БПОУ ВО «Грязовецкий политехнический техникум»

Рассмотрен

цикловой комиссией по общепрофессиональным дисциплинам и профессиональным модулям отделения «Электрификация и автоматизация сельского хозяйства»

Согласовано

зам. директора по ОМР
_____ Е. А. Ткаченко
«30» августа 2017 г.

Протокол № 1 от «30» августа 2017 г.

Председатель комиссии:
_____ Т. В. Невзорова

ПРАКТИЧЕСКИЕ (ЛАБОРАТОРНЫЕ) РАБОТЫ

ПМ.01. Участие в проектировании сетевой инфраструктуры

Специальность 09.02.02. Компьютерные сети

Грязовец
2017 г.

Лабораторные работы цикла МДК.01.01

Лабораторная работа № 1.

Настройка протоколов TCP/IP.

Цель занятия: Дать представление о семействе протоколов TCP/IP, его назначении, составе и настройке. Осуществить необходимые действия по настройке параметров сетевого окружения Windows для простейшего случая одноранговой сети.

Основные понятия:;

Используемые средства: Microsoft Virtual PC 2007. Две виртуальные машины с установленными Windows XP.

Теоретические сведения:

Семейство протоколов TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/межсетевой протокол) является стандартным семейством протоколов, предназначенным для больших объединенных сетей как локального, так и глобального масштаба.

Протоколы TCP/IP реализованы во множестве программ для работы с TCP/IP, доступных на многих компьютерных платформах. Сегодня программное обеспечение, поддерживающее TCP/IP, широко используется в Интернете и часто применяется для построения крупных частных объединенных сетей с маршрутизацией.

Основные протоколы семейства TCP/IP

•Протокол ARP (Address Resolution Protocol)

ARP разрешает IP-адреса,используемые программным обеспечением TCP/IP, в аппаратные адреса сетевых адаптеров локальной сети. ARP предоставляет узлам, расположенным в одной физической сети, следующие службы протокола: аппаратные адреса (илиMAC-адреса— адреса уровня управления доступом к среде передачи); когда наARP-запросотправляется ответ, то отправительARP-ответаи запрашивающий узел заносятIP-адресаи

аппаратные адреса друг друга в локальную таблицу, называемую кэшем ARP, для дальнейшего использования.

Пример: Для управления ARP в ОС Windows используется команда arp.exe. Ниже приведен пример содержимогоARP-кэшакомпьютера в локальной сети:

```
C:\arp.exe-a
Interface: 192.168.75.103 ---0x10004
Internet    AddressPhysical Address    Type
192.168.75.100    00-c1-28-01-94-85dynamic
192.168.75.104    00-07-95-09-2c-70dynamic
192.168.75.253    00-50-bf-7c-7f-02  dynamic
192.168.75.254    00-e0-18-3b-a3-d7dynamic
```

Маслов Алексей Сергеевич

Подписано цифровой подписью: Маслов Алексей Сергеевич
DN: 1.2.643.3.131.1.1=120C333530393030333234373532, 1.2.643.100.3=120B303635383138343232383 5, email=grtexn@mail.ru, c=RU, st=Вологодская область, l=г Грязовец, o=БПОУ ВО "Грязовецкий политехнический техникум", givenName=Алексей Сергеевич, sn=Маслов, cn=Маслов Алексей Сергеевич
Дата: 2017.05.13 20:06:23 +03'00'

•Протокол IP (Internet Protocol)

Межсетевой протокол IP (Internet Protocol) — это не ориентированный на установление соединения и ненадежный протокол передачи датаграмм, ответственный, главным образом, за адресацию и маршрутизацию пакетов между узлами.

Термин «не ориентированный на установление соединения» означает, что сеанс для обмена данными не устанавливается. Термин «ненадежный» означает, что доставка не гарантируется. IP всегда предпринимает все усилия, чтобы доставить пакет. IP-пакетможет быть потерян, доставлен вне очереди, дублирован или задержан. Протокол IP не пытается исправить ошибки этих типов. Подтверждение получения пакетов и повторное обращение за потерянными пакетами входят в круг обязанностей протокола более высокого уровня, например TCP.

•Протокол ICMP (Internet Control Message Protocol)

Протокол межсетевых управляющих сообщений. Используя ICMP, узлы и маршрутизаторы, связывающиеся по протоколу IP, могут сообщать об ошибках и обмениваться ограниченной управляющей информацией и сведениями о состоянии. ICMP-сообщенияобычно автоматически отправляются в следующих случаях:

-IP-датаграммане может попасть к узлу назначения.

-IP-маршрутизатор(шлюз) не может перенаправлять датаграммы с текущей скоростью передачи.

-IP-маршрутизаторперенаправляетузел-отправительна другой, более

выгодный маршрут к узлу назначения.

ICMP-сообщенияинкапсулируются и передаются вIP-датаграммах

•Протокол IGMP (Internet Group Management Protocol)

IGMP предоставляют протокол обмена и обновления информации об участии узлов в отдельных группах многоадресной рассылки. Многоадресный IP-трафикнаправляется по одному адресу, но обрабатывается несколькими узлами. Набор узлов, принимающих трафик с даннымIP-адресоммногоадресной рассылки, называется группой многоадресной рассылки.

IP-адресадля многоадресной рассылки зарезервированы и назначаются из диапазона адресов класса D (см. ниже): с 224.0.0.0 по 239.255.255.255.

•Протокол UDP (User Datagram Protocol)

UDP используется некоторыми программами вместо TCP для быстрой, простой и ненадежной (главное отличие от TCP) передачи данных между узлами TCP/IP.

UDP обеспечивает службу датаграмм, не ориентированную на установление соединения, что означает, что UDP не гарантирует ни доставку, ни правильность порядка доставки датаграмм. Узел-источник,которому требуется надежная связь, должен использовать либо протокол TCP, либо программу, которая сама обеспечивает подтверждения и следит за правильностью порядка датаграмм.

UDP-сообщенияинкапсулируются и передаются вIP-датаграммах

•Протокол TCP (Transmission Control Protocol)

Предоставляет надежную и ориентированную на установление соединения службу доставки пакетов. Протокол TCP:

-гарантирует доставку IP-датаграмм;

-выполняет разбиение на сегменты и сборку больших блоков данных, отправляемых программами;

-обеспечивает доставку сегментов данных в нужном порядке;

-выполняет проверку целостности переданных данных с помощью контрольной суммы;

-посылает положительные подтверждения, если данные получены успешно. Используя избирательные подтверждения, можно также посылать отрицательные подтверждения для данных, которые не были получены;

-предлагает предпочтительный транспорт для программ, которым требуется надежная передача данных с установлением сеанса связи, например для баз данных «клиент-сервер»и программ электронной

почты.

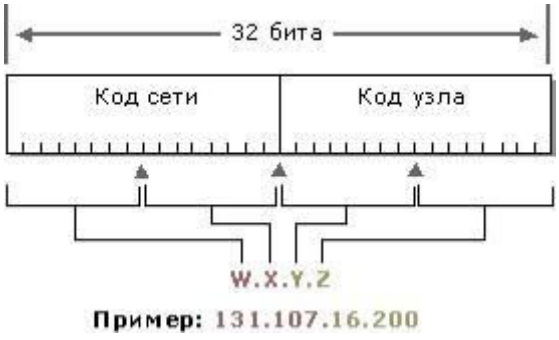
TCP основан на связи точка-точкамежду двумя узлами сети. TCP получает данные от программ и обрабатывает их как поток байтов. Байты группируются в сегменты, которым TCP дает последовательные номера, необходимые для правильной сборки сегментов наузле-приемнике.

TCP-сегментыинкапсулируются и передаются вIP-датаграммах.

Для обмена данными по протоколу TCP программы используют порты TCP. Каждый отдельный серверный порт TCP может совместно использоваться несколькими соединениями, так как все TCP-соединения

уникально идентифицируются двумя парами IP-адресови портов TCP

(по одной паре адрес/порт для каждого узла). Программы TCP используют зарезервированные или хорошо известные номера портов. Серверная часть каждой программы, использующей порты TCP, прослушивает определенный порт в ожидании поступающих на него сообщений. Все номера серверных портов TCP, меньшие 1024 (а также некоторые большие номера), зарезервированы.



Параметры конфигурации TCP/IP

Для правильной работы протокола TCP/IP в Windows необходимо настроить следующие параметры:

•IP-адрес

Каждому сетевому интерфейсу на каждом устройстве TCP/IP (узле или маршрутизаторе) должен быть назначен уникальный IP-адрес,принадлежащий данному сегменту сети.IP-адресявляется необходимым элементом конфигурации.

IP-адресимеет две части — код (идентификатор) сети и код (идентификатор) узла.

-Код сети, также называемый адресом сети, обозначает один сетевой сегмент в более крупной объединенной сети (сети сетей), использующей протокол TCP/IP. IP-адресавсех систем, подключенных к одной сети, имеют один и тот же код сети. Этот код также используется для уникального обозначения каждой сети в более крупной объединенной сети.

-Код узла, также называемый адресом узла, идентифицирует узел TCP/IP (рабочую станцию, сервер, маршрутизатор или другое TCP/IPустройство) в пределах одной сети. Код узла уникальным образом

обозначает систему в том сегменте сети, к которой она подключена.

Вот пример 32-битногоIP-адреса:10000011 01101011 00010000 11001000

Для облегчения восприятия человеком IP-адресазаписываются вточечно-десятичнойнотации.32-битныйIP-адресделится на четыре 8- битных октета. Октеты представляются в десятичной системе счисления и разделяются точками. Таким образом вышеприведенныйIP-адресв точечнодесятичной нотации выглядит так:

131.107.16.200.

На рисунке 4 показан пример IPадреса (131.107.16.200), разделенного

Рисунок 4 – Пример IP-адреса

на код сети и код узла. Часть, соответствующая коду сети (131.107), в данном случае определяется первыми двумя октетами IP-адреса.Часть, задающая код узла (16.200), обозначается последними двумя октетамиIP-адреса.

Сообщество Интернета определило пять классов IP-адресов.Адреса классов A, B и C могут назначаться узлам TCP/IP.

Класс адреса задает число бит в адресе, которые отводятся под коды сети и узла. Тем самым, класс адреса определяет и то, сколько всего может быть сетей данного класса и узлов в каждой из этих сетей и где в IP адресе проходит граница между кодом сети и номером узла.

В следующей таблице символы w.x.y.z обозначают четыре октета IPадреса. Эта таблица показывает:

-как значение первого октета (w) любого IP-адресазадает класс этого адреса;

-как октеты адреса данного класса делятся на код сети и код узла;

-число возможных сетей данного класса и число узлов в этих сетях.

Класс	Значение w	Код сети	Код узла	Число сетей	Число узлов в сети.
A	1–126	w	x.y.z	126	16 777 214
B	128–191	w.x	y.z	16 384	65 534
C	192–223	w.x.y	z	2 097 152	254
D	224–239	Зарезервировано для многоадресной рассылки	Неприменимо	Неприменимо	Неприменимо
E	240–254	Зарезервировано для экспериментальных целей	Неприменимо	Неприменимо	Неприменимо

Пример: Каким образом определяется число сетей и число узлов в вышеприведенной таблице? Рассмотрим класс С. Как видно из таблицы, код сети состоит из трех октетов – 24 бита. Надо, однако учесть, что из первого октета используется лишь 5 бит (т.к. значение w лежит между 192 и 223, то есть224-192=32=25).Таким образом число сетей составит224-(8-5)

= 221 = 2097152

Выбор сетевых адресов

Для частных TCP/IP-сетей,которые никак не подключены к Интернету, можно использовать любой допустимый диапазонIP-адресовклассов A, B или C.

Для частных TCP/IP-сетей,которые подключены к Интернету не напрямую, а с помощью преобразователя сетевых адресов (NAT) или шлюза уровня приложения, напримерпрокси-сервера,рекомендуется использовать частныеIP-адреса,приведенные в следующей таблице.

Идентификатор частной сети	Маска подсети	Диапазон IP-адресов
10.0.0.0	255.0.0.0	10.0.0.1 – 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 – 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 – 192.168.255.254

Эти диапазоны адресов зарезервированы для частных TCP/IP-сетейи не используются в Интернете.

•Маска подсети

Для каждого сетевого интерфейса на каждом устройстве TCP/IP (узле или маршрутизаторе) должна быть задана маска подсети, которая, будучи наложенной на IP-адрес,позволяет определить код (идентификатор) сети. ВсеIP-интерфейсыв одном сегменте сети должны использовать один и тот же код сети. Следовательно, всеIP-интерфейсыв одном сегменте сети должны иметь одну и ту же маску подсети. Маска подсети является необходимым элементом конфигурации.

Коды сетей и коды узлов в IP-адресеможно различить с помощью маски подсети. Каждая маска подсети представляет собой32-битноечисло, состоящее из последовательной группы единичных битов для выделения изIP-адресакода сети, и последовательной группы нулевых битов для выделения кода узла.

Например, вот маска подсети, которая обычно используется с IP-

адресом 131.107.16.200 из примера выше: 11111111 11111111 00000000 00000000

Эта маска подсети состоит из 16 единичных битов, за которыми следуют 16 нулевых битов, что означает, что части этого IP-адреса,соответствующие коду сети и коду узла, имеют одинаковую длину в 16 бит. Вточечно-десятичнойнотации эта маска будет иметь следующий вид: 255.255.0.0.

В следующей таблице показаны маски подсети для классов адресов Интернета.

Класс адреса	Биты маски подсети	Маска подсети
Класс A	11111111 00000000 00000000 00000000	255.0.0.0
Класс B	11111111 11111111 00000000 00000000	255.255.0.0
Класс C	11111111 11111111 11111111 00000000	255.255.255.0

Часто используются специальные маски подсети для деления сети на IP-подсети.Деление сети наIP-подсетипозволяет разделить стандартную частьIP-адреса,соответствующую коду узла, на подсети, которые являются подразделами исходного кода сети, основанного на классе.

Изменяя длину частей маски подсети, можно уменьшить число битов, используемых для кода узла. Во избежание неполадок с адресацией и маршрутизацией все компьютеры TCP/IP в одном сегменте сети должны использовать одну и ту же маску подсети.

Очень часто комбинация из IP-адресаи маски подсети записываются в виде:<IP-адрес>/<число_единичных_бит_маски_подсети>

Пример: Запись вида 192.168.10.15/24 означает адрес 192.168.10.15 и маску подсети 255.255.255.0

Часть IP-адреса,покрываемая единичными битами маски подсети называют ещесетевым префиксом.

Задача. Предположим, что организации для ее корпоративной сети назначен сетевой номер 140.25.0.0/16. При этом организация планирует разделить сеть на несколько подсетей, каждая из которых должна поддерживать до 60 устройств. Необходимо определить количество подсетей, их номера и адреса устройств.

Решение. На первом шаге необходимо определить число битов, требуемых для идентификации 60 устройств в подсети. Адрес конкретного устройства имеет определенное двоичное представление и верхняя граница адресного пространства для устройств одной подсети представляется степенью двойки. Это, в частности, означает, что невозможно выделить адресное пространство ровно для 60 устройств, так как 60 - не степень двойки. Ближайшая сверху степень - это 64 = 26. На самом деле, к числу устройств нужно прибавить 2, так как адреса, содержащие только нули или только единицы, не используются для адресации отдельных устройств. Здесь мы видим, что необходимый задел есть: 60+2=62<64. Однако, удовлетворяя существующие на сегодня потребности по числу рабочих мест, такой выбор не оставляет адресного пространства для возможного роста подсети (в наличии имеется всего 2 свободных адреса). И хотя следующая степень двойки равна 128 (27) и число адресов устройств будет равно27-2=126,то есть намного больше требуемого в настоящий момент, лучше будет выбрать именно это адресное пространство и получить 66(126-60)дополнительных адресов для каждой подсети. Такой выбор означает, что поле адреса устройства займет 7 бит.

На втором шаге определяется маска подсети и длина расширенного сетевого префикса. Так как для идентификации устройств из 32-разрядногоIP-адресарешено выделить 7 бит, то получаем расширенный сетевой префикс равный /25(32-7=25).Такой25-

разрядныйрасширенный сетевой префикс может быть выражен вдесятично-точечномпредставлении маской подсети 255.255.255.128. В следующей таблице показана запись маски подсети и расширенного сетевого префикса.

	Сетевой префикс	Номерподсети	Номер устройства
140.25.0.0/16	10001100. 00011001.	00000000.0	0000000
255.255.255.111111111.	11111111.	11111111.1	0000000

Или эквивалентная запись

	25-битовыйрасширенный сетевой префикс		Номер устройства
140.25.0.0/25	10001100. 00011001.	00000000.0	0000000

Мы видим, что 25-разрядныйрасширенный префикс предполагает выделение 9 бит (25 – 16) для идентификации подсетей. Теперь можно вычислить количество идентифицируемых подсетей: 29=512, то есть девять битов позволяют назначить адреса 512 подсетям. Понятно, что сетевой администратор имеет некоторую свободу действий при определении соотношения числа идентифицируемых устройств и числа подсетей. Выделяя большее число бит в поле идентификации устройств, администратор может включать в подсеть больше устройств. С другой стороны, чем меньше бит выделено для идентификации устройств, тем больше подсетей может создать администратор. Все зависит от текущих требований организации.

Определение номеров подсетей

Выделенные 512 подсетей пронумеруем от 0 до 511. Если выделить 9 разрядов для двоичного представления десятичных чисел от 0 до 511, то получим: 0(000000000)2, 1(000000001)2, 2(000000010)2, 3(000000011)2, ..., 511(111111111)2. Например, для определения подсети номер 3 (#3) сетевой администратор размещает двоичное представление числа 3 (000000011)2 в 9 битах номера подсети. Номера подсетей для рассматриваемого примера приводятся ниже. В каждом адресе курсивом выделен расширенный сетевой префикс всего адреса, в то время как9-битовоепредставление поля номера

подсети выделено полужирным шрифтом.

Базовая сеть: 10001100.00011001.00000000.00000000 = 140.25.0.0/16

Подсеть #0: 10001100.00011001.00000000.00000000 = 140.25.0.0/25

Подсеть #1: 10001100.00011001.00000000.10000000 = 140.25.0.128/25

Подсеть #2: 10001100.00011001.00000001.00000000 = 140.25.1.0/25

Подсеть #3: 10001100.00011001.00000001.10000000 = 140.25.1.128/25

Подсеть #4: 10001100.00011001.00000010.00000000= 140.25.2.0/25

Подсеть #5: 10001100.00011001.00000010.10000000= 140.25.2.128/25

Подсеть #6: 10001100.00011001.00000011.00000000= 140.25.3.0/25

……

Подсеть #510: 10001100.00011001.11111111.00000000=140.25.255.0/25

Подсеть #511: 10001100.00011001.11111111.10000000=140.25.255.128/25

Определение адресов устройств

Итак, администратор выделил 7 битов для идентификации устройств в каждой подсети. Это означает, что каждая подсеть имеет 126 (27-2)адресов для идентификации устройств. Устройства в подсети нумеруются от 1 до 126. Приведем перечень адресов устройств для подсети #3. При этом курсивом выделен расширенный сетевой префикс, в то время как полужирным шрифтом показано7-разрядноеполе номера устройства.

Подсеть #3: 10001100.00011001.00000001.10000000 = 140.25.1.128/25 Устройство #1:10001100.00011001.00000001.10000001 =

140.25.1.129/25

Устройство #2: 10001100.00011001.00000001.10000010 = 140.25.1.130/25

Устройство #3: 10001100.00011001.00000001.10000011 = 140.25.1.131/25

Устройство #4: 10001100.00011001.00000001.10000100 = 140.25.1.132/25

Устройство #5: 10001100.00011001.00000001.10000101 = 140.25.1.133/25

Устройство #6:10001100.00011001.00000001.10000110= 140.25.1.134/25
……
Устройство #125:10001100.00011001.00000001.11111101 = 140.25.1.253/25
Устройство #126:10001100.00011001.00000001.11111110 = 140.25.1.254/25

Определение широковещательного адреса

Для подсети #3 широковещательным адресом будет адрес, в котором все биты поля номера устройства установлены в единицу:

10001100.00011001.00000001.11111111 = 140.25.1.255.

Следует отметить, что широковещательный адрес для подсети #3 ровно на единицу меньше базового адреса подсети #4 (140.25.2.0).

Автоматическая настройка TCP/IP в Windows

Windows обеспечивает автоматическое выделение IP-адресовиз зарезервированного диапазона 169.254.0.1 — 169.254.255.254 с маской подсети 255.255.0.0. Автоматическая настройка адресов основного шлюза,DNS-сервераиWINS-серверане выполняется и предназначена для сетей, состоящих из одного сегмента и не подключенных к Интернету. Следовательно, указывать адреса основного шлюза,DNS-сервераи WINSсервера не нужно.

Ручная настройка

При ручной настройке свойств протокола TCP/IP в окне свойств сетевого окружения задаются IP-адрес,маска подсети и адреса основного шлюза,DNS-сервераиWINS-сервера.Ручная настройка необходима в сетях, состоящих из нескольких сегментов и не имеющихDHCP-сервера.

Практические задания:

1.Создать виртуальную машину. Установить Windows XP.

2.Загрузиться в Windows.

3.Произвести ручную настройку TCP/IP:

а) Открыть Панель управления->Сетевыеподключения. Нажать правую кнопку мыши на подключения по локальной сети. Выбрать Свойства.

б) На вкладке «Общие» выберите Протокол Интернета (TCP/IP) и нажмите кнопку Свойства.

в) Выберите переключатель «Используйте следующий IP-адрес»и ведите необходимые данные в поляIP-адрес,и маска подсети:

─IP-адрес:172.22.7.2 xx, где xx – номер рабочего места;

─Маска: 255.255.0.0;

─Основной шлюз: 172.22.0.1 ;

─Предпочитаемый DNS-сервер:172.22.0.1.

5.Проверить работоспособность путем подключения к серверу лаборатории 2-04.

Контрольные вопросы:

1.Если компьютер отключить из локальной сети, а вместо него поместить другой компьютер с такими же сетевыми настройками (имя, IPадрес и т.п.), смогут ли остальные компьютеры сети обращаться к этому компьютеру? Через какое время?

2.Гарантируется ли надежная доставка ICMP-сообщений?Почему?

3.Могут ли одновременно приходить разные запросы на один и тот же TCP порт компьютера?

4.Может ли у компьютера одновременно быть больше, чем один IP-

адрес?

5.Какую маску подсети следует применять с IP-адресом

192.168.75.100: 255.255.255.0 или 255.255.0.0?

6.Можно ли в частной локальной сети использовать в качестве IP адреса узла адрес 192.169.175.23?

7.Какие параметры TCP/IP протокола необходимо настроить в ОС (напр. Windows98) чтобы получить работоспособную сетевую станцию?

8.Можно ли при настройке TCP/IP протокола указать IP адрес, а поле «маска подсети» оставить пустым?

9.К какому классу IP адресов принадлежит адрес, присваиваемый ОС Windows компьютеру при автоматической настройке TCP/IP протокола

(DHCP нет)?

Задачи:

1.Какие из приведенных ниже масок подсети являются корректными и некорректными и почему?

А) 255.255.149.0 Б) 255.255.255.192 В) 149.255.255.0 Г) 255.255.255.255

2.Сколько компьютеров в сетевом сегменте позволяет иметь маска

255.255.255.240?

3.Пусть организации назначен сетевой адрес 200.35.1.0/24. В каждой подсети необходимо предусмотреть адресное пространство для 20 устройств. Определить расширенный сетевой префикс, максимальное количество узлов

вкаждой подсети и максимальное количество подсетей, которые могут быть сформированы в этом пространстве с таким расширенным сетевым префиксом. Определить широковещательный адрес для одной из подсетей.

4.Пусть IP-адреснекоторого узла подсети равен 198.65.12.67, а значение маски для этой подсети – 255.255.255.240. Определите номер подсети. Какое максимально количество узлов может быть в этой подсети?

5.Пусть поставщик услуг Интернет имеет в своем распоряжении адрес сети класса B. Для адресации узлов своей собственной сети он использует 254 адреса. Определите максимально возможное число абонентов этого

поставщика услуг, если размеры требуемых для них сетей соответствуют классу C.

6.Какие из перечисленных ниже адресов не могут быть использованы

вкачестве IP-адресаконечного узла сети, подключенной к Интернет? Для правильных адресов определите их класс: A, B, C, D или E.

127.0.0.1 201.13.123.245
226.4.37.105 103.24.254.0
154.12.255.255
13.13.13.13 204.0.3.1
193.256.1.16 194.87.45.0
161.23.45.305 195.34.116.255

Лабораторная работа № 2

«Использование протоколов telnet при работе в Интернет»

Цель работы

Ознакомиться с доступом к информации в сети Internet посредством протокола **telnet.** Получить навыки проверки соединений в сети Internet.

Подготовка к работе

Ознакомиться *с* **telnet,** форматом команд **ping, tracert.**

Содержание работы

1. Определить возможность установления соединения вашего компьютера с другим компьютером в локальной или глобальной сети, используя команду *ping*.

3. Используя команды cd и Is найти любой не очень большой файл.

4. Убедиться, что файлы успешно скопированы.

5. Проследить путь следования IP-пакета от компьютера локальной сети к какому-либо удаленному серверу используя команду **tracert.exe.** Записать весь путь в отчет.

6. Оформить отчет, (используя Word или даже Notepad)

Содержание отчета

Отчет должен содержать:

1. Цель работы

2. Результат проверки соединений с серверами.

3. Адрес удаленного сервера, путь к файлу, имя файла, скопированного на локальный сервер с помощью текстового ftp-клиента, время и скорость передачи файла.

4. Весь путь следования IP-пакета до удаленного сервера.

5. Выводы

Выполнение работы

1. Для запуска программы в среде Windows NT/9x выполните следующие действия:

- нажмите левой кнопкой мыши на кнопке **Пуск.**

- выберите пункт **«Выполнить»** и нажмите левую кнопку мыши

- в появившемся окне в поле **«Открыть»** введите имя выполняемой программы (можно также указать исполняемый файл с помощью кнопки **«Обзор»).**

- Нажав «Enter» запустите программу на исполнение.

2. Для проверки наличия и качества сетевого соединения с удаленной системой используется команда Ping.

Эта утилита (команда) отсылает запрос (несколько байт) на требуемый компьютер и ожидает ответа, определяя при этом время следования запроса и ответа.

Формат этой команды следующий:

ping [-t] [-a] [-n count] [-1 size] [-f] [-w timeout] список адресов

Параметры:

-t Отправка пакетов на указанный узел до команды

прерывания

-a Определение адресов по именам узлов.

-n count Количество запросов

-1 size Размер посылаемого пакета

-f Установка флага, запрещающего фрагментацию пакета.

-w timeout Время таймаута в миллисекундах.

После запуска программы на экране будет показываться время установки связи с заданным компьютером, если связь отсутствует и/или превышено заданное время таймаута, то в окне будет возникать сообщение «Request timeout» или «Destination host unreachable».

4. Чтобы проследить путь следования IP-пакета к удаленному серверу используется программа **tracert.exe.** Формат её вызова:

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

Параметры:

-d Без определения адресов по именам узлов.

-h максЧисло Максимальное число переходов при поиске узла.

-j сиисокУзлов Свободный выбор маршрута по списку узлов.

-w интервал Интервал ожидания каждого ответа в мсек.

После запуска данная программа в соответствии с заданными параметрами осуществляет посылку IP-пакета на компьютер-цель и выводит имена всех других компьютеров, находящихся между вами и заданным компьютером.

Протокол Telnet

Протокол **Telnet** (от слов telecommunication network телекоммуникационная сеть) обеспечивает возможность входа в удаленную систему. Он позволяет пользователю одного компьютера зарегистрироваться на удаленном компьютере, расположенном в другой части

сети. При этом пользователю кажется, что он работает за терминалом удаленного компьютера. **Telnet** может оказаться полезным, если вы, работая на медленном компьютере, хотите воспользоваться вычислительными ресурсами более мощной машины, а также если на удаленном компьютере имеется необходимое вам программное обеспечение.

Работу **Telnet** обеспечивает специальная программа (сервер), запущенная на компьютере, к которому вы подключаетесь, и обрабатывающая поступающие запросы. На вашем компьютере выполняется программа **Telnet,** которая обращается к серверу. В процессе установления соединения компьютеры договариваются о режиме эмуляции терминала в данном сеансе работы.

Для начала сеанса работы **Telnet** необходимо ввести доменное имя или IP-адрес удаленного компьютера. После установления соединения удаленная система обычно запрашивает имя пользователя и пароль, хотя это зависит от типа операционной системы и программного обеспечения **Telnet,** установленных на удаленном компьютере.

После установления соединения ваш компьютер играет роль терминала удаленной машины. Все вводимые вами команды выполняются на удаленном компьютере. **Telnet** лишь осуществляет обработку и передачу ваших команд на удаленный компьютер. **Telnet** автоматически заканчивает свою работу, когда вы выходите из удаленной системы.

Для завершения сеанса работы следует ввести соответствующую команду (для UNIX-систем — обычно **logout** или **<Ctrl>+<D>)**

Как закрыть сеанс связи с удаленным компьютером

Если вы работаете с **Telnet** из командной строки, то **Telnet** обычно сам завершает работу, когда вы выходите **(logout)** из удаленной системы. Однако иногда (например, когда удаленный компьютер "зависает") возникает необходимость принудительно закрыть сеанс связи путем выполнения команды на локальном компьютере. Для этого следует нажать <Ctrl>-<]>, чтобы перейти в командный режим **Telnet,** а затем ввести команду close, которая разорвет соединение с удаленным компьютером и завершит работу Telnet-клиента.

Ограничение по времени на простой системы

После того, как вы зарегистрировались для работы на удаленном компьютере, он начинает следить за вашей активностью в системе. Делается это по следующей причине. Клиент, получающий Telnet-доступ к

удаленному компьютеру, занимает часть его ресурсов. Поэтому системные администраторы для того, чтобы гарантировать максимально возможную доступность своей компьютерной системы и оптимальный режим ее работы, вводят ограничения на допустимое время простоя в **Telnet-сеансе.** То есть, если вы, зарегистрировавшись для работы на удаленном компьютере, в течение некоторого времени (как правило, около 15 минут) не производите никаких действий (ничего не вводите с клавиатуры), удаленный компьютер может прервать вашу рабочую сессию, и вам придется повторить процесс установления соединения.

cd [удаленная_директория|

Сменить директорию. Существуют также **'cdup'** или **'cd'** для возврата на один или выше

close

Обрывает PTP сеанс с удаленным сервером и возвращает к командному интерпретатору

delete (удаленный файл)

Стирает удаленный файл

dir [удаленная директория] [локальный_файл]

Is [удаленная директории] [локальный файл]

Выводит список файлов в директории либо не стандартный вывод, либо, если указано имя локального файла, в этот файл, (**dir** -вывод с дополнительной информацией).

get [удаленный_файл] [локальный_файл]

Вызывает передачу копии удаленного файла на ваш компьютер. В случае, если имя локального файла не было задано, то оно совпадает с именем удаленного файла.

hash

Служит переключателем для индикации каждого полученного блока данных в 1024 байта, повышает наглядность процедуры.

lcd

Меняет рабочую директорию на локальной машине (без аргумента - переход в домашнюю директорию пользователя)

mget [удаленные_файлы]

Для получения нескольких файлов

mkdir [имя директории]

Создает директорию на удаленной машине

open хост [порт]

Устанавливает соединение с заданным FTP сервером

prompt

Переключает интерактивную подсказку. Часто при использовании команды **'mget'** желательно предварительно набрать **'prompt',** чтобы не давать многократные подтверждения.

put [локальный файл) [удаленный файл]

Пересылает файл на удаленную систему. Если имя удаленного файла не указано, то оно совпадает с именем на локальной системе.

pwd

Выводит имя удаленной рабочей директории.

Quit

Синоним для 'b**ye'**

recv [удаленный файл] [локальный файл]

Синоним для команды 'get'

reget [удаленный_файл] [локальный файл]

"Дополучение" удаленного файла в том случае, когда часть его уже есть на локальной машине. Команда особенно полезна для получения больших файлов при возможных разрывах соединения, (поддерживается не всеми серверами и клиентами).

При большом количестве файлов перебор их имен - утомительная задача. Порой трудно перечислить 5-6 файлов, а если их сотня?

Выход есть. Существует система шаблонов, которую лучше всего изучать на примерах. Перед этим объяснение специальных знаков:

Символ '*****' обозначает любой набор символов.

Символ "?' обозначает один любой символ.

Примеры:

abc* - все файлы, начинающиеся на **abc**

abc? - все файлы, имеющие длину имени в четыре символа, начинающиеся на abc и заканчивающиеся на любой символ.

??abc? - файлы с именем в шесть символов, 3,4,5 символы abc и остальные любые.

*abc - все файлы, оканчивающиеся на **abc**

* - все файлы

Учтите, что большие и маленькие буквы РаЗлИчАюТсЯ.

Необходимо знать, что в распечатке команды **Is** первые десять знаков (например: **-rwxrwxrwx)** - это биты доступа к файлу или директории. Для вас

представляет интерес только первый символ. Если это '-', то он обозначает файл, если 'd' - то директорию.

Так например в строке:

-rw-r--r-users 11479 Janfilename.ext

«-rw-r--r--» - атрибут файла; **«filename.ext»** - имя файла; **«11479»** - размер файла; **«Jan»** - дата создания файла.

Контрольные вопросы

1. Где выполняются все команды во время **telnet** - соединения?

2. Для чего в первую очередь предназначена возможность организации терминальных соединений с сервером?

3. Расскажите порядок установления **telnet** - соединения с удаленным сервером.

4. Объясните назначение и формат команды **ping?**

5. Объясните назначение панелей и окон в основном окне **FlashFXP**.

6. Что такое «удаленный каталог», «удаленная машина»?

7. Как можно просмотреть файл, расположенный на удаленной машине?

8. Перечислите преимущества работы с **FlashFXP.**

9. Для чего компьютеру необходим IP - адрес?

16. Что позволяет узнать утилита **tracert?**

Лабораторная работа №3.,4 "Дистанционное управление компьютером"

1. Цель лабораторной работы

Одной из основных задач в практическом использование ЛВС является оперативная поддержка функционирования отдельных компьютеров сети и работы пользователей на этих компьютерах. Однако, довольно часто случаются ситуации, когда у пользователей возникают разного рода проблемы и им требуется техническая поддержка.

При этом, далеко не всегда тот, кто может помочь пользователю, присутствует рядом с ним, готовый дать совет или показать необходимые действия для решения тех или иных задач. Тем более, что для разрешения некоторых проблем технический специалист должен видеть, какие действия приводят к неадекватному, по мнению пользователя, поведению программ.

Находится постоянно «за спиной пользователя» вряд ли кому понравится, да это и не невозможно по разным причинам. В этих условиях производители ПО просто не могли обойти вниманием столь важный вопрос как удаленное администрирование узлов сети и оказание удаленной помощи ее пользователям. Знакомству именно с такими программными инструментами, встроенными в составе Windows XP, и посвящена данная лабораторная работа.

Целью данной лабораторной работы является

- Знакомство с настройкой и использованием удаленного рабочего стола (Remote Desktop).
- Получение сведений о реализации технологии удаленного помощника (Remote Assistance).
- Изучение технологии добровольной удаленной помощи.

Замечание:
В этом описание приводятся только общие подходы и инструкции по выполнению лабораторной работы . Для подробного знакомства с назначением, работой и командами используемых утилит Windows используйте встроенную справку (Пуск -> Справка и поддержка -> Найти <интересующий вас раздел> -> Начать поиск)

2. Организация дистанционное управление узлами ЛВС

Исходным состоянием для выполнения данной лабораторной работы является использование двух виртуальных машин на одном хостовом компьютере, с возможностью доступа к виртуальной сети виртуальных машин всей лаборатории (рис.5.1).

На первом этапе выполнения работы все основные настройки и манипуляции будут выполняться внутри виртуальной сети основного компьютера, поэтому необходимо, прежде всего убедиться в ее работоспособности.

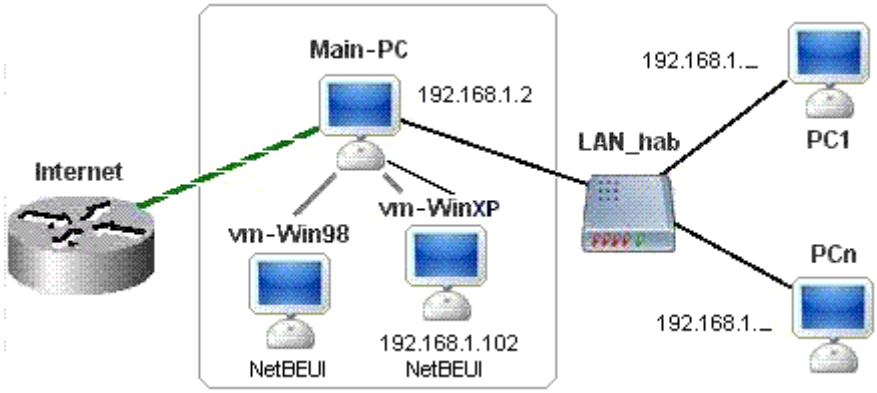


Рис.5.1. Структура виртуальной сети.

Задание 1.

1. Настроить требуемую конфигурацию, аналогично рис. 5.1, но со своими IP-адресами, именами vmWin98-<k> и vmWinXP-<k>.
2. Проверить наличие сетевого доступа между виртуальными машинами и основным компьютером, используя для этого инструмент сетевого окружения и консольную команду ping.

Если виртуальная сеть находится в работоспособном состоянии, то поставим задачу организовать в этой сети возможность удаленного администрирование компьютеров, входящих в её состав. Эти функции возложим на её сетевого администратора, то есть на Вас. Пусть, в нашей виртуальной сети ее администратор будет иметь логин и пароль

vm-admin

Для решения задачи организации удаленного администрирования необходимо выполнить следующую последовательность действий:

- На компьютере vm-WinXP организовать дополнительную учетную запись с правами администратора.
- Настроить компьютеры vm-Win98 и vm-WinXP на возможность дистанционного управления ими.
- Организовать к этим компьютерам подключение с других узлов ЛВС, для целей удаленного управления этими компьютерами.

Существует множество различных вариантов решения этой задачи. Мы кратко рассмотрим только наиболее простые и часто используемые, не претендуя на профессиональный подход к их использованию.

3. Настройка разрешений на удаленное управление в Windows 98 и Windows XP

Чтобы разрешить удаленное управление компьютером с операционной системой Windows 98 следует войти в Панель управления и выбрать режим Пароли. В появившемся окне выбрать вкладку Удаленное управление (рис. 5.2), на которой:

- Установить переключатель в режим разрешения удаленного управления.
- В поля Пароль и Подтверждения пароля ввести пароль пользователя, на которого эти разрешения распространяется.

  Напомню, что выше мы договорились, что это пользователь с логином и паролем vm-admin.

- По окончанию нажать кнопку ОК.

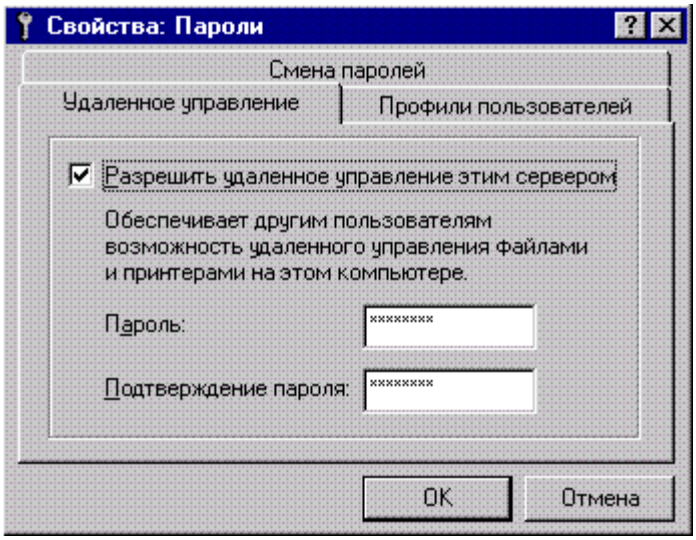


Рис.5.2. Вкладка настройки удаленного управление компьютером.

Система Windows XP является более совершенной и имеет более продвинутые инструменты удаленного доступа. Одним из возможных способов удаленного администрирования компьютера является подключение к его рабочему столу. Для этих целей Microsoft специально разработала протокол RDP (Remote Desktop Protocol — протокол удалённого рабочего стола).

Чтобы настроить компьютер с Windows XP на использование дистанционного управления его рабочим столом необходимо:

1. Войти в систему с правами администратора.
2. Выбрать Мой компьютер -> Свойства -> Удаленные сеансы (рис. 5.2).
3. На вкладке Удаленные сеансы установить флажок "Разрешить удаленное подключение к этому компьютеру".
4. Нажав кнопку Выбрать удаленных пользователей, можно выбрать пользователей, которые могут подключаться к этому компьютеру.
5. Затем нажать кнопку Применить и ОК.

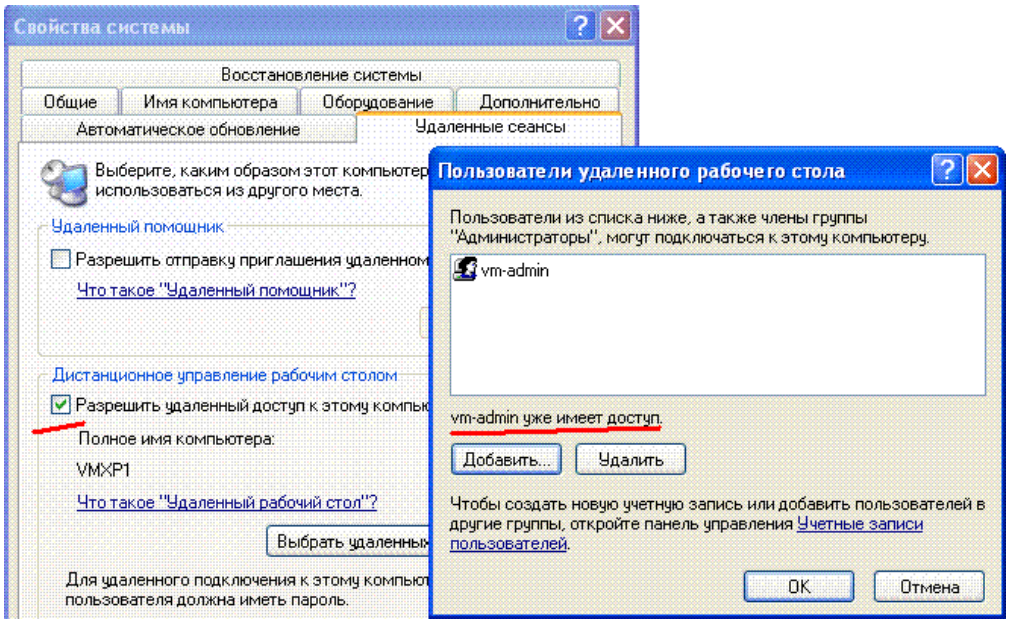


Рис.5.3. Вкладка Удаленные сеансы окна Свойства системы.

Задание 2.

1. Разрешить удаленное управление компьютером vmWin98-<k> пользователю с логином и паролем vm-admin.

2. На виртуальную машину vmWinXP-<k> добавить пользователя с логином и паролем vm-admin, наделенного правами администратора.

3. Разрешить удаленное подключение к этому компьютеру.

4. Подключение к удаленному рабочему столу

Работа удаленного рабочего стола основана на применение технологии Terminal Services (Службы терминалов) и протокола RDP. Компьютер, к которому выполняется подключение, выступает в роли сервера терминалов, что позволяет запускать на нем приложения с любого компьютера-клиента, поддерживающего протокол RDP.

Подключение возможно с использованием локальной сети, VPN, или интернет-соединения. На возможность комфортной работы значительное влияние оказывает пропускная способность соединения. При установлении соединения в Windows XP Remote Desktop производит вывод из сеанса текущего пользователя. Это значит, что он не сможет наблюдать за действиями пользователя, установившего соединение.

Для подключения с основного компьютера к удаленному рабочему столу виртуальной машины vm-WinXP (192.168.1.102) следует:

- Выбрать Пуск -> Программы -> Стандартные -> Связь -> Подключение к удаленному рабочему столу (рис.5.4) или, возможен второй вариант, а именно выбрать Пуск -> Выполнить -> в поле "Открыть" ввести mstsc.exe и нажать кнопку "OK".

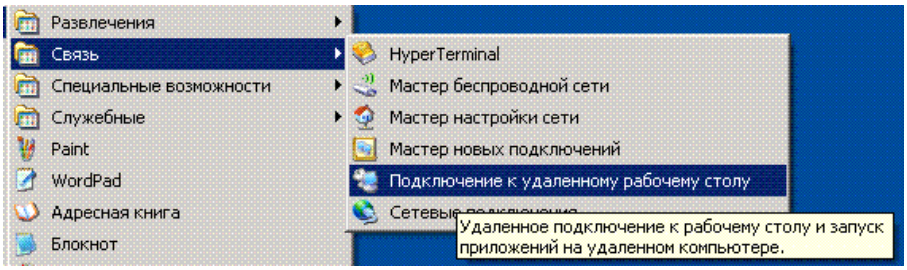


Рис.5.4. Подключение к удаленному рабочему столу.

- Затем в окне, приведенном на рис. 5.5, ввести имя или IP-адрес удаленного компьютера, к которому требуется подключиться, и нажать кнопку "Подключить".

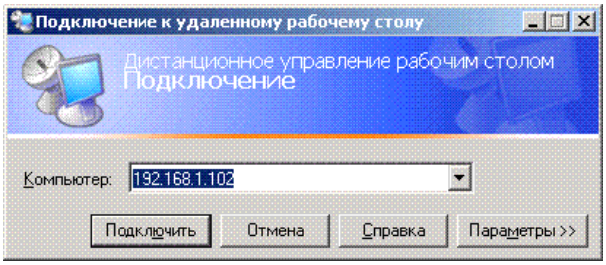


Рис.5.5. Подключение к удаленному рабочему столу.

Внимание!!!

Если подключение выполняется первый раз, то следует провести более тонкую настройку, задав параметры этого подключения.

Для задания параметров подключения надо нажать кнопку "Параметры" на форме, приведенной на рис. 5.5.

Более подробное описание параметров подключения вы найдете в Приложение 1 к лабораторной работе. Здесь мы приведем только вид вкладок с набором параметров, которые установлены в минимальные значения с учетом того, чтобы дополнительно не загружать ресурсы основного компьютера в процессе работы нашей виртуальной сети (рис. 5.6).

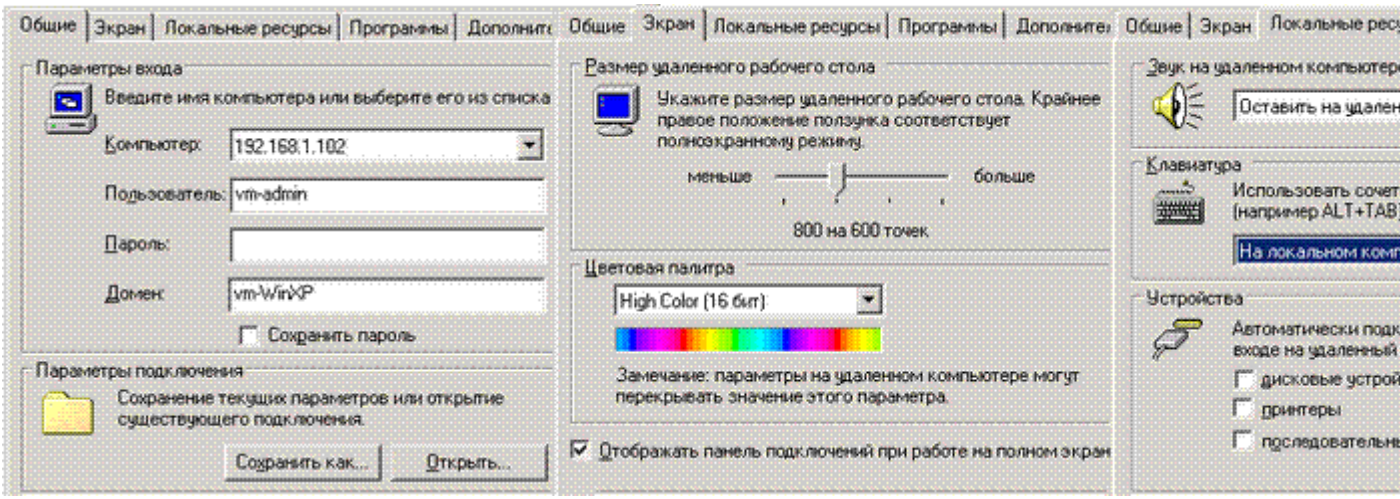


Рис.5.6. Вкладки настройки параметров подключения.

После того, как параметры будут установлены вы можете выполнить подключение. У вас на экране должен заблокироваться экран виртуальной машины vm-WinXP и появиться новое

окно удаленного рабочего стола пользователя vm-admin на виртуальной машине vm-WinXP (рис. 5.7).

Рис.5.7. Экран основного компьютера с заблокированным окном vm-WinXP и окном удаленного рабочего стола пользователя vm-admin на vm-WinXP.

Задание 3.

1. Выполните настройку параметров и подключитесь с основного ПК на удаленный рабочий стол виртуальной vmWinXP-<k>.

2. Находясь в удаленном рабочем столе, измените настройки рабочего стола пользователя vm-admin. Например, Пуск -> Свойство -> Классическое меню.

3. Закройте удаленный рабочий стол и войдите в vmWinXP-<k> как пользователь vm-admin. Убедитесь, что удаленно были изменены настройки рабочего стола этого пользователя.

4. Повторно подключитесь к удаленному рабочему столу и на диске C:/ создайте новую папку NewFromMain, а в ней текстовый файл FromMain.txt произвольного содержания. Сделайте вновь созданную папка полностью общедоступной.

5. Войдите в vmWin98-<k> и, используя Сетевое окружение, убедитесь, что на компьютере vmWinXP-<k> появилась новая общедоступная папка, а в ней новый файл. Создайте в этой папке текстовый файл FromWin98.txt.

6. Закройте удаленный рабочий стол, войдите на компьютере vmWinXP-<k> и убедитесь, что в нем удаленно была создана новая папка и в ней появились два файла, созданные на разных узлах ЛВС.

Следует отметить, что для подключения к удаленному рабочему столу можно использовать не только Windows XP Professional и старше, но и более ранние версии Windows. Это позволяет, например, на дисплее компьютера с MS Windows 98 отобразить удаленный рабочий стол Windows XP и управлять этим удаленным компьютером с компьютера с более слабой операционной системой.

Для этого необходимо загрузить с сайта Microsoft (http://www.microsoft.com/windowsxp/downloads/tools/rdclientdl.mspx) клиента RDP-протокола msrdpcli.exe. Также его можно скопировать из папки \Support\Tools компакт-диска Windows XP.

Задание для самостоятельной работы

1. Найдите на одном из компьютеров ЛВС лаборатории файл MSRDPCLI.EXE - клиент RDP для Windows.

2. Скопируйте его на виртуальную машину vmWin98-<k>.

3. Установите клиента RDP для Windows на виртуальную машину vmWin98-<k>.

4. Исследуйте возможность подключения к удаленному рабочему столу vmWinXP-<k>.

5. Технология удаленного помощника

Эта технология предназначена для удаленного управления компьютерами путем подключения к рабочему столу удаленного компьютера, используя протокол RDP (Remote Desktop Protocol). Она позволяет оказывать помощь пользователям, испытывающим те или иные проблемы.

Используя "Удаленный помощник", сетевой администратор может, не покидая своего рабочего места, подключиться к рабочему столу компьютера пользователя и совместно с ним решить возникшие проблемы. Пользователь, нуждающийся в помощи администратора, посылает запрос на оказание поддержки, используя один из следующих способов:

- посредством электронной почты;
- через программу обмена сообщениями Windows Messenger (при этом и пользователь, и администратор должны быть в режиме "он-лайн" системы обмена сообщениями);
- через файл, доступный по сети пользователю и администратору.

Все сеансы зашифровываются и могут быть защищены паролем. При решении возникших сложностей можно вести разговор по сети в режиме реального времени.

По умолчанию разрешение на использование "Удаленного помощника" в системе Windows отключено. Чтобы разрешить использование Удаленного помощника следует выбрать Свойства компьютера -> Удаленные сеансы, а затем поставить галочку для поля Удаленный помощник (рис. 5.8).

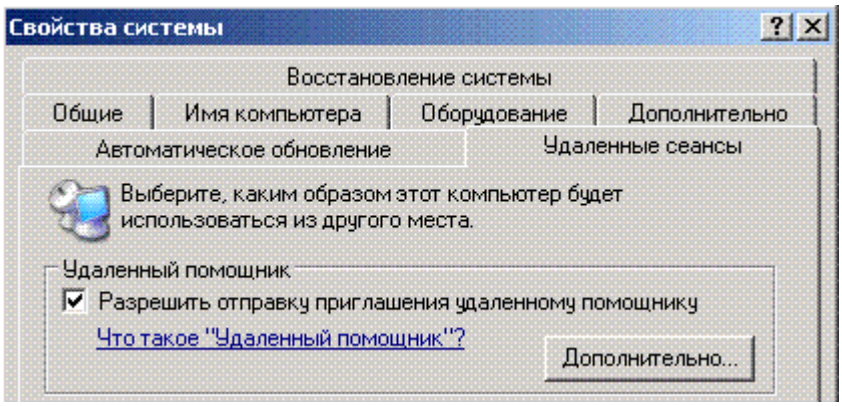


Рис.5.8. Установка разрешения на использование "Удаленного помощника.

Постановка задачи:

Пусть пользователем, которому требуется помощь, является пользователь vm-admin, работающий на виртуальной машине vmWinXP-<k>. И ему требуется консультация более опытного профессионала, которая может быть оказана с основного компьютера нашей виртуальной сети.

Рассмотрим на этом примере процесс создания запроса, ответа на запрос, подключения к рабочему столу пользователя и совместной работы в одном и том же сеансе системы Windows пользователя и удаленного профессионала-администратора.

Этап создания запроса на удаленную помощь:

1. Отправка пользователем запроса администратору на подключение "Удаленного помощника" инициируется из Центра справки и поддержки системы Windows. Для этого надо выбрать Пуск -> Справка и поддержка (рис. 5.9).

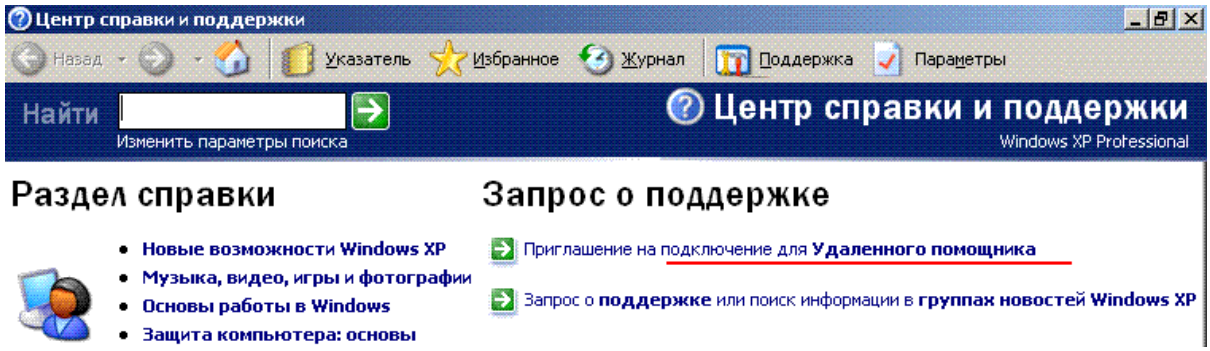


Рис.5.9. Окно центра справки и поддержки Windows.

2. В правой верхней части данного окна следует щелкнуть по ссылке "Приглашение на подключение для Удаленного помощника", что вызовет на экран новое окно - окно отправки приглашения (рис. 5.10).

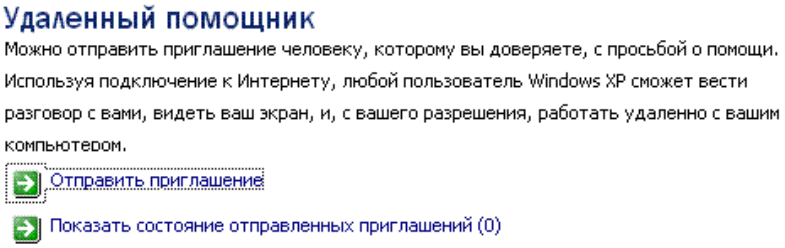


Рис.5.10. Окно отправки приглашения на подключение удаленного помощника.

3. Далее надо выбрать ссылку Отправить приглашение и вам будут предложены варианты способа связи с помощником. Для рассматриваемого примера, то есть для режима работы в одноранговой ЛВС, следует:
   - Выбрать вариант Сохранить приглашение в файл.
   - Указать имя пользователя, срок действия приглашения (по умолчанию - 1 час), задать пароль для данного конкретного приглашения. Пусть таким паролем будет HelpPsw.
   - После этого необходимо сохранить приглашение в файле общедоступной сетевой папки. В нашем примере папкой, доступной как на vmWinXP-<k>, так и с основного компьютера, является папка NewFromMain. По умолчанию имя

создаваемого файла - RAInvitation.msrcincident. Оставим это имя без изменения (рис. 5.11).

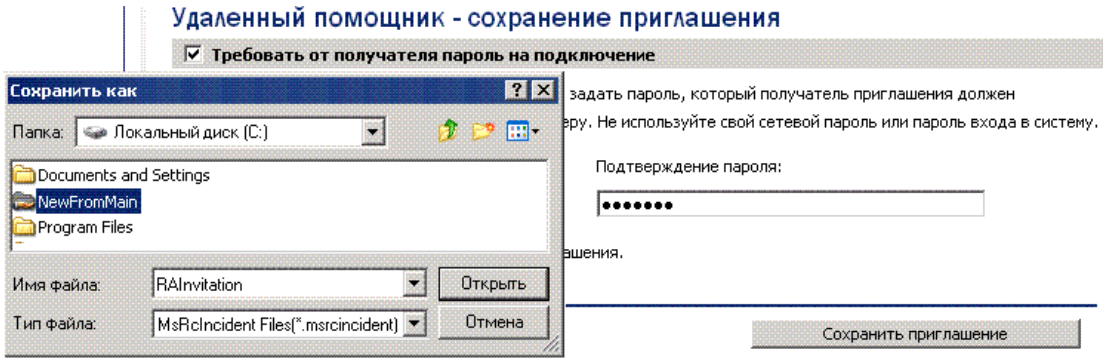


Рис.5.11. Формирование приглашения удаленному помощнику в файл RAInvitation.msrcincident.

