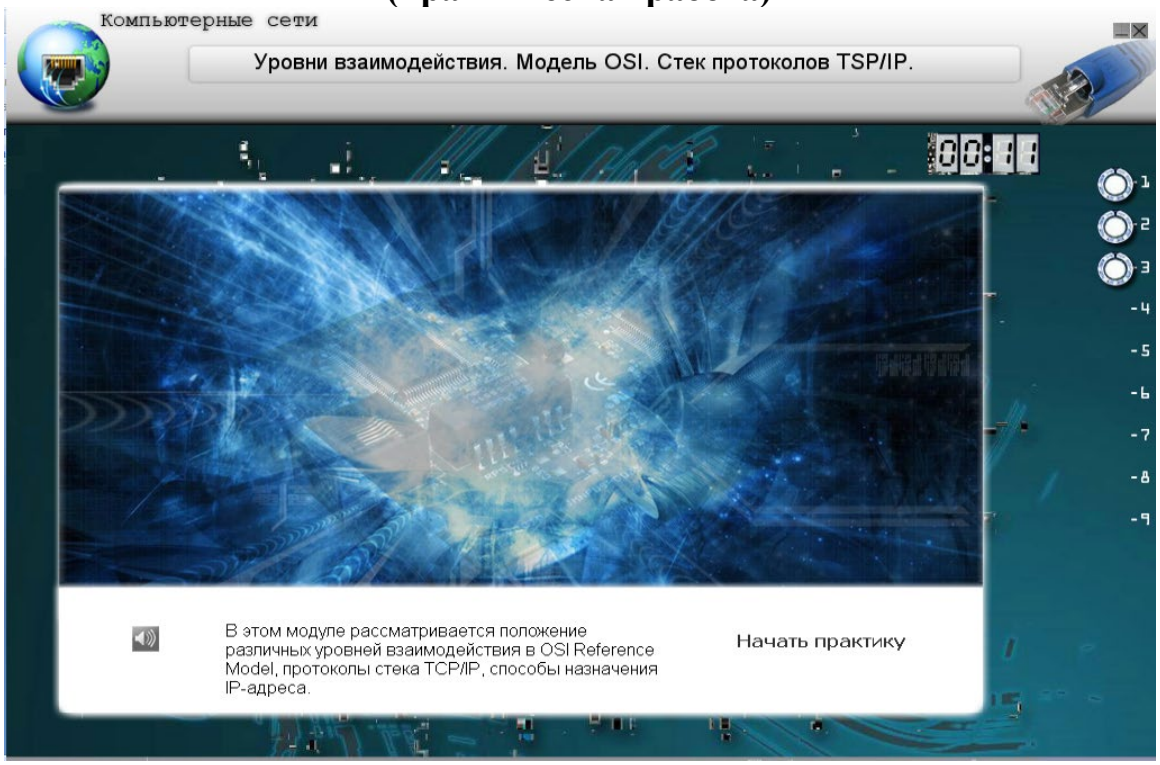
Работа выполнена на:

100%- «5»

75% - «4»

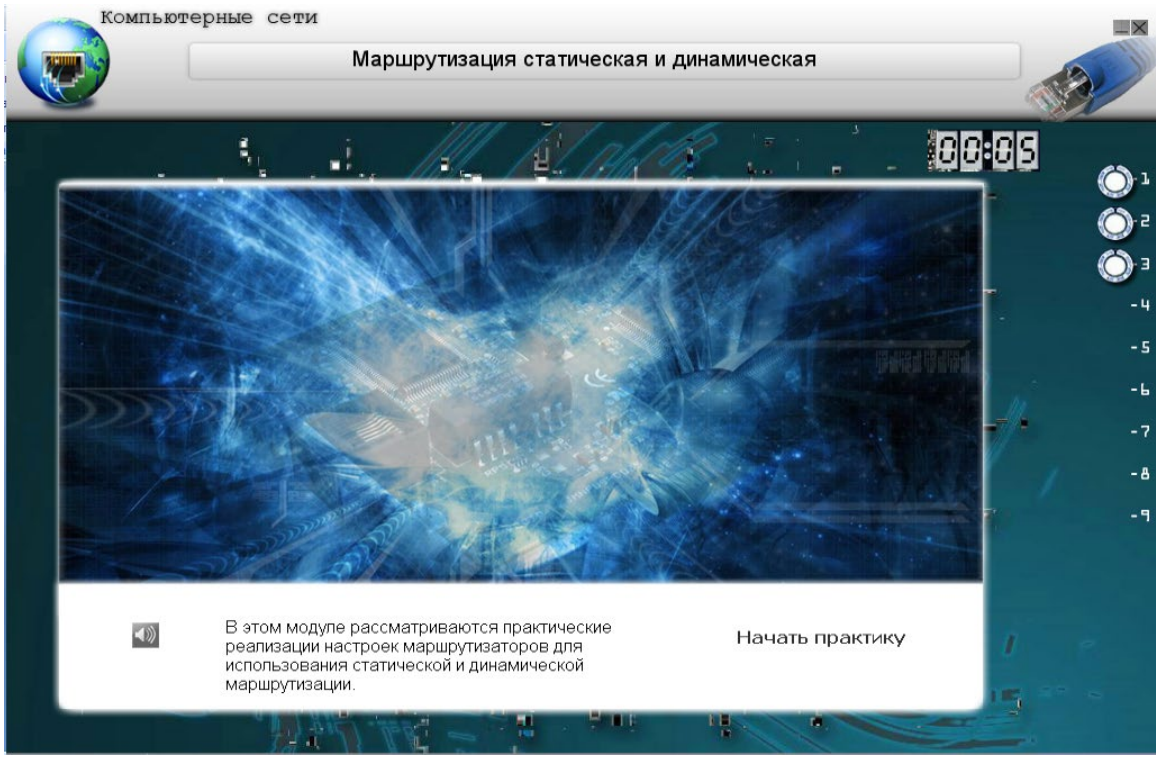
60% -«3»

ЭОР «Уровни взаимодействия. Модель OSI. Стек протоколов TCP/ IP» (практическая работа)



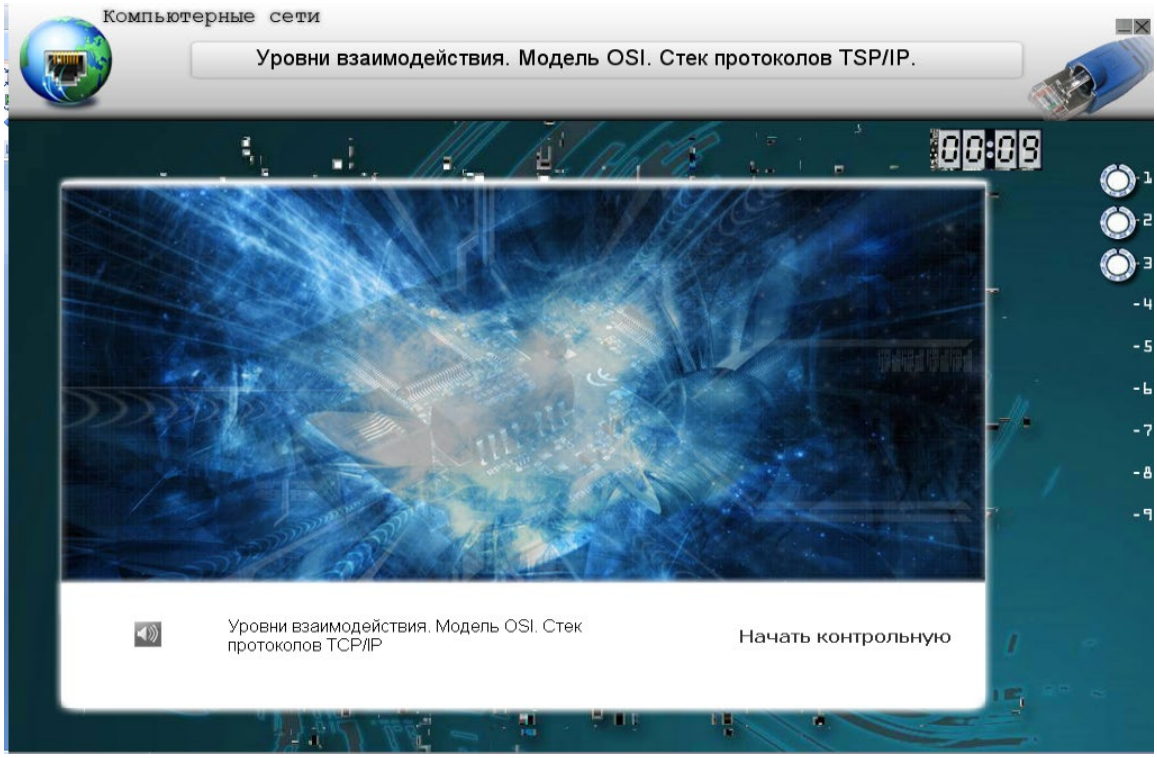
Критерии оценивания
Работа выполнена на:
100%- «5»
75% - «4»
60% -«3»

ЭОР «Маршрутизация статическая и динамическая»
(практическая работа)



Критерии оценивания
Работа выполнена на:
100%- «5»
75% - «4»
60% -«3»

Контрольная работа
ЭОР «Уровни взаимодействия. Модель OSI. Стек протоколов TCP/ IP»
(контрольная работа)



Критерии оценивания

Работа выполнена на:

90%- «5»

75% - «4»

60% -«3»

Тема 1.3. Методы передачи данных в глобальных сетях

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 8 «Дополнительные протоколы глобальных сетей»

Цель работы: В результате выполнения лабораторной работы изучить дополнительные протоколы глобальных сетей.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Протокол SLIP

Перед тем как закончить обсуждение методов передачи данных в глобальных сетях, следует познакомиться с тремя протоколами глобальных сетей, которые используются для удаленных коммуникаций, осуществляемых в этих сетях.

Два из этих протоколов (Serial Line Internet Protocol, SLIP и Point-to-Point Protocol, PPP) служат для инкапсуляции одного или нескольких протоколов локальных сетей (например, TCP/IP) при их передаче по каналам глобальной сети. Третий протокол (Signaling System 7, SS7) предназначен для определения самых быстрых маршрутов в телекоммуникационных сетях.

SLIP

Протокол Serial Line Internet Protocol (SLIP) (Межсетевой протокол для последовательного канала) изначально предназначался для UNIX-систем и служит для осуществления двухточечных коммуникаций между компьютерами, серверами и хостами, работающими с TCP/IP. Например, SLIP применяется в том случае, когда пользователь может передавать данные между удаленным домашним компьютером и UNIX-системой, находящейся в офисной локальной сети (рис. 1). Для подключения к UNIX-компьютеру

может использоваться коммутируемая телефонная линия, а коммуникации ведутся с помощью пакетов TCP/IP, инкапсулированных в SLIP.

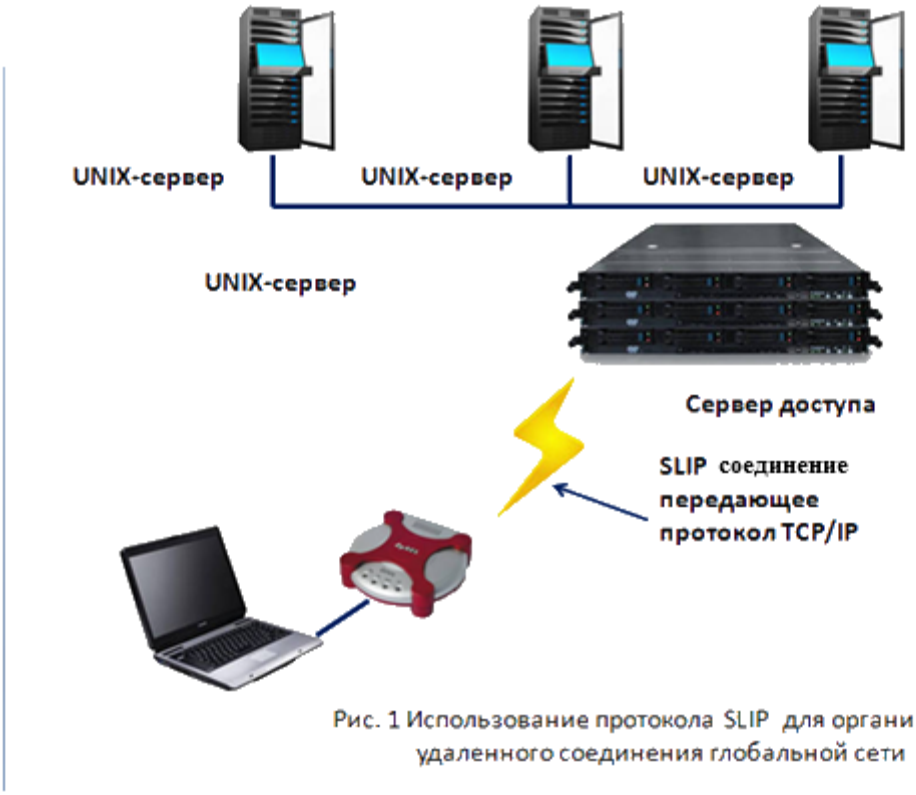


Рис. 1 Использование протокола SLIP для организации удаленного соединения глобальной сети

Для хоста SLIP является протоколом глобальной сети, координирующим сеансы связи по телефонной линии с использованием модемов. После того как протокольная информация (содержащая полезную нагрузку) достигает пункта назначения, заголовок и хвостовик SLIP удаляются и пакет TCP/IP остается в "чистом виде".

Нужно заметить, что SLIP является достаточно старым протоколом удаленных коммуникаций и содержит больше служебной информации, чем протокол PPP. Новой модификацией SLIP является протокол Compressed Serial Line Internet Protocol (CSLIP) (Межсетевой протокол для сжатого последовательного канала), который сжимает заголовок каждого пакета, передаваемого по каналу удаленной связи.

CSLIP уменьшает объем служебной информации SLIP-подключения благодаря тому, что он уменьшает размер заголовка, в результате чего скорость коммуникаций увеличивается. Однако на принимающем узле заголовок, нужно распаковать.

Оба протокола (SLIP и CSLIP) имеют общий недостаток: они не поддерживают аутентификацию сетевого подключения, препятствующую перехвату передаваемых данных. Кроме этого, они не позволяют ускорить передачу данных по соединению, автоматически организуя сетевые коммуникации на нескольких уровнях модели OSI. Еще одним минусом обоих протоколов является то, что они предназначены для асинхронной передачи данных, осуществляемой, например, при модемном соединении. Синхронные коммуникации (например, создание подключения через Интернет) эти протоколы не поддерживают. SLIP нельзя также использовать в том случае, когда сетевой администратор хочет в удаленном режиме (через Интернет) создать новую учетную запись в системах Windows NT Server с помощью средств удаленного администрирования. Систему Windows NT Server можно настроить на работу с протоколом SLIP, установив службы Remote Access Services (RAS), хотя это и не рекомендуется. RAS-сервер позволяет пользователям удаленно подключаться к этому серверу или через этот сервер входить в локальную сеть.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Настройте Windows Server на работу с протоколом SLIP, установив службы Remote Access Services (RAS)

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 9 «Установка и настройка сетевой карты»

Цель работы: В результате выполнения лабораторной работы научиться устанавливать и настраивать сетевую карту.

В процессе занятия решаются следующие задачи:

1. Изучить порядок установки настройки сетевого адаптера Windows XP, Windows Server 2003;
2. Изучить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

В настоящее время сеть Ethernet/Fast Ethernet распространена наиболее широко, ее аппаратура выпускается наибольшим числом производителей, и ее перспективы представляются самыми благоприятными.

Характеристики адаптеров

Сетевые адаптеры (NIC, Network Interface Card) Ethernet и Fast Ethernet могут сопрягаться с компьютером через один из стандартных интерфейсов:

• шина ISA (Industry Standard Architecture);
• шина PCI (Peripheral Component Interconnect);
• шина PC Card (она же PCMCIA).

Типы адаптеров

По конструктивной реализации сетевые платы делятся на:

• внутренние — отдельные платы, вставляющиеся в PCI, ISA или PCI-E слот

• внешние, подключающиеся через USB или PCMCIA интерфейс, преимущественно использовавшиеся в ноутбуках,

• встроенные в материнскую плату

На 100-мегабитных платах устанавливают только разъём для витой пары (8P8C, ошибочно называемый RJ-45).

Рядом с разъёмом для витой пары устанавливают один или несколько информационных светодиодов, сообщающих о наличии подключения и передаче информации.

Шина PCI сейчас практически вытеснила шину ISA и становится основной шиной расширения для компьютеров. Она обеспечивает обмен 32– и 64–разрядными данными и отличается высокой пропускной способностью (теоретически до 264 Мбайт/с), что вполне удовлетворяет требованиям не только Fast Ethernet, но и более быстрой Gigabit Ethernet. Важно еще и то, что шина PCI применяется не только в компьютерах IBM PC, но и в компьютерах PowerMac. Кроме того, она поддерживает режим автоматического конфигурирования оборудования Plug–and–Play. Видимо, в ближайшем будущем на шину PCI будет ориентировано большинство сетевых адаптеров. Недостаток PCI по сравнению с шиной ISA в том, что количество ее слотов расширения в компьютере, как правило, невелико (обычно 3 слота). Но именно сетевые адаптеры подключаются к PCI в первую очередь.

Шина PC Card (старое название PCMCIA) применяется пока только в портативных компьютерах класса Notebook. В этих компьютерах внутренняя шина PCI обычно не выводится наружу. Интерфейс PC Card предусматривает простое подключение к компьютеру миниатюрных плат расширения, причем скорость обмена с этими платами достаточно высока. Однако все больше портативных компьютеров оснащается встроенными сетевыми адаптерами, так как возможность доступа к сети становится неотъемлемой частью стандартного набора функций. Эти встроенные адаптеры опять же подключены к внутренней шине PCI компьютера.

При выборе сетевого адаптера, ориентированного на ту или иную шину, необходимо, прежде всего, убедиться, что свободные слоты расширения данной шины есть в компьютере, включаемом в сеть. Следует также оценить трудоемкость установки приобретаемого адаптера и перспективы выпуска плат данного типа. Последнее может понадобиться в случае выхода адаптера из строя.

Наконец, встречаются еще сетевые адаптеры, подключающиеся к компьютеру через параллельный (принтерный) порт LPT. Главное достоинство такого подхода состоит в том, что для подключения адаптеров не нужно вскрывать корпус компьютера. Кроме того, в данном случае адаптеры не занимают системных ресурсов компьютера, таких как каналы прерываний и ПДП, а также адреса памяти и устройств ввода/вывода. Однако скорость обмена информацией между ними и компьютером в этом случае значительно ниже, чем при использовании системной шины. К тому же они требуют больше процессорного времени на обмен с сетью, замедляя тем самым работу компьютера.

Параметры сетевого адаптера

Конфигурирование адаптера пользователем применялось в основном для адаптеров, рассчитанных на шину ISA. Конфигурирование подразумевает настройку на использование системных ресурсов компьютера (адресов ввода/вывода, каналов прерываний и прямого доступа к памяти, адресов буферной памяти и памяти удаленной загрузки). Конфигурирование может осуществляться путем установки в нужное положение переключателей (джамперов) или с помощью прилагаемой к адаптеру DOS–программы конфигурирования (Jumperless, Software configuration). При запуске такой программы пользователю предлагается установить конфигурацию аппаратуры при помощи простого меню: выбрать параметры адаптера. Эта же программа позволяет произвести самотестирование адаптера. Выбранные параметры хранятся в энергонезависимой памяти адаптера. В любом случае при выборе параметров необходимо избегать конфликтов с системными устройствами компьютера и с другими платами расширения.

При конфигурировании карты сетевого адаптера могут быть доступны следующие параметры:

• номер линии запроса на аппаратное прерывание IRQ

• номер канала прямого доступа к памяти DMA (если поддерживается)

• базовый адрес ввода/вывода

• базовый адрес памяти ОЗУ (если используется)

• поддержка стандартов автосогласования дуплекса/полудуплекса, скорости

• поддержка теггрированных пакетов VLAN (801.q) с возможностью фильтрации пакетов заданного VLAN ID

• параметры WOL (Wake-on-LAN)

В зависимости от мощности и сложности сетевой карты она может реализовывать вычислительные функции (преимущественно подсчёт и генерацию контрольных сумм кадров) аппаратно либо программно (драйвером сетевой карты с использованием центрального процессора).

Серверные сетевые карты могут поставляться с двумя (и более) сетевыми разъёмами. Некоторые сетевые карты (встроенные в материнскую плату) также обеспечивают функции межсетевого экрана (например, nforce).

Конфигурирование адаптера может выполняться и автоматически в режиме Plug–and–Play при включении питания компьютера. Современные адаптеры обычно поддерживают именно этот режим, поэтому их легко может установить пользователь.
В простейших адаптерах обмен с внутренней буферной памятью адаптера (Adapter RAM) осуществляется через адресное пространство устройств ввода/вывода. В этом случае никакого дополнительного конфигурирования адресов памяти не требуется. Базовый адрес буферной памяти, работающей в режиме разделяемой памяти, необходимо задавать. Он приписывается к области верхней памяти компьютера (UMA, Upper Memory Address) в диапазоне адресов A0000h—FFFFFh. В эту же зону адресов помещается и ПЗУ удаленной загрузки (Boot ROM), если предполагается его использование для создания бездисковой рабочей станции. Если используется конфигурирование вручную, то надо следить, чтобы не было конфликтов адресов адаптера с другими устройствами компьютера.

Порядок работы

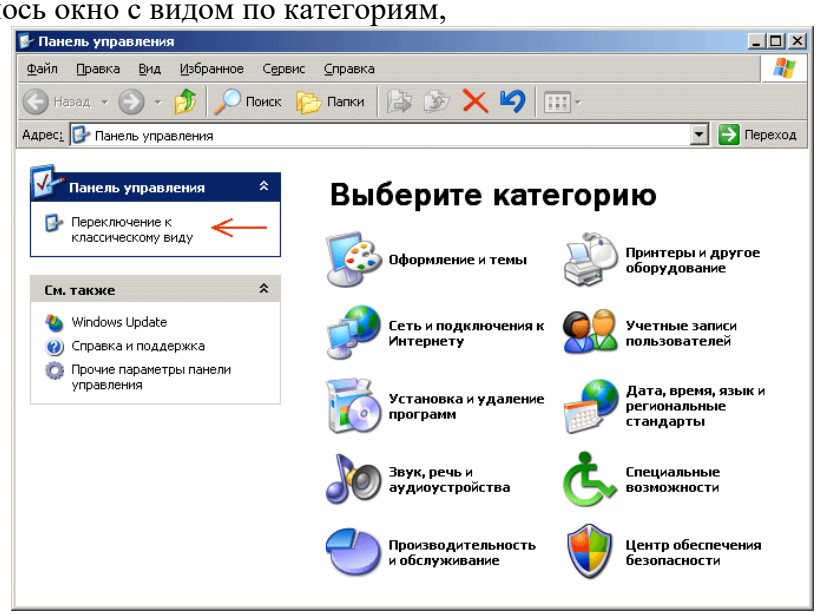
1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

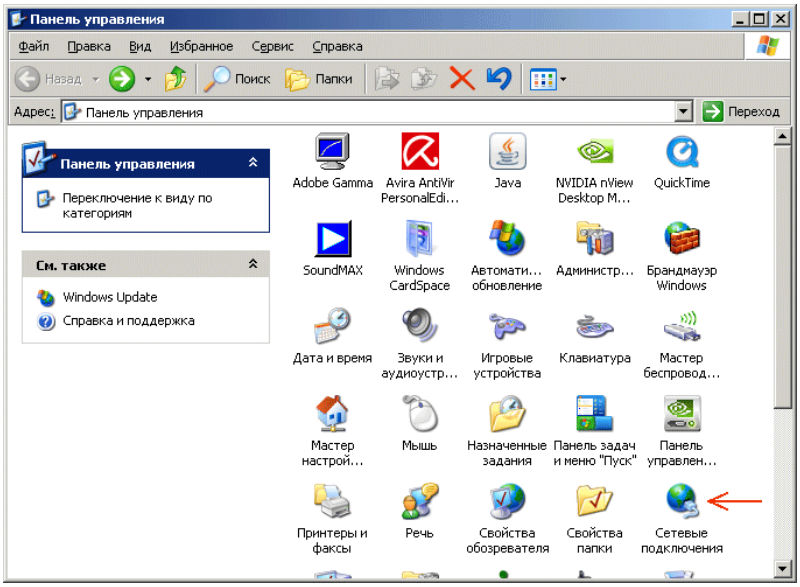
Настройка сетевых параметров

Нажмите "**Пуск**" > "**Настройка**" > "**Панель управлени**я"

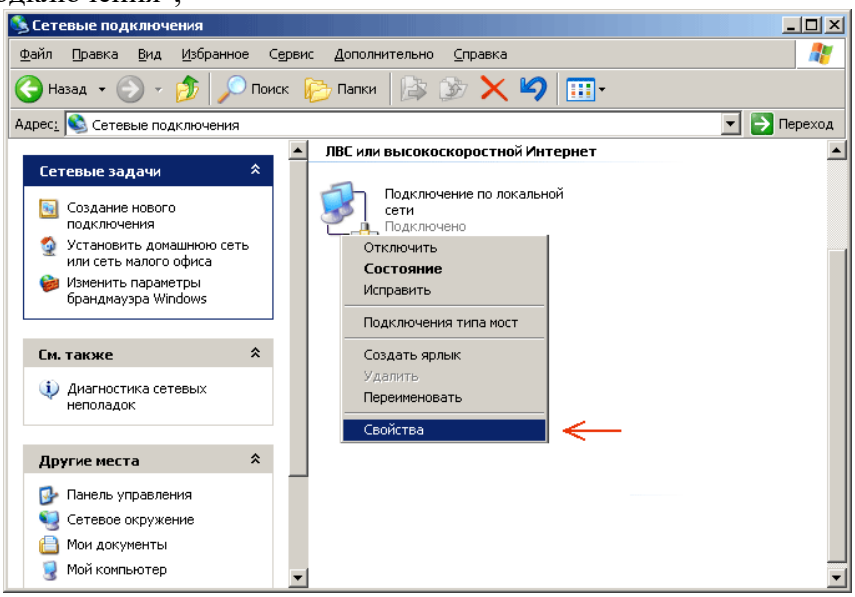
Если на экране появилось окно с видом по категориям,



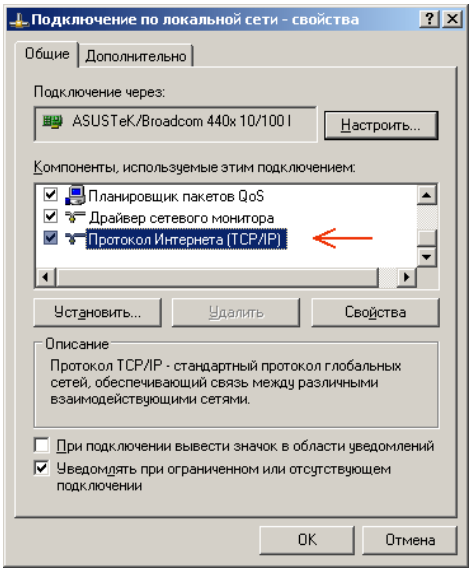
нажмите "Переключение к классическому виду"



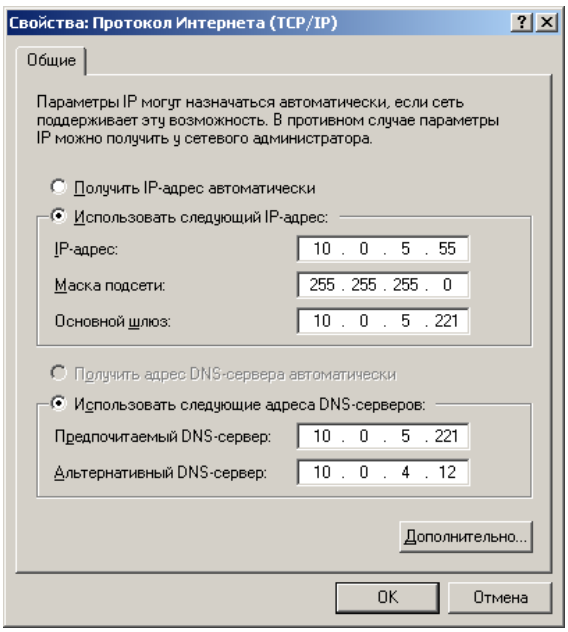
Нажмите "Сетевые подключения",



наведите курсор мыши на "Подключение по локальной сети" и нажмите правую кнопку мыши. Выберите "Свойства".



Выберите пункт "Протокол Интернета TCP/IP", нажмите "Свойства".



В появившемся окне укажите требуемый IP-адрес, маску подсети, адрес шлюза и адреса DNS-серверов. Нажмите "ОК" и закройте все относящиеся к сетевым настройкам окна.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Что такое сетевой адаптер?
2. Какие бывают конструктивные реализации сетевых адаптеров?
3. Чему равна скорость передачи данных по шине ISA и PCI?
4. Назовите важнейшие параметры сетевых адаптеров?
5. Какие системные параметры ПК используют сетевые адаптеры?
6. От чего зависит скорость работы сетевых адаптеров?
7. Что означает сертификат FCC класса A?
8. Что означает сертификат FCC класса B?
9. Что такое функция удалённой загрузки по сети?
10. На что влияет большой размер буферной памяти сетевого адаптера?
11. Что такое полудуплексный режим обмена?
12. Что такое полнодуплексный режим обмена?

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 10 «Восстановление компьютера после сбоя (работа с backup-ами)»

Цель работы: В результате выполнения лабораторной работы научиться.

В процессе занятия решаются следующие задачи:

1. Изучить порядок восстановления компьютера после сбоя, используя резервное архивирование в Windows;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Восстановление системы после сбоев

Современные операционные системы довольно устойчивы к сбоям и, как правило, стабильность системы тем выше, чем меньше изменений вносится в систему в процессе работы. Однако все же приходиться вносить изменения в конфигурацию операционной системы (установка нового ПО, обновление системы или драйверов, изменение системных параметров и компонент), в результате Windows может отреагировать неадекватно. Поэтому важно делать регулярные резервные копии, которые могут пригодиться при восстановлении системы.

