

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего  
образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ  
УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий  
Кафедра вычислительные системы и технологии

## ОТЧЕТ

по лабораторной работе №1

по дисциплине

Программное обеспечение вычислительных сетей

Одноранговые сети

РУКОВОДИТЕЛЬ:

\_\_\_\_\_ Кочешков А.А.

СТУДЕНТ:

\_\_\_\_\_ Сапожников В.О.

19-ИВТ-3

Работа защищена «\_\_» \_\_\_\_\_

С оценкой \_\_\_\_\_

## **Введение**

В данной работе будут использованы машины с следующими версиями ОС:

Виртуальные машины:

HOST1win7 – Windows 7 Максимальная, версия 6.1 (сборка 7601: Service Pack 1)

HOST2win7 – Windows 7 Максимальная, версия 6.1 (сборка 7601: Service Pack 1)

**Цель работы:** изучить свойства, методы организации и особенности использования одноранговых вычислительных сетей. Научиться выполнять установку, конфигурирование и управление ЛВС рабочей группы на базе ОС Microsoft Windows.

### **План работы**

1. Выполнить настройку компонентов сетевых средств Windows.
2. Изучить свойства сетевых ресурсов в Windows.
3. Изучить свойства локальных учетных записей пользователей в Windows.
4. Рассмотреть и сравнить способы распределения полномочий администрирования при управлении пользователями и ресурсами в рабочей группе
5. Ознакомиться с ролью реестра в конфигурировании сети.
6. Изучить возможности команды NET для конфигурирования и управления сетью.
7. Ознакомиться с назначением и спецификой применения среды команды NETSH.
8. Восстановить исходную конфигурацию всех настроек в системе.

#### **1. Выполнить настройку компонентов сетевых средств Windows.**

- Определить состав и свойства установленных компонентов:
  - Сетевые адаптеры
  - Протоколы
  - Клиенты
  - Службы
- Базовые свойства сетевого адаптера Ethernet
- Для установленных протоколов, клиентов и служб разобрать все доступные настройки.
- Назначить имя рабочей группы, имя компьютера (в формате NetBIOS и DNS).
- Назначить имя рабочей группы, имя компьютера. Сконфигурировать стек протоколов TCP/IP. Проверить работоспособность сети по различным протоколам, меняя привязки сетевого адаптера к протоколам и протоколов к клиентам и службам.

### **Теоретические сведения**

**Клиент** - компьютерное устройство, которое отсылает запросы серверу, касающиеся выполнения определенных задач или предоставления конкретной информации.

**Сервер** - компьютерное устройство, выполняющие определённые задачи или предоставляющее информацию в ответ на запрос клиента

**Сетевые протоколы** – стандарты, на основе которых выполняются программы, которые осуществляют сетевые коммуникации. Протоколы задают способы передачи сообщений и обработки ошибок в сети, а также

позволяют разрабатывать стандарты, не привязанные к конкретной аппаратной платформе. Разные протоколы зачастую описывают лишь разные стороны одного типа связи. Сетевые протоколы предписывают правила работы компьютерам, которые подключены к сети. Они строятся по многоуровневому принципу и несмотря на то, что каждый протокол предназначен для приема конкретных входных данных и генерирования определенного результата, все протоколы в системе можно заменять другими протоколами.

Для сетевых протоколов используется модель Open System Interconnection (OSI). Данная модель состоит из семи уровней:

- **Физический уровень.** На данном уровне определяются физические характеристики линий связи;
- **Канальный уровень.** На этом уровне определяются правила использования физического уровня узлами сети;
- **Сетевой уровень.** Этот уровень отвечает за адресацию и доставку сообщений;
- **Транспортный уровень.** Этот уровень обеспечивает контроль очередности прохождения компонентов сообщения;
- **Сеансовый уровень.** Данный уровень предназначен для координации связи между двумя прикладными программами, работающими на разных рабочих станциях;
- **Представительский уровень.** Этот уровень служит для преобразования данных из внутреннего формата компьютера в формат передачи;
- **Прикладной уровень.** Текущий уровень обеспечивает удобный интерфейс связи сетевых программ пользователя.

### Сетевой адаптер

**Сетевой адаптер** – это периферийное устройство компьютера, которое взаимодействует со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами.

Функции сетевого адаптера:

- Оформление передаваемой информации в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.
- Получение доступа к среде передачи данных.
- Кодирование последовательности бит кадра последовательностью электрических сигналов при передаче данных и декодирование при их приеме.
- Преобразование информации из параллельной формы в последовательную и обратно. Эта операция связана с тем, что для упрощения проблемы синхронизации сигналов и удешевления

линий связи в вычислительных сетях информация передается в последовательной форме, бит за битом, а не побайтно, как внутри компьютера.

- Синхронизация битов, байтов и кадров. Для устойчивого приема передаваемой информации необходимо поддержание постоянного синхронизма приемника и передатчика информации. Сетевой адаптер использует для решения этой задачи специальные методы кодирования, не использующие дополнительной шины с тактовыми синхросигналами. Эти методы обеспечивают периодическое изменение состояния передаваемого сигнала, которое используется тактовым генератором приемника для подстройки синхронизма. Кроме синхронизации на уровне битов, сетевой адаптер решает задачу синхронизации и на уровне байтов, и на уровне кадров.

Подключение машин HOST1win7 и HOST2win7 по локальной сети происходит через сетевые адаптеры Intel(R) PRO/1000 MT, представляющиеся VMware по умолчанию.



Сетевое подключение Intel(R) PRO/1000 MT

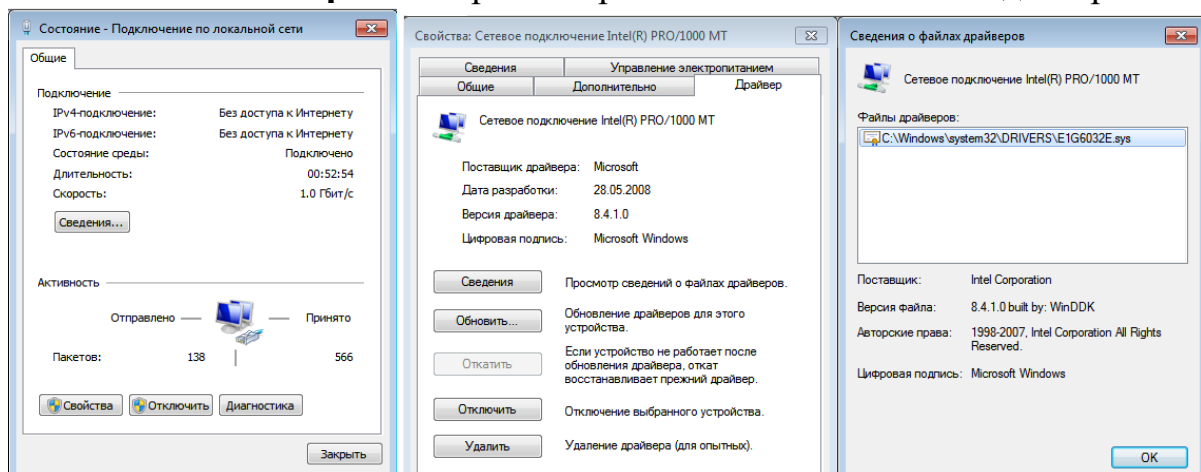
Тип устройства: Сетевые адаптеры

Изготовитель: Intel

Размещение: PCI гнездо 33 (PCI-шина 2, устройство 1, функция 0)

**Цель:** изучить основные характеристики и параметры сетевого адаптера

**Выполнение работы:** рассмотрим состояние сетевого адаптера:



- Состояние подключения: информация о подключение по протоколу IPv4, по протоколу IPv6, скорость подключение локальной сети, его состояние и длительность.
- Информацию об активности: кол-во переданных и полученных байт

Ознакомимся со свойствами сетевого подключения:

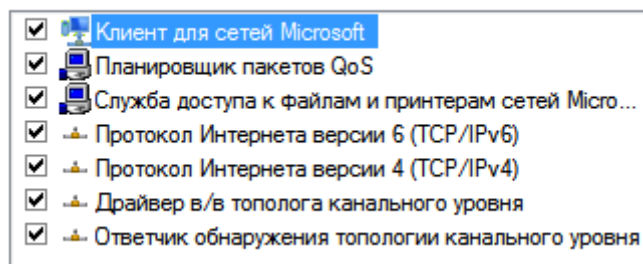
- Вкладка «Общие»: сведения о сетевом адаптере, его состоянии и

расположении

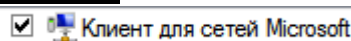
- Вкладка «Дополнительно»: сведения о свойствах адаптера, которые мы можем включить/отключить
- Вкладка «Драйвер»: сведения о текущем драйвере, его версии и изготовителе
- Вкладка «Сведения»: позволяет получить более полную информацию о каждом свойстве адаптера

Компоненты, используемые данным подключением:

Отмеченные компоненты используются этим подключением:



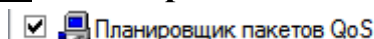
### **Клиент сетей Microsoft.**



**Цель:** ознакомиться с «Клиент для сетей Microsoft»

**Выполнение работы:** данный компонент позволяет подключаться к общим ресурсам на других компьютерах, оснащенных операционной системой Windows. В ОС Windows 10 данный клиент не имеет возможности изменения настроек. Его можно только удалить из списка сетевых подключений.

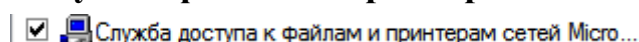
### **Служба: Планировщик пакетов QoS**



**Цель:** ознакомиться с «Планировщик пакетов QoS»

**Выполнение работы:** Данная служба осуществляет управление сетевым трафиком, в том числе и управление скоростью передачи и службой приоритетов.

### **Служба доступа к файлам и принтерам сетей Microsoft**



**Цель:** ознакомиться с «Служба доступа к файлам и принтерам сетей Microsoft»

**Выполнение работы:** Данная служба позволяет другим компьютерам получать доступ к ресурсам данного компьютера с помощью сети Microsoft.

## Протокол TCP/IP

**TCP/IP** - Набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет. Название TCP/IP происходит из двух наиважнейших протоколов семейства — Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были разработаны и описаны первыми в данном стандарте. Уровни протоколов TCP/IP расположены по принципу стека (англ. stack, стопка) — это означает, что протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы инкапсуляции. Например, протокол TCP работает поверх протокола IP.

Стек протоколов TCP/IP включает в себя четыре уровня:

1. прикладной уровень (application layer) - HTTP, RTSP, FTP, DNS
2. транспортный уровень (transport layer) – TCP, UDP, SCTP, DCCP
3. сетевой уровень (Internet layer) – IP (ICMP, IGMP – работают поверх IP), ARP
4. канальный уровень (link layer) – Ethernet, IEEE, Token Ring

Протоколы этих уровней полностью реализуют функциональные возможности модели OSI. На стеке протоколов TCP/IP построено всё взаимодействие пользователей в IP-сетях. Стек является независимым от физической среды передачи данных, благодаря чему, в частности, обеспечивается полностью прозрачное взаимодействие между проводными и беспроводными сетями.

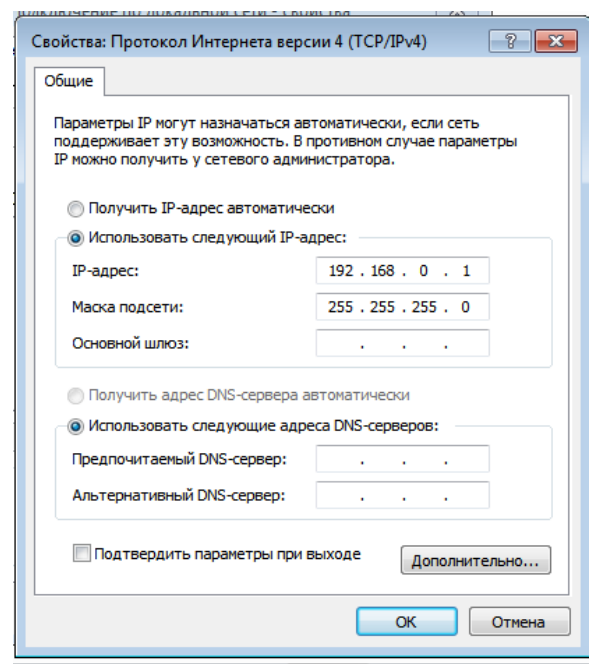
**Цель:** ознакомиться с протоколом TCP/IP и его настройкой

**Выполнение работы:** чтобы перейти к настройкам, необходимо зайти в свойства сетевого адаптера. IP-адрес можно задать двумя способами: автоматически и вручную. По умолчанию стоит автоматическая установка IP-адреса, но для эксперимента зададим его вручную.