4. Если все было сделано верно и файл был успешно сохранен в общедоступной папке ЛВС, на экран будет выдано подтверждение, аналогичное приведенному на рис. 5.12.

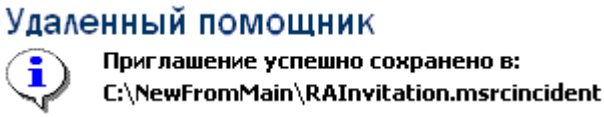


Рис.5.12. Подтверждение отправки приглашения.

5. Если используются электронная почта или Windows Messenger, то администратор в окне соответствующей программы увидит сообщение с приглашение оказать помощь. Если запрос на помощь организован в виде файла, то пользователь должен каким-то способом, например, по телефону или SMS, известить администратора о сохраненном приглашении и необходимости подключиться к его рабочему столу.

   Замечание:

   Следует отметить, что создав файл приглашения его можно отправить помощнику любым способом — скопировать его на гибкий или общий сетевой диск, отправить с помощью другой почтовой службы или FTP и т.д.

Этап реакции администратора на поступивший запрос:

1. Администратор, находясь за своим компьютером, в нашем примере это основной компьютер виртуальной ЛВС, через свое сетевое окружение заходит в общесетевую папку и обнаруживает там новый файл приглашения на удаленную помощь (рис. 5.13).

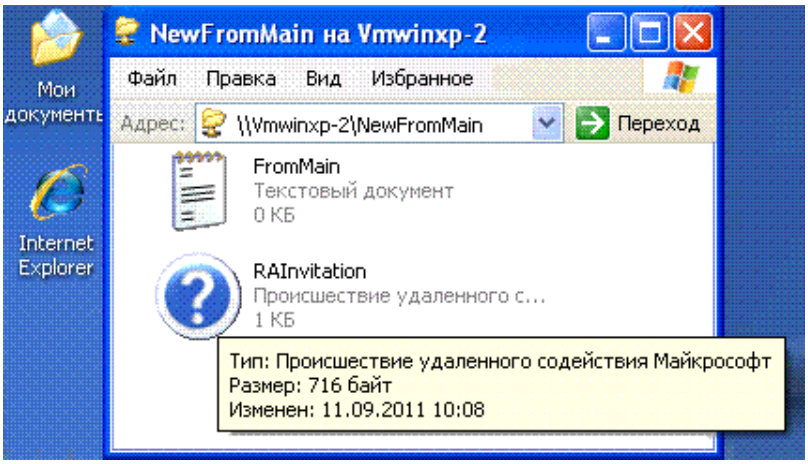


Рис.5.13. Новый файл приглашения в общесетевой папке ЛВС.

2. Администратор открывает сохраненный файл и видит параметры приглашения: дата, время и имя пользователя, отправившего приглашение (рис. 5.14). Он должен дополнительно запросить у пользователя пароль на текущее подключение и ввести его в поле Пароль (в нашем примере, HelpPsw), а затем нажать кнопку Да.

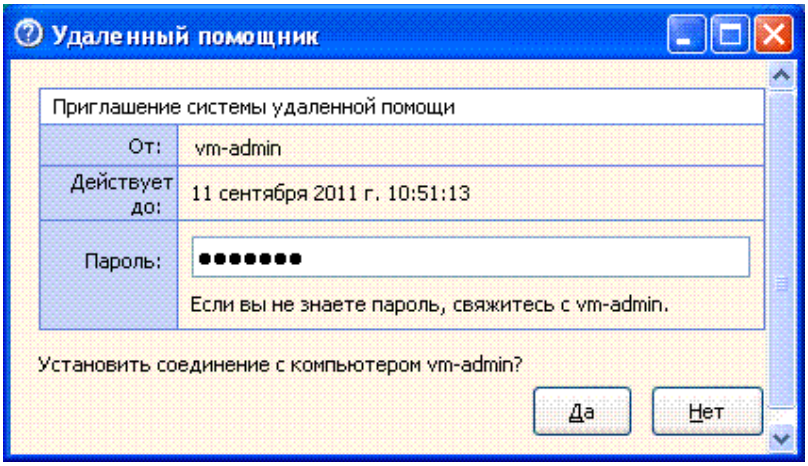


Рис.5.14. Окно подключения к удаленному компьютеру.

3. После установления соединения с компьютером пользователя, на рабочем месте администратора запускается своя копия удаленного помощника, а на на компьютере пользователя появляется сообщение о готовности администратора оказать удаленную помощь (рис. 5.15).

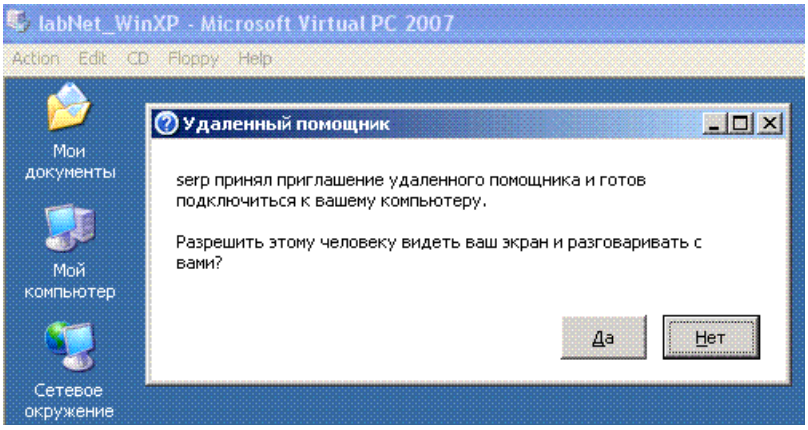


Рис.5.15. Сообщение на компьютере пользователя о готовности администратора к помощи.

Этап сеанса удаленной помощи:

1. На компьютере администратора в правой части окна Удаленный помощник появляется рабочий стол пользователя, который может отображаться либо в истинном, либо в масштабированном размерах. Левая часть окна отображает историю разговора с удаленным пользователем (рис. 5.16).

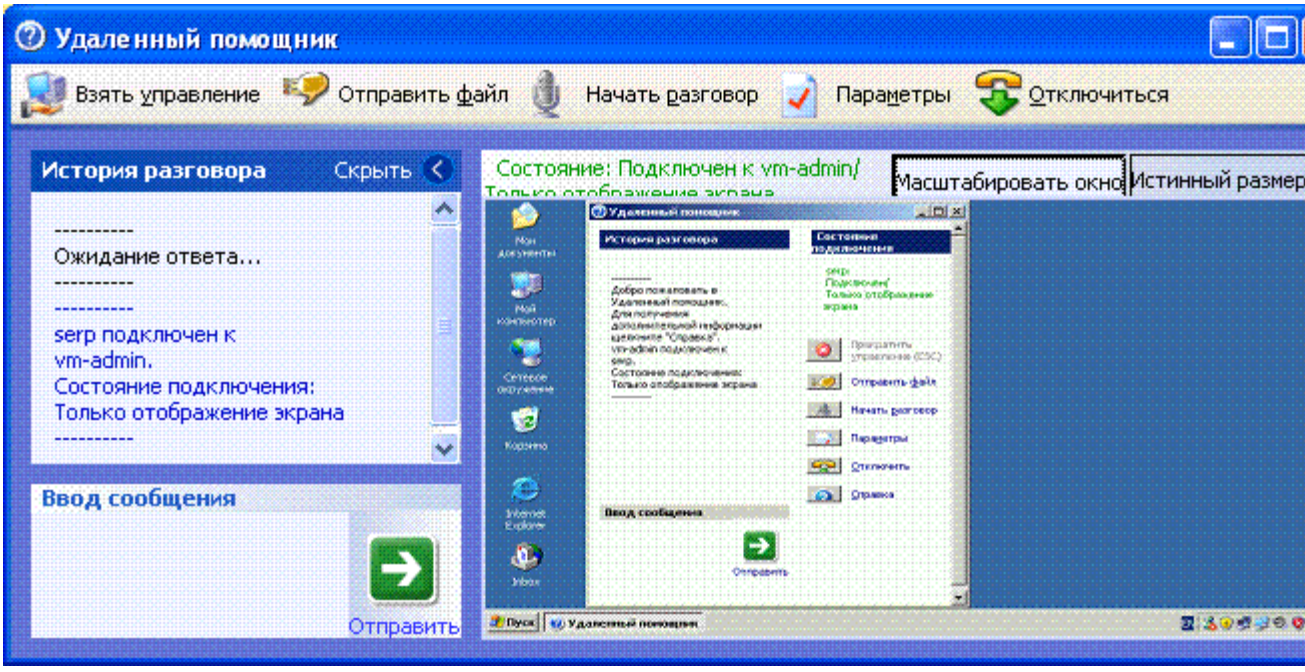


Рис.5.16. Окно удаленного помощника на компьютере администратора.

2. В это же время на компьютере пользователя также появляется окно удаленного помощника, которое отображает состояние подключения, историю разговора, основные режимы и параметры работы, а также строку ввода текстовых сообщений для передачи администратору.

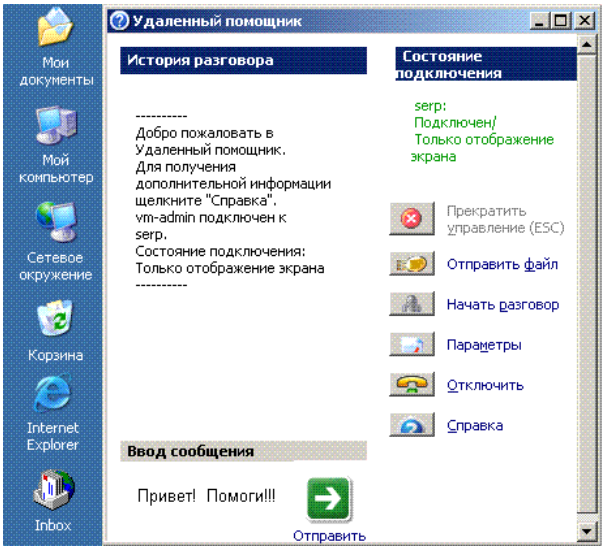


Рис.5.17. Окно удаленного помощника на компьютере пользователя.

3. Пользователь может либо установить мультимедийную связь с администратором, либо переслать файл с описанием возникших проблем, либо кратко описать проблему в тектовом сообщение. Например, "Привет! Помоги!!!" и нажать кнопку Отправить (рис. 5.17).
4. Администратор получит это текстовое сообщение, которое отобразится на его компьютере в панели История разговора.
    - Он может взять на себя управление удаленным компьютером. Для этого ему следует в панели инструментов окна Удаленный помощник (рис. 5.16) нажать кнопку Взять управление.
    - Это действие администратора приведет к тому, что на компьютере пользователя появится запрос о разрешение со стороны пользователя управлять его компьютером администратору (рис. 5.18).

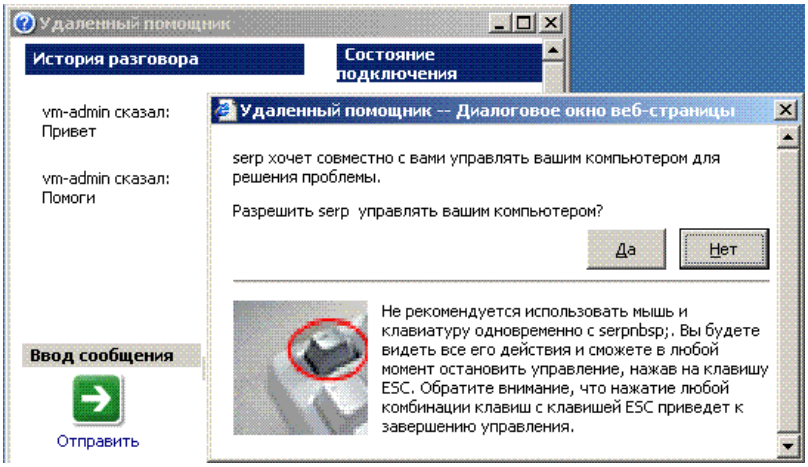


Рис.5.18. Запрос на разрешение удаленного управления компьютером пользователя.

5. Пользователь еще раз разрешает администратору подключиться к его ПК, после чего администратор и пользователь совместно работают в одной сессии системы Windows на компьютере пользователя.
6. Администратор может прекратить совместный сеанс работы, нажав кнопку "Вернуть управление", пользователь также может прекратить сеанс кнопкой "Отключить".
7. Можно сообщить другому пользователю о возможности повысить производительность системы, уменьшив количество отображаемых экраном цветов с помощью параметра Качество цветопередачи в меню «Отображение» (на панели управления).

Подводя итог, еще раз подчеркнем важность инструмента удаленного управления в больших организациях. Использование Удаленного рабочего стола и Удаленного помощника значительно экономит рабочее время и позволяет сократить количество вызовов сетевых администраторов на рабочие места пользователей.

Задание 4.

1. Выполните настройку параметров vmWinXP-<k> на возможность получения удаленной помощи с вашего основного компьютера.

2. Сформируйте на vmWinXP-<k>, как пользователь, запрос к основному компьютеру на оказание помощи. Ответьте, но уже как администратор, на поступивший запрос и установите сеанс помощи "основной ПК - vmWinXP-<k>".

3. Рассмотрите основные приемы и действия, доступные в этом сеансе: передача сообщений (чат), режимы отображения и управления удаленным компьютером, возможность обмена файлами, работа с разными масштабами окон и т.д.

4. Закрыв сеанс, повторите запрос с vmWinXP-<k>, установив время реакции на запрос 1 минута. Не реагируя, как администратор, в течение этого время на поступивший запрос, посмотрите его результат на обоих компьютерах.

5. Повторите запрос на помощь, воспользовавшись уже сформированным на vmWinXP-<k> списком приглашений.

6. Создайте несколько приглашений и познакомтесь с возможностью просмотра отправленных приглашений (рис. 5.10).

7. Запросите помощь у доступного вам соседа по ЛВС лаборатории, предварительно договорившись, на каких общедоступных ресурсах ЛВС лаборатории будет сохраняться файл запроса на помощь.

8. Если еще доступна настроенная на прошлых лабораторных работах система электронной почты ЛВС, воспользуйтесь ее для формирования запроса на удаленную помощь.

6. Технология добровольной удаленной помощи

Технологию удаленного помощника можно настроить и использовать таким образом, чтобы администраторы и персонал службы поддержки могли предложить удаленную помощь другим пользователям, когда те и не запускают сеанс удаленного помощника. Данная функция называется «Добровольной удаленной помощью» и рассчитана на использование в больших корпорациях с сетями на базе Active Directory (доменов).

Однако, эта технология доступна для использования и в небольших ЛВС на базе обычной рабочей группой. Именно эта технология и будет рассмотрена ниже.

Внимание:

Основное требование при настройке предложения удаленной помощи в рабочей группе заключается в том, что на компьютере пользователя должна быть создана точно такая же учетная запись, как и на компьютере администратора.

Если мы поставим задачу предлагать удаленную помощь с основного компьютера на виртуальную машину vmWinXP-<k>, то на последней должна быть учетная запись точно такая же, как и на основном компьютере. Например, если на основном компьютере администратор работает под учетной записью

с логином Vnet и паролем Vnet,
принадлежащей группе администраторов, то на удаленном компьютере также должна быть создана учетная запись с таким же логином и паролем, то есть с логином Vnet и паролем Vnet.

Задание 5.

Создать на vmWinXP-<k> учетную административную запись, аналогичную записи на основном компьютере. После чего перезагрузить компьютер.

Настройка удаленного компьютера пользователя

По умолчанию функция «Добровольной удаленной помощи» выключена и включить ее можно только с помощью параметра групповой политики "Предложение удаленной помощи". Именно эта политика определяет, может ли сетевой администратор предлагать удаленную помощь или давать указания пользователю узла ЛВС, если тот первым явно не запросил помощь через канал связи, электронную почту или службу мгновенных сообщений.

1. Запустить оснастку «Групповая политика» в консоли управления MMC. Для этого надо в меню Пуск выбрать пункт Выполнить, в поле Открыть ввести команду gpedit.msc, а затем нажать кнопку OK.

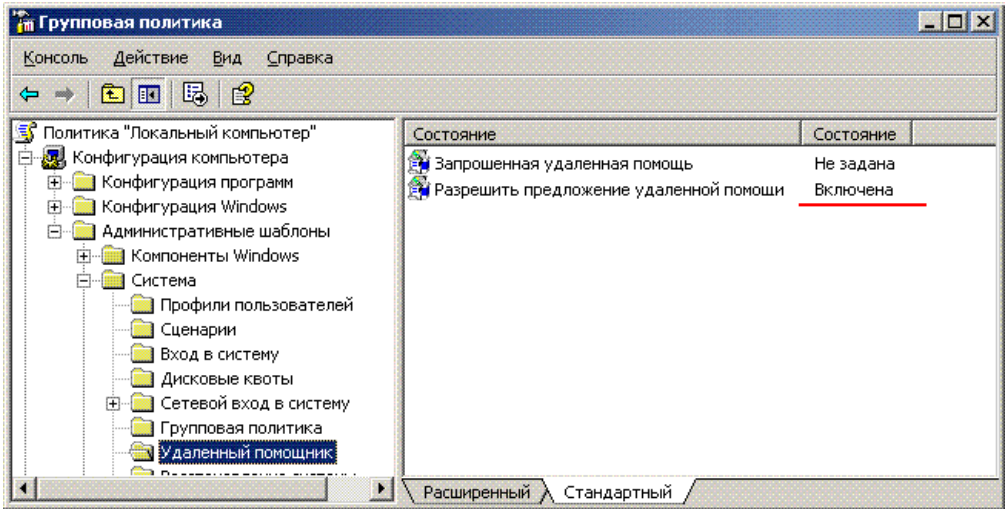


Рис.5.19. Окно оснастки «Групповая политика».

2. В левой панели окна Групповая политика (рис. 5.19) выбрать Политика «Локальный компьютер» -> Конфигурация компьютера -> Административные шаблоны -> Система -> Удаленный помощник. Затем дважды кликнуть мышкой на строке Разрешить предложение удаленной помощи и откроется окно, аналогичное, приведенному на рис. 5.20.

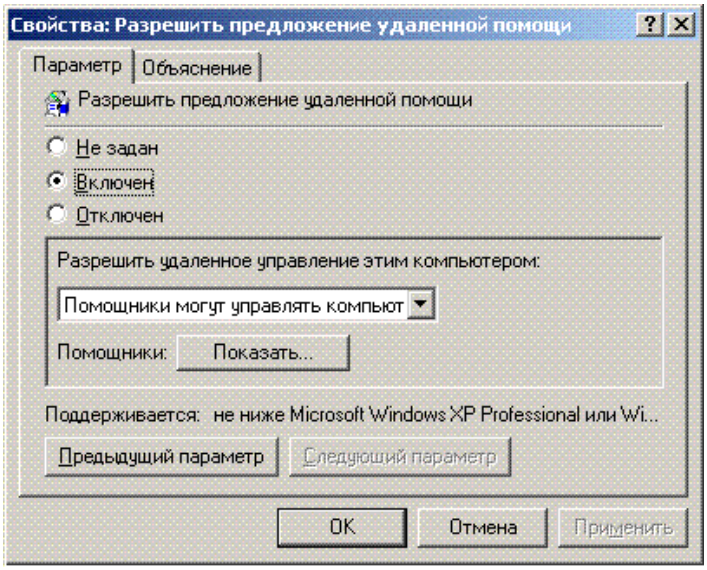


Рис.5.20. Окно свойств политики «Предложение удаленной помощи».

3. В диалоговом окне свойств политики (рис. 5.20) следует:

    - Выбрать режим Включен.
    - Из списка возможных действия, которые сможет предпринять администратор, называемый в этой оснастке помощником или экспертом, выбираем "Помощники могут управлять компьютером".
    - Далее важный момент - надо нажать кнопку Показать (список помощников) и в открывшемся окне следует вручную прописать логин учетной записи помощника, то есть нашего администратора.
4. Затем следует нажать кнопку ОК, чтобы закрыть диалоговое окно Вывод содержания, а потом еще раз кнопку ОК, чтобы закрыть диалоговое окно Предложение удаленной помощи.
5. По окончанию закройте оснастку «Групповая политика» консоли управления. Политика будет применена сразу после внесения изменений. Перезагружать компьютер не требуется.

Внимание:

Подключение к Vista или Windows 7 обычно проходит без проблем, а при подключении к XP бывают сложности. В этом случае проверьте запущены ли на удаленном компьютере службы "Центр справки и поддержки", "Диспетчер сеанса справки для удаленного рабочего стола", "Служба терминалов". Также рекомендуется отключить "Простой общий доступ к файлам".

Для того, чтобы отключить простой общий доступ надо:

- Открыть на удаленном компьютера пользователя любую папку и в её основном меню выбрать Сервис -> Свойство папки.
- В появившемся окне Свойство папки перейти на вкладку Вид.
- В списке Дополнительные параметра снять галочку у параметра Использовать простой общий доступ к файлам (рекомендуется).
- Нажать кнопку Применить и ОК, а затем следует выполнить перезагрузку компьютера.

Задание 6.

1. Выполните на vmWinXP-<k> настройку политики «Предложение удаленной помощи» в соответствии с описанным выше сценарием.

2. Отключите брандмауэр Windows. О его настройках речь пойдет ниже.

3. Для проверки удаленного доступа временно отключите на vmWinXP-<k> простой общий доступ.

Запуск предложения помощи на компьютере эксперта.

После настройки компьютера пользователя можно переходить к компьютеру эксперту-администратора, которым у нас является основной компьютер. Для формирования с компьютера администратора предложения о помощи следует:

1. Выбрать Пуск -> Справка и поддержка -> Использование служебных программ для просмотра сведений о компьютере и диагностики неполадок (рис. 5.21).

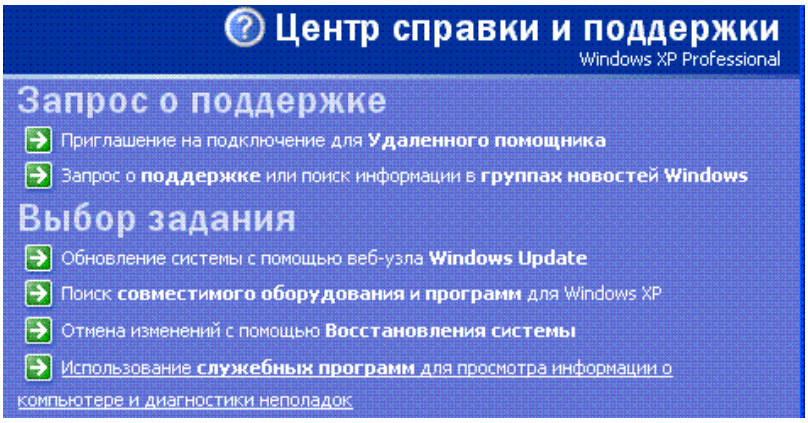


Рис.5.21. Окно Центра справки и поддержки.

2. В левой части окна Центра справки и поддержки в панели Сервис надо выбрать опцию Предложение удаленной помощи (рис. 5.22).

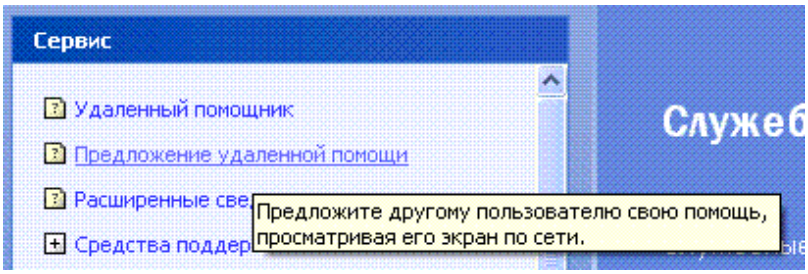


Рис.5.22. Панель Сервис окна Центра справки и поддержки.

3. Откроется страница «Предложение удаленной помощи» (рис. 5.23), на которой надо ввести имя или IP-адрес компьютера, которому предназначается предложение удаленной помощи. После этого нажать кнопку Подключиться.

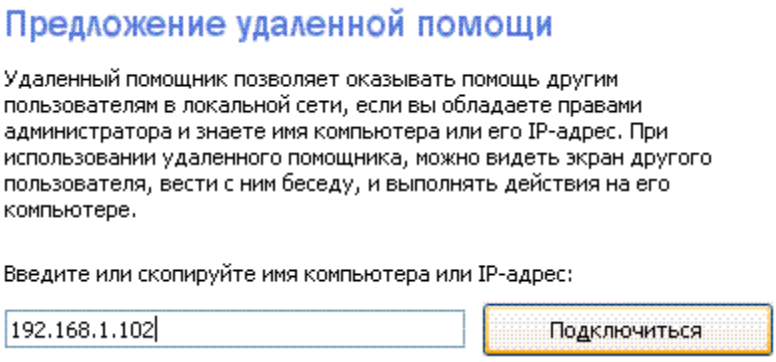


Рис.5.23. Страница «Предложение удаленной помощи» до связи с удаленным компьютером.

4. За этим последует приглашение (рис. 5.24) выбрать из раскрывающегося меню пользователя, которому необходимо оказать помощь. Выбрав пользователя, нажмите Запустить удаленного помощника.

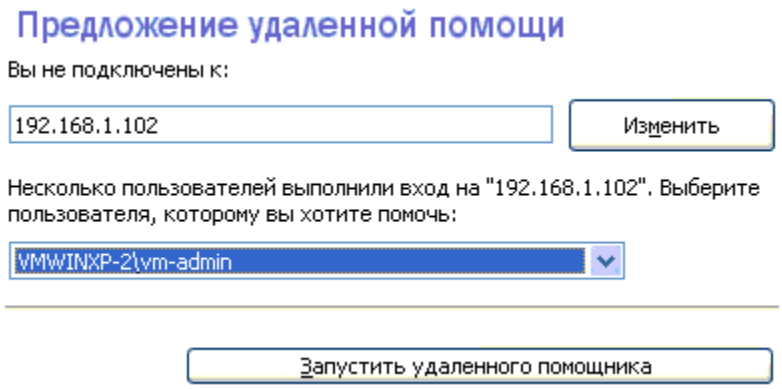


Рис.5.24. Страница «Предложение удаленной помощи» после установления связи.

5. Сеанс удаленной помощи начинается после того, как пользователь, которому предназначена помощь, получит соответствующее сообщение и нажмет кнопку «Да». В случае необходимости администратор может отправить запрос на получение контроля над компьютером начинающего пользователя.

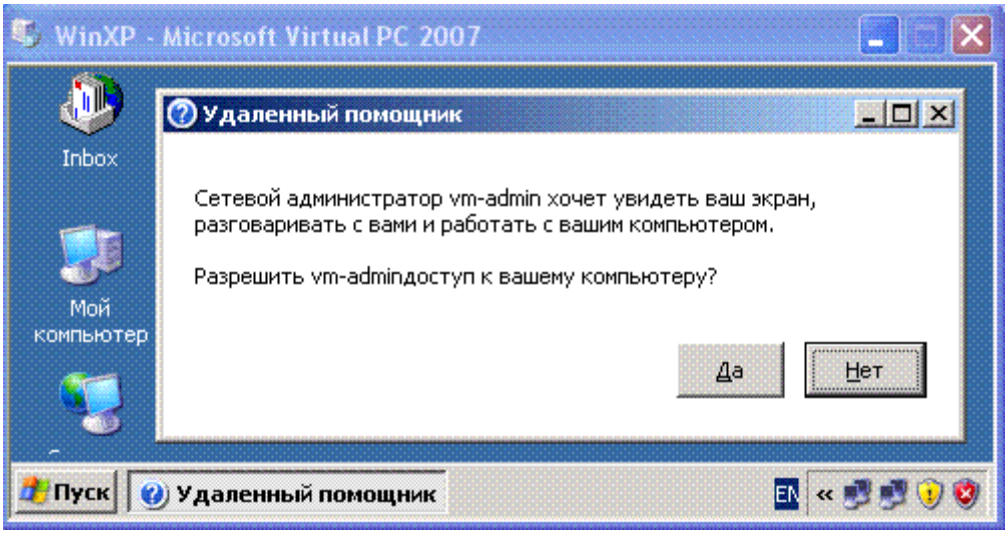


Рис.5.25. Компьютер пользователя: запрос администратора на удаленное подключение.

Дальнейшее взаимодействие пользователя и эксперта-администратора полностью повторяет процесс взаимодействия в случае удаленного помощника. Принципиальным моментом в этой технологии, что администратор может прийти на помощь пользователю или дать ему какие-либо указания без формирования со стороны пользователя достаточно сложных запросов через мессанджеры или электонную почту. Достаточно телефонного звонка или SMS и администратор на компьютере пользователя.

Задание 7.

1. Выполните с основного компьютера предложение удаленной помощи» на vmWinXP-<k>.

2. Проведите сеанс совместной работы, разорвите сеанс и повторите его еще раз.

3. Включите брандмауэр Windows и повторите п.1. Какой получился результат и почему?

Команды запуска предложения помощи на компьютере эксперта.

Рассмотренный выше подход по формированию предложения на удаленную помощь предполагал долгую навигацию по различным страницам и вкладкам Центра справки и поддержки. Для занятого и ленивого системного администратора это недопустимая потеря времени. Поэтому есть возможность осуществлять запуск удаленного помощника в режиме предложения помощи из командной строки или специально сформированных для этого командных файлов, используя следующие команды:

- в Windows XP

  C:\Windows\pchealth\helpctr\binaries\helpctr.exe /url hcp://CN=Microsoft%20Corporation,L=Redmond,S=Washington, C=US/Remote%20Assistance/Escalation/unsolicited/unsolicitedrcui.htm

- в Windows Vista

  C:\Windows\System32\msra.exe /expert

- в Windows 7

  C:\Windows\System32\msra.exe /offerra

Настройка брандмауэра для работы удаленного помощника.

В Vista и Windows 7 встроенный брандмауэр настраивается автоматически после включения удаленного помощника. В XP нужно вручную добавить в исключения брандмауэра следующие три программы:

- C:\WINDOWS\pchealth\helpctr\binaries\helpctr.exe
- C:\WINDOWS\pchealth\helpctr\binaries\helpsvc.exe
- C:\WINDOWS\system32\sessmgr.exe (правда для этой уже было создано правило под названием "Удаленный помощник")
- Кроме этого необходимо открыть порт TCP 135 для входящих подключений.

Для настройки брандмауэра Windows по добавлению новых ислючений следует выбрать Панель управления -> Брандмауэр Windows -> вкладка Исключения.
Задание 8.

1. Выполните с основного компьютера подключение к удаленному рабочему столу vmWinXP-<k>, используя для входа на него учетную запись vm-admin/vm-admin.

2. Проведите в удаленном сеансе настройку брандмауэра vmWinXP-<k> и включение его в работу. Не закрывайте удаленный рабочий стол.

3. Выполните с основного компьютера от имени администратора Vnet/Vnet предложение удаленной помощи на vmWinXP-<k>. Какой получился результат и почему?

7. Простейший вариант скрытия удаленных администраторов

Если в этой лабораторной работе вы делали все в той последовательности, как вам было предложено, то на текущий момент окно приглашения Windows после включения или перезагрузки vmWinXP-<k> будет иметь вид, аналогичный приведенному на рис. 5.26.

Рис.5.26. Стартовое окно приглашения Windows на vmWinXP-<k>.

Не кажется ли вам странным, что сетевые администраторы (vm-admin/vm-admin) и служба поддержки (Vnet/Vnet), которые должны бы оставаться в тени и быть незаметными, вылезают на первый план на компьютере рядового пользователя. Пользователя, для которого даже нет собственного административного или пользовательского входа на его же компьютер.

Попробуем устранить эту несуразность. Для этого поставим перед собой две задачи. Первая задача - это создать нового пользователя, которой будет локальным администратором своего компьютера vmWinXP-<k> и иметь имя

adminXP
И вторая задача - это скрыть от начальной загрузки учетные записи удаленных сетевых администраторов и помощников. Первая задача абсолютна ясна, а для реализации второй следует:

- Выбрать Панель управления -> Администрирование -> Локальная политика безопасности или, что то же самое, Пуск -> Выполнить -> ввести команду

  secpol.msc /s

  и нажать ОК. Это приведет к тому, что на экране дисплея появиться окно локальных параметров безопасности (рис. 5.27)

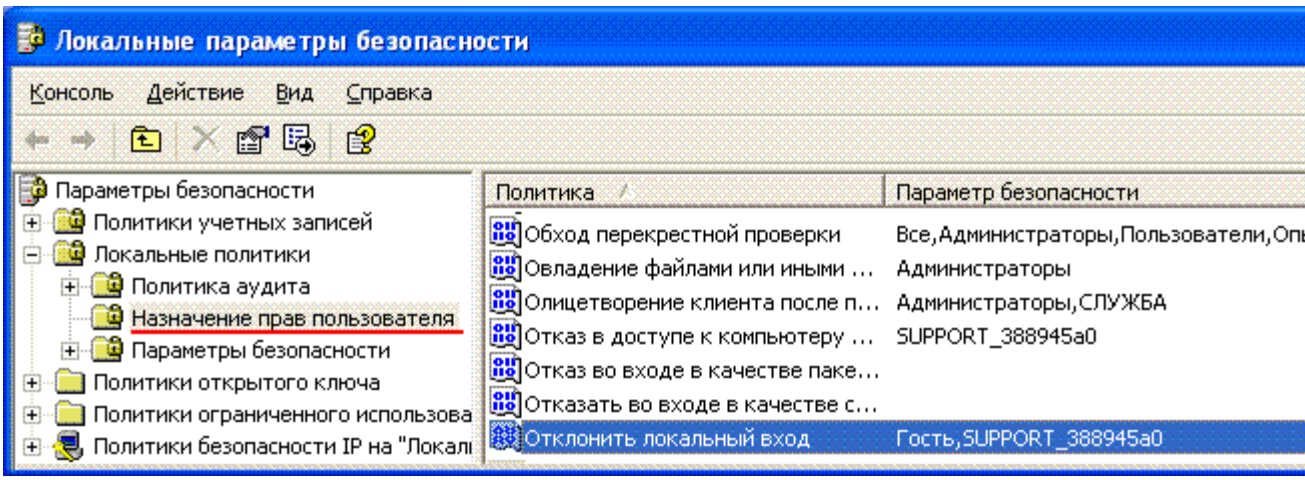


  Рис.5.27. Окно Локальные параметры безопасности.

- Далее надо найти в этом окне политику Отклонить локальный вход и дважды кликнуть мышкой по этой строке.

- В появившемся окне свойств этой политики следует добавить пользователей vm-admin и Vnet, нажать Применить, а затем ОК.
- Закрыть окно локальных параметров безопасности и перезагрузить компьютер.

Если обе, поставленные перед нами задачи, были успешно выполнены, то после перезагрузки вид стартового окна на vmWinXP-<k> будет иметь вид, аналогичный приведенному на рис. 5.28.

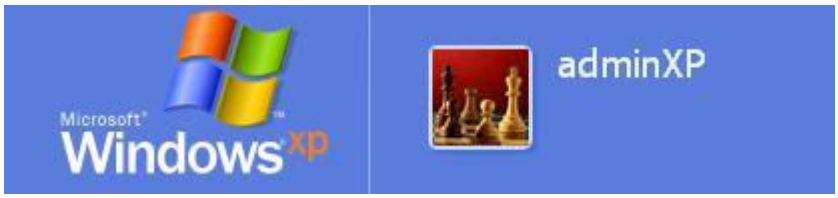


Рис.5.28. Новое стартовое окно Windows на vmWinXP-<k>.

Задание 9.

1. Так как логины и пароли на виртуальных машинах Windows XP всех участников лабораторного практикума должны быть одинаковы, то выполните со своего основного компьютера подключение к удаленному рабочему столу vmWinXP-<k+1> вашего соседа. Если по каким либо причинам это невозможно то к своей vmWinXP-<k>.

2. Добавьте на удаленном компьютере пользователя adminXP в качестве локального администратора этого компьютера.

3. Отключите на этом компьютере локальный вход удаленных администраторов и удаленно перезагрузите этот компьютер.

4. Убедитесь, что настройка удаленного компьютера выполнена верно и отключите удаленный рабочий стол.

5. После того, как ваш сосед закончил настройку вашей vmWinXP-<k> и освободил рабочий стол, проверьте сами настройку вашей vmWinXP-<k>.

6. Проведите тестирование связки "основной ПК - vmWinXP-<k>" по работе с удаленным помощником и предложением удаленной помощи для случая отключения локального входа сетевых администраторов и помощников.

Приложение к лабораторной работе

п1. Технология удаленного рабочего стола (Remote Desktop)

Существует целый ряд средств, позволяющих производить удаленное подключение к компьютеру для оказания технической поддержки. В качестве примера можно привести такие программы, как RAdmin, Carbon Copy и pcAnywhere. Microsoft тоже не осталась в стороне - в ОС Windows XP имеются встроенные инструменты для организации таких подключений - Remote Desktop (Удаленный рабочий стол) и Remote Assistance (Удаленный помощник).

Различие этих утилит вытекает из их названий - удаленный рабочий стол позволяет, находясь за одним компьютером, удаленно управлять другим, а удаленный помощник предназначен для оказания помощи в интерактивном режиме. В данном приложение рассмотрим только одну из этих утилит, а именно Remote Desktop.

Работа Remote Desktop реализуется применением технологии Terminal Services (Службы терминалов) и протокола RDP. При этом компьютер, к которому выполняется подключение, выступает в роли сервера терминалов. Это позволяет запускать приложения на компьютере с ОС Windows XP Professional с любого компьютера-клиента, работающего в среде Windows. Подключение возможно с использованием локальной сети, VPN, или интернет-соединения. На возможность комфортной работы значительное влияние оказывает пропускная способность соединения.

При установлении соединения в Windows XP Remote Desktop производит вывод из сеанса текущего пользователя. Это значит, что он не сможет наблюдать за действиями пользователя, установившего соединение. При передаче звука, если пропускной способности канала связи недостаточно, Remote Desktop изменяет его качество, снижая нагрузку на сеть. Помимо передачи изображения удаленного рабочего стола и звука, при использовании протокола RDP возможно подключение в качестве сетевых ресурсов дисков и принтеров локального компьютера и его портов, совместное использование буфера обмена. Для снижения объема передаваемых по сети данных можно изменять разрешение и количество цветов дисплея.

Замечание:

Как и любое удаленное подключение, использование Remote Desktop необходимо обеспечить соответствующим уровнем безопасности.

п1.1. Настройка требуемого уровня безопасности

Для изменения уровня безопасности собственной системы используется оснастка групповой политики консоли MMC. При настройке нужного уровня безопасности следует:

- Запустить консоль, для чего выбрать Пуск -> Выполнить -> Набрать gpedit.msc -> Нажать кнопку ОК.

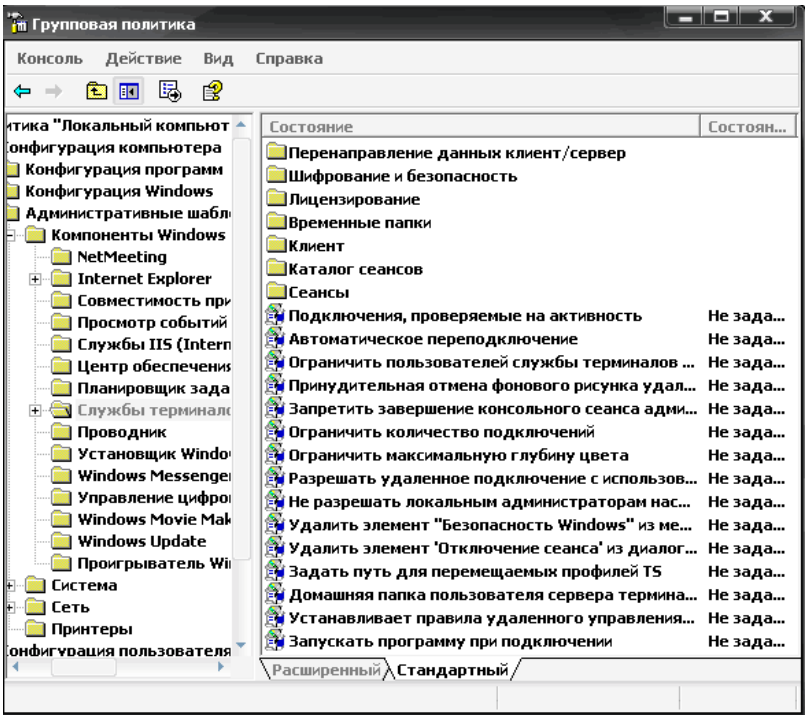


Рис.5.29. Оснастка групповая политика.

- Выбрать в левой части консоли Конфигурация компьютера -> Административные шаблоны -> Компоненты Windows -> Службы терминалов.
- Здесь вы можете задать, например, такие параметры как:
    - разрешение/запрет совместного использования буфера обмена
    - задать уровень шифрования передаваемых данных
    - разрешение/запрет перенаправления данных на локальные COM, LPT порты, принтеры
    - установить необходимый уровень шифрования передаваемых данных
    - требовать ввода пароля при каждом подключении вместо его автоматической подстановки

    Для получения справки по настройке какого-либо параметра, откройте его двойным щелчком мыши и перейдите на закладку «Объяснение».

Для создания соединения с помощью Remote Desktop обязательно необходима учетная запись с непустым паролем. Кроме этого для использования Remote Desktop необходимо установить и правильно настроить сервер удаленного рабочего стола на том компьютере, с которым необходимо устанавливать соединение.

п1.2. Подключение по локальной сети

Разрешаем удаленные подключения к компьютеру. Для этого:

- Заходим в свойства системы: Пуск - Панель управления - Система. Переходим на закладку "Удаленные сеансы" (рис. 5.3).
- Отмечаем флажок "Разрешить удаленный доступ к этому компьютеру".

  Администраторы этого компьютера получают доступ автоматически.

- Если необходимо предоставить доступ пользователю, не входящему в группу администраторов, щелкните кнопку "Выбрать удаленных пользователей".

    - В открывшемся диалоге "Пользователи удаленного рабочего стола" щелкните кнопку "Добавить".
    - Если необходимо указать пользователя другого компьютера сети с Active Directory, укажите место поиска, нажав кнопку "Размещение".
    - Далее щелкаем кнопки "Дополнительно", затем "Поиск".
    - Выберите учетные записи пользователей, которым необходимо предоставить удаленный доступ.
    - Нажмите "ОК" для закрытия всех диалоговых окон.
- Если компьютер защищен файрволлом, необходимо будет разрешить подключения по RDP-протоколу (по умолчанию – порт 3389).

С настройкой сервера мы закончили, перейдем к клиенту – тому компьютеру, с которого планируется производить подключение. Как правило, инструмент "Подключение к удаленному рабочему столу" устанавливается в Windows XP автоматически.

Но все же, стоит проверить, установлен он или нет – его установку мог отменить администратор. Для этого выберите Пуск –> Все программы –> Стандартные –> Связь. Если "Подключение к удаленному рабочему столу" в списке отсутствует, необходимо его установить. Для установки понадобится диск Windows XP.

- Установить диск в привод компакт-дисков.
- Когда появится заставка, выбрать "Выполнение иных задач".
- После этого переходим к режиму "Установка удаленного управления рабочим столом".

Запускаем "Подключение к удаленному рабочему столу" (рис. 5.5) и выбираем компьютер, к которому необходимо подключится. Можно воспользоваться выбором из списка, нажав кнопку с направленной вниз стрелкой в поле «Компьютер» или набором указать либо имя компьютера, либо его IP-адрес.

- Если компьютер отсутствует в списке, выберите строку «Поиск других». В этом случае будет выведен список компьютеров домена или рабочей группы с установленным Remote Desktop.
- Впрочем, возможна ситуация, когда при попытке поиска появляется сообщение, что в сети нет серверов терминалов. Если вы уверены, что сервер настроен правильно, введите вручную имя или IP-адрес необходимого компьютера.
- Если соединение не устанавливается, необходимо будет проверить работоспособность сети и убедится, что компьютер, с которым вы пытаетесь установить соединение, включен.

Перед подключением можно задать дополнительные параметры, нажав кнопку «Параметры». При этом в окне диалога появляются пять закладок, на которых устанавливаются дополнительные параметры соединения (рис. 5.6).

- На вкладке «Общие» можно указать пользователя, пароль и домен, к которому будет производится подключение.

  Для установки соединения в полностью автоматическом режиме установите флажок «Сохранить пароль» и нажмите кнопку «Сохранить как…». Разместив созданный файл соединения (пароль в нем шифруется), например, на рабочем столе, достаточно будет произвести по нему щелчок мышью, и соединение с удаленным компьютером будет установлено.

- На закладке «Экран» устанавливаются параметры отображения удаленного рабочего стола – размер стола, глубину палитры отображаемых цветов.

  Здесь также можно установить параметры отображения панели подключения в полноэкранном режиме. По умолчанию, если вы развернули рабочий стол во весь экран, вверху отображается панель, позволяющая мышью изменить размер окна удаленного рабочего стола, свернуть или закрыть его.

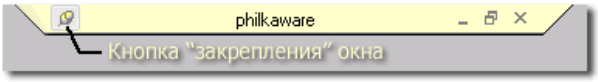


  Рис.5.30. Панель окна.

- Закладка «Локальные ресурсы».

  Здесь можно настроить перенаправление ресурсов удаленного и локального компьютеров. Вероятно, не для всех приложений будет важна передача звука. Если это так, можно ее отключить для снижения объема передаваемых данных.

  На этой же закладке можно настроить поведение при нажатии сочетаний «горячих клавиш». Один из наиболее важных разделов настроек – «Устройства». Установкой соответствующего флажка задаются устройства компьютера, инициирующего подключение, которые будут подключены к удаленному компьютеру. Например, при включении режима «Дисковые устройства» при входе на удаленный компьютер локальные диски будут подключены в качестве сетевых.

  Вам даже не придется настраивать разрешения доступа к дискам. Система перед подключением в таком режиме выдаст сообщение о снижении уровня безопасности при таком виде подключения. Вы можете отказаться от подключения или продолжить его установление. Таким же образом вы можете подключить локальные принтеры (например, вам необходимо будет распечатать что-нибудь с удаленного компьютера) и порты.

- Закладка «Программы» позволит запускать предопределенную программу при входе на удаленный компьютер и задавать рабочий каталог.
- Закладка «Дополнительно» целиком отвечает за параметры быстродействия сеанса связи.

  Вы можете выбрать из списка характеристики и способ соединения, наиболее соответствующий фактическому виду подключения. При этом будут автоматически выставлены параметры, влияющие на скорость передачи «полезных» данных – таких, например, как отображение визуальных эффектов и тем, рисунка рабочего стола и т. п. Вы также можете вручную отредактировать необходимые параметры.

Remote Desktop-сервер позволяет устанавливать несколько одновременных удаленных подключений. Для входа на компьютер, на котором уже запущена сессия пользователя, необходимо произвести вход либо под учетной записью пользователя, чей сеанс уже запущен, либо использовать учетную запись, входящую в группу Administrators на удаленном хосте. Важно при этом помнить, что пользователь, находящийся перед компьютером, к которому производится подключение, не сможет в этот момент работать на нем. Если же он войдет в систему, соединение будет разорвано, а удаленный пользователь получит такое сообщение:

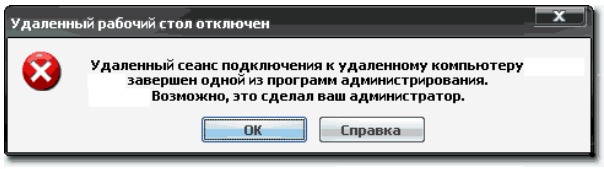


Рис.5.31. Отключение сеанса.

Замечание:
Для подключения к удаленному рабочему столу можно использовать не только Windows XP Professional, но и более ранние версии Windows. Для этого необходимо загрузить с сайта Microsoft клиент msrdpcli.exe(http://www.microsoft.com/windowsxp/downloads/tools/rdclientdl.mspx) или скопировать из папки \Support\Tools компакт-диска Windows XP.

п1.3. Интернет-подключение

Для установления соединения через сеть Интернет, необходимо установить на сервере компонент Remote Desktop Web Connection (Интернет-подключение к удаленному рабочему столу). Этот компонент является частью IIS (Информационные службы интернета). Если на компьютере установлена эта служба, для подключения достаточно будет использовать браузер Internet Explorer версии 4.0 или выше.

Проверьте, установлен ли в системе этот инструмент. Для этого откройте диалоговое окно «Установка и удаление программ» (Пуск – Панель управления). В левой области окна выберите раздел «Установка и компонентов Windows. Выбираем Internet Information Services (IIS), нажимаем кнопку «Состав…». Далее выбираем «Служба WWW», снова нажимаем «Состав…».

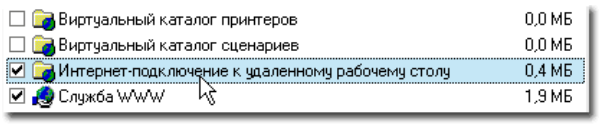


Рис.5.32. Установка веб-служб.

Установите флажок напротив строки «Интернет-подключение к удаленному рабочему столу». Автоматически будет отмечена и «Служба WWW», поскольку она является необходимым компонентом установки. Нажимаем «ОК», закрывая окна. В окне мастера установки компонентов Windows нажмите «Далее». Вам может потребоваться установочный компакт-диск Windows XP. После завершения установки нажмите «Готово». Закрываем окно установки программ. Теперь настроим доступ к компьютеру. Сделайте правый щелчок мышью на значке «Мой компьютер» и выберите строку «Управление». Откроется консоль управления компьютером. Нам необходимо проверить свойства папки tsweb, куда устанавливаются службы IIS.

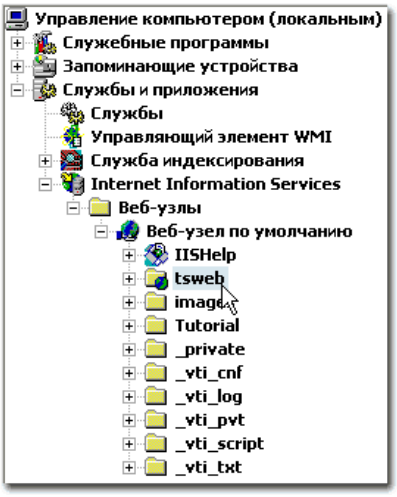


Рис.5.33. Каталог веб-узла.

Сделайте правый щелчок мышью на строке tsweb. Выберите «Свойства» и перейдите на закладку «Безопасность каталога». В разделе «Анонимный доступ и проверка подлинности» нажмите кнопку «Изменить».

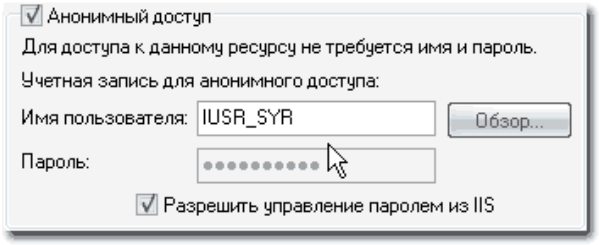


Рис.5.34. Разрешения доступа.

Убедитесь, что установлен флажок «Анонимный доступ».

При установке IIS система автоматически создаст пользователя IUSR – гостевую запись для обработки запросов от анонимных пользователей web. Это учетная запись с низким уровнем привилегий. Поскольку эта запись обрабатывает анонимные запросы к веб-ресурсам, права доступа будут определяться разрешениями NTFS. Если в системе работает файрволл и/или применяется технология переадресации NAT, для установки интернет-соединения необходимо разрешить подключение по 80-му порту и настроить перенаправление входящих подключений с этого порта на компьютер.

Итак, для Интернет-подключения к удаленному рабочему столу нам понадобится любой компьютер, имеющий доступ в Интернет с браузером Internet Explorer версии 4.0 или выше. Открываем IE, вводим в строку адреса URL Remote Desktop-сервера. Если компьютер не имеет DNS-имени, можно ввести его «белый» IP-адрес (в случае, если компьютер находится за NAT, необходимо указать IP-адрес маршрутизатора). Строка адреса должна содержать путь к папке страницы доступа. Если вы ничего не меняли в настройках, URL должен выглядеть таким образом:

http://computername/tsweb

где computername – DNS-имя или IP-адрес компьютера, к которому производится подключение. В папке tsweb (локально она расположена здесь - C:\WINDOWS\Web\TSWeb) находится архив msrdp.cab, в который упакован одноименный элемент управления, отвечающий за организацию связи клиента и сервера через web-сеть. При первом

соединении браузер попытается установить этот элемент как надстройку IE. Пользователь при этом получит запрос на установку элемента ActiveX. Подтверждаем установку, в результате, если все работает верно, мы должны увидеть в браузере веб-страницу такого вида:

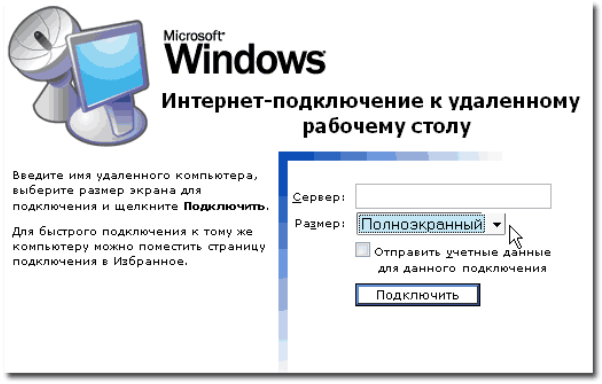


Рис.5.35. Интернет-подключение.

Выберите размер окна, в которое будет выводится удаленный рабочий стол. Можно указать сервер и, при установке флажка, ввести учетные данные. Осталось лишь нажать кнопку «Подключить» (если кнопка не «нажимается», скорее всего, либо не установлен ActiveX-элемент, либо в браузере запрещено выполнение сценариев). Далее последует привычный вход в систему, ничем не отличающийся от локального. Если размер окна был установлен не полноэкранным, то вы сможете в течении сессии изменять его размеры, как у любого Windows-приложения.

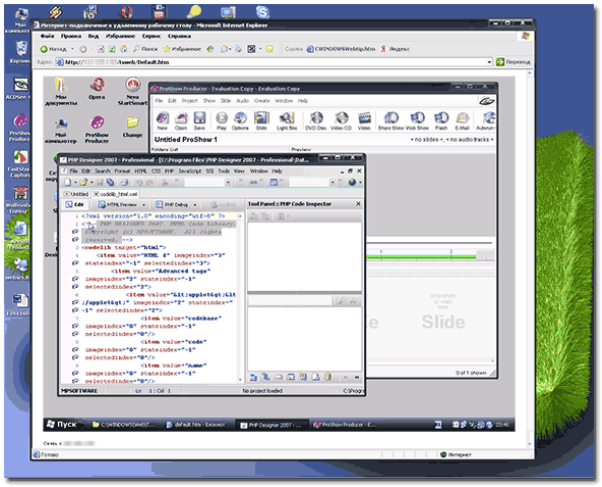


Рис.5.36. Вид работы Интернет-подключения.

Если необходимо во время Интернет-сессии подключить локальные диски в качестве сетевых, придется «подправить» содержание веб-страницы, к которой производится RDP-подключение. По умолчанию, эта страница расположена здесь - C:\WINDOWS\Web\TSWeb\default.htm. Откройте ее в любом текстовом редакторе. Найдите строку с текстом

MsRdpClient.AdvancedSettings2.RedirectDrives = FALSE

и измените FALSE на TRUE. Таким же образом можно изменить параметры RedirectPrinters, RedirectPorts и RedirectSmartCards, отвечающие соответственно за принтеры, порты и смарт-карты.

В обоих вариантах подключения – LAN и веб, вы можете, помимо совместного использования файлов, обмениваться информацией стандартными операциями через буфер обмена (Копировать/Вставить). Для окончания терминальной сессии достаточно закрыть окно веб-браузера.

Рассмотренные средства ОС Windows XP позволяют повысить производительность совместной работы, не прибегая к установке стороннего ПО.

Лабораторная работа №5.

«Использование протокола ftp при работе в Интернет»

Цель работы

Ознакомиться с доступом к информации в сети Internet посредством протокола **ftp .** Получить навыки проверки соединений в сети Internet.

Подготовка к работе

1. Ознакомиться *с* **ftp** форматом команд **ping, tracert.**

2. Изучить основные команды текстового ftp-клиент.

3. Научиться работать с графическим ftp-клиентом **FlashFXP**.

Содержание работы

1. Определить возможность установления соединения вашего компьютера с другим компьютером в локальной или глобальной сети, используя команду *ping*. Проверить соединение с :

• **10.0.232.223** – ftp сервер кафедры ИСТ и ПО

• **server04** – локальный файловый сервер.

2. Установить ftp соединение с одним из ftp-серверов, используя текстовый ftp-клиент **ftp.exe:**

• **10.0.232.223**

3. Используя команды cd и Is найти любой не очень большой файл.

4. Скопировать файл с ftp-сервера в локальную папку.

5. Скопировать любой файл из локальной папки на ftp-сервер.

6. Убедиться, что файлы успешно скопированы.

7. Прекратить сеанс связи с сервером и выйти из ftp системы.

8. Используя графический ftp-клиент **FlashFXP** подключиться к серверу.

9. Проследить путь следования IP-пакета от компьютера локальной сети к какому-либо удаленному серверу используя команду **tracert.exe.** Записать весь путь в отчет.

10. Оформить отчет, (используя Word или даже Notepad)

Содержание отчета

Отчет должен содержать:

1. Цель работы

2. Результат проверки соединений с серверами.

3. Адрес удаленного сервера, путь к файлу, имя файла,
скопированного на локальный сервер с помощью текстового ftp-клиента,
время и скорость передачи файла.