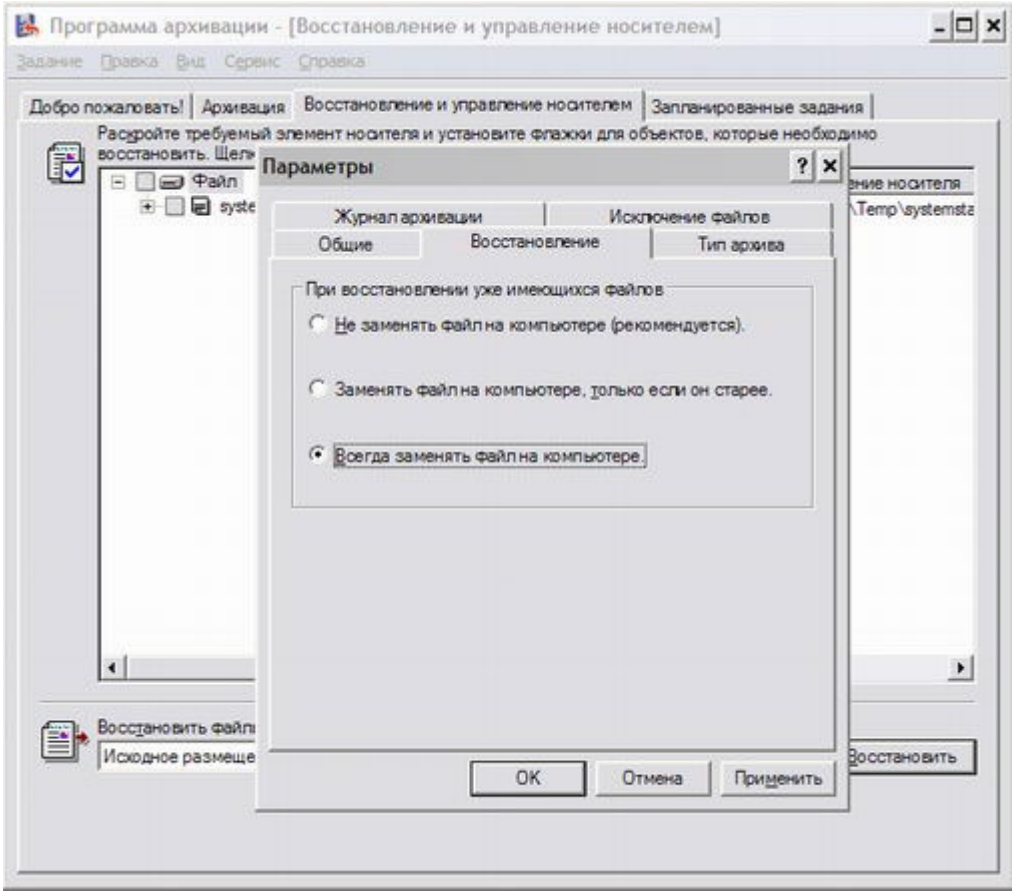
Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

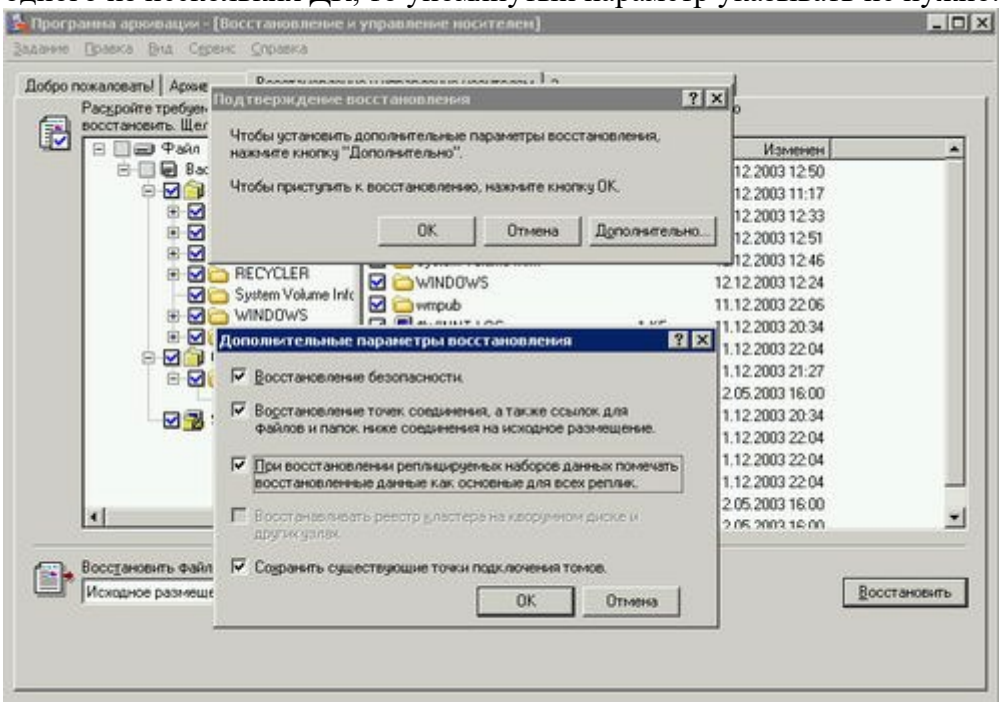
Выполните задания

Восстановление из резервной копии

Воспользуйтесь **Программой Архивации** (ntbackup. exe) для выполнения полного восстановления системы (включая Состояние Системы) с последней резервной копии. Обязательно необходимо воспользоваться Дополнительными параметрами и указать режим «Замены существующих данных» для восстановления файлов, уже имеющихся на компьютере. Это обеспечит восстановления всех файлов из вашей резервной копии, в противном случае при совпадении имен файлов архива и файлов новой копии системы - файлы из архива восстановлены не будут (рис. 1).



При восстановлении Состояния Системы доменного контроллера, который являлся единственным в домене, необходимо обязательно установить дополнительный параметр «При восстановлении реплицируемых наборов данных помечать восстановленные данные как основные для всех реплик» (рис. 2). В этом режиме будет построена новая база данных для службы Репликации файлов (ntfrs) из данных, расположенных в каталоге SYSVOL только этого контроллера домена. Если производится восстановление одного из нескольких ДК, то упомянутый параметр указывать не нужно.



Подготовка системы к восстановлению

Теперь, зная режимы и методы восстановления, осталось сделать все возможное, чтобы восстановления прошло легко и непринужденно. К сбоям в системы нужно относиться как к неизбежному

и «ожидать» их. Быть во всеоружии. Итак, как неприятности поджидают нас при выходе из строя оборудования или повреждении компонентов системы.

Важным моментом является создание отказоустойчивой конфигурации с самого начала. Повышайте стойкость системы к отказам:

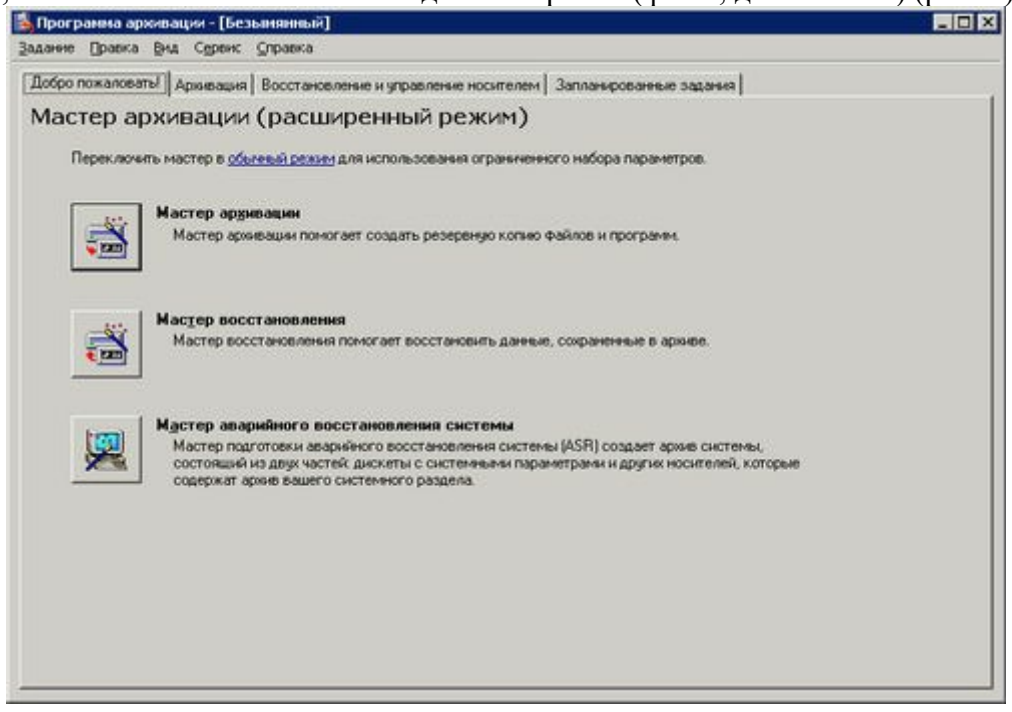
- используйте RAID массивы для хранения системных данных, это защитит их от сбоев жесткого диска. Есть возможность реализовать RAID массивы программным методом, не используя дорогие аппаратные контроллеры. Подробнее об этом смотрите встроенную справку Windows:
- использование Источника Бесперебойного Питания (ИБП) позволит серверу корректно завершить работу при сбое электропитания:
- имейте в резерве все то оборудование, которое возможно выйдет из строя (даже блоки питания):
- использование кластеров обеспечит избыточность и отказоустойчивость даже в случае выхода из строя одного из узлов. Однако все это достигается за счет высокой стоимости.

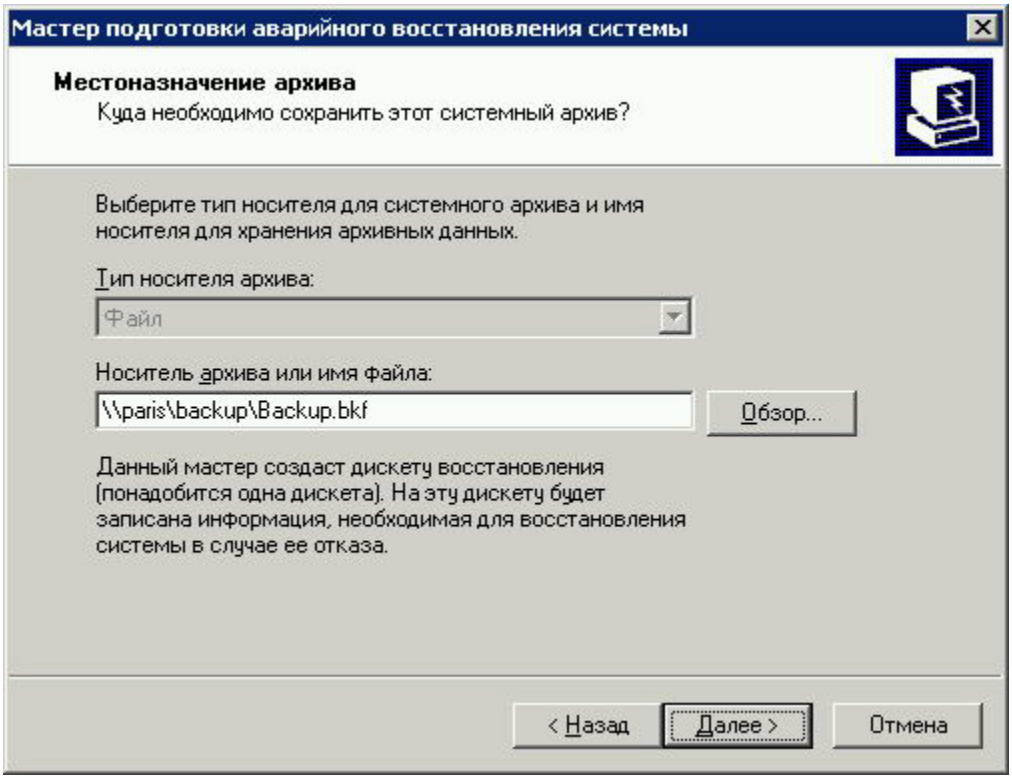
Выполняйте резервное копирование

Регулярное резервное копирование Windows и Состояния Системы это хороший задел для восстановления. В том случае, если вы не используете RAID массив, а ваш системный диск вышел из строя, то Windows можно будет восстановить из резервной копии. При этом потребуется сначала установить новую копию Windows Server 2003 перед восстановлением из архива. Создайте запланированное задание по архивации Состояния Системы и системного раздела на ленты или сетевые общие папки. Кроме того, желательно выполнять копирование всех локальных каталогов, предоставленных в общий доступ (дистрибутивы можно исключить из задания архивации). Это необходимо для того, чтобы после восстановления из полной резервной копии все общие папки по-прежнему были доступны для клиентов сервера. Для сопоставления локальных папок с общими папками из командной строки воспользуйтесь командой **net share**.

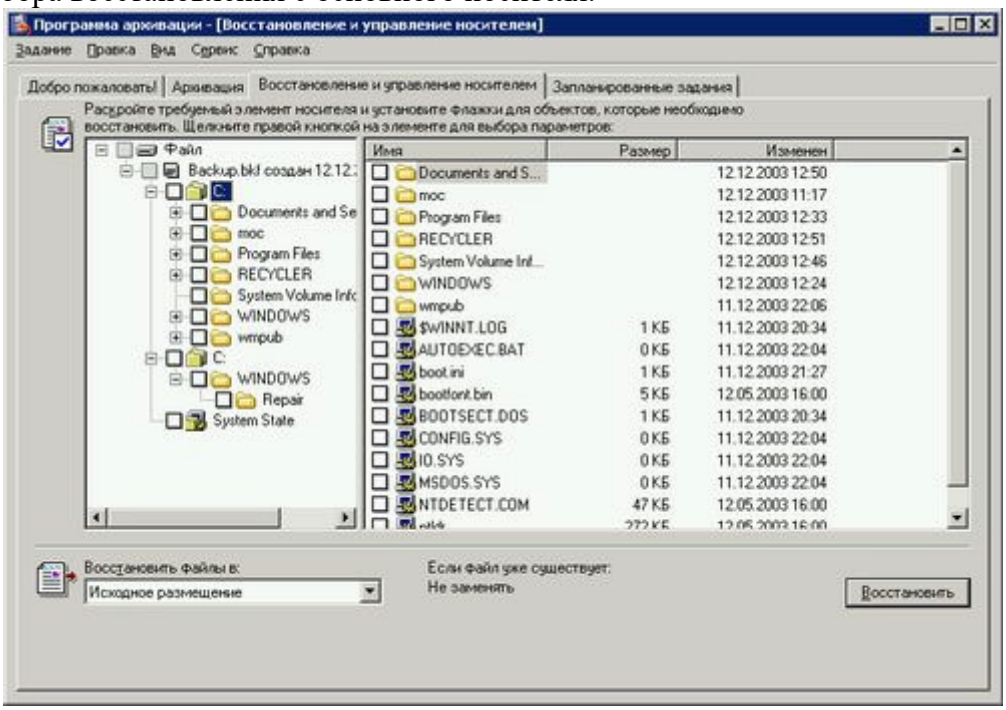
Создавайте наборы Аварийного Восстановления Системы

Windows Server 2003 создает Наборы Аварийного Восстановления Системы (ABC). Для этого следует запустить Мастер создания аварийного восстановления системы (рис. 3) из Программы Архивации (ntbackup. exe). Потребуется флешка, на которую будут сохранены информация об архиве, о конфигурации диска (основного или динамического) и данные, необходимые для выполнения процедуры восстановления, а также какой-либо носитель данных архива (флеш, диски и т.п.) (рис. 4).





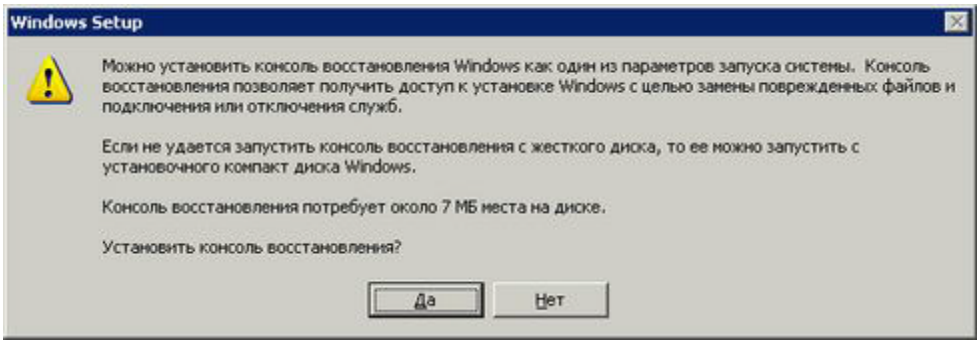
В набор будет включено Состояние Системы, системные службы, а также файлы, связанные с компонентами операционной системы (точнее системный раздел будет полностью) (рис. 5). Данные с других разделов должны включаться в ежедневные и недельные задания по резервному копированию сервера (сразу включайте Состояние Системы в ваши копии). Размер файла архива обычно составляет не менее 1,4 ГБ. После создания набора ABC вы должны хранить вместе дискету и носитель ABC, поскольку, чтобы иметь возможность воспользоваться носителем резервной копии вам будет нужна именно эта дискета. Дискета ABC не является загрузочной, она должна быть использована только для объединения набора восстановления с основного носителя.



Наборы Аварийного Восстановления выполняются Программой Архивации только в интерактивном режиме. Нельзя создать запланированные задания по их созданию. Рекомендуется создать Набор ABC сразу после установки и первоначальной настройки Windows и хранить его (не затирая). Это обеспечит начальную точку восстановления в будущем. К тому же архив, сделанный при помощи Мастера Аварийного Восстановления Системы, может быть использован для ручного восстановления после установки новой копии Windows.

Установите Консоль Восстановления

Консоль Восстановления можно использовать для того, чтобы вернуть способность загружаться Windows. Хотя Вы можете запустить Консоль Восстановления непосредственно загрузившись с установочного компакт диска Windows Server 2003, намного более удобным является установка Консоли в меню выбора вариантов загрузки Windows. Чтобы установить Консоль Восстановления, откройте меню «Пуск» - «Выполнить» и наберите **d: i386 winnt32. exe / cmdcons**, где d – буква вашего привода CD-ROM. (рис. 6.)



Время выполнения работы 90 мин;
Контрольные вопросы

Сделайте выводы.
Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно
3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 11 «Организация взаимодействия локальной и глобальной компьютерных сетей»

Цель работы: В результате выполнения лабораторной работы научиться обеспечивать полное сетевое взаимодействие виртуальной машины и host-систем.

В процессе занятия решаются следующие задачи:

1. Изучить порядок настройки сетевых параметров на Windows XP и Windows Server 2008, установленной на VirtualBox;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Создание компьютерных сетей вызвано практической потребностью пользователей удаленных друг от друга компьютеров в одной и той же информации. Сети представляют пользователям возможность не только быстрого обмена информацией, но и совместной работы на принтерах и других периферийных устройствах, а также одновременной обработки документов.

Локальная сеть объединяет компьютеры, установленные в одном помещении или в одном здании.

В небольших локальных сетях обычно все компьютеры равноправны, и такие сети называются одноранговыми. Для увеличения производительности, а также в целях обеспечения большей надежности при хранении информации в сети некоторые компьютеры специально выделяются для хранения файлов и программ-приложений. Такие компьютеры называются серверами, а сама сеть - сетью на основе серверов.

Для подключения к сети компьютер должен иметь специальную плату (сетевой адаптер), и соединяются компьютеры в сеть с помощью кабелей.

Региональные сети позволяют обеспечить совместный доступ к информации в пределах одного региона (города, страны и т.д.)

Корпоративные сети создаются организациями, заинтересованными в защите информации от несанкционированного доступа, такие сети могут объединять тысячи компьютеров по всему миру.

Потребности формирования единого мирового информационного пространства привели к созданию глобальной компьютерной сети Internet . Internet - это глобальная компьютерная сеть, объединяющая многие локальные, региональные сети и включающая в себя десятки миллионов компьютеров.

В каждой локальной сети имеется компьютер, подключенный к Internet , с высокой пропускной способностью- Internet сервер

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Рассмотрим использование Virtual Host-Only Ethernet Adapter, применение которого позволяет обеспечить **полное взаимодействие машин** между собой и **выход обеих во внешний мир**, хотя описание настройки будет приведено для каждого типа сетевого интерфейса.

Настройка Host-части VirtualBox

В качестве host-системы в данном случае выступает операционная система Windows Vista Home Premium SP2 (Windows Server 2008), а качестве гостевой Windows XP Pro SP3.

Итак, первым делом определимся с реальным подключением host-машины к сети Интернет и самое главное и нужное свойство это тип IP-адреса – статический или динамический.

В настройках приложения VirtualBox через меню «File» («Файл») открываем вкладку «Network» («Сеть») и производим следующие действия.

Сначала выставляем IPv4-адрес и IPv4-маску подсети (рис. 1).

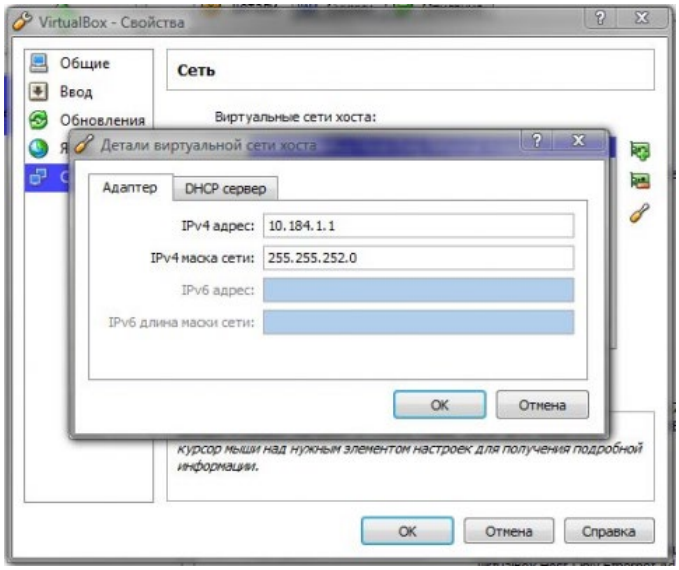


Рис.1: параметры адаптера.

Вводимый здесь IPv4-адрес обязательно должен находиться в диапазоне адресов реальных адаптеров;

IPV4-маска подсети должна соответствовать маске, используемой реальным адаптером.

Включаем DHCP-сервер (независимо от того, статический или динамический IP-адрес Вашего реального сетевого адаптера), рис.2.

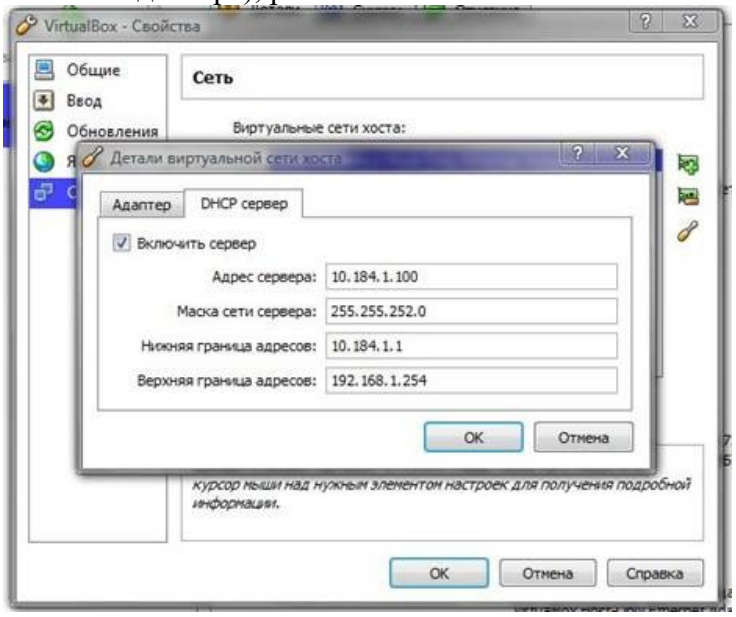


Рис.2: параметры DHCP-сервера.

Адрес сервера также должен находиться в диапазоне адресов реальных адаптеров, IPv4-маска подсети должна соответствовать маске, используемой реальным адаптером, верхняя и нижняя границы адресов должны захватывать все адреса, используемые в системе.

Сетевые настройки виртуальной машины

В настройках Settings (Настройки) установленной виртуальной машины открываем вкладку Network (Сеть) и производим следующие действия:

1. Включаем адаптер Host-only adapter;
2. Включаем адаптер NAT;
3. Включаем адаптер Bridge Adapter и для него выбираем Ваш реальный интерфейс сети Интернет, но т.к. речь идет о настройке именно для Virtual Host-Only Ethernet Adapter, то пока не важно, что там выбрано;
4. Включаем адаптер Internal Network;

5. Для каждого адаптера выбираем тип сетевой карты PCnet-Fast III (Am79C973), т.к. операционная система Windows XP, установленная гостевой, поддерживает только этот адаптер;
6. В настройках каждого адаптера ставим флаг о подключении кабеля.

Пояснение по каждому адаптеру:

- NAT – наипростейший способ предоставить гостевой ОС доступ в интернет, при таком режиме осуществляется просто перенаправление (транзакции) пакетов;
- Bridge Adapter - сетевой адаптер виртуальной машины получает такой же доступ в сеть, как и сетевой адаптер host-машины, но нет доступа во внешний мир;
- Internal Network - внутренняя сеть для объединения виртуальных машин в локальную сеть, без наружу и к host-машине;
- Host-only adapter - Ваша виртуалка как живая, она имеет доступ к сети Интернет, находится в одной локальной сети с реальной и имеет к ней доступ.

Настройка сетевого моста и шлюза Интернет

Теперь открываем папку «Сетевые подключения», с помощью клавиши «Ctrl» выделяем реальное подключение к сети интернет и VirtualBox Host-Only Network, созданный программой VirtualBox, и через контекстное меню правой кнопки мыши выбираем пункт «Сетевой мост». После этого это соглашаемся с сообщением о том, что данному адаптеру (сетевому мосту) присвоен адрес шлюза 192.168.0.1.

Примечание. Если Вы решили ограничиться сетевым интерфейсом NAT или Bridge, то сетевой мост Вам не нужен и эту часть настроек Вы можете пропустить.

В папке «Сетевые подключения» должна быть следующая картина:

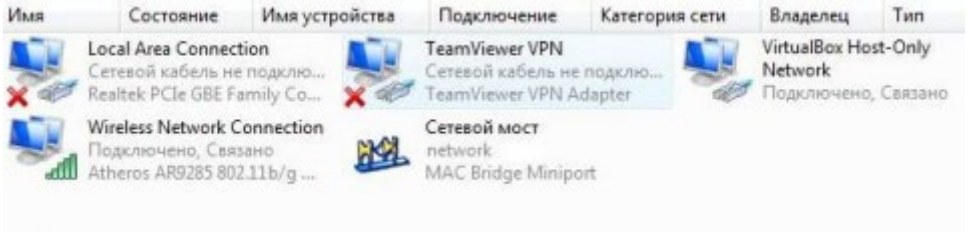


Рис.3: «Сетевые подключения»

Но это еще не все, открываем «Карту сети» и видим там следующее:

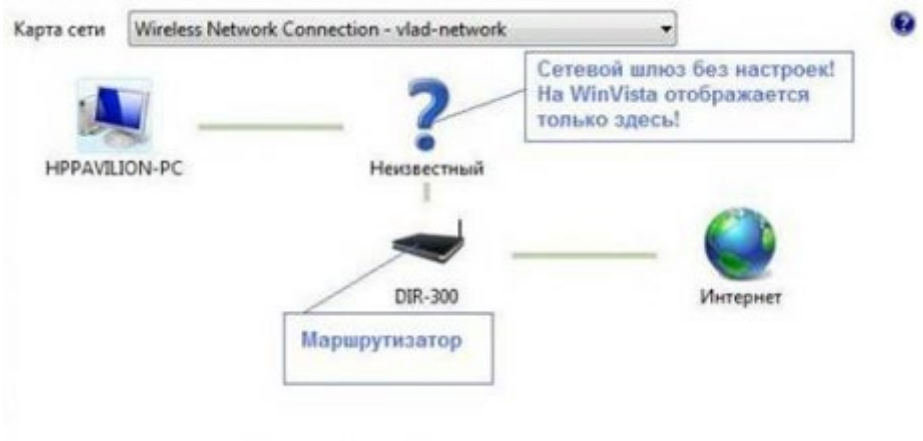


Рис.4: «Карта сети»

И самое теперь самое неприятное - у нас пропало подключение к Интернету. Для того чтобы привести положение дел в порядок, нужно настроить сетевой мост, рис.5:

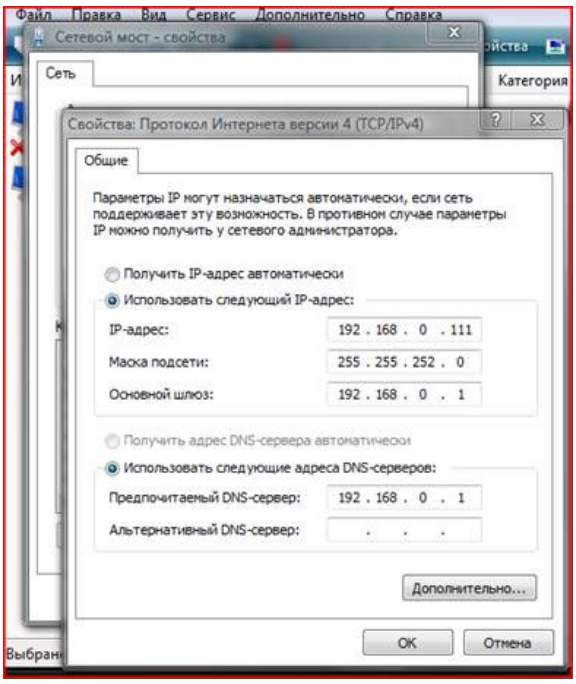


Рис.5: Настройка сетевого моста

Для IPv4-адреса используем любой адрес из установленного ранее диапазона адресов в DHCP-сервере VirtualBox, маску подсети берем ту же, шлюз уже выставлен, а адрес DNS-сервера **выставляем таким же, как и адрес шлюза**. Применяем настройки, нажимая кнопку OK.