Для протокола IPv4 установим следующие IP-адреса:

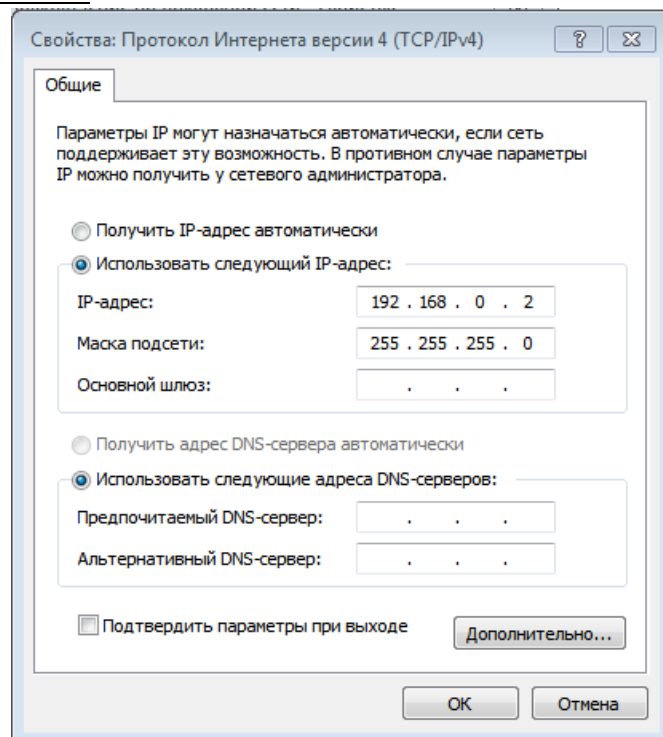
HOST1win7

IP-адрес: 192.168.0.1  
Маска: 255.255.255.0



## HOST2win7

IP-адрес: 192.168.0.2  
Маска: 255.255.255.0



Проверим, что компьютеры находятся в одной сети при помощи утилиты ping. С машины HOST1win7 обратимся к HOST2win7. (На момент выполнения данного пункта машины уже находятся в одной рабочей группе. Настройка рабочей группы будет рассмотрена далее)

```
ca. C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\win7Host1>ping 192.168.0.2

Обмен пакетами с 192.168.0.2 по 32 байтами данных:
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128

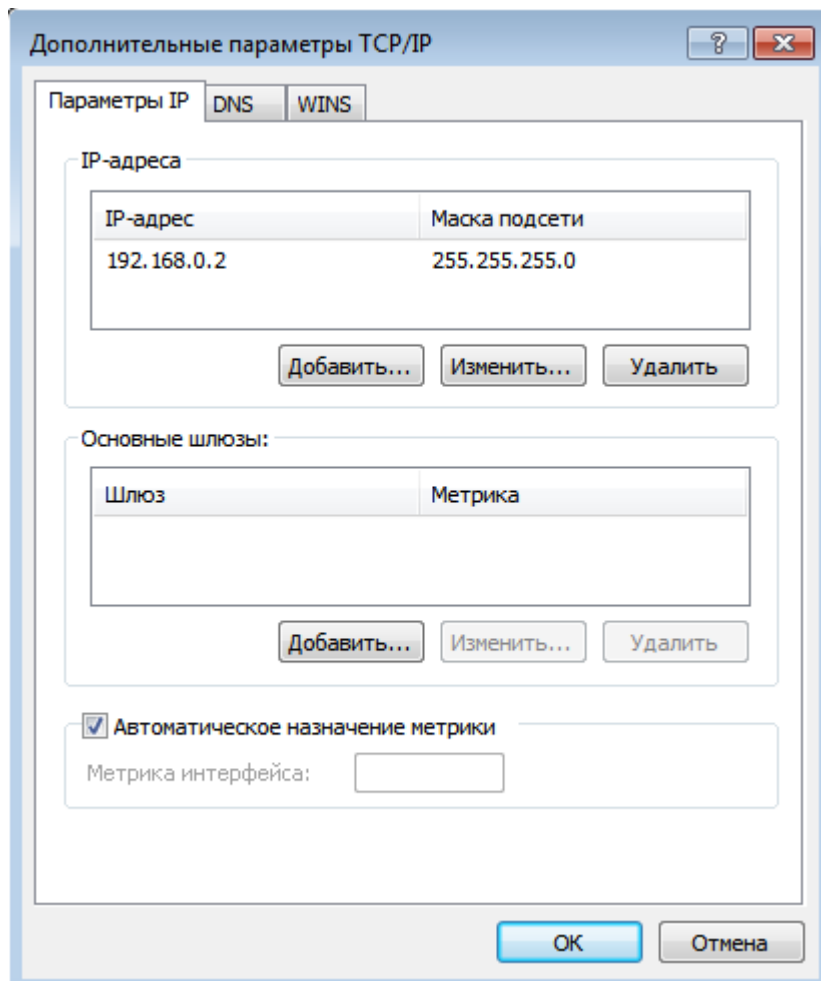
Статистика Ping для 192.168.0.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
C:\Users\win7Host1>
```

Пакеты доходят без потерь, значит компьютеры находятся в одной сети.

Так же имеются дополнительные настройки, во вкладке 'Дополнительно'. В данной вкладке есть 'Параметры IP' возможность задать список IP адресов и основных шлюзов, которые будут связаны с данным сетевым адаптером. Однако стоит помнить, что при задании нескольких адресов, должны быть заданы несколько основных шлюзов, чтобы была обеспечена возможность связи с компьютером по любому из списка заданных IP адресов. 'DNS' вкладка: задание DNS серверов по порядку



использования. 'WINS' вкладка: здесь можно задать имена для каждого компьютера, чтобы обращаться к каждому компьютеру не по IP адресу, а по WINS имени. Так же можно задать параметры NetBIOS, оставим её по умолчанию.

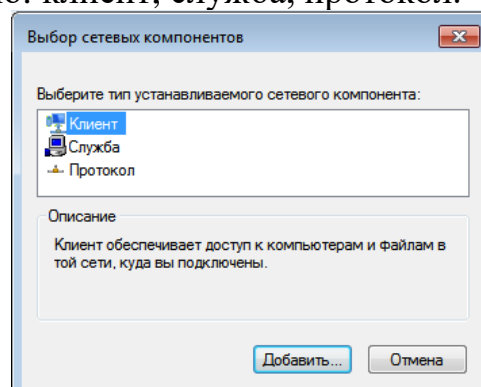


### **Компоненты, которые могут быть установлены дополнительно.**

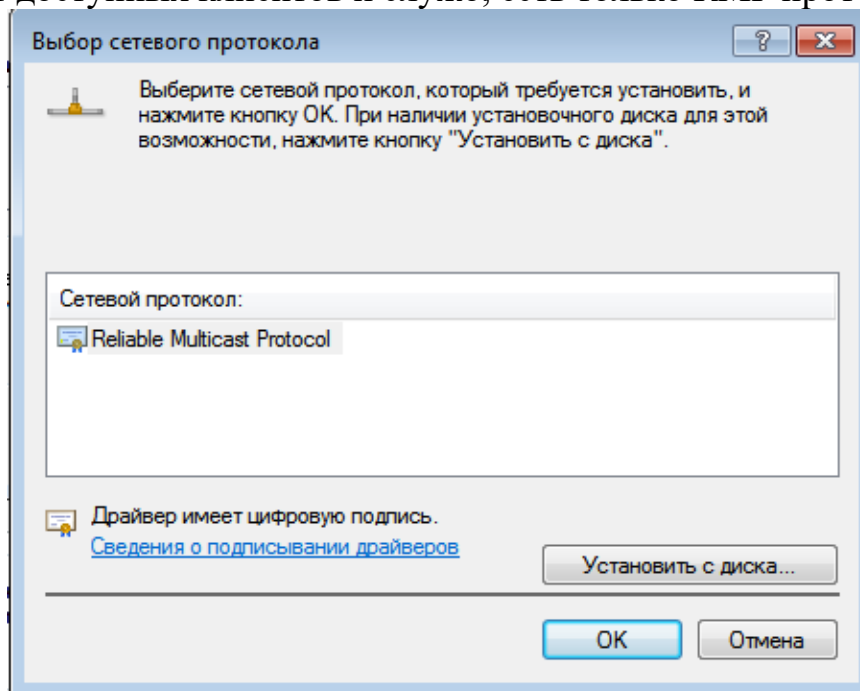
**Цель:** ознакомиться с компонентами, которые могут быть установлены дополнительно при базовой поставке используемой ОС.

**Выполнение работы:** помимо уже используемых компонентов могут быть установлены и дополнительные, которые могут идти как и в поставке используемой ОС, так и от сторонних разработчиков.

Сначала необходимо выбрать какой тип компонента мы хотим установить дополнительно: клиент, служба, протокол.



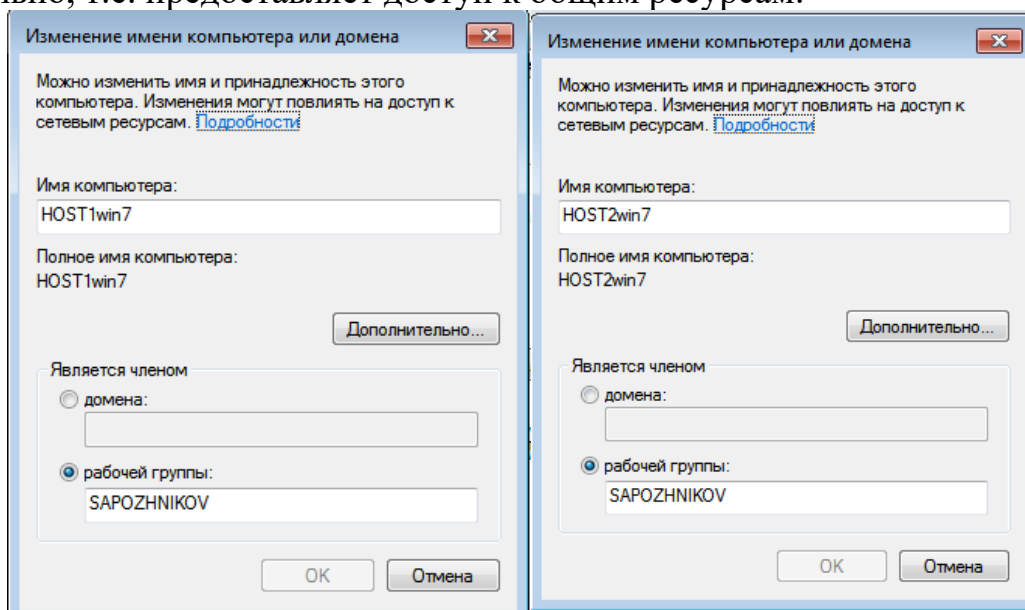
А затем сам компонент. К сожалению, в данной поставке Windows7 для установки нет доступных клиентов и служб, есть только RMP протокол.



RMP протокол (Надежный многоадресный протокол). Реализация протокола PGM (Pragmatic General Multicast или же сетевой протокол надёжной многоадресной передачи данных), повышающей надежность многоадресных рассылок.