4. Весь путь следования IP-пакета до удаленного сервера.

5. Выводы

Выполнение работы

1. Для запуска программы в среде Windows NT/9x выполните
следующие действия:

• нажмите левой кнопкой мыши на кнопке **Пуск.**

• выберите пункт **«Выполнить»** и нажмите левую кнопку мыши

• в появившемся окне в поле **«Открыть»** введите имя выполняемой
программы (можно также указать исполняемый файл с помощью
кнопки **«Обзор»).**

• Нажав «Enter» запустите программу на исполнение.

2. Для проверки наличия и качества сетевого соединения с удаленной
системой используется команда Ping.

Эта утилита (команда) отсылает запрос (несколько байт) на требуемый компьютер и ожидает ответа, определяя при этом время следования запроса и ответа.

Формат этой команды следующий:

ping [-t] [-a] [-n count] [-1 size] [-f] [-w timeout] список адресов

Параметры:

-t Отправка пакетов на указанный узел до команды

прерывания

-a Определение адресов по именам узлов.

-n count Количество запросов

-1 size Размер посылаемого пакета

-f Установка флага, запрещающего фрагментацию пакета.

-w timeout Время таймаута в миллисекундах.

После запуска программы на экране будет показываться время установки связи с заданным компьютером, если связь отсутствует и/или превышено заданное время таймаута, то в окне будет возникать сообщение «Request timeout» или «Destination host unreachable».

3. Для запуска текстового ftp-клиента в окне запуска введите «ftp. exe» и нажмите клавишу Enter. Появляется подсказка: «ftp>». Для получения подсказки по командам введите «help» или «?». Подробно назначение команд описано в разделе «Протокол ftp» данного методического пособия.

=Протокол FTP

В отличие от **Telnet,** протокол **FTP** (File Transfer Protocol) предназначен не для работы на удаленном компьютере, а для передачи файлов между подключенными к сети компьютерами. Так же как и **Telnet,** сервис FTP основан на совместном использовании двух программ — программы-сервера, которая выполняется постоянно в фоновом режиме на удаленном компьютере, и программы-клиента, которую вы должны запустить на своем компьютере, чтобы начать сеанс работы по протоколу FTP. Программа сервер занимается обработкой всех запросов, приходящих к ней от программы-клиента, поэтому если программа-сервер не предоставляет каких-либо возможностей вроде докачки и т. д., то каким бы навороченным клиентом вы ни пользовались все равно данные возможности так и останутся недоступными для вас. Протокол FTP позволяет передавать файлы как в текстовом, так и в двоичном формате между совершенно различными платформами.

Анонимный FTP

Обычно для передачи файлов между компьютерами вы должны войти в систему через **login** и иметь в них определенные права доступа к файлам, а также к FTP программе, запускаемой на обоих компьютерах. Но многие системы предлагают анонимные FTP серверы, то есть серверы с практически свободным доступом. Работая с серверами такого типа, вам не нужно иметь специального имени и пароля для установления соединения и передачи файлов. На анонимном сервере вы используете в качестве своего имени *"anonymous",* а в качестве пароля - свой e-mail адрес. Однако следует помнить, что используя анонимное соединение, вы, скорее всего, не сможете создавать, удалять, переименовывать файлы и каталоги, для этого нужно иметь пользователя на этом сервере с соответствующими правами.

Если вы хотите установить соединение с компьютером, не предоставляющим анонимного сервиса FTP, вы должны иметь права доступа к системе, т. с. иметь собственное имя пользователя и пароль.

Анонимные FTP-серверы - одно из главных средств

распространения программного обеспечения и информации в **Internet.** Большое количество программного обеспечения, часто предоставляемого

бесплатно, доступно на анонимных FTP-сервсрах. Наиболее известными анонимными FTP-серверами, содержащими очень большое количество различных ресурсов являются **ftp.cdrom.com, ftp.funet.fi. ftp.download.com.**

Использование текстового FTP-клиента

Чтобы получить FTP-доступ по адресу **ftp.radiant.ru** необходимо набрать в командной строке выражение **ftp.radiant.ru.**

После установления соединения с FTP-сервером вам необходимо зарегистрироваться на удаленном компьютере либо как пользователь со своим именем, либо как анонимный пользователь. Для этого в ответ на соответствующий запрос нужно ввести ваше имя пользователя или "anonymous" и пароль. Если вы устанавливаете соединение с анонимным FTP-сервером, вы можете использовать в качестве пароля любую последовательность символов (но вообще при этом в качестве пароля принято вводить свой e-mail адрес).

Большинство FTP-программ, работающих из командной строки, имеют стандартный набор команд. Наиболее полезные команды приведены ниже.

! [команда[аргументы)|

Выход в shell - интерпретатор на локальной системе.

ascii

Переключает в режим передачи текстовых файлов (обычно по умолчанию).

bin (или binary)

Переключает в режим передачи двоичных файлов

bye

Оканчивает работу с FTP сервером и приводит к выходу и из интерпретатора.

cd [удаленная_директория|

Сменить директорию. Существуют также **'cdup'** или **'cd'** для возврата на один или выше

close

Обрывает PTP сеанс с удаленным сервером и возвращает к командному интерпретатору

delete (удаленный файл)

Стирает удаленный файл

dir [удаленная директория] [локальный_файл]

Is [удаленная директории] [локальный файл]

Выводит список файлов в директории либо не стандартный вывод, либо, если указано имя локального файла, в этот файл, **(dir** -вывод с дополнительной информацией).

get [удаленный_файл] [локальный_файл]

Вызывает передачу копии удаленного файла на ваш компьютер. В случае, если имя локального файла не было задано, то оно совпадает с именем удаленного файла.

hash

Служит переключателем для индикации каждого полученного блока данных в 1024 байта, повышает наглядность процедуры.

lcd

Меняет рабочую директорию на локальной машине (без аргумента - переход в домашнюю директорию пользователя)

mget [удаленные_файлы]

Для получения нескольких файлов

mkdir [имя директории]

Создает директорию на удаленной машине

open хост [порт]

Устанавливает соединение с заданным FTP сервером

prompt

Переключает интерактивную подсказку. Часто при использовании команды **'mget'** желательно предварительно набрать **'prompt',** чтобы не давать многократные подтверждения.

put [локальный файл) [удаленный файл]

Пересылает файл на удаленную систему. Если имя удаленного файла не указано, то оно совпадает с именем на локальной системе.

pwd

Выводит имя удаленной рабочей директории.

Quit

Синоним для 'b**ye'**

recv [удаленный файл] [локальный файл]

Синоним для команды 'get'

reget [удаленный_файл] [локальный файл]

"Дополучение" удаленного файла в том случае, когда часть его уже есть на локальной машине. Команда особенно полезна для получения больших файлов при возможных разрывах соединения, (поддерживается не всеми серверами и клиентами).

При большом количестве файлов перебор их имен - утомительная задача. Порой трудно перечислить 5-6 файлов, а если их сотня?

Выход есть. Существует система шаблонов, которую лучше всего изучать на примерах. Перед этим объяснение специальных знаков:

Символ '*' обозначает любой набор символов.

Символ "?' обозначает один любой символ.

Примеры:

abc* - все файлы, начинающиеся на **abc**

abc? - все файлы, имеющие длину имени в четыре символа, начинающиеся на abc и заканчивающиеся на любой символ.

??abc? - файлы с именем в шесть символов, 3,4,5 символы abc и остальные любые.

*abc - все файлы, оканчивающиеся на **abc**

* - все файлы

Учтите, что большие и маленькие буквы РаЗлИчАюТсЯ.

Необходимо знать, что в распечатке команды **Is** первые десять знаков (например: **-rwxrwxrwx)** - это биты доступа к файлу или директории. Для вас

представляет интерес только первый символ. Если это '-', то он обозначает файл, если 'd' - то директорию.

Так например в строке:

-rw-r--r-users 11479 Janfilename.ext

«-rw-r--r--» - атрибут файла; **«filename.ext»** - имя файла; **«11479»** - размер файла; **«Jan»** - дата создания файла.

Пример работы с текстовым FTP-клиентом

Итак, вы загрузили FTP-клиент. Для того, чтобы начать сеанс обмена с сервером, необходимо сначала открыть соединение. Для этого существует

команда **open** имя_сервера

Слово **open** можно сократить до одной буквы о. Итак, попробуем:

ftp> o 192.168.1.1

Подождите несколько секунд пока компьютеры совершат соединение.

Теперь надо зарегистрироваться. Увидев приглашение **login:,** наберите слово **anonymous.** Нажмите Enter и введите свое имя, затем символ @ (без пробелов) и адрес вашей локальной машины. Если все сделано правильно, то появится сообщение о том, что вы вошли в систему.

Теперь вы можете копировать себе те файлы, доступ к которым вам определен как анонимному пользователю. Советуем начать исследование сервера с каталога **/pub,** так как обычно все полезные файлы помещаются именно сюда. Сейчас же вы находитесь в самом верхнем, так называемом root-каталоге. Для того, чтобы перейти в нужный каталог существует команда cd.

Например, в каталог **pub** текущего каталога можно перейти:

ftp> cd pub

Получить список файлов в текущем каталоге можно командой **dir:**

ftp> dir

Если в появившемся списке первым символом в строке является 'd', то в строке имя каталога, если '-' - имя файла.

Предположим, что вы нашли файл, который хотите переписать себе. Прежде, чем сделать это, надо установить двоичный режим передачи файлов **binary:**

ftp> binary

Возьмите себе за правило: как только соединитесь с сервером, сразу вводить эту команду. Если этого не сделать, то файл будет перекодирован и непригоден для использования (если только это не текст на английском языке). При появлении во время копирования файла сообщения 'Opening ASCII mode to transfer file' немедленно прервите передачу файла и запустите **binary.** Многие современные FTP-клиенты автоматически посылают эту команду.

Пересылает файл на локальный компьютер команда **get:**

ftp> get the_file_i_like. zip

Если Вы сразу захотите положить файл в определенное место на локальном компьютере, то укажите путь как второй аргумент команды:

ftp> get the_file_i_like. zip /x/xxx/my_new_file. zip

По умолчанию FTP-клиент кладет файл в текущую директорию на локальном диске.

Для FTP-клиента под Windows этой директорией будет каталог Windows. (Не забудьте перед загрузкой клиента проверить, достаточно ли у вас прав для записи в этот каталог. В противном случае вам придется явно указывать путь в каждой команде get).

Можно переписать содержимое сразу всего каталога, для этого надо указать его имя в команде get.

Зачастую требуемая информация расположена не в одном, а в нескольких файлах.

Для их пересылки можно использовать команду **mget,** которая понимает шаблоны групповых операций. В некоторых реализациях FTP-клиентов шаблоны групповых операций можно использовать и в команде get.

Теперь, когда файл копируется, можно отдохнуть. Время ожидания зависит от размера файла и возможностей вашего подключения к Internet.

Когда пересылка файлов будет закончена, FTP-клиент сообщит вам об этом, указав сколько байт и за какой срок было принято, подсчитав среднюю скорость передачи. Теперь можно выходить из FTP-клиента (при выходе он автоматически закроет соединение с сервером) и пользоваться этими файлами, так сказать, в домашних условиях.

Использование графического FTP-клиента FlashFXP

Как вы могли убедиться текстовые FTP-клиенты не блещут особым удобством пользования или простотой обращения. Когда вычислительных ресурсов машин не хватало на что-то большее, приходилось этим довольствоваться, но с появлением всевозможных графических ОС (или графических оболочек для ОС) стали появляться и FTP-клиенты, работающие со многими наворотами данных ОС. Работа с графическим FTP-клиентом доставляет куда большее удовольствие, чем работа в текстовом режиме. В данной лабораторной работе нами будет рассмотрена программа **FlashFXP,** отличающаяся невысокими требованиями к ресурсам, сравнительно небольшим размером дистрибутива, удобством пользования (поддержка докачивания прерванных файлов, возможность создания очереди с указанием времени старта и т. д.) и красотой исполнения.

Контрольные вопросы

1. Объясните назначение и формат команды **ping.**

2. Для чего предназначен протокол **ftp**, в чем его отличие от других протоколов?

3. В чем особенности анонимного **ftp**-подключения?

4. Назовите основные команды, которые используются при ftp-соединении. Расскажите их назначение.

5. Объясните, для чего нужны графические **ftp**-клиенты?

6. Отличаются ли друг от друга графические и текстовые **ftp**-клиенты на уровне команд, посылаемых серверу? Почему?

7. Объясните назначение панелей и окон в основном окне **FlashFXP**.

8. Что такое «удаленный каталог», «удаленная машина»?

9. Как можно просмотреть файл, расположенный на удаленной машине?

10. Перечислите преимущества работы с **FlashFXP.**

11. Для чего компьютеру необходим IP - адрес?

12. Что позволяет узнать утилита **tracert?**

Лабораторная работа № 6

Тема: «Создание виртуальной локальной сети.»

1 ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНОЙ РАБОТЫ

1.1 Цель работы: знакомство с программами организации виртуальной сети

1.2 В результате выполнения лабораторной работы студент должен знать:

- Особенности программ организации виртуальной сети

1.3Используемые программно-технические средства:

Персональная ЭВМ класса IBM PC стандартной конфигурации; операционная система Windows2000/XP/Vista, MicrosoftOfficeWord.

1.4В процессе выполнения лабораторной работы студент должен:

- Ознакомится с теоретическим материалом.
- Подготовить отчет по лабораторной работе.
- Отчитаться по исполненному заданию.

Перед выполнением лабораторной работы каждый студент обязан изучить правила техники безопасности при работе в помещении с электронно-вычислительной техникой.

1.5 Указания по оформлению отчета:

Отчет должен содержать: титульный лист, цель работы; ответы на контрольные вопросы; выводы.

1.6 Указания по сдаче зачета преподавателю

Для сдачи зачета необходимо:

1) выполнить практическое задание

2) предъявить отчет;

3) ответить на контрольные вопросы.

2 Теоретические сведения

Владельцы домашних ПК нередко сталкиваются с необходимостью объединить несколько компьютеров в локальную сеть, однако в силу ряда причин (удаленность друг от друга и т. д.) это бывает неосуществимо привычными способами. И тут на помощь придут специализированные утилиты, умеющие создавать виртуальные локальные сети между пользователями, подключенными к Интернету.

Самая очевидная область применения таких утилит – многопользовательские игры, не поддерживающие онлайновый режим, однако только ими дело отнюдь не ограничивается. Имеются все обычные вещи, доступные в локальной сети: просмотр содержимого папок с открытым доступом, работа с сетевыми принтерами, прослушивание библиотеки iTunes других пользователей и даже управление чужими компьютерами с помощью встроенных средств Remote Desktop.

LogMeIn Hamachi²

Freeware (для некоммерческого пользования)

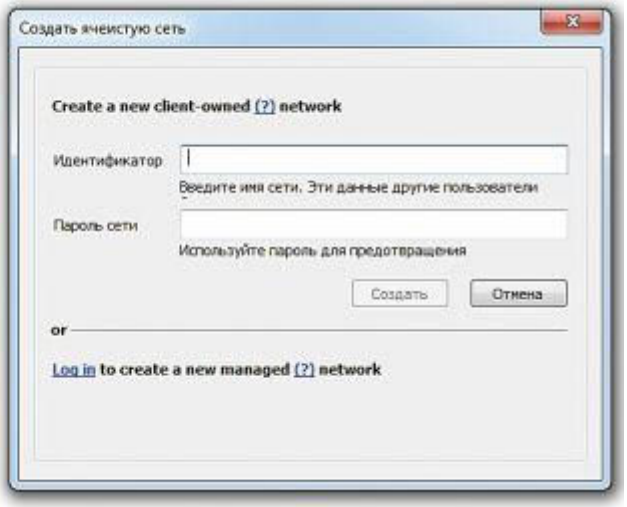
Разработчик LogMeIn

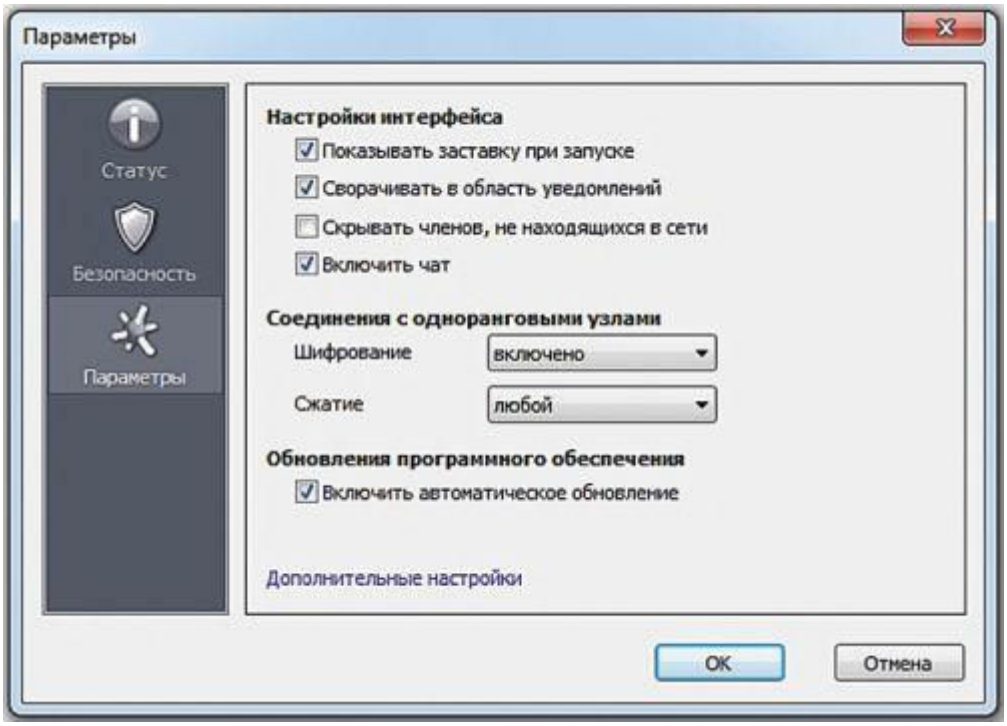
Сайт secure.logmein.com/products/hamachi2

Размер 3,1 МБ

Адрес загрузки secure.logmein.com/products/hamachi2/download.aspx

Работает и без учетной записи; присутствуют способы отображения реальных сетевых ПК в виртуальном окружении





Hamachi долгое время остается самой популярной утилитой для создания виртуальных сетей. Правда, после того как ее приобрела крупная компания

LogMeIn, специализирующаяся на сетевом ПО, появились определенные опасения за ее будущее, но, к счастью, они оказались напрасными – для некоммерческого применения программа остается бесплатной, с ограничением на 16 клиентов в сети. Если же есть необходимость подключать большее количество человек, стоит подумать о приобретении лицензии, позволяющей использовать утилиту для соединения 256 компьютеров. Обойдется такая возможность в $200 в год.

В отличие от рассмотренной ниже EasyVPN, Hamachi можно применять и без создания аккаунта: нажатием всего одной кнопки пользователь подключается к серверу и получает IP-адрес. Далее процедура создания виртуальной сети или подключения к уже существующей выглядит точно так же, как и в Comodo.

Отметим некоторые преимущества тех, кто не поленился потратить несколько минут на получение бесплатного аккаунта. В этом случае им не придется каждый раз заново настраивать программу на новом ПК, также они получат возможность управлять своей учетной записью через веб-интерфейс.

В режиме работы без авторизации, который называется *Mesh*, видны лишь компьютеры, ассоциированные с виртуальной сетью. При наличии же учетной записи появляется режим *Gateway virtual networking*, позволяющий им получать доступ ко всем ресурсам настоящей локальной сети другого пользователя. В режиме *Hub-and-spoke* можно работать лишь с избранными ПК в реальной сети.

Обратите внимание, что в Hamachi отсутствует функция управления удаленным Рабочим столом, поскольку для этого у LogMeIn существует отдельная утилита. Также программа может включать/выключать шифрование и сжатие трафика.

Одной из самых интересных возможностей Hamachi является создание с помощью веб-интерфейса специального инсталлятора утилиты, который умеет автоматически добавлять других пользователей в необходимую виртуальную сеть. Получить такой дистрибутив можно после несложных операций на сайте, использовать ссылку на программу позволяется многократно.

Comodo EasyVPN

Freeware (для некоммерческого пользования)

Разработчик Comodo

Сайт easy-vpn.comodo.com

Размер 6,44 МБ

Адрес загрузки easy-vpn.comodo.com/download.html

Богатая функциональность; простая настройка

Невозможность использовать одну и ту же учетную запись на нескольких ПК одновременно

Comodo EasyVPN – относительно новая разработка компании, известной несколькими хорошими и при этом бесплатными для некоммерческого применения программами (Comodo Firewall, Comodo Backup, Comodo Antivirus и др.). Не стала исключением и утилита для создания виртуальной сети, которая также распространяется бесплатно.

К достоинствам EasyVPN сразу отнесем простой удобный интерфейс и несложную настройку виртуальной сети. Пользователю необходимо завести аккаунт – возможно, это не очень удобно, зато позволит забыть о повторной настройке программы (все старые опции подхватятся заново даже после ее установки на новом ПК). К сожалению, зайти под одной учетной записью с нескольких компьютеров одновременно не получится – при ее активации на одном ПК другой будет автоматически отсоединен от сервера. Это происходит по причине того, что к учетной записи привязан один конкретный статический IP-адрес.

Comodo EasyVPN позволяет не только создавать виртуальные локальные сети для игр, но и имеет встроенный чат с функцией передачи файлов по защищенному каналу (впрочем, по умолчанию шифруется абсолютно весь трафик, а не одни файлы). Также частью EasyVPN является возможность удаленного управления ПК, причем все эти дополнительные опции не нуждаются в особых настройках – к примеру, для активации Remote Desktop требуется буквально одно нажатие на локальном компьютере и подтверждение на открытие доступа от пользователя на другом конце провода. В настройках можно выставить параметр соотношения качества картинки/скорости передачи.

EasyVPN также предусматривает развертывание закрытых виртуальных сетей, защищенных паролем, и дает возможность отключать шифрование трафика.

Работает утилита Comodo только в среде Windows, однако поддерживает все последние редакции ОС Microsoft, включая 64-битовые версии.

Remobo

Freeware

Разработчик AWIT Systems

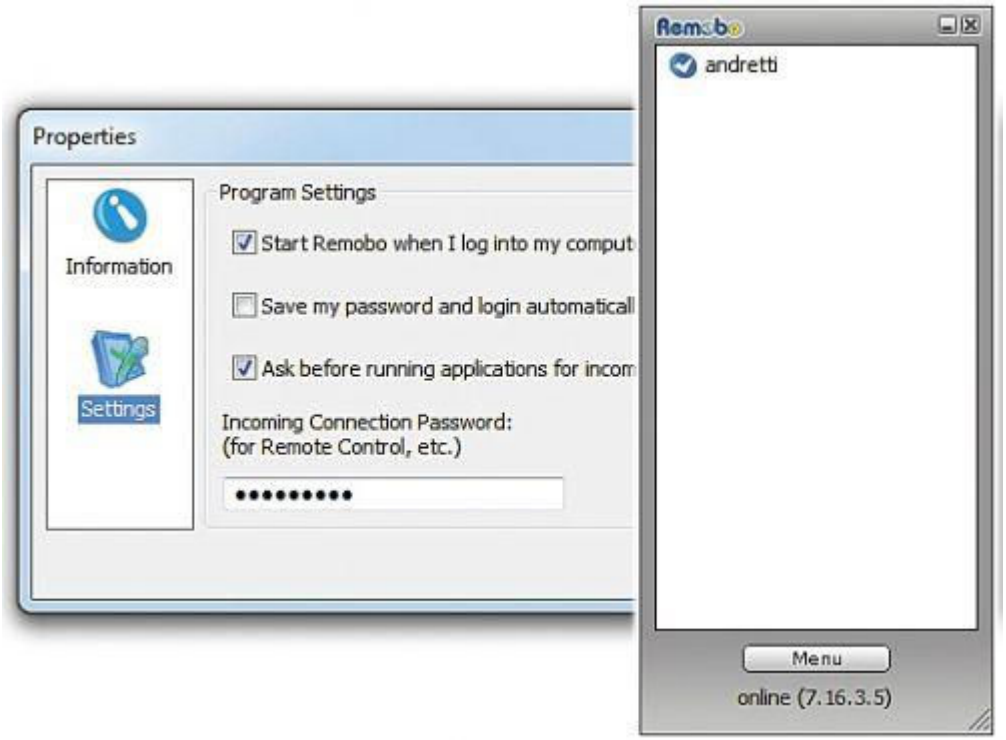
Сайт www.remobo.com

Размер 12,2 МБ

Адрес загрузки www.remobo.com/download.php

Поддержка BitTorrent для обмена файлами; запуск на нескольких ПК под одной учетной записью

Непривычный интерфейс



Утилита Remobo сейчас находится в стадии бета-тестирования, поэтому любые функции программы доступны всем желающим. В будущем, правда, планируется ввести премиум-аккаунты со специфическими возможностями, однако бесплатные базовые учетные записи останутся по-прежнему доступны любым пользователям.

В целом Remobo функционально повторяет своих конкурентов, хотя и выглядит несколько слабее. Одной из особенностей данной программы является специфическая опция обмена файлами – достаточно добавить в список нужный набор папок и файлов, и они становятся доступны для просмотра и скачивания другим пользователям. Самое интересное, что обмен информацией происходит по протоколу BitTorrent, для этого вместе с программой даже устанавливается одноименный клиент. Такое решение способно увеличить

скорость обмена данными, если одни и те же файлы доступны на разных компьютерах сразу нескольких пользователей.

В Remobo также встроены утилита для удаленного управления Рабочим столом и программа для обмена сообщениями.

Работает Remobo в Mac OS X и Linux, поддерживает 64-битовые версии Win-dows. В отличие от Comodo EasyVPN она позволяет использовать одну учетную запись для запуска программы сразу на нескольких компьютерах – таким образом, пользователь может объединить в виртуальную сеть все свои машины.

Wippien

Freeware (open source)

Разработчик

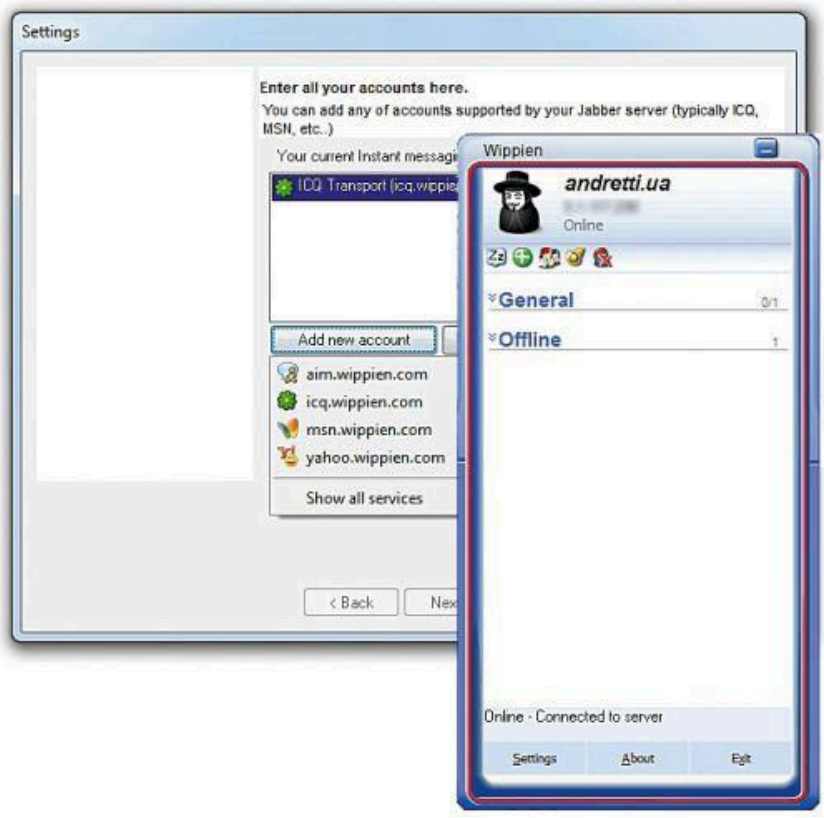
Сайт www.wippien.com

Размер 1,92 МБ

Адрес загрузки www.wippien.com/download.php

Поддержка распространенных протоколов обмена сообщениями; возможность бесплатного использования в коммерческих целях

Средняя функциональность



Wippien отличается от других утилит в первую очередь тем, что ее можно применять и в коммерческих целях, поскольку проект развивается как open source и любой желающий может при необходимости скачать не только саму программу, но и ее исходные коды.

Wippien базируется на Jabber, поэтому в качестве учетной записи можно как воспользоваться уже существующим JID, так и зарегистрировать новый аккаунт вида user_name@wippien.com.

Утилита поддерживает общение между пользователями и в отличие от остальных программ в данном обзоре позволяет делать это не только по внутреннему протоколу, но и в таких привычных сетях, как ICQ, MSN, AIM и Google Talk.

Тем, кому не нужны дополнительные возможности, предлагается урезанная версия Wippien – утилита MiniVPN. Этот дистрибутив программы распространяется без поддержки функции обмена сообщениями. Впрочем, для его использования все равно необходимо иметь установленную полную версию Wippien, которую следует хотя бы раз запустить для того, чтобы настройки сохранились в системе.

Кроме MiniVPN, доступно еще одно отдельное приложение – WippienService, позволяющее запускать Wippien в системе как сервис и работать таким образом с компьютером, даже если пользователь вышел из своей учетной записи Windows.

Wippien умеет функционировать и в 64-битовых версиях Windows, для этого необходимо отдельно скачать и установить 64-битовый драйвер. Также существует бета консольного клиента Wippien для Linux.

NeoRouter

Freeware

Разработчик NeoRouter

Сайт www.neorouter.com

Размер 8,4 МБ

Адрес загрузки www.neorouter.com/Downloads.html

Кросс-платформенность; установка на роутеры; поддержка прокси

Работает как сервер-клиент (можно создавать «одностороннюю» виртуальную сеть)

NeoRouter – наиболее кросс-платформенная утилита из вышерассмотренных. Она инсталлируется не только на все последние версии Windows (начиная с Windows 2000) и Mac OS X (начиная с Tiger), но и работает практически во всех основных дистрибутивах Linux (включая 64-битовые версии) и, что самое интересное, может быть установлена на роутеры, использующие прошивки tomato, fon и openwrt, которые расширяют возможности этих устройств.

NeoRouter отличается от других участников тем, что действует по принципу сервер-клиент. Необходимо установить серверную часть на одном из своих компьютеров и затем подключаться к нему с помощью отдельной программы Network Explorer. Между ПК создается прямое P2P-соединение, что позволяет обмениваться данными быстрее, чем при наличии промежуточного связывающего звена. Для подключения к удаленному компьютеру необязательно инсталлировать NeoRouter на каждой машине. Для этого достаточно использовать portable-версию программы, записанную на флеш-накопитель.

Еще одной особенностью NeoRouter является поддержка прокси (HTTP, SOCKS4 и SOCKS5); кроме того, функциональность программы можно расширять с помощью небольшого числа дополнений, доступных на сайте разработчика.

Настройка виртуальной локальной сети на примере Comodo EasyVPN

Рассмотрим процесс создания и подключения к виртуальной сети на примере двух человек. Процедура выполняется практически идентично во всех программах, мы будем основываться на Comodo EasyVPN.

Итак, оба пользователя устанавливают утилиту с сайта производителя (при этом следует согласиться на добавление в систему нового виртуального адаптера, когда инсталлятор спросит об этом). После запуска EasyVPN каждому из них необходимо создать аккаунт, что можно сделать прямо из программы, нажав на кнопку *Register a new account*.

Для развертывания сети один из пользователей выбирает в меню *Networks – Create a new network*. В появившемся окне следует указать имя сети и пароль (опцию *Enable VPN* советуем оставить включенной). После этого другой пользователь выбирает на своем компьютере пункт *Networks – Join a network* и вводит в появившемся диалоге название сети и пароль.

Теперь оба находятся в одной виртуальной сети и могут, к примеру, играть в компьютерные игры по LAN.

Еще один важный момент касается первого запуска утилиты и попытки ее выхода в Интернет. Установленный в системе файрвол может спросить, стоит ли добавить новую программу в белый список. Отвечать нужно утвердительно, иначе настроить виртуальную сеть не получится.

3. Контрольные вопросы

1. Охарактеризуйте программу LogMeIn Hamachi²
2. Охарактеризуйте программу Comodo EasyVPN
3. Охарактеризуйте программу Remobo
4. Охарактеризуйте программу Wippien
5. Охарактеризуйте программу NeoRouter
6. Опишите настройку виртуальной локальной сети на примере Comodo EasyVPN

Лабораторная работа № 7

Тема: «Настройка фильтрации TCP/IP»

1 ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНОЙ РАБОТЫ

1.1 Цель работы: знакомство с настройкой фильтрации TCP/IP.

1.2 В результате выполнения лабораторной работы студент должен знать:

- Особенности настройки фильтрации TCP/IP.

1.3Используемые программно-технические средства:

Персональная ЭВМ класса IBM PC стандартной конфигурации; операционная система Windows2000/XP/Vista, MicrosoftOfficeWord.

1.4В процессе выполнения лабораторной работы студент должен:

- Ознакомится с теоретическим материалом.
- Подготовить отчет по лабораторной работе.
- Отчитаться по исполненному заданию.

Перед выполнением лабораторной работы каждый студент обязан изучить правила техники безопасности при работе в помещении с электронно-вычислительной техникой.

1.5 Указания по оформлению отчета:

Отчет должен содержать: титульный лист, цель работы; ответы на контрольные вопросы; выводы.

1.6 Указания по сдаче зачета преподавателю

Для сдачи зачета необходимо:

1) выполнить практическое задание

2) предъявить отчет;

3) ответить на контрольные вопросы.

2 Теоретические сведения

2.1 Фильтрация

Сама фильтрация не представляет ничего сложного, в основе – указания чего можно пропускать, а чего нет (что следует уже из названия). Сложность только в том, что без понимания организации работы программ по протоколу tcp/ip эту фильтрацию не настроить.

А для организации фильтрации о протоколе tcp/ip надо знать следующее. TCP/IP – не является чем-то единым целом. Этот протокол является набором (стеком) из 255 IP-протоколов. Т.е., выражаясь образно, это не одна труба, по которой передается информация, и набор многих маленьких труб, связанных вместе. На этом и основана фильтрация. IP-пакет, помимо адреса источника и адреса назначения, имеет еще и третий параметр – номер ip-протокола из стека tcp/ip, который этот пакет использует. По этим параметрам вы и можете настроить фильтрацию. Т.е. пропускать пакеты 1) только с такого адреса источника 2) только на такой адрес назначения 3) только по такому-то номеру ip-протокола.

Наиболее часто используемы ip-протоколы в стеке tcp/ip являются протоколы №№ 1, 6 и 17. Они имеют собственные названия, соответственно ICMP, TCP, UDP. Эти ip-протоколы не просты, они имеют свои особенности.

2.1.1 ICMP. Этот протокол предназначен не для передачи информации, а для служебного пользования. По нему хосты передают друг другу различную служебную или управляющую информацию, связанную с работой протокола tcp/ip в целом. Пакеты ICMP внутри имеют дополнительную градацию по типам (это как tcp/ip состоит из набора ip-протоколов, так и icmp тоже состоит из типов icmp). Этим типам присвоены номера. И за каждым таким типом icmp-пакета закреплено конкретное служебное/управляющее назначение.

Думаю, многим известна такая утилита, как “ping”. С ее помощью мы можем протестировать доступность какого-либо хоста в сети (в обиходе - пропинговать). Если ответы пришли – значит хост (компьютер, сервер, и т.п.) доступен в сети. Это утилита работает так. По протоколу icmp, тип 8, отправляется запрос на удаленный хост. В ответ, хост, отправляет ответы по протоколу icmp, тип 0. Если вы захотите разрешить пользователям «пинговать», но при этом все остальные возможности icmp ограничить – то вам надо разрешить на выход пакеты тип 8 и на вход пакеты тип 0. Но чаще всего, в файрволах есть возможность более простого разрешения «пингования». Чаще всего это выглядит как в определенном параметре вводиться слово “ping”, и в этом случае файрволл автоматом разрешает оба типа (8 и 0) icmp-пакетов.

При работе в сети (в Интернет), время от времени возникает потребность просмотра маршрута движения (трассировка) пакетов от вас к какому-нибудь хосту (см. Часть 2. DNS и Маршрутизация). Для этого есть утилиты (для ОС Windows это “tracert”). Трассировка тоже работает по icmp протоколу. При этом используется тип пакетов icmp №11.

2.1.2 TCP и UDP. Эти два ip-протокола очень похожи. Они внутри себя тоже имею дополнительное разделение на типы. Это разделение и называется «порты». Но, в отличии от icmp – это разделение иное. Во первых – портов в tcp/udp значительно больше чем типов в icmp. Их номера (номера портов) находятся в диапазоне от 0 до 65535. Во вторых – за ними не закреплено никаких четких назначений (могут использовать какие угодно). И в третьих – при отправке пакета порт источника и порт получателя может быть разный (точнее так практически всегда). Т.е., для примера, пакет по протоколу tcp от вас выходит с порта 22345 и приходит к серверу на порт 80.

Если в плане портов tcp и udp одинаковы, то вот в методе передачи информации они отличаются. TCP – это «гарантированный» протокол. Если ваш компьютер отправил информацию по tcp, то в обязательном порядке к нему придет подтверждение, что информация получена. В случае же с udp, компьютер отправляет информацию и «забывает» об этом, т.е. дальнейшая судьба отправленных пакетов его абсолютно не интересует.

Вернемся к фильтрации. Так для фильтрации протоколов tcp и udp, параметров для фильтрации пакетов стало больше: 1- адрес источника, 2 – адрес назначения, 3 – собственно сам протокол (tcp или udp), 4 – порт источника, 5 – порт назначения.

Если «порт назначения» величина известная и фиксированная (ведь не зная порта подключения, подключится мы не сможем), то вот «порт источника» - величина чаще всего случайная (ОС сама неким случайным образом его назначает). Как следствие – очень часто параметр «порт источника» не указывается (точнее указывается все, 0-65535), а в некоторых файрволлах такой параметр вообще не предусмотрен.

Для примера. Допустим у нас есть в локальной сети компьютер с адресом 192.168.0.15, и ему надо дать возможность работы в Интернет. Но не любую работу разрешить, а только просмотр web-страниц и переписка по ICQ. Так уж сложилось, что большинство WEB серверов для своей работы используют протокол tcp, порт 80 (http). А для «защищенных» соединений – порт 443 (https). Сервер ICQ для работы использует протокол tcp, порт 5190. Для реализации этого примера нам нужно написать разрешающее правило фильтрации (а может быть три, если файрволл не позволяет в одном правиле указать несколько конкретных портов), которое будет содержать:

Код

Адрес источника - 192.168.0.15
Адрес назначения - любой
Протокол - tcp (или ip №6)
Порт источника - любой (или диапазон 0-65535)
Порт назначения - 80 (http), 443 (https), 5190 (icq)

Приведу пример, который в жизни не редко случается. Я запускаю свой браузер, набираю адрес сервера и вижу его страницы. Но когда я «пингую» его – то ответа нет (сервер отсутствует). Как такое может быть? Это результат

работы файрволла, который стоит на том сервере (или где-то еще между вами, в т.ч. это может быть и файрволл на вашем компьютере). И этот файрволл настроен, например, так, что он разрешает проходит пакетам по протоколу tcp (по которым работают web-сервера), а вот пакеты по протоколу icmp (по которым работает ping) он блокирует. Может быть и обратная ситуация, когда сервер «пингуется», а подключиться к нему не получается.

Ко всему выше написанному могу добавить следующее. Для организации выхода в Интернет нескольких компьютеров (компьютеров локальной сети), одних разрешающих правил фильтрации в файрволле недостаточно. Необходимо еще организовать трансляцию адресов (включить NAT). Это относится к так называемым «корпоративным» файрволлам (к коим можно отнести, например, ADSL-модем с функцией маршрутизации, обслуживающего несколько компьютеров). К персональным файрволлам это не относиться.

Кстати, раз зашла речь о «корпоративных» файрволлах, добавлю. В правилах написания фильтрации у них, помимо адресов источника и назначения, протокола, портов источника и назначения (для tcp и udp), добавляются еще два параметра – входящий сетевой интерфейс и исходящий сетевой интерфейс.

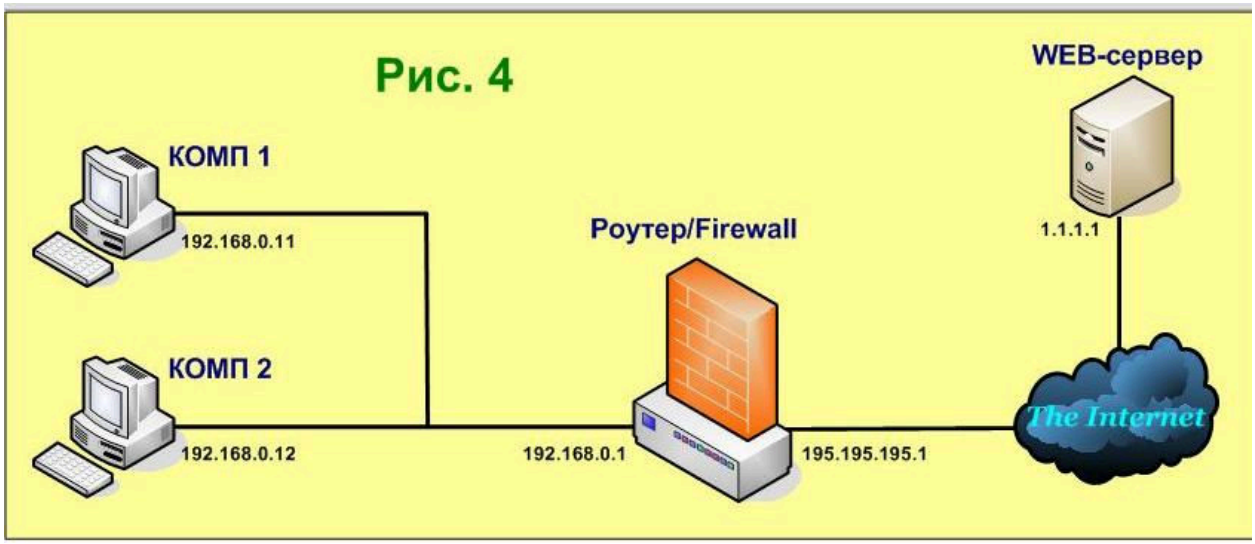
2.2 Трансляция адресов (NAT)

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

Возьмем ситуацию, когда у нас предполагается десяток, другой компьютеров, которые будут объединены в сеть с выходом в Интернет. Мы знаем, что бы работать в Internet, надо иметь ip-адрес, который выдается провайдером. Но у нас много компьютеров и один адрес им не назначишь, получается надо у провайдера просить столько адресов, сколько имеем компьютеров. Добавились компьютеры – значит опять к провайдеру выпрашивать адреса. Бредовая ситуация, не правда ли? Хотя бы потому, что ip-адресов в Интернете и так уже нехватка. И если бы все просили такие количества адресов, то развитие Интернета уже давно бы стояло, т.к. адреса бы уже давно закончились.

Да и к тому же мы знаем, что мы создаем свои локальные сети со «своими» ip-адресами, а потом подключаем свою сеть к Интернет, причем имея всего один «интернетовский» ip-адрес. Как это возможно?

Все это объясняется использованием NAT (трансляцией адресов). Что бы объяснить это понятие я дам другое определение. NAT – это замена в ip-пакете одного из ip-адресов (адреса источника или адреса назначения) на некий другой.



Возьмем рисунок 4. На рисунке мы имеем локальную сеть с адресами 192.168.0.x. В ней есть файрволл, к которому подключен Интернет с выделенным провайдером «интернетовским» адресом 195.195.195.1. И еще, для примера, приведен некий WEB-сервер в интернете, у которого ip-адрес 1.1.1.1.

Что бы это схема работала (т.е. компьютеры 1,2 выходили в Internet), на Firewall на интерфейсе 195.195.195.1 включена трансляция адресов со своего ip-адреса.

Включить трансляцию адресов со своего адреса на сетевом интерфейсе – это означает, что пакеты, которые выходят с этого сетевого интерфейса, преобразуются. Преобразование заключается в замене в пакете ip-адреса-источника на свой адрес (т.е. на адрес, который прописан на этом сетевом интерфейсе).

Подробнее. Вы захотели на компьютере 1 получить информация с WEB-сервера. В этом случае, компьютер 1 отсылает пакет с запросом информации. Характеристики этого пакета таковы: Адрес источника – 192.168.0.11, Адрес назначения – 1.1.1.1. Это пакет добежал до Firewall, прошел сквозь него, и побежал дальше в Internet. Но, когда он выходил с Firewall (выходил с сетевого интерфейса 195.195.195.1), он преобразовался, и теперь его характеристики таковы: Адрес источника – 195.195.195.1, Адрес назначения – 1.1.1.1. Вот наш

пакет успешно добежал до WEB-сервера. WEB-сервер его принял, прочитал. А прочитал он, что некий компьютер с адресом 195.195.195.1 хочет информации. Этот сервер добрым оказался, собрал нужную информацию, и послал ее в ответном пакете обратно компьютеру 195.195.195.1.

А вот если бы трансляцию (nat) на Firewall забыли включить, то к WEB-серверу запрос пришел бы от компьютера 192.168.0.11. Только вот смысла в ответе нет, т.к. всемирная сеть такие адреса отправки не признает, никуда не направляет.

Но вернемся к нашему ответному пакету. Вот он вернулся к Firewall. Подходя к Firewall, ответный пакет имеет параметры: Адрес источника – 1.1.1.1, Адрес назначения – 195.195.195.1. Firewall, умница, увидел, что это ответ на запрос, инициатором которого был Компьютер 1. И на входе (при входе пакета на сетевой интерфейс 195.195.195.1), сделал обратное преобразование адреса, т.е. вернул на место 192.168.0.11 вместо 195.195.195.1. Т.е. на выходе от Firewall и на подходе к компьютеру 1, наш ответный пакет имеет параметры: Адрес источника – 1.1.1.1, Адрес назначения – 192.168.0.11.

Вот и весь алгоритм трансляции адреса (надеюсь, вы поняли). Хочу обратить внимание на 2 момента.

1) Трансляция адреса для компьютеров локальной сети прозрачна. Т.е. наш компьютер 1 отправляет пакеты с 192.168.0.11 на 1.1.1.1, и в ответ получает пакеты с адреса 1.1.1.1 на адрес 192.168.0.11. А то, что где-то происходит подмена адреса, он (компьютер) даже и не в курсе.

2) Наш Firewall со своей трансляцией маскирует нашу сеть. С какого бы компьютера нашей локальной сети мы не работали, для Web-сервера это всегда один компьютер – 195.195.195.1. И о том, что на самом деле работает много компьютеров – ему не понять.

Мы рассмотрели трансляцию адреса источника. Теперь рассмотрим другой вариант. Допустим, на компьютере 1 мы организовали свой Web-сервер. И теперь хотим, что бы из Интернета люди могли к нему подключаться. Как это сделать? Ведь адрес 192.168.0.11 из Interneta не виден, а если набрать адрес 195.195.195.1, то наш Firewall решит, что кто-то именно к нему хочет подключиться. А т.к. на нем никаких web-серверов нет, то даст отбой.

Решение просто – надо использовать всю туже трансляцию адресов. Но по иной схеме, чем было описано выше. Нужно в настройках Firewall ему сказать, что если к тебе на интерфейс 195.195.195.1 придет запрос на

подключение по порту 80 протокола tcp (по этому протоколу/порту работают web-сервера), то транслируй адрес-назначение на ip 192.168.0.11.

В этом случае, некий пользователь Интернета для подключения набирает адрес 195.195.195.1. Firewall получает пакет запроса информации, и, согласно нашим указаниям, вместо адреса назначения 195.195.195.1 в пакет подставляет адрес 192.168.0.11. И далее этот пакет, согласно правилам маршрутизации уходит к компьютеру 1. Компьютер 1 собрал нужную информацию и отправил ответный пакет. Адрес источника этого пакета – 192.168.0.11. Пакет прошел через Firewall, и уже на выходе из него (на выходном интерфейсе), адрес источника подменился обратно на адрес 195.195.195.1
Но, не забудьте! Правила трансляции не дают разрешения на прохождение через Firewall. Необходимо еще в правилах фильтрации разрешить подключение любого компьютера из Инета к компьютеру 192.168.0.11 (хотя в некоторых файрволлах правила фильтрации и трансляции объединены).

Трансляция адреса-назначения очень часто называется словосочетанием «Публикация серверов». И здесь тоже хочу обратить внимание на один момент.

Такой тип трансляции опять-таки маскирует нашу сеть (наши сервера). Ведь некий пользователь Interneta отправляет запросы на адрес 195.195.195.1, и с него же получает ответы. Он в полной уверенности, что 195.195.195.1 и есть сервер, с которым он работает.

Дополнительные сведения.

Хочу сказать пару слов о таких понятиях, как «Серый адрес» и «Белый адрес». Белый адрес – это настоящий «интернетовский» ip-адрес. Серый адрес – это адрес в локальной сети. Компьютер, имеющий «серый» адрес, выходит в Интернет через NAT, где его пакетам присваивается «белый» адрес.

NAT "именно выход" в Интернет не ограничивает. А вот возможность подключения к вам из Интернет – блокирует. С одной стороны это ограничивает ваши возможности работы в Internete, но с другой стороны он дает 100% защиту, что к вам «непосредственно из вне» никто не подключиться (но вот от того, что запущенный у вас некий вирус сам от вас выйдет Internet и по этому соединению притащит/утащит все что ему нужно, конечно защиты нет). Если подключение к вам все-таки необходимо, то надо организовать еще одну трансляцию адресов. А именно «Публикацию вашего компьютера» по необходимым вам портам (ну или по всем портам).

3. Контрольные вопросы

1. Понятие фильтрации
2. Наиболее часто используемы ip-протоколы в стеке tcp/ip
3. Протокол ICMP
4. Протокол TCP
5. Протокол UDP
6. Трансляция адресов (поясните на примере)

Лабораторная работа № 8 .

Дополнительные протоколы глобальных сетей

Технология передачи PPP через Ethernet (PPPoE). Виртуальная частная сеть на основе туннельного протокола типа точка-точка (PPTP VPN).

1 Описание

1.1 Метод передачи PPP через Ethernet (PPPoE)

Протокол передачи данных типа точка-точка (Point-to-Point Protocol, PPP) представляет собой стандартный метод передачи мультипротокольных дейтаграмм через двухточечные линии передачи данных. В данной лабораторной работе изучается, как обеспечить PPP сессию и инкапсулировать пакеты PPP через Ethernet.

Технология использования стека PPP в сети Ethernet является относительно новой, но уже получила достаточное распространение. На данный момент она определяется документом RFC 2516. Родоначальниками разработки этого документа явились компании RedBack Networks, RouterWare, UUNET и другие. Использование этой технологии предоставляет провайдерам Интернет-услуг новые возможности в организации и учете доступа пользователей к сети. Это особенно актуально для тех провайдеров, которые планируют или уже предлагают своим пользователям доступ к Интернету при помощи сети Ethernet, например, в современных жилых комплексах, где кабельная разводка витой парой уже не является новшеством.

Заслуживает особого внимания тот факт, что для настройки маршрутизатора провайдера, установки концентратора в подъезде жилого здания, сетевой карты и небольшого программного обеспечения в компьютер пользователя не нужен модем, нет необходимости занимать единственную телефонную линию, так как провайдер услуг теперь может организовывать, ограничивать доступ и учет трафика пользователей таким образом, словно пользователь работает по обычному модемному каналу. Такая реализация стала возможной благодаря технологии PPPoE, которая запускает сессию PPP, но не поверх модемного соединения, а поверх сети Ethernet.

При этом, будет поддерживаться аутентификация пользователей по протоколам PAP и CHAP, динамическое выделение IP-адресов пользователям, назначение адреса шлюза, DNS-сервера и т.д. Также протокол PPP предоставляет дополнительные возможности – сжатие и шифрование трафика.

Технология PPPoE на данный момент является одной из самых дешевых при предоставлении пользователям доступа к услугам Интернет в жилых комплексах на базе Ethernet и при использовании технологии DSL. В частности, самый известный московский Интернет-провайдер МТУ-Интел использует эту технологию в услуге «СТРИМ – домашний Интернет-канал».

Так как принципом работы PPPoE является установление соединения "точка-точка" поверх общей среды Ethernet, то процесс функционирования PPPoE должен быть разделен на две стадии. В первой стадии два устройства должны сообщить друг другу свои адреса и установить начальное соединение, а во второй стадии запустить сессию PPP.

Стадия установления соединения между между клиентом (компьютером пользователя) и сервером (концентратором доступа провайдера) делится на несколько этапов.

На первом этапе клиент посылает широковещательный запрос PADI (PPPoE Active Discovery Initiation) на поиск сервера со службой PPPoE. Этот запрос получают все пользователи сети, но ответит на него только тот, у кого есть поддержка службы PPPoE. Ответный пакет от концентратора доступа PADO (PPPoE Active Discovery Offer) посылается в ответ клиенту, но если в сети есть много устройств со службой PPPoE, то клиент получит много пакетов PADO. В этом случае, программное обеспечение клиента выбирает необходимый ему концентратор доступа и посылает ему пакет PADR (PPPoE Active Discovery Request) с информацией о требуемой службе (требуемый класс обслуживания зависит от услуг провайдера), имя провайдера и т.д. После получения запроса, концентратор доступа подготавливается к началу PPP сессии и посылает клиенту пакет PADS (PPPoE Active Discovery Session-confirmation). Если все запрашиваемые клиентом службы доступны (в состав этого пакета входит уникальный номер сессии, присвоенный концентратором), то начинается второй этап - стадия установленной сессии. Если требуемые клиентом услуги не могут быть предоставлены, клиент получает пакет PADS с указанием ошибки в запросе услуги.

Сессия начинается с использованием пакетов PPP. При установлении PPP-сессии пользователь может быть аутентифицирован при помощи RADIUS, и его трафик будет учитываться как при обычном модемном доступе. Ему можно назначить динамический IP-адрес из пула адресов концентратора, установить настройки шлюза и DNS-сервера. При этом на концентраторе доступа клиенту соответственно ставится виртуальный интерфейс. Желательно, чтобы концентратор доступа посылал периодические запросы клиенту для определения его состояния. Эта операция необходима для того, чтобы клиент, который по какой-либо причине не оборвал сессию корректным образом, не считался существующим и для него не резервировались ресурсы концентратора доступа.

Завершение соединения PPPoE происходит по инициативе клиента или концентратора доступа при помощи посылки пакета PADT (PPPoE Active Discovery Terminate).

В протоколе PPPoE предусмотрены некоторые дополнительные функции, например, такие как защита от DoS атак (Denial of Service). Защита от некоторых типов DoS атака реализована путем добавления в пакеты PADI специального поля AC-Cookie, которое позволяют концентратору доступа ограничивать количество одновременных сессий PPPoE на одного клиента.

1.1.1 Настройка PPPoE-сервера

В данной лабораторной работе используется rp-pppoe - Roaring Penguin PPPoE Server and Client v.3.8 (/products/rp-pppoe/), поставляемый в составе многих дистрибутивов ОС Linux.

Для запуска сервера необходимо выполнить:

pppoe-server [options]

Параметры:

-I interface Указывает, какой Ethernet-интерфейс использовать (eth0, etH2…).

-C ac_name Имя концентратора доступа (access concentrator).

-S name Имя предлагаемой службы (service name). Может быть указано несколько раз.

-L ip Локальный IP-адрес (IP-адрес сервера).

-R ip Устанавливает стартовый удаленный IP-адрес. После установления ppp-сессии, IP-адреса клиентов назначаются, начиная со стартового IP-адреса.

-N num Максимальное количество сессий.

-k Запуск сервера в kernel-режиме.

Сервер будет использовать встроенную в ядро поддержку PPPoE.

Пример:

pppoe-server –I eth0 –C pppoe-test-ac –L 10.0.0.1 –R 10.0.0.2 –k

PPPoE сервер прослушивает указанный сетевой интерфейс и отвечает на discovery-запросы клиентов. После установления pppoe-сессии, сервер выделяет из пула IP-адрес для клиента и запускает pppd с необходимыми параметрами. Дополнительные параметры для pppd берутся из файла /etc/ppp/pppoe-server-options.

Некоторые дополнительные параметры для pppd:

require-pap Требуется аутентификация клиента методом PAP.

require-chap Требуется аутентификация клиента методом CHAP.

login Учетная запись пользователя проверяются по системной базе данных.

ms-dns ip Сервер будет передавать клиенту указанный адрес DNS-сервера.

noproxyarp Не добавлять в системную ARP-таблицу IP и MAC адреса клиентов.

ktune Разрешить pppd изменять некоторые опции ОС по необходимости

Если не указан параметр login, база данных учетных записей пользователей должна находится в файлах /etc/ppp/pap-secrets или /etc/ppp/chap-secrets в зависимости от метода аутентификации (PAP, CHAP).

1.1.2 Настройка PPPoE-клиента

PPPoE клиент, также как и сервер, может функционировать в двух режимах – user-mode и kernel-mode. В user-режиме транспортным уровнем для pppd служит pppoe - Roaring Penguin PPPoE Client. В kernel-режиме pppoe-сессия устанавливается через специальных плагин (rp-pppoe.so), который вызывает необходимые функции ядра ОС. Для использования kernel-режима ядро Linux должно быть собрано с поддержкой PPPoE. Обычно драйверы PPPoE собираются в виде модулей ядра – pppox.ko и pppoe.ko.

Для запуска клиента в user-режиме необходимо выполнить:

pppd pty ‘pppoe [pppoe-options]’ [pppd-options]

Параметры pppoe-клиента:

-A Выводит список доступных в сети концентраторов доступа.

-I interface Указывает, какой Ethernet-интерфейс использовать (eth0, etH2…).

-C ac_name Имя концентратора доступа, к которому необходимо подключиться.

-S name Имя службы концентратора, которую необходимо использовать.