Примечание. Если Ваш реальный сетевой адаптер использует динамический IPv4-адрес, то в настройках сетевого моста, а также для всех сетевых интерфейсов виртуальной машины (их настройки будут приведены далее) следует выбрать пункт «Получить IP-адрес автоматически», но в случае отсутствия подключения к интернету Вам следует произвести настройки, указанные для статического IP-адреса.

Снова открываем «Карту сети» и теперь видим там следующее, рис.6:

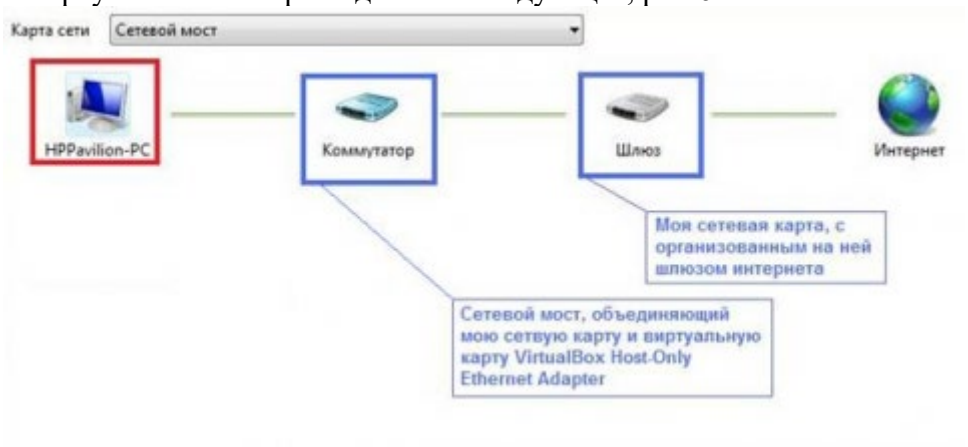


Рис.6: «Карта сети» после настройки сетевого моста

Примечание. Возможно, что у Вас в «Карте сети» элемент коммутатор отображаться не будет, но это не важно, а важно то, что наше подключение к Интернету снова активно!

Настройка сетевых подключений виртуальной машины

Теперь пора заняться настройками виртуальной машины, для чего запускаем её и переходим к папке «Сетевые подключения», рис.7.

Рис.7: «Сетевые подключения» виртуальной машины

Все созданные подключения на месте – давайте настроим каждое из них, для этого щелкнем правой кнопкой мыши на интерфейсе и в контекстном меню выберем пункт «Свойства»:

1. Для адаптера Virtual Host-Only Ethernet Adapter:

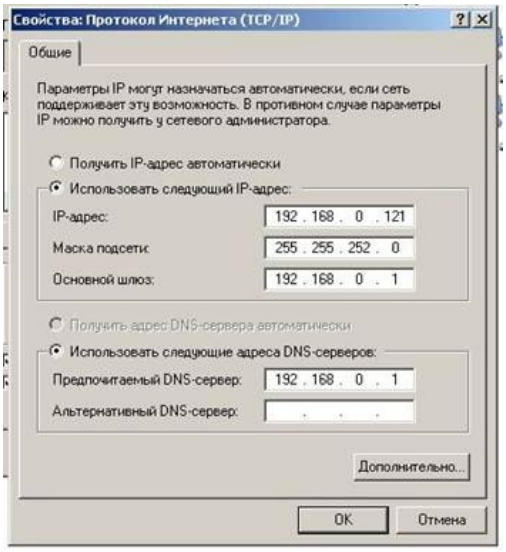


Рис.8: Virtual Host-Only Ethernet Adapter

2. Для адаптера NAT Ethernet Adapter просто выставляем получить IP- адрес автоматически;
3. Для адаптера Intranet Ethernet Adapter:

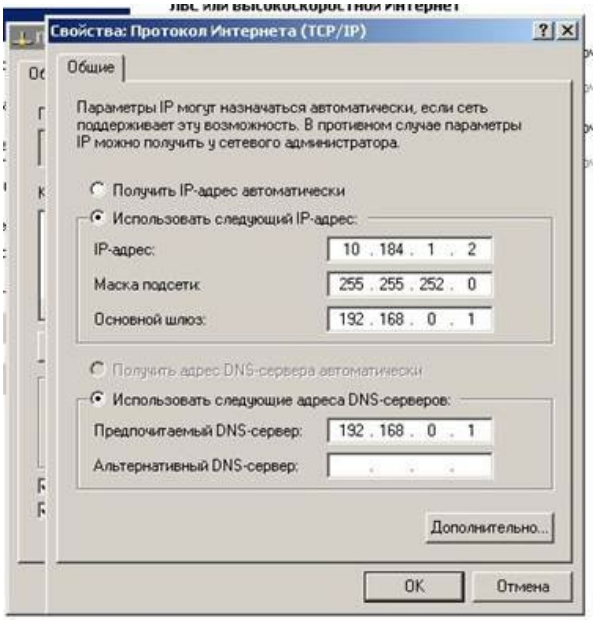


Рис.9: Intranet Ethernet Adapter

4. Для адаптера Bridge Ethernet Adapter:

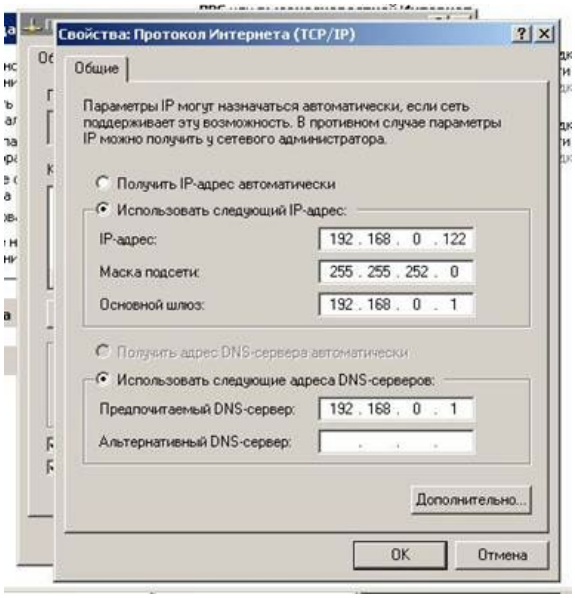


Рис.10: Bridge Ethernet Adapter

Примечание. Обратите внимание, что все использованные IPv4-адреса берутся из установленного ранее диапазона адресов в DHCP-сервере VirtualBox, при этом используется диапазон от адреса шлюза (192.168.0.1) до верхней границы адресов. Ни в коем случае не выставляйте адреса, не входящие в указанную область. Например, адаптер виртуальной машины с установленным для него IP-адресом 192.167.0.111 не позволит Вам подключиться настраиваемой сети. Адреса маски подсети, шлюза и DNS-сервера соответствуют адресам, заданным для сетевого моста для host-машины.

После того, как Вы произвели все указанные операции, в системном лотке появится уведомление «Интернет сейчас подключен», но это мы проверим в самом конце.

Настройка рабочих групп

После проведенных нами операций перезагружаем сначала виртуальную машину, а затем и host-машину. После того как наша реальная операционная система загрузилась, запускаем VirtualBox и включаем нашу виртуальную машину и на host-машине (Windows Vista) открываем «Карту сети»:

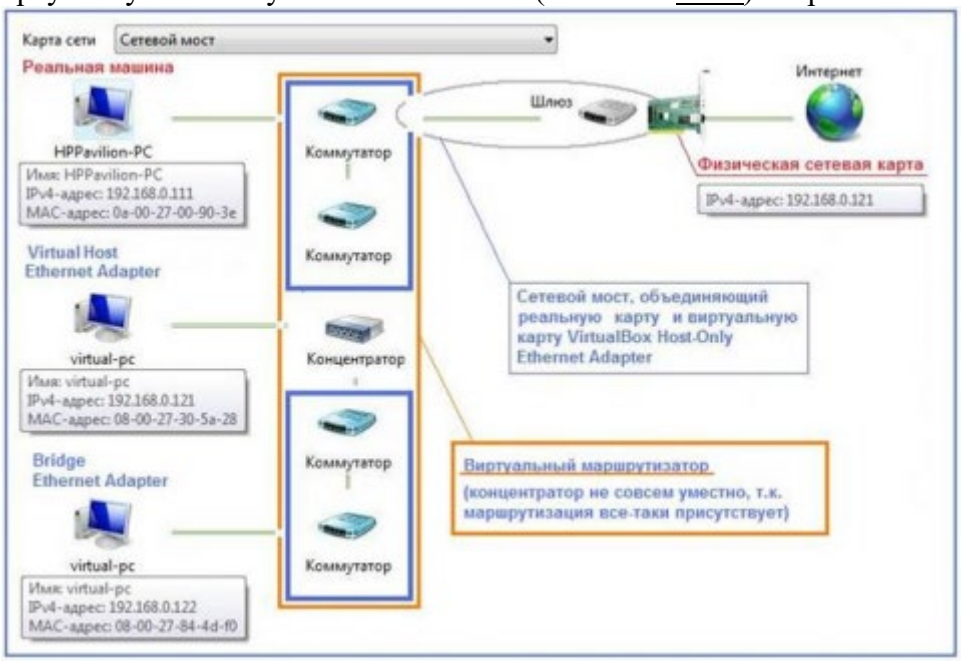


Рис.11: «Карта сети» после настроек виртуальной машины

Тут мы видим host-машину (HPPavilion-PC) и подключенную через два адаптера (Bridge Ethernet Adapter и Virtual Host-Only Ethernet Adapter) виртуальную машину (Virtual-PC). Для большей наглядности на изображении приведены краткие комментарии.

Самое главное – мы видим наши обе машины, то же самое можно определить, запустив сеанс командной строки на обеих машинах и выполнив в нем команду **net view**. На изображении ниже (рис.12) приведены результаты отработки данной команды – справа для Windows Vista, слева для Windows XP.

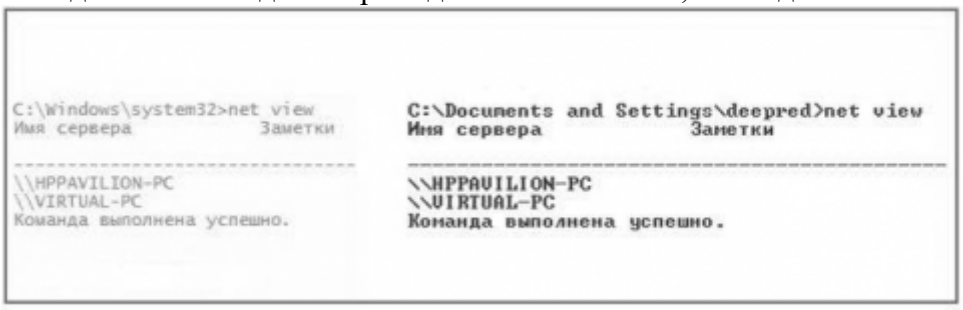


Рис.12: Результат выполнения команды net view

Теперь определимся с рабочими группами – в сети Интернет часто приводится некое требование, согласно которому обе машины должны находиться в одной рабочей группе, но это не так. В нашем случае рабочие группы разные, т.к. по умолчанию ОС Windows XP включена в Workgroup, а Windows Vista в MShome.

Чтобы увидеть, что это означает, перейдем в папку «Сетевое окружение» на нашей виртуальной машине. В данном расположении мы видим две рабочие группы - Workgroup и MShome:

Рис.13: Разные рабочие группы

Откроем рабочую группу MShome и увидим нашу host-машину (HPPavilion-PC).

Рис.14: Рабочая группа MShome и host-машина (HPPavilion-PC).

Вернемся на шаг назад и откроем рабочую группу Workgroup, в ней мы увидим нашу виртуальную машину (Virtual-PC).

Рис.15: Рабочая группа Workgroup и виртуальная машина (Virtual-PC).

Несмотря на то, что все работает, перенесем Virtual-PC, т.е. нашу виртуальную машину, в ту же рабочую группу, что и host-машина (HPPavilion-PC). Для этого откроем свойства Мой Компьютер, перейдем на вкладку «Имя компьютера» и нажмем кнопку «Изменить». В открывшемся окне в поле «Рабочая группа» введем имя рабочей группы, в которой состоит реальная машина (в нашем случае MShome), чтобы увидеть результат перейдем в папку «Сетевое окружение» обеих машин и убедимся, что обе станции находятся в одной рабочей группе.

Посмотрим, что у нас получилось сначала на нашей виртуальной машине Windows XP:

Рис.16: Общая рабочая группа на виртуальной машине

А теперь на host-машине Windows Vista:

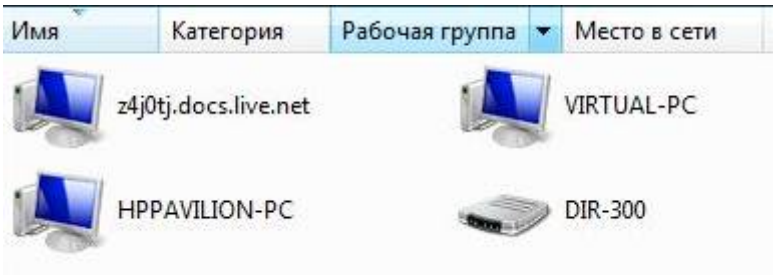


Рис.17: Общая рабочая группа на host-машине

Завершение настройки

Конечно, использовать все четыре адаптера в виртуальной машине нет никакого смысла, поэтому мы оставляем только один, но самый нужный - Virtual Host-Only Ethernet Adapter. Для этого на нашей виртуальной машине откроем папку «Сетевые подключения» и отключим ненужные нам интерфейсы. Дополнительно проверим, сохранились ли настройки указанного адаптера, выполнив команду **ipconfig** в окне командной строки. На изображении ниже приведен вид папки «Сетевые подключения», в которой мы обязательно должны видеть все наши четыре адаптера и Шлюз Интернета, который должен находиться в подключенном состоянии.

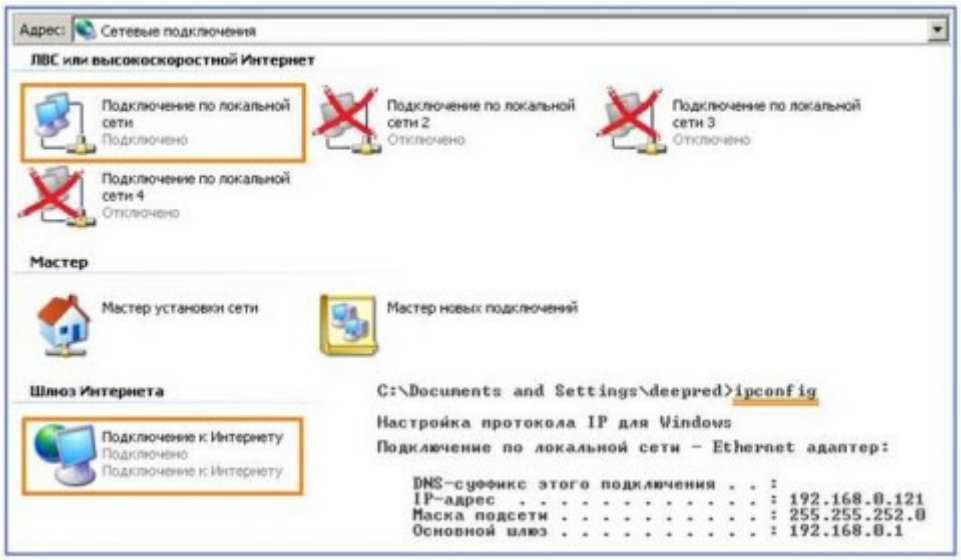


Рис.18: Окончательная конфигурация сетевого интерфейса.

Для того чтобы удостовериться, что подключение к Интернету действительно активно, снова откроем окно командной строки и выполним команду **ping** для узла ya.ru, результат вывода команды должен быть таким:

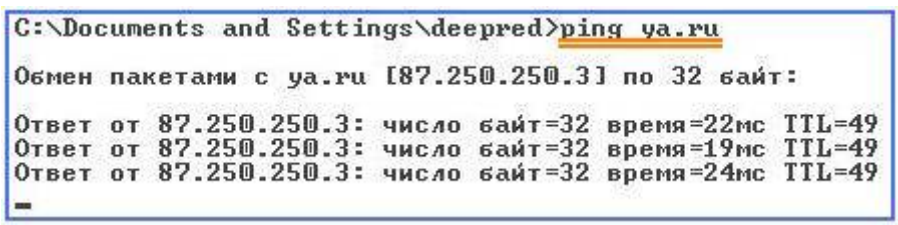


Рис.19: Вывод команды ping

Таким образом, все работает, взаимодействует, находится в одной сети, и обе машины имеют доступ к глобальной сети.

Примечание. Если при запуске Вашей host-машины или виртуальной машины Вы обнаружили, что на одной из них или на обеих отсутствует подключение к Интернету, следует проверить настройки Вашего сетевого моста, как правило, проблема заключается в отсутствии записи адреса основного шлюза и решается вводом оного (198.162.0.1).

Время выполнения работы 90 мин;

Контрольные вопросы

1. Как называются сети, перекрывающие территорию не более 10 м2?
2. Как называются сети, расположенные на территории государства или группы государств?
3. Какую топологию используют компьютерные сети?
4. Приведите основные технологии ЛКС.
5. Дайте характеристику ЛКС типа тонкий Ethernet.
6. Как называются заглушки, которые устанавливаются на концах шины?
7. С помощью чего ПК подключается к шине?
8. Какую топологию имеет ЛКС типа Ethernet на витой паре?
9. Какую топологию имеет АТМ?
10. Укажите тип протокола в сети Internet.
11. Укажите способы адресации в Internet.
12. Перечислите российские сети протокола X.25.

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 11 «Способы организации VPN»

Цель работы: изучить способы организации VPN

В процессе занятия решаются следующие задачи:

1. формированиея умения организации VPN сети.

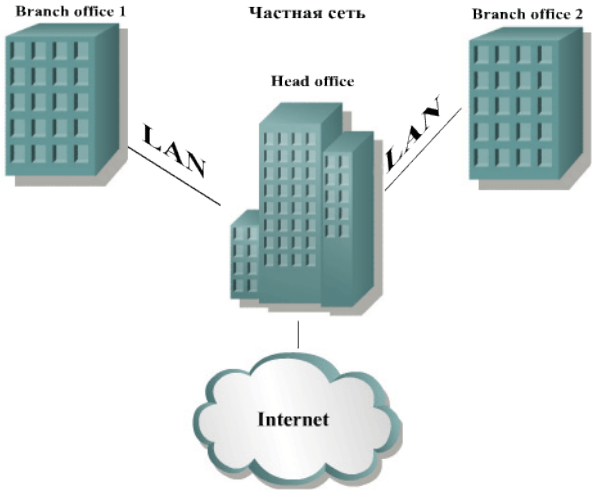
Краткие теоретические и справочно-информационные материалы по теме занятия.

В современных условиях развития информационных технологий, преимущества создания виртуальных частных сетей неоспоримы. Но прежде чем перечислить наиболее очевидные и полезные способы организации виртуальных частных сетей, необходимо определиться с самим понятием.

Виртуальная частная сеть или просто VPN (Virtual Private Network) – это технология, при которой происходит обмен информацией с удаленной локальной сетью по виртуальному каналу через сеть общего пользования с имитацией частного подключения «точка-точка». Под сетью общего пользования можно подразумевать как Интернет, так и другую интрасеть.

VPN versus PN

Организовывая безопасные каналы передачи информации в учреждениях несправедливо не рассмотреть вариант организации полноценной частной сети. На рисунке ниже изображен вариант организации частной сети небольшой компанией с 2 филиалами.



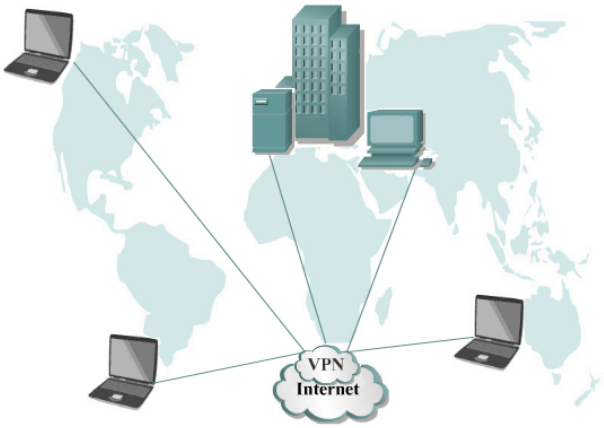
Доступ во внешнюю сеть может осуществляться как через центральный офис, так и децентрализовано. Данная организация сети обладает следующими неоспоримыми преимуществами:

- высокая скорость передачи информации, фактически скорость при таком соединении будет равна скорости локальной сети предприятия;
- безопасность, передаваемые данные не попадают в сеть общего пользования;
- за пользование организованной сетью ни кому не надо платить, действительно капитальные вложения будут только на стадии изготовления сети.

Способы организации:

В VPN наиболее целесообразно выделить следующие три основных способа:

1. Удаленный доступ отдельно взятых сотрудников к корпоративной сети организации через модем либо общедоступную сеть.



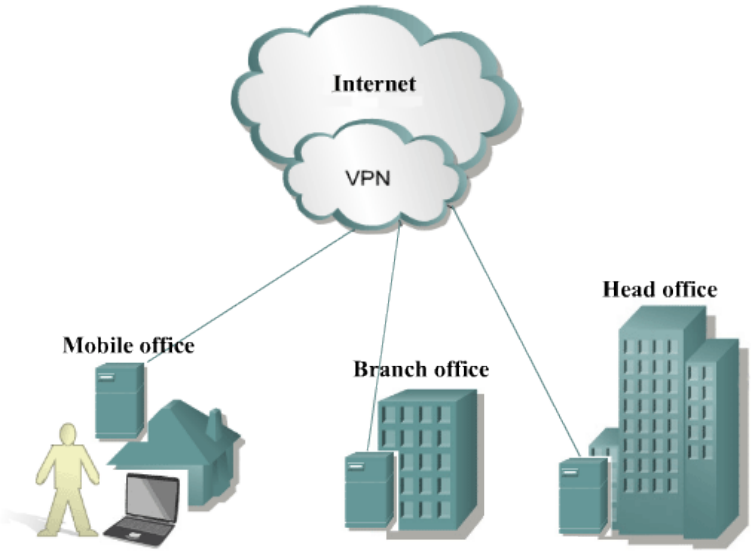
Организация такой модели виртуальной частной сети предполагает наличие VPN-сервера в центральном офисе, к которому подключаются удаленные клиенты. Удаленные клиенты могут работать на дому, либо, используя переносной компьютер, из любого места планеты, где есть доступ к всемирной паутине.

Данный способ организации виртуальной частной сети целесообразно применять в случаях:

географически не привязанного доступа сотрудников к корпоративной сети организации;

доступа к Интернету. Часто провайдеры создают для своих клиентов VPN подключения для организации доступа к ресурсам Интернет.

2. Связь в одну общую сеть территориально распределенных филиалов фирмы. Этот способ называется Intranet VPN.



При организации такой схемы подключения требуется наличие VPN серверов равное количеству связываемых офисов.

Данный способ целесообразно использовать как для обыкновенных филиалов, так и для мобильных офисов, которые будут иметь доступ к ресурсам «материнской» компании, а также без проблем обмениваться данными между собой.

3. Так называемый Extranet VPN, когда через безопасные каналы доступа предоставляется доступ для клиентов организации. Набирает широкое распространение в связи с популярностью электронной коммерции.

В этом случае для удаленных клиентов будут очень урезаны возможности по использованию корпоративной сети, фактически они будут ограничены доступом к тем ресурсам компании, которые необходимы при работе со своими клиентами, например, сайта с коммерческими предложениями, а VPN используется в этом случае для безопасной пересылки конфиденциальных данных. Средства защиты информации – протоколы шифрования.

Поскольку данные в виртуальных частных сетях передаются через общедоступную сеть, следовательно, они должны быть надежно защищены от посторонних глаз. Для реализации защиты передаваемой информации существует множество протоколов, которые защищают VPN, но все они подразделяются на два вида и работают в паре:

* протоколы, инкапсулирующие данные и формирующие VPN соединение;

*протоколы, шифрующие данные внутри созданного туннеля.

Первый тип протоколов устанавливает туннелированное соединение, а второй тип отвечает непосредственно за шифрование данных. Рассмотрим некоторые стандартные, предлагаемые всемирно признанным мировым лидером в области разработки операционных систем, решения.

В качестве стандартного набора предлагается сделать выбор из двух протоколов, точнее будет сказать наборов:

1. PPTP (Point-to-Point Tunneling Protocol) – туннельный протокол «точка-точка», детище Microsoft и является расширением PPP (Point-to-Point Protocol), следовательно, использует его механизмы подлинности, сжатия и шифрования. Протокол PPTP является встроенным в клиент удаленного доступа Windows XP. При стандартном выборе данного протокола компанией Microsoft предлагается использовать метод шифрования MPPE (Microsoft Point-to-Point Encryption). Можно передавать данные без шифрования в открытом виде.

Инкапсуляция данных по протоколу PPTP происходит путем добавления заголовка GRE (Generic Routing Encapsulation) и заголовка IP к данным обработанных протоколом PPP.

2. L2TP (Layer Two Tunneling Protocol) – более совершенный протокол, родившийся в результате объединения протоколов PPTP (от Microsoft) и L2F (от Cisco), вобравший в себя все лучшее из этих двух протоколов. Предоставляет более защищенное соединение, нежели первый вариант, шифрование происходит средствами протокола IPSec (IP-security). L2TP является также встроенным в клиент удаленного доступа Windows XP, более того при автоматическом определении типа подключения клиент сначала пытается соединиться с сервером именно по этому протоколу, как являющимся более предпочтительным в плане безопасности.

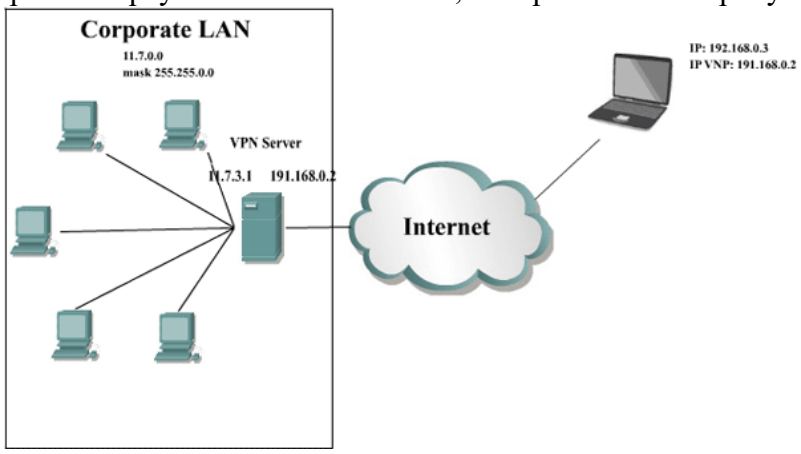
Инкапсуляция данных происходит путем добавления заголовков L2TP и IPSec к данным обработанным протоколом PPP. Шифрование данных достигается путем применения алгоритма DES (Data Encryption Standard) или 3DES. Именно в последнем случае достигается наибольшая безопасность передаваемых данных, однако в этом случае придется расплачиваться скоростью соединения, а также ресурсами центрального процессора.

В вопросе применения протоколов компания Microsoft и Cisco образуют некий симбиоз, судите сами, протокол PPTP – разработка Microsoft, но используется совместно с GRE, а это продукт Cisco, далее более совершенный в плане безопасности протокол L2TP – это ни что иное, как гибрид, вобравший в себя все лучшее PPTP (уже знаем чей) и L2F, да правильно, разработанный Cisco. Возможно именно поэтому VPN, при правильном подходе в организации, считается надежным способом передачи конфиденциальных данных.

Рассмотренные здесь примеры протоколов не являются единственными, существует множество альтернативных решений, например, PopTop – Unix реализация PPTP, или FreeSWAN – протокол для установления IPSec соединения под Linux, а также: Vtun, Racoon, ISAKMPD и др.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия. Организуем простой вариант виртуальной частной сети, изображенный на рисунке ниже.

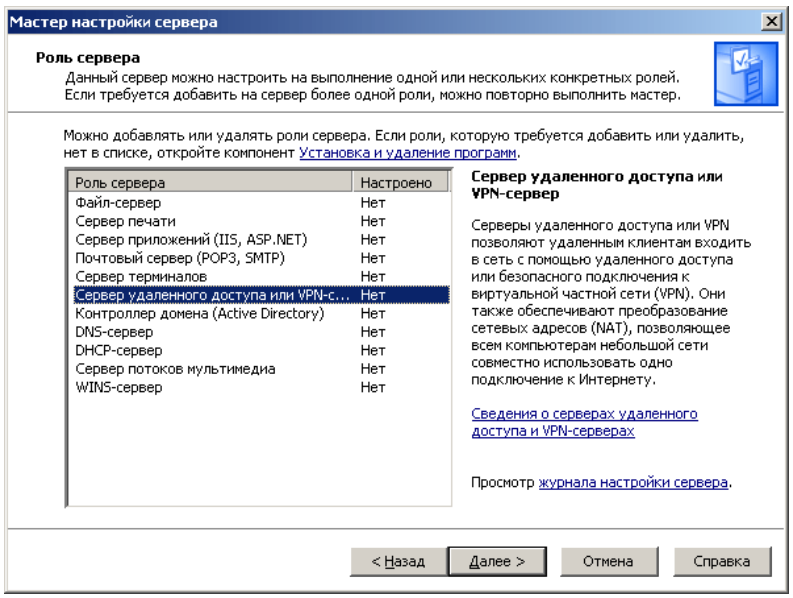


Удаленный сотрудник или сотрудница находится вне офиса и имеет доступ в сеть общего пользования, пускай это будет Интернет.