### Назначение имени компьютера и рабочей группы

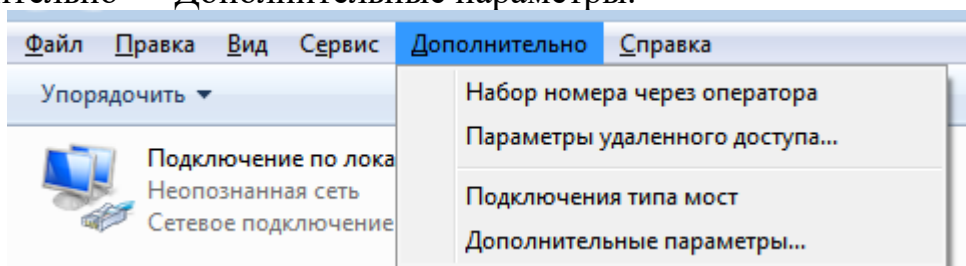
Для того, чтобы изменить имя компьютера и рабочей группы, достаточно в свойствах системы поменять имя группы и компьютера. Здесь указаны имена компьютеров и имя рабочей группы, в которую они входят. После данной настройки служба доступа к файлам функционирует правильно, т.е. предоставляет доступ к общим ресурсам.



## Настройки привязок и проверка работоспособности протоколов IPv4 и IPv6

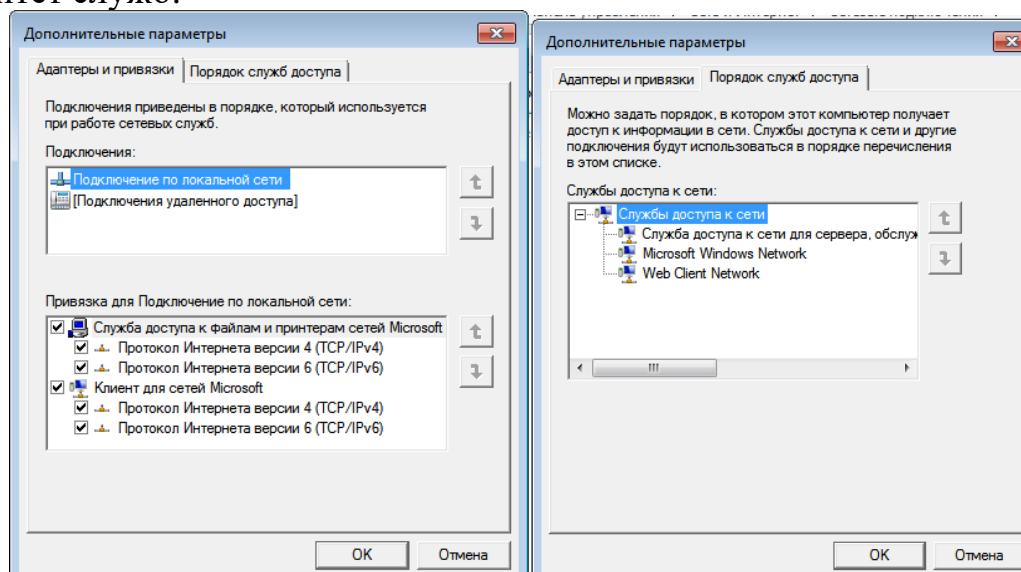
**Цель:** определить свойства привязок, меняя привязки и передавая файлы по сети. Определить какой из доступных протоколов используется при передаче и почему.

**Выполнение работы:** обычно настройки привязок скрыты от пользователей, чтобы их найти необходимо вызвать дополнительное меню сетевых подключений, что делается при помощи клавиши «alt». переходим Дополнительно → Дополнительные параметры.



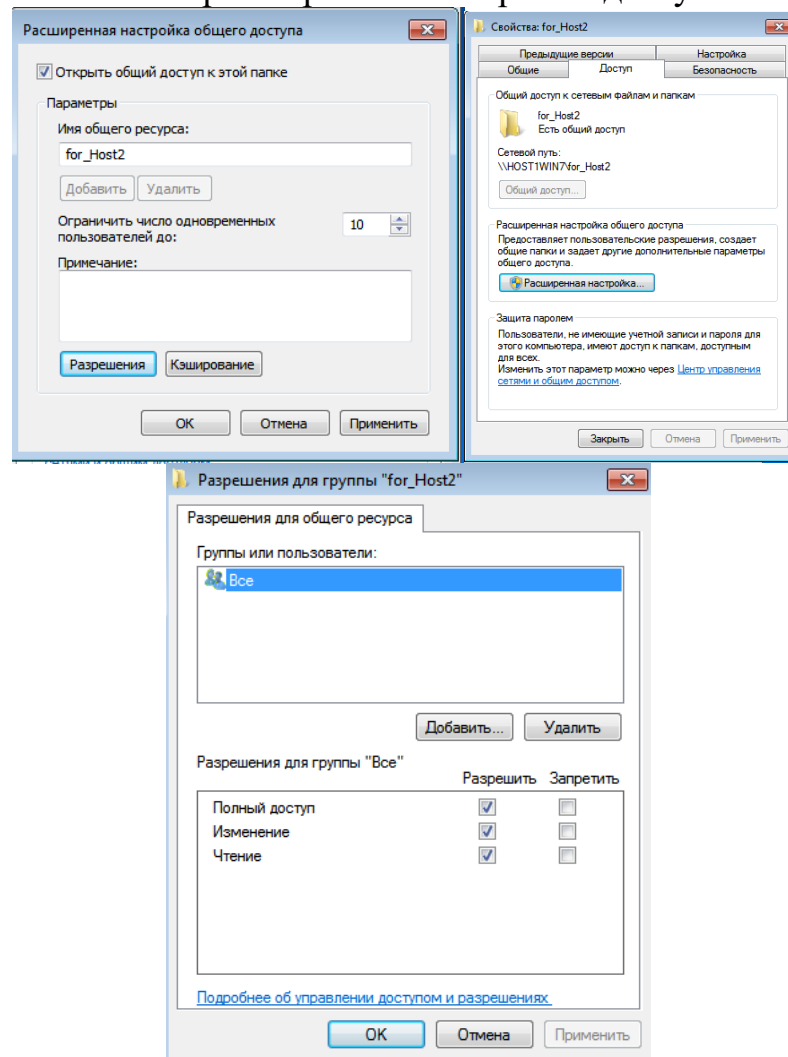
Привязки используются для выставления приоритета протоколов передачи данных. По умолчанию в данной поставке windows 7 приоритет отдается протоколу версии IPv4.

Во вкладке «Порядок служб доступа» так же можно изменить приоритет служб.

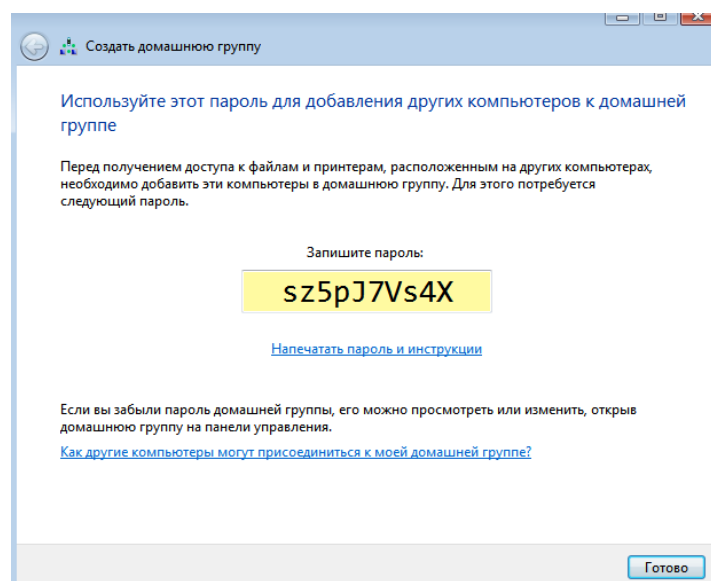


Проведем эксперимент по работе с общими файлами в сети, чтобы выявить задействованные протоколы.

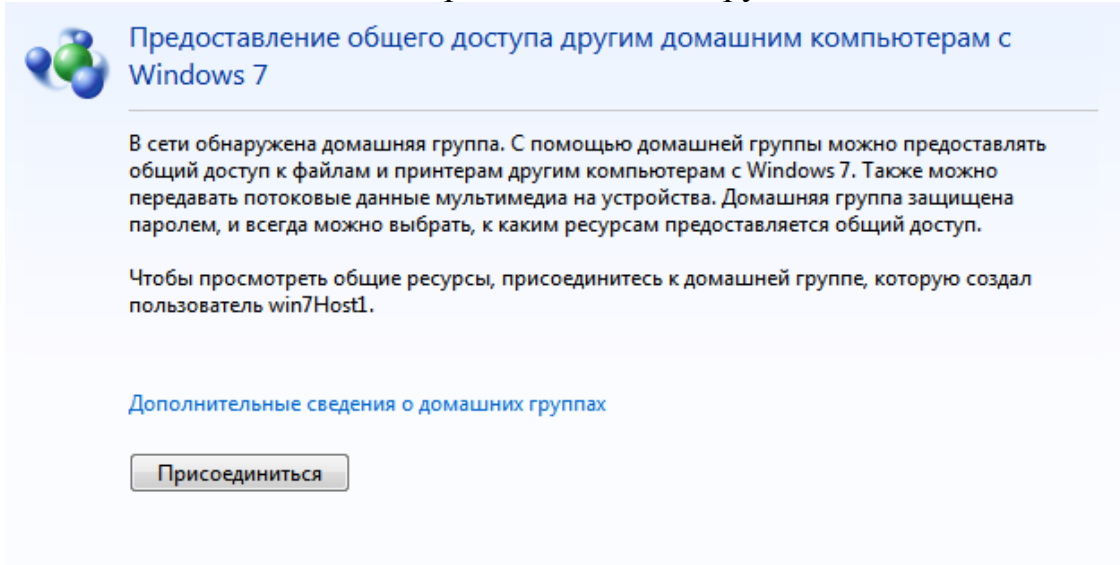
Создадим на машине HOST1win7 папку под названием “for\_Host2” и предоставим доступ к ней. Для этого перейдём к настройке «Доступ» в меню свойства папки. Изменим расширенные настройки доступа.



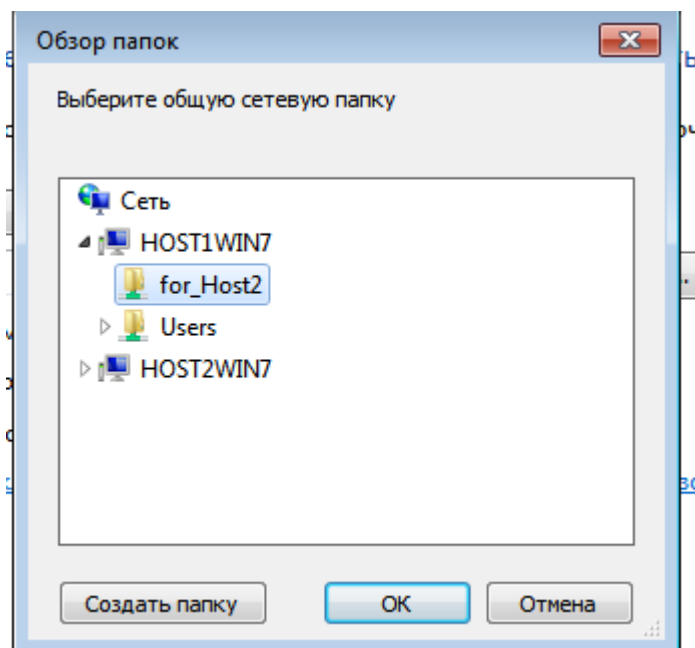
Создадим на машине HOST1win7 домашнюю группу для доступа к файлам.



На машине HOST2win7 присоединимся к группе.



На машине HOST2win7 добавим папку, к которой предоставили доступ. Для этого выберем пункт «Подключить сетевой диск» в меню Сети. Далее выберем букву, которой будет обозначаться диск и укажем путь к папке.