Параметры для pppd могут быть следующими:

defaultroute Установить шлюз по умолчанию (default route) на адрес сервера

debug Выводить дополнительные сообщения о состоянии в системный журнал событий

noipdefault pppd должен использовать IP-адрес, полученный с сервера

persist Пересоздавать соединение при потере связи

usepeerdns Использовать IP-адреса DNS-серверов, полученные с сервера

user name Имя учетной записи, которое pppd будет использовать при аутентификации на сервере. Все параметры данной учетной записи должны находится в файлах /etc/ppp/pap-secrets или /etc/ppp/chap-secrets в зависимости от метода аутентификации.

Также можно использовать параметры require-pap, require-chap, noproxyarp и ktune, описанные выше.

Пример:

pppd pty ‘pppoe –C pppoe-test-ac’ user test

Для запуска клиента в kernel-режиме необходимо выполнить:

pppd plugin rp-pppoe.so [ethX] [plugin-options] [pppd-options]

где ethX - Ethernet-интерфейс (eth0, etH2…)

Опции плагина:

rp_pppoe_ac ac_name Имя концентратора доступа.

rp_pppoe_service name Имя службы концентратора.

Пример:

pppd plugin rp-pppoe.so eth0 rp_pppoe_ac pppoe-test-ac user test

1.1.3 PPPoE клиент для Windows XP/2003 (встроен в ОС)

1.2 PPTP VPN

Документация по созданию виртуальной частной сети на основе туннельного протокола типа точка-точка содержится в файле pptp-vpn-howto.txt (см. материалы для подготовки к лабораторной работе).

2 Рабочее задание

2.1 PPPoE

1. Следуя инструкциям в документации, и используя справочное руководство [1], настроить PPPoE сервер в kernel-режиме.
2. На другом компьютере настроить PPPoE клиент и подключиться к серверу в разных режимах (user, kernel).
3. Подключиться к PPPoE серверу с ОС Windows.

2.2 PPTP VPN

1. Ознакомиться с документацией по созданию PPTP VPN (/usr/doc/labs/lab4/pptp-vpn-howto.txt).

2. Следуя инструкциям в документации, и используя справочное руководство [2], настроить VPN сервер poptop.
3. На другом компьютере настроить pptp клиент и подключиться к серверу.
4. Подключиться к VPN серверу с ОС Windows.

Лабораторная работа № 9

Тема: **«Установка и настройка сетевой карты»**

ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНОЙ РАБОТЫ

1.1 Цель работы: научиться устанавливать и настраивать сетевой адаптер.

1.2 В результате выполнения лабораторной работы студент должен знать:

о Основные настройки сетевого адаптера

1.3 Используемые программно-технические средства:

Персональная ЭВМ класса IBM PC стандартной конфигурации; операционная система Windows2000/XP/Vista, MicrosoftOfficeWord.

1.4 В процессе выполнения лабораторной работы студент должен:

о Ознакомится с теоретическим материалом.

о Подготовить отчет по лабораторной работе.

о Отчитаться по исполненному заданию.

Перед выполнением лабораторной работы каждый студент обязан изучить правила техники безопасности при работе в помещении с электронно-вычислительной техникой.

1.5 Указания по оформлению отчета:

Отчет должен содержать: титульный лист, цель работы; ответы на контрольные вопросы; выводы.

Указания по сдаче зачета преподавателю

Для сдачи зачета необходимо:

1) выполнить практическое задание

2) предъявить отчет;

3) ответить на контрольные вопросы.

Теоретические сведения

Установка сетевых адаптеров

На рисунках 1 и 2 показаны сетевые карты ISA и PCI, которые еще не установлены в слот.

Сетевая карта ISA

Сетевая карта PCI

Установить сетевую карту на материнскую плату очень просто.
Удалите на корпусе заглушку, если она есть, поставьте сетевую карту примерно так, как показано на рисунке 2 и приложив небольшое усилие утопите ее в слот до упора. После того,

как карта встала в слот, сразу закрепите ее винтом.
На рисунках 3 и 4 показаны установленные карты.

Карта ISA установлена

Лабораторная работа № 10-11

Тема: **«Восстановление компьютера после сбоя. (работа с backup-ами)»**

ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНОЙ РАБОТЫ

1.1 Цель работы: научиться создать резервные копии стандартными средствами windows.

1.2 В результате выполнения лабораторной работы студент должен знать:

о Возможности архивирования данных в ОС Windows;

о Виды архивов;

о Параметры архивирования

1.3 Используемые программно-технические средства:

Персональная ЭВМ класса IBM PC стандартной конфигурации; операционная система Windows2000/XP/Vista, MicrosoftOfficeWord.

1.4 В процессе выполнения лабораторной работы студент должен:

о Ознакомится с теоретическим материалом.

о Подготовить отчет по лабораторной работе.

о Отчитаться по исполненному заданию.

Перед выполнением лабораторной работы каждый студент обязан изучить правила техники безопасности при работе в помещении с электронно-вычислительной техникой.

1.5 Указания по оформлению отчета:

Отчет должен содержать: титульный лист, цель работы; ответы на контрольные вопросы; выводы.

Указания по сдаче зачета преподавателю

Для сдачи зачета необходимо:

1) выполнить практическое задание

2) предъявить отчет;

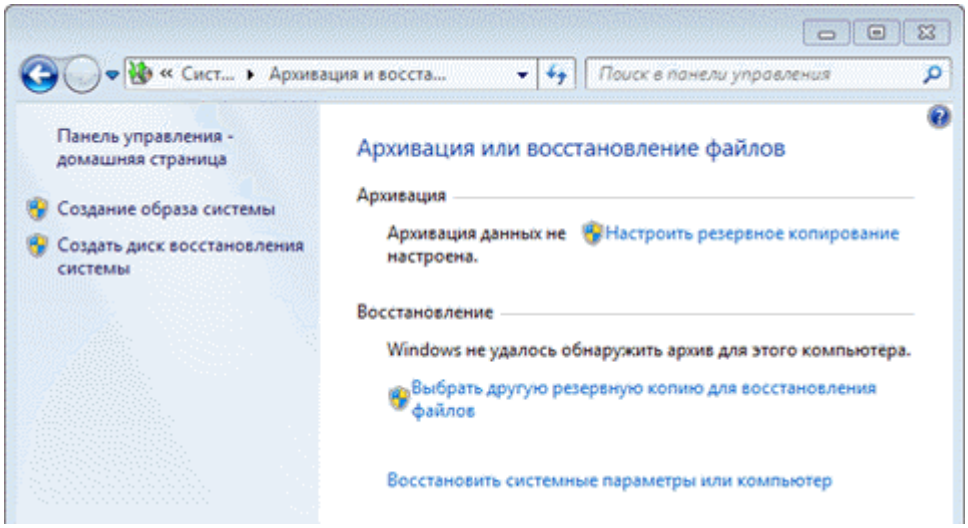
3) ответить на контрольные вопросы.

Теоретические сведения

С помощью элемента панели управления **Архивация и восстановление** вы можете:

- выполнять архивацию заданных папок по расписанию и восстанавливать их из резервной копии

- создать полный образ системы
- создать загрузочный диск для восстановления Windows 7



Лабораторная работа №12,13 ,14Монтаж телекоммуникационного оборудования.

Цель работы

Познакомиться с основными компонентами сетевого оборудования, их назначением и характеристиками. Получить представление о построении кабельной системы, стандартах

ее проектирования и монтажа. Получить навыки по подключению отдельного ПК к ЛВС, исследованию топологии и организации ЛВС небольшого подразделения. Изучить простейшие приемы работы в сетевой среде и команды ОС, используемые для этого.

1. Сетевое оборудование.

Для продуктивной работы фирм компьютеры, телефоны и периферийное оборудование объединяют в единую сеть. Это позволяет совместно использовать данные, принтеры и доступ в Интернет. Большое влияние на качество, скорость и надежное соединение оказывает сетевое оборудование.

Различают пассивное и активное оборудование. Пассивное оборудование должно соответствовать определенным стандартам, активное должно обеспечивать работу сети на разных скоростных режимах и поддерживать все основные сетевые протоколы и стандарты.

При создании кабельной структуры, необходимо учитывать совместимость всех ее составляющих. Основными стандартами по кабельным системам являются:

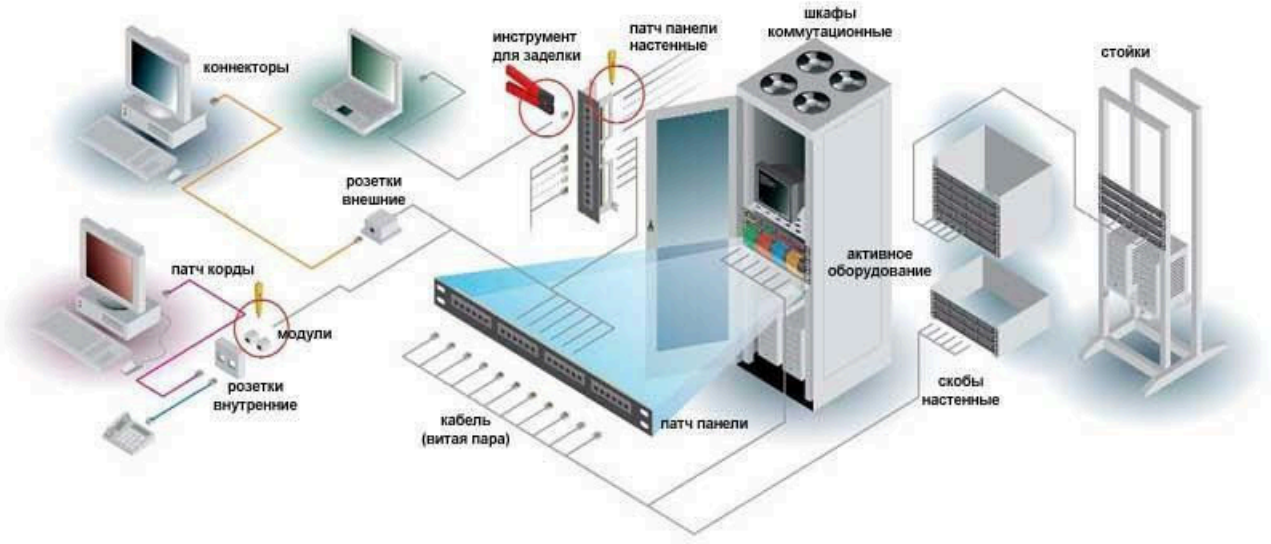
- Международный стандарт ISO/IEC 11801 Generic Cabling for Customer Premises (www.iso.ch, www.iec.ch).

- Европейский стандарт EN 50173 Information technology–Generic cabling systems
- Американский стандарт ANSI/TIA/EIA 568-B Commercial Building Telecommunication Cabling Standard (www.tiaonline.org, www.eia.org)

Стандарты определяют среду передачи, параметры разъемов, линии и канала, в том числе предельно допустимые длины, топологию и характеристики функциональных элементов системы.

2. Структурированная кабельная система (СКС).

Представляет собой иерархическую кабельную среду передачи электрических или оптических сигналов в здании, разделённую на структурные подсистемы и состоящую из элементов — кабелей, разъёмов, панелей, шкафов и вспомогательного оборудования.



СКС сочетает удобство эксплуатации, качество передачи данных и надежность. Строится таким образом, чтобы каждый интерфейс (точка подключения к системе) обеспечивал доступ ко всем ресурсам сети. Кабели прокладывают от ПК до распределительных

пунктов, которые ../../../../Documents and Settings/Administrator/My

Documents/ecolan/st_structure.htm - topologyобъединяют магистральными линиями.

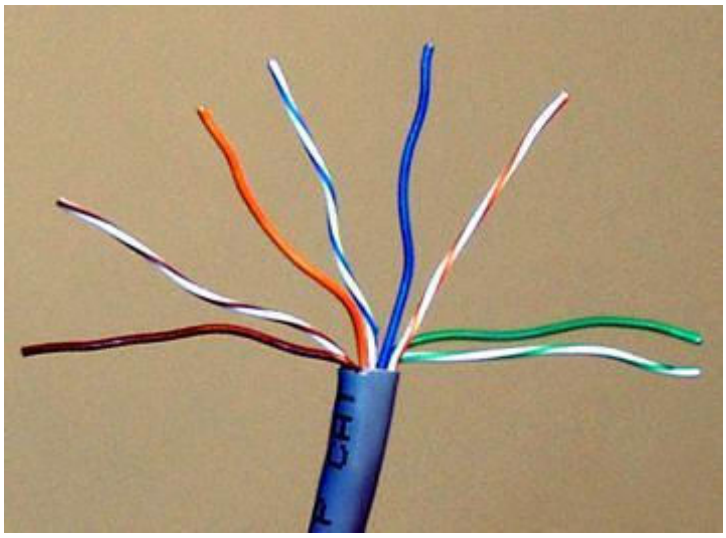
2.1. Пассивное сетевое оборудование.

Сетевое оборудование не потребляющее электрическую энергию называется пассивным.

К пассивному оборудованию относятся розетки, кабель, вилки, патч-панели и т.п. Основными компонентами являются сетевой кабель и монтируемая на нем вилка.

2.1.1. Сетевой кабель и вилка.

При монтаже кабельной системы наиболее часто используют неэкранированную «витую пару» 5 категорий (UTP 5 cat). Он состоит из нескольких пар медных проводов, покрытых пластиковой оболочкой.

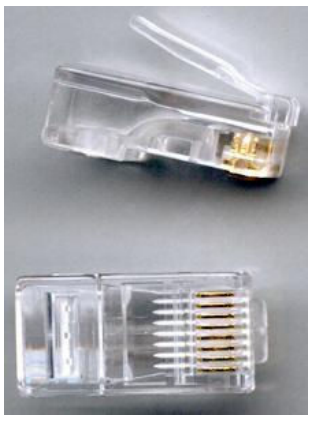


Провода, составляющие каждую пару, скручены друг вокруг друга, что обеспечивает защиту от взаимных наводок.

Изоляция каждого провода окрашена в свой цвет:

- бело-зеленый
- зеленый
- бело-оранжевый
- оранжевый
- бело-синий
- синий
- бело-коричневый
- кор ичневый.

Рис.1. Кабель неэкранированная «витая пара»



Провода с одинаковым цветом составляют 4 пары:

- оранжевый / бело-оранжевый,
- зеленый / бело-зеленый,
- синий / бело-синий,

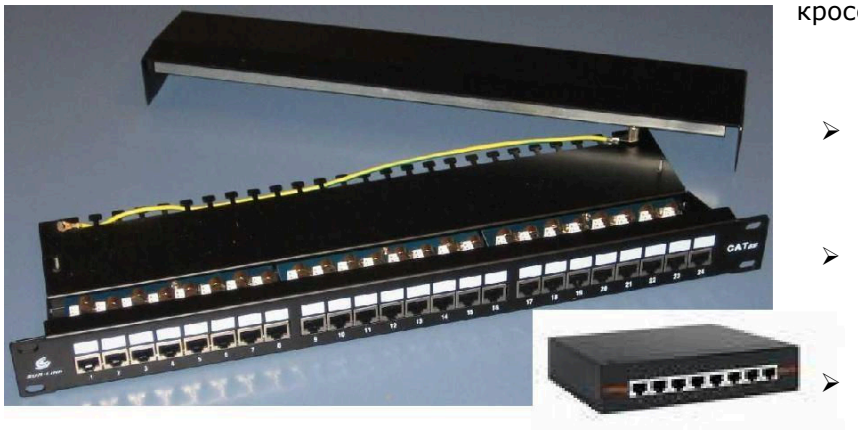
- коричневый / бело-коричневый.

Для подключения кабеля «витая пара» используются вилки RJ-45, которые монтируются на концах кабеля. Вилка имеет восемь контактов и монтируется на кабель при помощи специального инструмента.

Рис.2. Вилка RJ-45

2.1.2. Коммутационная панель (кросс-панель, патч-панель)

Представляет собой панель с множеством разъёмов, расположенных на лицевой стороне. На тыльной стороне панели находятся контакты, предназначенные для фиксированного электрического соединения с кабелями.



Основными характеристиками кросс-панелей являются:

- способ крепления (на стену или в стойку),
- количество портов (как правило от 12 до 48),
- категория(3, 5e, 6),
- экранированные и неэкранированные.

Рис.3. Кросс-панели для крепления в стойку и на стенку.

Существует два способа использования панелей:

В первом случае, коммутационная панель используется как точка коммутации между портами активного сетевого оборудования (АСО) и портами рабочих мест, через кабель горизонтальной подсистемы СКС. Коммутация осуществляется коммутационными шнурами от панели до портов АСО.

Во втором случае, так называемое двойное представление порта, коммутационные панели используются попарно, одна из панелей представляет порты АСО, а вторая - порты рабочих мест. Коммутация осуществляется коммутационными шнурами между панелями.

2.1.3. Коммутационный шнур (патч-корд).

Коммутационный кабель или патч-корд (от англ. patching cord — соединительный шнур) представляет собой электрический кабель для подключения одного электрического устройства к другому.

Может быть любых размеров, на одном или обоих концах кабеля присутствуют разъемы (коннекторы).

Патч-корды делятся на телефонные (RJ11 и RJ12), компьютерные (RJ45) и патч-корды для 110-го кросса, неэкранированные (UTP) и экранированные (STP), обычные и реверсивные.

Применяются для подключения ПК к розетке, двух коммутационных панелей друг к другу и так далее.

Главное отличие коммутационного шнура от кабеля внутренней прокладки - использование многожильного провода, вместо цельного. Это снижает передаточные характеристики кабеля, но повышает гибкость и уменьшает радиус безопасного изгиба шнура.

2.1.4. Телефонные и компьютерные розетки.

Являются составной частью СКС. Состоят из пластмассового корпуса и установленных в этом корпусе телефонных (RJ12) или компьютерных (RJ45) соединительных разъемов.

В гнезда лицевой части розеток вставляются разъемы патч-кордов. На обратной стороне этих гнезд находятся контакты, предназначенные для фиксированного соединения с кабелями, и соединённые с разъёмами электрически.

Телефонные и компьютерные розетки предназначены для подключения оконечных устройств (телефонов и сетевых карт компьютеров) при помощи патч-кордов к локальным телефонным и компьютерным сетям.

2.2. Активное сетевое оборудование.

К активному сетевому оборудованию относятся сетевые адаптеры, концентраторы (hub), коммутаторы (switch), маршрутизаторы (router), , принт-серверы и т.п.

2.2.1. Сетевые адаптеры.

Для подключения к ЛВС компьютер должен быть оснащен сетевой платой (адаптером). К сетевому адаптеру должен прилагаться драйвер, предназначенный для связи адаптера с операционной системой Windows. Что бы выяснить совместимость сетевого адаптера с ОС Windows надо обратиться к списку совместимого оборудования HCL, предоставляемому компанией Microsoft по адресу http://www.microsoft.com/hcl/. В списке указаны адаптеры, которые были протестированы для работы в этой ОС.

Для организации ЛВС лучше всего выбрать одинаковые сетевые карты. Это упрощает настройку сети, хотя это и не обязательно. Все сетевые карты выполняют одну и туже функцию - связь компьютеров между собой. Однако есть ряд особенностей и технологий, которые, могут отсутствовать у дешевых сетевых карт и присутствовать у более дорогих.

Рис.4. Устройство сетевой карты.

BootRom – специальная микросхема, которая позволяет загружать ПК по сети. То есть, при соответствующей настройке, компьютер может работать вообще без жёсткого диска. Загрузка через сеть настраивается в Bios ПК, которые поддерживают возможность удалённой загрузки. У дешёвых сетевых карт BootRom либо вообще отсутствует, либо под него есть разъем, но нет самой микросхемы.

Wake-on-Lan - позволяет включать удалённый компьютер через сеть. При этом ПК должен быть с ATX блоком питания. В настройках Bios надо разрешить активацию ПК по запросу с порта, на который установлена карта (как правило, это PCI). Сетевая карта должна быть соединена 3-х жильным шнуром с WOL разъемом на материнской плате. Если карта встроена в материнскую плату, последнее, как правило, не требуется

2.2.2. Концентраторы и коммутаторы.

Объединить компьютеры можно при помощи концентратора (hub) или коммутатора (switch). Внешне они выглядят одинаково, но между ними есть очень важное отличие.

Рис.5. Сетевой коммутатор.

Hub (Концентратор). При поступлении пакета данных от сетевой карты, Hub просто делит и усиливает сигнал так, что его получают все пользователи сети, но принимает только та сетевая карт, которой адресован пакет данных. Очевидно, что при одновременной работе нескольких пользователей скорость сети резко падает. В настоящее время большинство фирм попросту прекратили выпуск концентраторов, и перешли на выпуск более эффективных коммутаторов (Switch).

Switch (Коммутатор) в отличие от Hub анализирует откуда и куда отправлен пакет информации и соединяет только эти компьютеры, в то время как остальные каналы остаются свободными. Конечно, лучше использовать Switch, так как он работает гораздо быстрее особенно в сетях с большим количеством пользователей. Внешне Switch практически не отличается от Hub.

2.2.3. Принт-серверы.

Принт-сервер – это устройство (в том числе и, например, ПК), подключаемое к локальной сети и к принтеру, оснащенному интерфейсом LPT или USB.

Принт-сервер превращает обычный принтер в сетевой принтер.

Кроме того, принт-сервер заодно может предоставить дополнительные возможности (например дополнительную память для печати больших документов, разграничение прав доступа к принтеру и ограничение на печать, и т.д.).

Рис.6. Принт-сервер HP JetDirect 620N

3. Монтаж кабельной системы и подключение сетевого оборудования.

3.1. Правила монтажа кабельной системы

Основные правила, которые необходимо соблюдать при монтаже кабельной системы:

- Не допускайте растяжения кабеля во время монтажных работ.
- Радиус изгиба кабеля должен быть не меньше 10 внешних диаметров кабеля.
- Удалять оболочку кабеля следует лишь настолько, сколько требуется для монтажа.
- Сохраняйте целостность скручивания пар как можно ближе к месту монтажа, что обеспечивает минимальное влияние сигналов различных пар друг на друга. Раскрученные во время монтажа кабельные пары не следует скручивать снова, т.к. неправильное скручивание отрицательно влияет на рабочие характеристики.
- Кабели ЛВС не должны располагаться рядом с силовыми проводами (220в), флуоресцентными лампами, силовыми трансформаторами и другими устройствами, мощные электромагнитные поля которых, создают помехи и оказывают отрицательное воздействие на качество передачи сигнала.

3.2. Монтаж вилки RJ-45.

Вилка RJ-45 монтируется обжимным способом с помощью специального обжимного инструмента в соответствии с одним из стандартов T568A или T568B.

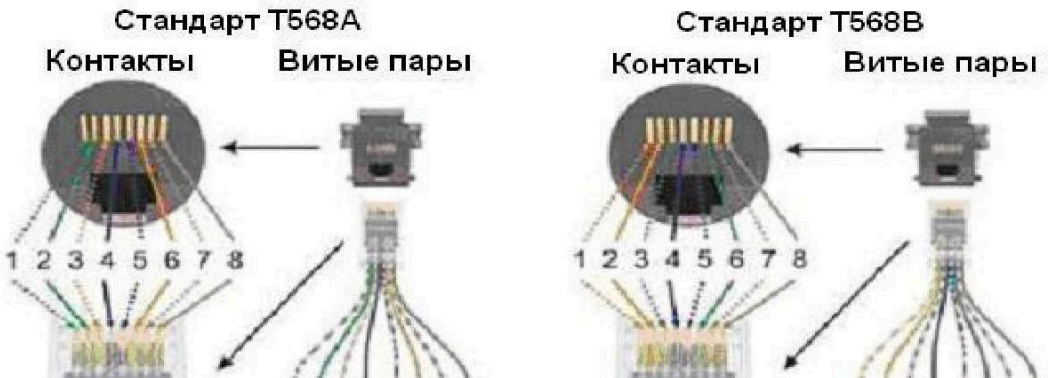


Рис.7. Стандарты подключения RJ-45.

Правила монтажа определяются типом предполагаемого соединения. Возможны два варианта:

- Компьютер соединяется с сетевым концентратором (hub) или коммутатором (switch) используя «прямую» разводку кабеля (стандарт T568B);

- Соединение между коммутаторами или концентраторами, такие как “hub – hub”, “switch – switch”, “hub – switch” производятся с помощью кабеля с «перевернутой» разводкой (Uplink или Crossover). С одной стороны кабель разводится по стандарту T568A, а с другой по стандарту T568B.

Более подробно о порядке разделки кабеля изложено в Приложении.

3.3. Подключение сетевого оборудования.

Коммутаторы и концентраторы подключаются к локальной сети одинаково. Если используется несколько коммутаторов, то они объединяются между собой кабелем UTP с «перевернутой» разводкой (T568A – T568B). Длина кабеля должна быть не менее 0,5 м.

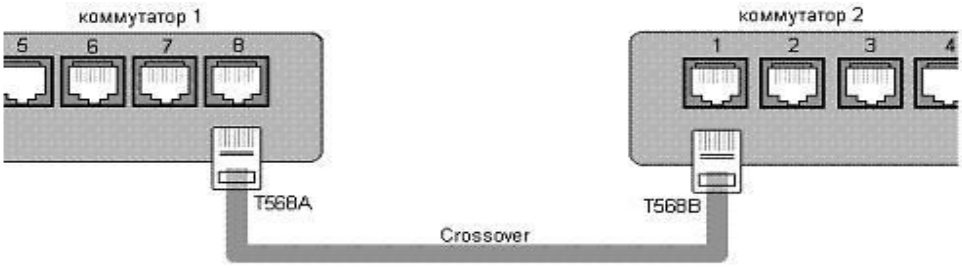


Рис.6. Соединение коммутаторов кабелем с разводкой по стандарту T568A – T568B

Во многих моделях коммутаторов наряду с простыми портами используется дополнительный порт “Uplink”. Он совмещен с одним из простых портов и имеет «перевернутую» разводку в соответствии со стандартом T568A. Используя этот порт можно подключать второй коммутатор простым кабелем (T568B – T568B).

Рис.7. Использование порта “Uplink” для подключения кабеля T568B – T568B.

На рисунке показано применение дополнительного порта “Uplink” совмещенного с портом №8. При этом сам порт №8 должен оставаться пустым.

В современных коммутаторах реализована функция автоматического определения типа кабеля. Каждый порт коммутатора может сам определить стандарт подключенного к нему кабеля и порт сам определяет, в каком режиме ему работать. Функция автоматического определения типа кабеля значительно облегчает работу администратора сети.

Для подключения ПК к ЛВС необходимо:

- установить сетевой адаптер, поддерживающий сетевую технологию Ethernet
- осуществить физическое подключение к сетевому оборудованию с помощью кабеля

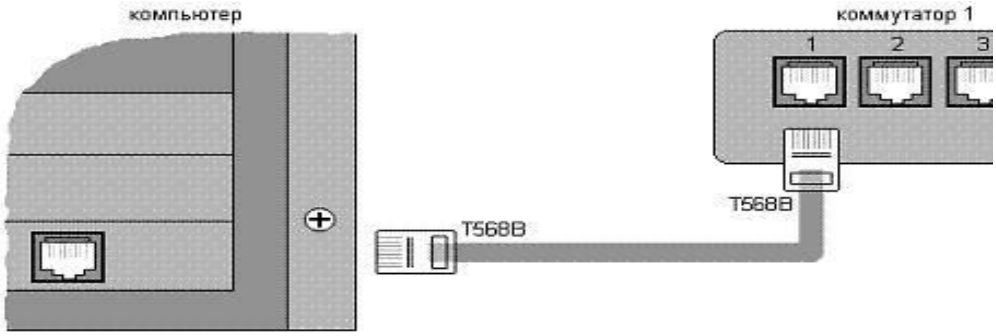


Рис.8. подключения ПК к коммутатору ЛВС кабелем Т568В – Т568В.

Для соединения двух ПК между собой с использованием только сетевых адаптеров используют кабель с «перевернутой» разводкой (Uplink или Crossover) по стандарту Т568А – Т568В.

4. Задание на лабораторную работу

1. Изучить состав и назначение основных компонентов сетевого оборудования.

Ответить на контрольные вопросы. Выяснить состав сетевых компонентов, используемых

в составе лаборатории и способ их соединения в ЛВС. Изучить правила разделки и подключения кабеля типа витая пара по стандартам T568A и T568B.

Отчет: Физическая топология ЛВС лаборатории. Электрическая схема подключения сетевого адаптера Вашего компьютера к ЛВС.

2. Определить состав и основные характеристики оборудования и системного программного обеспечения, установленного в Вашем компьютере.

Для определения состава оборудования ПК:

- Способ 1. Используйте окно «Свойства системы».
  - ✓ Откройте это окно путем ” Мой компьютер” -> ” Свойства” или нажав WIN+Break.
  - ✓ Воспользуйтесь вкладками «Общие» и «Оборудование» -> «Диспетчер устройств».
- Способ 2. Откройте окно «Запуск программы» (WIN+R), и введите команду msinfo32.

Отчет: Перечень и основные характеристики оборудования и системного программного обеспечения для конкретного ПК.

3. Определить сетевое имя компьютера и рабочую группу, в которую он входит.

Для этого в окне «Свойство системы» воспользуйтесь вкладкой «Имя компьютера».

Отчет: Сохранить значение параметров.

4. Определить состав установленных в компьютере сетевых адаптеров и познакомиться с их основными свойствами.

Для определения состава и характеристик, установленных в ПК сетевых адаптеров воспользуйтесь оснасткой «Диспетчер устройств».

- Откройте окно «Диспетчер устройств»:
  - ✓ Откройте окно «Запуск программы» (”Пуск”->”Выполнить” или WIN+R),
  - ✓ Введите команду devmgmt.msc и нажмите ”ОК”.
- В появившемся окне найдите узел дерева «Сетевые адаптеры» и раскройте его.

- Просмотрите все вкладки окна свойств сетевых адаптеров, уделив особое внимание вкладкам «Общие» и «Дополнительно».

Отчет: количество сетевых адаптеров, установленных в компьютере, перечень основных свойств и их значениях для конкретного сетевого адаптера, теоретическое описание каждого из этих свойств на основе технической литературы и сайтов разработчиков или поставщиков.

5. Определить MAC-адреса установленных в компьютере сетевых адаптеров и назначенные этим сетевым интерфейсам IP-адреса.

Откройте окно командной строки (”Пуск”->”Выполнить”, далее в текстовой строке ввести команду cmd и нажать Enter) и выполните команды:

- ipconfig /all.
- getmac /v /fo list
- ping <сетевое имя компьютера>

Отчет: полный протокол выполнения этих команд с вашими пояснениями и выводами. Анализируете полученный результат, а не сами команды, подробное знакомство с которыми это предмет следующих лабораторных работ.

6. Проверить текущее состояние сетевых подключений Вашего компьютера.

В окне «Сетевые подключения» (”Пуск”->”Панель управления”->”Сетевые подключение”) для доступных вам подключений правой кнопкой мыши установите режим «Состояние».

Используйте вкладки «Общие» и «Поддержка» (плюс «Подробности») окна «Состояние…». На этих вкладках познакомьтесь со всеми выводимыми параметрами, нажимая кнопку «?» и активируя указатель мышки над интересующим параметром.

Проверьте наличие значка сетевого соединения в области уведомлений экрана вашего компьютера. При его наличии ознакомьтесь с параметрами всплывающего окне над этим значком и действием в ответ на клик мышки на этом значке.

Отчет: результаты выполнения этого пункта задания с вашими выводами и сравнительным анализом с предыдущими заданиями.

7. При наличии сетевых подключений ПК к ЛВС определить список, доступных вам рабочих групп, список компьютеров вашей рабочей группы с их именами и IP-адресами.

Откройте окно командной строки и выполните команды:

- net view /domain – для просмотра доступных вам рабочих групп.
- net view – для просмотра доступных вам компьютеров вашей рабочей группы.
- ping <сетевое имя компьютера вашей рабочей группы> - для всех ПК группы.

Сравните результаты с результатами просмотра «Сетевого окружения».

Отчет: полный протокол выполнения этих команд с вашими пояснениями и выводами. Анализируете полученный результат, а не сами команды, подробное знакомство с которыми это предмет следующих лабораторных работ.

8. На схему физической топологии, полученной в п.1 задания на лабораторную работу нанести логическую топологию сети с указанием рабочих групп, имен и адресов каждого компьютера сети.

Отчет: схема логической топологии сети с полной ее спецификацией, совмещенная с физической топологией.

Дополнительные сведения.

Результаты выполнения из командной строки, описанных выше команд, могут быть просмотрены не только на экране, но и перенаправлены в текстовый файл. Это файл потом может быть просмотрен, сохранен или вставлен в какой-либо документ. Например, отчет по лабораторной работе. Так, команда

```
ping ws1 > d:\student\ping1.txt
```

вызовет формирование текстового файла ping1.txt с результатами работы команды ping.

Совокупность таких команд может составлять командный файл. Запуск на выполнение командного файла позволит получить один текстовый файл, содержащий результаты

выполнения сразу нескольких команд. То есть получить один текстовый файл, содержащий все интересующие вас сетевые настройки конкретного компьютера.

5. Контрольные вопросы.

1. На какие два больших класса подразделяют все сетевое оборудование, и чем они отличаются друг от друга.

2. Что такое структурированная кабельная система, и каково ее назначение.

3. Какие элементы относятся к классу пассивного сетевого оборудования.

4. Какие типы кабельных сред могут использоваться для передачи данных в ЛВС.

5. Что определяют стандарты T568A и T568B.

6. Зачем в кабелях типа ”витая пара” отдельные проводники перекручивают между собой. Какое количество витых пар содержать кабели категории 5e и 6.

7. В чем разница между UPT и STP. Каково различие в их использовании.

8. Что такое RJ11, RJ12 и RJ45, в чем их различие и какова область использования.

9. Каково назначение патч-корда и в чем его отличие кабеля внутренней прокладки.

10. Что общего и в чем различие коммутационных панелей и концентраторов.

11. Для каких целей используют концентраторы и коммутаторы.
12. Укажите основные отличия в работе концентраторов и коммутаторов.
13. Каковы отличия в кабельном подключении одного ПК к сетевой карте другого ПК, по сравнению с его подключением к коммутатору ЛВС.
14. Какие основные ограничения следует учитывать при прокладке кабелей ЛВС.
15. Для чего и как используются коммутационные панели.
16. Что обозначает аббревиатура WOL, и какую технологию она поддерживает.
17. Какую функцию работы сетевого адаптера поддерживает микросхема BootRom.
18. Что определяют основные стандарты по кабельным системам.
19. Какие параметры относятся к основными характеристиками кросс-панелей.
20. Для каких целей в коммутаторах используют порт “Uplink”.
21. Укажите последовательность операций, выполняемых при монтаже вилки RJ45.
22. Какой кабель и почему используется при подключении ПК к компьютерной розетки.

Приложение 1. Разделка кабелей в локальных сетях

В данном разделе мы рассмотрим практические приемы работы с кабелями, их разделку и подключение.

П.1.1. Разделка коаксиальных кабелей.

Для разделки разъемов коаксиального кабеля рекомендуется использовать специальные инструменты:

	Устройство для обрезки кабеля (cable stripper)	Устройство для обжима разъема (crimming tool)
		

BNC разъемы для разделки под обжим поставляются в следующем комплекте:

- центральный контакт
- корпус разъема
- фиксирующая трубочка

Разделка разъема начинается с обрезания кабеля. Устройство обрезания должно быть настроено так, чтобы:

- лезвие, режущее внутреннюю изоляцию кабеля, прорезало изоляцию почти до центрального проводника, но не более;
- среднее лезвие, обрезающее оплетку кабеля, слегка подрезало внутреннюю изоляцию, но ни в коем случае не оставляло не прорезанных проволочек в оплетке;

- лезвие, прорезающее наружную изоляцию, резало не на полную глубину изоляции - по надрезанному кольцу лучше потом оторвать кусочек изоляции вручную.

Затем проводят опрессовку разъема на кабеле с помощью устройства обжима в следущей последовательности:

- Вначале на центральный проводник обрезанного кабеля надевают центральный контакт разъема, так чтобы он упирался о внутреннюю изоляцию кабеля. Если это невозможно, следует слегка укоротить центральный проводник кабеля.

- Затем вставляют центральный контакт надетый на кабель в обжимное устройство так, чтобы он упирался выступающим на его конце буртиком во внутренний край гнезда обжимного устройства, предназначенного для обжима центральных контактов, и обжимается.

- Затем надевают на кабель фиксирующую трубочку.

- Далее, например отверткой, слегка раздвигают проводники оплетки и надевают корпус разъема.

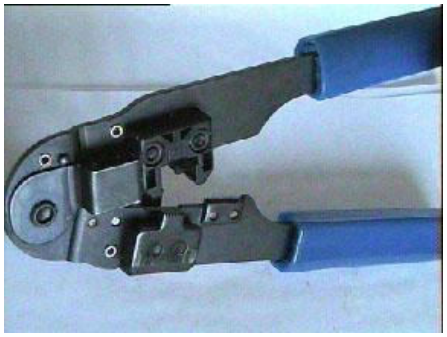
- Продвигают трубочку к корпусу разъема, стремясь к тому, чтобы она прижала проводники оплетки к корпусу разъема. В этот ответственный момент нужно добиться того, чтобы центральный контакт разъема находился на одном уровне с

краем корпуса разъема. Для этого можно поставить край корпуса разъема на твердую поверхность и надавить кабель вниз до достижения желаемого результата.

- Затем аккуратно вставляют фиксирующую трубочку в устройство обжима и сначала слегка придавливают ее к корпусу разъема, следя за тем чтобы между ней и корпусом не образовался зазор, а затем проводят обжим с таким усилием, чтобы сработал контрольный флажок устройства обжима. Если длина фиксирующей трубочки превышает ширину губок обжимателя, то нужно повторить обжим со смещением вдоль трубочки. Иногда бывает полезно повторить обжим с поворотом на 60 или 120 градусов, если грани на трубочке после первого обжима получились неодинаковыми.

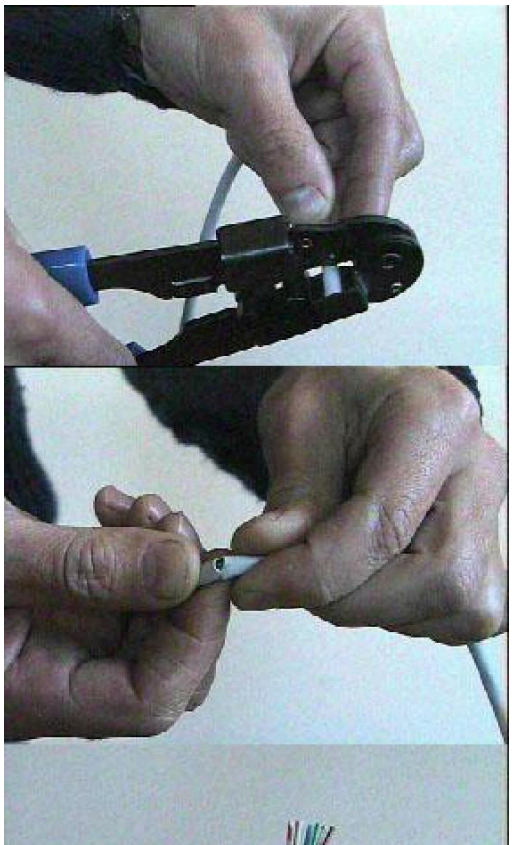
П.1.2. Разделка витой пары .

Для разделки витых пар используют специальное устройство, которое имеет три рабочие области и соответственно выполняет три функции.



- Ближе всего к рукояткам устройства располагается область, в которой установлен нож для обрезания проводников витой пары.
- В центре находится гнездо для обжима разъема.
- В верхней части устройства--область для зачистки наружной изоляции витой пары (внутренняя изоляция проводников не зачищается, а как уже было сказано прорезается контактами разъема).

Последовательность операций при разделке разъема витой пары такова.



1. Вначале проводят зачистку наружной изоляции кабеля.

При зачистке плоского кабеля его упирают в специальный выступ на устройстве, расположенный

в области зачистки, чтобы получить глубину зачистки под стандартный разъем, зажимают кабель и рывком производят зачистку.

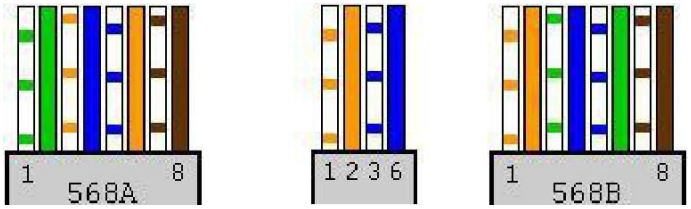
Немного более сложным выглядит процесс зачистки круглых кабелей витых пар. Наружную изоляцию круглого кабеля лучше только слегка надрезать, осторожно поворачивая его в области зачистки, а затем снять кусочек изоляции по кольцевому надрезу вручную.

2. После зачистки разводят провода витой пары в одной плоскости в определенном порядке,

выравнивают длину всех проводов и еще раз ровно подрезают.

Порядок разводки проводов для разъемов RJ-45 определяется стандартом EIA/TIA568B.

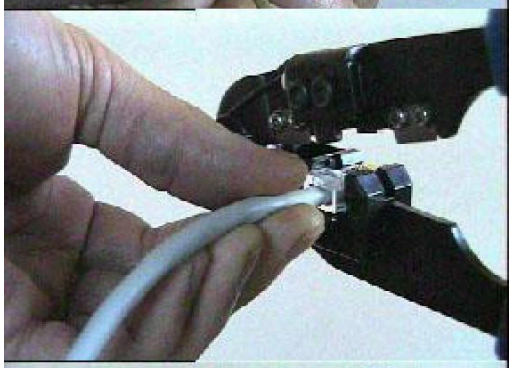
Цифрами на рисунке обозначены номера контактов для витой пары с восьмью и четырьмя жилами



.

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

3а. Если конструктивно разъем выполнен без вставки, то проводники аккуратно заправляются в его корпус до упора в торец разъема. Затем вставляют разъем в гнездо обжимного устройства и надавливают до тех пор пока устройство полностью не закроется.



3б. Если в конструкцию разъема входит вставка, то сначала на проводники витой пары надевается вставка.

Вставка имеет форму крышки спичечного коробка, на одной из поверхностей которого имеются прорези по количеству проводников в витой паре.

Вставку надевают на проводники таким образом:

чтобы прорези были обращены к корпусу разъема.

После насаживания вставки проводники витой пары еще раз подрезают и выравнивают срез с краем вставки.

Для закрепления вставки в этом положении полезно

у противоположного ее конца обжать проводники пальцами, чтобы вставка не смещалась.

Затем вставку с проводниками вставляют в корпус разъема до тех пор пока она не упрется в торец разъема и обжимают разъем также как в случае разъема без вставки.

Многие считают, что это самый сложный этап прокладки сети. Поводков так много, в них так легко запутаться, нужно покупать специальный обжимной инструмент и т.д. На самом деле все довольно просто. Для обжима витой пары вам потребуются специальные клещи и коннекторы RJ-45.

После того как кабеля обжаты вставляем их в разъемы сетевой платы с одной и коммутатора с другой стороны. Осталось только настроить сеть на компьютерах.

Следует отметить, что практически все сети начинались именно так - что в результате приводит к моткам кабелей в коридорах и кабинетах, а если кабели не подписаны и сеть не 10 компьютеров то это просто ужас для обслуживающего персонала. Лучшим решением в этом случае будет СКС.

Лабораторная работа № 15

Тема: «Построение СКС»

1 ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНОЙ РАБОТЫ

1.1 Цель работы: знакомство с особенностями построения СКС

1.2 В результате выполнения лабораторной работы студент должен знать:

- Особенности организации VPN

1.3Используемые программно-технические средства:

Персональная ЭВМ класса IBM PC стандартной конфигурации; операционная система Windows2000/XP/Vista, MicrosoftOfficeWord.

1.4В процессе выполнения лабораторной работы студент должен:

- Ознакомится с теоретическим материалом.
- Подготовить отчет по лабораторной работе.
- Отчитаться по исполненному заданию.

Перед выполнением лабораторной работы каждый студент обязан изучить правила техники безопасности при работе в помещении с электронно-вычислительной техникой.

1.5 Указания по оформлению отчета:

Отчет должен содержать: титульный лист, цель работы; ответы на контрольные вопросы; выводы.

1.6 Указания по сдаче зачета преподавателю

Для сдачи зачета необходимо:

1) выполнить практическое задание

2) предъявить отчет;

3) ответить на контрольные вопросы.

2. Теоретический материал. Построение локальных сетей по стандартам физического и канального уровней. Структурированная кабельная система

Хотя на основе оборудования только этого уровня трудно построить достаточно крупную корпоративную сеть, именно кабельные системы, сетевые адаптеры, концентраторы, мосты и коммутаторы представляют наиболее массовый тип сетевых устройств.

За исключением кабельной системы, которая является протокольно независимой, устройство и функции коммуникационного оборудования остальных типов существенно зависят от того, какой конкретно протокол в них реализован. Концентратор Ethernet устроен не так, как концентратор Token Ring, а сетевой адаптер FDDI не сможет работать

в сети Fast Ethernet. С другой стороны, даже в рамках одной технологии оборудование разных производителей может заметно отличаться друг от друга. В этой главе будут рассмотрены наиболее типичные варианты реализации основных и дополнительных устройств физического и канального уровней.

Кабельная система является фундаментом любой сети. Как при строительстве нельзя создать хороший дом на плохо построенном фундаменте, так и сеть, отлично работающая на плохой кабельной системе, - это явление из области ненаучной фантастики. Если в кабелях ежедневно происходят короткие замыкания, контакты разъемов то отходят, то снова входят в плотное соединение, добавление новой станции приводит к необходимости тестирования десятка контактов разъемов из-за того, что документация на физические соединения не ведется, то ясно, что на основе такой кабельной системы любое, самое современное и производительное оборудование будет работать из рук вон плохо. Пользователи будут недовольны большими периодами простоев и низкой производительностью сети, а обслуживающий персонал будет в постоянной «запарке», разыскивая места коротких замыканий, обрывов и плохих контактов. Причем проблем с кабельной системой становится намного больше при увеличении размеров сети.

Ответом на высокие требования к качеству кабельной системы стали структурированные кабельные системы.

2.1. Иерархия в кабельной системе

Структурированная кабельная система (Structured Cabling System, SCS) - это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Структурированная кабельная система представляет своего рода «конструктор», с помощью которого проектировщик сети строит нужную ему конфигурацию из стандартных кабелей, соединенных стандартными разъемами и коммутируемых на стандартных кроссовых панелях. При необходимости конфигурацию связей можно легко изменить - добавить компьютер, сегмент, коммутатор, изъять ненужное оборудование, а также поменять соединения между компьютерами и концентраторами.

При построении структурированной кабельной системы подразумевается, что каждое рабочее место на предприятии должно быть оснащено розетками для подключения телефона и компьютера, даже если в данный момент этого не требуется. То есть хорошая структурированная кабельная система строится избыточной, В будущем это может сэкономить средства, так как изменения в подключении новых устройств можно производить за счет перекоммутации уже проложенных кабелей.

Структурированная кабельная система планируется и строится иерархически, с главной магистралью и многочисленными ответвлениями от нее (рис. 2.1).

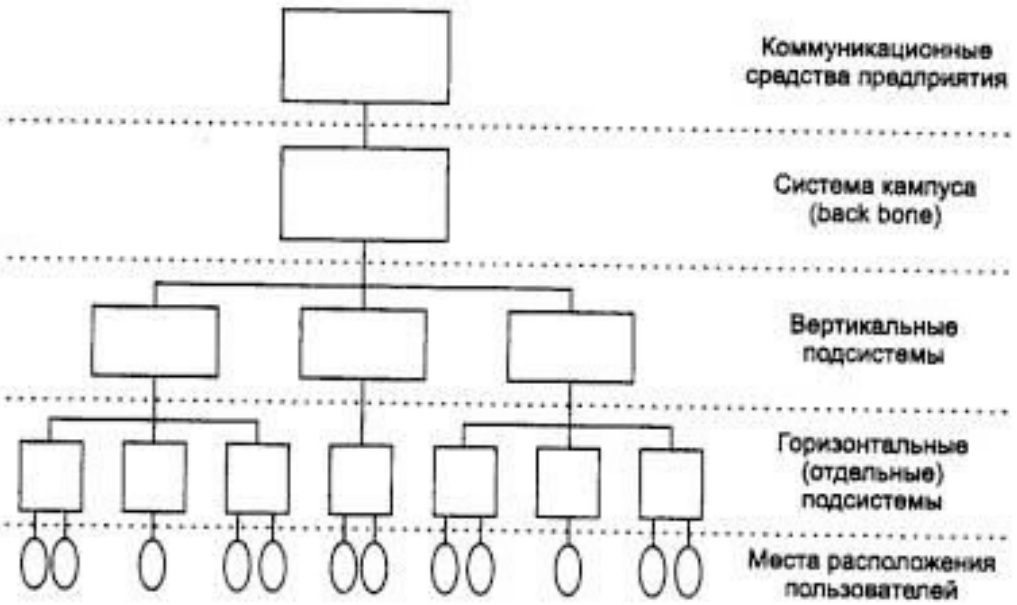


Рис. 2.1. Иерархия структурированной кабельной системы

Эта система может быть построена на базе уже существующих современных телефонных кабельных систем, в которых кабели, представляющие собой набор витых пар, прокладываются в каждом здании, разводятся между этажами, на каждом этаже используется специальный .кроссовый шкаф, от которого провода в трубах и коробах подводятся к каждой комнате и разводятся по розеткам. К сожалению, в нашей стране далеко не во всех зданиях телефонные линии прокладываются витыми парами, поэтому они непригодны для создания компьютерных сетей, и кабельную систему в таком случае нужно строить заново.

Типичная иерархическая структура структурированной кабельной системы (рис. 2.2) включает:

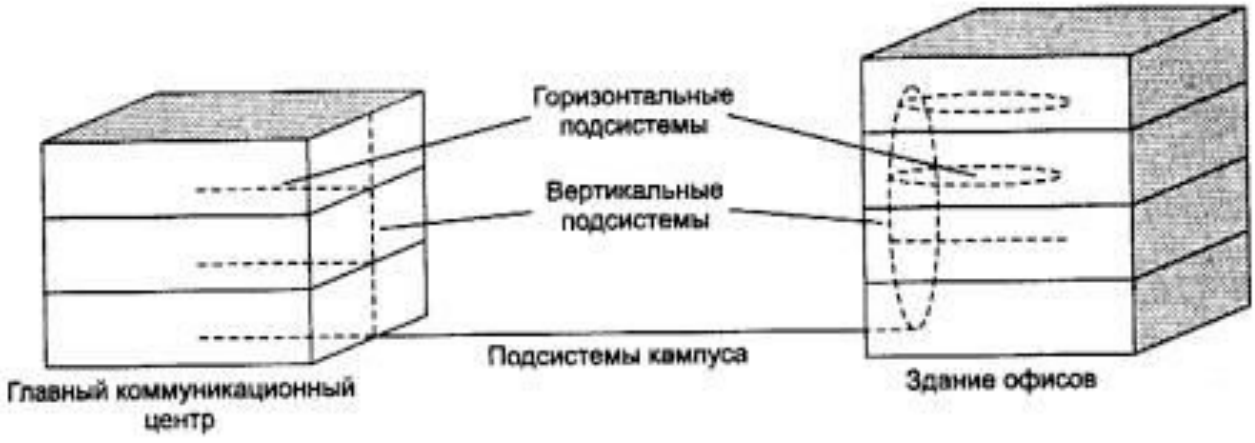


Рис. 2.2. Структура кабельных подсистем

- горизонтальные подсистемы (в пределах этажа);
- вертикальные подсистемы (внутри здания);
- подсистему кампуса (в пределах одной территории с несколькими зданиями).

Горизонтальная подсистема соединяет кроссовый шкаф этажа с розетками пользователей. Подсистемы этого типа соответствуют этажам здания. *Вертикальная подсистема* соединяет кроссовые шкафы каждого этажа с центральной аппаратной здания. Следующим шагом иерархии является *подсистема кампуса,* которая соединяет несколько зданий с главной аппаратной всего кампуса. Эта часть кабельной системы обычно называется магистралью (backbone).

Использование структурированной кабельной системы вместо хаотически проложенных кабелей дает предприятию много преимуществ.

- *Универсальность.* Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеоинформации и даже передачи сигналов от датчиков пожарной безопасности или охранных систем. Это позволяет автоматизировать многие процессы контроля, мониторинга и управления хозяйственными службами и системами жизнеобеспечения предприятия.
- *Увеличение срока службы.* Срок морального старения хорошо структурированной кабельной системы может составлять 10-15 лет.
- *Уменьшение стоимости добавления новых пользователей и изменения их мест размещения.* Известно, что стоимость кабельной системы значительна и определяется в основном не стоимостью кабеля, а стоимостью работ по его прокладке. Поэтому более выгодно провести однократную работу по прокладке кабеля, возможно, с большим запасом по длине, чем несколько раз выполнять прокладку, наращивая длину кабеля. При таком подходе все работы по добавлению или перемещению пользователя сводятся к подключению компьютера к уже имеющейся розетке.
- *Возможность легкого расширения сети.* Структурированная кабельная система является модульной, поэтому ее легко расширять. Например, к магистрали можно добавить новую подсеть, не оказывая никакого влияния на существующие подсети. Можно заменить в отдельной подсети тип кабеля независимо от остальной части сети. Структурированная кабельная система является основой для деления сети на легко управляемые логические сегменты, так как она сама уже разделена на физические сегменты.
- *Обеспечение более эффективного обслуживания.* Структурированная кабельная система облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой. При шинной организации кабельной системы отказ одного из устройств или соединительных элементов приводит к трудно локализуемому отказу всей сети. В структурированных кабельных системах отказ одного сегмента не действует на другие, так как объединение сегментов осуществляется с помощью концентраторов. Концентраторы диагностируют и локализуют неисправный участок.
- *Надежность.* Структурированная кабельная система имеет повышенную надежность, поскольку производитель такой системы гарантирует не только качество ее отдельных компонентов, но и их совместимость.

Первой структурированной кабельной системой, имеющий все современные черты такого типа систем, была система SYSTIMAX SCS компании Lucent Technologies (ранее - подразделение AT&T). И сегодня компании Lucent Technologies принадлежит основная доля мирового рынка. Многие другие компании также выпускают качественные

структурированные кабельные системы, например AMP, BICC Brand-Rex, Siemens, Alcatel, MOD-TAP. На российском рынке успешно завоевывает себе место под солнцем отечественная структурированная кабельная система АйТи-СКС московской компании «АйТи».

2.2. Выбор типа кабеля для горизонтальных подсистем

Большинство проектировщиков начинает разработку структурированной кабельной системы с горизонтальных подсистем, так как именно к ним подключаются конечные пользователи. При этом они могут выбирать между экранированной витой парой, неэкранированной витой парой, коаксиальным кабелем и волоконно-оптическим кабелем. Возможно использование и беспроводных линий связи.

Горизонтальная подсистема характеризуется очень большим количеством ответвлений кабеля (рис. 2.3), так как его нужно провести к каждой пользовательской розетке, причем и в тех комнатах, где пока компьютеры в сеть не объединяются. Поэтому к кабелю, используемому в горизонтальной проводке, предъявляются повышенные требования к удобству выполнения ответвлений, а также удобству его прокладки в помещениях. На этаже обычно устанавливается кроссовая панель, которая позволяет с помощью коротких отрезков кабеля, оснащенного разъемами, провести перекоммутацию соединений между пользовательским оборудованием и концентраторами/коммутаторами.

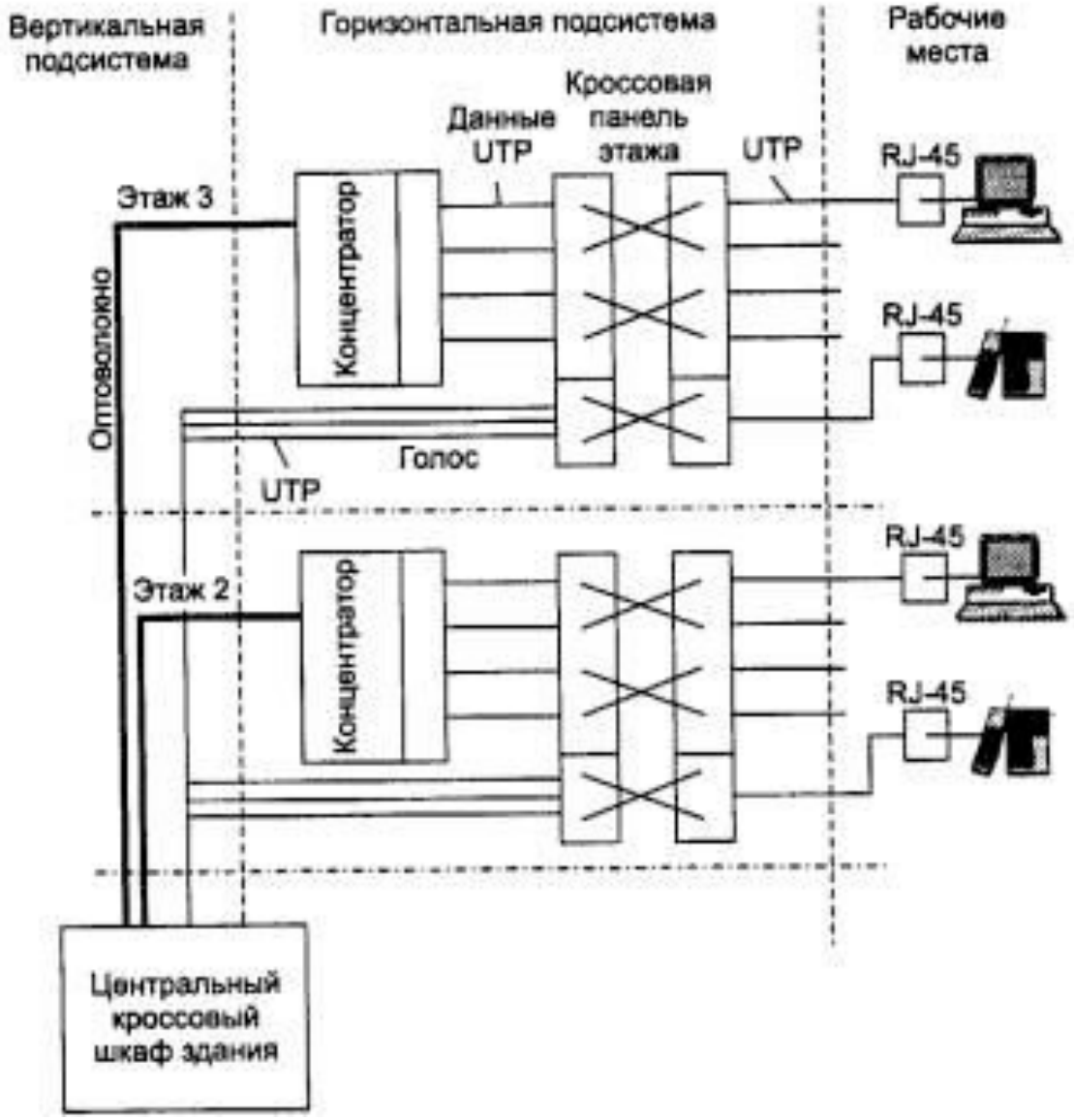


Рис. 2.3. Структура кабельной системы этажа и здания

Медный провод, в частности неэкранированная витая пара, является предпочтительной средой для горизонтальной кабельной подсистемы, хотя, если пользователям нужна очень высокая пропускная способность или кабельная система прокладывается в агрессивной среде, для нее подойдет и волоконно-оптический кабель. Коаксиальный кабель - это устаревшая технология, которой следует избегать, если только она уже широко не используется на предприятии. Беспроводная связь является новой и многообещающей технологией, однако из-за сравнительной новизны и низкой помехоустойчивости лучше ограничить масштабы ее использования неответственными областями.