Адрес сети, к которой необходимо получить доступ 11.7.0.0 маска подсети соответственно 255.255.0.0. Данная корпоративная сеть – это доменная сеть, под управлением Windows 2003 Server Corporate Edition. На сервере имеется два сетевых интерфейса с IP адресами, внутренним для корпоративной сети 11.7.3.1 и внешним 191.168.0.2. Следует отметить, что при проектировании сети VPN сервер ставится в самую последнюю очередь, поэтому Вы сможете без особых проблем организовать VPN доступ к уже отлаженной и сформированной сети организации, но, в тоже время, если в управляемой сети произошли существенные изменения, то, возможно, Вам потребуется перенастроить VPN сервер.

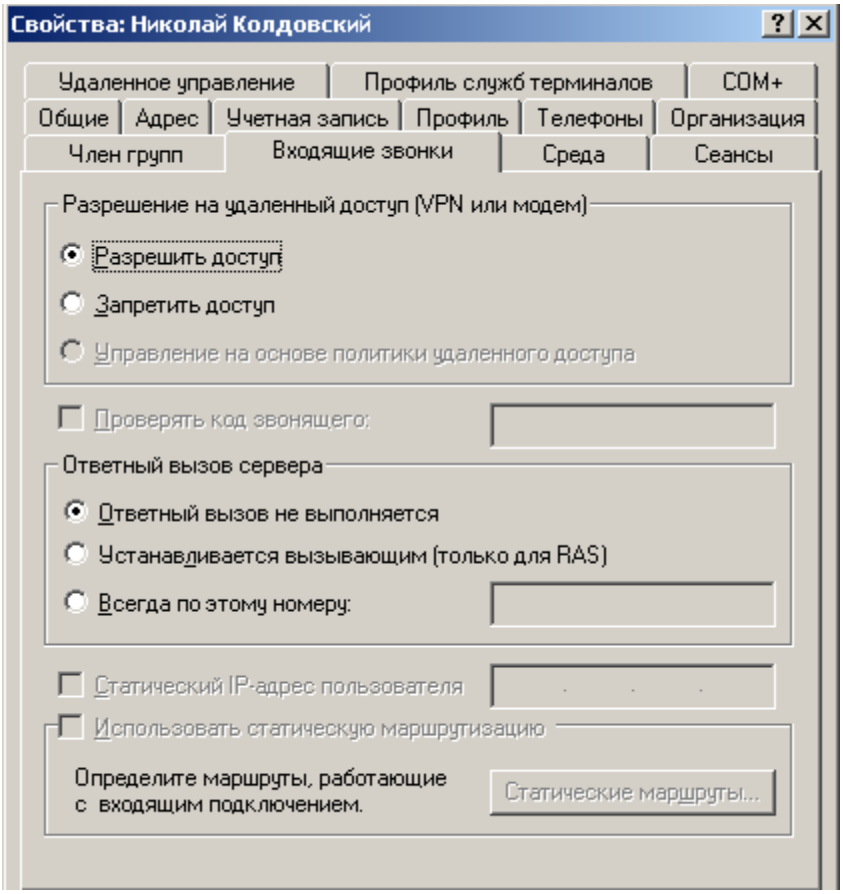
В нашем случае имеется уже сформированная сеть, с адресами, описанными выше, необходимо настроить VPN сервер, а также разрешить определенным пользователям доступ из внешней сети. В корпоративной сети имеется внутренний сайт, к которому мы и попытаемся получить доступ посредствам виртуальной частной сети.

В Windows 2003 Server установка роли VPN сервера осуществляется достаточно просто.



Следуя подсказкам мастера, устанавливаем необходимые параметры: на втором шаге выбираем удаленный доступ (VPN или модем); потом удаленный доступ через Интернет; на 4-м шаге указываем интерфейс сервера, подключенный к Интернету, в нашем случае 191.168.0.2; далее определяем способ назначения адресов удаленным клиентам, в нашем случае это будут автоматически назначенные адреса; если у Вашей сети имеется RADIUS сервер, для централизованной проверки подлинности подключений, выберете его, если нет, тогда оставьте эту задачу VPN серверу.

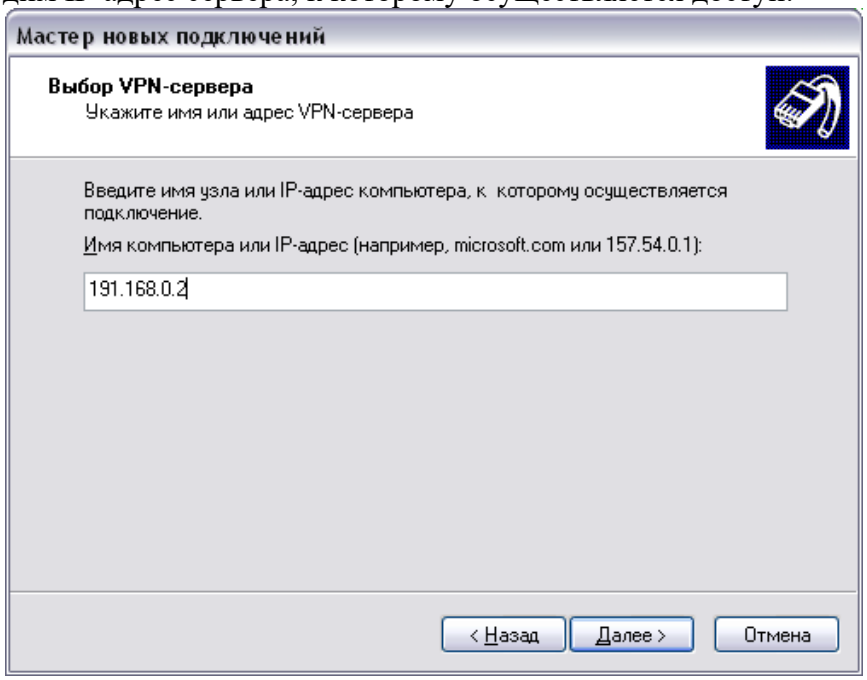
Итак, VPN сервер создан, после проделанных установок, переходим к управлению пользователями нашего домена и для работников, которые нуждаются в удаленном доступе к внутренней сети организации, разрешаем этот самый доступ, установив на вкладке «Входящие звонки» соответствующий переключатель.



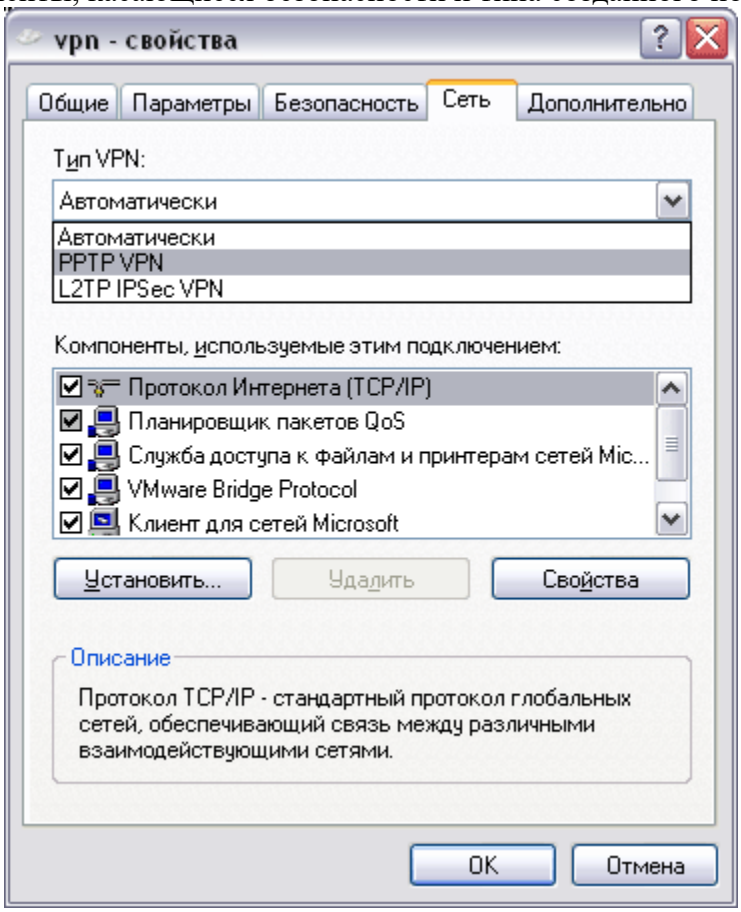
При конфигурировании виртуальной частной сети следует помнить, что для корректной работы необходимо, чтобы установленный брандмауэр разрешал протоколы, используемые VPN.

С серверной частью закончили, переходим к созданию клиента виртуальной частной сети на удаленном компьютере. Для этого необходимо запустить мастер сетевых подключений. На втором шаге,

следуя подсказкам, выбрать пункт «Подключить к сети на рабочем месте». На третьем шаге «Подключение к виртуальной частной сети». Следующий шаг – вводим название подключения. Пятый шаг – выбираем, следует ли предварительно подключаться к Интернету (если Вы подключаетесь с места с постоянным доступом, выберете «нет», если же используете, например, мобильный телефон в качестве модема, тогда следует выбрать предварительный набор номера для подключения к Интернету). На предпоследнем шаге вводим IP-адрес сервера, к которому осуществляется доступ.

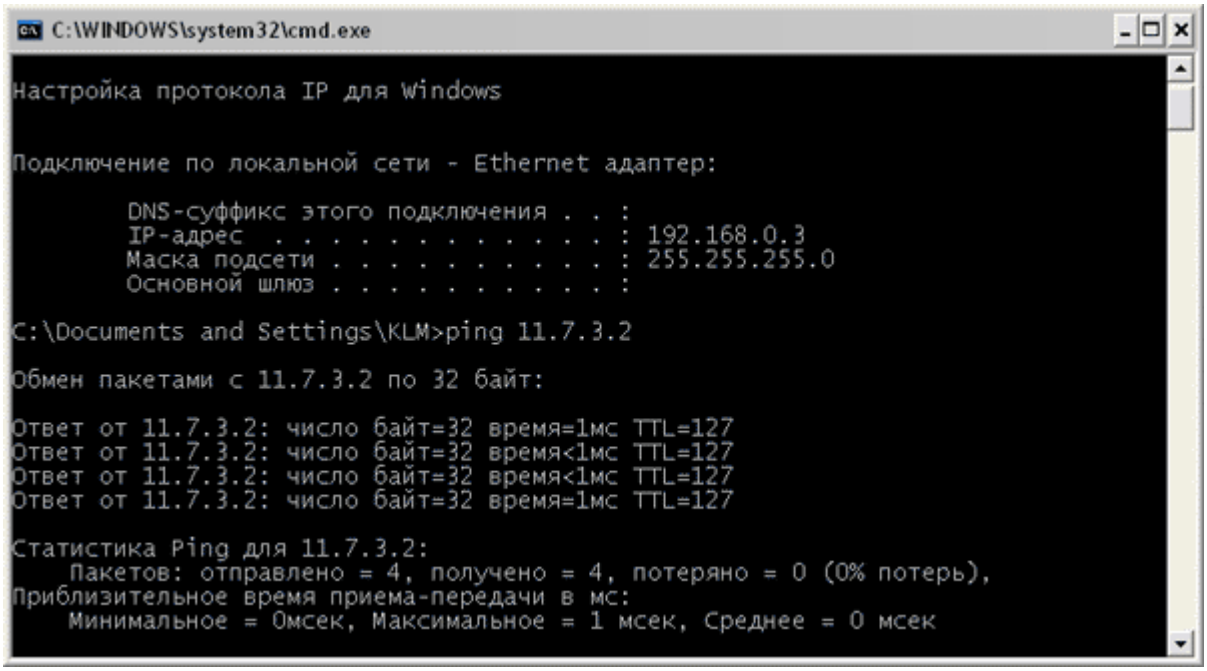


Для уже созданного подключения можно в любой момент откорректировать свойства, а также настроить некоторые моменты, касающиеся безопасности и типа созданного подключения.



Проверка

Конфигурирование удаленного доступа завершено, пришло время проверить его работоспособность. Начнем традиционно, со всеми любимой команды «ping», просто попробуем «пропинговать» какую-нибудь рабочую станцию из нашей корпоративной сети.



Время выполнения работы 90 мин;
Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки*:*
1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ

11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 12 « Порядок проектирования локальной сети»

Цель работы: Научиться проектировать и настраивать ЛВС

В процессе занятия решаются следующие задачи:

1. формированиея умения проектирование и настройки сети.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Процесс построения (проектирования) сети представляет собой упрощенное моделирование не наступившей действительности и включает в себя следующие основные этапы:

1. *Анализ задач*, для решения которых создается сеть, а также определение объема финансирования проекта.
2. *Проектирование физической структуры* - этап, на котором анализируются начальные условия (планировка здания, имеющиеся технические средства и т.п.) и создается детальный проект физической организации сети.
3. *Проектирование инфраструктуры* – этап, на котором определяются протоколы взаимодействия, используемые службы, политика безопасности и т.п. - т.е. логическая организация сети.
4. *Развертывание* - этап, связанный с прокладкой линий связи, установкой и настройкой оборудования.

Этап анализа является одним из важнейших, поскольку определяет все остальные решаемые задачи: как физическую структуру сети (например, места расположения компьютеров), так и логическую (используемые протоколы, службы и т.п.). Именно на данном этапе выступает основное различие компьютерных сетей. Основной целью использования учебных компьютерных сетей в образовательных заведениях выступает организационно-методическая поддержка учебно-воспитательного процесса средствами современных сетевых технологий.

На *этапе проектирования* решаются следующие задачи:

1. На основе определенных целевых требований к сети определяется необходимый состав оборудования и, прежде всего, компьютеров: количество, характеристики и т.д.
2. Определяется физическое расположение рабочих мест и определяются этажи и аудитории, которые будут охватываться сетью. При решении этой задачи должна учитываться принципиальная возможность прокладки линий связи к рабочим местам/помещениям.
3. Исходя из решаемых задач, стоимости и расположения, определяется тип физических линий связи, соединяющих рабочие места, состав и расположение коммуникационного оборудования (например, концентраторов).
4. Определяется способ подключения к Интернету: выбирается провайдер – организация, обеспечивающая подключение организации к сети Интернет. При выборе провайдера учитываются факторы: характеристики возможных физических соединений с провайдером, требования к оборудованию и необходимое дополнительное оборудование, начальная стоимость подключения, стоимость эксплуатации подключения, технологические ограничения подключения (невозможность использования некоторых служб).
5. Исходя из технических требований, определяется узел проектируемой сети, который будет являться шлюзом для подключения к Интернету и определяется место его расположения. При этом учитывается удобство физического соединения шлюза с проектируемой сетью и удобство подведения физических линий для подключения к Интернету.

Приведем общий алгоритм, описывающий процесс построения сети.

1. Определение исходных данных.

    - Определение целей использования сети.
    - Определение требований к сети
    - Характеристики используемого оборудования (компьютеры, сетевое оборудование, принтеры, модемы и др.)
    - Характеристика сетевого ПО (операционные системы, серверное ПО, антивирусное ПО)
    - Примерная схема здания в котором планируется строить сеть.
2. Проектирование сети
    - Способ сегментирования и объединения сегментов (определение необходимых сегментов оборудования для их формирования).
    - Выбор типа кабеля (как правило выбирается неэкранированная витая пара)
    - Определение активных устройств (модемы, маршрутизаторы и т.п.)
    - Выбор программного обеспечения (серверные и клиентские ОС, серверное программное обеспечение и т.п.).
    - Разработка схемы сети (указываются узлы сети и длины соединительных кабелей).
3. Определение стоимости
    - Анализ основных направлений затрат
    - Составление примерной сметы затрат.
4. Примерный план проведения работ.
5. Развертывание сети.

При создании новой сети желательно учитывать следующие факторы:

- требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу);
- структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия); основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальней перспективе); характер передаваемой по сети информации;
- технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов);
- возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля;
- обслуживание сети и контроль ее безотказности и безопасности;
- требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д. (например, если предполагается использование одного ресурса многими пользователями, то следует использовать серверную ОС);
- необходимость подключения к другим сетям (например, глобальным);
- имеющиеся компьютеры и их программное обеспечение, а также периферийные устройства (принтеры, сканеры и т.д.).

При выборе размера (под размером сети в данном случае понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними) и структуры сети необходимо учитывать:

- количество компьютеров (следует оставлять возможность для дальнейшего роста количества компьютеров в сети);
- требуемую длину линий связи сети (например, если расстояния очень большие, может понадобиться использование дорогого оборудования).
- способы объединения частей сети (для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы, причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля.
- Возможность масштабирования (например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент).

Пример. Пусть небольшое предприятие занимает три этажа, на каждом по пять комнат, и включает в себя три подразделения, по три группы. В этом случае можно построить сеть таким образом (рис. 1):

- Рабочие группы занимают по 1–3 комнаты, их компьютеры объединены между собой репитерными концентраторами. Концентратор может использоваться один на комнату, один на группу или один на весь этаж. Концентратор целесообразно расположить в помещении, в которое имеет доступ минимальное количество сотрудников.
- Подразделения занимают отдельный этаж. Все три сети рабочих групп каждого подразделения объединяются коммутатором, а для связи с сетями других подразделений используется маршрутизатор. Коммутатор вместе с одним из концентраторов лучше поместить в отдельной комнате.
- Общая сеть предприятия включает три сегмента сетей подразделений, объединенных маршрутизатором. Этот же маршрутизатор может использоваться для подключения к глобальной сети.
- Серверы рабочих групп располагаются в комнатах рабочих групп, серверы подразделений – на этажах подразделений.

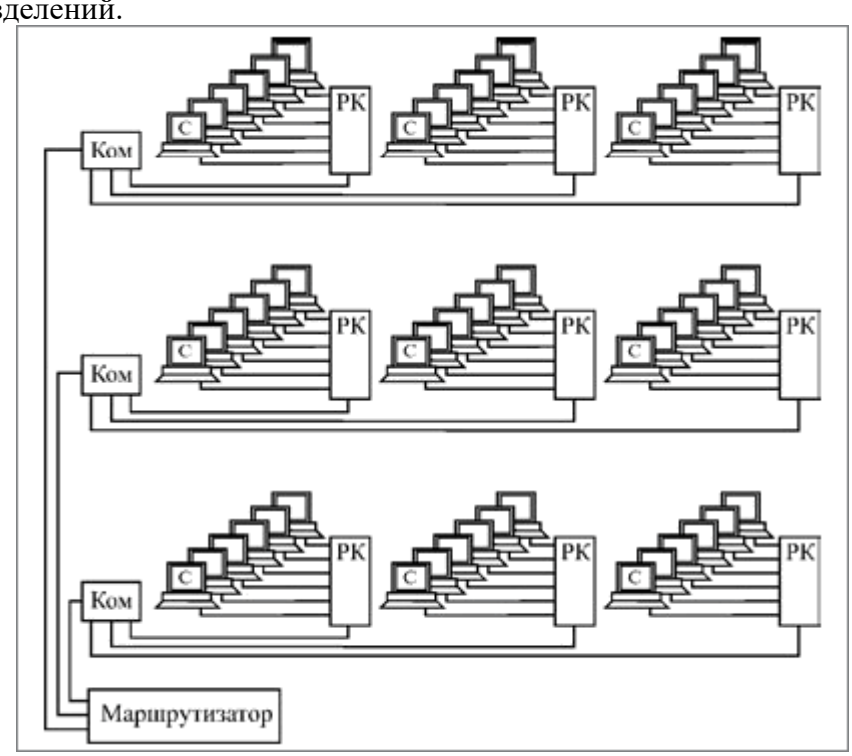


Рисунок 1. Структура сети предприятия (С – серверы рабочих групп, РК – репитерные концентраторы, Ком – коммутаторы)

При выборе сетевого оборудования надо учитывать множество факторов, в частности:

- уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;
- скорость передачи информации и возможность ее дальнейшего увеличения;
- возможные топологии сети и их комбинации (шина, пассивная звезда, пассивное дерево);
- метод управления обменом в сети (CSMA/CD, полный дуплекс или маркерный метод);
- разрешенные типы кабеля сети, максимальную его длину, защищенность от помех;
- стоимость и технические характеристики конкретных аппаратных средств (сетевых адаптеров, трансиверов, репитеров, концентраторов, коммутаторов).

В настоящее время для организации локальных сетей в подавляющем большинстве случаев используется неэкранированная витая пара UTP. Более дорогие варианты на основе экранированной витой пары, оптоволоконного кабеля или беспроводных соединений применяются на предприятиях, где в этом существует действительно острая необходимость. Например, оптоволокно может использоваться для связи между удаленными сегментами сети без потери скорости.

При выборе сетевого программного обеспечения (ПО) надо, в первую очередь, учитывать следующие факторы:

- Какую сеть поддерживает сетевое ПО: одноранговую, сеть на основе сервера или оба этих типа;
- Максимальное количество пользователей (лучше брать с запасом не менее 20%);
- Количество серверов и возможные их типы;

- Совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;
- Уровень производительности программных средств в различных режимах работы;
- Степень надежности работы, разрешенные режимы доступа и степень защиты данных;
- Какие сетевые службы поддерживаются;
- Стоимость программного обеспечения, его эксплуатации и модернизации.

Еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае одноранговой сети лучше выделить для этого отдельного специалиста (администратора), который будет иметь всю информацию о конфигурации сети и распределении ресурсов и следить за корректным использованием сети всеми пользователями. Если сеть большая, то одним сетевым администратором уже не обойтись, нужна группа, возглавляемая системным администратором.

После установки и запуска сети решать эти вопросы, как правило, слишком поздно.

При проектировании следует определить возможные направления финансовых затрат (к данному этапу проектирования необходимые предпосылки для решения этой задачи уже имеются):

- Дополнительные компьютеры и апгрейд существующих компьютеров. Необязательное направление затрат: при достаточном количестве и качестве существующих компьютеров их апгрейд не требуется (или требуется в минимальном объеме – например, для установки более современных сетевых карт); в одноранговой сети не нужен (хотя и желателен) также специальный файл-сервер.
- Сетевые аппаратные средства (кабели и все, что необходимо для организации кабельной системы, сетевые принтеры, активные сетевые устройства – повторители, концентраторы, маршрутизаторы и т.д.).
- Сетевые программные средства, прежде всего, сетевая ОС на необходимое число рабочих станций (с запасом).
- Оплата работы приглашенных специалистов при организации кабельной системы, установке и настройке сетевой ОС, при проведении периодической профилактики и срочного ремонта. Необязательное направление затрат: для небольших сетей со многими из этих работ может и должен справляться штатный сетевой администратор (возможно, с помощью других сотрудников данного предприятия).

Примерное распределение стоимости установки сети с использованием различных сред передачи данных приведено на рисунке 2.

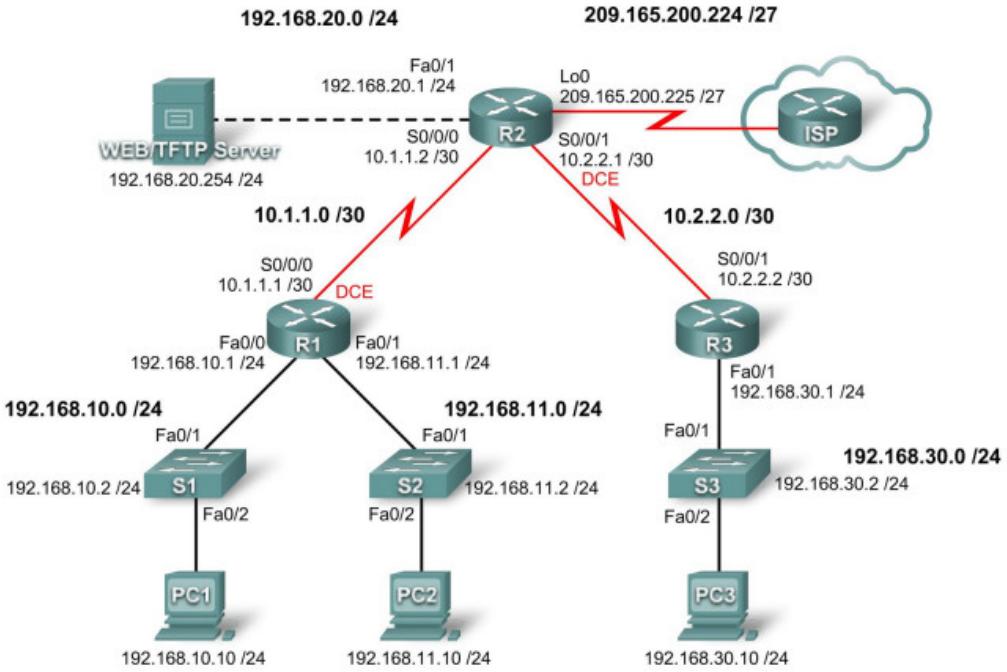
Рисунок 2. Примерное распределение стоимости сети на базе различных сред передачи данных.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

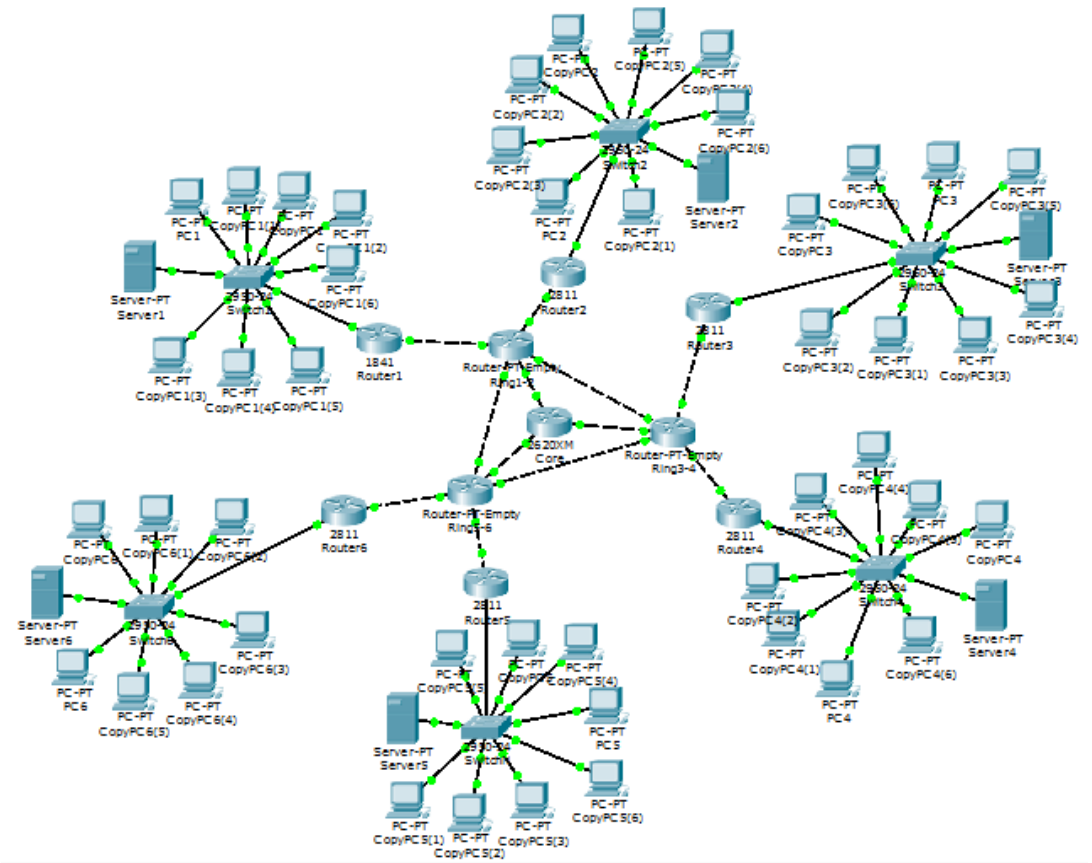
Задание 1

1. Соберите схему сети , изображенную на рисунке.
2. Настройте оборудование.



Задание 2

1. Соберите схему сети , изображенную на рисунке.
2. Настройте оборудование.



Задание 3

Учитывая исходную информацию (примерный план здания образовательного заведения, количество и специфику устанавливаемых ПК и где) спроектировать учебную компьютерную сеть (собрать исходные данные; выбрать: размер и структуру сети, оборудование, сетевые программные средства; спроектировать кабельную систему; рассчитать примерную стоимость оборудования).

1. Ознакомьтесь с решением поставленной задачи:

- для этого откройте файл, содержащий пример выполнения задания (скачать у преподавателя в формате **DOC**;
- ознакомьтесь с содержимым файла;

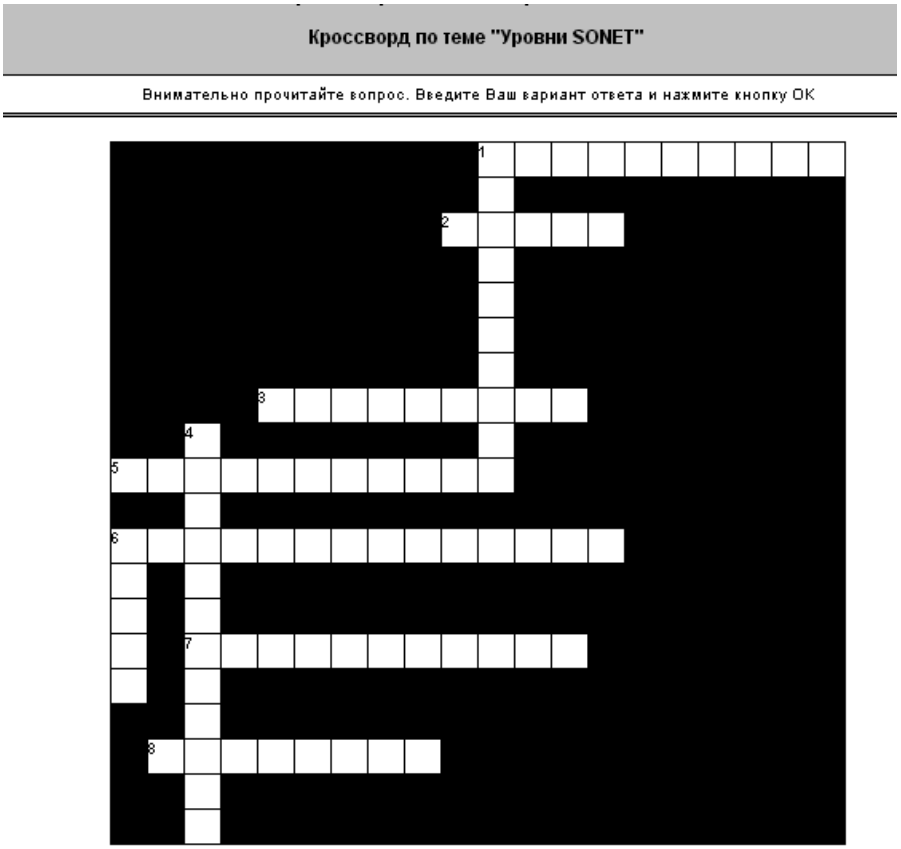
2. Выполните расчеты стоимости программного обеспечения в таблице «Составление сметы примерных затрат».
3. Модифицируйте план проектирования сети, увеличив количество компьютеров до 36 (например, добавьте еще 1 кабинет информатики на 1-м этаже).
4. Сохраните результат работу в личной папке.