С машины HOST2win7 воспроизведем видео файл, находящийся в общей папке на машине HOST1win7.

Контроль трафика будем осуществлять при помощи утилиты командной строки netstat со следующими ключами:

- “-s” – Отображение статистики протокола
  - “-p <протокол>” – Отображение подключений для протокола, задаваемых этим параметром. Для работы с протоколом IPv4 необходимо указать IP, для IPv6 указываем IPv6
  - «-t интервал» – Отображение текущего подключения в состоянии offload. Повторный вывод статистики через указанный интервал в секундах
- Выполним проверку работы протокола IPv4



Отключим протокол IPv6 и проведем эксперимент еще раз.

```

Статистика IPv4
Получено пакетов = 20393
Получено ошибок в заголовках = 0
Получено ошибок в адресах = 26
Направлено датаграмм = 0
Получено неизвестных протоколов = 0
Отброшено полученных пакетов = 306
Доставлено полученных пакетов = 20698
Запросов на вывод = 5329
Отброшено маршрутов = 0
Отброшено выходных пакетов = 18
Выходных пакетов без маршрута = 4
Требуется сборка = 0
Успешная сборка = 0
Сбоев при сборке = 0
Успешно фрагментировано датаграмм = 0
Сбоев при фрагментации датаграмм = 0
Создано фрагментов = 0

```

```

Статистика IPv4
Получено пакетов = 20592
Получено ошибок в заголовках = 0
Получено ошибок в адресах = 26
Направлено датаграмм = 0
Получено неизвестных протоколов = 0
Отброшено полученных пакетов = 306
Доставлено полученных пакетов = 20897
Запросов на вывод = 5372
Отброшено маршрутов = 0
Отброшено выходных пакетов = 18
Выходных пакетов без маршрута = 4
Требуется сборка = 0
Успешная сборка = 0
Своев при сборке = 0
Успешно фрагментировано датаграмм = 0
Своев при фрагментации датаграмм = 0
Создано фрагментов = 0

```

```

Статистика IPv4
Получено пакетов = 22137
Получено ошибок в заголовках = 0
Получено ошибок в адресах = 26
Направлено датаграмм = 0
Получено неизвестных протоколов = 0
Отброшено полученных пакетов = 396
Доставлено полученных пакетов = 22442
Запросов на вывод = 5647
Отброшено маршрутов = 0
Отброшено выходных пакетов = 18
Выходных пакетов без маршрута = 4
Требуется сборка = 0
Успешная сборка = 0
Сбоев при сборке = 0
Успешно фрагментировано датаграмм = 0
Сбоев при фрагментации датаграмм = 0
Создано фрагментов = 0

```

```

Статистика IPv4

Получено пакетов = 22282
Получено ошибок в заголовках = 0
Получено ошибок в адресах = 26
Направлено датаграмм = 0
Получено неизвестных протоколов = 0
Отброшено полученных пакетов = 306
Доставлено полученных пакетов = 22587
Запросов на вывод = 5682
Отброшено маршрутов = 0
Отброшено выходных пакетов = 18
Выходных пакетов без маршрута = 4
Требуется сборка = 0
Успешная сборка = 0
Сбоев при сборке = 0
Успешно фрагментировано датаграмм = 0
Сбоев при фрагментации датаграмм = 0
Создано фрагментов = 0

```

Кол-во полученных пакетов по протоколу IPv4 заметно выросло.

```

Статистика IPv6

Получено пакетов                      = 1161735
Получено ошибок в заголовках          = 0
Получено ошибок в адресах            = 0
Направлено датаграмм                 = 0
Получено неизвестных протоколов       = 0
Отброшено полученных пакетов          = 805
Доставлено полученных пакетов         = 1163322
Запросов на вывод                     = 359712
Отброшено маршрутов                   = 0
Отброшено выходных пакетов            = 1
Выходных пакетов без маршрута         = 5
Требуется сборка                      = 0
Успешная сборка                      = 0
Сбоев при сборке                      = 0
Успешно фрагментировано датаграмми   = 0
Сбоев при фрагментации датаграмми    = 0
Созвано фрагментов                   = 0

```

```

Статистика IPv6

Получено пакетов                      = 1161735
Получено ошибок в заголовках         = 0
Получено ошибок в адресах           = 0
Направлено датаграмм                 = 0
Получено неизвестных протоколов      = 805
Отброшено полученных пакетов         = 1163322
Доставлено полученных пакетов        = 359712
Запросов на вывод                    = 0
Отброшено маршрутов                  = 0
Отброшено выходных пакетов           = 1
Выходных пакетов без маршрута        = 5
Требуется сборка                     = 0
Успешная сборка                     = 0
Сбоев при сборке                     = 0
Успешно фрагментировано датаграмм   = 0
Сбоев при фрагментации датаграмм    = 0
Создано фрагментов                   = 0

```

```

Статистика IPv6

Получено пакетов                = 1161735
Получено ошибок в заголовках    = 0
Получено ошибок в адресах      = 0
Направлено датаграмм           = 0
Получено неизвестных протоколов = 0
Отброшено полученных пакетов    = 805
Доставлено полученных пакетов   = 1163322
Запросов на вывод               = 359712
Отброшено маршрутов             = 0
Отброшено выходных пакетов      = 1
Выходных пакетов без маршрута   = 5
Требуется сборка                = 0
Успешная сборка                = 0
Сбоев при сборке                = 0
Успешно фрагментировано датаграмм = 0
Сбоев при фрагментации датаграмм = 0
Создано фрагментов             = 0

```

```

Статистика IPv6

Получено пакетов                = 1161735
Получено ошибок в заголовках    = 0
Получено ошибок в адресах      = 0
Направлено датаграмм            = 0
Получено неизвестных протоколов = 0
Отгружено полученных пакетов    = 805
Запущено полученных пакетов     = 1163322
Отгружено на вывод               = 359712
Отгружено маршрутов             = 1
Отгружено входящих пакетов      = 0
Выходящих пакетов без маршрута  = 5
Требуется сборка                 = 0
Успешная сборка                = 0
Сбоев при сборке                = 0
Успешно фрагментировано датаграмм = 0
Сбоев при фрагментации датаграмм = 0
Создано фрагментов              = 0

```

А кол-во полученных пакетов по протоколу IPv6 осталось неизменным, чего и следовало ожидать.

**Вывод:** Передача файлов внутри локальной сети происходит приоритетно по протоколу TCP/IP v6. Если протокол отключён в настройках сети, то передача будет происходить по протоколу TCP/IPv4.



Если попробовать отключить протокол IPv4 оставив только IPv6, то пропадет подключение по локальной сети. Для работы протокола IPv6 без IPv4 нужны подходящие условия и настройки, что выходит за рамки данной работы.

## 2. Изучение свойств сетевых ресурсов в Windows

**Компьютерная сеть** по определению представляет собой распределенную систему. Ее предназначение — совместная работа пользователей. Такая работа подразумевает доступ к сетевым ресурсам, как-то файлы и каталоги, принтеры и т.д. Для пользователя обращение к сетевым ресурсам должно быть прозрачным, т.е.:

- Удаленные ресурсы должны выглядеть так, словно они являются локальными и обращение к ним из приложений происходит единообразно.
- Клиенту должно быть безразлично, какая платформа используется в качестве сервера общего доступа.

При этом нужно учитывать и то, что не всякий пользователь должен иметь доступ к конкретному ресурсу, и не всякий ресурс должен быть доступен всем. Т.е. необходимо обеспечить возможности управления общим доступом, как на уровне пользователей, так и на уровне отдельных ресурсов.

Указанные возможности предоставляют специальные протоколы общего доступа.

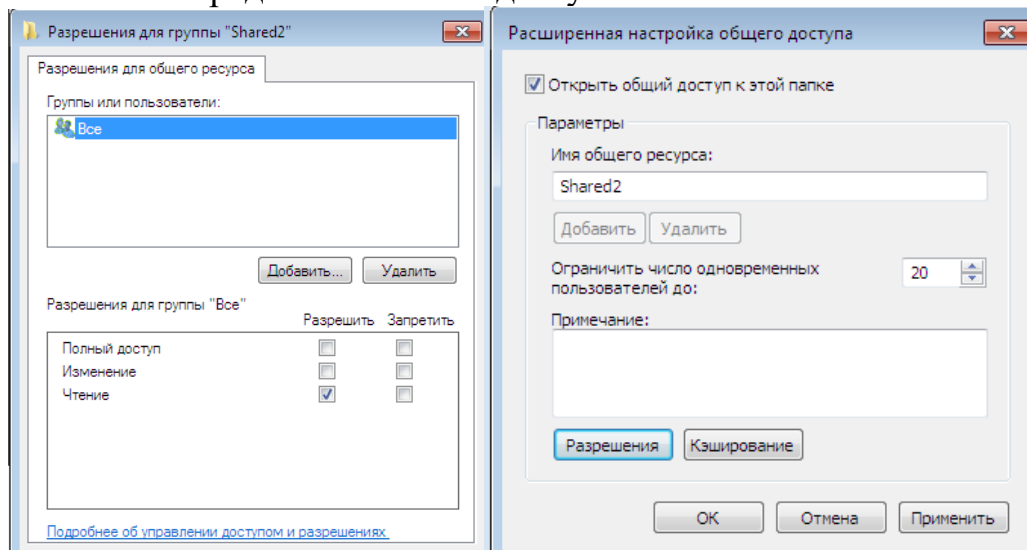
**Сетевой диск** — назначенный логический диск (папка), который служит для хранения «общих» файлов, доступных для всех пользователей, на других персональных компьютерах, включенных в общую локальную сеть.

**Сетевое окружение** — компонент операционной системы Windows, элемент рабочего стола. В графическом виде отображаются компьютеры локальной сети (если сеть присутствует).

### Способы подключения сетевых ресурсов

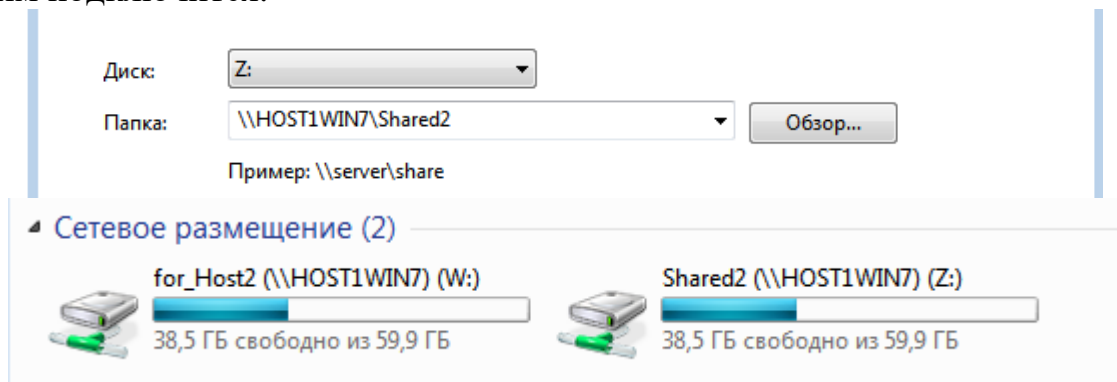
**Цель:** изучить способы подключения сетевых ресурсов.