При выборе кабеля принимаются во внимание следующие характеристики: полоса пропускания, расстояние, физическая защищенность, электромагнитная помехозащищенность, стоимость. Кроме того, при выборе кабеля нужно учитывать, какая кабельная система уже установлена на предприятии, а также какие тенденции и перспективы существуют на рынке в данный момент.

Экранированная витая пара, STP, позволяет передавать данные на большее расстояние и поддерживать больше узлов, чем неэкранированная. Наличие экрана делает ее более

дорогой и не дает возможности передавать голос. Экранированная витая пара используется в основном в сетях, базирующихся на продуктах IBM и Token Ring, и редко подходит к остальному оборудованию локальных сетей.

Неэкранированная витая пара UTP по характеристикам полосы пропускания и поддерживаемым расстояниям также подходит для создания горизонтальных подсистем. Но так как она может передавать данные и голос, она используется чаще.

Однако и коаксиальный кабель все еще остается одним из возможных вариантов кабеля для горизонтальных подсистем. Особенно в случаях, когда высокий уровень электромагнитных помех не позволяет использовать витую пару или же небольшие размеры сети не создают больших проблем с эксплуатацией кабельной системы.

Толстый Ethernet обладает по сравнению с тонким большей полосой пропускания, он более стоек к повреждениям и передает данные на большие расстояния, однако к нему сложнее подсоединиться и он менее гибок. С толстым Ethernet сложнее работать, и он мало подходит для горизонтальных подсистем. Однако его можно использовать в вертикальной подсистеме в качестве магистрали, если оптоволоконный кабель по каким-то причинам не подходит.

Тонкий Ethernet - это кабель, который должен был решить проблемы, связанные с применением толстого Ethernet. До появления стандарта 10Base-T тонкий Ethernet был основным кабелем для горизонтальных подсистем. Тонкий Ethernet проще монтировать, чем толстый. Сети на тонком Ethernet можно быстро собрать, так как компьютеры соединяются друг с другом непосредственно.

Главный недостаток тонкого Ethernet - сложность его обслуживания. Каждый конец кабеля должен завершаться терминатором 50 Ом. При отсутствии терминатора или утере им своих рабочих свойств (например, из-за отсутствия контакта) перестает работать весь сегмент сети, подключенный к этому кабелю. Аналогичные последствия имеет плохое соединение любой рабочей станции (осуществляемое через Т-коннектор). Неисправности в сетях на тонком Ethernet сложно локализовать. Часто приходится отсоединять Т-коннектор от сетевого адаптера, тестировать кабельный сегмент и затем последовательно повторять эту процедуру для всех присоединенных узлов. Поэтому стоимость эксплуатации сети на тонком Ethernet обычно значительно превосходит стоимость эксплуатации аналогичной сети на витой паре, хотя капитальные затраты на кабельную систему для тонкого Ethernet обычно ниже.

Основные области применения оптоволоконного кабеля - вертикальная подсистема и подсистемы кампусов. Однако, если нужна высокая степень защищенности данных, высокая пропускная способность или устойчивость к электромагнитным помехам, волоконно-оптический кабель может использоваться и в горизонтальных подсистемах. С волоконно-оптическим кабелем работают протоколы AppleTalk, ArcNet, Ethernet, FDDI и Token Ring, а также новые протоколы 100AnyLAN, Fast Ethernet, ATM.

Стоимость установки сетей на оптоволоконном кабеле для горизонтальной подсистемы оказывается весьма высокой. Эта стоимость складывается из стоимости сетевых адаптеров (около тысячи долларов каждый) и стоимости монтажных работ, которая в случае оптоволокна гораздо выше, чем при работе с другими видами кабеля.

Преобладающим кабелем для горизонтальной подсистемы является неэкранированная витая пара категории 5. Ее позиции еще более укрепятся с принятием спецификации 802.3ab для применения на этом виде кабеля технологии Gigabit Ethernet.

На рис. 2.4 показаны типовые коммутационные элементы структурированной кабельной системы, применяемые на этаже при прокладке неэкранированной витой пары. Для сокращения количества кабелей здесь установлен 25-парный кабель и разъем для такого типа кабеля Telco, имеющий 50 контактов.

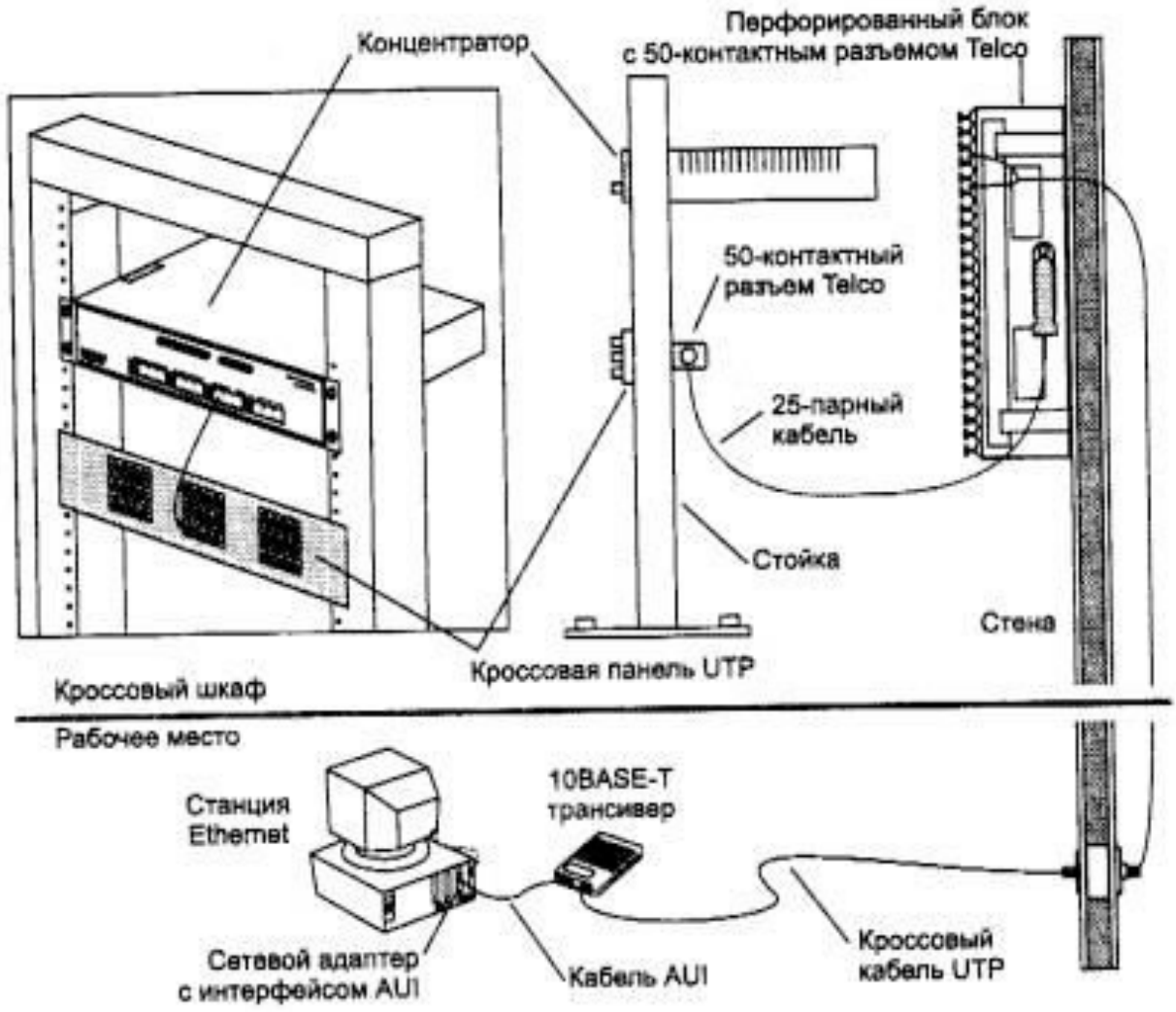


Рис. 2.4. Коммутационные элементы горизонтальной кабельной подсистемы для UTP

2.3. Выбор типа кабеля для вертикальных подсистем

Кабель вертикальной (или магистральной) подсистемы, которая соединяет этажи здания, должен передавать данные на большие расстояния и с большей скоростью по сравнению с кабелем горизонтальной подсистемы. В прошлом основным видом кабеля для вертикальных подсистем был коаксиал. Теперь для этой цели все чаще используется оптоволоконный кабель.

Для вертикальной подсистемы выбор кабеля в настоящее время ограничивается тремя вариантами.

- Оптоволокно - отличные характеристики пропускной способности, расстояния и защиты данных; устойчивость к электромагнитным помехам; может передавать голос, видеоизображение и данные. Но сравнительно дорого, сложно выполнять ответвления.
- Толстый коаксиал - хорошие характеристики пропускной способности, расстояния и защиты данных; может передавать данные. Но с ним сложно работать, хотя специалистов, имеющих подобный опыт работы, достаточно много.
- Широкополосный кабель, используемый в кабельном телевидении, - хорошие показатели пропускной способности и расстояния; может передавать голос, видео и данные. Но очень сложно работать и требуются большие затраты во время эксплуатации.

Применение волоконно-оптического кабеля в вертикальной подсистеме имеет рад преимуществ. Он передает данные на значительно большие расстояния без необходимости регенерации сигнала. Он имеет сердечник меньшего диаметра, поэтому может быть проложен в более узких местах. Так как передаваемые по нему сигналы являются световыми, а не электрическими, оптоволоконный кабель не чувствителен к электромагнитным и радиочастотным помехам, в отличие от медного коаксиального кабеля. Это делает оптоволоконный кабель идеальной средой передачи данных для промышленных сетей. Оптоволоконному кабелю не страшна молния, поэтому он хорош для внешней прокладки. Он обеспечивает более высокую степень защиты от несанкционированного доступа, так как ответвление гораздо легче обнаружить, чем в случае медного кабеля (при ответвлении резко уменьшается интенсивность света).

Оптоволоконный кабель имеет и недостатки. Он дороже чем медный кабель, дороже обходится и его прокладка. Оптоволоконный кабель менее прочный, чем коаксиальный. Инструменты, применяемые при прокладке и тестировании оптоволоконного кабеля, имеют высокую стоимость и сложны в работе. Присоединение коннекторов к оптоволоконному кабелю требует большого искусства и времени, а следовательно, и денег.

Для уменьшения стоимости построения межэтажной магистрали на оптоволокне некоторые компании, например AMP, предлагают кабельную систему с одним коммутационным центром. Обычно, коммутационный центр есть на каждом этаже, а в здании имеется общий коммутационный центр (см. рис. 3.3.), соединяющий между собой коммутационные центры этажей. При такой традиционной схеме и использовании волоконно-оптического кабеля между этажами требуется выполнять достаточное большое число оптоволоконных соединений в коммутационных центрах этажей. Если же коммутационный центр в здании один, то все оптические кабели расходятся из единого кроссового шкафа прямо к разъемам конечного оборудования - коммутаторов, концентраторов или сетевых адаптеров с оптоволоконными трансиверами.

Толстый коаксиальный кабель также допустим в качестве магистрали сети, однако для новых кабельных систем более рационально использовать оптоволоконный кабель, так как он имеет больший срок службы и сможет в будущем поддерживать высокоскоростные и мультимедийные приложения. Но для уже существующих систем толстый коаксиальный кабель служил магистралью системы многие годы, и с этим нужно считаться. Причинами его повсеместного применения были широкая полоса пропускания, хорошая защищенность от электромагнитных помех и низкое радиоизлучение.

Хотя толстый коаксиальный кабель и дешевле, чем оптоволокно, но с ним гораздо сложнее работать. Он особенно чувствителен к различным уровням напряжения заземления, что часто бывает при переходе от одного этажа к другому. Эту проблему сложно разрешить. Поэтому кабелем номер 1 для горизонтальной подсистемы сегодня является волоконно-оптический кабель.

2.4. Выбор типа кабеля для подсистемы кампуса

Как и для вертикальных подсистем, оптоволоконный кабель является наилучшим выбором для подсистем нескольких зданий, расположенных в радиусе нескольких километров. Для этих подсистем также подходит толстый коаксиальный кабель. При выборе кабеля для кампуса нужно учитывать воздействие среды на кабель вне помещения. Для предотвращения поражения молнией лучше выбрать для внешней проводки неметаллический оптоволоконный кабель. По многим причинам внешний кабель производится в полиэтиленовой защитной оболочке высокой плотности. При подземной прокладке кабель должен иметь специальную влагозащитную оболочку (от дождя и подземной влаги), а также металлический защитный слой от грызунов и вандалов. Влагозащитный кабель имеет прослойку из инертного газа между диэлектриком, экраном и внешней оболочкой.

Кабель для внешней прокладки не подходит для прокладки внутри зданий, так как он выделяет при сгорании большое количество дыма.

Выводы

- Кабельная система составляет фундамент любой компьютерной сети. От ее качества зависят все основные свойства сети.
- Структурированная кабельная система представляет собой набор коммуникационных элементов - кабелей, разъемов, коннекторов, кроссовых панелей и шкафов, которые удовлетворяют стандартам и позволяют создавать регулярные, легко расширяемые структуры связей.
- Структурированная кабельная система состоит из трех подсистем: горизонтальной (в пределах этажа), вертикальной (между этажами) и подсистемы кампуса (в пределах одной территории с несколькими зданиями).
- Для горизонтальной подсистемы характерно наличие большого количества ответвлений и перекрестных связей. Наиболее подходящий тип кабеля - неэкранированная витая пара категории 5.
- Вертикальная подсистема состоит из более протяженных отрезков кабеля, количество ответвлений намного меньше, чем в горизонтальной подсистеме. Предпочтительный тип кабеля - волоконно-оптический.
- Для подсистемы кампуса характерна нерегулярная структура связей с центральным зданием. Предпочтительный тип кабеля - волоконно-оптический в специальной изоляции.
- Кабельная система здания строится избыточной, так как стоимость последующего расширения кабельной системы превосходит стоимость установки избыточных элементов.

3. Контрольные вопросы

3.1. Иерархия в кабельной системе

3.2. Выбор типа кабеля для горизонтальных подсистем

3.3. Выбор типа кабеля для вертикальных подсистем

3.4. Выбор типа кабеля для подсистемы кампуса

Лабораторная работа № 16,17

Расчет магистральных подсистем подсистем базовых станций сети стандарта GSM-900
Задание:

Выполнить территориально-частотное планирование подсистемы базовых станций сети GSM-900 на заданной территории. Территория представляет собой городскую застройку, разделенную на две зоны: центральную и периферийную. Для каждой зоны задан радиус R, количество абонентов N в ЧНН, нагрузка от одного абонента Y в ЧНН. При расчете необходимо учитывать следующие ограничения:

• на реализацию системы выделено 27 частотных каналов,

• вероятность блокировки вызова составляет 5%,

• в кластер объединяются 3-4 соты,

• каждая сота разделена на 3 сектора,

• радиус соты в городской застройке 0.4 – 6 км,

• эффективность использования частотного канала должна составлять 70-100%.

Необходимо рассчитать количество сот в системе, количество частотных каналов в соте, выполнить присвоение частот в кластере.

Также необходимо рассчитать количество оборудования BSS, используя при построении сети оборудование фирмы Huawei.

^ 1. Частотно-территориальное планирование сети

В качестве исходных данных возьмем значения, приведенные в таблице 1.
Таблица 1

Для центральной зоны			Для периферийной зоны		
R_1, км	N_1, чел	Y_1, Эрл	R_2, км	N_2, чел	Y_2, Эрл
6,5	21000	0,016	25	60000	0,011

Расчет:

1.1 Рассчитаем площадь центральной зоны S_1:

$$S_1 = \pi \cdot R_1^2 = 3{,}14 \cdot 6{,}5^2 = 132.665\,км^2$$

и площадь периферийной зоны S_2:

$$S_2 = \pi \cdot (R_2 - R_1)^2 = 3{,}14 \cdot (25^2 - 6{,}5^2) = 1829.835\,км^2$$

1.2 Определим суммарную нагрузку в каждой зоне**:**

$$Y_{\Sigma 1} = Y_1 \cdot N_1 = 0{,}016 \cdot 21000 = 336\,Эрл.$$

$$Y_{\Sigma 2} = Y_2 \cdot N_2 = 0{,}011 \cdot 60000 = 660\,Эрл.$$

1.3 Выбрав радиус соты R_1 и R_2 для каждой зоны, находим площадь соты:

$$S_{соты1} = \frac{3}{2} \cdot \sqrt{3} \cdot R_{соты1}^2 = \frac{3}{2} \cdot \sqrt{3} \cdot 2^2 = 10{,}4\,км^2.$$

$$S_{соты2} = \frac{3}{2} \cdot \sqrt{3} \cdot R_{соты2}^2 = \frac{3}{2} \cdot \sqrt{3} \cdot 3^2 = 23.4\,км^2.$$

1.4 Определим количество сот в каждой зоне, учитывая перекрытие сот в пределах 20 – 30%

$$N_{сот\,1} = \frac{S_1}{S_{соты1}} \cdot 1{,}2 = \frac{132.665}{10{,}4} * 1{,}2 = 16 сот$$

$$N_{сот\,2} = \frac{S_2}{S_{соты2}} \cdot 1{,}2 = \frac{1829.835}{23.4} * 1{,}2 = 94\,соты$$

1.5 Определим суммарную нагрузка в соте $Y_{соты\ 1}$ и $Y_{соты\ 2}$:

$$Y_{соты\ 1} = \frac{Y_{\Sigma 1}}{N_{сот1}} = \frac{336}{16} = 21 Эрл$$

$$Y_{соты\ 2} = \frac{Y_{\Sigma 2}}{N_{сот2}} = \frac{660}{94} = 7{,}02\,Эрл.$$

1.6 Определим нагрузку в секторе $Y_{сект\ 1}$ и $Y_{сект\ 2}$:

$$Y_{сект\ 1} = \frac{Y_{соты\ 1}}{3} = \frac{21}{3} = 7 Эрл.$$

$$Y_{сект2} = \frac{Y_{соты\ 2}}{3} = \frac{7{,}02}{3} = 2{,}34\,Эрл.$$

1.7 Количество информационных каналов:

при определении количества информационных каналов в секторе заложим превышение

рассчитанной нагрузки на 20%.

$Y_{сект\,1} * 1{,}2 = 7 * 1{,}2 = 8{,}4 Эрл$

$Y_{сект\,2} * 1{,}2 = 2{,}34 * 1{,}2 = 2{,}808 Эрл$

По таблице Эрлангов с учетом 5% блокировки вызова находим необходимое количество каналов трафика ТСН в секторе для каждой зоны:

$N_{инф.кан.сект1}$ = 13 каналов,

$N_{инф.кан.сект2}$ = 6 каналов.

1.8 Определим общее количество каналов:

зная количество каналов трафика ТСН, по таблице 2 находим необходимое количество каналов управления ССН.

Таблица 2. Соотношение между ТСН и ССН.

ССН	ТСН
1	≤15
2	≤22
3	≤29

Далее, находим общее количество каналов в секторе:

$N_{общ.сект1}$ = ТСН ССН = 13 1 = 14 каналов,

$N_{общ.сект2}$ = ТСН ССН = 6 1 = 7 каналов.

1.9 Находим количество частотных каналов в секторе:

$N_{ЧК\,сект\,1} = N_{общ.сект.1} / 8 = 14 / 8 = 2 канала$

$N_{ЧК\,сект\,2} = N_{общ.сект.2} / 8 = 7 / 8 = 1 канал$

Если эффективность использования частотных каналов низкая, то необходимо найти такой радиус соты, при котором эффективность использования частотных каналов была в пределах 70-100%. В нашем задании эффективность составила 87,5% для центральной зоны и 87,5% для периферийной зоны.

1.10 Общее количество частотных каналов в системе:

(если в кластере 3 соты)

$N_{\sum ЧК\,1} = N_{ЧК\,сект\,1} \cdot 3 \cdot 3 = 18 каналов$

$N_{\sum ЧК\,2} = N_{ЧК\,сект\,2} \cdot 3 \cdot 3 = 9 каналов$

Если максимальное значение из двух чисел больше 27 – максимального количества

частотных каналов, значит необходимо уменьшить радиус соты.

Далее необходимо назначить номера частотных каналов, т.е. присвоить номиналы частот, частотным каналам в каждом секторе. Назначение нужно выполнять таким образом, чтобы номера частотных каналов соседних кластеров отличались на 2 и более.

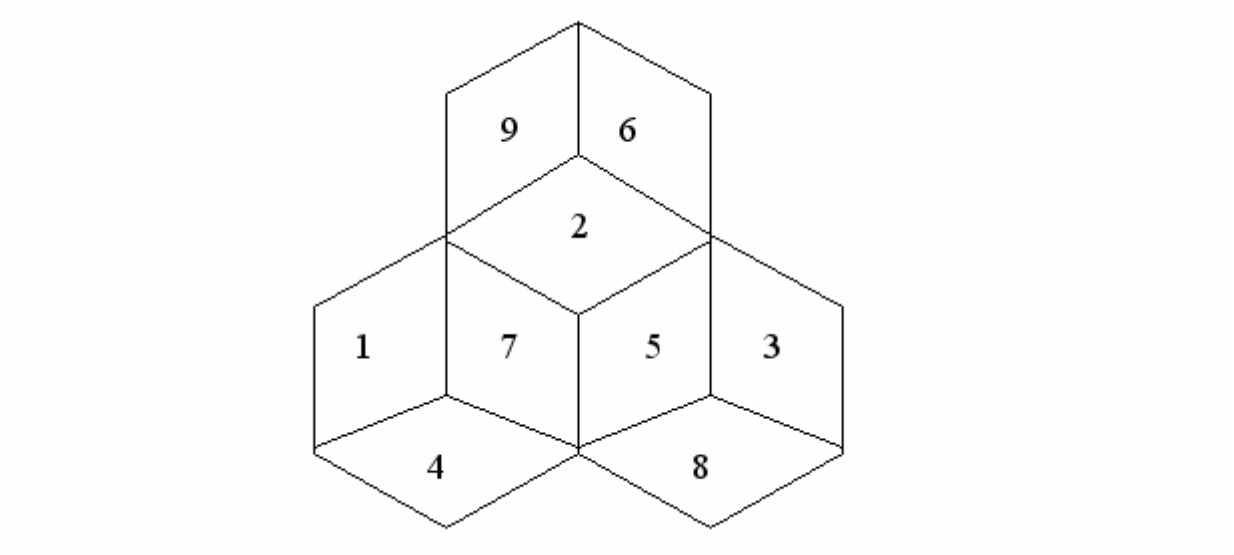


Рис.1. Назначение частотных каналов.

^ 2. Расчет оборудования

На рис. 2 показана обобщенная схема построения сети GSM. Всю сеть можно логически разделить на несколько частей: подсистему базовых станций (BSS), подсистему коммутации (NSS), подсистему ТЭ и ТО (OMC). Кроме того, в отдельную подсистему можно выделить сеть пакетной передачи GPRS.

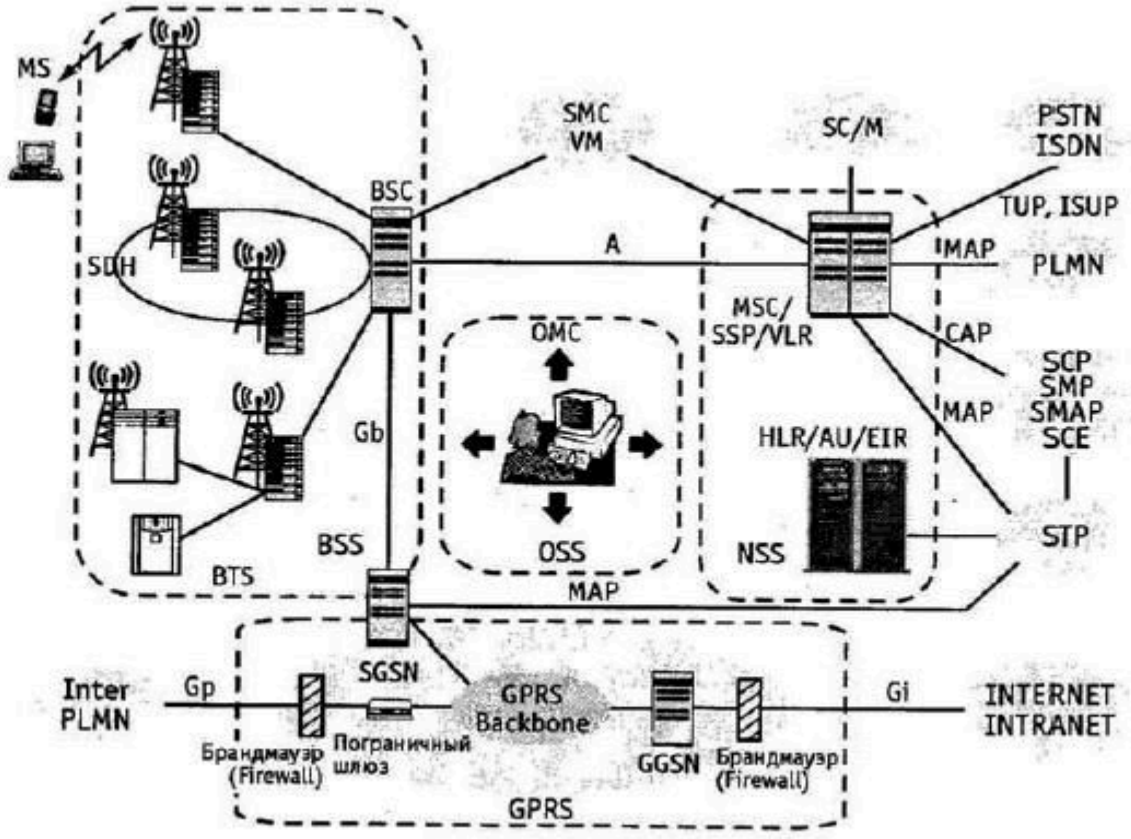


Рис. 2. Обобщенная схема построения сети GSM.
Более подробно рассмотрим подсистему базовых станций. Подсистема базовых станций (BSS) состоит из:

- базовых приемопередающих станций (BTS) различных типов и конфигураций

- контроллера базовых станций (BSC).

Функционально к BSS также относится модуль транскодера TC (часто устанавливается на стороне MSC), который находится между BSC и MSC и осуществляет функции кодирования/декодирования информации, а также мультиплексирования/демультиплексирования по схеме 4:1.

Интерфейс Abis между БС и контроллером является внутренним (каждый производитель оборудования GSM реализует его по-своему), поэтому при установке базовых станций необходимо также использовать контроллер той же компании производителя. Стыковка оборудования NSS и BSS различных поставщиков возможна по открытому A-интерфейсу (между MSC и BSC).

Базовая приемопередающая станция (BTS) выполняет преобразование сигналов радиосвязи в сигналы проводной сети, беспроводное демультиплексирование и мультиплексирование, кодирование радиоканала и функцию перескока по частоте и хэндовера. Компания Huawei предлагает несколько типов базовых станций M900/M1800, которые рассчитаны на различное количество модулей приемопередатчиков (*Transceiver Unit, TRU или TRX*) и имеют разное конструктивное исполнение. Все типы базовых станций позволяют комбинировать модули приемопередатчиков 900 и 1800 МГц. На настоящий момент для продаж в России сертифицированы базовые станции внутреннего типа исполнения BTS312 (12 TRU) и BTS30 (6 TRU).

Базовая станция M900/M1800 состоит из трех частей (рис. 3): основного блока, блока приемопередатчиков (TRU) и антенно-фидерной системы.
Основной блок состоит из:

- блока синхронизации/передачи и управления (TMU),
- блока распределения синхронизации (TDU),
- дополнительного блока передачи (TEU),
- блока питания дополнительного блока передачи (TES),
- блока мониторинга работы вентилятора (FMU),
- блока электропитания (PSU),
- блока мониторинга электропитания и состояния окружающей среды (PMU),
- блока распределения электропитания (SWITCH BOX),
- блока вентилятора (FAN BOX),

- воздухозаборника (AIR BOX).

Блок приемопередатчиков, как следует из названия, включает в себя несколько модулей TRU. В рамках одной BTS возможно смешивание TRU, работающих в диапазоне 900 и 1800 МГц.

Однако следует учесть, что в таком случае для каждого модуля TRU необходимо предусмотреть отдельный модуль комбайнеров (CDU).
Антенно-фидерная система состоит из:

- антенны,
- блока комбайнера (Combiner and Divider Unit, CDU),
- блока мачтового усилителя (Tower Amplification unit, TA),
- системы кабелей с низким потреблением мощности (low consumption transmission cables). Его основные функции - передача и прием радиосигнала, а также выдача аварийной сигнализации.

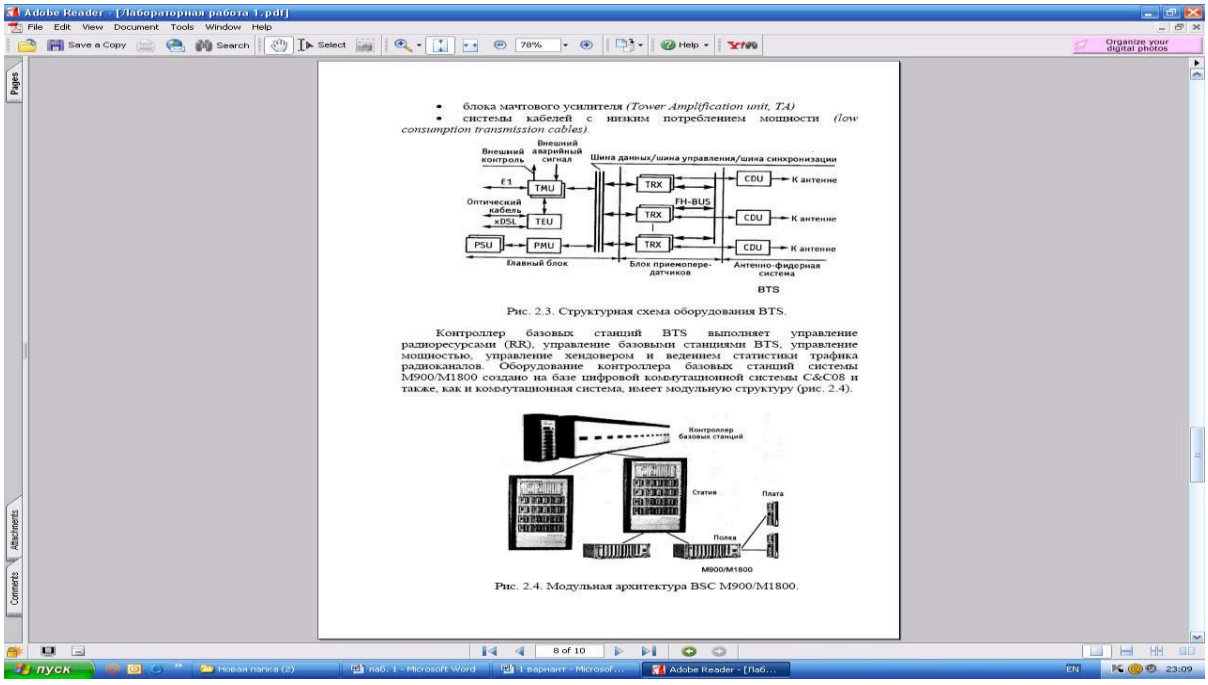


Рис. 3. Структурная схема оборудования BTS.
Контроллер базовых станций BTS выполняет управление радиоресурсами (RR), управление базовыми станциями BTS, управление мощностью и ведением статистики трафика радиоканалов. Оборудование контроллера базовых станций системы M900/M1800 создано на базе цифровой коммутационной системы C&C08 и также, как и коммутационная система, имеет модульную структуру.

Аппаратная часть M900/M1800 BSC состоит из административно-коммуникац. модуля (AM/CM), базового модуля (BM) и центральной базы данных (CDB).

Если емкость M900/M1800 BSC не превышает 128TRU, требуется только один модуль BM, а потребности в модуле AM/CM в этом случае нет. Если емкость BSC превышает 128TRU, необходим модуль AM/CM, а число BM зависит от самой емкости (максимально можно сконфигурировать 8 BM) (Кол-во TRU / 128).

На первом этапе расчета оборудования необходимо выбрать тип BTS. Выбор основывается на количестве частотных каналов, используемых в соте. Для нашего примера выбираем BTS30 6TRX, которая рассчитана на 6 частотных каналов, т.к. в сотах обеих зон используется по три частотных канала.

Количество модулей TRX в BTS равно кол-ву частотных каналов в соте, т.е. равно 9.

Количество модулей CDU равно количеству секторов в соте, т.е. также равно 3.

Количество потоков E1 определяется из соотношения 1TRX – 2 канальных интервала, поэтому нам достаточно 1 потока E1 и, соответственно, одного модуля TMU.

Для расчета оборудования BSC необходимо найти общее количество модулей TRX:

$$\sum TRX = N_{СОТ1} * 3 * N_{ЧКСЕКТ1} + N_{СОТ2} * 3 * N_{ЧКСЕКТ2} = 16 * 3 * 2 + 94 * 3 * 1 = 378$$
$$\sum BM = \sum TRX / 128 = 378 / 128 = 3$$

Таблица 3. Состав оборудования BTS.

	центральная зона	**периферийная зона**
Тип BTS	BTS312	BTS30
Количество BTS	16	94
Количество модулей TRX в BTS	6	3
Количество модулей TRX	96	282
Количество модулей CDU в BTS	3	3
Количество модулей CDU	48	282
Количество модулей TMU в BTS	1	1

Количество модулей TMU	16	94

Таблица 4. Состав оборудования M900/M1800 BSC.

Центральная база данных (CDB)	1
Модуль AM/CM	1
Модуль BM	3

Вывод: произведя вычисления, для проектируемой сети мобильной радиосвязи стандарта GSM-900 получили:

- 16 сот в центральной зоне, 94 сот в периферийной зоне;

- количество частотных каналов в соте центральной зоны 6, периферийной зоны 3;

- количество TRX в проектируемой сети равно 378.

Лабораторные работы цикла МДК.01.02.

Цель и задачи выполнения практических работ

Данные методические указания предназначены для закрепления теоретических знаний, полученных в рамках лекционного курса, и приобретения необходимых практических навыков и умений в решении профессиональных задач по программе междисциплинарного курса МДК 01.02. Математический аппарат для построения компьютерных сетей специальности 09.02.02

В сборнике содержатся методические указания по выполнению следующих практических работ:

ПР.1. Решение задач на тему: Матрица инцидентности. Изоморфизм графов.

ПР.2. Решение задач на тему: Элементы графов и орграфов: путь, длина,

источники, стоки, степени вершин. Деревья. Эйлеров цикл. Плоские и планарные графы

ПР.3. Решение задач на тему: Алгоритм поиска кратчайшего пути. Алгоритм Белламана-Форда (геометрический и аналитический способ задания).

ПР.4. Решение задач на тему: Алгоритм поиска кратчайшего пути. Алгоритм Дейкстры (геометрический и аналитический способ задания).

ПР.5. Решение задач на тему: Алгоритм поиска кратчайшего пути. Алгоритм Флойда-Уоршелла.

ПР.6. Решение задач на тему: Случайные события.

ПР.7. Решение задач на тему: Правило суммы и правило произведения — основные комбинаторные принципы.

ПР.8. Решение задач на тему: Задачи на перестановки, размещения и сочетания.

ПР.9. Решение задач на тему: Полная вероятность. Формула Байеса

ПР.10. Решение задач на тему: Математическое ожидание и дисперсия дискретной случайной величины

ПР.11. Решение задач на тему: Применение неравенств Маркова и Чебышева для решения комбинаторных задач.

ПР.12.Решение на тему: Задачи теории очередей.

ПР.13. Решение задач на тему: Распределение Пуассона. Гауссовское распределение.

ПР.14. Решение задач на тему: Системы массового обслуживания.

В результате выполнения вышеназванных практических работ, предполагается достичь следующих результатов:

1. уметь:
   - Применять алгоритмы поиска кратчайшего пути;

- Планировать структуру сети с помощью графа с оптимальным расположением узлов;
- Использовать математический аппарат теории графов;

2. знать:
   - Вероятностные и стохастические процессы, элементы теории массового обслуживания, основные соотношения теории очередей, основные понятия теории графов;
   - Алгоритмы поиска кратчайшего пути;
   - Основные проблемы синтеза графов атак;
   - Построение адекватной модели;
   - Система топологического анализа защищенности компьютерной сети;
   - Архитектуру сканера безопасности;
   - Экспертные системы.
3. актуализировать общие и профессиональные компетенции:

Код	Наименование результата обучения
Профессиональные компетенции	
П.К. 1.1.	Выполнять проектирование кабельной структуры компьютерной сети
П.К. 1.2.	Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.
П.К. 1.3.	Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.
П.К. 1.4.	Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.
П.К. 1.5.	Выполнять требования нормативно-технический документации, иметь опыт оформления проектной документации.
Общие компетенции	
О.К. 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
О.К. 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
О.К. 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
О.К. 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
О.К. 5	Использовать информационно-коммуникационные технологии для

	совершенствования профессиональной деятельности.
О.К. 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
О.К. 7	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
О.К. 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
О.К. 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Тематика практических занятий и задания к ним

Практическое занятие 1.

Решение задач по теории графов. Матрица инцидентности. Изоморфизм графов.

1. Цель занятия:

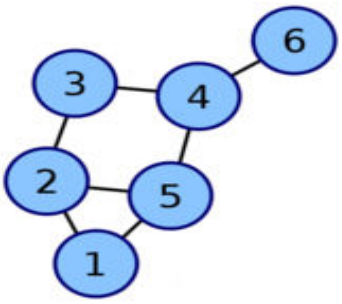
❖ Получить практические навыки, при представлении графов в матричной форме.

❖ Изучить методы построения матриц инцидентности и матриц инциденций

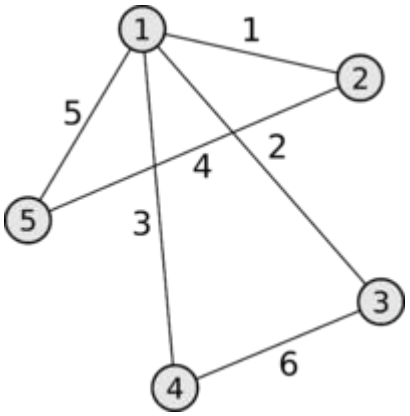
2. Продолжительность занятия: 4 часа
3. Необходимые принадлежности:
   - ПК, подключенный к ГКС
   - Методические рекомендации
4. Краткие теоритические сведения:

Матрица инцидентности — одна из форм представления графа, в которой указываются связи между инцидентными элементами графа (ребро(дуга) и вершина). Столбцы матрицы соответствуют ребрам, строки — вершинам. Ненулевое значение в ячейке матрицы указывает связь между вершиной и ребром (их инцидентность).

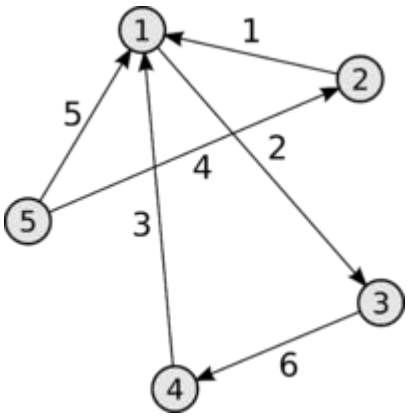
В случае ориентированного графа каждой дуге <x,y> ставится в соответствие "-1" в строке вершины x и столбце дуги <x,y> и "1" в строке вершины y и столбце дуги <x,y>; если связи между вершиной и ребром нет, то в соответствующую ячейку ставится "0".



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

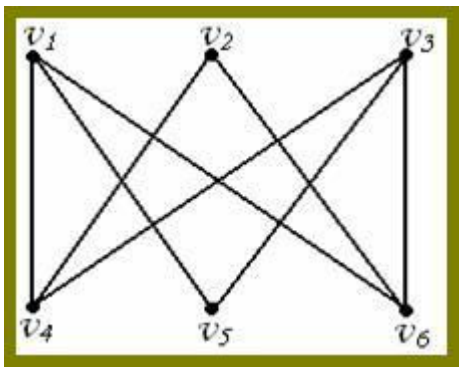


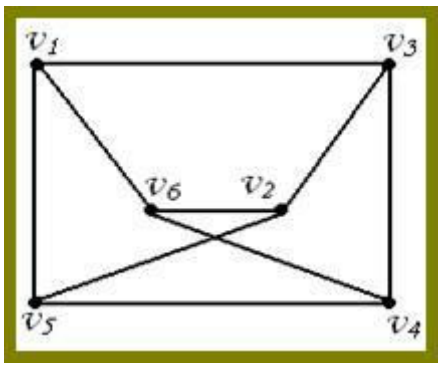
$$\begin{pmatrix} -1 & 1 & -1 & 0 & -1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

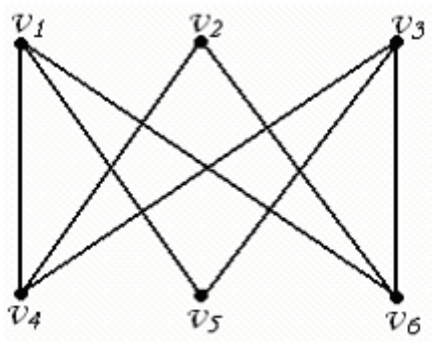
Графы G’ и G’’ называются ***изоморфными***, если существует взаимно-однозначное соответствие (биекция) между их ребрами и вершинами, причем ребра соединяют соответствующие вершины.

Изоморфизм графов означает, что можно так переобозначить вершины первого графа, что в новых обозначениях вершины и ребра будут совпадать со вторым графом.

Пример:







5. Задания:

Решите ниже перечисленные задачи

6. Порядок выполнения практической работы

Задача 1.

Построить матрицы смежности и инцидентности для графа *G = (V, X)*

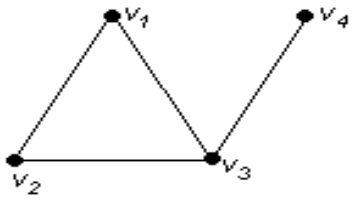


Рис. 25.

Задача 2

Построить матрицы смежности и инцидентности для орграфа *D= (V, X)*

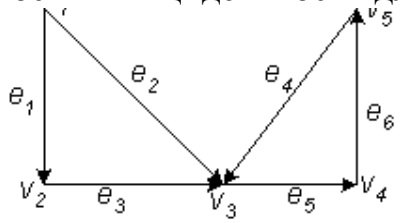


Рис. 27.

Задача 3.

Задана матрица

$$B = \begin{pmatrix} 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 3 & 1 & 0 & 2 \end{pmatrix}$$

Нарисовать на плоскости орграф G = (X, U), единственный с точностью до изоморфизма, имеющий заданную матрицу B своей матрицей смежности. Найти матрицу инцидентности $C=C_{ij}$ орграфа G.

Задача 4

Задана симметрическая матрица A неотрицательных целых чисел.

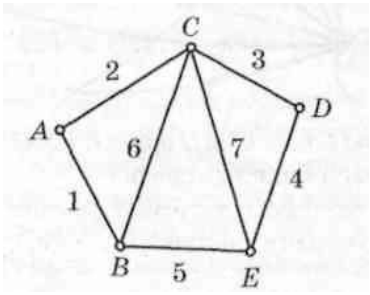
$$A=\begin{matrix} 1211 \\ 2011 \\ 1102 \\ 1120 \end{matrix}$$

1. Нарисовать на плоскости граф G=(X,U)(единственный с точностью до изоморфа), имеющий заданную матрицу A своей матрицей смежности. Найти матрицу инцидентности $R= (r_{ij})$ графа G.
2. Нарисовать на плоскости орграф G=(X,U) (единственный с точностью до

изоморфизма), имеющий заданную матрицу А свое матрицей смежности. Найти
матрицу инцидентности C=(C_{ij}) орграфа G.

Задача5.

Эйлерову цепь в неориентированном графе *G*, изображенном на рис.



Задача 6

Задан граф $G\ V, E$,где $V = \ v_1, v_2, v_3, v_4, v_5\ ; E_{v_1} = \ v_1, v_3, v_5\ ; E_{v_2} = \emptyset; E_{v_3} = \ v_1, v_2, v_5\ ; E_{v_4} = \ v_1\ ; E_{v_5} = \ v_1, v_2, v_3, v_4, v_5\ .$

1. Задайте граф с помощью бинарного отношения, т. ею совокупности множества V и подмножества множества упорядоченных пар $v_i, v_j\ \in V \times V.$

2. Изобразите орграф на рисунке.

3. Постройте матрицу смежности.

Оформите и сдайте отчет

7. *Содержание отчета:*

1) Номер и тема лабораторной работы;
2) Цель работы;
3) Необходимые принадлежности; задание; методика работы;
4) Ход выполнения лабораторной работы (этапы);
5) Выводы по выполненной работе.

8. *Контрольные вопросы:*

1.Что такое граф.

2. Как строятся матрицы смежности

3. Как строятся матрицы инциденций

4. Что такое изоморфизм графов

Практическое занятие 2.

Решение задач по теории графов. Элементы графов и орграфов: путь, длина, источники, стоки, степени вершин. Деревья. Эйлеров цикл. Плоские и планарные графы

1. Цель занятия:

- Получить практические навыки построения графов
- Сформировать представление об основных понятиях теории графов.
- Отработать на примерах основные понятия теории графов

2. Продолжительность занятия: 4 часа**.**

Краткие теоретические сведения:

Степенью или валентностью вершины p n графа Г, обозначаемой через d n , называют число рёбер (дуг), инцидентных этой вершине. Вершина степени 1 называется висячей или концевой. Ребро, инцидентное висячей вершине, называется висячим. Вершина степени 0 называется изолированной. По определению петля при вершине p n , добавляет 2 в степень соответствующей вершины.

Маршрут в графе Г представляет собой конечную чередующуюся последовательность вершин и рёбер. Маршрут называется открытым, если его концевые вершины различны, в противном случае он называется замкнутым. Маршрут называется цепью, если все его рёбра различны. Цепь называется элементарной, если при обходе по какому-нибудь направлению каждая вершина цепи встречается только один раз. Замкнутый маршрут образует цикл. Цикл может быть простым, если он содержит отличные друг от друга рёбра, сложным – в противном случае, элементарным, если при обходе по какому-нибудь направлению каждая вершина цикла встречается только один раз. Очевидно, нет смысла вводить для цепи термин “простая цепь”, если термин “простой”, как в определении графа и цикла, означает отсутствие повторяющихся рёбер.

Последовательность дуг, при которой конец одной дуги является началомдругой, называется путём. Если начальная и конечная точки путисовпадают, образуется контур. Длиной пути (или контура) называют число дуг, которые его образуют. Петля – контур единичной длины. Будем также под длиной пути от одной вершины до другой понимать количество рёбер, входящих в соответствующий маршрут. То есть будем применять термин “длина пути” не только к орграфам. Во всех случаях для орграфов и для неориентированных графов дуги и рёбра будем считать столько раз, сколько раз они входят в путь или маршрут.

Дерево — *это* связный ациклический граф. *Связность означает наличие путей между любой* парой *вершин, ацикличность — отсутствие циклов и то, что между парами вершин имеется только по одному пути.*

Лес - упорядоченное множество упорядоченных деревьев.

Эйлеров цикл *— это цикл графа, проходящий через каждое ребро (дугу) графа ровно по одному разу*

Планарный граф — граф, который может быть изображён на плоскости без пересечения ребер. Иначе говоря, граф планарен, если он изоморфен некоторому **плоскому графу**, т.е. графу, изображённому на плоскости так, что его вершины — это точки плоскости, а рёбра — кривые на ней. Области, на которые граф разбивает плоскость, называются его **гранями.**
Граф G наз. плоским, если он может быть изображен на плоскости так, что вершинам соответствуют различные точки плоскости, а линии, соответствующие ребрам (исключая их концевые точки), не проходят через точки, соответствующие вершинам, и не пересекаются.

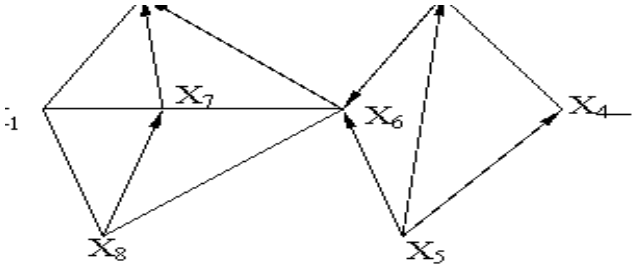
5. Задание

В следующих задачах найти путь, длину графа, установить планарность графа

6. Порядок выполнения работы

Решите следующие задачи:

Задача 1.



Каждое ребро полного графа с 11 вершинами покрашено в один из двух цветов: красный или синий. Докажите, что либо "красный", либо "синий" граф не является плоским.

Задача 2.

Найти все пути из X4 в X7 в графе G=(X,Г) изображенном на рисунке.

Задача 3.

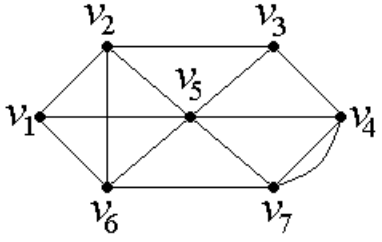
На пришкольном участке растут 8 деревьев: яблоня, тополь, береза, рябина, дуб, клен, лиственница и сосна. Рябина выше лиственницы, яблоня выше клена, дуб ниже березы, но выше сосны, сосна выше рябины, береза ниже тополя, а лиственница выше яблони. Расположите деревья от самого низкого к самому высокому.

Задача 4.

У Наташи есть 2 конверта: обычный и авиа, и 3 марки: прямоугольная, квадратная и треугольная. Сколькими способами Наташа может выбрать конверт и марку, чтобы отправить письмо?

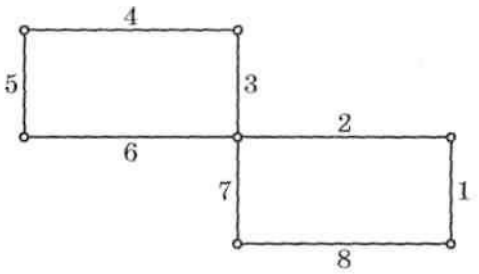
Задача 5.

Найдите Эйлерову цепь в неориентированном графе *G*.



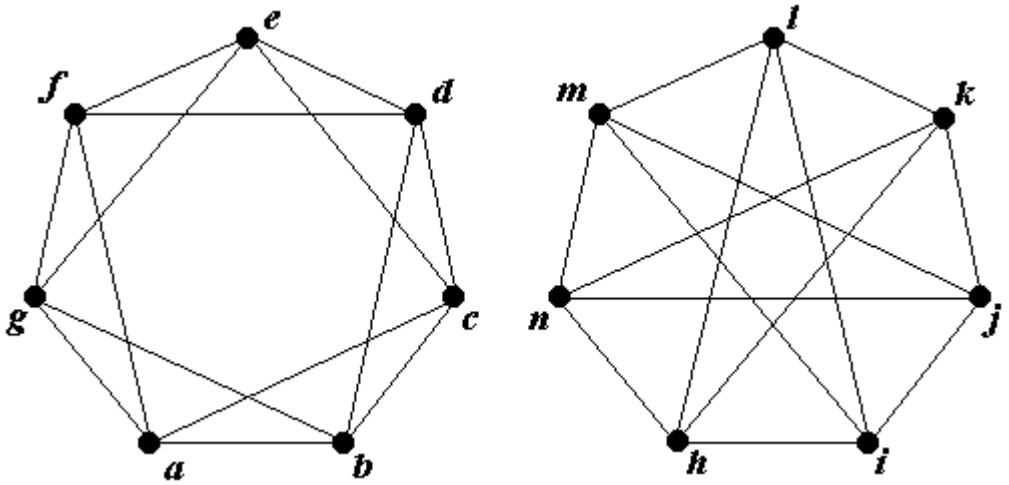
Задача 6.

Найдите эйлеров цикл в эйлеровом графе.



Задача 7.

Постройте эйлеров цикл для второго графа



Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

1) Номер и тема практической работы;
2) Цель работы;
3) Необходимые принадлежности; задание; методика работы;
4) Ход выполнения практической работы (этапы);
5) Выводы по выполненной работе.

8. Контрольные вопросы

1. Докажите, что в связном графе существует эйлерова цепь тогда и только тогда, когда граф содержит не более двух вершин нечётной степени.

2. Докажите, что изоморфизм сохраняет циклы графа.

3. На основании решения какой задачи Леонард Эйлер вывел постулаты теории графов.

4. Чему равна степень изолированной вершины.

5. Что такое петля.

Практическое занятие 3.

Решение задач по теории графов. Алгоритм поиска кратчайшего пути. Алгоритм Беллмана-Форда (геометрический и аналитический способ задания).

1. Цель занятия:

Получить практические навыки, необходимые, при программировании и построении алгоритмов поиска кратчайшего пути

Нахождение кратчайшего пути в ориентированных и неориентированный графах

2. Продолжительность занятия: 4 часа.

Краткие теоретические сведения:

Зада́ча о кратча́йшем пути́ (англ. shortest path problem) — задача поиска самого короткого пути (цепи) между двумя точками (вершинами) на графе, в которой минимизируется сумма весов ребер, составляющих путь.

Кратчайшая (простая) цепь часто называется геодезической. Задача о кратчайшем пути является одной из важнейших классических задач теории графов. Сегодня известно множество алгоритмов для ее решения.

У данной задачи существуют и другие названия: задача о минимальном пути или, в устаревшем варианте, задача о дилижансе.

Значимость данной задачи определяется ее различными практическими применениями. Например в GPS-навигаторах, где осуществляется поиск кратчайшего пути между двумя перекрестками. В качестве вершин выступают перекрестки, а дороги являются ребрами, которые лежат между ними. Сумма расстояний всех дорог между перекрестками должна быть минимальной, тогда найден самый короткий путь.

Существуют различные постановки задачи о кратчайшем пути:

- **Задача о кратчайшем пути в заданный пункт назначения.** Требуется найти кратчайший путь в заданную вершину назначения t, который начинается в каждой из вершин графа (кроме t). Поменяв направление каждого принадлежащего графу ребра, эту задачу можно свести к задаче о единой исходной вершине (в которой осуществляется поиск кратчайшего пути из заданной вершины во все остальные).
- **Задача о кратчайшем пути между заданной парой вершин.** Требуется найти кратчайший путь из заданной вершины u в заданную вершину v.
- **Задача о кратчайшем пути между всеми парами вершин.** Требуется найти кратчайший путь из каждой вершины u в каждую вершину v. Эту задачу тоже можно решить с помощью алгоритма, предназначенного

для решения задачи об одной исходной вершине, однако обычно она решается быстрее.

5. Задание.

С помощью алгоритма Беллмана — Форда найти решения задач.

Продемонстрировать реализацию этого алгоритма на языке программирования

6. Порядок выполнения работы.

Задача 1.

Определить наименьшую стоимость проезда из 1 в s менее чем с k пересадками.

Реализовать алгоритм на языке программирования C++ и Pascal

Задача 2.

Дан ориентированный граф, в котором могут быть кратные ребра и петли. Каждое ребро имеет вес, выражающийся целым числом (возможно, отрицательным). Гарантируется, что циклы отрицательного веса отсутствуют.

Дан ориентированный граф, в котором могут быть кратные ребра и петли. Каждое ребро имеет вес, выражающийся целым числом (возможно, отрицательным). Гарантируется, что циклы отрицательного веса отсутствуют.

Реализовать алгоритм на языке программирования C++ и Pascal.

Задача 3.

В Летней Компьютерной Школе (ЛКШ) построили аттракцион "Лабиринт знаний". Лабиринт представляет собой **N** комнат, занумерованных от **1** до **N**, между некоторыми из которых есть двери. Когда человек проходит через дверь, показатель его знаний изменяется на определенную величину, фиксированную для данной двери. Вход в лабиринт находится в комнате **1**, выход - в комнате **N**. Каждый ученик проходит лабиринт ровно один раз и попадает в ту или иную учебную группу в зависимости от количества набранных знаний (при входе в лабиринт этот показатель равен нулю). Ваша задача показать наилучший результат.

Реализовать алгоритм на языке программирования C++ и Pascal.

Задача 4.

Во входном файле в первой строке записано число **N** (**1** $\leq$ **N** $\leq$ **100**) - количество вершин графа. В следующих **N** строках находится по **N** чисел - матрица смежности графа. Веса ребер не превышают по модулю **10000**. Если ребра нет, соответствующее значение равно **100000**.

Реализовать алгоритм на языке программирования C++ и Pascal.