Время выполнения работы 90 мин;
Составьте отчет о проделанной работе в тетради для самостоятельных работ.
Критерии оценки*:*
1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Кроссворд «Уровни SONET»



По горизонтали	По Вертикали
1) Ответственный участок сети, во многом определяющий все свойства сети в целом (Gigabit Ethernet или 10 Gigabit Ethernet;) 2) Данное слово обозначает структуру, содержащую некоторую информацию 3) Уровень, который обнаруживает неисправности (если таковые появляются) и выполняет аварийное переключение 5) Кабель, имеющий длину до 71 км; 6) Уровень инкапсулирует данные, гарантирует их отправку в нужном порядке 7) Это стеклянная или пластиковая нить, используемая для переноса света внутри себя посредством полного внутреннего отражения. 8) Уровень, аналогичный Физическому уровню модели OSI	1) Уровень, обеспечивает выбор коммуникационного канала для сигнала 4) Кабель, имеющий длину до 9,6 км; **6)** Это система передачи данных, основанная на синхронизации по времени передающего и принимающего устройства.

Критерии оценивания

Кроссворд разгадан на:

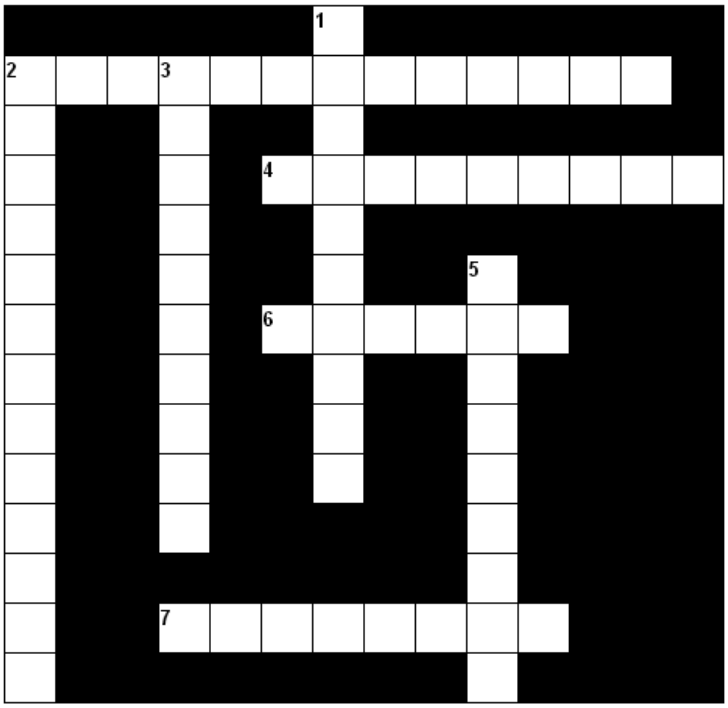
100%- «5»

75% - «4»

60% -«3»

Кроссворд «Методы передачи в сетях»

Внимательно прочитайте вопрос/ Введите ответ и нажмите ОК



По горизонтали	По Вертикали
2) В каких сетях широко используется Сети Frame Relay? **4)** На какой уровень в Frame Relay перемещены функции сетевого уровня? 6) Сеть Frame Relay является сетью с коммутацией... 7) На какие каналы ориентирована Frame Relay ?	**1)** Как называются упакованные данные, пересылаемые без установки коммуникационного канала 2) Виртуальный канал, по которому передаются пакеты сетей X.25 3) Виртуальный канал, по которому передаются пакеты сетей X.25 5) Для каких сетей используется технология Frame Relay (FR) при маршрутизации протоколов ?

Критерии оценивания

Кроссворд разгадан на:

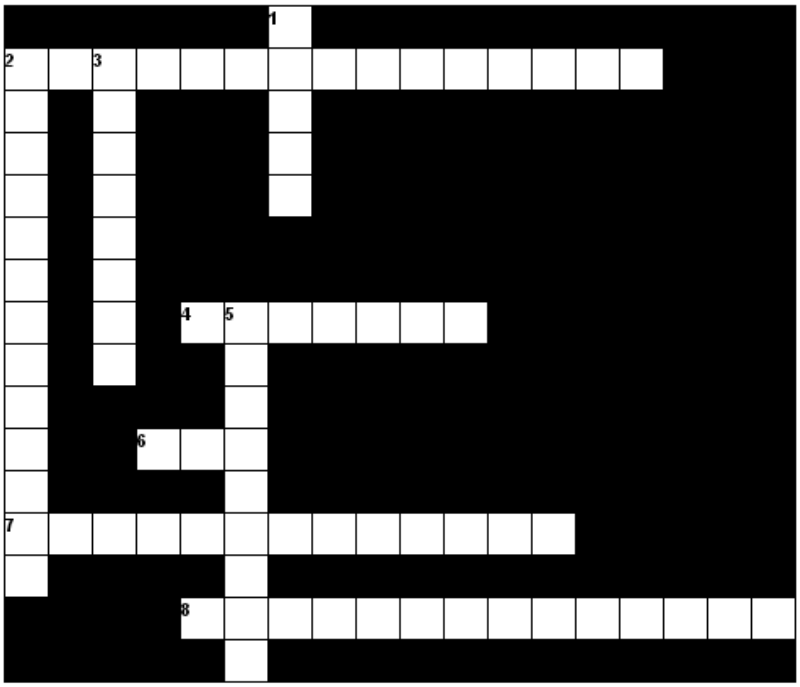
100%- «5»

75% - «4»

60% -«3»

Кроссворд «Сети»

Внимательно прочитайте вопрос

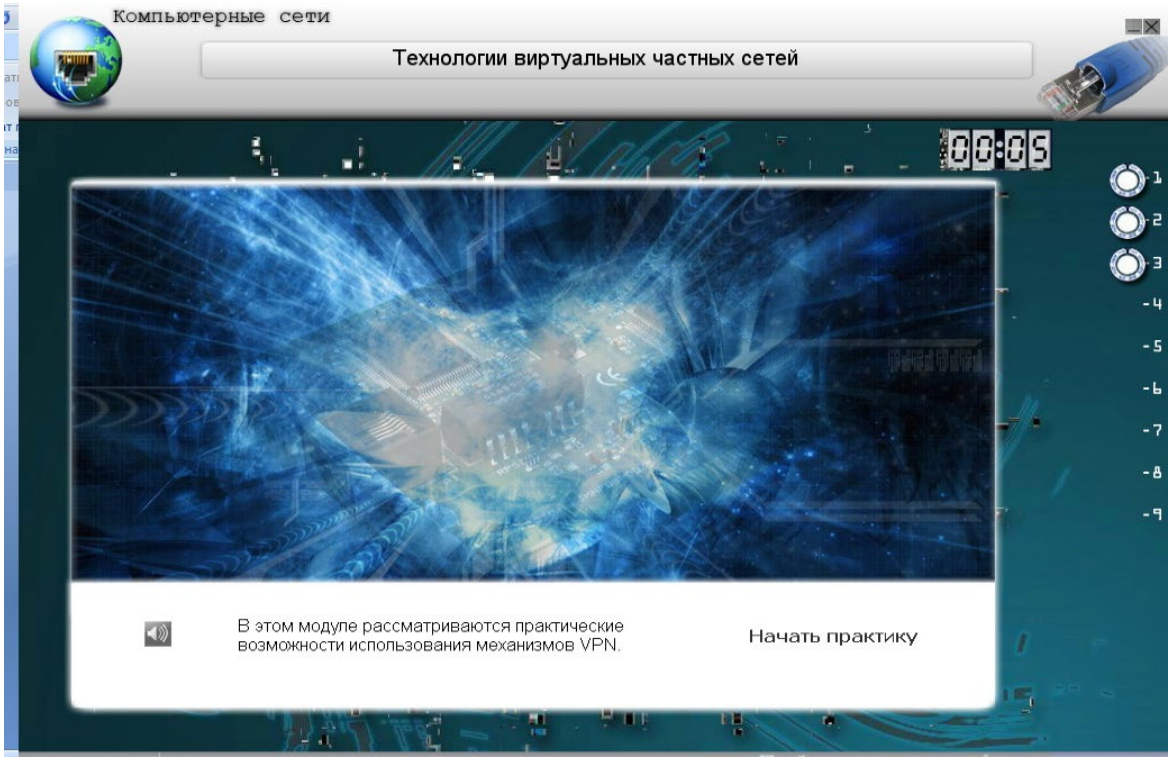


По горизонтали	По Вертикали
2) Одним из достоинств сетей ISDN, является наличие этого стека протоколов. 4) Интерфейс, поддерживаемый узкополосной ISDN-сетью. 6) Количество каналов, из которых состоит интерфейс базового уровня. 7) Это служба позволяет конечному пользователю подключать к линии несколько устройств. 8) Название ISDN-сетей, предназначеных для коммуникаций со скоростями от 155 Мбит/с до 1 Гбит/с по оптоволоконному кабелю?	**1)** Как называется в сетях ISDN группа из 24 каналов? 2) Устройство в сетях ISDN, применяемое для подключения клиентов к PRI-интерфейсу. 3) Интерфейс, поддерживаемый узкополосной ISDN-сетью 5) Одна из услуг, предоставляемые сетью ISDN

Критерии оценивания

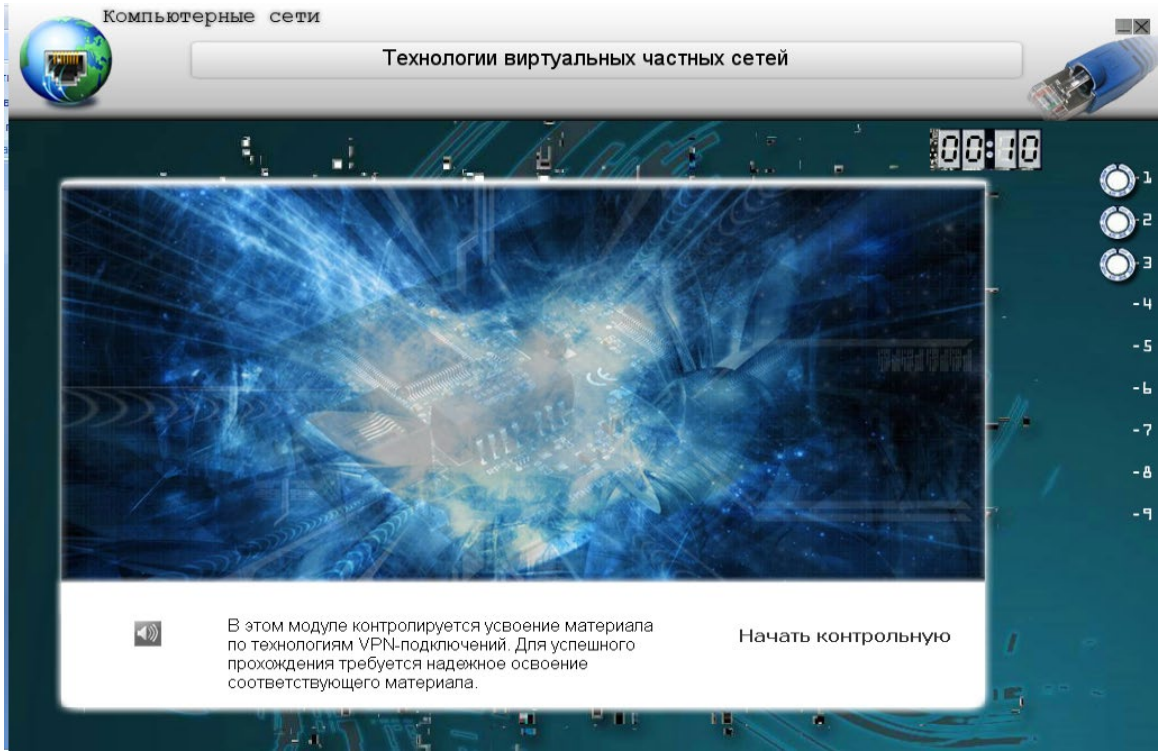
Кроссворд разгадан на:
100%- «5»
75% - «4»
60% -«3»

ЭОР «Технологии виртуальных частных сетей»
(практическая работа)



Критерии оценивания
Работа выполнена на:
100%- «5»
75% - «4»
60% -«3»

Контрольная работа
ЭОР «Технологии виртуальных частных сетей»



Критерии оценивания
Работа выполнена на:
90%- «5»
75% - «4»
60% -«3»

Тема 1.4 Проектирование архитектуры локальной сети

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 12 «Монтаж телекоммуникационного оборудования»

Цель работы: В результате выполнения лабораторной работы научиться производить монтаж разнообразного телекоммуникационного оборудования.

В процессе занятия решаются следующие задачи:

1. Изучить порядок монтажа телекоммуникационного оборудования: роутеров, свитчей, wi-fi-точек, интернет-точек;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

При проектировании и инсталляции структурированных кабельных систем (СКС) в коммерческих зданиях и центрах обработки данных (ЦОД) практически стандартным решением стали **телекоммуникационные шкафы.** Телекоммуникационные шкафы позволяют разместить большое количество пассивного и активного оборудования в ограниченном пространстве; распределить кабельные потоки; защитить телекоммуникационные кабели, пассивное и активное оборудование от различных внешних воздействий.

Телекоммуникационный шкаф состоит из следующих основных элементов: каркаса, боковых стенок, дверей, крышки, направляющих, которые имеют отверстия для монтажа оборудования. Расстояние между отверстиями в направляющих стандартизовано, поэтому пассивное или активное оборудование со стандартным 19-ти дюймовым креплением можно установить между направляющими. Для установки

оборудования в 19-ти дюймовые телекоммуникационные шкафы с 19-ти дюймовым креплением не надо ничего подгонять, не требуется специализированный инструмент, монтаж телекоммуникационного оборудования проводится при помощи обычной отвертки за считанные минуты.

Телекоммуникационные шкафы обычно поставляются с двумя парами направляющих, устанавливаемых спереди и сзади, но иногда встречаются шкафы с одной парой направляющих, которые в основном используются для монтажа пассивного оборудования. Две пары направляющих позволяют установить большее количество оборудования, закрепить тяжелое активное оборудование в нескольких точках. Согласно требованию **стандарта TIA 942 «Телекоммуникационная инфраструктура центров обработки данных»** телекоммуникационные шкафы должны обязательно иметь передние и задние направляющие, которые можно установить на заданное расстояние.

Телекоммуникационные шкафы обеспечивают защиту установленного оборудования от внешнего воздействия: влаги, пыли и грязи, физического повреждения, а также защиту от электромагнитного излучения. Для обеспечения эффективной защиты от электромагнитного излучения необходимо установить металлическую дверь и обязательно заземлить шкаф.

В телекоммуникационных шкафах **двери могут быть стеклянные, металлические сплошные и металлические перфорированные**. Серверные шкафы со стеклянными дверями позволяют администратору сети, не открывая дверь шкафа, видеть светодиоды и состояние активного оборудования. Дверь с перфорацией обеспечивает дополнительную подачу холодного воздуха к активному оборудования через отверстия в двери.

Ввод кабелей в телекоммуникационный шкаф можно осуществлять несколькими способами: снизу, сверху и гораздо реже ввод осуществляется с боковой стороны. Для ввода кабелей производители телекоммуникационных шкафов делают отверстия или заглушки, которые легко выламываются или снимаются. Рекомендуется использовать **щеточные кабельные вводы**, что позволяет существенно уменьшить попадание пыли внутрь телекоммуникационного шкафа через кабельный ввод и обеспечить более эффективное охлаждение при подаче холодного воздуха из-под фальш-пола за счет снижения «протечки» холодного воздуха через щеточный кабельный ввод.

Телекоммуникационные шкафы поставляются **в собранном или разобранном виде**. Разборная конструкция позволяет внести части шкафа в любой дверной проем и затем собрать его в телекоммуникационном помещении, рационально использовать место для хранения на складах и облегчить проведение такелажных работ. Телекоммуникационные шкафы в собранном виде позволяют их быстро установить на объекте и сэкономить время.

Порядок работы

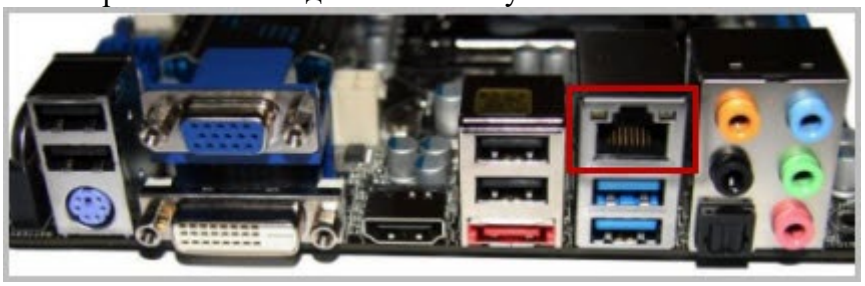
1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

1. Осмотрите помещение, в котором будет проложена будущая сеть.
2. Изобразите план помещения на обычном листке бумаги или специализированном ПО.
3. Отметьте на нем места, где стоят компьютеры, принтеры, подсчитайте количество пользователей вашей сети. Возможно, вы захотите переставить компьютеры.
4. Выберите место, где будет расположен **коммутатор**. Учтите, чтобы расстояние от коммутатора до каждого компьютера было не более 90 метров, поскольку при расстоянии свыше 100 метров сигнал в витой паре будет затухать (в таком случае используются повторители). Коммутатор должен размещаться рядом с электрической розеткой и подальше от пользователей.
5. Отметьте путь прокладки кабеля от коммутатора до каждого компьютера. Кабель должен идти вдоль стен.
6. Чтобы скрыть кабель от посторонних глаз, можно использовать специальные **короба для кабеля**.
7. Подсчитайте длину (в метрах) витой пары, необходимую для соединения компьютеров с коммутатором. Подойдите к первому компьютеру и измерьте рулеткой длину кабеля от данного компьютера до места, где будет располагаться коммутатор. Прибавьте еще 2-3 метра на всякий случай. Вот и получилась длина кабеля для соединения данного ПК с коммутатором. То же самое проделываете со вторым, третьим и т.д. компьютерами. В

результате вы получите список длин витой пары для каждого компьютера. Сложите их вместе – вот вам и общая длина кабеля, которую необходимо приобрести.

8. Осмотрите каждый компьютер на наличие в нем сетевой карты. Практически в любом современном компьютере имеется интегрированная в материнскую плату сетевая карта. Посмотрите на заднюю стенку системного блока и найдите **разъём RJ-45:**



9. В ноутбуках тоже имеется такой разъем:

10. **Коннекторы RJ-45**. Для каждого компьютера у вас будет свой отрезок кабеля, на обоих концах которого будут закреплены коннекторы RJ-45. Один из коннекторов вставляется в разъем сетевой карты, другой – в разъем коммутатора.

Монтаж оборудования и прокладка сети.

1. Проверьте работоспособность сетевых карт на всех компьютерах.
2. Обжимаем кабель
3. Обжатые кабели подключаем одним концом к разъемам сетевых карт всех компьютеров, а другим концом к разъемам коммутатора. Включаем все компьютеры и коммутатор, если до этого они были выключены.
4. Проверяем работоспособность сети на физическом уровне.

Время выполнения работы 90 мин**;**

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1**.** Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 13 «Проектирование и монтаж кроссовых»

Цель работы: В результате выполнения лабораторной работы научиться производить монтаж разнообразного телекоммуникационного оборудования.

В процессе занятия решаются следующие задачи:

1. Изучить порядок проектирования и монтажа кроссовых ;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Кроссовая представляет собой помещение, в которое вводятся кабели внутренней магистральной подсистемы и кабели горизонтальной подсистемы. Соответственно, в этих помещениях размещаются коммутационные панели, активное сетевое оборудование, обслуживающее группу пользователей, а также вспомогательные устройства. Запрещается располагать в кроссовых оборудование, которое не имеет непосредственного отношения к функционированию кроссовой (к примеру, силовые распределительные щиты).

Кроссовые, как и аппаратные, являются помещениями, требующими особого внимания со стороны проектировщиков и эксплуатационных служб. В то же время, к кроссовой выдвигаются менее жесткие требования, поскольку она будет обслуживать относительно небольшое количество рабочих мест, тогда как аппаратная – все здание или даже комплекс зданий. Необходимо отметить также, что в СКС с количеством рабочих мест около 100 (а таковых в России наибольшее количество) кроссовая часто может являться единственным техническим помещением, таким образом, автоматически совмещаясь с аппаратной.

Наиболее часто для оборудования кроссовых применяются шкафы размером 800x800 мм (ШхГ), и значительно реже – шкафы меньших габаритов, таких как 600x600 мм, 600x800 мм. Минимальный рекомендуемый размер помещения 3,0×2,2 м, что диктуется необходимостью центрального расположения шкафов и доступа к ним со всех сторон. Если помещение меньшего размера – необходимо рассмотреть возможность применения шкафов меньших габаритов (к примеру, 600x400 мм), и размещения части пассивного и актививного оборудования с использованием схемы настенного монтажа. Высота помещения не менее 2.5 м.

Если через помещение кроссовой проходят вертикальные трассы (стояки), применение фальшпола и фальшпотолка нежелательно, поскольку затруднит подвод кабелей.

Обязательно оборудование кроссовой следующими инженерными системами:

- Пожарной и охранной сигнализации;
- Вентиляции и освещения;

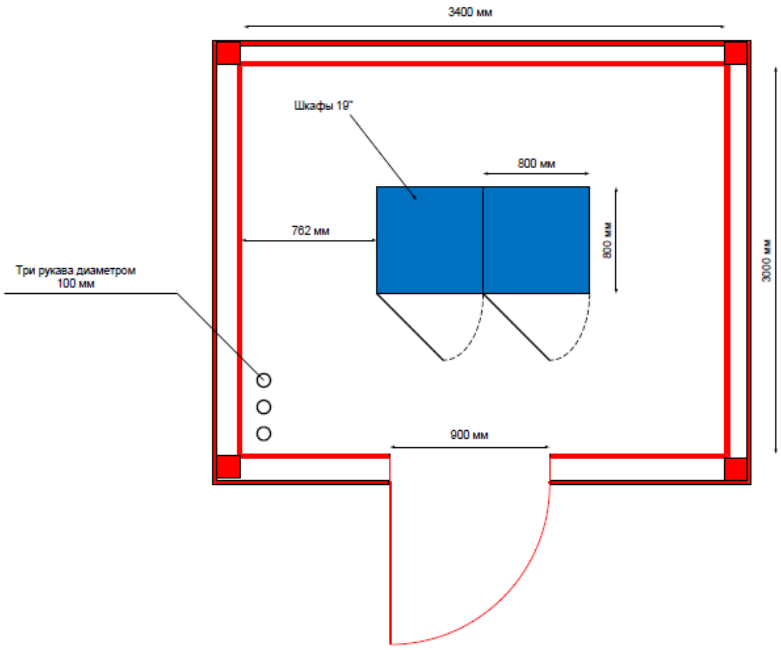
- Защитного и, желательно, телекоммуникационного заземления.

Система электропитания кроссовой организуется аналогично системе электропитания аппаратной.

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

5. Нарисуйте план серверной комнаты;



6. **Разработайте проект кроссовой:**

Задание на проектирование

1. Кабельная система располагается на 4 этажах кирпичного здания.
2. На четвёртом этаже предусмотрена две отдельная серверная комната с центральным кроссом.
3.Кроссы для коммутации оборудования расположены на каждом этаже здания
4.В здании размещается 108 рабочих станций, а так же 6 серверов.
5. Общее количество розеток ЛВС - 114.
6. Рабочие места располагаются следующим образом:

-нулевой этаж - 6 рабочих мест;
-первый этаж - 23 рабочих места;
-второй этаж - 27 рабочих мест;
третий этаж - 18 рабочих мест;
четвёртый этаж - 40 рабочих мест;

Время выполнения работы 90 мин;

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 14 «Построение кабельной проводки СКС»

Цель работы: В результате выполнения лабораторной работы научиться производить монтаж разнообразного телекоммуникационного оборудования.

В процессе занятия решаются следующие задачи:

1. Получить представление о видах структурированных кабельных систем (СКС) и оборудовании, применяемом для их монтажа;
2. Получить практические навыки монтажа кабельных систем на основе сетевых карт **Ethernet** / **FastEthernet**;
3. Изучить назначение прямого и кроссированного соединения (**T568A** и **T568B**).

Краткие теоретические и справочно-информационные материалы по теме занятия.

Аббревиатура «СКС» расшифровывается как «структурированная кабельная система» (SCS, Structured Cabling System). Дать однозначное толкование понятию «структурированная кабельная система» практически невозможно, т.к. это объемный и сложный комплекс понятий, соглашений, стандартов, рекомендаций и требований, предъявляемых к современной телекоммуникационной инфраструктуре.

В рамках определений международного стандарта ISO/IEC 11801, СКС — это универсальная структурированная телекоммуникационная кабельная система офисного здания, способная поддерживать широкий диапазон приложений. СКС представляет собой универсальную кабельную проводку для локальной сети, проектируемую и устанавливаемую без привязки к их конкретным сетевым технологиям. Поскольку подавляющее большинство локальных сетей устанавливается в офисных зданиях, населенных персоналом с компьютерами и телефонами, существующие стандарты на СКС предполагают, что они будут устанавливаться в зданиях именно такого типа. В случае развертывания сети на промышленных объектах или в жилых зданиях основные положения стандартов на СКС не теряют актуальности, но их применение должно учитывать специфику конкретных условий.

СКС обладает как минимум следующими признаками:

- является универсальной, т.е. дает возможность использовать ее для передачи сигналов основных существующих и перспективных видов сетевой аппаратуры различного назначения;
- позволяет быстро и с минимальными затратами организовывать новые рабочие места и менять топологию трактов передачи без прокладки дополнительных кабельных линий;
- позволяет организовать единую службу эксплуатации;
- создается на этапе строительства здания или переоборудования его помещений под офис и имеет гарантированный срок эксплуатации 10 и более лет.

СКС поддерживает различные телекоммуникационные приложения (передачу речи, данных и видеоизображений), дает возможность применения различных компонентов и продукции различных производителей, а также реализации «мультимедийной среды» (в которой используются несколько типов передающих сред — коаксиал, экранированная и обычная витая пара, оптическое волокно).

Элементами СКС являются взаимозаменяемые кабельные компоненты: кабели и проводники, пассивное коммутационное оборудование (информационные розетки рабочих мест, патч-панели, кроссовое оборудование и принадлежности) служащее для их соединения или физического окончания (терминирования).

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Часть 1.1. Соединение компьютеров на физическом уровне

1. Определить, какой стандарт соединения требуется для связи двух **однородных устройств**, например, компьютеров.
2. Удалить внешнюю оболочку кабеля на длину **12-13 мм** (1/2 дюйма). В обжимном инструменте имеется специальный **нож и ограничитель**.
3. Расплести кабель и расположить провода для **перекрёстного** соединения.
4. Повернуть вилку **металлическими контактами вверх** или пластмассовым «хвостиком» вниз и вставить в неё кабель. Проверить **правильность расположения** проводов и зубьев каждого контакта.
5. Используя обжимной инструмент, обжать вилку с кабелем.
6. С помощью кабельного тестера **проверить правильность** соединения коннекторов.

Часть 1.2. Соединение компьютеров на физическом уровне с помощью пач-панели

1. На **рисунке 1** представлена схема сети, которую необходимо собрать.
2. Составить **план сети**, определив и отметив на плане стандарты соединений.
3. Используя монтажный инструмент, собрать сеть.
4. Соединить два компьютера собранной сетью. Признаком наличия соединения будут горящие **индикаторы Link** на сетевых адаптерах.
5. В случае если сеть не работает, использовать кабельный тестер для **локализации неисправностей.**

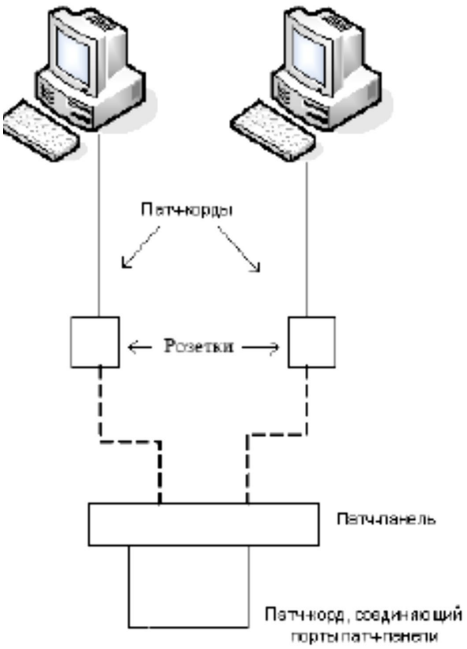


Рис. 1

Часть 2. Разработка плана кабельной системы этажа (в соответствии с введенными стандартами)

Руководствуясь положениями из **СНИП 2.09.04-87**, определить положение сетевых розеток (локальная сеть, телефония). Исходя из соответствующих **стандартов**, составить схему проводки кабелей, установки розеток, а также таблицу спецификаций материалов.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Зачем нужна смена стандартов при соединении однородных устройств?
2. Чем отличаются стандарты витой пары категорий 5, 5e, 6, 7?
3. Заполнить таблицу параметров кабельных сегментов в соответствии с их типом и назначением:

Тип кабеля	Названия стандартов, регламентирующих применение данных линий связи (ISO/IEC)	Основные области применения	Максимальная длина кабельного сегмента для сетей Ethernet (без использования повторителя)
Коаксиальный кабель			
Оптоволоконный кабель			
Витая пара категории 5			
Витая пара категории 5е			
Витая пара категории 6			
Витая пара категории 7			

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 15 «Расчёт магистральных подсистем»

Цель работы: В результате выполнения лабораторной работы научиться производить монтаж разнообразного телекоммуникационного оборудования.