**Выполнение работы:** на машине HOST1win7 создадим папку с именем Shared2 и предоставим к ней доступ только на чтение.

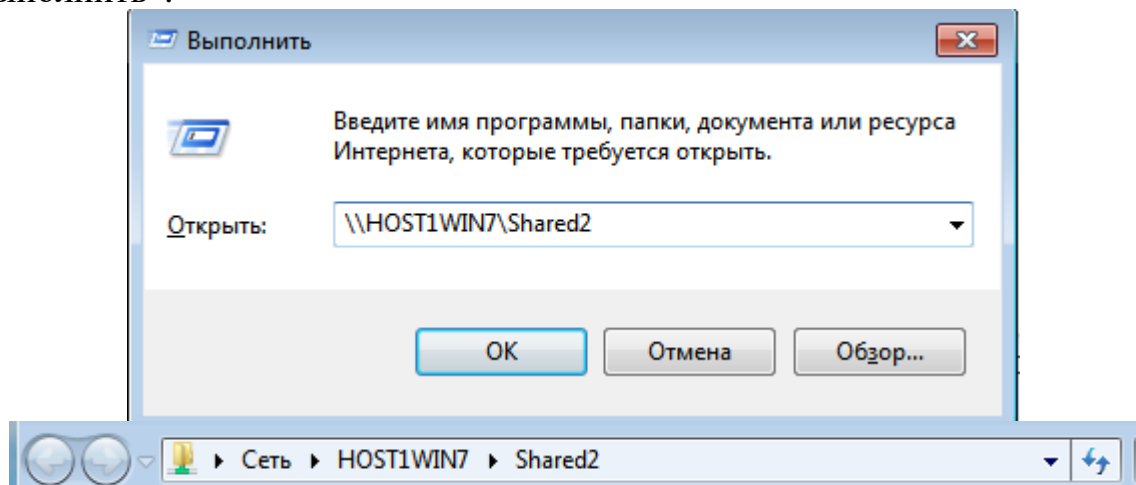




На машине HOST2win7 подключим сетевой диск воспользовавшись интерфейсом подключения сетевых дисков и укажем путь к папке к которой хотим подключиться.



Так же перейти к сетевому диску можно при помощи диалогового окна “Выполнить”:



Еще одним способом подключения сетевого является использование команды net командной оболочки cmd:

```
net use z: \\HOST1WIN7\Shared2
```

z – имя присваиваемое диску

\\HOST1WIN7\Shared2 - путь к сетевому ресурсу

```
C:\Users\win7Host2>net use z: \\HOST1WIN7\Shared2  
Команда выполнена успешно.
```

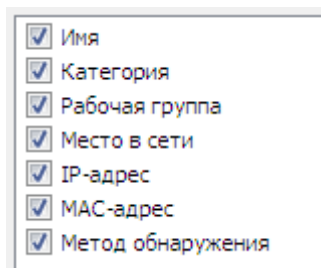
```
C:\Users\win7Host2>_
```



## Способы подключения сетевых ресурсов

**Цель:** научиться находить полную информацию о сетевом подключении и понимать её.

**Выполнение работы:** настроим отображение сети в режиме таблицы со всеми свойствами: имя, категория, рабочая группа, место в сети, IP-адрес, MAC-адрес, метод обнаружения.



Полученный список доступных сетевых устройств:

Имя	Категория	Рабочая группа	Место в сети	IP-адрес	MAC-адрес	Метод об...
Компьютер (2)						
HOST1WIN7	Компьютер	SAPOZHNIKOV	Неопознанная сеть	127.0.0.1		WSD
HOST2WIN7	Компьютер	SAPOZHNIKOV	Неопознанная сеть	192.168.0.2	00:0c:29:0a:c5:f4	WSD
Устройства мультимедиа (2)						
HOST1WIN7: win7Host1:	Устройства мультимедиа		Неопознанная сеть	127.0.0.1		SSDP
HOST2WIN7: win7Host2:	Устройства мультимедиа		Неопознанная сеть	192.168.0.2	00:0c:29:0a:c5:f4	SSDP

В сети обнаружено 4 устройства:

- 2 компьютера – 2 используемые виртуальные машины
- 2 устройства мультимедиа – DLNA сервер данных виртуальных машин (общие мультимедиа данные)

Компьютеры подключены к общей рабочей группе SAPOZHNIKOV.

Машина HOST2win7 имеет заданный ей ранее статический IP-адрес.

IP-адрес компьютера Sukhorukov-2-PC отображается как 127.0.0.1. Это стандартное, официально зарезервированное доменное имя для частных IP-адресов (в диапазоне 127.0.0.1 — 127.255.255.254). Этот адрес устанавливается на специальный сетевой интерфейс «внутренней петли» в сетевом протоколе TCP/IP.

Отличаются протоколы, которые были использованы для обнаружения устройств. Компьютеры были обнаружены по протоколу WSD, а устройства мультимедиа по протоколу SSDP.

**WSD (Web Services for Devices - веб-сервис для устройств).** WSD разработан для автоматического обнаружения, настройки и управления. WSD реализует функции Plug and Play для сетевых устройств. При этом каждый раз, при отправке задания, корректность IP-адреса проверяется. Это обеспечивает постоянную связь между клиентами сети. Протокол получает непрерывную информацию о том, в каком состоянии находится конкретное устройство.

**SSDP (Simple Service Discovery Protocol - Простой протокол обнаружения сервисов)** - сетевой протокол, основанный на наборе протоколов Интернета, служащий для объявления и обнаружения сетевых сервисов. SSDP позволяет обнаруживать сервисы, не требуя специальных механизмов статической конфигурации или действий со стороны серверов,

таких как DHCP или DNS. Данный протокол является основой протокола обнаружения Universal plug-and-play (UPnP) и предназначен для использования в домашних сетях и в малом бизнесе.

### Консоль «Управление компьютером»

**Цель:** научиться наблюдать за состоянием сеансов и сетевых ресурсов при помощи консоли управления компьютером

**Выполнение работы:** с помощью консоли «Управление компьютером» можно наблюдать состояние сеансов подключения и состояние общих ресурсов. Запустим консоль на машине HOST1win7.

В меню «Служебные программы», подменю «Общие папки» можно увидеть информацию об общих ресурсах, текущих подключениях и каталогах, к которым предоставлен доступ.

В меню «Общие ресурсы» отображается информация о каталогах, к которым может подключиться другой пользователь, у которого есть доступ. Также можно видеть какие каталоги сейчас используются и сколько подключений к ним осуществлено

Общий ресурс	Путь к папке	Тип	Количество клиентских подключений	Описание
ADMIN\$	C:\Windows	Windows	0	Удаленный Admin
CS\$	C:\	Windows	0	Стандартный общий р...
for_Host2	C:\for_Host2	Windows	1	Тест
IPC\$		Windows	0	Удаленный IPC
Shared2	C:\Shared2	Windows	1	
Users	C:\Users	Windows	1	

В меню «Сеансы» можно увидеть пользователей, которые в данный момент подключены к общим ресурсам. Отображается информация и компьютере, типе операционной системы, времени подключения.

Пользователь	Компьютер	Тип	Количество открытых файлов	Время подключения	Время простоя	Гость
HomeGroupUser\$	HOST2win7	Windows	4	01:39:29	00:50:43	Нет

В меню «Открытые файлы» отображаются файлы, которые сейчас используются другими пользователями.

Открытый файл	Пользователь	Тип	Блокир.	Режим открытия
C:\for_Host2\	HomeGroupUs...	Windows	0	Нет доступа
C:\Shared2\	HomeGroupUs...	Windows	0	Нет доступа
C:\Users\	HomeGroupUs...	Windows	0	Нет доступа
C:\Users\win7H...	HomeGroupUs...	Windows	0	Чтение

## Административные сетевые ресурсы

**Цель:** изучить свойства административных ресурсов и научиться работать с ними.

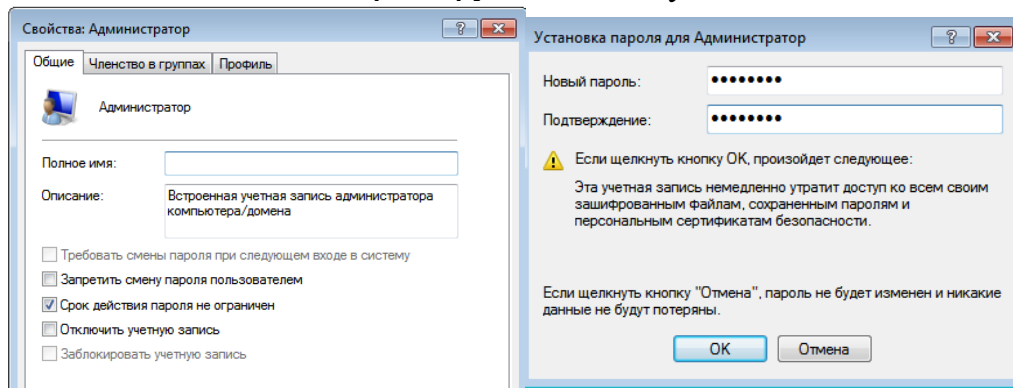
**Выполнение работы:** в меню общих сетевых ресурсов находятся 3 ресурса, заканчивающихся на \$: ADMIN\$, C\$, IPC\$. Это административные ресурсы

Общий ресурс	Путь к папке	Тип	Количество клиентских подключений	Описание
ADMIN\$	C:\Windows	Windows	0	Удаленный Admin
C\$	C:\	Windows	0	Стандартный общий р...
for_Host2	C:\for_Host2	Windows	1	Тест
IPC\$		Windows	0	Удаленный IPC
Shared2	C:\Shared2	Windows	1	
Users	C:\Users	Windows	1	

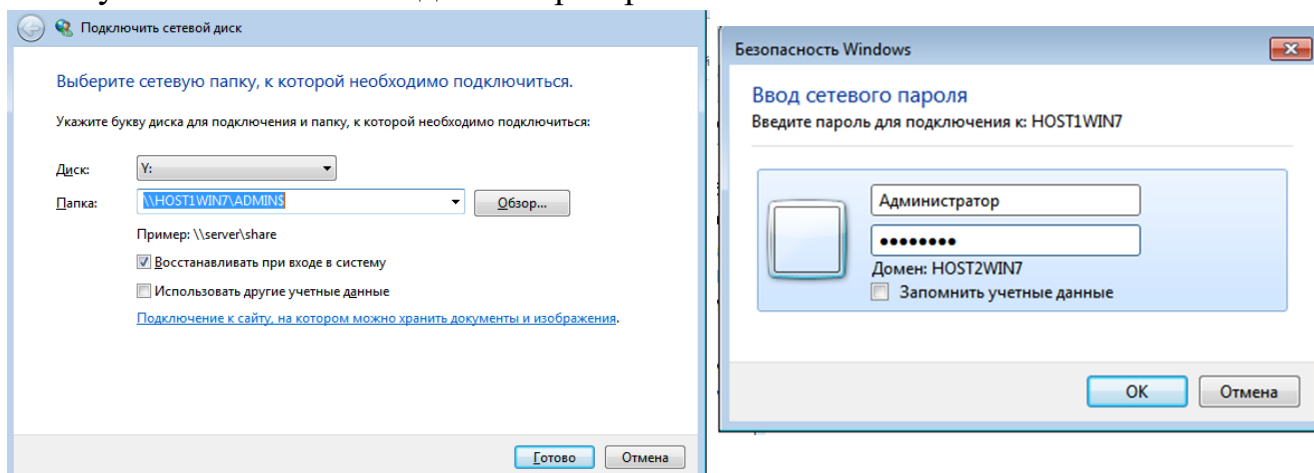
Свойства административных ресурсов:

- Создаются системой автоматически
- Скрыты и не участвуют в сетевом обнаружении
- Доступны только административным учетным записям

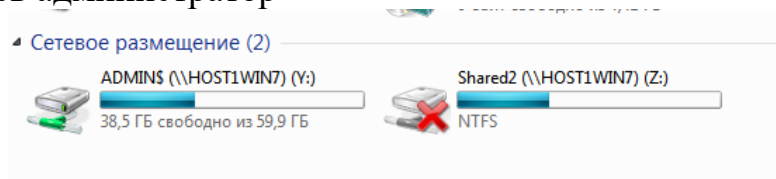
На машине HOST1win7 в консоли «Управление компьютером» перейдем в раздел «Локальные пользователи и группы». Для учетной записи «Администратор» установим пароль и уберем галочку «Отключить учетную запись». После чего перезагрузим машину HOST1win7



Теперь попробуем подключиться удаленно к административным ресурсам с машины HOST2win7. Подключимся к каталогу ADMIN\$ с помощью учётной записи «Администратор»



Удалось подключиться к административным ресурсам используя учётную запись администратор