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

1) Номер и тема практической работы;
2) Цель работы;
3) Необходимые принадлежности; задание; методика работы;

4) Ход выполнения практической работы (этапы);
5) Выводы по выполненной работе.

8. Контрольные вопросы

1. Чем отличается кратчайший путь от остова
2. Какими языками программирования реализуется алгоритм Беллмана-Форда
3. Путь прохождения алгоритма Беллмана-Форда от первоначальной вершины до остальных.

Практическое занятие 4.

Решение задач по теории графов. Алгоритм поиска кратчайшего пути. Алгоритм Дейкстры (геометрический и аналитический способ задания).

1. Цель занятия:

- Получить практические навыки при программировании и построении алгоритмов поиска кратчайшего пути
- Нахождение кратчайшего пути в ориентированных и неориентированный графах

2. Продолжительность занятия: 4 часа.

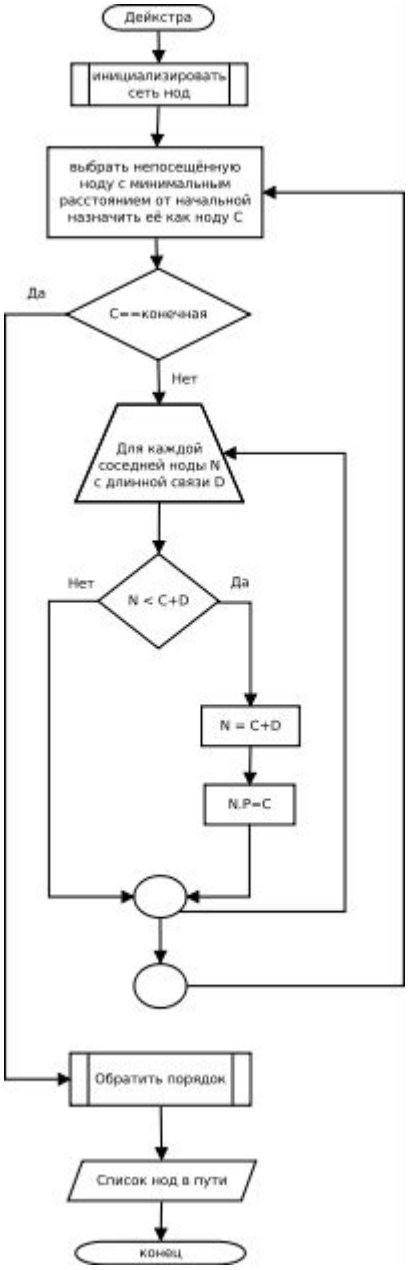
Краткие теоретические сведения:

Алгори́тм Де́йкстры (англ. Dijkstra's algorithm) — алгоритм на графах, изобретённый нидерландским учёным Э. Дейкстрой в 1959 году. Находит кратчайшее расстояние от одной из вершин графа до всех остальных. Алгоритм работает только для графов без рёбер отрицательного веса. Алгоритм широко применяется в программировании и технологиях, например, его используют протоколы маршрутизации OSPF и IS-IS.

Время работы алгоритма Дейкстры

Сложность алгоритма Дейкстры зависит от способа нахождения вершины v, а также способа хранения множества непосещенных вершин и способа обновления меток. Обозначим через n количество вершин, а через m — количество ребер в графе G.

- В простейшем случае, когда для поиска вершины с минимальным d[v] просматривается все множество вершин, а для хранения величин d — массив, время работы алгоритма есть O(n2 + m). Основной цикл выполняется порядка n раз, в каждом из них на нахождение минимума тратится порядка n операций, плюс количество релаксаций (смен меток), которое не превосходит количества ребер в исходном графе.
- Для разреженных графов (то есть таких, для которых m много меньше n2) непосещенные вершины можно хранить в двоичной куче, а в качестве ключа использовать значения d[i], тогда время извлечения вершины из U станет log n, при том, что время модификации d[i] возрастет до log n. Так как цикл выполняется порядка n раз, а количество релаксаций не больше m, скорость работы такой реализации O(n*log n + m*log n)
- Если для хранения непосещенных вершин использовать фибоначчиеву кучу, для которой удаление происходит в среднем за O(log n), а уменьшение значения в среднем за O(1), то время работы алгоритма составит O(n*log n + m)



Блок-схема алгоритма Дейкстры

5. Задание

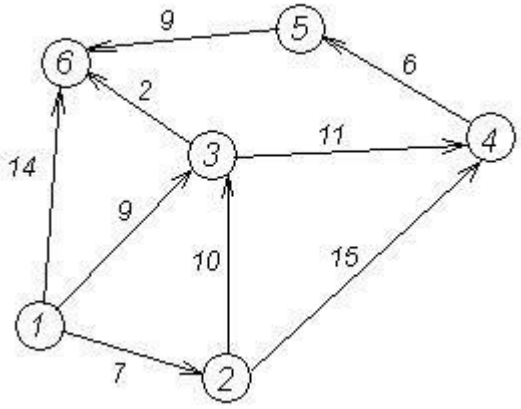
Найти с помощью алгоритма Дейкстры кратчайшие пути в графах.

6. Порядок выполнения работы

Задача 1.

Найти расстояния от 1-й вершины до всех остальных.

Реализовать алгоритм на языке программирования C++ и Pascal.



Задача 2.

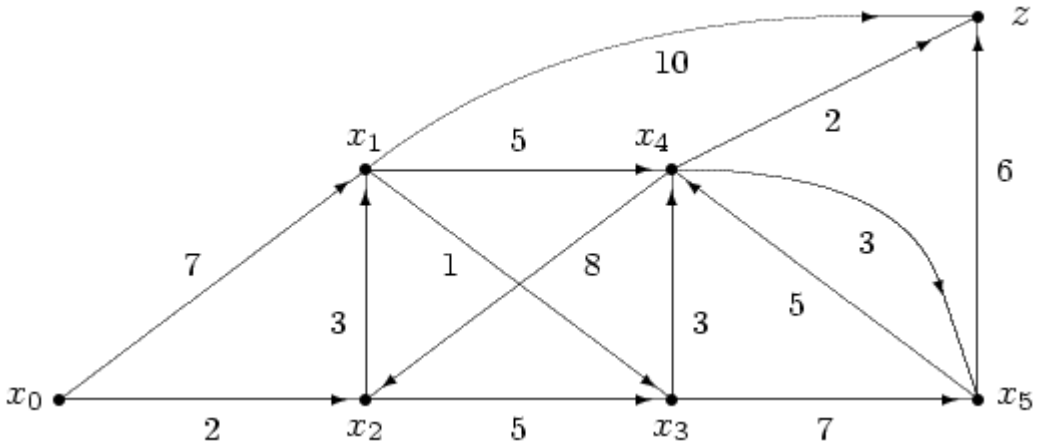
необходимо добраться на самолете из города A в город B при условии, что между ними нет прямого авиационного сообщения, затратив при этом минимальные средства (при условии, что заданы возможные промежуточные аэропорты, для каждой пары аэропортов известно, существует ли между ними прямой маршрут, и если да, то известна минимальная стоимость перелета по этому маршруту).

Реализовать на языке программирования C++ и Pascal

Задача 3.

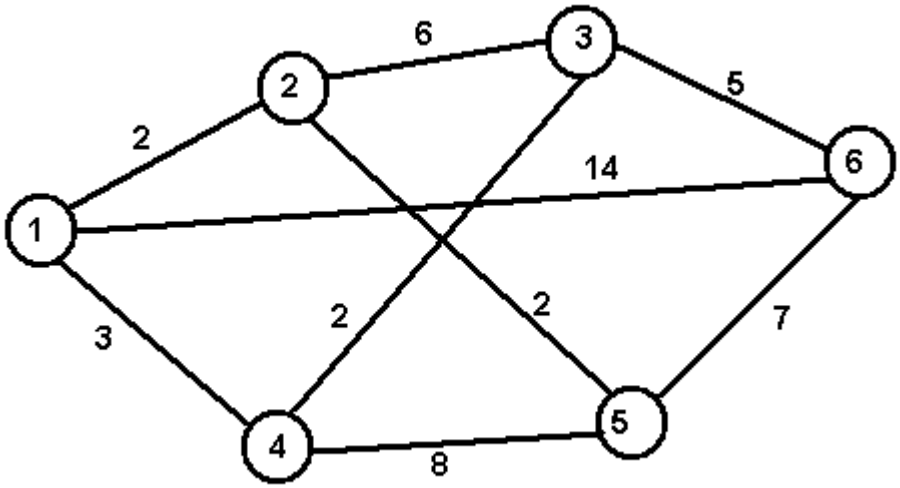
Пусть Г(X, U, Ф) — простой орграф, для каждого ребра u ∈ U определен вес w(u)≥0.

Найти кратчайший путь между выделенными вершинами x_0 и z.



Задача 4.

Найдите кратчайший путь из вершины **1** в вершину **6**, используя **алгоритм Дейкстры**:



Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

- Номер и тема практической работы;
- Цель работы;
- Необходимые принадлежности; задание; методика работы;
- Ход выполнения практической работы (этапы);
- Выводы по выполненной работе.

8. Контрольные вопросы:

1. Достоинства и недостатки алгоритма Дейкстры
2. Основное отличие алгоритма Дейкстры от алгоритма Беллмана-Форда.
3. В чем заключается сложность алгоритма Дейкстры
4. Что такое отрицательный вес ребра

Практическое занятие 5.

Решение задач по теории графов. Алгоритм поиска кратчайшего пути.

Алгоритм Флойда-Уоршелла.

1. Цель занятия:

- Получить практические навыки при программировании и построении алгоритмов поиска кратчайшего пути.
- Нахождение кратчайшего пути в ориентированных и неориентированный графах

2. Продолжительность занятия: 4 часа.

Краткие теоретические сведения:

Алгоритм Флойда — Уоршелла — динамический алгоритм для нахождения кратчайших расстояний между всеми вершинами взвешенного ориентированного графа. Разработан в 1962 году Робертом Флойдом и Стивеном Уоршеллом, хотя в 1959 году Бернард Рой (Bernard Roy) опубликовал практически такой же алгоритм, но это осталось незамеченным.
Более строгая формулировка этой задачи следующая:
есть ориентированный граф G = (V, E) каждой дуге v -> w этого графа сопоставлена неотрицательная стоимость C[v, w]. Общая задача нахождения кратчайших путей заключается в нахождении для каждой упорядоченной пары вершин v, w) любого пути от вершины v в вершины w, длина которого минимальна среди всех возможных путей от v к w.

Оценка сложности алгоритма.

Время выполнения этой программы имеет порядок $0(V^3)$, поскольку в ней практически нет ничего, кроме вложенных друг в друга трех циклов. Доказательство "правильности" работы этого алгоритма также очевидно и выполняется с помощью математической индукции по k, показывая, что на k-й итерации вершина k включается в путь только тогда, когда новый путь короче старого.

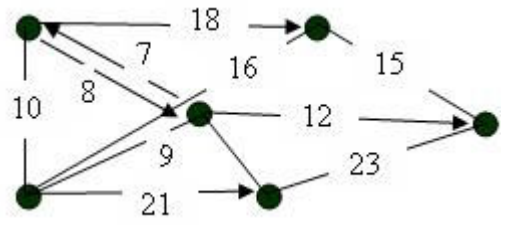
5. Задание.

С помощью алгоритма Флойда-Уоршилла найти решения следующих задач.

6. Порядок выполнения работы

Задача 1.

Необходимо найти кратчайшие пути между каждой парой вершин в графе, представленном на рисунке:



Задача 2.

Дан непустой взвешенный граф $G=(V, E)$ с произвольными весами ребер (дуг). Требуется найти длины кратчайших путей между всеми парами вершин графа, если в графе нет циклов (контуров) отрицательной суммарной длины, либо обнаружить наличие таких контуров.

Задача3.

Дан ориентированный взвешенный граф G = (V, E) с весовой функцией w: E→ R. Для каждой пары вершин u, vÎ V требуется найти кратчайший путь из u в v, т.е. путь наименьшей длины (длина пути определяется как сумма весов всех его ребер). Таким образом, ответом в задаче о кратчайших путях можно считать таблицу, в которой на пересечении строки u и столбца v находится вес кратчайшего пути из u в v (конечно, дополненную информацией о самих путях).

Задача 4.

Прочитать из файла граф, заданный там списком ребер с весами. Подсчитать длины кратчайших путей из каждой вершины в каждую, вывести кратчайший путь между какой-либо парой вершин.

Задача 5.

Задан взвешенный ориентированный граф (не более 100 вершин) без циклов отрицательного веса. Заданы m запросов вида (i; j). На каждый такой запрос требуется вывести длину кратчайшего пути из вершины i в вершину j.

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

1) Номер и тема практической работы;
2) Цель работы;
3) Необходимые принадлежности; задание; методика работы;
4) Ход выполнения практической работы (этапы);
5) Выводы по выполненной работе.

8. Контрольные вопросы.

1. Что такое динамический алгоритм
2. Дайте характеристику понятия «время выполнения алгоритма»
3. Вложенные друг в друга циклы.

Практическое занятие 6.
Решение задач по комбинаторике. Случайные события.

1. Цель занятия:

- Получить практические навыки в решении комбинаторных задач.
- знакомство с основными законами случайных событий.

2. Продолжительность занятия: 4 часа.

Краткие теоретические сведения:

В современной науке и технике изучаются и широко используются статистические законы, которым подчиняются различные случайные события. В радиофизике уделяется много внимания таким случайным явлениям, как шум усилителей, нестабильность генераторов, рассеяние волн на случайных неоднородностях среды и другим. Не менее важные примеры можно привести из других разделов физики.
Любое измерение, с какой бы тщательностью оно ни выполнялось, не дает абсолютно точного результата, поэтому, приступая к работе в лаборатории, необходимо иметь некоторые сведения о статистических законах, чтобы оценивать точность измерений.
Систематическое изложение статистических понятий и законов составляет содержание математической дисциплины «теория вероятностей» и специальных разделов физики (статистическая механика, статистическая радиофизика и т.п.)
Цель этой работы – познакомиться на простых примерах с некоторыми понятиями, которыми пользуются для описания случайных явлений, и некоторыми статистическими законами.
Случайное событие. Познакомимся с этим понятием на примере случайных явлений, которые можно наблюдать в опытах с доской Гальтона. Это доска, поставленная вертикально, в которую набито много гвоздей. На гвозди можно бросать через воронку дробинки или сыпать зерна. Упавшие частицы попадают в ряд ячеек, расположенные внизу. Бросим дробинку в воронку доски Гальтона. Она совершит сложный путь по гвоздям и упадет в одну из ячеек. Проделаем много раз такой опыт, соблюдая с максимальной тщательностью неизменность условий опыта, и убедимся, что опыты невозможно абсолютно точно воспроизвести. Дробинки летят по-разному. Попадание одной дробинки в какую-то ячейку назовем событием. Чтобы выразить то обстоятельство, что при самом тщательном соблюдении постоянства контролируемых внешних условий дробинки летят по разным путям, которые нельзя до опыта предсказать, говорят: падение дробинки – случайное событие.
Случайная величина. Случайное событие можно описывать количественно с помощью случайных величин. Например, номер ячейки, в которую упала частица, путь, пройденный ею, и время падения – это случайные величины, описывающие одно и то же событие.

В рассмотренном примере номер ячейки может принимать только счетное множество значений. Такие случайные величины называют дискретными. Величины, которые принимают непрерывный ряд значений (например, время падения), называют непрерывными случайными величинами.

Относительная частота и вероятность события. Произведем бросание частицы на доску Гальтона N раз. (Можно бросать одну частицу N раз или N одинаковых частиц один раз.) Каждое такое бросание называют испытанием. Обозначим через N_k число испытаний, при которых частица попадает в ячейку с номером k. Отношение N_k/N называется относительной частотой события, заключающегося в попадании частицы в ячейку k. Если произвести несколько серий испытаний с N опытами в каждой серии, то обнаружится, что относительная частота – случайная величина, но чем больше N, тем меньше она меняется от серии к серии. Иначе говоря, N_k/N слабо флюктуирует при большом N. Это свойство будем называть устойчивостью относительной частоты события. Устойчивость относительных частот при большом числе испытаний– частный случай проявления основного статистического закона, который называют законом больших чисел.

5. Задания.

При помощи формального аппарата теории вероятности решить следующие задачи

6. Порядок выполнения работы

Задача1.

Даны следующие события:

A={при бросании монеты выпадает "орел"};
B={при бросании кубика выпадает тройка};
C={при бросании кубика выпадает шестерка};
D={из колоды карт вытянут карту красной масти};
E={из колоды карт вытянут туза};
F={из колоды карт вытянут пику}.

Определите, какие из следующих событий более вероятные, какие - менее вероятные, и расположите их на вероятностной шкале.

Задача 2.

Какова вероятность того, что «доминошка», наудачу извлеченная из полного набора домино, имеет сумму очков, равную 5?

Задача 3.

Одновременно бросают два кубика.

а) Сколько равновозможных исходов у этого эксперимента?
б) Какова вероятность того, что на кубиках выпадет равное количество очков?
в) Какова вероятность, что на первом кубике выпадет количество очков больше, чем на втором?

г) Какая сумма будет выпадать чаще 5 или 6?

Задача 4.

На двери первого подъезда стоит кодовый замок, в котором нужно правильно нажать три цифры из десяти, а на двери второго подъезда - семь цифр из десяти. Порядок цифр при этом не учитывается. К какому замку труднее подобрать код?

Задача 5.

Из 20 экзаменационных билетов 3 содержат простые вопросы. Пять студентов по очереди берут билеты. Найти вероятность того, что хотя бы одному из них достанется билет с простыми вопросами.

Задача 6.

Из множества всех последовательностей длины 10, состоящих из цифр 0; 1; 2; 3, наудачу выбирается одна. Какова вероятность того, что выбранная последовательность содержит ровно 5 нулей, причем два из них находятся на концах последовательности.

Задача 7.

Имеется 100 одинаковых деталей, среди которых 3 бракованных. Найти вероятность того, что взятая наудачу деталь без брака.

Задача 8.

Код банковского сейфа состоит из 6 цифр. Найти вероятность того, что наудачу выбранный код содержит различные цифры?

Задача 9.

В компании 10 акционеров, из них трое имеют привилегированные акции. На собрание акционеров явилось 6 человек. Найти вероятность того, что среди явившихся акционеров:

а) все трое акционеров с привилегированными акциями отсутствуют;
б) двое присутствуют и один не явился.

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета:

.Номер и тема практической работы;
.Цель работы;
.Необходимые принадлежности; задание; методика работы;
.Ход выполнения практической работы (этапы);
.Выводы по выполненной работе.

8. Контрольные вопросы:

- Что такое событие?

- Что такое вероятность наступления события?
- Что такое абсолютный результат.
- Охарактеризуйте термин испытание.

Практическое занятие 7.

Решение задач по комбинаторике. Правило суммы и правило произведения — основные комбинаторные принципы.

1. Цель занятия:

- Получить практические навыки в решении комбинаторных задач.

2. Продолжительность занятия: 4 часа

Краткие теоретические сведения:

Рождение комбинаторики как раздела математики связано с трудами великих французских математиков 17 века Блеза Паскаля (1623–1662) и Пьера Ферма (1601–1665) по теории азартных игр. Эти труды содержали принципы определения числа комбинаций элементов конечного множества. С 50-х годов 20 века интерес к комбинаторике возрождается в связи с бурным развитием кибернетики.

Комбинаторика изучает количество комбинаций, подчиненных определенным условиям, которые можно составить из элементов, безразлично какой природы, заданного конечного множества. При непосредственном вычислении вероятностей часто используются формулы комбинаторики.

Основные правила комбинаторики – это **правило суммы** и **правило произведения**.

- **Правило суммы**

Если некоторый элемент A можно выбрать **n** способами, а элемент B можно выбрать **m** способами, то выбор «либо A, либо B» можно сделать **n + m** способами.

Правило произведения

Если элемент A можно выбрать **n** способами, а элемент B можно выбрать **m** способами, то пару A и B можно выбрать **n • m** способами.

5. Задание.

С помощью правил суммы и произведения решить следующие задачи

6. Порядок выполнения работы.

Задача 1.

Сколько существует трехзначных чисел, начинающихся с 3 или 4? Трехзначные числа, о которых идет речь в задаче, разбиваются на два непересекающихся класса. К одному из них относятся числа, начинающиеся с 3, а ко второму - с 4. Для подсчета чисел в первом классе заметим, что существует один возможный исход для первой цифры (она должна быть равна 3), 10 исходов для второй и 10 исходов для последней цифры.

Задача 2.

Государственный регистрационный знак легкового автомобиля состоит из трех цифр и трех букв русского алфавита (не считая кода города). Будем

считать, что в номере можно задействовать любую последовательность букв и цифр. Сколько различных автомобильных номеров может выдать ГИБДД?

Задача 3.

Ребенку предложили мешок с конфетами трех наименований: «Мишка на севере» (A), «Карамель» (B) и «Шоколад» (C). Сколькими способами ребенок может выбрать две конфеты из мешка?

Задача 4.

Целые числа в компьютере представляются строчкой из N двоичных знаков. Первый из них отведен на знак (+ или -), а остальные N - 1 отвечают за модуль целого числа. Сколько различных целых чисел может использовать компьютер?

Задача 5.

По меню в ресторане можно выбрать ровно три из семи главных блюд. Сколькими способами Вы можете сделать заказ?

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

1) Номер и тема практической работы;
2) Цель работы;
3) Необходимые принадлежности; задание; методика работы;
4) Ход выполнения практической работы (этапы);
5) Выводы по выполненной работе.

8. Контрольные вопросы.

- Что изучает комбинаторика как наука?
- Основные комбинаторные правилам
- Что такое выборка?

Практическое занятие 8.

Решение задач по теории вероятностей. Задачи на перестановки, размещения и сочетания.

1. Цель занятия:

- Научиться решать задачи, используя правила комбинаторики;
- Решать задачи, используя операции над множествами;

2. Продолжительность занятия: 4 часа.

Краткие теоретические сведения:

Перестановки. Упорядоченные выборки, объемом *N* из *N* элементов, где все элементы различны, называются перестановками из *N* элементов. Число перестановок из *N* элементов обозначается *Pn*. $P_n=A^n_n=n\cdot(n-1)\cdot\ldots\cdot2\cdot1=n!$

Размещения. Упорядоченные выборки объемом *M* из *N* элементов (*M* < *N*), где все элементы различны, называются размещениями. Число размещений из *N* элементов по *M* обозначается A_n^m . $A^k_n=n!/(n-k)!$

Сочетания. Неупорядоченные выборки объемом *M* из *N* элементов (*M* < *N*) называются сочетаниями. Их число обозначается C_n^m . $C^k_n=A^k_n/k!=n!/(n-k)!k!$

5. Задания

С помощью правил размещения, сочетания, перестановки решить следующие задачи.

6. Ход выполнения работы:

Задача 1.

Пусть даны цифры: 7; 8; 9; 4; 5; 6. Определить сколько двузначных чисел можно составить из этих цифр.

Задача 2.

На библиотечной полке стоят 30 книг, причем 27 - книги разных авторов и еще 3 книги автора. Сколькими способами можно расставить эти книги так, чтобы книги одного автора стояли рядом друг с другом?

Задача 3.

Учитель хочет назначить 3 студентов для уборки класс из учеников. Сколькими способами можно это сделать?

Задача 4.

В пассажирском поезде 9 вагонов. Сколькими способами можно рассадить в поезде 4 человека, при условии, что все они должны ехать в различных вагонах?

Задача 5.

В пассажирском поезде 9 вагонов. Сколькими способами можно рассадить в поезде 4 человека, при условии, что все они должны ехать в различных

вагонах?

Задача 6.

В группе 9 человек. Сколько можно образовать разных подгрупп при условии, что в подгруппу входит не менее 2 человек?

Задача 7.

Группу из 20 студентов нужно разделить на 3 бригады, причем в первую бригаду должны входить 3 человека, во вторую — 5 и в третью — 12. Сколькими способами это можно сделать.

Задача 8.

Для участия в команде тренер отбирает 5 мальчиков из 10. Сколькими способами он может сформировать команду, если 2 определенных мальчика должны войти в команду?

Задача 9.

Сколько слов можно получить, переставляя буквы в слове Гора и Институт?

Задача 10.

Каких чисел от 1 до 1 000 000 больше: тех, в записи которых встречается единица, или тех, в которых она не встречается?

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

6) Номер и тема практической работы;
7) Цель работы;
8) Необходимые принадлежности; задание; методика работы;
9) Ход выполнения практической работы (этапы);
10) Выводы по выполненной работе.

8. Контрольные вопросы

Приведите формулы определяющие число сочетаний, размещений и перестановок без повторений

Приведите формулы определяющие число сочетаний, размещений и перестановок с повторениями

Что такое неупорядоченная выборка?

Практическое занятие 9.

Решение задач по теории вероятностей. Полная вероятность. Формула Байеса

1. Цель занятия

- Получить практические навыки, необходимые для решения задач теории вероятности по формуле Байеса

2. Продолжительность занятия: 4 часа

Краткие теоретические сведения:

Пусть событие А может произойти при выполнении одного из несовместных событий $B_1, B_2, \ldots, B_n$. Если эти события (их еще называют гипотезами) образуют полную группу несовместных событий, то вероятность события А вычисляется по формуле полной вероятности: $P(A)=P\left(B_1\right)P_{B_1}(A)+\ldots+P\left(B_n\right)P_{B_n}(A).$

- Если событие *A* произошло, то это может изменить вероятности гипотез B_1, B_2, ..., B_n которые вычисляются по *формуле Байеса*

$$P_A\left(B_i\right)=\frac{P\left(B_i\right)P_{B_i}(A)}{P(A)},i=1,2,\ldots,n.$$

(*формуле Бейеса*):

- Вероятности исходных событий $P\left(B_i\right)$ называются *априорными вероятностями*. Вероятности этих событий в предположении, что *A* наступило - $P_A\left(B_i\right)$ - *апостериорными вероятностями*.

5. Задание.

Решить задачи теории вероятности применяя формулу Байеса

6. Ход выполнения работы

Задача 1.

В эксперименте используются карточки белого и зеленого цветов, на которых изображены геометрические фигуры: квадрат или треугольник. Вероятность того, что на зеленой карточке изображен треугольник, равна 0,85. Для белой карточки эта вероятность равна 0,9. Найти вероятность того, что наудачу взятая карточка будет содержать треугольник, если в эксперименте используется одинаковое количество карточек зеленого и белого цветов

Задача 2.

Прибор, установленный на борту самолета, может работать в двух режимах: в условиях нормального крейсеровского полёта и в условиях перегрузки при взлете и посадке. Крейсерский режим полета составляет 80% всего времени полёта, условия перегрузки–20%. Вероятность выхода прибора из строя за время полета в нормальном режиме равна 0,1, в условиях перегрузки–0,4. Найти вероятность того, что прибор не откажет в течение всего полёта.

Задача 3.

Имеются три урны с шарами. В первой урне 4 белых и 5 черных, во второй – 5 белых и 4 черных, в третьей–6 белых шаров. Некто выбирает наугад одну из урн и вынимает из нее шар.
Найти вероятность того, что: а) этот шар окажется белым,
б) белый шар вынут из второй урны.

Задача 4

Имеется 10 одинаковых урн, из которых в девяти находятся по два черных и по два белых шара, а в одной –5 белых и 1 черный шар. Из урны, взятой наудачу, извлечен белый шар. Какова вероятность того, что шар извлечен из урны, содержащей 5 белых шаров.

Задача 5

На вход радиолокационного устройства с вероятностью 0,8 поступает смесь полезного сигнала с помехой, а с вероятностью 0,2 – только помеха. Если поступает полезный сигнал с помехой, то прибор регистрирует наличие какого -
то сигнала с вероятностью 0,7; если только помеха – то с вероятностью 0,3. Известно, что устройство зарегистрировало наличие какого - то сигнала. Найти вероятность того, что в его составе есть полезный сигнал

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые принадлежности; задание; методика работы;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

8. Контрольные вопросы

- Понятие условной вероятности.
- Несовместные события.
- Что такое априорная вероятность?
- Дайте определение понятия гипотеза.

Практическое занятие 10.

Решение задач по теории вероятностей. Математическое ожидание и дисперсия дискретной случайной величины.

1. Цель занятия:

Получить практические навыки в решении задач теории вероятности.

2. Продолжительность занятия: 4 часа.

Краткие теоретические сведения:

Случайной называют величину, которая в результате испытания примет случайно одно и только одно значение из множества возможных значений.

Дискретной (прерывной) называют случайную величину, которая принимает отдельные возможные значения с определенными вероятностями.

Непрерывной называют случайную величину, которая может принимать все значения из некоторого конечного или бесконечного промежутка.

Пример 1. Случайной величиной является число очков, выпавших при бросании игральной кости, или рост случайно выбранного из учебной группы студента. В первом случае мы имеем дело с дискретной случайной величиной (она принимает значения из дискретного числового множества M={1, 2, 3, 4, 5, 6}; во втором случае - с непрерывной случайной величиной (она принимает значения из непрерывного числового множества - из промежутка числовой прямой I=[100, 3000]).

Математическим ожиданием дискретной случайной величины называют сумму произведений всех ее возможных значений на их вероятности.

Если дискретная случайная величина принимает только значения $x_1, x_2, ..., x_n$, вероятности которых соответственно равны $p_1, p_2, ..., p_n$. Тогда математическим ожидание определяется равенством:

$$M(X) = x_1p_1 + x_2p_2 + ... + x_np_n.$$

Дисперсией (рассеянием) дискретной случайной величины называют математическое ожидание квадрата отклонения случайной величины от ее математического ожидания:

$$D(X) = M[X - M(X)]^2.$$

5. Задание.

Применив математическое ожидание решите следующие задачи.

6. Ход выполнения работы

Задача 1.

Выпущено 1000 лотерейных билетов: на 5 из них выпадает выигрыш в сумме 500 рублей, на 10 – выигрыш в 100 рублей, на 20 – выигрыш в 50 рублей, на

50 – выигрыш в 10 рублей. Определить закон распределения вероятностей случайной величины X – выигрыша на один билет.

Задача 2.

Найти математическое ожидание числа очков, выпадающих при бросании игральной кости.

Задача 3.

Устройство состоит из трех независимо работающих элементов. Вероятность отказа каждого элемента в одном опыте равна 0,1. Составить закон распределения числа отказавших элементов в одном опыте, построить многоугольник распределения. Найти функцию распределения F(x) и построить ее график. Найти математическое ожидание, дисперсию и среднее квадратическое отклонение дискретной случайной величины.

Задача 4.

На полке из 6 книг 3 книги по математике и 3 по физике. Выбирают наудачу три книги. Найти закон распределения числа книг по математике среди выбранных книг. Найти математическое ожидание этой случайной величины.

Задача 5.

На элеватор прибыло $N_1 = 6$ машин агрофирмы «А1» и $N_2 = 9$ машин агрофирмы «А2». Под разгрузку случайным образом загоняются $n = 6$ машин. Число машин фирмы «А1», попавших под разгрузку -случайная величина.

1) составить рад распределения этой случайной величины.

2) найти функцию распределения и построить ее график.

3) найти математическое ожидание, дисперсию и среднеквадратическое отклонение этого распределения.

4) определить коэффициент асимметрии.

Задача 6.

Из поступающих в ремонт 10 часов 7 нуждаются в общей чистке механизма. Часы не рассортированы по виду ремонта. Мастер, желая найти часы, нуждающиеся в чистке, рассматривает их поочередно и, найдя такие часы, прекращает дальнейший просмотр. Составить закон распределения числа просмотренных часов. Найти математическое ожидание и дисперсию этой случайной величины.

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

.Номер и тема практической работы;

.Цель работы;

.Необходимые принадлежности; задание; методика работы;

.Ход выполнения практической работы (этапы);

.Выводы по выполненной работе.

8. Контрольные вопросы

- Что такое степень характеризующая существенные черты распределения случайной величины?
- Что такое степень разбросанности значений случайной величины относительно среднего?
- Перечислите свойства математического ожидания.
- Когда две случайные величины независимы?

Практическое занятие 11.

Решение задач по распределениям. Применение неравенств Маркова и Чебышева для решения комбинаторных задач.

1. Цель занятия:

Получить практические навыки, необходимые для решения задач распределения вероятностей

2. Продолжительность занятия: 2 часа.

Краткие теоретические сведения:

Если случайная величина **X** принимает только неотрицательные значения и имеет математическое ожидание **M(X)**, то для любого положительного **A** верно неравенство:

$$P(X > A) \le \frac{M(X)}{A}.$$

Это выражение читается и понимается следующим образом: вероятность того, что случайная величина ***X*** в результате испытания примет значение большее ***A***, где ***A*** – произвольное положительное число, не превышает величины $\frac{M(X)}{A}$, где ***M(X)*** – математическое ожидание случайной величины ***X***.

Неравенство Маркова может быть записано и в другой форме: $P(X \le A) \ge 1 - \frac{M(X)}{A}.$

Область применения неравенства Маркова - любые **неотрицательные** случайные величины.

Неравенство Чебышева справедливо для **любых** случайных величин, имеющий математическое ожидание и дисперсию. Оно может быть записано в виде:

$$P(|X - M(X)| < \varepsilon) \ge 1 - \frac{D(X)}{\varepsilon^2}.$$

Читать и понимать данное соотношение следует так: вероятность того, что

отклонение случайной величины **X** от ее математического ожидания по абсолютной величине меньше числа ε, где $\varepsilon > 0$, будет не менее, чем $1 - \frac{D(X)}{\varepsilon^2}$.

$$P(|X - M(X)| > \varepsilon) \le \frac{D(X)}{\varepsilon^2}.$$

Неравенство Чебышева может быть представлено и в другой форме:

5. Задание.

По неравенствам Маркова и Чебышева оценить вероятность отклонения случайной величины от ее математического ожидания.

6. Ход выполнения работы.

Задача 1.

За сутки на станцию скорой помощи поступает в среднем 500 вызовов. Определить вероятность того, что за следующие сутки на станцию поступит а) более 600 вызов; б) не более 800 вызовов.

Задача 2.

Сумма всех вкладов в отделении банка составляет 2 млн. руб., а вероятность того, что случайно взятый вклад не превысит 10 тыс. руб. равна 0,6. Оценить число вкладчиков банка.

Задача 3.

Оценить вероятность того, что отклонение любой случайной величины от ее математического ожидания по абсолютной величине не превышает 3σ, где σ - среднее квадратическое отклонение.

Задача 4.

Измеряется длина деталей в партии, состоящей из 100 одинаковых ящиков. Для определения средней длины детали из каждого ящика взяли по одной. Оценить вероятность того, что средняя длина 100 отобранных деталей отличается от средней длины деталей во всей партии не более, чем на 5 (ед. длины) по абсолютной величине, если известно, что среднее квадратическое отклонение длины детали в каждом ящике менее 7 (ед. длины).

Задача 5.

Используя неравенство Чебышева, оценить вероятность того, что $|X - M(X)| < 0{,}1$, если $D(X) = 0{,}01$.

Задача 6.

Дано: $P(|X - M(X)| < \varepsilon) \ge 0{,}9;\ D(X) = 0{,}004$. Используя неравенство Чебышева, найти ε.

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

- Номер и тема лабораторной работы;
- Цель работы;
- Необходимые принадлежности; задание; методика работы;

- Ход выполнения лабораторной работы (этапы);
- Выводы по выполненной работе.

8. Контрольные вопросы.

- Что такое сходимость по вероятности.
- Для каких величин справедливо неравенство Маркова?
- Для каких величин справедливо неравенство Чебышева?
- Какие границы, рассматриваемого случайного события, устанавливает неравенство Чебышева?

Практическое занятие 12.

Решение задача по теории очередей. Задачи теории очередей.

Цель работы: получить практические навыки решения задач по теории очередей.

Продолжительность занятия: 2 часа.

Порядок выполнения работы:

1. Ознакомиться с заданием.
2. Определить номер варианта (в соответствии с номером в журнале).
3. Выполнить задания в соответствии с вариантом.
4. Ответьте на контрольные вопросы.

Методические указания

Очередь – это линия ожидания. Теория очередей – часть более широкой теории, в рамках которой проводятся оперативные исследования и создаются математические модели. Все это делается с одной целью – решить проблемы, которые создает стояние в очередях. Здесь важно найти компромиссный вариант, учитывающий систему расходов и среднее время ожидания в очереди. анализировать телефонную систему в Копенгагене, чтобы разрешить проблему загруженности телефонных линий.

Первопроходцем в теории очередей был датский математик **Агнер Краруп** (1878-1929), взявшийся анализировать телефонную систему в Копенгагене, чтобы разрешить проблему загруженности телефонных линий.

В теории изучения очередей существуют **законы Харпера**, подобные знаменитым законам Мерфи.

- Первый закон Харпера: неважно, в какую очередь ты становишься – всегда есть одна, движущаяся быстрее остальных.
- Второй закон Харпера: если ты переходишь в другую очередь, та, которую ты покинул, начинает двигаться быстрее.

Проблема очередей

Современный человек проводит в ожидании более или менее значительную часть своей жизни. Разве есть среди нас те, кто никогда не стоял в очереди? Мир ожидания очень разнообразен: очереди машин на въезде на платную дорогу, очереди самолетов на выезде на взлетную полосу и, как следствие, очереди пассажиров к стойкам регистрации; очередь к банкоматам в больших зданиях, очередь на прием к врачу или очередь телефонных звонков, которые должны быть обработаны на пожарной станции... Это лишь некоторые примеры. **Теория очередей** пытается создать модели, поддающиеся последующей математической обработке.

Модели очередей

Некоторые модели очередей очень просты, другие требуют применения сложных математических теорий. Первичная классификация разбивает их на две большие группы.

Детерминированная очередь – наиболее простая модель, которую можно заранее спрогнозировать, опираясь на известные условия, например, временные интервалы прибытия и ожидания. Это «очередь без сюрпризов».

Вероятностная очередь не может быть описана без применения вероятностей. Это более реалистичная модель, чем предыдущая. В дождливый день, например, есть большая вероятность того, что увеличатся очереди на стоянках такси и уменьшатся очереди в кассы зоопарка.

Условие задачи:

В мастерской работает 4 мастера. Клиенты приходят на обслуживание в среднем каждые 10 минут, время обслуживания 1 клиента составляет 30 минут. Определить вероятности первых 7-и состояний системы, вероятность отказа и среднюю длину очереди.

Построение математической модели СМО

Тип системы: СМО с ожиданием

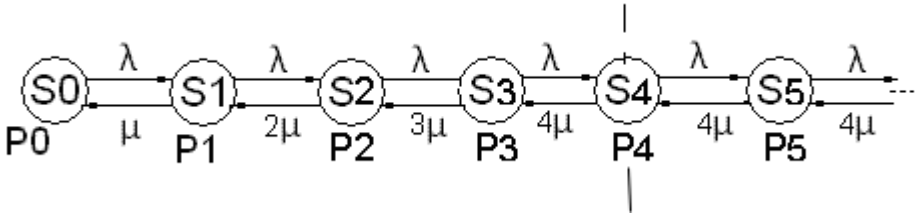
Количество каналов: n=4

Интенсивность поступления заявок: $\lambda = 1/10$

Интенсивность обслуживания: $\mu = 1/30$

Коэффициент загрузки каналов: $\alpha = \lambda/\mu = 3$

Размеченный граф состояний системы:



S0 – состояние, в котором в системе отсутствуют заявки;
S1 – состояние, при котором в системе 1 заявка;
S4 – состояние, при котором в системе 4 заявки, все каналы заняты;
S5 – состояние, при котором в системе 5 заявок, 1 заявка в очереди.

Решение задачи

$$P0 = 1/ \left(\sum_{k=0}^{n-1} \frac{\alpha^k}{k!} + \frac{\alpha^n}{n!(1-\alpha/n)}\right)$$

I. при k<=nPk=P0* $\alpha^k/k!$

II. при k>nPk=P0* $\alpha^k/(n!*n^{k-n})$

Ротк = Pn=P4

$$Lq = Pn * \frac{\alpha * n}{(n-\alpha)^2}$$

P0=0.0379 P1=0.1132 P2=0.1698 P3=0.1698 P4=0.1274

Содержание отчёта:

1. Название и цель работы.
2. Указать номер варианта, привести условия заданий своего варианта.
3. Представить результат выполнения заданий.
4. Ответы на контрольные вопросы.
5. Вывод о проделанной работе.

Задание:

Выполните задания согласно варианту.

Вариант 1

На станции работает несколько касс по продаже жетонов. Среднее время обслуживания составляет 1 минуту, а интенсивность потока заявок на обслуживание равна 3 (чел в минуту). Определить среднюю длину очереди для семи работающих касс и время пребывания в очереди.

Вариант 2

В мастерской работает 5 мастеров. Клиенты приходят на обслуживание в среднем каждые 20 минут, время обслуживания 1 клиента составляет 1,5 часа. Определить среднее число клиентов в системе и среднюю длину очереди.

Вариант 3

АТС имеет 6 линий связи. Поток заявок имеет интенсивность 1 вызов минуту, а время каждого разговора составляет в среднем 3 минуты. Определить вероятность отказа и вероятность того, что ни одна линия связи не будет занята.

Вариант 4

АТС имеет 5 линий связи. Поток заявок имеет интенсивность 2 вызова в минуту, а время каждого разговора составляет в среднем 3 минуты. Определить вероятность отказа и вероятность того, что ни одна линия связи не будет занята.

Вариант 5

На станции работает несколько касс по продаже жетонов. Среднее время обслуживания составляет 0.5 минуты, а интенсивность потока заявок на обслуживание равна 8 (чел. в минуту). Определить среднюю длину очереди для 5 работающих касс.

Вариант 6

В мастерской работает 8 мастеров. Клиенты приходят на обслуживание в среднем каждые 10 минут, время обслуживания 1 клиента составляет 1 час. Определить среднее число свободных мастеров и среднюю длину очереди.

Вариант 7

На станции работает несколько касс по продаже жетонов. Среднее время обслуживания составляет 2 минуту, а интенсивность потока заявок на обслуживание равна 2 (чел в минуту). Определить среднюю длину очереди для шести работающих касс и время пребывания в очереди.

Вариант 8

СМО имеет 6 обслуживающих каналов. Поток заявок, поступающих на обслуживание, имеет интенсивность 0,1 (заявок в мин.). Время обслуживания составляет в среднем 20 минут. Вычислить вероятности состояний системы среднее время пребывания заявки в очереди.

Вариант 9

СМО имеет 5 обслуживающих каналов. Время поступления заявок составляет 5 минут. Время обслуживания составляет в среднем 20 минут. Вычислить вероятности состояний системы среднее время пребывания заявки в очереди.

Вариант 10

Два мастера обслуживают 10 устройств, требующих постоянной регулировки. Среднее время, необходимое для регулировки 1-го устройства одним мастером составляет 2 часа, а интенсивность потока заявок на обслуживание устройств 0,2. Определить среднюю длину очереди и вероятность отказа.

Контрольные вопросы:

1. Сформулируйте определение детерминированной очереди?
2. Сформулируйте определение вероятностной очереди?
3. Что называют СМО?
4. Сформулируйте определение СМО?
5. Перечислите области применения теории очередей?

Практическое занятие 13

Решение задач по системе массового обслуживания. Распределение Пуассона. Гауссовское распределение

1. Цель занятия:

- Получить практические навыки, необходимые для решения задач теории распределения

2. *Продолжительность занятия:* 4 часа.

Краткие теоретические сведения:

Распределение Пуассона

Играет важную роль в ряде вопросов физики, теории связи, теории надежности, теории массового обслуживания и т.д. Всюду, где в течение определенного времени может происходить случайное число каких-то событий (радиоактивных распадов, телефонных вызовов, отказов оборудования, несчастный случаях и т.п.).

Рассмотрим наиболее типичную ситуацию, в которой возникает распределение Пуассона. Пусть некоторые события (покупки в магазине) могут происходить в случайные моменты времени. Определим число появлений таких событий в промежутке времени от 0 до T.

Случайное число событий, происшедших за время от 0 до T, распределено по закону Пуассона с параметром l=aT, где a>0 – параметр задачи, отражающий среднюю частоту событий. Вероятность k покупок в течение большого интервала времени, (например, – дня) составит

$P(Z=k) = \frac{\lambda^k}{k!} e^{-\lambda}$

Нормальное (гауссовское) распределение

Нормальное (гауссовское) распределение занимает центральное место в теории и практике вероятностно-статистических исследований. В качестве непрерывной аппроксимации к биномиальному распределению его впервые рассматривал А.Муавр в 1733 г. Через некоторое время нормальное распределение снова открыли и изучили К.Гаусс (1809 г.) и П.Лаплас, которые пришли к нормальной функции в связи с работой по теории ошибок наблюдений.

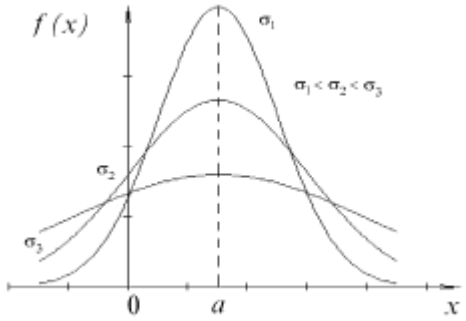
Непрерывная случайная величина *X* называется *распределенной по нормальному закону*, если ее плотность распределения равна

$$f(x) = \frac{1}{\sqrt{2\pi}\,\sigma} \exp -\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2,$$

$$-\infty < x < \infty, \quad \sigma > 0, \quad -\infty < \mu < \infty.$$

где μ совпадает с математическим ожиданием величины X: μ =M(X), параметр s совпадает со средним квадратическим отклонением величины X: s =s(X). График функции нормального распределения, как видно из рисунка, имеет вид куполообразной кривой, называемой Гауссовой, точка максимума

имеет координаты (a; $\frac{1}{\sigma\sqrt{2\pi}}$). Значит, эта ордината убывает с возрастанием значения s (кривая «сжимается» к оси Ox) и возрастает с убыванием значения s (кривая «растягивается» в положительном направлении оси Oy). Изменение значений параметра μ (при неизменном значении s) не влияет на форму



кривой, а лишь перемещает кривую вдоль оси Ox.

Нормальное распределение с параметрами μ =0 и s=1 называется нормированным. Функция распределения СВ в этом случае будет иметь вид:

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$$

5. Задание

Решить задачи теории распределения применяя Гауссовское распределение и распределение Пуассона.

6. Ход выполнения работы.

Задача 1.

Микропроцессор имеет 10000 ранзисторов, работающих независимо друг от друга. Вероятность того, что транзистор выйдет из строя во время работы прибора, является величиной маловероятной и составляет 0,0007. Определить математическое ожидание M (X) и среднее квадратическое отклонение S (X) случайной величины X — числа транзисторов, выйдут из строя во время работы процессора.

Задача 2.

В рыбацком городке 99,99% мужчин хотя бы раз в жизни были на рыбалке. Проводят социологические исследования среди 10000 наугад выбранных мужчин. Определить дисперсию D (X) и среднее квадратическое отклонени S (X) случайной величины X — числа мужчин, которые ни разу не были на рыбалке.

Задача 3.

Среднее число бракованных деталей, изготавливаемых станком-автоматом в течение одного часа, равно 6. Составить закон распределения дискретной случайной величины X – числа бракованных деталей, которые будут

изготовлены станком-автоматом в ближайшие полчаса. Найти числовые характеристики $M(X);\ D(X);\ \sigma(X);\ V(X)\%$ этой случайной величины.

Задача 4.

Два равносильных игрока играют в игру, ничьи в которой исключаются. Составить закон распределения случайной величины X – числа партий, которые выиграет первый игрок, если будут играться 4 партии. Найти числовые характеристики этой случайной величины.

Задача 5.

В магазин привезли 300 стеклянных бутылок с минеральной водой. Известно, что в среднем при перевозке одна из 500 бутылок разбивается. Составить закон распределения случайной величины X – числа разбитых бутылок в привезенной партии. Найти числовые характеристики этой случайной величины.

Задача 6.

Случайная величина X распределена по закону Пуассона. Найти математическое ожидание, дисперсию и $P(X=3)$, если $a=4$.

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

1) Номер и тема практической работы;
2) Цель работы;
3) Необходимые принадлежности; задание; методика работы;
4) Ход выполнения практической работы (этапы);
5) Выводы по выполненной работе.

8. Контрольные вопросы

- При анализе каких результатов используется Пуассоновское распределение?
- Чем по сути являются математическое ожидание и дисперсия?
- Самое простое распределение случайной величины.

Практическое занятие 14

Решение задач по системе массового обслуживания. Системы массового обслуживания

1. Цель занятия:
   - Получить практические навыки, необходимые для решения задач систем массового обслуживания.
   - Приобретение навыков построения математической модели и определения характеристик системы массового обслуживания.
2. Продолжительность занятия: 4 часа

Краткие теоретические сведения:

Основы знаний об очередях, иногда называемые теорией очередей или теорией массового обслуживания, составляют важную часть теории управления производством. Очереди — обычное явление. Они могут носить форму ожидания ремонта автомобиля в центре автосервиса или ожидания студентами консультации у профессора. В таблице перечислены некоторые примеры возникновения очередей в системах массового обслуживания:

Ситуация	Ожидающие в очереди	Процесс обслуживания
Супермаркет	Покупатели	Прием кассиром оплаты за покупки
Приемная врача	Пациенты	Прием доктором и мед-сестрой
Компьютер	Компьютерные про-граммы	Выполнение программ процессором
Телефонная компания	Абоненты	Выполнение заказов на междугородние переговоры

Каждая СМО состоит из определенного числа обслуживающих единиц (приборов, устройств, пунктов, станций), которые будем называть ***каналами обслуживания***. Каналами могут быть линии связи, рабочие точки, вычислительные машины, продавцы и др. По числу каналов СМО подразделяют на ***одноканальные*** и ***многоканальные***.

Заявки поступают в СМО обычно не регулярно, а случайно, образуя так называемый ***случайный поток заявок (требований)***. Обслуживание заявок, вообще говоря, также продолжается какое-то случайное время. Случайный характер потока заявок и времени обслуживания приводит к тому, что СМО оказывается загруженной неравномерно: в какие-то периоды времени скапливается очень большое количество заявок (они либо становятся в очередь, либо покидают СМО необслуженными), в другие же периоды СМО работает с недогрузкой или простаивает.

Предметом теории массового обслуживания является построение математических моделей, связывающих заданные условия работы СМО (число каналов, их производительность, характер потока заявок и т.п.) с показателями эффективности СМО, описывающими ее способность справляться с потоком заявок.

В качестве ***показателей эффективности СМО*** используются: среднее число заявок, обслуживаемых в единицу времени; среднее число заявок в очереди; среднее время ожидания обслуживания; вероятность отказа в обслуживании без ожидания; вероятность того, что число заявок в очереди превысит определенное значение и т.п.

СМО делят на два основных типа (класса): ***СМО с отказами*** и ***СМО с ожиданием (очередью)***. В СМО с отказами заявка, поступившая в момент, когда все каналы заняты, получает отказ, покидает СМО и в дальнейшем процессе обслуживания не участвует (например, заявка на телефонный разговор в момент, когда все каналы заняты, получает отказ и покидает СМО необслуженной). В СМО с ожиданием заявка, пришедшая в момент, когда все каналы заняты, не уходит, а становится в очередь на обслуживание.

СМО с ожиданием подразделяются на разные виды в зависимости от того, как организована очередь: с ограниченной или неограниченной.

5. Задание.

Решить задачи используя математический аппарат построения СМО.

6. Ход выполнения работы.

Задача 1.

На диспетчерский пульт поступает поток заявок, который является потоком Эрланга второго порядка. Интенсивность потока заявок равна 6 заявок в час. Если диспетчер в случайный момент оставляет пульт, то при первой же очередной заявке он обязан вернуться к пульту. Найти плотность распределения времени ожидания очередной заявки и построить ее график. Вычислить вероятность того, что диспетчер сможет отсутствовать от 10 до 20 минут.

Задача 2.

Дисплейный зал имеет 5 дисплеев. Поток пользователей простейший. Среднее число пользователей, посещающих дисплейный зал за сутки, равно 140. Время обработки информации одним пользователем на одном дисплее распределено по показательному закону и составляет в среднем 40 минут. Определить, существует ли стационарный режим работы зала; вероятность того, что пользователь застанет все дисплеи занятыми; среднее число пользователей в дисплейном зале; среднее число пользователей в очереди; среднее время ожидания свободного дисплея; среднее время пребывания пользователя в дисплейном зале.

Задача 3.

В двухканальную систему массового обслуживания (СМО) с отказами поступает стационарный пуассоновский поток заявок. Время между поступлениями двух последовательных заявок распределено по показательному закону с параметром $\lambda=5$ заявок в минуту. Длительность обслуживания каждой заявки равна 0,5 мин. Методом Монте-Карло найти среднее число обслуженных заявок за время 4 мин. Указание: провести три испытания.

Задача 4.

Интенсивность потока телефонных звонков в агентство по заказу железнодорожных билетов, имеющему один телефон, составляет 16 вызовов в час. Продолжительность оформления заказа на билет равна 2.4 минуты. Определить относительную и абсолютную пропускную способность этой СМО и вероятность отказа (занятости телефона). Сколько телефонов должно быть в агентстве, чтобы относительная пропускная способность была не менее 0,75.

Задача 5.

Система массового обслуживания — билетная касса с одним окошком и неограниченной очередью. Касса продает билеты в пункты А и В. Пассажиров, желающих купить билет в пункт А, приходит в среднем трое за 20 мин, в пункт В — двое за 20 мин. Поток пассажиров простейший. Кассир в среднем обслуживает трех пассажиров за 10 мин. Время обслуживания — показательное. Вычислить финальные вероятности P0, P2, P3, среднее число заявок в системе и в очереди, среднее время пребывания заявки в системе, среднее время пребывания заявки в очереди.

Оформите отчет, сделайте выводы по работе.

7. Содержание отчета

Номер и тема лабораторной работы;
Цель работы;
Необходимые принадлежности; задание; методика работы;
Ход выполнения лабораторной работы (этапы);
Выводы по выполненной работе.

8. Контрольные вопросы

1. Как иначе называют поток?
2. Как называют поток, состоящий из требований на обслуживание?
3. Поток требований, который уже обслуженных
4. Что называют системой обслуживания?

Практические работы МДК.01.01.

Практическая работа № 1.

Тема: Исследование топологии локальной сети.

Цели работы: научиться выбирать топологию сети по поставленной задаче, графически изображать выбранную топологию сети.

Оборудование: ПК с подключением к сети Internet.

Теоретическая часть

При выборе топологии сети вам необходимо найти компромисс между стоимостью сетевого оборудования и его производительностью, учесть возможный рост сети, необходимость подключения к сети дополнительных компьютеров и рабочих станций.

Для этого необходимо, прежде всего, оценить количество компьютеров в сети и разбить их на группы (сегменты). Рассчитать количество коммутационного оборудования.

Ход работы

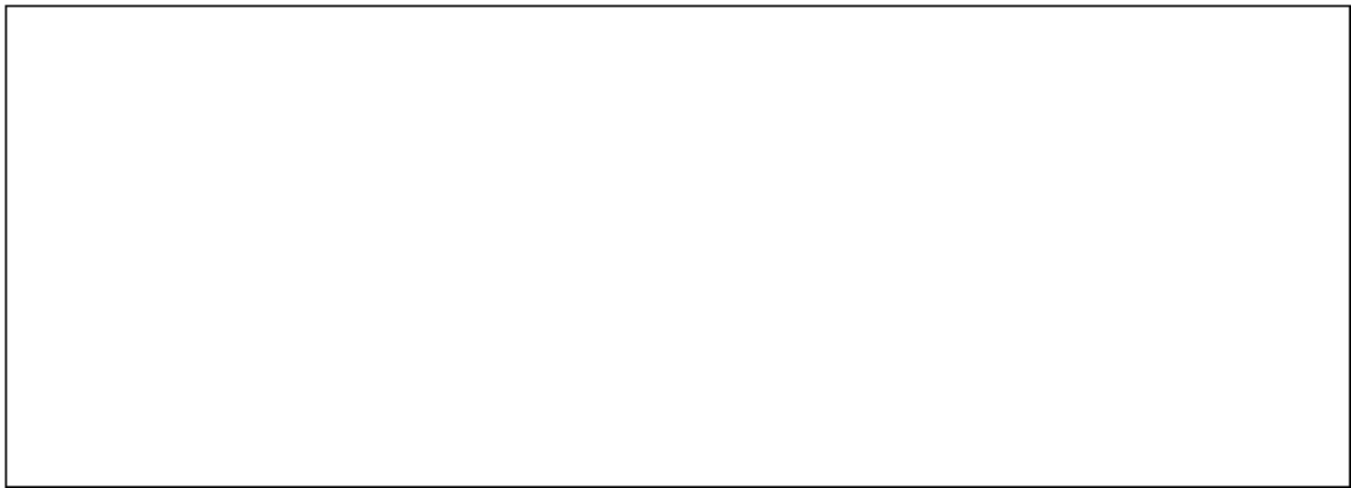
ЗАДАЧА

1. Количество компьютеров в сети: _____ (№ по списку в журнале + 16).
2. Количество сегментов в сети: _____(дает преподаватель).
3. Максимальное количество портов на коммутаторе ____(№ по списку в журнале х 2 + 10).
4. Наличие коммутаторов в сети (да / нет) (дает преподаватель).
5. Необходимость расширения (да / нет) (дает преподаватель).

1. **Обоснуйте выбор топологии по поставленной задаче.**

Топология _____.
_____
_____
_____
_____
_____
_____.

2. **Графически изобразите топологию по поставленной задаче.**



Практическая работа 2,3.
Выполнение работ с коаксиальным кабелем и витой парой.

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.

Цели

Выполняя эту лабораторную работу, вы научитесь:

работать с «тонким» коаксиальным кабелем и кабелем «витая пара» категории 5 (или более высокой);

устанавливать на концах кабелей (*заделывать*) коннекторы BNC и RJ-45;

проверять качество заделки коннекторов;

использовать прямые и перекрестные кабели на основе «витой пары» для связи компьютеров, концентраторов и коммутаторов.

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

Цель работы

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

Изучение тонкого коаксиального кабеля

1. Возьмите отрезок коаксиального кабеля и исследуйте его строение.

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

---

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

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

Монтаж BNC-коннектора на коаксиальном кабеле

Возьмите отрезок коаксиального кабеля длиной 2–3 метра.