В процессе занятия решаются следующие задачи:

1. Научить производить расчет магистральных подсистем;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Трассы кабелей подсистемы внутренних магистралей в подавляющем большинстве случаев имеют вертикальную организацию (проходят по стоякам), в силу чего протяженность их невелика (в российской практике обычно 20-70 м).

По этой причине расчет производится сложением длин отдельных кабельных сегментов, реализуемых на однотипных кабелях.

При расчете расхода кабелей, применяемых для построения подсистемы внешних магистралей учитывается вид трассы и, в зависимости от вида трассы, коэффициент неравномерности прокладки. На

основании РД 45.120-2000, п. 12.10.1, при определении потребляемого количества прокладываемых кабелей, в проектах должны предусматриваться их запасы с учетом неровности местности, укладки кабелей в грунт, а также выкладки их по форме котлованов, колодцев, подвески на опорах воздушных линий связи и расхода на разделку концов кабелей при проведении измерений электрических или оптических характеристик и сращивания строительных длин кабелей. Коэффициенты приведены в таблице.

Коэффициент неравномерности прокладки кабелей

Тип трассы	**Количество кабеля на 1 км трассы**	
	Медные многопарные кабели	**Оптические кабели**
Кабельная канализация	1,02	1,057
Коллектор	1,01	1,02*
Прокладка на опорах	1,025	1,05
Прокладка в грунт механизированная	1,02	1,02*
Прокладка в грунт ручная	1,04	1,04*

***Длина запаса оптического кабеля на монтаж муфты и производство контрольных измерений учитывается дополнительно и составляет: для муфты, смонтированной в котловане 30 м; для муфты, смонтированной в коллекторе 14 м.**

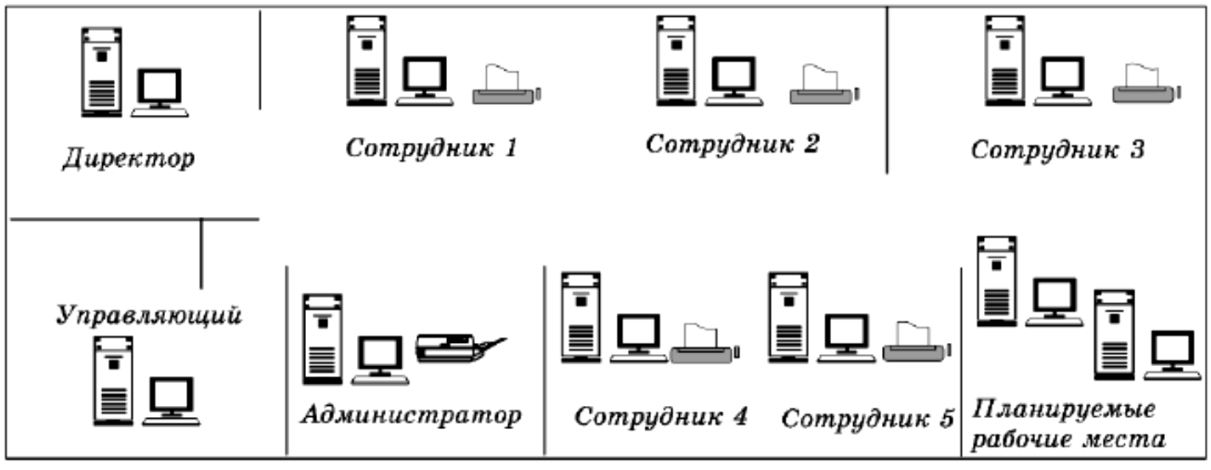
Также в расчет необходимо включать запас кабеля при оконечных и промежуточных муфтах, в местах подключения оптического кабеля к приемопередающим устройствам, а также в местах установки соединительных муфт необходимо предусматривать запас кабеля. Согласно СНиП 3.05.07-85, п.3.132, запас должен быть не менее 2 м у каждого сращиваемого оптического кабеля или приемопередающего устройства.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

1. Вам поручено установить сеть для небольшой, но развивающейся компании, занимающей половину этажа. В состав компании входят директор, управляющий, администратор и пять сотрудников. Планируется принять на работу еще двух сотрудников. У каждого сотрудника есть компьютер. Если необходимо обменяться информацией приходится делать это устно или с использованием съемных носителей, что неудобно. Лазерный принтер имеются у администратора. У каждого сотрудника имеется сканер. Какую топологию вы предложите для компании? Оцените суммарную длину кабеля в каждом из предложенных случаев и выберите оптимальный вариант.



Для ранее разработанной сети (см. п. 1) составить проект прокладки кабеля витая пара категории 5 в кабельных каналах, согласно выбранной вами сетевой топологии.

Время выполнения работы 90 мин**;**

Контрольные вопросы

1. Нарисуйте схему сети, построенной по топологии типа шина. Сеть должна включать 5 компьютеров.
2. Имеются 3 компьютера, расположенных на расстоянии 200 м друг от друга. Какую топологию вы выберете для создания сети?
3. Имеется комната площадью 20 м2. В ней необходимо поставить 10 компьютеров, объединенных сетью. Нарисуйте схему сети.
4. Нарисуйте схему сети, построенной по топологии типа звезда. Сеть должна включать 5 компьютеров.
5. В организации имеется 3 отдела. В каждом отделе по 8 компьютеров. Все отделы расположены на одном этаже здания. Зарисуйте схему сети.

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. 1**.** Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 16 «Способы подключения сетевого оборудования»

Цель работы: В результате выполнения лабораторной работы научиться производить монтаж разнообразного телекоммуникационного оборудования.

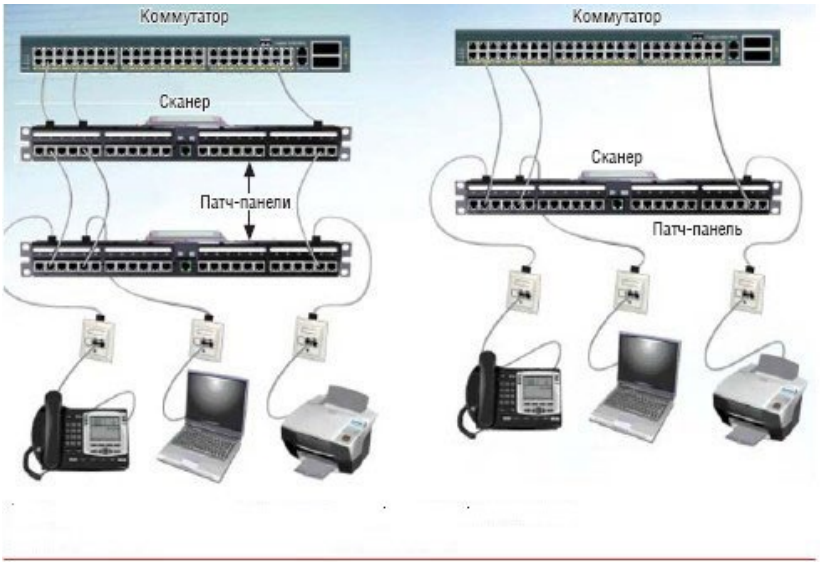
В процессе занятия решаются следующие задачи:

1. Получить практические навыки подбора коммутационного оборудования по критериям различной степени формализации;
2. Приобрести опыт работы с описаниями и техническими спецификациями оборудования.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Способы подключения сетевого оборудования

- Прямое соединение (Interconnect)
- Кроссовое соединение (Cross-connect)
- Связь между кроссами



Прямое соединение (Interconnect) и кроссовое соединение (Cross-connect)

Прямое соединение подразумевает, что активное оборудование подключается непосредственно к панелям, на которых терминированы кабели. При этом активное и коммутационное оборудование должно располагаться рядом друг с другом, а каналы передачи организуются путем соединения портов оборудования и панелей шнурами с вилками соответствующих типов.

Кроссовое соединение фактически представляет собой вывод портов активного оборудования на отдельную панель. В этой схеме используются 2 панели и 2 шнура – коммутационный и аппаратный, причем аппаратный может быть выполнен в виде так называемого “монтажного шнура” – с вилкой, установленной только на одном конце.

Cross-connect применяется в случаях, когда активное оборудование оснащено портами вывода, отличными от модульных (RJ45), к примеру – интерфейсами на основе Telco. Применение схемы cross-connect обеспечивает следующие преимущества:

- Минимизация вероятности повреждения портов активного оборудования;
- Разгрузка лицевых панелей коммутационного поля от шнуров за счет вывода части шнуров на оборотную сторону панелей. При этом также обеспечивается улучшение читабельности маркировки на панелях и улучшаются эстетические характеристики;
- Увеличение удобства подключения активного оборудования, порты которого выведены на заднюю панель;
- Возможность реализации системы интерактивного управления СКС при условии применения соответствующей элементной базы.

Недостаток этой схемы заключается в большей стоимости реализации меньшей плотности портов на единицу высоты монтажного конструктива. Связь между кроссами, по сути дела, является развитием схемы cross-connect, в случае, когда активное и коммутационное оборудование располагается в отдельных монтажных конструктивах. Эта схема подразумевает установку в конструктиве с активным оборудованием отдельной панели (зачастую поставляемой в комплекте с этим оборудованием), и прокладка отрезка многопарного кабеля до соседнего конструктива, содержащего коммутационное оборудование. При таком подключении образуется дополнительное соединение, что заметно ухудшает электрические характеристики канала передачи. По этой причине связь между кроссами применяется только для подключения низкоскоростного оборудования. Стоит отметить, что в случаях, когда кроссовая панель оборудования является его неотъемлемой частью, такая конфигурация считается соответствующей требованиям стандартов (не более 4х точек соединения на канал передачи данных). В подсистемах СКС, реализуемых на основе волоконной оптики, в подавляющем большинстве случаев реализуется схема interconnect. Схема cross-connect практически нереализуема при применении стандартных типов оборудования.

Правила подключения активного оборудования

- Схема interconnect используется при построении СКС, обслуживающих 50-100 рабочих мест, либо при выдвижении заказчиком жестких требований по снижению стоимости инсталлируемой системы. Также данный вариант предпочтителен в случаях, когда длина горизонтальных кабелей близка к максимально допустимой стандартами (90 м). В этом случае за счет меньшего количества соединений увеличивается помехозащищенность линий и появляется возможность применять аппаратные шнуры увеличенной сверх норматива длины.
- Схема cross-connect применяется в крупномасштабных СКС с целью повышения удобства эксплуатации. Также желательно применять этот вариант подключения, когда плотность портов оборудования ЛВС менее 24 на 1U высоты, для более эффективного использования коммутационных панелей.
- Схема cross-connect в обязательном порядке применяется в случаях, когда планируется установка активного сетевого оборудования с Telco-разъемами, а также в случаях, когда в составе СКС планируется применение систем интерактивного управления СКС.
- Для передачи низкоскоростных приложений, не требовательных к рабочим характеристикам канала передачи, допускается использование соединения между кроссами.

Распределитель этажа

Техническое помещение, в котором установлено оборудование РЭ, содержит активное сетевое оборудование, обслуживающие ограниченную группу пользователей (как правило, расположенных на одном этаже, в отдельных случаях - на смежных этажах). Как правило, это коммутаторы, обслуживающие сегмент сети, также могут располагаться выносные блоки телефонных станций. В РЭ допускается применение всех трех вышеописанных способов подключения активного оборудования. Выбор одного из способов подключения зависит от условий конкретного проекта (количество подключаемых рабочих мест, требования заказчика к стоимости и удобству обслуживания системы и т.п.). При отсутствии ограничений желательно применять схему cross-connect/ Максимальная длина шнура или совокупности шнуров, расположенных в РЭ зависит от выбранного способа подключения оборудования, а также от длины шнура на рабочем месте. Стандарт ISO/IEC 11801:2002 требует, чтобы суммарная длина шнуров не превышала 10 м.

Распределитель здания и Распределитель кампуса

В крупных кроссовых узлах устанавливается сетевое оборудование ядра сети, УПАТС, контроллеры систем управления зданием и сигнализацией и другое ключевое активное оборудование.

В РК для подключения активного оборудования наиболее часто применяется схема interconnect, хотя рост масштабов сетей и усложнение архитектуры ведет инсталляторов СКС к применению схемы cross-connect в РЗ, что не противоречит стандартам.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

В соответствии с вариантом подобрать **активное сетевое оборудование**, способное обеспечить весь **необходимый функционал**, требуемый в задании (см. приложение №6).

Каждый вариант состоит из **трёх типов задач**, требующих различные методы и подходы для их решения. При подборе оборудования необходимо соблюдать принцип **минимизации финансовых затрат**. Ограничения по производителям оборудования нет, однако рекомендуется обратить внимание на оборудование **LinkSys**, **CISCO**, **DLINK**, **ASUS**, **HP**.

Вариант 1

1. Подобрать коммутатор с **48 портами** Fast Ethernet и **двумя портами** Gigabit Ethernet, поддерживающий технологию управления потоком **IEEE 802.3x**.

2. Подобрать коммутационное оборудование для сети **небольшого офиса**. В состав сети входят **15 компьютеров с равным уровнем доступа**. Максимальная нагрузка на сеть возможна при одновременном доступе к файловой базе данных **объемом 96 Мб**. Обеспечить возможность подключения существующей **IDS**

(системы обнаружения вторжения), осуществляющей **мониторинг** всего передаваемого внутри локальной сети **трафика**.

2. Подобрать коммутационное оборудование для сети **крупного автосервиса**. Требуется создать инфраструктуру для обслуживания **6 ремонтных боксов**. Необходимо обеспечить работоспособность **специализированного программного обеспечения** и **доступность** всех сетевых **ресурсов** пользователям. Каждый сотрудник имеет **коммуникационное устройство** с беспроводным интерфейсом, которое служит для оповещения о поступивших заказах и контроля за их выполнением. Каждое из них должно строго **контролироваться** и работать **на всей территории** автосервиса. Расстояние между наиболее удаленными точками территории автосервиса 340 метров.

Вариант 2

1. Подобрать **неуправляемый** коммутатор с **16 портами** 10/100/1000Base-T и поддержкой технологии **IEEE 802.1p QoS**.

2. Подобрать коммутационное оборудование для проведения **чемпионата России по киберспорту.** Необходимо обеспечить совместную работу **минимум 90 компьютеров**. Следует избежать ситуации задержек в игре из-за недостаточной
производительности коммутационного оборудования. Пиковый трафик, генерируемый средней современной сетевой игрой, составляет **10Мб\с**. Предусмотреть возможность компактной установки коммутационного оборудования **в стойку**.

3. Подобрать коммутационное оборудование для **телевизионной компании**. Требуется обеспечить раздельную работу 4 студий, каждая из которых должна работать в собственной VLAN сети. Количество компьютеров в студиях 40.

Вариант 3

1. Подобрать коммутатор с возможностью подключения **7 IP- видеокамер** по проводной сети Fast Ethernet с возможностью обеспечивать **электропитание камер по линии связи** (Powerover Ethernet).

2. Подобрать коммутационное оборудование для сети **крупного предприятия**. Требуется организовать **изолированные потоки данных** для разных отделов. Также необходимо создать высокоскоростной **back-bone (выделенную магистральную сеть)** для связи отделов между собой с возможностью **доступа к ресурсам и сервисам** предприятия. На предприятии **25 отделов**. В каждом отделе до **30 компьютеров**.

3. Подобрать коммутационное оборудование для сети **общеобразовательной школы,** в которой имеется **несколько небольших компьютерных классов**. Требуется учесть дальнейшее **увеличение парка машин** и **возможность удалённого управления** всем сетевым оборудованием. Также необходимо обеспечить **распределение нагрузки сети** таким образом, чтобы исключить возможность **намеренного блокирования** каналов связи.

Вариант 4

1. Подобрать коммутатор третьего уровня с минимум **44 портами** FastEthernet с поддержкой протокола **OSPF**, **зеркалирование портов** в режиме Many-to-one.

2. Подобрать коммутационное оборудование для сети **студии видеомонтажа**. В студии создан вычислительный кластер для обсчета цифрового видео из **4 компьютеров**. Оборудование должно быть гарантированно **неблокирующим**, то есть обладать внутренней шиной такой производительности, чтобы гарантированно обработать максимально возможные потоки между всеми нагруженными портами коммутатора.

3. Подобрать коммутационное оборудование для **загородного ресторанного комплекса**. Комплекс состоит из **5 залов** и **2 открытых веранд**. В каждом зале находятся **4 терминала** для управления заказами, а на верандах **по 2**. Требуется обеспечить работу терминалов управления заказами во всех помещениях, доступность терминалам **10 сетевых принтеров** и возможность работы **трём компьютерам менеджеров**.

Вариант 5

1. Подобрать управляемый коммутатор второго уровня с **минимум 8 портами** FastEthernet и **двумя оптическими** портами **SFP**.

2. Подобрать коммутационное оборудование для ядра крупной **корпоративной сети**. Обеспечить коммутацию **18 каналов** от подразделений, каждый из которых имеет пропускную способность в **100 Мб\с**. Необходимо реализовать фильтрацию на основе **IP адресов** и автоматический **мониторинг** состояния
оборудования.

3. Подобрать коммутационное оборудование для **городской больницы**. Требуется обеспечить доступ к **общей больничной базе** во всех кабинетах и к глобальной **сети интернет**. Необходимо предусмотреть возможность **блокирования доступа** к базе из **внешней сети** и **доступ в интернет по WiFi** для посетителей на всей территории больницы.

Вариант 6

1. Подобрать управляемый коммутатор **второго уровня** с минимум **16 портами** FastEthernet и поддержкой **Spanning Tree**.
2. Подобрать коммутационное оборудование для использования в качестве **узловых точек** растущей сети кабельного **интернет-провайдера**. Необходимо обеспечить **удаленное управление** устройством и **возможность подключения** к нему точек доступа **WiFi** без прокладки к ним линий **электропитания**.
3. Подобрать коммутационное оборудование для информационной сети **студенческого общежития**. Необходимо обеспечить высокоскоростную передачу данных между всеми узлами сети. Общежитие имеет **4 этажа**, следовательно, необходима **магистраль передачи данных** между этажами. На каждом этаже по **100 комнат**, в каждой из которых должен быть доступ к сети. Необходимо обеспечить **контроль** распределения адресов в сети и **мониторинг** сетевого трафика.

Вариант 7

1. Подобрать коммутатор **третьего уровня** с возможностью **объединения в стек**, минимум с **30 портами** FastEthernet и **фильтрацией по IP** адресам.
2. Подобрать коммутационное оборудование для **DATA-центра** хостинговой компании. Через сеть в среднем передается **4 Терабайта** в день. Необходимо обеспечить соединение сетей с **разными канальными протоколами** (**FastEthernet**, **GigabitEthernet** на витой паре и **FastEthernet** по оптическим каналам), обеспечить масштабируемость решения.
3. Подобрать коммутационное оборудование для проведения **выставки информационных технологий**. Требуется обеспечить **зону покрытия WiFi** на всей территории выставки, а также возможность **удалённого управления** цифровыми проекторами. Координация выставки будет происходить и **специального центра**, который представляет собой **несколько компьютеров**. Все они должны иметь **доступ к сети,** и **только они** должны иметь **доступ к управлению** проекторами.

Вариант 8

1. Подобрать неуправляемый коммутатор минимум с 7 портами 10/100Base-TX и 1 оптическим портом 100Base-FX.
2. Подобрать коммутационное оборудование для **локальной сети**, компьютеры в которой расположены двумя группами в **двух помещениях**, которые в настоящий момент удалены друг от друга на расстояние (по кабельной трассе) **90 м**. В каждом помещении находятся **20 компьютеров**. При подборе оборудования необходимо учесть **скорый переезд одного отдела** в соседнее здание на расстояние по кабельной трассе **1800 м**. Необходимо обеспечить **минимальные финансовые затраты** и не приобретать оборудование, которое может не понадобиться.
3. Подобрать коммутационное оборудование для **главного узла** компании, занимающейся **продажей трафика** через свою сетевую инфраструктуры. Требуется обеспечить максимально возможную **пропускную способность** и **полезную скорость** передачи данных, компактность и масштабируемость решения.

Приложение 6 **Функции коммутаторов**

Функции коммутаторов 2 уровня

Spanning Tree Protocol (приблизительный перевод – связующее дерево) – описывается стандартами IEEE 802.1d (STP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). Технология позволяет использовать сложносвязанные топологии сетей основанных на коммутаторах. STP снимет ограничение на использование только древовидных топологий в таких сетях. Принцип работы заключается в выделении логического древовидного графа в сложносвязанном графе реальной сети. Технология применяется для повышения отказоустойчивости ЛВС или для реализации резервных каналов связи между несколькими ЛВС.

Автоопределение типа кабеля MDI/MDI-X – позволяет автоматически определить тип соединения в подключенном кабеле витая пара (прямой или кроссовый).

Автосогласование между режимами Full-duplex или Half-duplex –автоматическое определение возможного режима передачи данных по линии. В режиме Full-duplex данные передаются в двух

направлениях одновременно по разным парам. При режиме Half-duplex данные могут передаваться только в одну сторону одновременно. Функция автосогласования между режимами позволяет избежать проблем с использованием разных режимов на разных устройствах.

Агрегация каналов (анг. Link aggregation for parallel links или pool) –описывается стандартом IEEE 802.3ad и предназначена для повышения пропускной способности канала за счет объединения нескольких портов в один высокоскоростной порт с суммарной скоростью объединенных портов. Максимальная скорость определенная стандартом составляет 8 Гбит/сек.

Виртуальные локальные сети (анг. VLAN) – описывается стандартом IEEE 802.1q и позволяет внутри одной физической локальной сети построить несколько отдельных логических сетей (виртуальных сетей), узлы которых изолированы от остальных участков сети.

Возможность установки в стойку (анг. rackmount) – возможность установки коммутатора в стойку или в коммутационный шкаф. Наибольшее распространение получили 19 дюймовые шкафы и стойки, которые стали для современного сетевого оборудования стандартом де-факто.

Возможность установки дополнительных модулей – эта возможность подразумевать наличие слотов расширения или портов подключения внешних модулей, позволяющие разместить дополнительные интерфейсы. В качестве дополнительных интерфейсов выступают гигабитные модули, использующие витую пару, и оптические интерфейсы, способные передавать данные по оптоволоконному кабелю. Диагностика кабеля – технология, позволяющая контролировать состояние подключенных кабелей на основе медной витой пары или оптических линий. При помощи этой функции может быть определено местонахождение коротких замыканий, разрывов, несовпадений волнового сопротивления.

Зеркалирование портов (анг. Port Mirroring)- технология, позволяющая перенаправлять весь трафик с одного (One-to-One) или с нескольких (Many-to-One) портов на единственный порт коммутатора. Технология применяется для содержательного анализа сетевого трафика, проходящего через коммутатор.

Объединение в стек – технология, позволяющее объединять через специальные физические интерфейсы нескольких коммутаторов в одно логическое устройство. Стекирование целесообразно производить, когда в итоге требуется получить коммутатор с большим количеством портов (больше 48 портов). Различные производители коммутаторов используют свои фирменные технологии стекирования, к примеру, Cisco использует технологию стекирования StackWise (шина между коммутаторами 32 Гбит/сек) и StackWise Plus (шина между коммутаторами 64 Гбит/сек).

Приоритетизация трафика по тегам (анг. Priority tags) – описывается стандартом IEEE 802.1p и позволяет отсортировать кадры по степени важности, выставив приоритеты. Более приоритетные кадры будут отправляться в первую очередь, например, высокий приоритет выставляется пакетам VoIP и низкий— пакетам FTP.

Сбор статистики – одна из основных функций сетевого оборудования, дающая возможность анализировать трафик, тем самым выявлять уязвимые места инфраструктуры и в кратчайшие сроки ликвидировать их. Сбор статистики может осуществляться средствами самого сетевого оборудования или специально установленными серверами («примеры»).

Удаленное управление – возможность конфигурирования устройства через сетевое соединение, например средствами протокола SNMP (Simple Network Management Protocol), через встроенный в устройство Web-сервер или через консольный доступ, осуществляемый через ssh или telnet. Консольный доступ может осуществляться через локальные интерфейсы, такие как RS232 (COM-порт).

Управление потоком (анг. Flow Control) – описывается стандартов IEEE 802.3x и обеспечивает защиту от потерь пакетов при их передаче по сети. Принцип действия упрощенно заключается в согласовании работы взаимодействующих устройств, когда передающее и принимающее устройство согласуют интенсивность потока кадров в случае переполнения буфера приемника.

Управляемое питание по витой паре (Power over Ethernet/PSE) – описывается стандартом IEEE 802.af. Функция позволяет обеспечить питание (до 15,4 Ватт на порт) подключенных к коммутатору устройств таких, как IP-камеры, Wi-Fi точки доступа, IP-телефоны или многофункциональные терминалы.

Фильтрация многоадресных рассылок – технология, позволяющая фильтровать широковещательные рассылки канального уровня, которые обычно передаются без ограничений по всем портам коммутатора. Применяется для оптимизации трафика в крупных сетях.

Фильтрация трафика по MAC адресам – технология, позволяющая составлять ACL (списки контроля доступа) по отношения к адресам канального уровня. Используется для привязки подключенных устройств к порту коммутатора или для разрешения передачи трафика от определенных устройств на выбранный порт.

Функции коммутаторов 3-го уровня

L3 коммутация – упрощенно, возможность коммутатора проводить продвижение пакетов не на основе MAC адресов, а на основе IP адресов. Поддержка протоколов маршрутизации – составление таблиц коммутации с помощью протоколов маршрутизации.

Фильтрация по параметрам IP и TCP\UDP – осуществление фильтрации трафика по алгоритмам формального межсетевого экарана, т.е. основываясь на значении IP адресов или портов TCP \ UDP.

Время выполнения работы 90 мин**;**

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1**.** Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 17 «Настройка Wi-Fi-роутера»

Цель работы: В результате выполнения лабораторной работы научиться производить монтаж разнообразного телекоммуникационного оборудования.

В процессе занятия решаются следующие задачи:

1. Научить производить расчет магистральных подсистем;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

В офисе на несколько рабочих мест, оборудованных компьютерами, или же в обычной квартире, где есть настольный ПК и ноубук, **wifi роутер** может оказаться очень полезным.

Wifi роутер представляет собой сетевое устройство, которое служит для создания беспроводной сети между компьютерами, мобильными устройствами (ноубуки, кпк, планшетники, мобильные телефоны). Также wifi роутер может выполнять функцию точки доступа wifi, а также функции ethernet-маршрутизатора для подключения ПК.

Настроить wifi роутер можно как для работы по внутренней сети, так и для выхода в интернет. Настройка wifi роутеров разных моделей может иметь некоторые отличия, однако приведенные ниже инструкции актуальны для подавляющего большинства современных моделей wifi роутеров.

Порядок работы

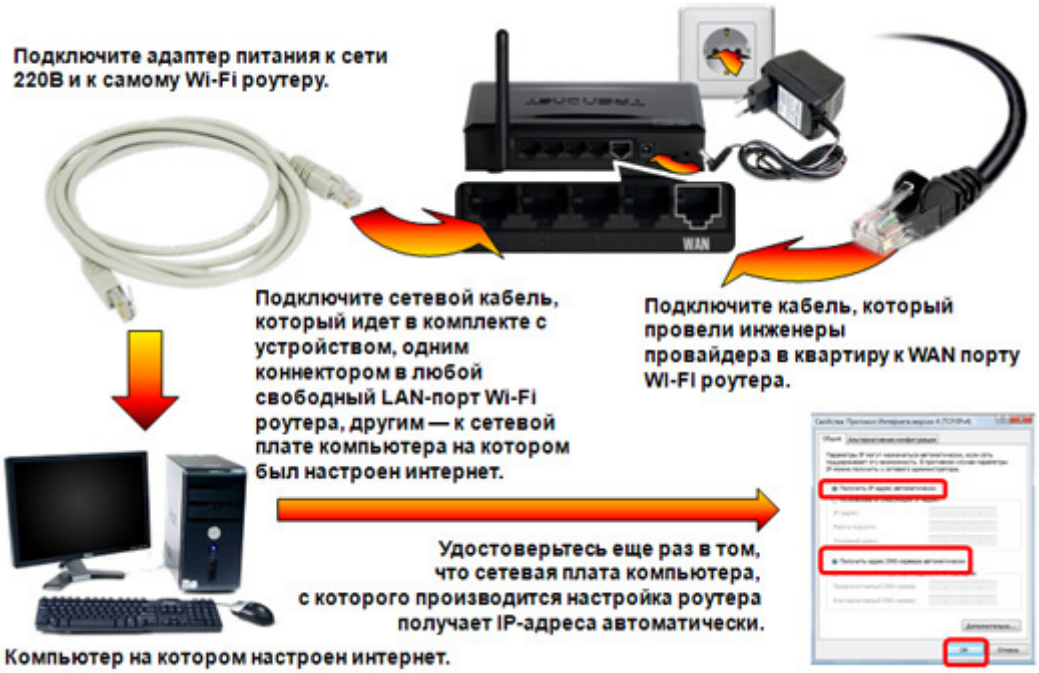
1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Для настройки внутренней сети и интернета через wifi роутер понадобятся такие «ингредиенты»:

- готовое подключение к интернету от провайдера (например, по кабелю-"витой паре")
- компьютер с сетевой картой
- сетевой кабель с «прямым» обжимом
- wifi роутер

1. **Подключите оборудование по схеме:**



Интерфейс wifi роутера имеет, как правило, 4 внутренних порта (LAN) и 1 внешний (WAN). Во внешний порт подключается кабель, по которому осуществляется соединение с интернетом. Внутренние порты служат для подключения компьютеров к внутренней сети.