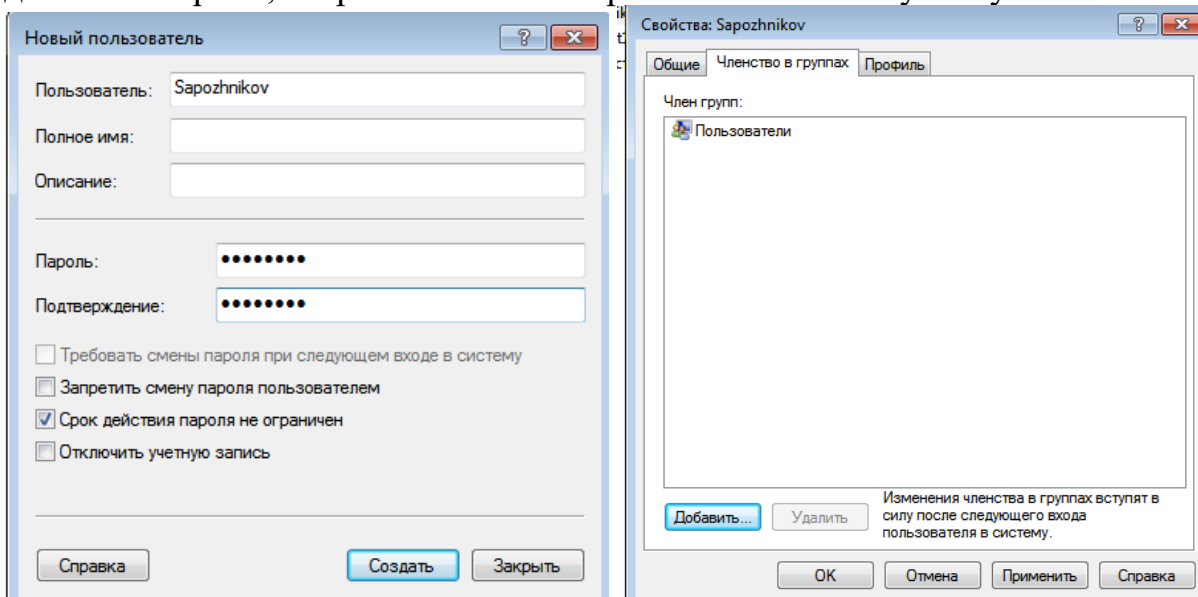
### 3. Изучение свойств сетевых ресурсов в Windows

#### Локальные пользователи

**Цель:** научиться создавать и редактировать учетные записи локальных профилей windows

**Выполнение работы:** на машине HOST1win7 создадим локального пользователя. Сделать это можно, перейдя в управление компьютером → локальные пользователи → нажать ПКМ на папку пользователи.

При создании пользователя (в дальнейшем в общих свойствах профиля) можно задать имя пользователя, описание, установить срок действия пароля, запретить менять пароль и отключить учетную запись.

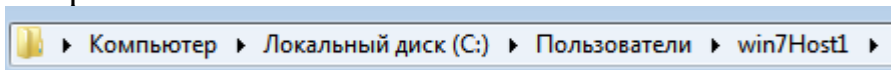


Во вкладке «Членство в группах» можно добавить пользователя к той или иной группе. По умолчанию всегда доступна группа пользователи. Члены данной группы не могут менять параметры ОС, данные других пользователей и не могут проводить установку ПО, которое просит доступ к системным файлам.

#### Структура домашнего каталога






























**Цель:** изучить структуры домашнего каталога

**Выполнение работы:** Домашний каталог находится по адресу <root>\Users\<username>. Для машины HOST1win7 путь выглядит следующим образом:



В домашнем каталоге содержатся главные элементы каталога, определяющие свойства и данные персональной учетной записи, и реестр. К

главным элементам так же относятся: Загрузки, Изображения, Мои документы, Мои видеозаписи, Мои документы, Рабочий стол и т.д. Реестр содержит раздел текущего пользователя, который хранится в файле NTUSER.DAT. Другие файлы реестра содержат «Логи» и снимки.

 AppData	08.04.2022 16:40	Папка с файлами	
 Application Data	08.04.2022 16:40	Папка с файлами	
 Cookies	08.04.2022 16:40	Папка с файлами	
 Local Settings	08.04.2022 16:40	Папка с файлами	
 NetHood	08.04.2022 16:40	Папка с файлами	
 PrintHood	08.04.2022 16:40	Папка с файлами	
 Recent	08.04.2022 16:40	Папка с файлами	
 SendTo	08.04.2022 16:40	Папка с файлами	
 Главное меню	08.04.2022 16:40	Папка с файлами	
 Загрузки	08.04.2022 16:40	Папка с файлами	
 Избранное	08.04.2022 16:40	Папка с файлами	
 Изображения	08.04.2022 16:40	Папка с файлами	
 Контакты	08.04.2022 16:40	Папка с файлами	
 Мои видеозаписи	08.04.2022 16:40	Папка с файлами	
 Мои документы	09.04.2022 18:52	Папка с файлами	
 Мои документы	08.04.2022 16:40	Папка с файлами	
 Моя музыка	08.04.2022 16:40	Папка с файлами	
 Поиски	08.04.2022 16:40	Папка с файлами	
 Рабочий стол	09.04.2022 18:42	Папка с файлами	
 Сохраненные игры	08.04.2022 16:40	Папка с файлами	
 Ссылки	08.04.2022 16:40	Папка с файлами	
 Шаблоны	08.04.2022 16:40	Папка с файлами	
 NTUSER.DAT	10.04.2022 17:01	Файл "DAT"	768 КБ
 ntuser.dat.LOG1	10.04.2022 17:01	Файл "LOG1"	256 КБ
 ntuser.dat.LOG2	08.04.2022 16:40	Файл "LOG2"	0 КБ
 NTUSER.DAT{016888bd-6c6f-11de-8d1d-...	08.04.2022 16:43	Файл "BLF"	64 КБ
 NTUSER.DAT{016888bd-6c6f-11de-8d1d-...	08.04.2022 16:43	Файл "REGTRANS...	512 КБ
 NTUSER.DAT{016888bd-6c6f-11de-8d1d-...	08.04.2022 16:43	Файл "REGTRANS...	512 КБ
 ntuser	08.04.2022 16:40	Параметры конф...	1 КБ

#### **4. Способы распределения полномочий администрирования при управлении пользователями и ресурсами в рабочей группе**

Существуют три характерных организации распределения полномочий администрирования:

- 1. Полностью децентрализованное управление.** При этом способе организации каждый пользователь владеет собственным компьютером, договаривается с остальными участниками сети о способе организации сетевых ресурсов и отвечает только за свою часть.
- 2. Централизованное управление.** Один администратор отвечает за устройство сети, имеет полномочия на всех узлах и делает всё строго по установленным правилам. Данный способ используется, если в силу каких-либо причин каждый пользователь не способен или не желает сам организовывать совместный доступ. Так же данный способ организации управления используется при более жёстких требованиях к устройству сети.
- 3. Распределение полномочий между группой администраторов.** Несколько человек отвечают за отдельные участки сети и устройства, подключенные к ним. Этот тип организации используется в больших сетях, когда один человек не может настроить и нести ответственность за всё сам.

Каждый тип организации имеет свои случаи и области применения. Например, в рамках школы более предпочтительно централизованное управление, в рамках небольшого офиса – децентрализованное, в рамках большого предприятия – распределённое.

Есть несколько способов организации доступа пользователей к сетевым ресурсам. К ним относятся:

- 1. Доступ с помощью персональной учётной записи каждого пользователя.** Режим в сети, когда у каждого человека есть на рабочем месте персональная учётная запись с секретным паролем. Данный вариант является основным при организации доступа к ресурсам.
- 2. Доступ с помощью одной общей учётной записи для всех пользователей, например, student.** Данный тип доступа используется для доступа к каталогам, когда нет необходимости идентифицировать человека. Если пользователь знает пароль общей учётной записи, то он может получить доступ к любому ресурсу, доступному все пользователям сети.
- 3. Доступ с помощью гостевой учётной записи «Гость».** Используется для анонимного входа, без аутентификации, когда нет

задач защиты данные. Используется встроенная учётная запись без пароля, которой предоставлен ограниченный круг ресурсов.

При подключении к сетевому ресурсу между клиентом и сервером создается сеанс, в котором клиент посылает запрос на установку соединения с аутентификаций учётной записи на сервере. Сервер принимает имя и пароль учётной записи, проверяет по базе локальных пользователей и отображает на локальную запись серверного узла. Далее от имени локального пользователя серверного узла строится сеанс и процесс для работы с файлами.

При данном подключении существуют два метода аутентификации:

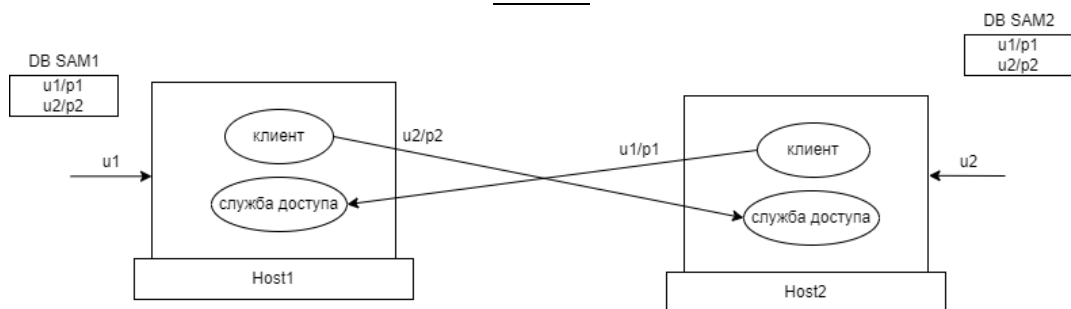
- 1. Сквозная аутентификация.** Клиентская служба при подключении к сети использует учетную запись локального входа. Сервер принимает запрос и пытается аутентифицировать по имени и паролю в базе локальных пользователей.
- 2. Явная аутентификация.** При подключении к серверу клиент указывает имя и пароль учётной записи, которая есть в локальных пользователях на сервере.

**Цель:** реализовать доступ пользователей к сетевым ресурсам с помощью персональной учетной записи.

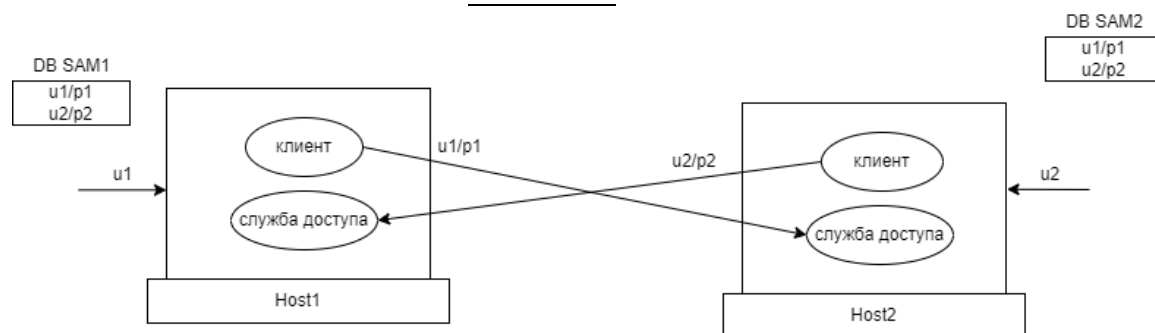
**Выполнение работы:**

При данном виде подключения существуют 2 метода аутентификации:

#### Явная



#### Сквозная



Сам доступ пользователей к сетевым ресурсам с помощью персональной учетной записи возможен лишь в небольших группах, т.к. каждый компьютер в сети должен иметь по учетной записи каждого



пользователя. При большем кол-ве поддерживать такой доступ становится проблематично, т.к. пользователи могут менять данные и пароли, а эти изменения придется вносить на каждую машину в сети.