Отрежьте на конце кабеля небольшой кусок в 2–3 см, чтобы удалить поврежденную или окислившуюся часть кабеля.

Наденьте на кабель трубочку, используемую для обжима экранирующей оплетки, и сдвиньте ее немного вниз, чтобы она не мешала дальнейшей работе.

Возьмите *устройство для зачистки кабеля RG-58*, заложите конец кабеля в подпружиненную часть (как показано на рис. 4.1) и проверните инструмент один-два раза вокруг кабеля, следя за тем, чтобы устройство все время оставалось перпендикулярным кабелю.

Рис. 4.1. 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.

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.

Аккуратно удалите надрезанные части — после этого конец кабеля должен выглядеть, как показано на рис. 4.2.

Рис. 4.2. Коаксиальный кабель RG-58 после зачистки

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.

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. 4.3.

Рис. 4.3. 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.

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

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).

Равномерно обмотайте экранирующую оплетку вокруг хвостовой части корпуса коннектора, как показано на рис. 4.4, и наденьте трубочку на обмотанный оплеткой хвостовик.

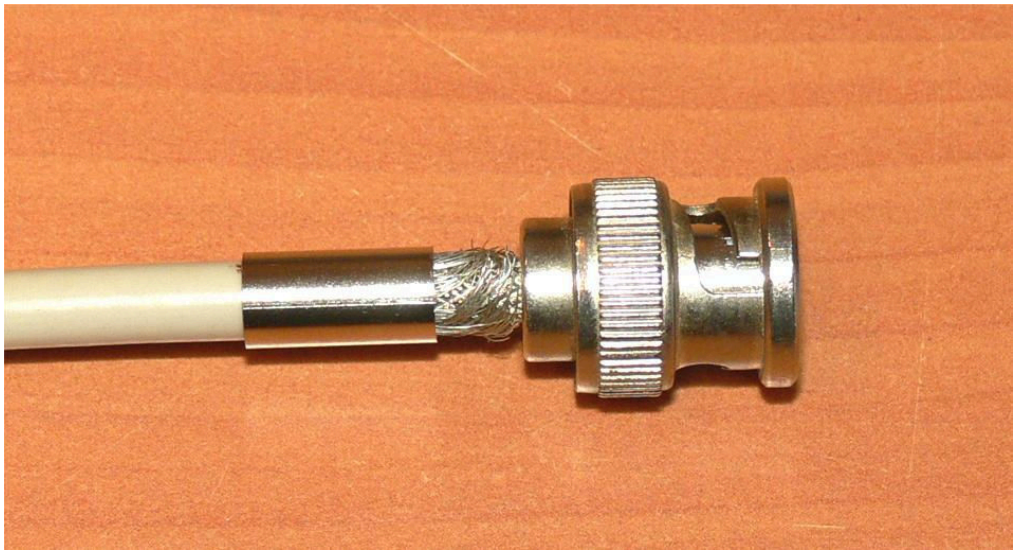


Рис. 4.4. Коаксиальный кабель с установленной основной частью коннектора и не полностью надетой обжимной трубочкой

Наконец, следует поместить хвостовую часть коннектора в обжимное устройство (рис. 4.5) и одним движением обжать ее.

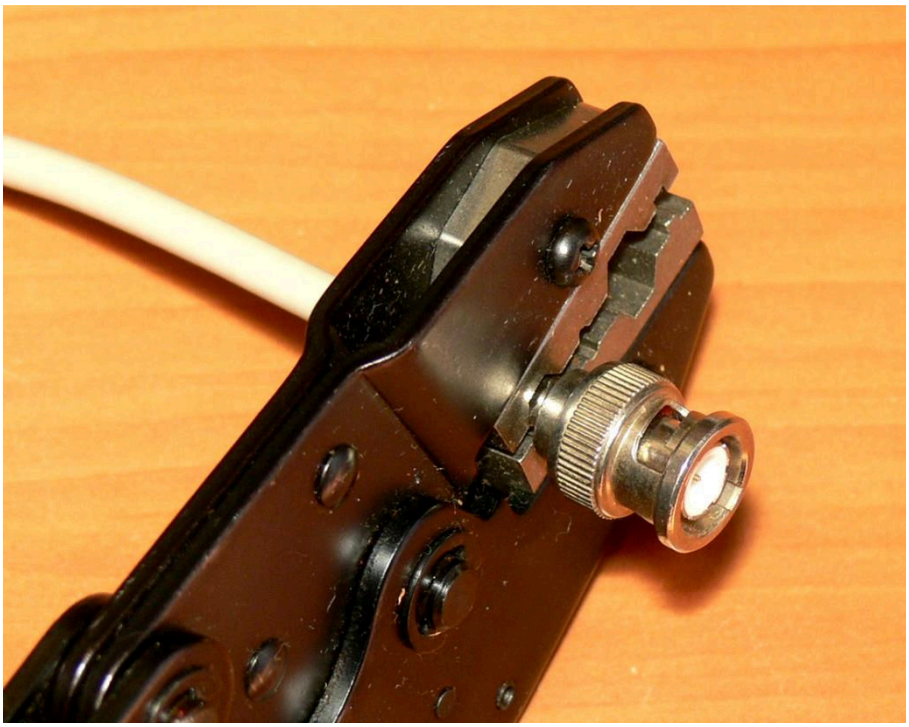


Рис. 4.5. Коннектор BNC в обжимном инструменте

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?

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»

2. Возьмите отрезок кабеля «витая пара» длиной 2–3 метра.

Отрежьте на конце кабеля небольшой кусок в 2–3 см, чтобы удалить поврежденную или окислившуюся часть кабеля.

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. 4.6, слегка сожмите ручки и вращающим движением надрежьте внешнюю оплетку кабеля (аккуратно, чтобы не разрезать проводники).

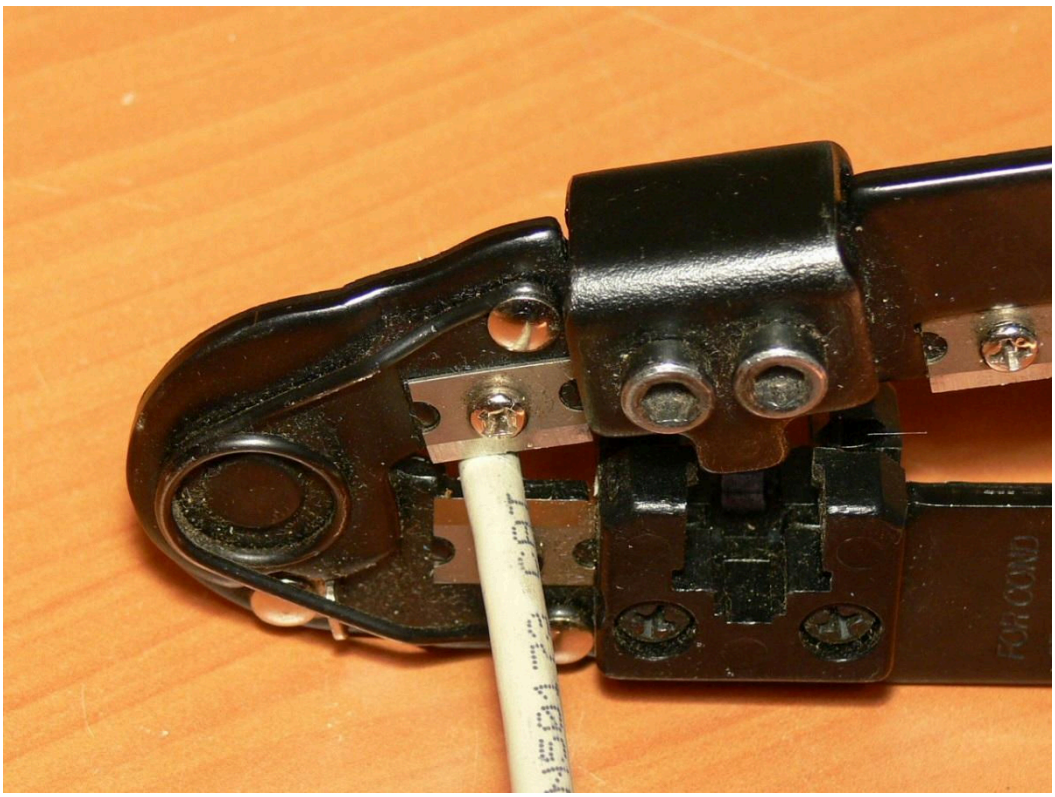


Рис. 4.6. Обрезка внешней изоляции на кабеле «витая пара»

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.

Удалите надрезанный кусок внешней оплетки кабеля, расплетите и выпрямите все проводники. После этого конец кабеля должен выглядеть, как показано на рис. 4.7.

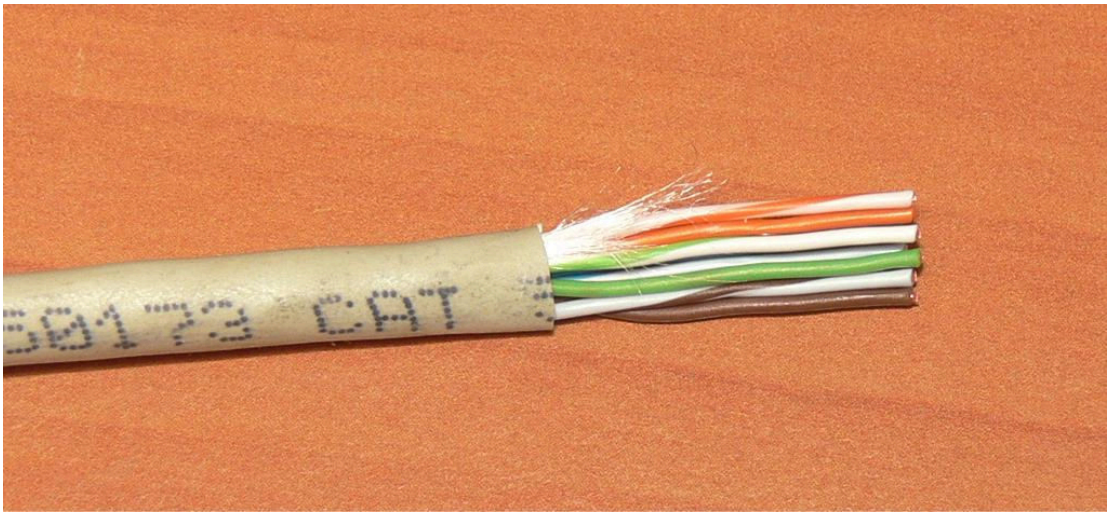


Рис. 4.7. Кабель «витая пара» с расплетенными и выпрямленными проводниками

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. 4.8).

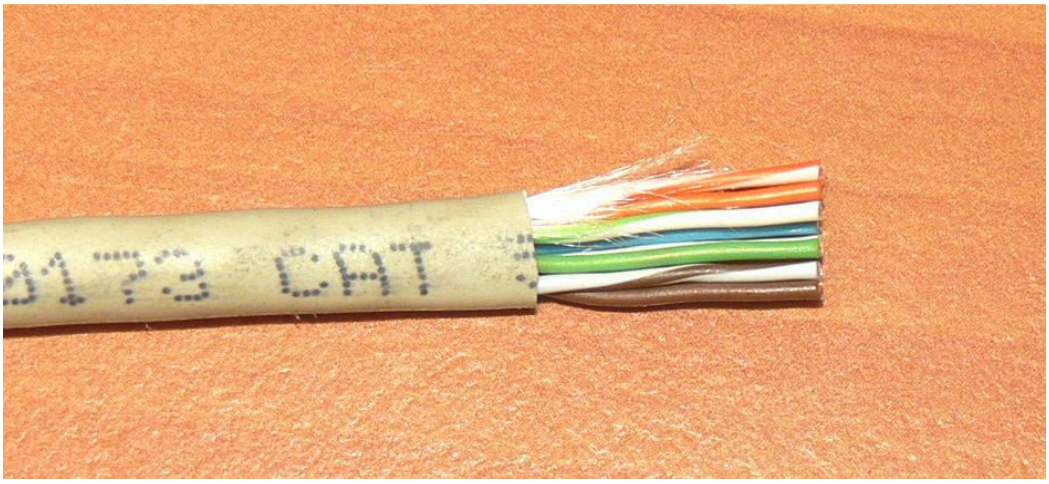


Рис. 4.8. Кабель «витая пара» с подготовленными к монтажу в коннектор проводниками

Вставьте проводники в коннектор, следя за тем, чтобы расположение проводников не нарушилось, затем поместите коннектор в обжимное устройство до фиксации защелкой (рис. 4.9) и обожмите разъем.

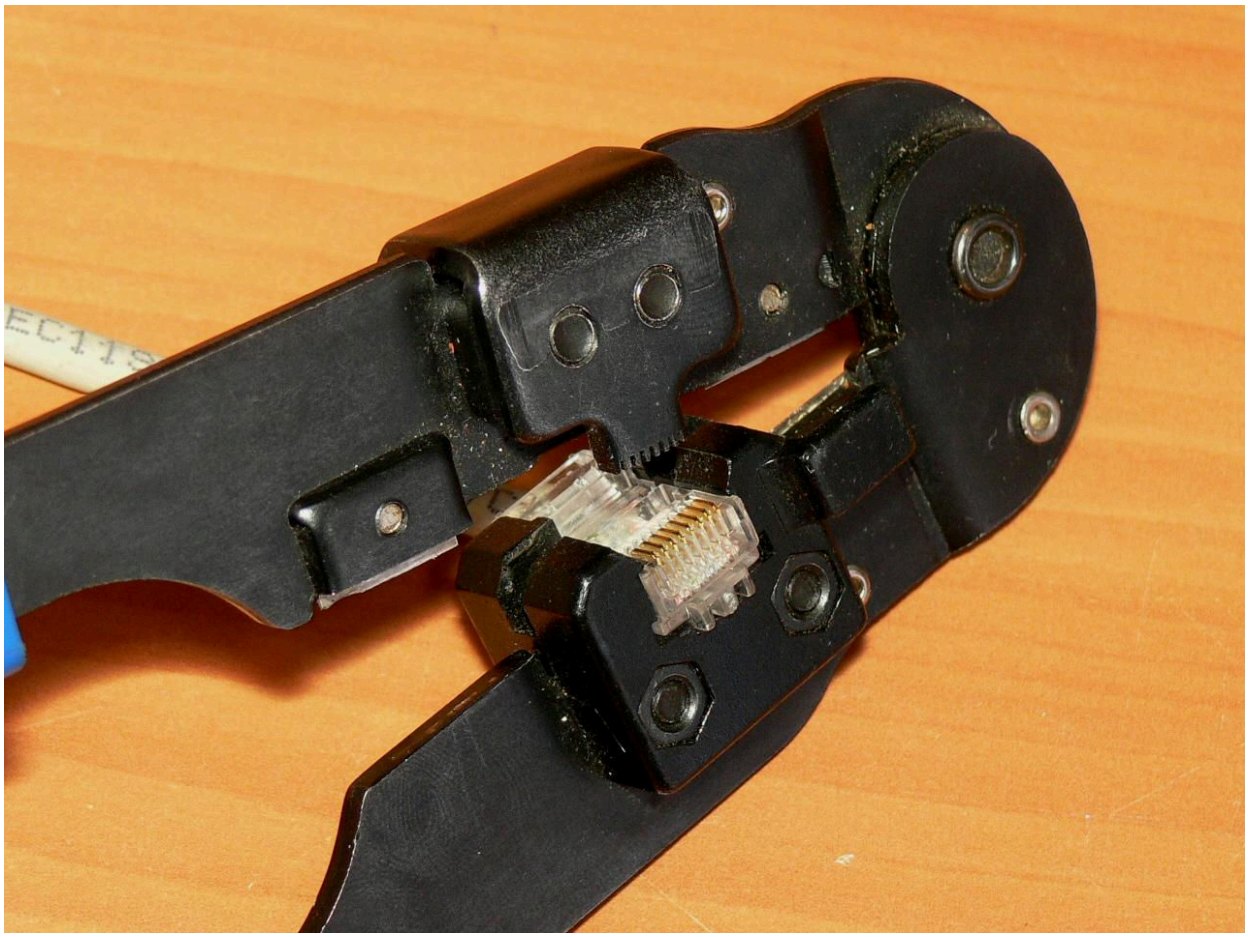


Рис. 4.9. Коннектор RJ-45 в обжимном инструменте

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

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

Какие устройства соединяются с помощью прямого кабеля?

---

4. Возьмите прибор для проверки кабелей.

5. Используя разъемы для коннекторов RJ-45, соедините обе части прибора: основную («MASTER») и удаленную («REMOTE») с помощью только что изготовленного кабеля (рис. 4.10), после чего нажмите кнопку включения питания на основной («MASTER») части прибора. Обратите внимание на мигающие светодиодные индикаторы.

Рис. 4.10. Проверка качества заделки коннекторов RJ-45 с помощью специального тестера

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

---

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

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

Изготовление перекрестного кабеля на базе «витой пары»

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

Какие устройства можно соединять с помощью перекрестного кабеля?

Задание 2.
Использование кабелей на базе «витой пары»

Цель работы

В этом задании вы должны проверить возможность соединения компьютеров, концентраторов и коммутаторов с помощью прямых и перекрестных кабелей на основе «витой пары».

Предварительные условия

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 `\\Compx`, где `Compx` — 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 `\\Compx`, где `Compx` — 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 автоопределения 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 `\\Compx`, где `Compx` — 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.

ПРАКТИЧЕСКАЯ РАБОТА №4

Тема работы: Выполнение работ с оптиковолоконным кабелем.

Цель работы: Научиться выполнять работы с оптиковолоконным кабелем.

Теоретическая часть

Разделка волоконно-оптического кабеля

Волоконно-оптический кабель представляет собой несколько оптических волокон, которые вместе с армирующими нитями заключены в защитную полимерную оболочку. Для защиты от агрессивных внешних воздействий кабель помещают в броневую защиту из гофрированной алюминиевой или стальной защитной ленты либо из стальной проволоки. Из-за того, что оптическое волокно в достаточной степени чувствительно к осевым и радиальным деформациям, для его разреза непригодны недорогие кабелерезы, которые используются для работы с медными кабелями. Рекомендуется использовать инструмент, лезвия которого рассчитаны на резку стали.

Начальный этап разделки волоконно-оптических кабелей – удаление верхнего слоя защитных и броневых покровов, выполняется теми же инструментами, что и разделка обычных кабелей. Полимерная изоляция и фольга вскрываются резаками, а стальная проволока выкусывается бокорезами. Рекомендуется применять кабельные ножи: они позволяют снимать полимерное покрытия с кабеля диаметром от 4 до 35 мм, и при этом кабельный нож имеет специальную насадку, ограничивающую глубину разреза оболочки, что исключает повреждение оптоволоконных жил.

Но в дальнейшей работе без специальных инструментов все равно не обойтись:
* ножницы или кусачки с керамическими лезвиями используются для удаления армирующих нитей из кевлара. Обычные ножницы эти тонкие, гибкие и прочные волокна не режут, а выдавливают или гнут;
* стрипперы предназначены для снятия буферного слоя. Их применение снижает риск повреждения оптического волокна: в первую очередь, из-за того, что его рабочие поверхности имеют фиксированную настройку;
* скалыватель оптических волокон применяется для отсекания лишнего отрезка волокна под углом 90 град. Скалыватели бывают ручные и автоматические. При подготовке оптоволокна для последующей сварки или соединения волокон при помощи сплайса рекомендуется использовать автоматические скалыватели, которые позволяют получить чистый и ровный скол без дефектов под углом 90±0,5 град. Например, скол с углом более 2 град. может привести к увеличению потерь в соединении до 1 дБ, что при оптическом общем бюджете системы в 15–25 дБ – зачастую непозволительная роскошь;
* микроскопы позволяют диагностировать разъемы оптических волокон на качество полировки жилы, наличие трещин, царапин;
* кримперы предназначены для обжимки наконечников, разъемов и контактов.

Соединение волоконно-оптического кабеля

Широко применяется три способа монтажа оптоволокна:
* сварка оптических волокон;
* соединение при помощи механических разъемов;
* соединение при помощи сплайса.

Сварка оптических волокон

Сварка оптоволокна осуществляется с помощью специальных сварочных аппаратов и обычно выполняется в три этапа:

* подготовка и зачистка кабеля, получение качественного торца;
* сваривание сварочным аппаратом;
* тестирование и оценка качества соединения.

Сварочный аппарат осуществляет соединение оптоволокна с хорошими параметрами места соединения просто и быстро. Современные сварочные аппараты позволяют снизить потери в месте соединения до 0,04 дБ и менее. Аппарат автоматически выполняет все необходимые операции: юстирует оптоволокна, расплавляет концы оптоволокон, сваривает их. Наиболее функциональные (но и, к сожалению, более дорогие) модели так же проверяют качество соединения. После чего место сварки защищают, обычно при помощи термоусаживающей трубки.

Соединение при помощи механических разъемов
Сварка оптического волокна также используется при оконцовке волокна коннекторами. Для этих целей используются готовые волоконно-оптические перемычки – пигтейлы (англ. Pigtail – гибкий проводник). Пигтейл обычно изготавливается в заводских условиях, он представляет собой отрезок оптоволоконного кабеля, которое имеет с одной стороны оптический коннектор. Волокно оптического кабеля сваривается с волокном пигтейла, а уже при помощи коннектора его подключают к оборудованию.

Соединение при помощи сплайса
Сплайс – устройство для сращивания волоконно-оптического кабеля без применения сварки. В сплайс через специальные направляющие навстречу друг другу вводятся подготовленные концы оптических волокон и фиксируются в нем. Для уменьшения вносимых потерь стык между волокнами помещают в специальный (иммерсионный) гель, который зачастую находится внутри сплайса.

Технология соединения при помощи сплайса включает в себя несколько этапов:
* разделка волоконно-оптического кабеля;
* обработка торцов;
* выполнение соединения;
* тестирование и оценка качества соединения;
* нанесение защитных покрытий, восстановление защитной оболочки и брони.

Применение сплайсов облегчает процесс сращивания оптоволокна, но работа с ними требует практических навыков. Вносимые потери при этом методе соединения волокон меньше, чем при использовании пары волоконно-оптических вилок и адаптера, но все же могут составлять 0,1 дБ и выше. Согласно требованиям стандартов на СКС IS0 11801, TIA EIA 568B вносимые потери в сплайсе не должны превышать 0,3 дБ. Для этого в ходе монтажа проводится корректировка положения волокон относительно друг друга, в процессе работ также необходимо проводить постоянный замер потерь на месте соединения.

Кроме того, следует принимать во внимание тот факт, что со временем потери в месте соединения при помощи сплайса могут увеличиться из-за смещения волокон в пространстве или высыхания иммерсионного геля.

ПРАКТИЧЕСКАЯ РАБОТА №5

Тема работы: Исследование типов интерфейсов данных.

Цель работы: Научиться определять типы данных.

Теоретическая часть

1. Разновидности интерфейсов

Интерфейсы отличаются по способу доступа к командным файлам программ.

Командный (текстовый) интерфейс. Всякая операционная система имеет командный интерфейс (иногда в скрытой форме).

Если снять шелуху текстовых или графических оболочек или интерфейсов, то «на глубине» вы всегда найдете командный интерфейс.

В первой из ОС (OS/360) взаимодействие с пользователями было жестко поделено между следующими компонентами:

Ш Командный язык оператора ЭВМ (лицо, ответственное за управление вычислительным прочесом). Это язык диалогового режима - команда запуска - остановки задач, привязки носителей информации к устройствам, получения информации о заданиях, ожидающих выполнения, вывода, наличия свободной памяти и свободных устройств и др.

Ш Язык управления заданиями (JCL - Job Control Language), на котором прочие пользователи (программисты, разработчики и просто конечные пользователи) описывали состав и структуру процесса обработки данных - последовательность запуска программ, входные и выходные файлы, условия, при которых те или иные программы должны быть выполнены или пропущены и др. Это язык пакетной обработки, не допускающий вмешательства пользователя в собственно процесс вычисления, компиляции и пр.

По мере развития ЭВМ, ОС, появления и широкого распространения диалоговых устройств (видеотерминалов) в последующих ОС произошла интеграция данных компонентов в единый командный язык. Для разграничения между командами оператора, администратора, конечно пользователя используются методы разделения доступа и назначения привилегии, в то время как формат команд является достаточно единообразным.

Далее, после распространения ПЭВМ данное разграничение сошло на нет (в ОС MS-DOS), поскольку пользователь ПК в едином лице соединяет функции оператора, администратора, конечно пользователя. Затем с появлением локальных сетей и более мощных ПК, работающих в многопользовательских режимах, в сетевых ОС и ОС ПЭВМ, вновь организуется разграничение доступа и т.д. Таким образом данный процесс является циклическим (точнее, спиралевидным).

В большинстве ОС в настоящее время сложился более или менее унифицированный формат командной строки. Командная строка включает в себя:

· Тип операции (мя команды или программы);

· Рабочий вход (входные файлы или устройства);

· Рабочий выход (выходные файлы или устройства)

· Управляющий вход (управляющие параметры или ключи команды);

· Управляющий выход (обычно - протокол, содержащий диагностику ошибок, код завершения или другую информацию)

Рис 1. Типовая структура командной строки языков ОС

Текстовый или графический полноэкранный интерфейс. Он имеет, как правило, в верхней части экрана систему меню с подсказками. Меню часто бывает выпадающим (ниспадающим - pull-down).

Для управления компьютером курсор экрана или курсор мыши после поиска в древе каталогов устанавливается на командные файлы программ (*.exe, *.com, *.bat) и для запуска программы нажимается клавиша <Enter> или правая кнопка мыши. Различные файлы могут выделяться разным цветом или иметь разный рисунок. Каталоги (папки) отличаются от файлов размером или рисунком. Данный интерфейс является основным для всех видов программных оболочек.

Графический многооконный пиктографический интерфейс. Представляет собой рабочий стол (DeskTop), на котором располагаются пиктограммы (значки или иконки программ). Все операции производятся, как правило, мышью. Для управления компьютером курсор мыши подводят к пиктограмме и запуск программы осуществляют щелчком левой кнопки мыши по пиктограмме. Это наиболее удобный и перспективный интерфейс, осебенно при работе с программами. Примеры: интерфейс с компьютеров Apple Macintosh? Windows 3.1, Windows 95/98, OS/2, X Windows.

2. Графический интерфейс пользователя

Графический интерфейс пользователя (GUI - Graphics User Interface). Появление ОС и оболочек с развитыми диалоговыми графическими средствами (OS Macintosh, Windows 3.1, а особенно Windows 95/98/ME, а также NT/2000) и средств программирования, позволяющих создавать графические интерфейсы (FoxPro for Windows и пр.), а особенно - объектно-ориентированных систем программирования - привело к внедрению и широкому распространению элементов экранного интерфейса.

Графические интерфейсы иногда обозначают следующей аббревиатурой - WIMPD (Windows, Menu, Pointing Device) - окна, меню, указывающие устройство, как основные действующие элементы в подобном интерфейсе.

Оболочка Microsoft Windows не была изначально Операционной системой, так как она существует «поверх» операционной системы типа MS-DOS. Она возникла в виде стандартизатора графического интерфейса и прижилась исключительно потому, что пользователь хотел видеть программу, с которой ему часто приходится работать, красивой, практичной, удобной и легкой в освоении и использовании.

Для ОС UNIX также был создан специальный графический интерфейс - X Windows; фирма IBM выпустила вместе с операционной системой OS/2 свой вариант графического интерфейса пользователя - Presentation Manager.

Функции, используемые программой пользователя при работе с графическим пользовательскиминтерфейсом, схожи, как и сами интерфейсы.

Рис 2. Рабочий стол Windows XP, пиктограммы, окна приложений.

Графический интерфейс включает следующие понятия - рабочий стол, окна, пиктограммы, элементы графического интерфейса (виджеты), указывающие устройства (мышь).

3. Основные элементы графических интерфейсов (виджеты, widgets)

Виджет - это заготовка части пользовательского интерфейса (кнопка, часть меню, пиктограмма и т.д.) с параметрами, привязываемая к окну экрана терминала. Наиболее распространенные: кнопка (Button); радиокнопка (Radio Button); флажок (Check Box); список (List); полосы прокрутки и т.д.

Управляющие кнопки (Button) - предназначены для выполнения действий. Какое именно действие выполняет кнопка, написано непосредственно на ней. Если в конце названия кнопки присуствует три точки, то такая кнопка вызовет новое диалоговое окно.

Поле ввода - область, где пользователь может вводить информацию с клавиатуры. В этой области указатель мыши принимает новую форму. Если в этот момент щелкнуть кнопкой мыши, то в поле появится курсор и можно вводить данные.

Список - элемент, содержащий все возможные в каждом конкретном случае значения, которые пользователь может установить. Добавить или изменить эти значения непосредственно в списке нельзя.

Раскрывающийся список (List) - при нажатии на пиктограмму со стрелкой открывается список всех возможных значений, которые можно выбрать для установки в этом элементе. Если список длинный, то появится линейка прокрутки, с помощью которой можно посмотреть все элементы списка.

Поле ввода с раскрывающимся списком - это комбинация элементов поле вывода и раскрывающегося списка. Такой элемент позволяет как непосредственно вводить данные в поле ввода, так и заполнять его значением из раскрывающегося списка. Аналогично работает поле вода со списком. Отличие только в том, что список виден постоянно, а не открывается. Поле ввода со счетчиком - обычно используется для ввода числовых значений. Его можно заполнить как обычное поле ввода или воспользоваться кнопочками, расположенными справа. В этом случае значение в поле будет изменятся (соответственно увеличиваться и уменьшатся) с наиболее оптимальным шагом и при этом не превысит предельный значений. Поэтому рекомендуется пользоваться именно счетчиком.

Флажок - переключатель для режима работы, описание которого находится справа от квадрата. Он может быть включен (установлен) - внутри квадрата изображен значок, или выключен (сброшен) - внутри пусто. Для установки или сброса флажка необходимо щелкнуть мышью в квадрате или на его описание. Такой элемент вполне самостоятельно определяет свой параметр. И поэтому называется независимым.

Литература

· И.И. Попов «Операционные системы, среды и оболочки»

· Интернет энциклопедия mail.ru

- Создание базового класса "Строка", строки идентификатора и десятичной строки. Создание графического интерфейса

  Разработка графического интерфейса для ввода начальных значений, отображения результатов и тестирования методов собственного класса на языке программирования C++. Подсветка цветом выбранных операндов в процессе их инициализации и вывода на дисплей.

  курсовая работа [234,6 K], добавлен 27.12.2014

- Разработка системы контроля доступа к файлам

  Анализ методов и средств контроля доступа к файлам. Проблемы безопасности работы с файлами, средства контроля доступа ним. Идеология построения интерфейса, требования к архитектуре. Работа классов системы. Оценка себестоимости программного продукта.

  дипломная работа [2,5 M], добавлен 21.12.2012

- Переназначение выхода и входа программ, программные каналы

  Особенности загрузки операционной системы Linux в режиме терминала, входа в систему и регистрации пользователей. Выполнение переназначения файлов, его использование для работы с командами операционной системы. Применение программных каналов (конвейеров).

  лабораторная работа [21,5 K], добавлен 12.05.2013

- Командная строка MS-DOS

  Понятие и использование командной строки. Открытие командной строки. Команды, выполняемые с помощью командной строки. Как выполнить команду с повышенными привилегиями. Изменение внешнего вида окна командной строки с помощью параметров командной строки.

  презентация [948,2 K], добавлен 22.10.2014

- Разработка и реализация графического интерфейса для СПП СБкЗ_ПП с использованием системы автоматической генерации интерфейсов OntoDev

  Анализ графических пользовательских интерфейсов современных систем оптимизации программ. Создание математической модели и алгоритма системы управления СБкЗ_ПП, ее архитектурно-контекстная диаграмма. Техническая документация программного средства.

ПРАКТИЧЕСКАЯ РАБОТА №6

Тема работы: Изучение IP-протокола.

Цель работы: Научиться проверять работоспособность сетевого подключения.

Теоретическая часть: Существуют различные утилиты, позволяющие быстро продиагностировать IP-подключение. Однако большинство операций легко может быть выполнено с использованием команд самой операционной системы.

Пользователи Windows XP для диагностики сетевого подключения могут воспользоваться специальным мастером. Эта программа вызывается из меню задачи *Сведения о системе* (*Пуск > Все программы > Стандартные > Служебные > Сведения о системе > меню Сервис > Диагностика сети*):

В ходе выполнения лабораторной работы Вы познакомитесь с утилитами, запускаемыми из командной строки, позволяющими детально продиагностировать работоспособность подключения Вашего компьютера к сети.

Ход работы:

Ipconfig

Для отображения параметров IP-протокола используются утилиты *ipconfig* (Windows NT/2000/XP) и *winipcfg* (Windows 9x). Эта утилита выводит на экран основные параметры настройки протокола TCP/IP: значения адреса, маски, шлюза.

1. Нажмите кнопку *Пуск*, выберите строку меню *Выполнить*, наберите символы cmd и нажмите клавишу *Enter* на клавиатуре.

2. В открывшемся окне наберите *ipconfig /all*. При нормальной работе компьютера на экран должен вывестись примерно такой листинг:

Windows IP Configuration

Host Name: vest

Primary Dns Suffix: tvs. *****

Node Type: Hybrid

IP Routing Enabled: No

WINS Proxy Enabled: No

DNS Suffix Search List: tvs. *****

*****

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix. : tvs. *****

Description. . . : Intel(R) PRO/100 S Desktop Adapter

Physical Address. : 00-02-B3-8D-44-53

Dhcp Enabled. . . : Yes

Autoconfiguration Enabled: Yes

IP Address: 83.172.10.54

Subnet Mask. . . : 255.255.255.0

Default Gateway. : 83.172.10.254

DHCP Server. . . : 83.172.10.2

DNS Servers. . . : 192.168.0.1

83.172.10.2

Primary WINS Server: 83.172.10.2

Secondary WINS Server: 213.183.109.3

Lease Obtained. . : 24 августа 2004 г. 9:40:41

Lease Expires. . : 27 октября 2004 г. 9:40:41

Отключите сетевое подключение, повторите команду. При отсутствующем соединении на экран выводится примерно такой листинг:

Windows IP Configuration

Host Name: vest

Primary Dns Suffix: tvs. *****

Node Type: Hybrid

IP Routing Enabled: No

WINS Proxy Enabled: No

DNS Suffix Search List: tvs. *****

*****

Ethernet adapter Local Area Connection:

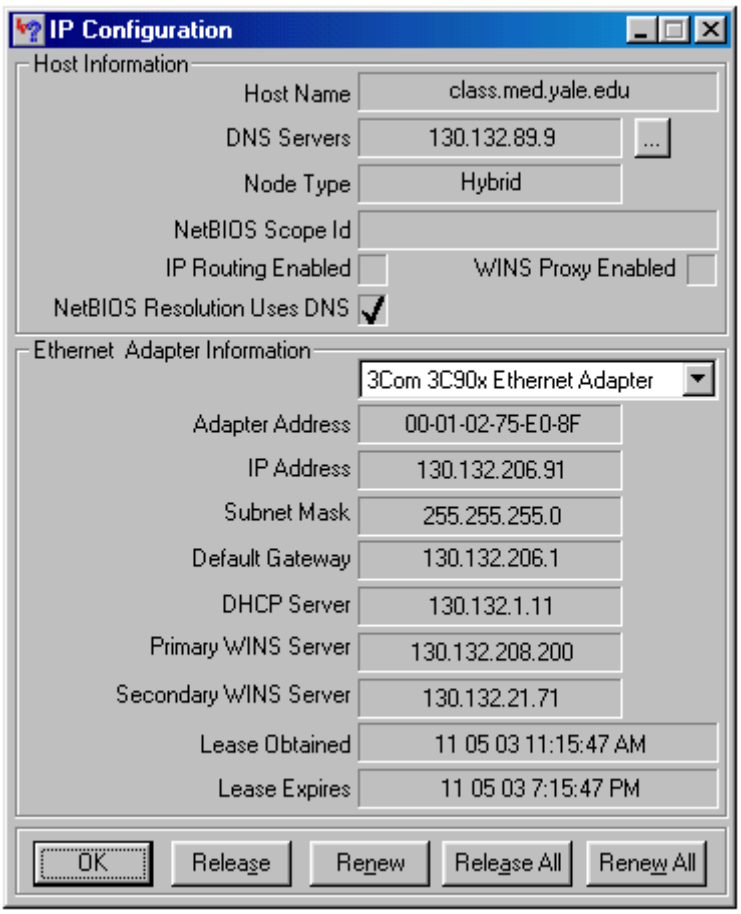
Media State. . . : Media disconnected

Description. . . : Intel(R) PRO/100 S Desktop Adapter

Physical Address. : 00-02-B3-8D-44-53

Обратите внимание, что программа вывела на экран только данные о "физических" параметрах сетевой карты и указала, что отсутствует подключение сетевого кабеля (*Media disconnected*).

В составе Windows 95/98/ME существует программа, которая в графическом режиме показывает основные настройки протокола TCP/IP:



Это *winipcfg*. Для вызова программы следует набрать ее имя в командной строке и нажать клавишу *Enter* (это возможно только в том случае, если Вы работаете с ОС Windows 95/98/ME).

Ping

Команда используется для проверки протокола TCP/IP и достижимости удаленного компьютера. Она выводит на экран время, за которое пакеты данных достигают заданного в ее параметрах компьютера.

Проверка правильности установки протокола TCP/IP. Откройте командную строку и выполните команду:

```
ping 127.0.0.1
```

Адрес 127.0.0.1 — это личный адрес любого компьютера. Таким образом, эта команда проверяет прохождение сигнала "на самого себя". Она может быть выполнена без наличия какого-либо сетевого подключения. Вы должны увидеть приблизительно следующие строки:

> Pinging 127.0.0.1 with 32 bytes of data:
>
> Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
>
> Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
>
> Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
>
> Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
>
> Ping statistics for 127.0.0.1:
>
> Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
>
> Approximate round trip times in milli-seconds:
>
> Minimum = 0ms, Maximum = 0ms, Average = 0ms

По умолчанию команда посылает пакет 32 байта. Размер пакета может быть увеличен до 65 кбайт. Так можно обнаружить ошибки при пересылке пакетов больших размеров. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 миллисекунды). Потом показывается еще один параметр протокола — значение TTL. TTL — "время жизни" пакета. На практике это число маршрутизаторов, через которые может пройти пакет. каждый маршрутизатор уменьшает значение TTL на единицу. При достижении нулевого значения пакет уничтожается. Такой механизм введен для исключения случаев зацикливания пакетов.

Если будет показано сообщение о недостижимости адресата, то это означает ошибку установки протокола IP. В этом случае целесообразно удалить протокол из системы, перезагрузить компьютер и вновь установить поддержку протокола TCP/IP.

Проверка видимости локального компьютера и ближайшего компьютера сети. Выполните команду

ping 192.168.0.19

На экран должны быть выведены примерно такие строки:

Pinging 212.73.124.100 with 32 bytes of data:

Reply from 192.168.0.19: bytes=32 time=5ms TTL=60

Reply from 192.168.0.19: bytes=32 time=5ms TTL=60

Reply from 192.168.0.19: bytes=32 time=4ms TTL=60

Reply from 192.168.0.19: bytes=32 time=4ms TTL=60

Ping statistics for 212.73.124.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 4ms, Maximum = 5ms, Average = 4ms

Наличие отклика свидетельствует о том, что канал связи установлен и работает.

Tracert

При работе в Сети одни информационные серверы откликаются быстрее, другие медленнее, бывают случаи недостижимости желаемого хоста. Для выяснения причин подобных ситуаций можно использовать специальные утилиты.

Например, команда *tracert*, которая обычно используется для показа пути прохождения сигнала до желаемого хоста. Зачастую это позволяет выяснить причины плохой работоспособности канала. Точка, после которой время отклика резко увеличено, свидетельствует о наличии в этом месте "узкого горлышка", не справляющегося с нагрузкой.

В командной строке введите команду:

tracert 192.168.0.19

Вы должны увидеть примерно такой листинг:

Tracing route to 192.168.0.19

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 192.168.0.19

Trace complete.

Route

Команда **Route** позволяет просматривать маршруты прохождения сетевых пакетов при передаче информации.

Выведите на экран таблицу маршрутов TCP/IP, для этого в командной строке введите команду **route print**.

Net view

Выводит список доменов, компьютеров или общих ресурсов на данном компьютере. Вызванная без параметров, команда **net view** выводит список компьютеров в текущем домене.

1. В командной строке введите команду **net view** и вы увидите список компьютеров своей рабочей группы.

2. В командной строке введите команду **net view \\192.168.0.250** для просмотра общих ресурсов расположенных на компьютере **192.168.0.250**

Net send

Служит для отправки сообщений другому пользователю, компьютеру или псевдониму, доступному в сети.

1. В командной строке введите команду **net send 192.168.0.1** Привет. Проверка связи.

Ваше сообщение получит пользователь **192.168.0.1**

2. В командной строке введите команду **net send *** Привет. Проверка связи.

Ваше сообщение получат все пользователи рабочей группы.

Практическая работа № 7 «Разложение ip по подсетям»

Цель: обобщение и систематизация знаний по теме «Адресация в сетях»

Вид работы: фронтальный

Время выполнения: 2 часа

Задания к работе

Задание 1. Переведите следующие двоичные числа в десятичные.

Двоичное значение

1. 1111011
2. 1001001101
5. 10101100.00101000.00000000.00000000
6. 01011110.01110111.10011111.00000000

3. 101101111
4. 1011110001
7. 10010001 0110000 10000000 00011001
8. 01111111 00000000 00000000 00000001

Задание 2. Переведите следующие десятичные числа в двоичные.

Десятичное значение

1. 250
2. 19
3. 348
4. 93
5. 874
6. 109.128.255.254
7. 131.107.2.89
8. 129.46.78.0

Задание 3. Укажите классы следующих IP-адресов.

Адрес

1. 126.102.128.0
2. 1.191.248.0
3. 185.74.41.184
4. 96.247.128.0
5. 168.224.0.1
6. 201.76.98.5
7. 186.112.0.10
8. 28.0.0.0

Задание 4. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

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

Контрольные вопросы:

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

2. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему?

Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?

3. Когда необходим уникальный идентификатор сети?

4. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

Практическая работа №8 ftp-протокол.

Цель работы: Изучить ftp протокол.

Задачи работы:

- Произвести настройки ftp-сервера;
- Настройки и использование защищенного терминала ssh;
- Получить основные сведения о протоколе Telnet;
- Установить и настроить веб-сервер Apache.

Теоретическая часть

Настройка ftp-сервера

FTP (англ. File Transfer Protocol - протокол передачи файлов) - протокол, предназначенный для передачи файлов в сетях передачи данных. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. Он и сегодня широко используется для распространения программного обеспечения и доступа к удалённым хостам.

Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов, передаются по разным портам. Исходящий порт 20, открываемый на стороне сервера, используется для передачи данных, порт 21 для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов.

Vsftpd (Very Secure FTP Daemon или Очень Защищенный FTP Демон) является одним из самых простых в конфигурировании и наиболее часто используемым FTP сервером. Vsftpd обслуживает ftp серверы debian, redhat, ubuntu и прочих крупных компаний. Благодаря предельной простоте настройки, поднятие ftp сервера с помощью vsftpd редко занимает более 5 - 10 минут.

В данной лабораторной работе предполагается показать принцип создания файлового сервера, на который все пользователи смогут складывать файлы, удалять их, создавать директории и т.д.

Установка vsftpd

Установка vsftpd приведена на рис. 4.1. Перед установкой необходимо проверить, что есть соединение с Internet.

```
work@work:~$ sudo apt-get install vsftpd
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 4.1. Установка ftp

Настройка vsftpd

Конфигурирование vsftpd осуществляется редактированием файла /etc /vsftpd.conf (Рис. 4.2). Комментариев (при минимальном знании английского) обычно достаточно, чтобы разобраться что к чему:

- anon_root - директория для анонимных пользователей (/var/ftp/ по умолчанию в большинстве дистрибутивов);
- anonymous_enable - разрешить доступ анонимным пользователям;
- local_enable - разрешить доступ локальным пользователям;
- write_enable - разрешить запись;
- anon_upload_enable - разрешить запись анонимным пользователям

Таким образом, можно отредактировать эти записи в конфиге следующим образом (не стоит удалять остальные опции, если вы не знаете, что они делают):

#возможность работы в автономном режиме

listen=YES

#позволяем анонимных пользователей, учетки anonymous и ftp являются синонимами

anonymous_enable=YES

#разрешаем локальных пользователей (локальные пользователи - это те, которые

#зарегестрированы в системе, то есть на них есть учетные записи)

local_enable=YES

#разрешаем любые формы записи на FTP сервер

write_enable=YES

#разрешаем анонимным пользователям upload

anon_upload_enable=YES

#разрешаем анонимным пользователям создавать директории

anon_mkdir_write_enable=YES

#разрешаем анонимным пользователям переименовывать файлы

anon_other_write_enable=YES

#у анонимов пароль спрашивать не будем

no_anon_password=YES

#директория для доступа анонимных пользователей (если пользователь присутствует)

anon_root=/home/ftp/

#разрешаем соединение по 20 порту

connect_from_port_20=YES

#поддержка древних FTP клиентов

async_abor_enable=YES

#используем родное время, а не GMT

use_localtime=YES

#небольшое приветствие

ftpd_banner=Hello! We come in peace!

#возможность работы как фоновый процесс

background=YES

Должны ли пользователи находится только в своих директориях

YES/NO chroot_local_user=YES

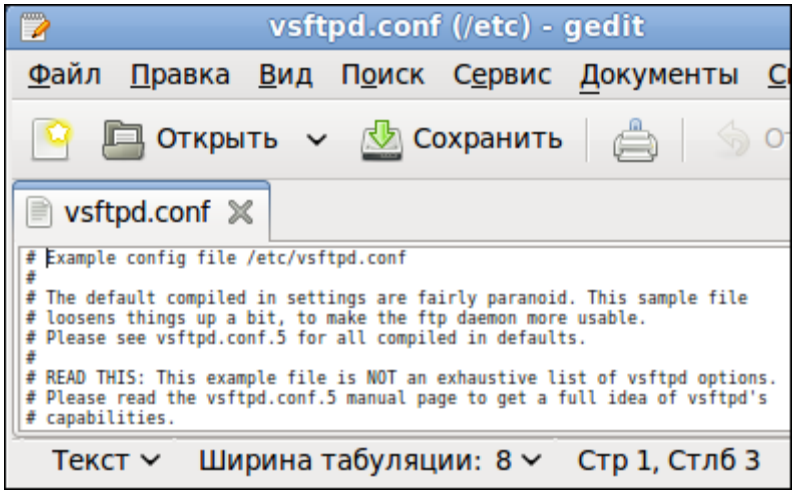


Рис. 4.2. Файл конфигурации ftp

Telnet

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.

Назначение протокола TELNET в предоставлении достаточно общего, двунаправленного, восьмибитного байт-ориентированного средства связи. Его основная задача заключается в том, чтобы позволить терминальным устройствам и терминальным процессам взаимодействовать друг с другом. Предполагается, что этот протокол может быть использован для связи вида терминал-терминал («связывание») или для связи процесс-процесс («распределенные вычисления»).

В протоколе не предусмотрено использование ни шифрования, ни проверки подлинности данных. Поэтому он уязвим для любого вида атак, к которым уязвим его транспорт, то есть протокол TCP. Для функциональности удалённого доступа к системе в настоящее время применяется сетевой протокол SSH (особенно его версия 2), при создании которого упор делался именно на вопросы безопасности. Так что следует иметь в виду, что сессия Telnet весьма беззащитна, если только не осуществляется в полностью контролируемой сети или с применением защиты на сетевом уровне (различные реализации виртуальных частных сетей). По причине ненадёжности от Telnet как средства управления операционными системами давно отказались.

Сетевой протокол ssh

SSH - это специальный сетевой протокол, позволяющий получать удаленный доступ к компьютеру с большой степенью безопасности соединения.

В основном, ssh реализован в виде двух приложений – ssh-сервера и ssh-клиента. В Ubuntu используется свободная реализация клиента и сервера ssh - OpenSSH. При подключении клиент проходит процедуру авторизации у сервера и между ними устанавливается зашифрованное соединение. OpenSSH сервер может работать как с протоколом ssh1, так и с протоколом ssh2. В настоящее время протокол ssh1 считается небезопасным, поэтому его использование крайне не рекомендуется.

Установить OpenSSH можно так:

```
work@work:~$ sudo aptitude install ssh
```

Рис. 4.3. Установка OpenSSH

Метапакет ssh содержит в себе и клиент и сервер, при этом скорее всего будет установлен только сервер, т. к. клиент часто бывает установлен в Ubuntu по умолчанию.

SSH сервер автоматически прописывается в автозагрузку при установке. Управлять его запуском/остановкой или перезапуском можно при помощи команд:

sudo service ssh stop|start|restart

Основным файлом конфигурации ssh-сервера является файл /etc/ssh/sshd_config, который должен быть доступным для чтения/редактирования только суперпользователю. После каждого изменения этого файла необходимо перезапустить ssh-сервер для применения изменений.

Сам по себе, неправильно настроенный ssh сервер - огромная уязвимость в безопасности системы, т. к. у возможного злоумышленника есть возможность получить практически неограниченный доступ к системе. Помимо этого, у sshd есть много дополнительных

полезных опций, которые желательно включить для повышения удобства работы и безопасности.

Для правильной настройки ssh с точки зрения безопасности необходимо отредактировать всего семь параметров:

1. PermitRootLogin – отключение возможности авторизации под суперпользователем;
2. AllowUsers, AllowGroups - предоставление доступа только указанным пользователям или группам;
3. DenyUsers, DenyGroups - блокировка доступа определенным пользователям или группам;
4. Port - изменение порта SSHD;
5. LoginGraceTime - изменение времени ожидания авторизации;
6. ListenAddress - ограничение авторизации по интерфейсу;
7. ClientAliveInterval - рассоединение при отсутствии активности в шелле.

Сменить стандартный порт (22) на котором слушает sshd. Это связано с тем, что многочисленные сетевые сканеры постоянно пытаются соединиться с 22-м портом и как минимум получить доступ путем перебора логинов/паролей из своей базы. Даже если у вас и отключена парольная аутентификация - эти попытки сильно засоряют журналы и (в большом количестве) могут негативно повлиять на скорость работы ssh-сервера. Если же вы по какой либо причине не желаете изменить стандартный порт вы можете использовать как различные внешние утилиты для борьбы брутфорсерами, например fail2ban, так и встроенные, такие как MaxStartups.

По умолчанию root-доступ разрешен. Это означает, что клиент при подключении в качестве пользователя может указать root, и во многих случаях получить контроль над системой. При условии, что по умолчанию в Ubuntu пользователь, добавленный при установке системы имеет возможность решать все административные задачи через sudo, создавать возможность root доступа к системе как минимум странно. Рекомендуется отключить эту опцию совсем.

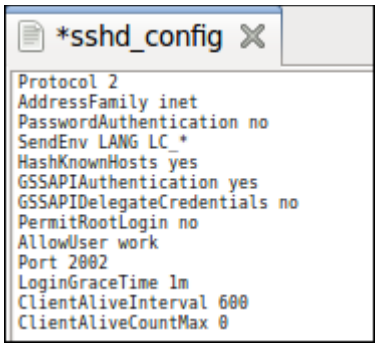


Рис. 4.4. Файл конфигурации ssh

Разрешенная по умолчанию парольная аутентификация является практически самым примитивным способом авторизации в ssh. С одной стороны это упрощает конфигурацию и подключение новых пользователей (пользователю достаточно знать свой системный логин/пароль), с другой стороны пароль всегда можно подобрать, а пользователи часто пренебрегают созданием сложных и длинных паролей. Специальные боты постоянно сканируют доступные из интернета ssh сервера и пытаются авторизоваться на них путем перебора логинов/паролей из своей базы. Настоятельно не рекомендуется использовать парольную аутентификацию.

Как уже было сказано, ssh может работать с протоколами ssh1 и ssh2. При этом использование небезопасного ssh1 крайне не рекомендуется.

В конечном итоге файл конфигурации должен выглядеть так, как на рис. 4.4.

Для удаленного доступа с операционной системы Windows необходимо установить на ней специальный клиент – putty (рис 4.5).

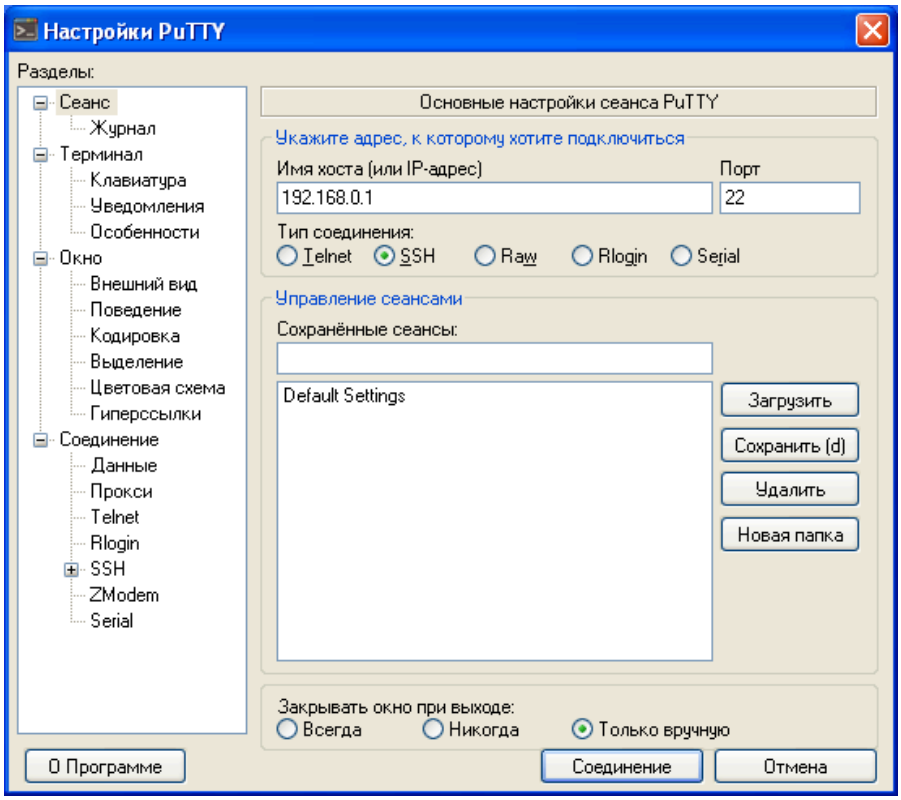


Рис. 4.5. PuTTy

Для настройки сессии введите IP хоста (192.168.0.1). Так же настройте кодировку в пункте Translation, поменяв её на UTF-8.

Веб-сервер

Apache HTTP-сервер – свободный веб-сервер. Apache является кроссплатформенным программным обеспечением, поддерживает операционные системы Linux, BSD, Mac OS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv6.

Для установки apache2 введите команду, представленную на рис. 4.6.

```
work@work:~$ sudo apt-get install apache2
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 4.6. Установка apache2

Файлы конфигурации Apache2 находятся в директории: /etc/apache2:

- conf.d/
- sites-available/
- sites-enabled/
- mods-available/
- mods-enabled/
- apache2.conf
- envvars
- httpd.conf
- ports.conf

В Ubuntu основным файлом настройки Apache2 является apache2.conf. Он играет роль системного файла, в котором собраны основные и самые важные настройки сервера.

Файл httpd.conf - пустой и предназначен для добавления дополнительных настроек, он включен в основной файл настройки apache2.conf

В файле envvars описаны переменные среды, необходимые для функционирования Apache-сервера.

В ports.conf вынесены настройки портов на которые можно будет подключиться к серверу или конкретному сайту на нем.

В папке conf.d находятся дополнительные конфигурационные файлы.

Для описания всех доступных сайтов используется папка sites-available в которой расположены файлы с описанием виртуальных хостов - VirtualHosts, опубликованные же сайты находятся в папке sites-enabled в виде ссылок на файлы доступных сайтов из папки sites-available.

Таким же образом в папках mods-available и mods-enabled настраивается доступность модулей используемых сервером.

Теперь необходимо подготовить компьютер к работе веб-сервера. Прежде всего необходимо создать единую папку для всех сайтов, которые будут там размещаться, например /home/user/www. Лучшее место для такой папки это домашний каталог пользователя. Далее в этой папке необходимо создать папку сайта. Например, /home/user/www/site1. И в эту папку кинуть файлы сайта.

Следующая команда (рис. 4.7) создает запись виртуального хостинга копируя стандартную запись из файла конфигурирования Apache:

```
work@work:~$ sudo cp /etc/apache2/sites-availab
le/default /etc/apache2/sites-available/site1
```

Рис. 4.7. Копирование файла конфигурации

Теперь необходимо отредактировать файл, который находится по директории /etc/apache2/sites-available/site1. Необходимо настроить имя сервера, URL сервера и

директорию, по которой находятся файлы сайта. После настроек файл конфигурации должен выглядеть, например, так, как на рис. 4.8.

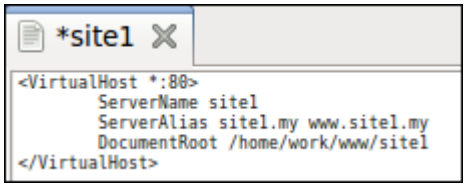


Рис. 4.8. Файл конфигурации сайта site1

Теперь необходимо как-то научить операционную систему распознавать домен .my. Для этого достаточно прописать необходимые строки в файле /etc/hosts, например так, как на рис. 4.9.

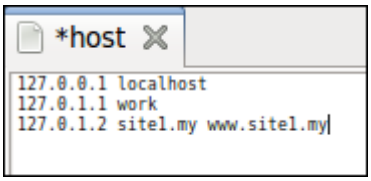


Рис. 4.9. Редактирование файла hosts

Для начала необходимо разместить ссылку на VirtualHost в папку sites-enabled, и перечитать конфигурацию сервера Apache. Для создания ссылки можно выполнить такую команду и перечитать параметры (рис. 4.10). После этого ваш сайт, файлы которого размещаются в директории /home/user/www/site1 будет отображаться в браузере по адресу: site1.my или www.site1.my.