Для начала нам понадобится настроить wifi роутер. Для это следует **соединить wifi роутер с настольным ПК** при помощи сетевого кабеля «прямого» обжима.

Если соединение выполнено успешно, то в сетевых подключениях компьютера отобразится новое сетевое подключение. Правым щелчком мыши следует вызвать контекстное меню и выбрать в нем пункт «свойства». Откроется окно редактирования свойств сетевого подключения.

В этом окне следует выбрать пункт **«Протокол интернета (TCP/IP)»** и нажать кнопку «свойства», после чего откроется окно редактирования свойств. В данном окне следует выбрать пункт «Использовать следующий IP-адрес» (или аналогичный, т. е. ручные настройки IP-адреса). Далее необходимо вручную ввести следующие данные:

IP-адрес:192.168.02 (192.168.1.2)
Маска подсети:255.255.255.0
Основной шлюз:192.168.0.1 (192.168.1.1)
DNS:192.168.0.1 (192.168.1.1)

В данном случае 192.168.0.1 или 192.168.1.1 — стандартный локальный IP-адрес, присваиваемый wifi роутеру, а 192.168.0.2 или 192.168.1.2 — локальный IP-адрес компьютера. Производителем wifi роутера могут быть указаны другие настройки локального IP, тогда нужно использовать их.

Проверить правильность IP-адресов можно, выполнив команду «ping». Для этого необходимо войти в командную строку Windows (пуск-> выполнить-> cmd) и ввести следующую команду:
ping 192.168.x.1
где 192.168.x.1 — локальный IP-адрес роутера
Если IP-адрес пингуется, то можно переходить к следующему этапу, а именно — к настройке wifi роутера через веб-интерфейс. Как правило, в руководстве к роутеру указано, как войти в интерфейс управления роутером. Если же такой информации нет, то следует в адресную строку браузера ввести адрес **http://192.168.x.1**.

На открывшейся странице появится приглашение **ввести логин и пароль для доступа к wifi роутеру**. Эти данные должны быть указаны в инструкции к роутеру. Если же их нет, можно попробовать логин «admin», пароль - «admin» или же пустой. Это стандартные логин и пароль на большинстве моделей роутеров.

Теперь стала доступной **панель администрирования роутера**. В настройках wifi роутера следует выбрать раздел "wifi" (возможно, он будет называться «wireless», т. е. «беспроводной»). Затем следует выбрать текущий профиль пользователя или же создать новый и **в настройках профиля указать следующие данные**:
SSID:{название вашей сети}
Channel:auto
Wireless Mode: auto
Authentication Method: WPA-PSK
WEP Encrypting:TKIP
WPA Pre-Shared Key: укажите пароль для доступа в сеть

Остальные настройки можно оставить в значении «по умолчанию». Затем следует перезапустить роутер через веб-интерфейс и **приступить к настройкам wifi на мобильных устройствах**: ноутбуке, КПК, мобильном телефоне и т. д.
Для этого войдя в настройки беспроводного соединения, следует вручную прописать IP-адрес, маску подсети, шлюз:

IP-адрес – выбирается из диапазона свободных адресов (192.168.0/1.0-255)
Маска – 255.255.255.0
Основной шлюз – 192.168.(0/1).1

Затем, сохранив и применив полученные настройки, **следует указать также в настройках авторизации WEP-шифрование и тип аунтефикации по WPA-PSK и TKIP**. После этого остается ввести пароль от сети и подключиться.
Если нужно «раздать» по внутренней сети интернет, то нужно подключить сетевой кабель, идущий от интернет-провайдера к внешнему интерфейсу на wifi роутере.

Затем в настройках роутера нужно указать параметры внешнего интерфейса -провайдера.

Время выполнения работы 90 мин**;**

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 18 «Создание рабочих чертежей»

Цель работы: В результате выполнения лабораторной работы научиться производить монтаж разнообразного телекоммуникационного оборудования.

В процессе занятия решаются следующие задачи:

1. изучить государственные стандарты по оформлению чертежей ГОСТ 2.303–68 «Линии чертежа», ГОСТ 2.304–81 «Шрифты», производить расчет магистральных подсистем;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Используйте справочную систему программы AutoCad для получения необходимой информации.

Порядок работы

2. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

1. Используя ПО AutoCad создайте архитектурный чертеж здания техникума БРИЭТ, в соответствии с требованиями ГОСТ.

Время выполнения работы 90 мин**;**

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 19 «Создание спецификации»

Цель работы: В результате выполнения лабораторной работы: Научить разрабатывать спецификации для сборочных чертежей в ручном и полуавтоматическом режимах, познакомиться с основными разделами спецификации и приемами работы с ними

В процессе занятия решаются следующие задачи:

1. Изучить государственные стандарты по оформлению чертежей ГОСТ 2.303–68 «Линии чертежа», ГОСТ 2.304–81 «Шрифты» . производить расчет магистральных подсистем;

2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Спецификация представляет собой состав сборочной единицы, необходимый для ее изготовления. Каждый сборочный чертеж должен содержать спецификацию. Согласно ГОСТ 2.102-68 спецификация является основным конструкторским документом для сборочных единиц. На основе спецификации формируются все остальные сборочные документы.

Система проектирования спецификаций предполагает создание спецификаций в ручном и автоматическом режиме.

Создание спецификаций в ручном режиме – это самый простой способ получения спецификации в КОМПАС-ГРАФИК. Использование этого метода целесообразно в том случае, когда нужно быстро подготовить спецификацию, или тогда, когда на данный момент ее разработки нет ни сборочного чертежа, ни чертежей деталей, входящих в сборку.

Основным способом получения спецификаций в КОМПАС-ГРАФИК является создание спецификаций в полуавтоматическом режиме. Модуль проектирования в этом случае устанавливает связи между спецификацией, листом или листами сборочного чертежа и рабочими чертежами деталей. Необходимые для создания спецификации данные накапливаются в листе или листах чертежа на сборочную единицу непосредственно во время работы над этими документами.

Порядок ввода данных может быть совершенно произвольным.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

I. Создание спецификации к сборочной единице ПК.02.06.01.00 в ручном режиме.

1. Любым способом запустите КОМПАС-ГРАФИК. Если в рабочем окне программы открыты какие-либо окна документов, закройте их.

2. Для создания новой спецификации выполните команду Файл – Создать - Спецификацию или нажмите кнопку Новая спецификация на Панели управления. На экране появится бланк спецификации

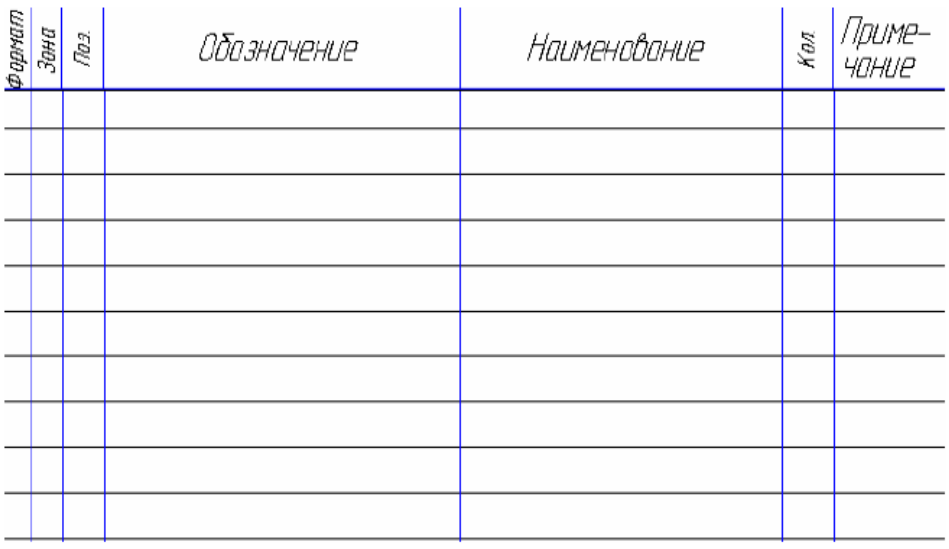


Рис.1

Сразу после создания спецификация переходит в нормальный режим, который предназначен для заполнения бланка и элементы заполнения основной надписи в нем автоматически гасятся.

3. Панель управления перешла в режим работы со спецификацией:

По умолчанию система создает простую спецификацию по ГОСТ 2.102-68. Убедитесь в этом с помощью команды Настройка – Параметры текущей спецификации**.** В диалоговом окне настройка параметров текущей спецификации в качестве стиля документа должен быть установлен соответствующий стиль (рис.2).

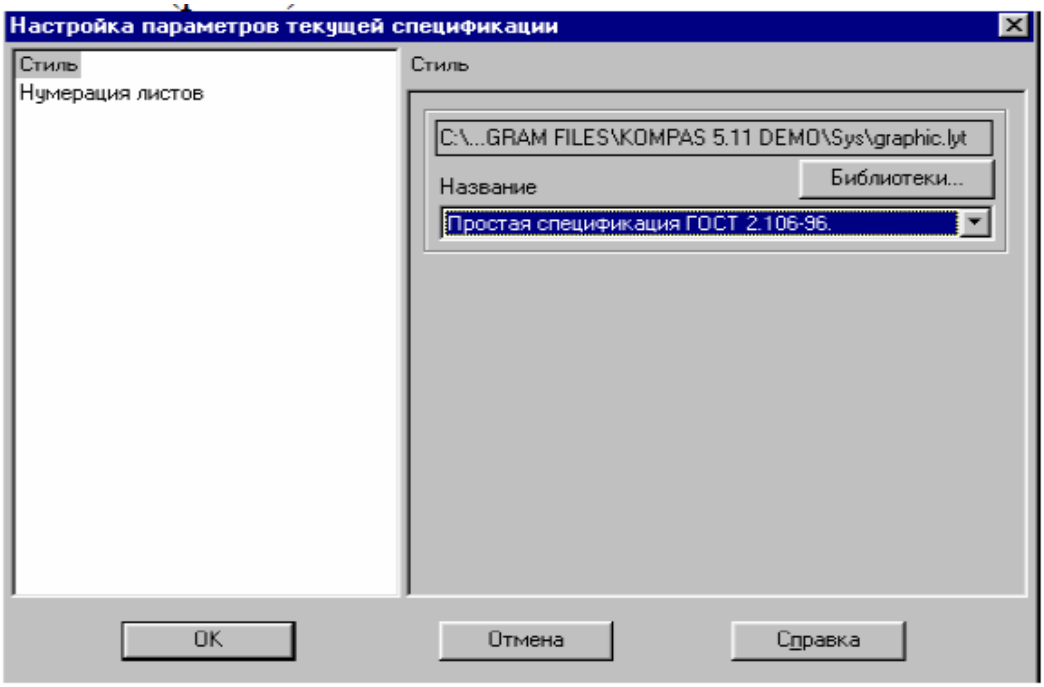


Рис.2

Выполните команду Настройка – Настройка спецификации. На экране появится диалоговое окно Настройка спецификации. Так как спецификация будет создана в ручном режиме, отключите опцию Связь сборочного чертежа со спецификацией (рис.3).

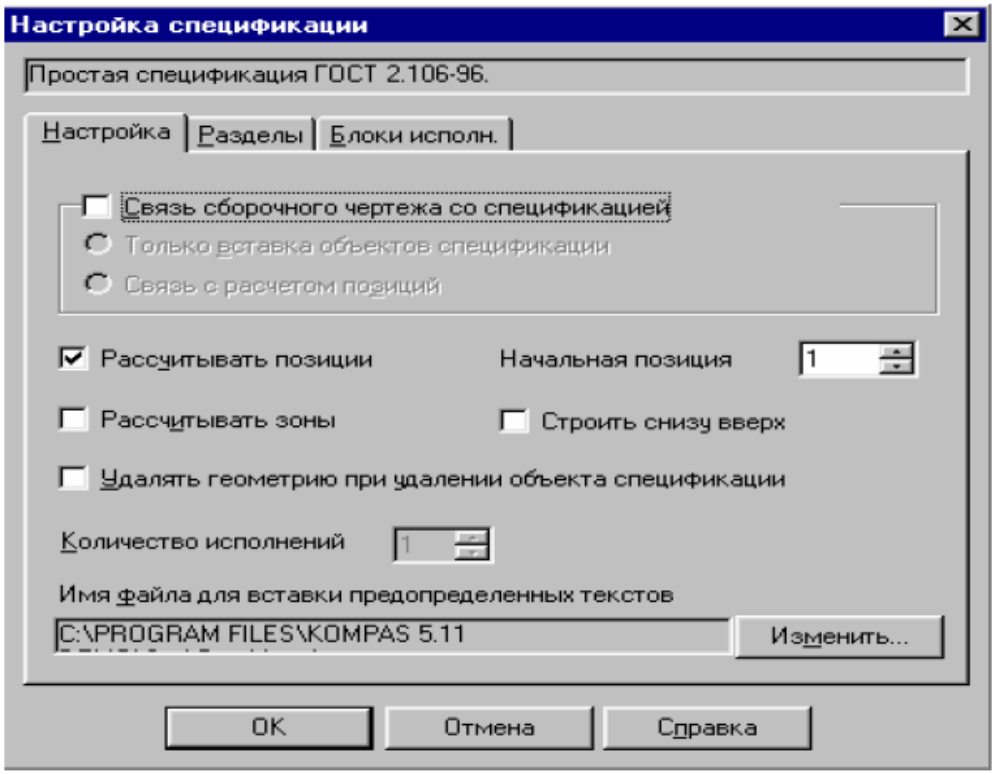


Рис.3

Выполните команду Файл – Сохранить как**.** В диалоговом окне Укажите имя файла для записи откройте папку *Blok* , а в поле Имя файла введите имя документа пк**.02.06.01.00.SPW** (SPW – расширении спецификаций в системе КОМПАС-ГРАФИК). Запишите документ на диск щелчком на кнопке Сохранить (рис.4).

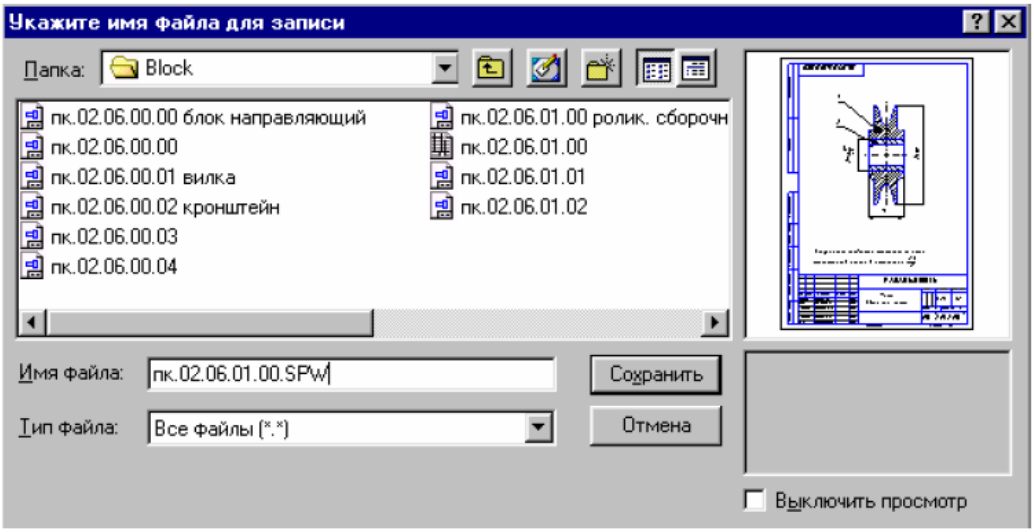


Рис.4

Создание раздела Детали

1. Выполните команду Редактор – Добавить раздел. В диалоговом окне Выберите раздел и тип объекта сделайте текущим раздел Детали и щелкните на кнопке Создать (рис.5).

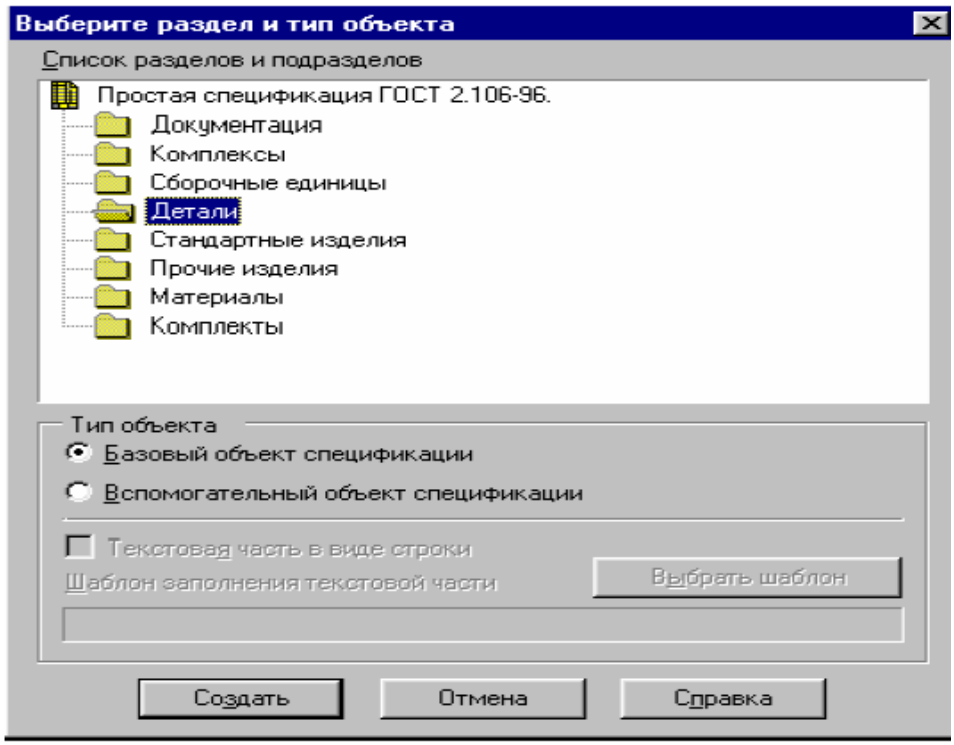


Рис.5

В бланке спецификации появилось название раздела, а его первая строка стала доступной для редактирования. В ячейке Позиция система автоматически проставила номер первой позиции (рис.6).

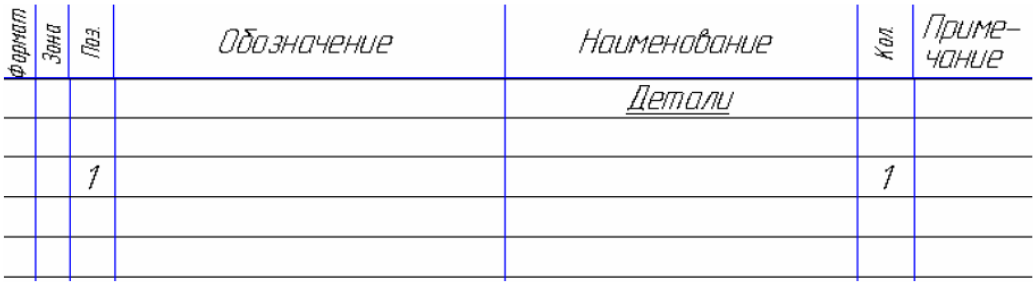


Рис.6

Заполните первую строку так, как показано на Рис.7. После заполнения каждой ячейки в строке не нажимайте клавишу [Enter] – это приведет к формированию новой пустой строки в данной ячейке. Для перехода к нужной ячейке пользуйтесь мышью или клавиатурными командами [Tab] для перемещения слева направо и [Shift]+[Tab] справа налево (рис.7).

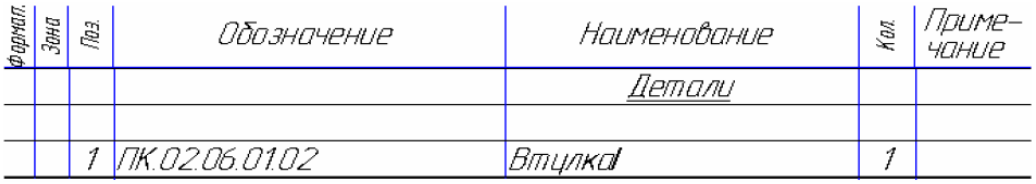


Рис.7

После заполнения всех ячеек строки подтвердите создание объекта, щелкнув мышью в любом свободном месте чертежа.

5. Для создания второго объекта выполните команду Редактор – Добавить базовый объект. Система создаст новую строку, которую заполните в соответствии с Рис.8. подтвердите создание объекта щелчком объекта в свободном месте спецификации.

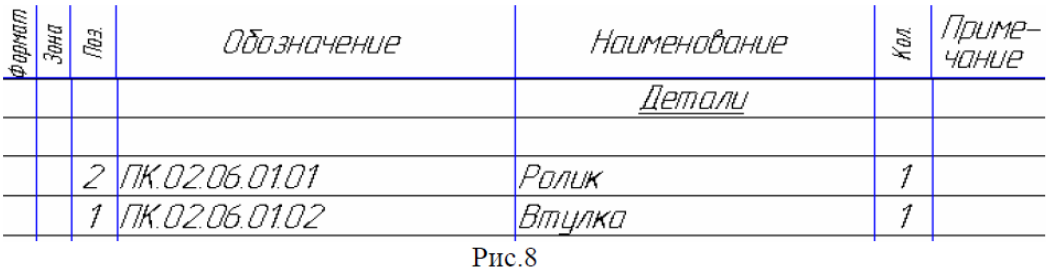


Рис.8

За настройку текущего раздела отвечают кнопки в Строке параметров. Например, правая кнопка Сортировка включает или выключает режим автоматической сортировки в разделе. По умолчанию в разделе Детали активны режимы Проставлять позиции, Подключить геометрию и Автоматическая сортировка.

Создание раздела Документация

1. Для создания нового раздела воспользуйтесь кнопкой Создать раздел на Панели управления. В диалоговом окне Выберете раздел и тип объекта сделайте текущим раздел Документация и щелкните на кнопке Создать (рис.9).

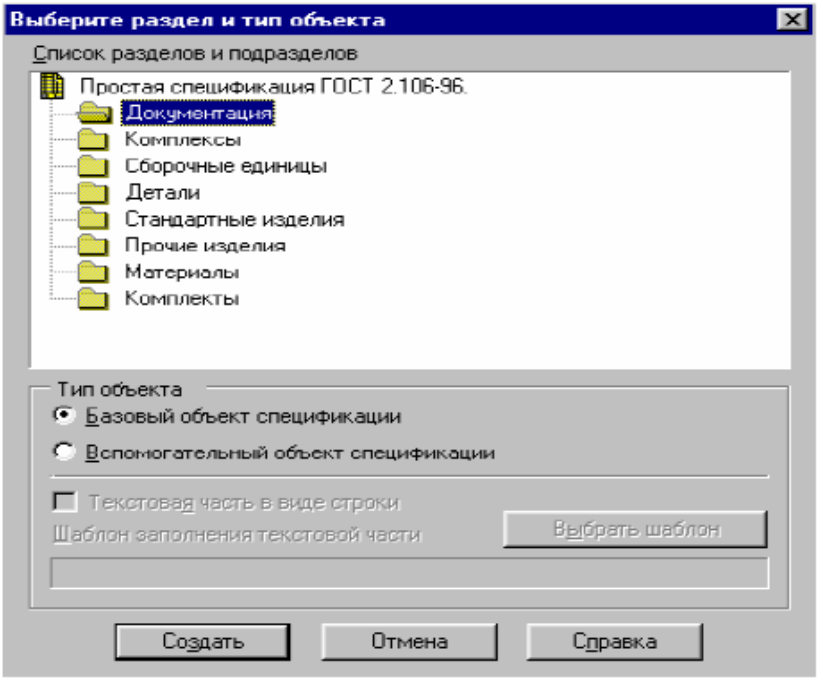


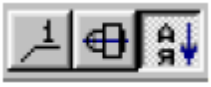
Рис.9

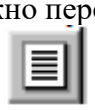
Заполните новую строку как показано на рис.10. Подтвердите создание объекта с помощью клавиатурной команды [Ctrl]+[Enter].

Формат	Зона	Поз.	Обозначение	Наименование	Кол.	Приме-чание
				Документация		
			ПК.02.06.01.00СБ	Сборочный чертеж		
				Детали		
А4		1	ПК.02.06.01.01	Ролик	1	
А4		2	ПК.02.06.01.02	Втулка	1	

Рис.10

После создания объекта раздел Документация останется текущим. В Строке параметров по умолчанию активен лишь режим автоматической сортировки. Режим простановки позиций и подключения геометрии отключены



Чтобы получить доступ к штампу, нужно перейти в режим разметки страниц. Для смены режима щелкните на кнопке Разметка страниц  на Панели управления. В этом режиме система автоматически делит заполненную таблицу на необходимое количество страниц, добавляет к каждой из них элементы оформления и выводит их на

экран. Чтобы увидеть всю страницу целиком, щелкните на кнопке Масштаб по высоте листа  в Строке текущего состояния.

Заполнение основной надписи спецификации аналогично заполнению основной надписи любого другого документа КОМПАС-ГРАФИК. Выполните двойной щелчок мышью в области штампа – система войдет в режим его редактирования. Заполните основную надпись так, как показано на рис.11. Для выхода из режима работы со штампом щелкните мышью в любом месте чертежа.

					ПК.02.06.01.00			
Изм.	Лист	№ докум.	Подп.	Дата				
Разраб.		Иванов А.В.			Ролик	Лит.	Лист	Листов
Пров.		Петров Ю.П.						1
Н.контр.		Сидоров А.А.				АО"КАСКАД"		
Утв.		Попов М.М.						

Рис.11

Время выполнения работы 90 мин**;**

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1**.** Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 20 «Программные средства проектирования локальных сетей»

Цель работы: В результате выполнения лабораторной работы научиться проектировать локальную вычислительную сеть.

В процессе занятия решаются следующие задачи:

1. Научить производить правильный выбор топологии сети, расчет стоимости сетевого оборудования;

2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Проектирование конфигурации ЛВС относится к этапу проектирования технического обеспечения автоматизированных систем и осуществляется на этом этапе после распределения функции автоматизированной системы по абонентским станциям ЛВС, выбора типов абонентских станций, определения физического расположения абонентских станций.

Задание на проектирование включает требования к ЛВС, указания о доступных компонентах аппаратных и программных средств, знания о методах синтеза и анализа ЛВС, предпочтения и критерии сравнения вариантов конфигурации ЛВС.

Рассмотрим варианты топологии и состав компонент локальной вычислительной сети.

1.1. Топология ЛВС.
Топология сети определяется способом соединения ее узлов каналами связи. На практике используются 4 базовые топологии:

- звездообразная (рис. 1 ,а , 1 ,б);
- кольцевая (рис. 2);
- шинная (рис. 3);
- древовидная или иерархическая (рис. 4).

Топология сети влияет на надежность, гибкость, пропускную способность, стоимость сети и время ответа [1, табл. 1].
Выбранная топология сети должна соответствовать географическому расположению сети ЛВС, требованиям, установленным для характеристик сети, перечисленным в табл. 1. Топология влияет на длину линий связи.
Топология звезда Топология распределенная звезда

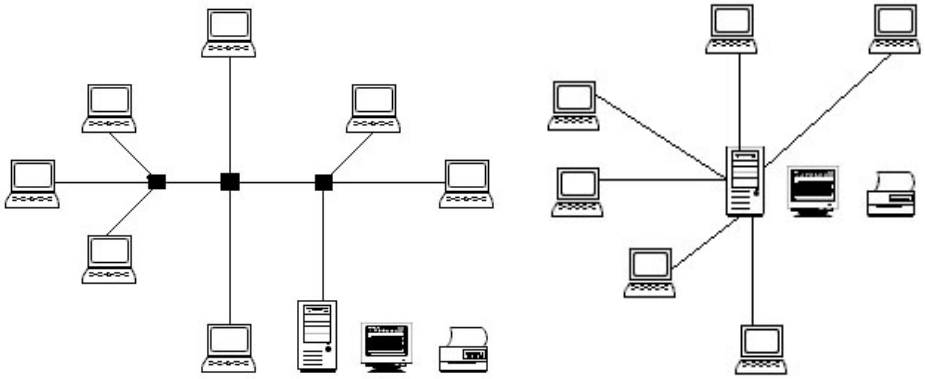


Рис.1.

Сравнительные данные по характеристикам ЛВС Таблица 1.

P5. Характеристика	Качественная оценка характеристик		
	Шинной и древовидной сети	Кольцевой сети	Звездообразной сети
I. Время ответа Юта.	В маркерной шине **t отв.** предсказуемо и зависит от числа узлов сети. В случайной шине t отв. зависит от нагрузки	**$t_{отв.}$** Есть функция от числа узлов сети	**$T_{отв.}$** зависит от нагрузки и временных характеристик центрального узла

2. Пропускная способность С	В маркерной шине зависит от количества узлов. В случайной шине С увеличивается при спорадических малых нагрузках и падает при обмене длинными сообщениями в стационарном режиме	С падает при добавлении новых узлов	С зависит от производительности центрального узла и пропускной способности абонентских каналов
3. Надежность	Отказы АС не влияют на работоспособность остальной части сети. Разрыв кабеля выводит из строя шинную ЛВС.	Отказ одной АС не приводит к отказу всей сети. Однако использование обходных схем позволяет защитить сеть от отказов АС	Отказы АС не влияют на работоспособность остальной части сети. Надежность ЛВС определяется надежностью центрального узла

Топология кольцо

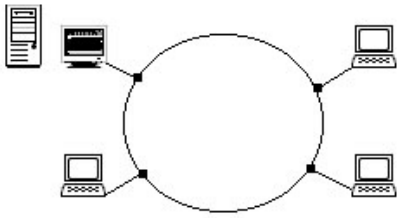


Рис.2

Топология линейная шина

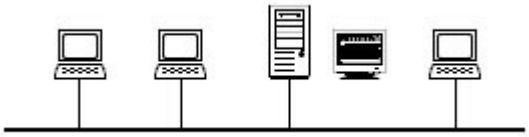
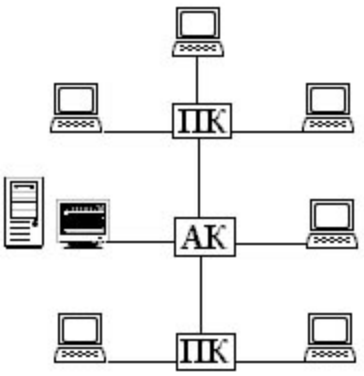


Рис.3

Иерархическая сеть с концентраторами



АК - активный концентратор ПК - пассивный концентратор

Рис. 4.