Сквозная аутентификация является более удобной, т.к. нет необходимости помнить и указывать данные другой записи для входа. Так же удобно отследить изменения, вносимые пользователями, что сложнее сделать при явной аутентификации.

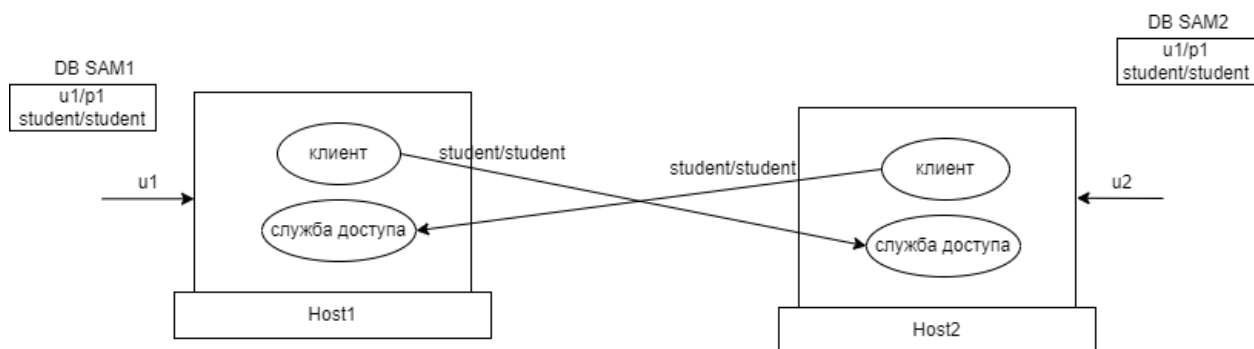
Рассмотрим проблему, связанную с явной аутентификацией.

Если на компьютере 1 работает, который содержит общие файлы, с общими данными работает пользователь А, а затем под пользователем А подключается ещё кто-то и вносит изменения, то идентифицировать был ли это сам пользователь А или кто-то под его записью становится сложнее (хотя это и можно сделать по адресу машины с которой были внесены изменения).

**Вывод:** данная схема подключений работоспособна только на маленькие группы, локальные группы.

**Цель:** реализовать доступ пользователей к сетевым ресурсам с помощью общей записи

**Выполнение работы:** для примера общей записи возьмем student с паролем student.



При данном виде подключения возможна только явная аутентификация под записью студента. Данная схема подключения работоспособна на группах больше, чем при подключении с персональной записью, т.к. необходимо поддерживать только одну запись – запись студента на каждой машине. Локальные записи используются только для локальной работы, а доступ к сетевым ресурсам происходит под записью студент.

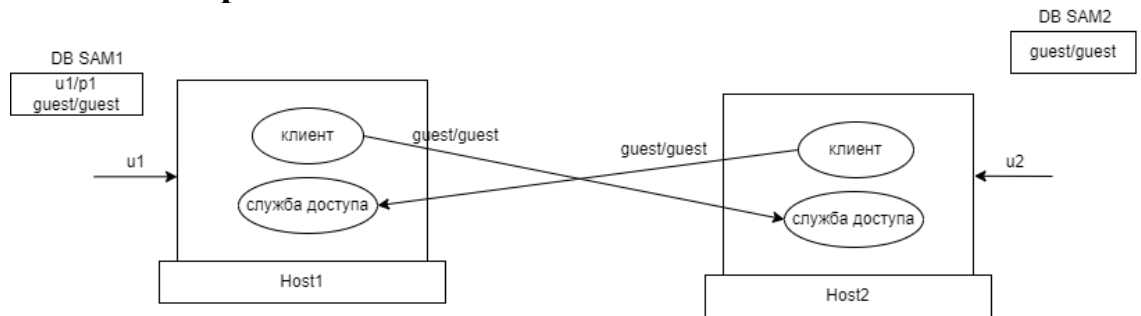
Если обращение к сетевым ресурсам происходит часто имеет смысл настроить сценарий входа, чтобы при обращении к общим ресурсам происходил автоматический вход в запись student. При такой настройке пользователь даже может и не знать, что обращается к сетевым ресурсам из под другой записи.

Явным минусом такого подхода является обезличенность при работе с сетевыми ресурсами. Из-за этого запись student требует особых настроек и ограничений.

**Вывод:** данная схема поддерживает большее кол-во машин, но также имеет недостатки в виде обезличенности и необходимости ограничений.

**Цель:** реализовать доступ пользователей к сетевым ресурсам с помощью записи гостя

**Выполнение работы:**



Данный способ чем-то похож на способ, указанный выше, только вместо данных записи student мы любое новое не аутентифицированное подключение отображаем как гостя.

Для работы данной системы необходимо открыть доступ гостю к общим ресурсам. Наверное, для гостей мы захотим иметь ещё больше ограничений, чем для student из варианта выше.

**Вывод:** данная схема скорее всего будет работоспособна в том случае если мы хотим только читать общие ресурсы.

Все из перечисленных видов подключений является локальными решениями, если нам необходимо работать с большим кол-ом машин, то необходимо переходить от группы к домену.

## 5. Роль реестра в конфигурации сети

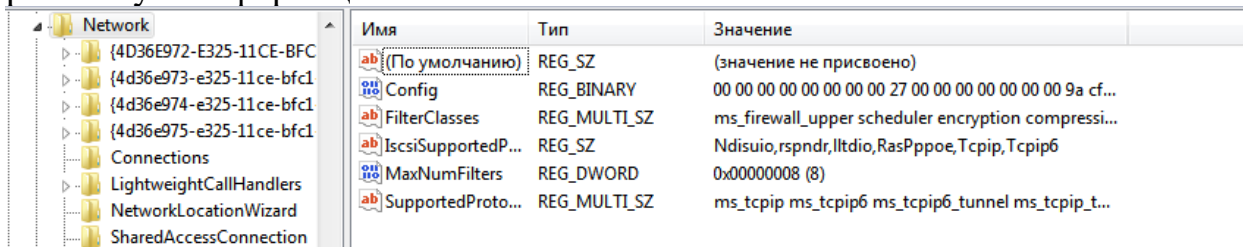
**Системный реестр, или реестр Windows** – это база данных для хранения настроек операционной системы, установленных программ, параметров пользователя и оборудования, кроме того, в реестре хранится информация об устройствах компьютера (конфигурации).

Реестр можно открывать с помощью интерфейса «Выполнить», используя команду `regedit`.

Как и другие системные настройки, конфигурация сети и профилей пользователей хранится в реестре. Например, ключ реестра

`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network`

содержит довольно много подключей, имена большей части которых представляют собой GUID (globally unique identifier) таких объектов, как сетевые подключения, службы, клиенты и т.д. Эти ключи содержат самую различную информацию об этих объектах:

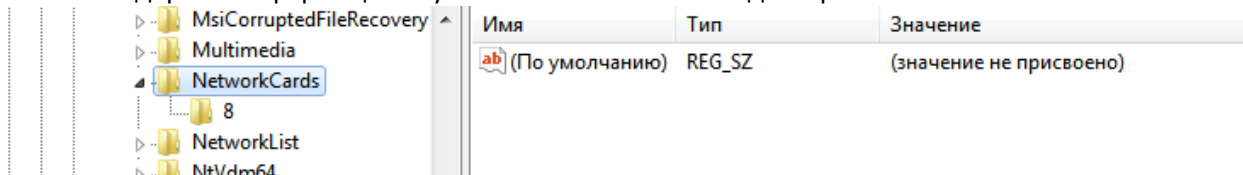


Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
Config	REG_BINARY	00 00 00 00 00 00 00 00 27 00 00 00 00 00 00 9a cf...
FilterClasses	REG_MULTI_SZ	ms_firewall_upper_scheduler_encryption_compressi...
IscsiSupportedP...	REG_SZ	Ndisuio, rspndr, lldio, RasPppoe, Tcpiip, Tcpiip6
MaxNumFilters	REG_DWORD	0x00000008 (8)
SupportedProto...	REG_MULTI_SZ	ms_tcpip ms_tcpip6 ms_tcpip6_tunnel ms_tcpip_t...

Ключ

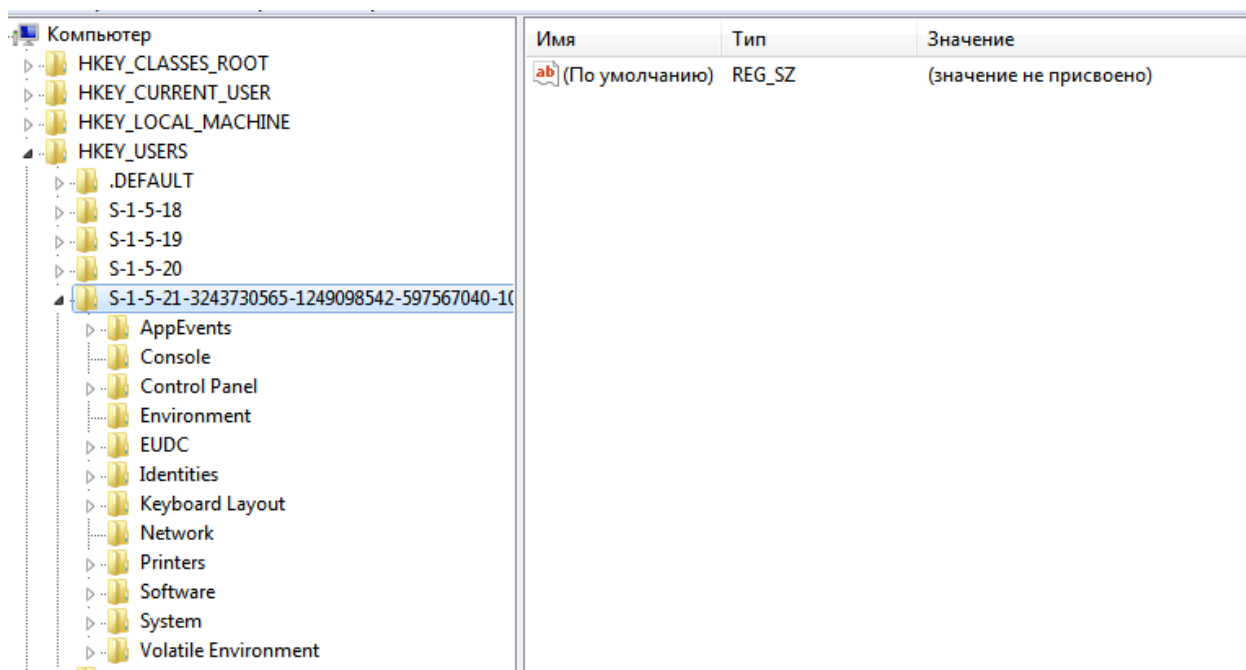
`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards`

содержит информацию о установленных сетевых адаптерах.



Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)

Раздел **HKEY\_USERS** содержит все активные загруженные профили пользователей компьютера. Внутри **HKEY\_USERS** находится все то, что связано с пользователем, идентифицируется по Security ID. Система генерирует уникальный SID для каждой учетной записи. Ключ Default содержит профиль по умолчанию, который копируется во вновь создаваемый профиль. Раздел **HKEY\_USERS** содержит список всех пользователей данного файла реестра. Необходимости в изменении информации этого раздела никогда не возникает, но его можно использовать в справочных целях.



Раздел HKEY\_CURRENT\_USER является корневым для данных конфигурации пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, параметры панели управления. Эти сведения сопоставлены с профилем пользователя. Раздел HKEY\_CURRENT\_USER содержит множество настроек программного обеспечения, которые содержат информацию о конфигурации рабочего стола и клавиатуры. Кроме того, этот раздел содержит информацию о параметрах меню Пуск. Все настройки, специфичные для пользователя, хранятся в этом разделе.