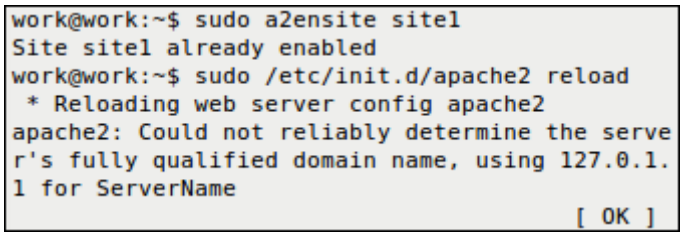


Рис. 4.10. Активация сайта

Практическая работа

1. На виртуально машине разверните ftp-сервер;
2. Разрешите анонимный доступ для всех пользователей на данный ftp-сервер. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
3. Настройте разграничение прав доступа к определенным кактологам пользователей на ftp-сервере. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
4. Настройте смешанный режим доступа анонимных и зарегестрированных пользователей. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
5. Установить ssh-сервер на вашу операционную систему Linux. Настройет ssh с точки зрения безопасности;

6. На вашей основной операционной системе установить ssh-клиент (если основная операционная система Linux) или putty (если основная операционная система Windows). Проверьте работу ssh, настроив клиент соответствующим образом;
7. Установить веб сервер на Linux Ubuntu;
8. Создайте простую html-страничку. Разместите её на веб-сервере по веб-адресам: work.my и www.work.my.

Контрольные вопросы

1. Каково назначение ftp-сервера?
2. Каким образом производится настройка vsftpd?
3. Каково назначение сетевого протокола SSH?
4. Какие основные параметры рекомендуется менять при настройки SSH с точки зрения его безопасности и почему?
5. Каково назначение Telnet? Почему Telnet не рекомендуется использовать?
6. Каково назначение Apache?
7. Какие основные конфигурационные файлы Apache существуют?

Практическая работа №9

Изучение и настройка маршрутизатора.

Цель: научиться настройке сети на основе маршрутизатора D-Link DIR-300 NRU.

Задача: настройка сети на основе маршрутизатора D-Link DIR-300 NRU. План занятий:

Ознакомление с маршрутизатором

Настройка маршрутизатора

Настройка L2TP соединения

Настройка беспроводной сети

Настройка маршрутизации

Настройка портов

Контроль выполненной работы

Продолжительность занятий 6 часов.

Версия продукта: рисунки и технологии, задействованные в работе браузер Mozilla Firefox и роутер D-Link DIR-300 NRU Rev.2. По принципу действия настройка используемых продуктов схожа с другими браузерами и другими моделями маршрутизаторов.

Требования к уровню подготовки:

Знание стандартной модели компьютерных сетей, существующей терминологии;

Знание аппаратного обеспечения, умение выполнять настройки сетевого оборудования;

Знание сетевых возможностей современных операционных систем, использование первичных навыков сетевого администрирования.

В результате выполнения заданий данной практической работы обучающийся должен обладать следующими знаниями и умениями:

общее представление об устройстве сетей;

базовые знания о программных средствах, предназначенных для работы в Internet;

знания о настройке сетевых подключений;

умения по настройке сетевых подключений;

знания о настойке беспроводных маршрутизаторов в общем виде.

умения по настройке беспроводных маршрутизаторов в общем виде.

.1 Ознакомление с маршрутизатором

Устройство DIR-300NRU представляет собой беспроводной маршрутизатор со встроенным 4-портовым коммутатором, который позволяет быстро и просто организовать беспроводную и проводную сеть дома и в офисе.

Вы можете подключить беспроводной маршрутизатор DIR-300NRU к кабельному или DSL-модему или выделенной Ethernet-линии, чтобы использовать высокоскоростное соединение с сетью Интернет для решения широкого круга профессиональных задач. Встроенный 4-портовый коммутатор маршрутизатора позволяет подключать компьютеры, оснащенные Ethernet-адаптерами, игровые консоли и другие устройства к Вашей сети.

Используя беспроводной маршрутизатор DIR-300NRU, Вы сможете быстро организовать беспроводную сеть дома и в офисе, что позволит Вашим сотрудникам или членам Вашей семьи подключаться к беспроводной сети практически в любой точке (в зоне действия беспроводной сети). Маршрутизатор работает с беспроводными устройствами стандарта 802.11b/g.

В маршрутизаторе реализовано множество функций для беспроводного интерфейса. Устройство поддерживает несколько стандартов безопасности (WEP, WPA/WPA2, IEEE 802.1X), фильтрацию подключаемых устройств по MAC-адресу, несколько режимов работы (точка доступа, клиент, мост), а также позволяет использовать технологии WPS и WMM.

Беспроводной маршрутизатор DIR-300NRU оснащен встроенным межсетевым экраном. Расширенные функции безопасности позволяют минимизировать последствия действий хакеров и предотвращают вторжения в Вашу сеть и доступ к нежелательным сайтам для пользователей Вашей локальной сети.

Внешний вид устройства.

Ознакомьтесь с внешним видом устройства маршрутизатора D-Link DIR-300 NRU.

Рис. 1 **Передняя панель.**

Рис. 2 **Описание значений световых индикаторов**

Рис. 3 **Задняя панель.**

Рис. 4 **Описание разъемов**

Установка устройства

Итак, давайте найдем и запустим установочную программу, для этого

Зайдите в «ПРИЛОЖЕНИЯ» - «DIR-300 NRU» - «DIR-300.exe», запускаем и выбираем «Install Router» (Рис.5).

Рис. 5

Вас приветствует окно, где нужно выбрать язык установки, жмем «Далее» (Рис.6).

Рис. 6

Выберете имя пользователя и пароль для входа в настройки маршрутизатора (Рис.7).

Рис. 7

Происходит автоматическая проверка подключения маршрутизатора к сети, для этого подключите ваш коаксиальный кабель в WAN-Порт маршрутизатора, а ваш ПК подсоедините к LAN-Порту маршрутизатору патч-кордом и подождите 30 секунд и нажмите «Далее» (Рис.8).

Рис. 8

Выберете тип подключения к Internet широкополосный (Рис.9)

Рис. 9

Ввести новый пароль безопасности маршрутизатора (Рис.10).

Рис. 10

Укажите имя, ключ безопасности беспроводной сети, в зависимости от выбранного уровня безопасности (Рис.11), (Рис.12).

Рис. 11

Рис. 12

Подтверждение настроек. Возможность сохранить все настройки в тестовом файле Network Security Setting.txt (Рис.13)

Рис. 13

Последняя автоматическая настройка параметров маршрутизатора и подтверждение удачной настройки сети, нажмите «Готово» (Рис.14).

Рис. 14

.2 Настройка маршрутизатора

беспроводной сеть маршрутизатор учебный

Веб-интерфейс. Откройте браузер (рекомендуется Mozilla Firefox), в адресной строке введите #"justify">По умолчанию пароль отсутствует, его можно будет указать в настройках маршрутизатора.

В некоторых версиях прошивок требуется дополнительно ввести указанный на картинке код (captcha).

Перед нами появилось изображение (Рис. 15):

Рис. 15

Обновление прошивки

Прошивка маршрутизатора - это комплекс программ, обеспечивающих его работоспособность и функционал. В некоторых случаях установленная на заводе прошивка не обеспечивает требуемую стабильность или не поддерживает нужные функции.

Рекомендуется использовать следующие версии прошивок с поддержкой L2TP DIR-300 ревизия B (максимальная скорость порядка 20 мегабит/с): dir300b_v2.05_abnj.bin.

При необходимости можно загрузить файл перевода интерфейса маршрутизатора на русский язык: dir300b_v2.05_abnj_langpack_ru.bin

Для обновления прошивки достаточно указать путь к прошивке и нажать «Apply» в разделе «Firmware Update» вкладки «Maintenance» (Рис. 4).

После обновления прошивки имеет смысл сбросить настройки в изначальное состояние («Save and Restore»).

Далее будет приведен вариант настройки для русского интерфейса.

Рис. 16

.3 Настройка L2TP соединения

Сеть и Интернет

После обновления прошивки повторно введите логин и пароль, переключитесь на вкладку «Установка», выберите «Установка Интернет».

Существует два варианта настройки соединения - вручную и с помощью мастера установки. Для маршрутизатора DIR-300 ревизии «B» с прошивкой dir300b_v2.05_abnj.bin (поддерживается L2TP Dual Access) настраивать нужно с помощью мастера установки.

Рис. 17

Мастер установки Интернет-соединения

Требуется указать пароль для доступа к маршрутизатору, по умолчанию - пусто

Укажите сетевые реквизиты (Рис. 21).

Внимание! DNS-сервер и клонирование MAC-адреса при настройке DIR-300revB потребуется указать позже в режиме ручной настройки!

Рис. 21

Нажмите «Подключение». Остальные настройки прописываются в режиме ручной настройки (Рис. 22).

Рис. 22

Настройка Интернет-соединения вручную (Рис.23)

Тип интернет-соединения: Russia L2TP (Dual Access).

В настройках выбранного соединения необходимо указать IP-адрес, маску подсети (255.255.255.0), шлюз - Ваш шлюз, DNS-сервер (можно выбрать один из двух имеющихся - 10.0.0.1 или 10.0.0.2). Для защиты соединения в сетях используется привязка MAC-IP. Если Вы настраиваете сеть с компьютера, ранее подключенного напрямую, то имеет смысл выбрать пункт «Клонирование MAC-адреса», в ином случае потребуется сбросить привязку по MAC-адресу.

В графе «IP-адрес/Имя Сервера» введите адрес VPN-сервера (vpn.akado-ural.ru для L2TP-протокола), «Учетная запись L2TP» - логин, в «Пароль L2TP» - пароль для доступа в Интернет, строкой ниже его повторите.

В графе «MTU» по умолчанию установлено значение 1400. Такое же значение по умолчанию установлено для VPN-соединения в ОС семейства Windows. Производитель рекомендует оставить значение по умолчанию.

Если Вы хотите, чтобы маршрутизатор автоматически подключался к VPN-серверу при каждом включении, то нужно выбрать «Всегда»/«Всегда включено».

Нажмите «Сохранить настройки» и подождите некоторое время.

Рис. 23

.4 Настройка беспроводной сети

Рис. 24

Мастер установки беспроводного соединения

Задайте имя беспроводной сети, тип шифрования и ключ сети. Нажмите «Далее» (Рис.25).

Рис. 25

Установите пароль беспроводной сети (Рис.26).

Рис. 26

Далее подробные сведения о настройке вашей беспроводной сети с выбранными вами параметрами. Нажмите «Сохранить» (Рис.27).

Все настройки можно изменить вручную.

Рис. 27

Настройка беспроводного соединения вручную (Рис.28).

Включите беспроводной доступ к сети (отметить галочкой) и выберете время доступа к беспроводной сети «По расписанию» или «Всегда».

Задайте имя беспроводной сети

Выберете беспроводной канал подключения (значения 1-12 или автоматическое назначение)

Режим безопасности (отключить - работа беспроводной сети без ключа безопасности, WPA или WPA/WPA2)

При выборе WPA или WPA/WPA2 выберете тип шифра и аутентификацию. Далее придумайте свой ключ сети.

Сохранить настройки

Рис. 28

.5 Настройка маршрутизации

На вкладке «Расширенные настройки» нужно выбрать «Маршрутизация» и прописать маршрут:

Интерфейс - Физический интерфейс WAN;

Назначение - 10.0.0.0;

Маска подсети - 255.0.0.0;

Шлюз - Ваш шлюз.

Используемые маршруты нужно отметить галочкой (Рис.29).

Рис. 29

.6 Настройка портов

Не все программы могут корректно работать через маршрутизатор. Для некоторых программ (DC++, Radmin/RDP/HTTP/FTP-сервера) нужно настроить переадресацию портов. Рассмотрим эту процедуру на примере P2P-клиента.

Установить p2p-клиент. Открыть папку «Приложение» в ней найти файл «olympusp2p.exe», запустить его. Следовать инструкциям установки.

После установки запустить и в P2P-клиенте зайти в Файл → Настройки → Настройки подключения → Ручная настройка фаервола. Указанные там номера TCP и UDP-портов потребуется прописать в настройках маршрутизатора, как указано ниже(Рис.). Если к сети подключается несколько компьютеров, то порты в P2P-клиентах должны быть разными, при необходимости значения можно изменить (Рис.30).

Рис. 30

В настройках маршрутизатора вкладке «Расширенные настройки» выбрать пункт «Перенаправление портов», прописать TCP и UDP-порты, указанные в P2P-клиенте, и сохранить настройки. Используемые правила должны быть отмечены галочкой. Аналогично можно настроить проброс портов для других приложений (Рис.31).

Если номера портов идут подряд, как в данном случае, то можно пробросить диапазон портов.

Практическая работа № 10

Тема: Диагностика правильности настроек маршрутизаторов.

Цели работы: ОСВОЕНИЕ ПРИНЦИПОВ РАБОТЫ С МАРШРУТИЗАТОРОМ. АНАЛИЗ ТЕКУЩЕЙКОНФИГУРАЦИИ С КОМАНД ПОДГРУППЫ SHOW ВЫПОЛНЕНИЕ БАЗОВОЙ НАСТРОЙКИ С ПОМОЩЬЮ УТИЛИТЫ SETUP.

Оборудование: ПК, консольный кабель, маршрутизатор CISCO Catalyst 1600.

Учебные пособия: В.Г. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2007. – 958 с.

Теоретическая часть

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.

Цель маршрутизации – это выбор оптимального маршрута доставки данных из одной сети в другую.

Для обеспечения маршрутизации строятся специальные таблицы, которые называются таблицами маршрутизации.

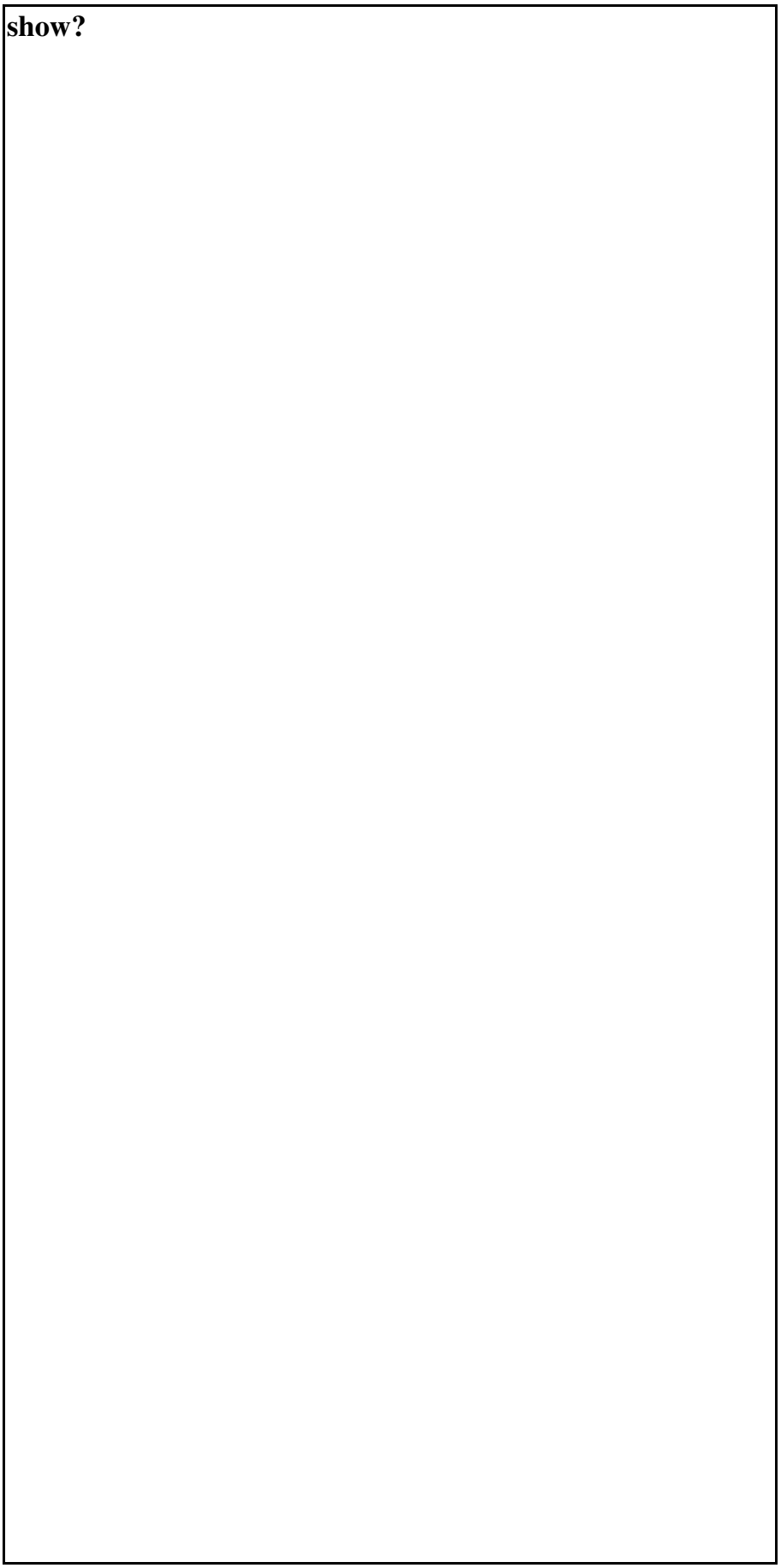
Существует два способа получения информации о сети назначения и занесения ее в таблицу маршрутизации:

- **Статический:** Маршрутизатор узнает о маршруте, когда администратор настраивает этот маршрут вручную. В этом случае при изменении топологии сети записи о маршрутах должны обновляться вручную.
- **Динамический:** Маршрутизатор динамически изучает маршруты, после того как на нем настроен протокол маршрутизации. Протокол маршрутизации автоматически обновляет маршруты при получении информации о смене сетевой топологии. Маршрутизатор изучает и поддерживает маршруты к удаленным сетям, обмениваясь обновлениями маршрутной информации с другими маршрутизаторами в сети.

Ход работы

Данная лабораторная работа поможет вам ознакомиться с командой маршрутизатора – show. Команда show – наиболее важная команда сбора информации. Setup – это утилита cisco IOS, которая может помочь установить некоторые параметры основной конфигурации маршрутизатора. Утилита Setup не предназначена для ввода сложных параметров протоколов маршрутизатора. Целью режима установки является задание минимальной конфигурации для маршрутизатора, который не может найти свою конфигурацию через другой источник.

Вы должны подсоединить рабочую станцию к маршрутизатору, при помощи консольного кабеля (roll-over). Ознакомьтесь со следующими командами:


show?
show flash
show cdp
show clock
show running-config
show cdp interface

show hosts	**show startup-config**	**show cdp neighbors**
show users	**show interface**	**show cdp neighbors detail**
show history	**show protocol**	
show arp	**show version**	

Практическое занятие № 12

Тема: Изучение и настройка коммутаторов сетей.

Цели работы: Научиться производить базовую конфигурацию коммутатора.

Оборудование: ПК, консольный кабель, коммутатор CISCO Catalyst 2960.

Учебные пособия: В.Г. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2007. – 958 с.

Теоретическая часть

Коммутаторы локальных сетей (*LAN)* обрабатывают и передают данные на уровне кадров, что соответствует канальному уровню модели *OSI*. Принятие решения на коммутацию выполняется на основании анализа физических адресов (*MAC-media access control*) источника и назначения, которые находятся в заголовке кадра.

Коммутатор постоянно изучает MAC-адреса в сети для формирования своей таблицы MAC-адресов. Когда все MAC-адреса занесены в таблицу, коммутатор может быстро и точно принять решение о передаче или фильтрации. Коммутатор строит таблицу MAC-адресов, прослушивая поступающие кадры и проверяя поле MAC-адреса источника. Если пришел кадр с новым MAC-адресом источника, то коммутатор создает новую запись в таблице MAC-адресов в соответствие с интерфейсом, на который этот кадр пришел.

Если на порт коммутатора приходит кадр с MAC-адресом, неизвестным коммутатору, то он транслирует кадр на все свои порты кроме того, на который он пришел. Занесение в таблицу MAC-адресов произойдет тогда, когда рабочая станция, которой был адресован данный кадр, ответит, и ответ придет на конкретный порт коммутатора.

Список основных команд для начального конфигурирования коммутатора.

Команда	
configure terminal	вход в режим глобальной конфигурации

hostname name	устанавливается имя коммутатора
line con 0	переход в подрежим конфигурирования доступа по консольному порту
line vty 5 15	переход в подрежим конфигурирования доступа через Ethernet порты с указанием числа одновременно открываемых сессий.
login	вход в подрежим конфигурирования пароля при доступе через консоль (cons) или по telnet сессии (vty)
password pass	установка пароля на подключение по консоли (cons) или через telnet (vty)
enable pass	установка пароля на вход в привилегированный режим (пароль сохраняется в открытом виде)
enable secret pass	установка пароля на вход в привилегированный режим (пароль сохраняется в зашифрованном виде)
ip address addr subn	установка адреса коммутатора для подключения к нему по *Telnet*
ip default-gateway addr	установка адреса шлюза для подключения через удаленную сеть
interface fastethernet 0/x	вход в подрежим конфигурации интерфейса с номером *X*
duplex{ auto || full || half }	настройка интерфейса на режим передачи информации
speed{10|100|1000| auto| nonegotiate }	настройка скорости работы интерфейса
switchport port-security mac-address mac-addr	статическое добавление MAC-адреса к списку адресов, имеющих доступ к данному порту коммутатора
switchport port-security mac-address sticky	разрешение доступа рабочей станции (*WS*), которая подключена к данному порту и первой начнет передачу
switchport port-security maximum число	максимальное число статических MAC-адресов, которым разрешен доступ к одному порту; применяется одновременно ко всем интерфейсам в режиме глобальной конфигурации
switchport port-security violation {protect | restrict | shutdown}	действия коммутатора, если к порту пытается подключиться *WS* с неразрешенным *MAC*-адресом

Практическая работа № 13

Тема: Диагностика работоспособности и правильности настроек коммутаторов сетей.

Цели работы: Научиться производить анализ конфигурации. Настраивать безопасность а портах коммутатора.

Оборудование: ПК, консольный кабель, коммутатор CISCO Catalyst 2960.

Теоретическая часть

Самым простым и доступным способом выяснить проблемы, возникающие при настройке и работе коммутатора, является использование команд подгруппы "show" в привилегированном режиме "enable".

Список основных команд подгруппы show для просмотра настроек коммутатора.

Команда

show interface fastethernet 0/x	показывает состояние интерфейса X
show interface vlan 1	показывает ip-адрес для конфигурации
show interfaces [interface-id | vlan-id] [description | etherchannel | pruning | stats |status [err-disabled] | switchport | trunk]	отображение информации о специфике настройки и работы интерфейса
show mac address- table [aging-time | count | dynamic | static] [address hw-addr] [interface interface-id] [vlan vlan-id]	показывает опционально таблицу MAC-адресов
show port-security [interface interface-id][address]	показывает информацию о настройках безопасности на интерфейсе
show running-config	показывает файл текущей конфигурации
show startup-config	показывает файл конфигурации, хранимой в энергонезависимой памяти (NVRAM)
show version	показывает версию программного обеспечения коммутатора и тип оборудования

Настройка безопасности на портах коммутатора

Настройка списков рабочих станций, которые могут подключаться к портам коммутатора, по терминологии Cisco называется - *port security*. Поскольку известно, что к одному порту коммутатора может быть подключено одно устройство, то можно ограничить доступ в сеть другим устройствам через данный порт. Если устройство, которому запрещен доступ через порт, делает такие попытки, то могут быть предприняты следующие действия:

1. *Protect* - Отбросить кадр.
2. *Restrict* - Отбросить кадр и послать уведомление на SNMP счетчик событий о несанкционированном доступе.
3. *Shutdown* - Выключить порт. Из этого состояния его можно будет вывести командой глобальной конфигурации *errdisable recovery cause secure-violation* или командами режима настройки интерфейса *shutdown – no shutdown*.

Для применения port security на интерфейсе необходимо использовать команду подрежима конфигурации интерфейса "*switchport port-security*".

Важно заметить, что в коммутаторе *Cisco2950* опцию *port security* можно применять только к интерфейсам, которые не подключены к другим коммутаторам. Для указания того, что порт коммутатора не подключен к другому коммутатору, необходимо использовать команду "*switchport mode access*".

Практическая работа № 14

Тема: Принцип организации VPN.

Средства построения сетей vpn

Защищенные сети VPN можно строить на основе разнообразных программных и аппаратных средств [8, 9]. Отметим следующие решения:

● VPN на базе сетевых операционных систем;

● VPN на базе маршрутизаторов и межсетевых экранов;

● VPN на базе специализированных аппаратных устройств.

*VPN на базе сетевых операционных систем***.** Многие современные операционные системы (ОС) поддерживают функцию маршрутиза-ции IP-пакетов, службы сервера удаленного доступа и сервера VPN. Установив на сервер с такой ОС две или более интерфейсных сетевых карты, можно достаточно легко и недорого настроить полноценный сервер VPN. Протоколы туннелирования стандартные – PPTP, L2TP, IPSec и др. Недостатки данного решения: относительно невысокая пропускная способность сервера VPN, особенно для протоколов IPSec/L2TP, и ограниченный у компьютера набор интерфейсов гло-бальных сетей (только один-два порта RS-232C). Для выхода на ско-ростные цифровые каналы необходимо приобретать и устанавливать специальные, довольно дорогие, сетевые карты.

VPN на базе маршрутизаторов и межсетевых экранов. Маршрутиза-торы и межсетевые экраны, находящиеся на границе корпоративной сети с открытой общественной, являются естественным местом рас-положения сервера VPN.

Маршрутизаторы могут поддерживать функции формирования защищенных туннелей по умолчанию или в качестве дополнительной возможности, предлагаемой за отдельную плату. Маршрутизаторы имеют большой набор разнообразных сетевых интерфейсов, что облегчает реализацию VPN. Интеграция VPN с маршрутизатором упрощает администрирование. Недостатки данного решения: работа VPN может отрицательно повлиять на другой трафик, может также снизиться пропускная способность маршрутизатора.

Межсетевые экраны (МЭ) также могут включать в свой состав и RAS. Учитывая, что МЭ специально предназначены для защиты информационного взаимодействия с открытыми сетями, можно сделать вывод, что при реализации этими устройствами и функций VPN обеспечивается комплексная защита всего информационного обмена. Недостаток решения: операции, связанные с шифрованием данных, дополнительно загружают процессор МЭ и снижают его пропускную способность.

VPN на базе специализированных аппаратных устройств. Представ-ляют собой отдельные устройства на основе специализированной ОС реального времени, имеющие два или более сетевых интерфейсов и *аппаратную* криптографическую поддержку – так называемый “чер-ный ящик VPN” (VPN Black Box) – и ориентированные на формиро-вание защищенных туннелей. Этот вариант построения VPN может быть использован в сетях, требующих высокой производительности. Чаще всего его применяют для создания туннелей “сеть-сеть” на основе протокола туннелирования IPSec. Недостаток решения – мо-дернизация устройства в будущем может оказаться слишком дорого-стоящей или невозможной.

1.8. Схемы сетей vpn с протоколом pptp на основе ос Windows Server 2003/xp

Компания Microsoft разработала много дополнительных средств в своих ОС Windows Server 2003/XP с целью построения VPN, доста-точно защищенных и удобных в настройке (служба RAS, протоколы PPP, MS-CHAP v2, MPPE, PPTP и др.).

Как следует из вышеизложенного, виртуальную частную сеть образуют серверы VPN (другое название – “шлюзы VPN”) и VPN-клиенты. Каждый VPN-клиент создает отдельный защищенный туннель с сервером VPN, поэтому сервер в общем случае должен поддерживать и обслуживать множество клиентских соединений. Так сервер VPN на основе ОС Windows Server 2003 поддерживает одновременно до 1000 туннелей.

Функции сервера VPN – выполнять задачи установленного прото-кола туннелирования и маршрутизировать принятые по туннелю пакеты в корпоративную сеть и обратно. При организации туннеля с использованием протокола PPTP, основу которого составляет прото-кол PPP, многие функции сервера VPN можно реализовать с помо-щью сервера удаленного доступа RAS. В ОС Windows Server 2003 для создания программных маршрутизаторов, серверов RAS и VPN используется одна многофункциональная оснастка **Служба маршрути-зации и удаленного доступа** (Routing and Remote Access Service).

Относительно VPN-клиентов можно сказать, что программное обеспечение для их поддержки имеется во всех популярных ОС от компании Microsoft и, прежде всего, в ОС Windows XP. VPN-клиенты настраиваются из окна **Сетевые соединения** (Network Connection) выбором **Создать соединение** (New Connection).

Остановимся на базовых схемах VPN.

На рис. 9 представлена схема VPN “клиент-сеть” с использовани-ем местной городской телефонной сети и сети Internet. В отличие от ранее рассмотренной схемы на основе сервера RAS (см. рис. 4), здесь трафик клиента защищен на всем пути от этого клиента до сервера VPN корпоративной сети.

Среда Internet должна *обеспечивать маршрутизацию* IP-пакетов *между* сервером RAS ISP и сервером VPN.

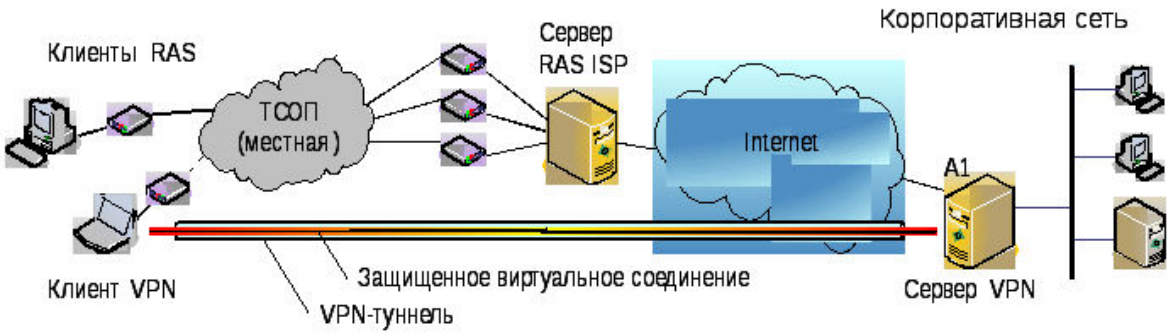


Рис. 9. Туннель “клиент-сеть” по ТСОП и сети Internet

На рис. 10 представлена схема VPN “клиент-сеть” с использова-нием только внутренних каналов связи корпоративной сети. Упро-щенный вариант предыдущей схемы.

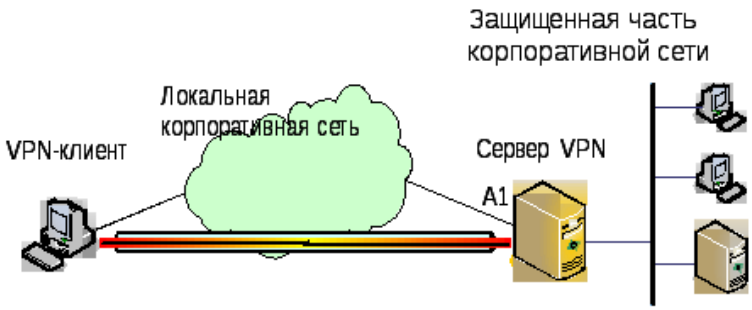


Рис. 10. Туннель “клиент-сеть” внутри корпоративной сети

Эта схема интересна тем, что позволяет с помощью VPN защитить от перехвата внутрисетевой трафик привилегированных клиентов сети (администраторов, директора) к особо важной части сети.

Среда корпоративной сети должна *обеспечивать маршрутизацию* IP-пакетов *между* VPN-клиентом и сервером VPN.

На рис. 11 представлена схема VPN “сеть-сеть” с использованием каналов Internet. Данная схема, в отличие от ранее рассмотренной (см. рис. 6), обеспечивает защиту трафика клиентов на всем пути его прохождения по сети Internet.

Среда Internet должна *обеспечивать маршрутизацию* IP-пакетов *между* серверами S1 и S2.

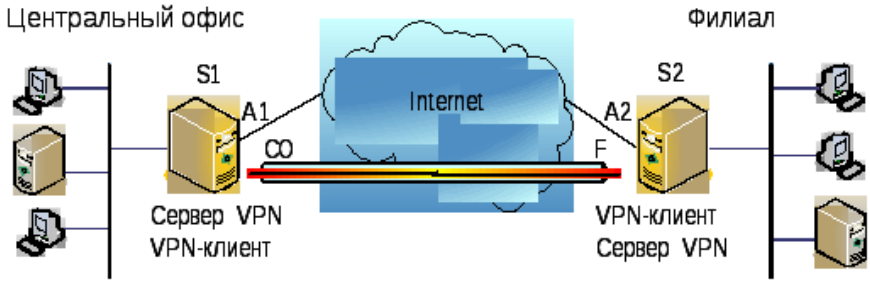


Рис. 11. Туннель “сеть-сеть” по каналам Internet

В этой схеме автоматически инициировать туннель может любая сторона, когда у нее появится трафик в другую сеть. После образования туннеля каждый из серверов S1, S2 будет выполнять и роль VPN-клиента, и роль VPN-сервера.

Для обеспечения безопасности при создании туннеля в данной конфигурации VPN интерфейсам вызова по требованию (A1 и A2) необходимо присвоить произвольные символьные *имена интерфей-сов* и пароли (на рис. 11 это имена CO и F). Имена интерфейсов и пароли здесь выступают в роли учетных данных фиктивных пользо-вателей, которым требуется установить соединение с противополож-ной стороной.

Когда на сервере S1 вводится имя CO (и пароль), то эта пара будет сохранена в локальной базе учетных данных пользователей сервера S1. Аналогично имя F (и пароль) после ввода на S2 будут сохранены в базе учетных данных пользователей сервера S2.

При настройке интерфейсов вызова по требованию на каждом сервере необходимо еще указать имя интерфейса и пароль *противо-положной* стороны. Эти учетные данные хранятся на сервере как дополнительные атрибуты интерфейса.

С именами интерфейсов связаны следующие термины, использу-емые при конфигурировании VPN “сеть-сеть”.

● Сервер **S1:** CO (и пароль) – учетные данные “входящего под- ключения”,

F (и пароль) – учетные данные “исходящего под- ключения”.

● Сервер **S2**: F (и пароль) – учетные данные “входящего под- ключения”,

CO (и пароль) – учетные данные “исходящего под- ключения”.

Если серверу S1 потребуется создать туннель к S2, то S1 посылает в запросе имя F (и пароль). Сервер S2 сравнивает полученные учет-ные данные входящего подключения с имеющимися данными в своей базе учетных данных пользователей. При совпадении – туннель создается.

Практическая работа № 15

Тема: «**Способы организации VPN**.»

ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ РАБОТЫ

1.1 Цель работы: познакомиться со способами организации VPN.

1.2 В результате выполнения лабораторной работы студент должен знать:

o Понятие VPN

o Настройку VPN сервера на базе Windows 2003

o Настройку клиентов

o Возможные неисправности и способы их диагностирования

1.3 Используемые программно-технические средства:

Персональная ЭВМ класса IBM PC стандартной конфигурации; операционная система Windows2000/XP/Vista, MicrosoftOfficeWord.

1.4 В процессе выполнения лабораторной работы студент должен:

o Ознакомится с теоретическим материалом.

o Выполнить практическую часть работы

o Подготовить отчет по лабораторной работе.

o Отчитаться по исполненному заданию.

Перед выполнением лабораторной работы каждый студент обязан изучить правила техники безопасности при работе в помещении с электронно-вычислительной техникой.

1.5 Указания по оформлению отчета:

Отчет должен содержать: титульный лист, цель работы; ответы на контрольные вопросы; выводы.

Указания по сдаче зачета преподавателю

Для сдачи зачета необходимо:

1) выполнить практическое задание

2) предъявить отчет;

3) ответить на контрольные вопросы.

Теоретические сведения

Виртуальная частная сеть позволяет подключить сетевые компоненты через другую сеть, например Интернет. Из компьютера под управлением Windows Server 2003 можно сделать сервер удаленного доступа, чтобы другие пользователи могут подключаться к нему с помощью виртуальной частной сети, а затем войдите в сеть и получить доступ к общим ресурсам. Виртуальные частные сети достигают этого "туннелированием", через Интернет или другую публичную сеть таким образом, что предоставляет такую же безопасность и возможности как и частные сети. Данные отправляются в общедоступной сети с использованием ее инфраструктуры маршрутизации, но для пользователя, выглядит как будто данные передаются по выделенному частному каналу.

2.1 Общие сведения о VPN

Виртуальная частная сеть — средства подключения к виртуальной частной сети (например, к офисной сети) при помощи общедоступной сети (например, Интернет). Виртуальная частная сеть объединяет достоинства подключения удаленного доступа к серверу удаленного доступа с простотой и гибкостью подключений к Интернету. С помощью подключения к Интернету, вы можете путешествовать по всему миру и тем не менее, в большинстве ситуаций подключаться к офисной сети локальным вызовом на подходящий номер телефона для доступа к Интернету. Если высокоскоростное подключение (кабель или DSL) к Интернету есть на компьютере и в офисе, можно взаимодействовать с офисом на полной скорости Интернета, который намного быстрее, чем любой тип коммутируемого подключения через аналоговый модем. Эта технология позволяет подключиться другими компаниями или филиалами через общедоступную сеть, обеспечивая защищенный обмен данными предприятия. VPN-подключения через Интернет логически функционирует как выделенный канал глобальной сети (WAN).

Виртуальные частные сети проверенных ссылки служат для убедитесь, что только авторизованные пользователи могут подключаться к сети. Чтобы убедиться в том, что

данные безопасного, передаваемых по сети, VPN-подключение использует туннельный протокол точка-точка (PPTP) или протокол (L2TP) для шифрования данных.

Практическая работа № 16

Тема: Порядок проектирования локальной сети.

Цели работы: изучить основные этапы проектирования локальной сети, научиться определять исходные данные, определять размеры и структуру сети.

Оборудование: ПК.

Учебные пособия: В.Г. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2007. – 958 с.

Теоретическая часть

На рисунке приведена примерная последовательность этапов и варианты выбора при проектировании локальной сети.

Ход работы.

Определение исходных данных для проектирования сети:

1. **Цели использования сети.** Для точной формулировки целей проектирования сети необходимо составить инфологическую модель организации, в которой выявляются потоки информации, циркулирующие внутри организации, каналы по которым данная информация перемещается, степень критичности и чувствительности информации. Расставьте приоритеты по целям (1 – важная, 2 – существенная, 3 нормальная).

Централизованное хранение информации в базах даны

Архивирование и резервное копирование информации

Обеспечение информационной безопасности в рамках ЛВС организации

Взаимодействие локальной сети организации с глобальной сетью Internet

Характеристики сети и ее составляющих. Для достижения поставленных целей сеть должна иметь следующие характеристики:

Наличие доступа в Internet, скорость доступа

Пропускная способность

Наличие сервера и его производительность

Производительность рабочих станций

Отказоустойчивость компонентов сети

Возможность расширения

Характеристики существующих компьютеров и других устройств. В случае если у организации уже имеется информационная инфраструктура, необходимо определить список оборудования, которое может быть использовано в создаваемой сети, и список оборудования которое нуждается в модернизации.

Определение размеров и структуры сети. На данном этапе необходимо выбрать топологию сети. Описать достоинства и недостатки для заказчика:

Выбранная топология

Достоинства

Звезда

Шина

Гибридная

Вывод:
_____
_
_____
_____
_____
_____.

Практическая работа №17

Санитарно-гигиенические требования к размещению компьютерного оборудования.

Цель: ознакомиться с санитарно-гигиеническими требованиями к размещению компьютерного оборудования.

Учебные помещения не размещаются в подвальных и цокольных этажах здания.

Этажность здания общеобразовательного учреждения не должна превышать 3 этажей.

Гардеробы размещаются на 1 этаже с обязательным оборудованием ячеек для каждого класса. Гардеробы оснащаются вешалками для одежды и ячейками для обуви. Не следует устраивать гардеробы в учебных помещениях и рекреациях.

Набор помещений создает условия для изучения обязательных учебных дисциплин (с учетом национальной и региональной специфики), а также дополнительных предметов по выбору обучающихся в соответствии с их интересами и дифференциацией по направлениям для углубленного изучения одного — двух — трех предметов. Учебные классы не следует располагать вблизи помещений, являющихся источниками шума и запахов (мастерских, спортивных и актовых залов, пищеблока).

Учебные помещения включают: рабочую зону (размещение учебных столов для обучающихся), рабочую зону учителя, дополнительное пространство для размещения учебно — наглядных пособий, технических средств обучения (ТСО), зону для индивидуальных занятий обучающихся и возможной активной деятельности.

Площадь кабинетов принимается из расчета 2,5 кв. м на 1 обучающегося при фронтальных формах занятий, 3,5 кв. м — при групповых формах работы и индивидуальных занятиях.

Площадь и использование кабинетов информатики должны соответствовать гигиеническим требованиям, предъявляемым к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы.

Оптимальные размеры рабочей зоны обучающихся зависят от угла видимости (связанного с расстоянием от доски до первых боковых рядов — парт). При каждом кабинете или группе из 2 — 3 кабинетов организуется лаборантская (наличие лаборантской обязательно в кабинетах химии, физики, биологии, информатики).

Спортивный зал следует размещать на 1 этаже в пристройке. Его размеры предусматривают выполнение полной программы по физвоспитанию и возможность внеурочных спортивных занятий.

Количество и типы спортивных залов предусматриваются в зависимости от вида общеобразовательного учреждения и его вместимости. Площади спортивных залов приняты 9 х 18 м, 12 х24 м, 18 х 30 м при высоте не менее 6 м.

При спортивных залах должны быть предусмотрены снарядные, площадью 16 — 32 кв. м в зависимости от площади спортзала; раздевальные для мальчиков и девочек, площадью 10,5 кв. м каждая; душевые, площадью 9 кв. м каждая; уборные для девочек и мальчиков, площадью 8 кв. м каждая; комната для инструктора, площадью 9 кв. м. В состав помещений физкультурно-спортивного назначения необходимо включать помещение (зону), оборудованное тренажерными устройствами, а также, по возможности, бассейн.

В зависимости от назначения учебных помещений могут применяться столы ученические (одноместные и двухместные), столы аудиторные, чертежные или лабораторные. Расстановка столов, как правило, трехрядная, но возможны варианты с двухрядной или однорядной (сблокированной) расстановкой столов.

Каждый обучающийся обеспечивается удобным рабочим местом за партой или столом в соответствии с его ростом и состоянием зрения и слуха. Для подбора мебели соответственно росту обучающихся производится ее цветовая маркировка. Табуретки или скамейки вместо стульев не используются.

Парты (столы) расставляются в учебных помещениях по номерам: меньшие — ближе к доске, большие — дальше. Для детей с нарушением слуха и зрения парты, независимо от их номера, ставятся первыми, причем обучающиеся с пониженной остротой зрения должны размещаться в первом ряду от окон. Детей, часто болеющих ОРЗ, ангинами, простудными заболеваниями, следует рассаживать дальше от наружной стены.

При оборудовании учебных помещений соблюдаются следующие размеры проходов и расстояния между предметами оборудования в см:

между рядами двухместных столов — не менее 60;

между рядом столов и наружной продольной стеной — не менее 50 — 70;

между рядом столов и внутренней продольной стеной (перегородкой) или шкафами, стоящими вдоль этой стены, — не менее 50 — 70;

от последних столов до стены (перегородки), противоположной классной доске, — не менее 70, от задней стены, являющейся наружной, — не менее 100, а при наличии оборотных классов — 120;

от демонстрационного стола до учебной доски — не менее 100;

от первой парты до учебной доски — 2,4 — 2,7 м;

наибольшая удаленность последнего места обучающегося от учебной доски — 860;

высота нижнего края учебной доски над полом — 80 — 90;

угол видимости доски (от края доски длиной 3 м до середины крайнего места обучающегося за передним столом) должен быть не менее 35 градусов для обучающихся II — III ступени и не менее 45 градусов для детей 6 — 7 лет.

Кабинеты физики и химии должны быть оборудованы специальными демонстрационными столами, где предусмотрены пульты управления проектной аппаратурой, подача воды, электричества, канализации. Для обеспечения лучшей видимости учебно-наглядных пособий демонстрационный стол рекомендуется устанавливать на подиум. В кабинетах физики и химии устанавливают двухместные ученические лабораторные столы (с надстройкой и без нее) с подводкой электроэнергии, сжатого воздуха (лаборатория физики). Лаборатория химии оборудуется вытяжными шкафами, расположенными у наружной стены возле стола преподавателя.

В мастерских для трудового обучения размещение оборудования осуществляется с учетом создания благоприятных условий для зрительной работы, сохранения правильной рабочей позы и профилактики травматизма. Столярные мастерские оборудуются верстаками, расставленными либо под углом 45 градусов к окну, либо в 3 ряда перпендикулярно светонесущей стене так, чтобы свет падал слева, расстояние между ними должно быть не менее 80 см в переднее — заднем направлении. В слесарных мастерских допускается как левостороннее, так и правостороннее освещение с перпендикулярным расположением верстаков к светонесущей стене. Расстояние между рядами одноместных верстаков — не менее 1,0 м, двухместных — 1,5 м. Тиски крепятся к верстакам на расстоянии 0,9 м между их осями. Слесарные верстаки должны быть оснащены предохранительной сеткой, высотой 0,65 — 0,7 м. Сверлильные, точильные и другие станки должны устанавливаться на специальном фундаменте и оборудоваться предохранительными сетками, стеклами и местным освещением. Инструменты, используемые для столярных и слесарных работ, должны соответствовать возрасту обучающихся. В слесарных и столярных мастерских и кабинетах обслуживающего труда устанавливаются умывальники и электрополотенца. В каждом кабинете (мастерской) для оказания первой медицинской помощи должны быть аптечки. Все работы выполняются обучающимися в специальной одежде (халат, фартук, берет, косынка). При выполнении работ, создающих угрозу повреждения глаз, следует использовать защитные очки.

Стены учебных помещений должны быть гладкими, допускающими их уборку влажным способом.

Полы должны быть без щелей и иметь покрытие дощатое, паркетное или линолеум на утепленной основе. Полы туалетных и умывальных комнат должны выстилаться керамической или мозаичной шлифованной плиткой; не используют цементные, мраморные или другие аналогичные материалы.

10. Требования, предъявляемые к кабинетам оборудованных техническими средствами обучения и средствами вычислительной техники. Воздействия, оказываемые компьютерной техникой и мобильной связью на здоровье учащихся.

Помещения, в которых размещаются компьютерные учебные классы, должны оборудоваться в соответствии с Санитарными правилами и нормами. «Гигиенические требования к персональным электронно-вычислительным машинам. СанПиН 2.2.2/2.4.1340-03». Помещения должны иметь естественное и искусственное освещение. Расположение рабочих мест с компьютерами не допускается в цокольных и подвальных помещениях.

Окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток.

Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и т.п.

Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе электронно-лучевой трубки (ЭЛТ) в учебном классе должна быть не менее 6,0 кв. м, а при продолжительности работы менее 4-х часов в день допускается минимальная площадь 4,5кв. м.

Помещения с ПК должны оборудоваться системами отопления, кондиционирования воздуха или эффективной приточно - вытяжной вентиляций.

В помещениях, оборудованных ПЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ.

Поверхность пола в помещениях эксплуатации ПК должна быть ровной, без выбоин, нескользкой, удобной для очистки и влажной уборки, обладать антистатическими свойствами.

Шумящее оборудование (печатающее устройство, сервера и т.п.), уровни шума которого превышают нормативное, должно размещаться вне помещений с ПЭВМ.

Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки.

При входе в учебный класс с компьютерной техникой должны быть оборудованы встроенные или пристенные шкафы (полки) для хранения портфелей, сумок студентов.

Комплектация компьютерного класса:

10-11 компьютеров, размещение которых соответствует санитарно- техническим нормам (из расчета 6 кв. м при высоте потолка 3 м на 1 рабочее место);

колонки (по необходимости);

принтер с допустимым уровнем шума (по необходимости);

проектор (по необходимости);

сканер (по необходимости);

оборудование для организации локальной сети;

программное обеспечение;

учебно-методическая литература, необходимая для обеспечения полноценного учебного процесса;

маркерная доска.

Компьютерный класс должен быть оснащен

средствами пожаротушения;

светильниками местного освещения (по необходимости);

стендом методической информации;

информационным стендом (в коридоре у входа в класс);

системой сигнализации;

кондиционерами (по необходимости);

медицинской аптечкой.

В компьютерном классе на окнах устанавливается жалюзи и распашные решетки.

Стенд методической информации должен содержать:

инструкции по технике безопасности и о правилах работы;

комплексы упражнений для гимнастики, физкультурных пауз, минуток, глаз;

перечни Интернет ссылок на электронные источники (на которые разрешен доступ из класса) для получения дополнительной информации по дисциплинам, ведущихся в классе;

рекомендованные литературные источники;

методические рекомендации по прохождению дисциплин, ведущихся в классе;

ответы на наиболее часто задаваемые вопросы.

Информационный стенд должен содержать:

расписание работы класса;

график самостоятельной работы в классе;

текущие объявления преподавателей;

расписание консультаций преподавателей;

дополнительные информационные материалы (по необходимости).

Варианты воздействия ЭМП на биоэкосистемы, включая человека, разнообразны: непрерывное и прерывистое, общее и местное, комбинированное от нескольких источников и сочетанное с другими неблагоприятными факторами среды и т.д.

На биологическую реакцию влияют следующие параметры ЭМП:

интенсивность ЭМП (величина);

частота излучения;

продолжительность облучения;

модуляция сигнала;

сочетание частот ЭМП,

периодичность действия.

Сочетание вышеперечисленных параметров может давать существенно различающиеся последствия для реакции облучаемого биологического объекта.

В подавляющем большинстве случаев облучение происходит полями

относительно низких уровней, ниже перечисленные последствия относятся к

таким случаям.

Многочисленные исследования в области биологического действия ЭМП позволят определить наиболее чувствительные системы организма человека: нервная, иммунная, эндокринная и половая. Эти системы организма являются критическими. Реакции этих систем должны обязательно учитываться при оценке риска воздействия ЭМП на население. Биологический эффект ЭМП в условиях многолетнего длительного воздействия накапливается, в результате возможно развитие отдаленных последствий, включая дегенеративные процессы центральной нервной системы, рак крови (лейкозы), опухоли мозга, гормональные заболевания.

Особо опасны ЭМП могут быть для детей, беременных (эмбрион), людей с заболеваниями центральной нервной, гормональной, сердечно-сосудистой системы, аллергиков, людей с ослабленным иммунитетом.

Практическая работа №18
Оформление проектной документации

Часто понятия СКС и ЛВС используют взаимозаменяемо. В основе сети передачи данных лежит структурированная кабельная система. СКС обеспечивает физическую среду передачи сигналов. Сетевое, серверное и абонентское оборудование, подключенное к СКС, упрощенно называют компьютерной и телефонной сетью.

Проектирование локальной сети подразумевает:

- проектирование структурированной кабельной системы (СКС);
- проектирование компьютерной сети;
- проектирование телефонной сети.

Проект СКС включает магистральную и горизонтальную подсистемы. Магистральная подсистема служит для связи между распределительными пунктами зданий и этажей. Горизонтальная подсистема объединяет абонентов в общую сеть для доступа к магистральным ресурсам.

Техническое задание

Техническое задание можно считать первым этапом создания СКС. Этот документ включает требования Заказчика по числу распределительных пунктов и рабочих мест, их расположению, категории или классу системы. В большинстве случаев требуется комплексное решение – компьютерная и телефонная сеть плюс электропитание должны быть у каждого пользователя.

С целью создания долговечной системы на этапе проектирования СКС в подсистемы закладывают резерв по пропускной способности и количеству линий. Цена такого подхода, безусловно, выше, однако избыточность системы обеспечивает снижение эксплуатационных издержек. Следует учитывать, что в пределах срока службы СКС может смениться три-четыре поколения компьютеров и сетевых устройств.

До начала разработки проектной документации мы помогаем Заказчику сформулировать оптимальные требования и обсуждаем все важные аспекты создаваемых систем.

Рабочий проект СКС

Рабочий проект СКС – это детально проработанный документ, раскрывающий все аспекты реализации системы. Качественно составленный рабочий проект может обеспечить монтаж даже сторонними исполнителями. Проектирование СКС и локальной сети ведется с учетом современных норм и отраслевых стандартов.

Рабочий проект структурированной кабельной системы включает:

- титульный лист и лист согласования;
- пояснительную записку;
- структурную схему;

- структурную схему системы телекоммуникационного заземления;
- схемы кабельных проводок, расположения элементов телекоммуникационной инфраструктуры;
- схемы размещения панелей в телекоммуникационных шкафах / стойках;

- схемы подключений кабелей на панелях / кроссах;

- схемы организации рабочих мест;
- таблицы подключений магистральной и горизонтальной подсистем, системы телекоммуникационного заземления;
- спецификацию материалов.

Пояснительная записка содержит изложение принципов и особенностей проектируемой сети, систем телекоммуникационного заземления и администрирования. Поэтажные планы дают точное пространственное расположение каждого элемента системы на архитектурных чертежах здания. Структурные схемы отражают количественные параметры подсистем СКС: особенности, конфигурацию, число рабочих мест, число кабелей в горизонтальной и магистральной подсистемах, тип монтажных конструктивов и панелей. Таблицы соединений содержат перечень всех элементов инфраструктуры, их назначение, привязку к помещениям, портам, кабельным трассам. Спецификация включает точный перечень требуемых для реализации проекта материалов.

Итог этапа рабочего проектирования – создание функционально полного комплекта документации, предоставляющего исчерпывающую информацию для проведения монтажных работ.

Исполнительная документация

В процессе выполнения монтажных работ в систему вносятся изменения. После завершения работ Заказчик получает комплект актуальной исполнительной документации без дополнительной оплаты.

Преимущества Заказчика

- Заказчик получает полную и точную документацию систем. Проект соответствует европейским и международным стандартам, российским нормам и правилам;
- Мы используем терминологию международных и европейских стандартов с профессиональным переводом смыслового значения. Наш словарь терминов используется многими компаниями отрасли;
- Заказчик не переплачивает за необоснованную избыточность систем. Мы рассчитываем каждый метр кабеля и каждый элемент системы, вплоть до крепежа, проектируем оптимальные маршруты прокладки кабелей, необходимый резерв кабель-каналов;
- Заказчик не теряет время. Мы приступаем к монтажу через два - три дня после утверждения Заказчиком технического задания, выполняя проектирование и монтаж систем параллельно;
- Мы строго выполняем требования электромагнитной совместимости при параллельной прокладке силовых и слаботочных кабелей;
- При проектировании силовых и слаботочных кабельных систем в комплексе Заказчик получает дополнительную экономию на кабель каналах;
- Мы обеспечиваем эквипотенциальность заземления силовых и слаботочных систем.

Практическая работа №19

Тема: Порядок тестирования и приемоздаточных испытания компьтерной сети.

Теоретическая часть

1. Порядок приемки кабельных систем

1.1. Общие положения

Испытания проводятся на территории здания или комплекса зданий – объекта работ. Тестированию подлежат все установленные в здании или комплексе зданий кабельные линии. В испытаниях участвуют представители Заказчика и исполнителя.

Процедура тестирования производится в соответствии с TSB-67 (TIA/IEC) и, частично, ISO/IEC 11801. Качество и наличие заземления не входит в рамки тестирования СКС.

1.2.Объект испытаний

Объектом испытаний является структурированная кабельная система. Эта система использует для передачи данных медный кабель категории 5е неэкранированная витая пара.

1.3.Цель испытаний

В процессе испытаний должны быть достигнуты следующие цели:

- осуществлен контроль целостности проложенных кабельных путей;

- произведена проверка качества компонентов и выполнения работ;

- произведена проверка соответствия кабельной системы требованиям стандартов в соответствии с ТЗ и ТУ проекта;

- откорректированы ошибки и несоответствия в маркировке кабельных линий;

- установлены и исправлены недоработки и ошибки монтажа;

- выполнена паспортизация кабельной системы.

1.4.Объем и порядок проведения испытаний

Перечень этапов испытаний и последовательность проведения испытаний. Количественные характеристики, подлежащие оценке

Процесс испытания структурированной кабельной системы представляет собой 4 этапа и производится в следующем порядке:

1) Выборочный (не менее 5%) визуальный осмотр горизонтальных и вертикальных кабельных трасс. На этом этапе проверяется целостность оболочки кабеля, правильность расположения и крепления кабельных жгутов, а также местоположения кабельных трасс.

2) Выборочный (не менее 5%) визуальный осмотр рабочих мест. На этом этапе проверяется правильность прокладки кабеля в месте расположения информационной розетки, целостность оболочки и изоляции, а также правильность подсоединения проводников пары к контактам модульного гнезда. Кроме того, измеряются такие количественные характеристики, как развив проводников в паре и зазор между оболочкой кабеля и корпусом модульного гнезда.

3) Визуальный осмотр кроссового оборудования. При этом проверяется целостность оболочки и изоляции проводников кабеля, правильность его разделки, наличие меток портов и соответствие текущего состояния системы предоставляемой документации.

4) Измерение электрических характеристик медного кабеля (неэкранированная витая пара) с помощью кабельных тестеров. Измеряются: комплексное электрическое сопротивление кабельных линий, затухание сигнала, переходное затухание на ближнем конце (NEXT), отношение затухания к переходному затуханию (ACR), сопротивление петли постоянному току, задержка распространения сигнала и длина линий. Проверяется правильность разводки кабеля.

1.5. Характеристики, подлежащие оценке и порядок проведения этапов испытаний

Осмотр кабельных трасс

Перед осмотром кабельных трасс необходимо обеспечить доступ к их элементам. Осмотр производится на произвольно выбранных участках. При обнаружении несовпадений расположения кабельных трасс с указанными на этажном плане производится полный осмотр всех кабельных трасс.

При осмотре кабельных трасс необходимо руководствоваться следующими положениями:

- кабельные трассы должны быть защищены от случайного доступа;

- не допускается повреждение оболочки кабеля;

- не допускается скручивание и сдавливание кабеля.

Осмотр рабочих мест.

Осмотр производится на произвольно выбран