1.2. Выбор типов линий связи

В качестве линий связи могут выступать кабели со скрученными парами проводов *(витые пары), коаксиальные кабели, волоконно-оптические кабели, радио, инфракрасные* ИК-, СВЧ - каналы.

В набор параметров линий связи ЛВС входят: полоса пропускания и скорость передачи данных, способность к двухточечной, многоточечной и/или широковещательной передаче (то есть допустимые

применения), максимальная протяженность и число подключаемых абонентских систем, топологическая гибкость и трудоемкость прокладки, устойчивость к помехам и стоимость.
При выборе типов кабеля учитывают следующие показатели:

- стоимость монтажа и обслуживания;
- скорость передачи информации;
- ограничения на величину расстояния передачи информации (без дополнительных усилителей-повторителей *(repeater);*
- безопасность передачи данных.

Главная проблема заключается в одновременном обеспечении показателей, например, наивысшая скорость передачи данных ограничена максимально возможным расстоянием передачи данных, при котором еще обеспечивается требуемый уровень защиты данных. Легкая наращиваемость и простота расширения кабельной системы влияют на ее стоимость.
Условия физического расположения помогают определить наилучшим образом тип кабеля и его топологию. Каждый тип кабеля имеет собственные ограничения по максимальной длине: ***витая пара*** обеспечивает работу на коротких отрезках, ***одноканальный коаксиальный кабель -*** на больших расстояниях, ***многоканальный коаксиальный а волоконно-оптический кабель -*** на очень больших расстояниях.
Скорость передачи данных тоже ограничена возможностями кабеля: самая большая - у ***волоконно-оптического,*** затем идут ***одноканальный коаксиальный, многоканальный кабели*** **и** ***витая пара.*** Под требуемые характеристики можно подобрать имеющиеся в наличии кабели.
В табл. 2 приводятся характеристики линий связи ЛВС **Ethernet.**

Характеристики линий связи Ethernet Таблица2

Параметр	Тип линии связи		
	Тонкопроводная (моноканал)	Толстопроводная (моноканал)	Широкополосная (поликанал)
Максимальная длина (без повторителен),м	185	500	1900
Тип кабеля	RG58	Коаксиальный кабель в тефлоновой или полихлорвиниловой оболочке	Телевизионный коаксиальный кабель
Максимальное число АС	30	200	1023
Скорость передачи, Мбит/с	10	10	10

Этапы конфигурирования ЛВС
Конфигурирование ЛВС - это многокритериальная оптимизационная задача, так как на выбор конфигурации ЛВС влияет большое число факторов. В качестве целевой функции при решении этой задачи можно взять минимизацию величины стоимости ее аппаратного и программного обеспечения при условиях удовлетворения всех требований пользователя к передаче информации в полном объеме, времени ответа, пропускной способности и надежности сети.
Проектирование конфигурации ЛВС требует решения ряда задач, включающих выбор комплекса программно-аппаратных средств локальной вычислительной сети, выбор типов сетей связи в данном комплексе, трассировку кабельной сети ЛВС в зданиях и помещениях. В процессе построения ЛВС необходимо учитывать ряд требований прикладного характера, например, физическое расположение пользователей, количество и типы оконечных систем, требования к передаче данных (типы данных, среднюю нагрузку), требования пользователей к программным и аппаратным ресурсам. Расстояние между оконечными системами, наличие несовместимых оконечных систем и требование к контролю

доступа пользователей к отдельным участкам ЛВС могут привести к необходимости предусматривать в составе сети различные ***шлюзы*** **и** ***мосты.*** В любой ЛВС существенным фактором является максимально достижимая пропускная способность сети связи. Она характеризует предел допустимых функциональных возможностей сети. Поэтому перед выбором ЛВС необходимо оценить, какая пропускная способность требуется пользователям данной прикладной области.

Вот некоторые отличительные характеристики и факторы, влияющие на выбор комплекса программно-аппаратных средств локальных вычислительных сетей и проектирование соответствующей конфигурации:

1) характеристики среды передачи информации или кабельной системы, такие как: помехозащищенность, защита от климатических воздействий, протяженность без промежуточного усиления сигнала, стоимость приобретения и установки;
2) максимальная протяженность сети;
3) предполагаемое количество оконечных систем;
4) основная сфера применения (на производственном предприятии, в учреждении или в учебной сфере);
5) функциональное назначение, то есть классы решаемых задач (научная деятельность, образование, резервирование мест, удаленный ввод/вывод, "распределенная обработка данных, управление и учет, финансовые операции);
6) тип передаваемой информации (данные, изображения, речь);
7) оценка пропускной способности сети;
8) сетевое программное обеспечение;
9) интерсетевое обеспечение (необходима ли связь с другими сетями ЭВМ);
10) показатель надежности сети в целом и отдельных ее частей;

Проектирование конфигурации ЛВС проходит через три основных этапа:

1) определение требований к ЛВС;
2) синтез альтернативных конфигураций ЛВС;
3) выбор наиболее предпочтительной конфигурации из имеющихся вариантов.

Проектирование ЛВС необходимо производить с учетом стратегического планирования развития АСУ, принимая во внимание возможность увеличения количества, АС в ЛВС, подключения новых участков ЛВС в других подразделениях предприятия (учреждения).

Исходные данные для проектирования ЛВС представляют собой формальное описание конкретной прикладной области (например, цеха механообработки, администрации производственного объединения, бухгалтерии, отдела кадров и т.д.). Основой является план зданий и помещений с отмеченными на нем местоположениями существующих ЭВМ.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Выбор топологии ЛВС:

Исходные данные к заданию

Пользователи: студенты, преподаватели, инженеры, программисты, лаборанты, техники кафедры автоматизированных систем управления УГАТУ.

Рекомендуемое число клиентских станций: 30-60 с расположением в 4-5 комнатах.

Функции:

1) реализация учебного процесса на лабораторных, практических занятиях, выполнение курсового и дипломного проектирования;
2) организация учебного процесса, подготовка к проведению **занятий,** разработка методического обеспечения;
3) разработка программного обеспечения для работы в сети;
4) профилактика и ремонт оборудования.

Расчет стоимость оборудования ЛВС:

предлагается провести по прайс-листу сетевого оборудования одной из компаний г.Уфы (например компаний Кламас, Форте, Фермо …) на дату проектирования ЛВС. В список включить только

аппаратные средства (в т.ч. системы резервного копирование, бесперебойного питания, зеркалирования …), программное обеспечение не учитывать при расчете стоимости.
Включить затраты по проектированию и монтажу ЛВС.

Требования к проектируемой сети

Проектируемая ЛВС должна удовлетворять целому ряду требовании. Наиболее значительные из них связаны с передачей данных и состоят в следующем:
ЛВС должна выполнять разнообразные функции по передаче данных, включая пересылку файлов, поддержку терминалов (в том числе графических), электронную почту, обмен с внешними запоминающими устройствами, обработку сообщений доступ к файлам и базам данных.
ЛВС должна допускать подключение большого набора стандартных и специальных устройств, в том числе: ЭВМ, терминалов, устройств внешней памяти, принтеров, графопостроителей, факсимильных устройств, контрольного и управляющего оборудования, аппаратуры подключения к другим ЛВС и сетям (в том числе и к телефонным) и т.д.
ЛВС должна доставлять данные адресату с высокой степенью надежности (коэффициент готовности сети должен быть не менее 0.96), должна соответствовать существующим стандартам, обеспечивать "прозрачный" режим передачи данных, допускать простое подключение новых устройств и отключение старых без нарушения работы сети длительностью не более 1 с ; достоверность передачи данных должна быть не больше +1E-8.

2.2. Перечень задач по проектированию ЛВС

2.2.1. Выбрать топологию ЛВС (и обосновать выбор).

2.2.2. Нарисовать функциональную схему ЛВС и составить перечень аппаратных средств.

2.2.3. Выбрать оптимальную конфигурацию ЛВС.

2.2.4. Произвести ориентировочную трассировку кабельной сети и выполнить расчет длины кабельного соединения для выбранной топологии с учетом переходов между этажами. Поскольку существуют ограничения на максимальную длину одного сегмента локальной сети для определенного типа кабеля и заданного количества рабочих станции, требуется установить необходимость использования повторителей.

Время выполнения работы 90 мин**;**

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1**.** Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Сетевое передающее оборудование

Лабораторная работа № 21 «Программные средства проектирования локальных сетей»

Цель работы: В результате выполнения лабораторной работы научиться проектировать локальную вычислительную сеть с помощью специализированного ПО.

В процессе занятия решаются следующие задачи:

1. Изучить ПО для проектирования ЛВС;
2. Научить учащихся проводить администрирование ЛВС;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия;

Выполните задания

Используя ресурсы сети Интернет найдите ПО для создания проекта будущей ЛВС. Скачайте и установите это ПО. Используя возможности ПО создайте проект сети общеобразовательной школы (проект здания и расположения кабинетов придумайте сами).

Время выполнения работы 90 мин**;**

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в ходе выполнения работы т.е.команды введены правильно, но в ходе выполнения работы возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1**.** Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 13 «Оформление проектной документации»

Цель работы: Научиться правильно оформлять проектную документацию.

В процессе занятия решаются следующие задачи:

2. формированиея умения оформления проектной документации ЛВС.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Ответьте на вопросы:

Вопрос № 1. Что такое проектно-сметная документация. Определения.

Вопрос № 2. Законодательные аспекты работы с проектно-сметной документацией в проектировании сетей.

Вопрос № 3. Общие сведения о проектно-изыскательских работах.

Вопрос № 4. Стадийность проектирования. Требования и стандарты оформления проектной документации.

Вопрос № 5. Состав проектной документации. Требования Законодательства.

Вопрос № 6. Проектная документация.

Вопрос № 7. Рабочая документация.

Вопрос № 8. Сметная документация.

Вопрос № 9. Экспертиза проектно-сметной документации.

Вопрос № 10. Правовое обеспечение экспертизы проектно-сметной документации. Государственная экспертиза проектной документации на особо опасные, технически сложные и уникальные объекты.

Вопрос № 11. Согласование и утверждение проектно-сметной документации.

Вопрос № 12. Введение в исполнительную документацию.

Вопрос № 13. Цели ведения исполнительной документации.

Вопрос № 14. Состав приемо-сдаточной документации.

Вопрос № 15. Исполнительная документация. Последовательность ведения исполнительной и приемо-сдаточной документации.

Вопрос № 16. Контроль качества исполнения строительно-монтажных работ.

Время выполнения работы 90 мин;

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Изучаемая тема: Организация, принципы построения и функционирования компьютерных сетей.

Практическая работа № 14 «Порядок тестирования и приёмо-сдаточных испытаний локальной сети»

Цель работы: Научиться производить тестирование и испытания ЛВС по определенному порядку.

В процессе занятия решаются следующие задачи:

1. формированиея умения составлять порядок тестирование и испытания ЛВС.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Используя информационные источники создайте методичку по организации порядка тестирования и ПСИ локальной сети.

Примерное содержание методического руководства:

1. Перечень основных работ;
2. Подготовка и область измерений;
3. Определение кластера;
4. Процедура приемки сети с проведением драйв тестов;
5. Процесс сбора данных;
6. Критерии приемки сети на основе анализа статистических данных;

Время выполнения работы 90 мин;

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно

3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2016. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2017. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2017.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2020.
5. Microsoft Windows Server 2019. Справочник администратора [электронная версия]/Пер. с англ. — М.: Русская Редакция, 2019. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2019: Справочник администратора[электронная версия]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2020.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия]/ С. В. Бормотов — СПб.: Питер, 2016. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2019 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2019. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2019.- 1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2019. – 944 с., ил.

Кроссворд «Сети»

По горизонтали	По вертикали
1: Процесс слежения за сетевой безопасностью организации, создание оптимальной работоспособности компьютеров и программного обеспечения для пользователей 2: сведения о чём-либо, независимо от формы их представления 4: величина, характеризующая количестве бит, символов или блоков, передаваемых за единицу времени 5: любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах 6: процесс переноса данных (цифрового битового потока) в виде сигналов от точки к точке 9: система физических каналов связи 10: стандарт, описывающий правила взаимодействия функциональных блоков при передаче данных 11: процесс присоединения сетевого оборудования	1: технология передачи данных по сети (ADSL) 3: устройство, применяющееся в системах связи для физического сопряжения информационного сигнала со средой его распространения 4: некая логическая связь между двумя устройствами в сети 7: представление фактов и идей в формализованном виде, пригодном для передачи и обработки в некотором информационном процессе. 8: так называется часть ячейки, содержащая служебную информацию

Критерии оценивания

Кроссворд разгадан на:

100%- «5»

75% - «4»

60% -«3»

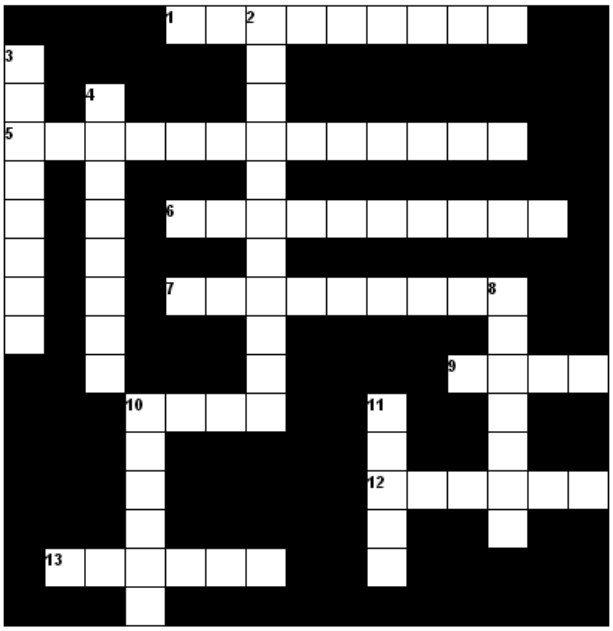
РУБЕЖНЫЙ КОНТРОЛЬ

Кроссворд «Проектирование сетевой инфраструктуры»

Проектирование сетевой инфраструктуры

Кроссворд

Внимательно прочитайте вопрос.
Введите ответ в соответствующие клетки.



По горизонтали	По вертикали
1: Способ описания конфигурации сети, схема расположения и соединения сетевых устройств. 5: Специализированный сетевой компьютер или устройство, пересылающее пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором. 6:Компьютерные сети требуют установки на концах коаксиального кабеля данный элемент для поглощения "блуждающего" сигнала 7: Совокупность возможностей, способов и методов взаимодействия двух систем, устройств или программ для обмена информацией между ними, определённая их характеристиками, характеристиками соединения, сигналов обмена и т. п. 9: Топология компьютерной сети 10: Сколько уровней эталонной модели OSI? 12: Конструкция из одного или нескольких изолированных друг от друга проводников (жил), или оптических волокон, заключённых в оболочку. 13: Часть системы памяток, в которую процессор обращается при выполнении операций	2: Сетевое оборудование, предназначенное для увеличения расстояния сетевого соединения путём повторения электрического сигнала «один в один». 3: Удаленный... 4: Набор соглашений интерфейса логического уровня, которые определяют обмен данными между различными программами. 8: Сетевой анализатор трафика 10: Компьютер, специальное компьютерное оборудование или программное обеспечение, принимающее запросы от клиентов, предназначено для выполнения определенных сервисных функций. 11: Некоторое количество информации, организованное определённым способом, идущее по протоколу

Критерии оценивания

Кроссворд разгадан на:

100%- «5»

75% - «4»

60% -«3»

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ.

Контрольный тест по ПМ.01 "Проектирование сетевой инфраструктуры"

Задание #1
Вопрос:
Активные угрозы становятся видимыми на уровне (модели OSI):

Выберите один из 4 вариантов ответа:
1) канальном;
2) канальном;
3) физическом;
4) транспортном.

Задание #2
Вопрос:
Установите порядок действий при работе с беспроводным сетевым адаптером.

Укажите порядок следования всех 3 вариантов ответа:
__ подключить адаптер к компьютеру
__ настроить адаптер для динамического или ручного получения IP-адреса
__ просмотреть список доступных беспроводных сетей и подключиться к выбранной сети

Задание #3
Вопрос:
Обозначение семейства протоколов, охватывающих проблемы безопасности на IP-уровне:

Выберите один из 4 вариантов ответа:
1) FTP;
2) Ipsec.
3) UDP;
4) TCP/IP;

Задание #4
Вопрос:
_____ служит для подключения компьютера к локальной вычислительной сети (ЛВС).

Запишите ответ:
_____

Задание #5
Вопрос:
Этап проектирования, на котором создается детальный проект физической организации сети:

Выберите один из 4 вариантов ответа:
1) проектирование физической структуры;
2) проектирование инфраструктуры;
3) анализ;

4) развертывание.

Задание #6
Вопрос:
Объект сети, который могут использовать несколько пользователей одновременно:

Выберите один из 4 вариантов ответа:
1) рабочая станция;
2) сервер;
3) сетевой ресурс;
4) рабочая группа.

Задание #7
Вопрос:
Канал связи - это

Выберите один из 4 вариантов ответа:
1) средство передачи сигналов;
2) совокупность проводников.
3) путь или средство, по которому передаются сигналы;
4) это логический путь для передачи данных от одной системы к другой;

Задание #8
Вопрос:
Количество времени требуемое для передачи файла объемом 10 Мбайт при скорости модемного соединения 56000 бит/с:

Выберите один из 4 вариантов ответа:
1) около 24 минут;
2) около 26 минут;
3) около 28 минут;
4) около 30 минут.

Задание #9
Вопрос:
- это модель взаимодействия открытых систем.

Запишите ответ:
_____

Задание #10
Вопрос:
Метод CSMA/CD реализует множественный доступ:

Выберите один из 4 вариантов ответа:
1) с предотвращением коллизий;
2) с передачей полномочий;
3) с разделением по частоте.
4) с разделением по времени;

Задание #11
Вопрос:
Порядок подключения компьютера под управлением Windows XP к домену:

Укажите порядок следования всех 4 вариантов ответа:
__ Ввести имя и пароль администратора домена

__ Открыть диалоговое окно Изменение имени компьютера
__ Ввести имя домена
__ Выбрать принадлежность к домену

Задание #12
Вопрос:
Максимальное количество уникальных адресов в сети с маской подсети 255.255.255.240:

Выберите один из 4 вариантов ответа:
1) 25;
2) 30.
3) 15;
4) 20;

Задание #13
Вопрос:
OSI - это:

Выберите один из 4 вариантов ответа:
1) модель взаимодействия открытых систем;
2) сетевое программное обеспечение.
3) международная организация по стандартизации;
4) сетевая операционная система;

Задание #14
Вопрос:
Способ определения того, какая из рабочих станций сможет следующей использовать канал связи:

Выберите один из 3 вариантов ответа:
1) управление привилегиями;
2) метод доступа;
3) администрирование.

Задание #15
Вопрос:
В записи "host-a.mspu.edu.ru" узлом в поддомене mspu является _____ .

Запишите ответ:

_____

Задание #16
Вопрос:
Назначение серверной операционной системы:

Выберите один из 3 вариантов ответа:
1) все выше перечисленные.
2) управление приложениями;
3) обслуживание всех пользователей сети;

Задание #17
Вопрос:
Зону Hotspot также называют зоной:

Выберите один из 4 вариантов ответа:
1) доступа;

2) подключения.
3) работы;
4) мониторинга;

Задание #18
Вопрос:
Стандартная команда ОС Windows для отправки сообщений в локальной сети _____ .

Запишите ответ:

_____

Задание #19
Вопрос:
Модель взаимодействия открытых систем - это

Выберите один из 4 вариантов ответа:
1) модель, описывающая архитектуру построения локальной вычислительной сети.
2) модель, описывающая технологию установления соединения;
3) модель, описывающая правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи;
4) модель, описывающая методы доступа и распределения сетевых ресурсов;

Задание #20
Вопрос:
Расположите в порядке увеличения стоимости:

Укажите порядок следования всех 3 вариантов ответа:
__ Сеть на основе оптоволокна
__ Беспроводная сеть
__ Сеть на основе витой пары

Задание #21
Вопрос:
При выключении станции или ее уходе из беспроводной сети происходит _____ .

Запишите ответ:

_____

Задание #22
Вопрос:
Сетевой компьютер оснащается:

Выберите один из 4 вариантов ответа:
1) концентратором;
2) модемом;
3) коммутатором.
4) сетевым адаптером;

Задание #23
Вопрос:
С помощью сервиса _____ станция может сменить беспроводную сеть.

Запишите ответ:

_____

Задание #24
Вопрос:

Уровень модели OSI предназначенный для представления данных в нужной форме:

Выберите один из 4 вариантов ответа:
1) представительский;
2) сеансовый;
3) транспортный.
4) прикладной;

Задание #25
Вопрос:
Время требуемое для передачи 10 растровых изображений с разрешением 200x200 и битовой глубиной цвета - 32 при скорости инфракрасного соединения 115200 бит/с:

Выберите один из 4 вариантов ответа:
1) 111 с;
2) 110 с;
3) 113 с.
4) 112 с;

Задание #26
Вопрос:
Оснастка позволяющая контролировать в ОС Windows доступ к сетевым ресурсам:

Выберите один из 4 вариантов ответа:
1) шаблоны безопасности;
2) службы компонентов.
3) мониторинг IP-безопасности;
4) общие папки;

Задание #27
Вопрос:
Метод CSMA/CD реализует множественный доступ с предотвращением _____ .

Запишите ответ:

_____

Задание #28
Вопрос:
Стандартная команда ОС Windows для отправки сообщений в локальной сети:

Выберите один из 4 вариантов ответа:
1) send msg;
2) net send;
3) msg send.
4) message;

Задание #29
Вопрос:
Модель взаимодейсвия открытых систем имеет обозначение:

Выберите один из 4 вариантов ответа:
1) IOS.
2) ISO;
3) SOI;
4) OSI;

Задание #30

Вопрос:

Уровень модели OSI предназначенный для сопряжения с физическими средствами соединения:

Выберите один из 4 вариантов ответа:

1) прикладной;
2) физический;
3) транспортный.
4) представительский;

Задание #31

Вопрос:

Использование технологии кэширования позволяет:

Выберите один из 4 вариантов ответа:

1) ускорять доступ к сетевым ресурсам;
2) увеличивать скорость работы сети.
3) повышать конфиденциальность;
4) клиенту использовать ресурс в автономном режиме;

Задание #32

Вопрос:

Максимальное количество узлов в сети с маской подсети 255.255.255.240:

Выберите один из 4 вариантов ответа:

1) 20;
2) 13;
3) 25;
4) 30.

Задание #33

Вопрос:

_____ уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор маршрута наиболее быстрого и надежного пути.

Запишите ответ:

_____

Задание #34

Вопрос:

В топологии беспроводной связи точка-точка:

Выберите один из 4 вариантов ответа:

1) несколько сетевых адаптеров объединяются одной точкой доступа;
2) несколько точек доступа объединяются одним сетевым адаптером.
3) два сетевых адаптера либо две точки доступа соединяются между собой;
4) несколько сетевых адаптеров соединяются с одной точкой доступа;

Задание #35

Вопрос:

Элементы, включаемые в состав сети:

Выберите несколько из 5 вариантов ответа:

1) сетевые компьютеры;
2) каналы связи;
3) сервера;

4) сетевое оборудование.
5) преобразователи сигналов;

Задание #36
Вопрос:
Установите соответствие названия приложений выполняемым задачам:

Укажите соответствие для всех 3 вариантов ответа:
1) Стандартное приложение ОС Windows для подключения к другим компьютерам, узлам Telnet, электронным доскам объявлений, интерактивным службам или ведомому компьютеру с помощью модема, нуль-модемного кабеля
2) Приложение для доступа к удаленному рабочему столу
3) Стандартное приложение ОС Windows для доступа к удаленному рабочему столу

__ Hyper Terminal
__ Remote Desktop Connection
__ VNC

Задание #37
Вопрос:
Протокол обмена служебной информацией между точками доступа описывает спецификация стандарта IEEE 802.11:

Выберите один из 4 вариантов ответа:
1) 802.11d;
2) 802.11f/
3) 802.11c;
4) 802.11e;

Задание #38
Вопрос:
Термин _____ (Wireless Fidelity) используется в качестве общего имени для стандарта 802.11.

Запишите ответ:

_____

Задание #39
Вопрос:
SSID - это:

Выберите один из 4 вариантов ответа:
1) сетевой адрес беспроводного устройства;
2) MAC-адрес беспроводного устройства;
3) символьное имя беспроводной сети;
4) IP-адрес беспроводного устройства.

Задание #40
Вопрос:
Назначение команды subst:

Выберите один из 4 вариантов ответа:
1) управление удаленными ресурсами;
2) создание\удаление созданных ранее сетевых папок.
3) подключение локального компьютера к удаленной сети;
4) подключение удаленного ресурса в качестве локального диска;

Задание #41

Вопрос:

Установите соответствие между спецификацией стандарта и его назначением:

Укажите соответствие для всех 5 вариантов ответа:

1) работа в частотном диапазоне 5 Ггц
2) описывает протокол обмена служебной информацией между точками доступа
3) универсальные требования к физическому уровню
4) создание мультисервисных беспроводных сетей для корпораций и индивидуальных потребителей
5) работа в частотном диапазоне 2,4 Ггц

__ 802.11b
__ 802.11f
__ 802.11d
__ 802.11a
__ 802.11e

Задание #42

Вопрос:

Расположите в порядке близости к конечному пользователю:

Выберите один из 3 вариантов ответа:

1) линия связи -> канал связи -> логический канал;
2) канал связи -> логический канал -> линия связи;
3) канал связи -> линия связи -> логический канал.

Задание #43

Вопрос:

Файл, объемом 700 Мбайт, был получен из сети за 6,4 часа. Определите примерную скорость соединения (бит/с):

Выберите один из 4 вариантов ответа:

1) 350000.
2) 200000;
3) 250000;
4) 300000;

Задание #44

Вопрос:

- параметр, характеризующий загрузку сети.

Запишите ответ:

_____

Задание #45

Вопрос:

Соответствие между определением и его расшифровкой

Укажите соответствие для всех 3 вариантов ответа:

1) логический путь для передачи данных от одной системы к другой
2) путь или средство, по которому передаются сигналы
3) совокупность оборудования и физических средств связи

__ Канал связи - это
__ Линия связи - это
__ Логический канал - это

Задание #46

Вопрос:

Спецификация 802.11 ___ устанавливает универсальные требования к физическому уровню (процедуры формирования каналов, псевдослучайные последовательности частот и т.д.).

Запишите ответ:

_____

Задание #47

Вопрос:

Этап проектирования, связанный с прокладкой линий связи, установкой и настройкой оборудования:

Выберите один из 4 вариантов ответа:

1) проектирование физической структуры;
2) развертывание.
3) проектирование инфраструктуры;
4) анализ;

Задание #48

Вопрос:

- это средство, располагаемое между защищаемым внутренним сегментом сети и внешней сетью и контролирующее все информационные потоки во внутренний сегмент.

Запишите ответ:

_____

Задание #49

Вопрос:

_____ уровень обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним уровнем и непосредственно примыкает к прикладным процессам.

Запишите ответ:

_____

Задание #50

Вопрос:

- это специализированный компьютер, предоставляющий свои ресурсы в использование клиентам сети и управляющий сетью.

Запишите ответ:

_____

Ответы:

1) (1 б.) Верные ответы: 4;
2) (1 б.) Верные ответы:
   1;
   2;
   3;
3) (1 б.) Верные ответы: 2;
4) (1 б.) Верный ответ: "Сетевой адаптер".
5) (1 б.) Верные ответы: 1;
6) (1 б.) Верные ответы: 3;
7) (1 б.) Верные ответы: 3;
8) (1 б.) Верные ответы: 1;
9) (1 б.) Верный ответ: "OSI".

10) (1 б.) Верные ответы: 1;
11) (1 б.) Верные ответы:
4;
1;
3;
2;
12) (1 б.) Верные ответы: 3;
13) (1 б.) Верные ответы: 1;
14) (1 б.) Верные ответы: 2;
15) (1 б.) Верный ответ: "host-a".
16) (1 б.) Верные ответы: 1;
17) (1 б.) Верные ответы: 2;
18) (1 б.) Верный ответ: "net send".
19) (1 б.) Верные ответы: 3;
20) (1 б.) Верные ответы:
1;
3;
2;
21) (1 б.) Верный ответ: "дизассоциация".
22) (1 б.) Верные ответы: 4;
23) (1 б.) Верный ответ: "реассоциация".
24) (1 б.) Верные ответы: 1;
25) (1 б.) Верные ответы: 2;
26) (1 б.) Верные ответы: 4;
27) (1 б.) Верный ответ: "коллизий".
28) (1 б.) Верные ответы: 2;
29) (1 б.) Верные ответы: 4;
30) (1 б.) Верные ответы: 2;
31) (1 б.) Верные ответы: 1;
32) (1 б.) Верные ответы: 2;
33) (1 б.) Верный ответ: "Сетевой".
34) (1 б.) Верные ответы: 3;
35) (1 б.) Верные ответы: 1; 2; 4; 5;
36) (1 б.) Верные ответы:
1;
3;
2;
37) (1 б.) Верные ответы: 2;
38) (1 б.) Верный ответ: "Wi-Fi".
39) (1 б.) Верные ответы: 3;
40) (1 б.) Верные ответы: 4;
41) (1 б.) Верные ответы:
5;
2;
3;
1;
4;
42) (1 б.) Верные ответы: 1;
43) (1 б.) Верные ответы: 3;
44) (1 б.) Верный ответ: "Трафик".
45) (1 б.) Верные ответы:
2;
3;
1;

46) (1 б.) Верный ответ: "d".
47) (1 б.) Верные ответы: 2;
48) (1 б.) Верный ответ: "Брандмауэр".
49) (1 б.) Верный ответ: "Прикладной".
50) (1 б.) Верный ответ: "Сервер".

Конец

Критерии оценивания