Список некоторых ключей, хранящихся в НКCU:

- **AppEvents** - Вложенные ключи, определяющие события, связанные с приложениями. звуковая реакция компьютера действия пользователя.
- **Environment** - Параметры, которые соответствуют настройке переменных среды для пользователя, на текущий момент зарегистрированного в системе.
- **Console** - Данный подключ, содержит вложенные ключи, которые определяют опции и размер окна для консоли.
- **ControlPanel** - Вложенные ключи соответствующих параметров, настройка которых осуществляется средствами Панели управления (Control Panel).
- **Printers** - Вложенные ключи, описывающие принтеры, установленные на компьютере и доступные зарегистрировавшемуся на текущий момент пользователю.



## 6. Возможности команды NET для конфигурирования и управления сетью

Утилита NET.EXE командной оболочки cmd.exe позволяет подключать и отключать сетевые диски, запускать и останавливать системные службы, добавлять и удалять пользователей, управлять совместно используемыми ресурсами, устанавливать системное время, отображать статистические и справочные данные об использовании ресурсов.

**Цель:** получить навыки работы с утилитой net.exe

**Выполнение работы:**

```
C:\Users\win7Host1>net /h
Синтаксис данной команды:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

Утилита имеет множество команд, многие из которых в свою очередь имеют дополнительные флаги. Рассмотрим лишь некоторые команды, которые кажутся более весомыми и соответствуют теме лабораторной работы.

net use - отобразить список сетевых дисков, подключенных на данном компьютере. В колонке "Локальный" отображается буква сетевого диска, а в колонке "Удаленный" - имя удаленного сетевого ресурса.

```
C:\Users\win7Host2>net use
Новые подключения будут запомнены.

Состояние   Локальный   Удаленный           Сеть
-----
OK           Z:          \\HOST1WIN7\ADMIN$  Microsoft Windows Network
OK           Z:          \\HOST1WIN7\IPC$    Microsoft Windows Network
Команда выполнена успешно.
```

net use Z: /delete – ОТКЛЮЧИТЬ сетевой диск

```
C:\Users\win7Host2>net use Z: /delete
Z: успешно удален.

C:\Users\win7Host2>net use
Новые подключения будут запомнены.

Состояние   Локальный   Удаленный           Сеть
-----
OK           Z:          \\HOST1WIN7\IPC$    Microsoft Windows Network
Команда выполнена успешно.
```

```
net use z: \\HOST1WIN7\Shared2
```

z – имя присеваемое диску

\\HOST1WIN7\Shared2 - путь к сетевому ресурсу

```
C:\Users\win7Host2>net use z: \\HOST1WIN7\Shared2
Команда выполнена успешно.
```

```
C:\Users\win7Host2>_
```

Сетевое размещение (2)



net share - позволяет выделить ресурсы системы для сетевого доступа. При запуске без других параметров, выводит информацию обо всех ресурсах данного компьютера, которые могут быть совместно использованы.

```
C:\Users\win7Host2>net share
```

Общее имя	Ресурс	Заметки
C\$	C:\	Стандартный общий ресурс
IPC\$		Удаленный IPC
ADMIN\$	C:\Windows	Удаленный Admin
Users	C:\Users	

Команда выполнена успешно.

net share <имя сетевого диска> - получить информацию о разделяемом ресурсе с указанным именем

```
C:\Users\win7Host1>net share shared2
Имя общего ресурса      Shared2
Путь                     C:\Shared2
Заметки
Макс. число пользователей  Не ограничен
Системная ошибка 5.

Отказано в доступе.
```

net share <имя каталога>=<путь> – добавить новый разделяемый каталог под указанным именем.

```
C:\Users\win7Host1>net share NEW_SHARE="C:\Share3"
NEW_SHARE успешно назначен общим.
```

`net accounts` - эта команда используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON). При использовании этой команды без указания параметров, выводятся текущие значения параметров, определяющих требования к паролям и входу в сеть, - время принудительного завершения сессии, минимальную длину пароля, максимальное и минимальное время действия пароля и его уникальность.

```
C:\Users\win7Host1>net accounts
Принудительный выход по истечении времени через:          Никогда
Минимальный срок действия пароля (дней):                  0
Максимальный срок действия пароля (дней):                  0
Минимальная длина пароля:                                  0
Хранение неповторяющихся паролей:                           Нет
Блокировка после ошибок ввода пароля:                       Никогда
Длительность блокировки (минут):                            30
Сброс счетчика блокировок через (минут):                    30
Роль компьютера:                                             РАБОЧАЯ СТАНЦИЯ
Команда выполнена успешно.
```

`net localgroup` - отобразить список групп пользователей данного компьютера

```
C:\Users\win7Host1>net localgroup
Псевдонимы для \\HOST1WIN7
-----
*HomeUsers
*IIS_IUSRS
*Администраторы
*Гости
*Криптографические операторы
*Операторы архива
*Операторы настройки сети
*Опытные пользователи
*Пользователи
*Пользователи DCOM
*Пользователи журналов производительности
*Пользователи системного монитора
*Пользователи удаленного рабочего стола
*Репликатор
*Читатели журнала событий
Команда выполнена успешно.
```

`Net config` - отображает информацию о настройке служб рабочей станции или службы сервера. Без параметров выводиться список настраиваемых служб

```
C:\Users\win7Host1>net config
Допускается управление следующими выполняющимися службами:

Сервер
Рабочая станция

Команда выполнена успешно.
```

`Net computer` - добавляет/удаляет компьютер из БД домена

```
C:\Users\win7Host1>net computer
Синтаксис данной команды:

NET COMPUTER
\\имя_компьютера [/ADD | /DEL]
```

Net view – отображает список общих ресурсов компьютера. Без параметров отображается список всех компьютеров в текущем домене или сети.

```
C:\Users\win7\Host1>net view
Имя сервера          Заметки
-----
\\HOST1WIN7
\\HOST2WIN7
Команда выполнена успешно.
```

## 7. Среда команды NETSH

**Цель:** получить навыки работы со служебной программой net.exe

**Выполнение работы:** служебная программа netsh (network shell) – наиболее полное и функциональное стандартное средство управления сетью с использованием командной строки в среде Windows

При запуске NETSH.EXE без параметров на экран выводится приглашение к вводу внутренних команд оболочки. Набор команд представляет собой многоуровневую структуру, позволяющую выполнять необходимые действия в выбранном контексте.

```
C:\Users\win7\Host1>netsh
netsh>help

Применимы следующие команды:

Команды в этом контексте:
?..          - Переход на один контекстный уровень вверх.
abort       - Отображение списка команд.
add         - Отмена изменений, сделанных в режиме работы вне сети.
advfirewall - Добавление элемента конфигурации в список элементов.
alias       - Изменения в контексте 'netsh advfirewall'.
branchcache - Добавление псевдонима.
bridge      - Изменения в контексте 'netsh branchcache'.
bye         - Изменения в контексте 'netsh bridge'.
commit      - Выход из программы.
delete      - Применение изменений, сделанных в автономном режиме.
dhcpcclient - Удаление элемента конфигурации из списка элементов.
dnscclient  - Изменения в контексте 'netsh dhcpcclient'.
dump        - Изменения в контексте 'netsh dnscclient'.
exec        - Отображение сценария конфигурации.
exit        - Запуск файла сценария.
firewall    - Выход из программы.
help        - Изменения в контексте 'netsh firewall'.
http        - Отображение списка команд.
interface  - Изменения в контексте 'netsh http'.
ipsec       - Изменения в контексте 'netsh interface'.
lan         - Изменения в контексте 'netsh ipsec'.
mbn         - Изменения в контексте 'netsh lan'.
namespace  - Изменения в контексте 'netsh mbn'.
nap         - Изменения в контексте 'netsh namespace'.
netio       - Изменения в контексте 'netsh nap'.
offline    - Изменения в контексте 'netsh netio'.
online      - Переход в режим работы вне сети.
p2p         - Переход в оперативный режим.
popd        - Изменения в контексте 'netsh p2p'.
pushd       - Получение контекста из стека.
quit        - Помещение текущего контекста в стек.
ras         - Выход из программы.
rpc         - Изменения в контексте 'netsh ras'.
set         - Изменения в контексте 'netsh rpc'.
show        - Обновление параметров конфигурации.
trace       - Отображение информации.
unalias     - Изменения в контексте 'netsh trace'.
wcn         - Удаление псевдонима.
wfp         - Изменения в контексте 'netsh wcn'.
winhttp     - Изменения в контексте 'netsh wfp'.
winsock     - Изменения в контексте 'netsh winhttp'.
wlan        - Изменения в контексте 'netsh winsock'.

Доступны следующие дочерние контексты:
advfirewall branchcache bridge dhcpcclient dnscclient firewall http interface ipsec lan mbn namespace nap netio p2p ras rpc trace wcn wfp winhttp winsock wlan

Чтобы получить справку по команде, введите эту команду,
затем пробел и "?"
```

При необходимости, можно выполнить нужное действие без использования интерактивного режима, указав в качестве параметров командной строки последовательный набор внутренних команд NETSH и необходимых параметров.



netsh interface ip show config – посмотреть сведения о работе протокола TCP/IP.

```
C:\Users\win7Host1>network interface ip show config
"network" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\Users\win7Host1>netsh interface ip show config

Настройка интерфейса "Подключение по локальной сети"
  DHCP включен:                Нет
  IP-адрес:                     192.168.0.1
  Префикс подсети:              192.168.0.0/24 <маска 255.255.255.0>

  Метрика интерфейса:          10
  DNS-серверы со статической настройкой: Нет
  Зарегистрировать с суффиксом: Только основной
  WINS-серверы со статической настройкой: Нет

Настройка интерфейса "Loopback Pseudo-Interface 1"
  DHCP включен:                Нет
  IP-адрес:                     127.0.0.1
  Префикс подсети:              127.0.0.0/8 <маска 255.0.0.0>
  Метрика интерфейса:          50
  DNS-серверы со статической настройкой: Нет
  Зарегистрировать с суффиксом: Только основной
  WINS-серверы со статической настройкой: Нет
```

netsh interface ip set address name="Подключение по локальной сети" source=static addr=192.168.0.3 mask=255.255.255.0 – сменить ip адрес.

name – имя сетевого подключения

source=static – статический IP-адрес.

addr – значение IP-адреса

mask – значение маски сети

```
C:\Windows\system32>netsh interface ip set address name="Подключение по локальной
сети" source=static addr=192.168.0.3 mask=255.255.255.0

C:\Windows\system32>netsh interface ip show config

Настройка интерфейса "Подключение по локальной сети"
  DHCP включен:                Нет
  IP-адрес:                     192.168.0.3
  Префикс подсети:              192.168.0.0/24 <маска 255.255.255.0>

  Метрика интерфейса:          10
  DNS-серверы со статической настройкой: Нет
  Зарегистрировать с суффиксом: Только основной
  WINS-серверы со статической настройкой: Нет

Настройка интерфейса "Loopback Pseudo-Interface 1"
  DHCP включен:                Нет
  IP-адрес:                     127.0.0.1
  Префикс подсети:              127.0.0.0/8 <маска 255.0.0.0>
  Метрика интерфейса:          50
  DNS-серверы со статической настройкой: Нет
  Зарегистрировать с суффиксом: Только основной
  WINS-серверы со статической настройкой: Нет
```

## 8. Восстановить исходную конфигурацию всех настроек

После выполнения лаборанткой работы все машины необходимо вернуть в исходное состояние: вернуть настройки протоколов, удалить сетевые диски и общедоступные каталоги, удалить созданных пользователей.

## **Вывод**

В данной работе были изучены основные сетевые свойства одноранговой ЛВС и утилиты операционной системы, предназначенные для детального конфигурирования ЛВС. Также были рассмотрены общие ресурсы, их свойства и доступ к ним с разных узлов с различной конфигурацией.

В этой работе были созданы некоторые профили, которые затем конфигурировались определенным образом для правильной работы сети для того, чтобы ЛВС можно было проще контролировать и конфигурировать в зависимости от задания. Также было произведено ознакомление с реестром, были рассмотрены свойства некоторых из ветвей реестра и приведены основные параметры.

В данной работе были рассмотрены утилиты для администраторов такие как: net и netsh. Данные утилиты позволяют облегчить работу администратора.