ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ЦЕНТР ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Гидравлика, гидропневмоавтоматика и тепловые процессы»

Лабораторный практикум
по дисциплине

«Сети ЭВМ»

Автор
Полешкин М.С.

Ростов-на-Дону, 2017

Аннотация

Практикум содержит содержат основные сведения по работе с локальными вычислительными сетями и направленны на получение практических навыков установки, настройки и эксплуатации сетей ЭВМ, а так же методами и работе с программами отладки в ОС MS Windows.

Пособие рекомендовано студентам 3 курса очной и заочной форм обучения направления 13.03.03 «Энергетическое машиностроение» и студентам других направлений, изучающим курсы по локальным компьютерным сетям.

Автор: Доцент, к.т.н. Полешкин М.С.

Рецензент: Доцент, к.т.н. Дымочкин Д.Д.

Содержание

ВВЕДЕНИЕ

В современную эпоху развития информационных технологий, все болью значимость приобретают информационные ресурсы. Вместе с получением, организацией и потреблением информации, становится задача передачи данных к потребителю, быстро, стабильно, безопасно и без потери качества.

Соединение компьютеров в виде локальных, региональных и в итоге глобальных сетей важная и актуальная задача. Создание компьютерных сетей вызвано потребностью совместного использования информации на удаленных друг от друга компьютерах. Основное назначение компьютерных сетей – совместное использование ресурсов и осуществление связи как внутри одной организации, так и за ее пределами. Разделяемыми ресурсами могут быть данные, приложения, периферийные устройства.

Компьютерная сеть – представляет комплекс распределенной компьютерной техники, оборудования, обвязки, соединенной между собой системой передачи данных и специализированного программного обеспечения.

В процессе обучения технологиям компьютерных сетей вызывает затруднения практическая часть исследования телекоммуникационных систем: построение топологии сети, настройка интерфейсов, взаимодействие сетевых протоколов. Причинами этому являются высокая стоимость оборудования, организация рабочих мест для учащихся, размещение сетевых устройств.

В связи с этим появилось программное обеспечение, позволяющее проводить моделирование телекоммуникационных систем. Благодаря симуляторам компьютерных сетей эксперименты в этой области можно проводить гораздо удобнее и экономнее, чем на реальном оборудовании.

Практическая работа № 1

Подготовка к подсоединению ПЭВМ к локальной компьютерной сети

1. Цель работы - приобретение практических знаний и навыков в выборе и установке сетевых адаптеров, монтажу и разделке сетевого кабеля, физическому присоединению ЭВМ к кабельной системе при создании локальной компьютерной сети по технологии Ethernet [1,3,4].

2. Теоретические основы.

Сетевой стандарт Ethernet был разработан в 1975-х г. в исследовательском центре корпорации Xerox, после чего доработан совместно DEC, Intel и XEROX (отсюда сокращение DIX) и впервые опубликован как 'BlueBookStandart' для Ethernet I в 1980 г. Этот стандарт получил дальнейшее развитие и в 1985 г. вышел новый – Ethernet II (известный также как DIX).

На основе стандарта Ethernet DIX был разработан стандарт IEEE 802.3, одобренный в 1985 году для стандартизации комитетом по LANIEEE (*Institute of Electrical and Electronics Engineers*). В зависимости от вида физической среды передачи данных стандарт IEEE 802.3 имеет модификации (число 10 вначале каждой обозначает скорость передачи данных 10 Мбит/сек):

- 10Base-5 (применяется коаксиальный кабель диаметром 0,5 дюйма – т.н. *толстый коаксиал* с волновым сопротивлением 50 Ом; максимальная длина сегмента сети без повторителей 500 м, считается бесперспективным).
- 10Base-2 (коаксиальный кабель диаметром 0,25 дюйма – т.н. *тонкий коаксиал,* волновое сопротивление 50 ом; максимальная длина сегмента сети без повторителей 185 м, считается бесперспективным).
- 10Base-T (кабель на основе неэкранированной витой пары – UTP, *Unshielded Twisted Pair*; физическая топология – звезда с концентратором в центре, максимальное расстояние между концентратором и конечным узлом – до 100 м).

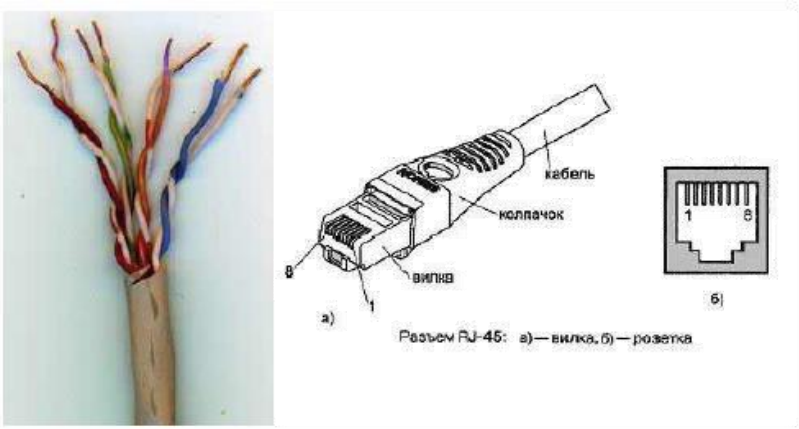
• 10Base-F (двухволоконный волоконно-оптический кабель, топология сети аналогична 10Base-T; варианты: FOIRL допускает расстояние до 1000м, 10Base-FL и 10Base-FB – до 2000 м).

В 1995 г. принят стандарт Fast Ethernet (IEEE 802.3u), в 1998 г. – Gigabit Ethernet (IEEE 802.3z), в 2002 г. - 10 Gigabit Ethernet (IEEE 802.3ae).

Ethernet и Fast Ethernet применяют один и тот же метод разделения среды передачи данных CSMA/CD (*Carrier Sense Multiple Access with Collision Detection,* метод коллективного доступа с опознав**а**нием несущей и обнаруж**е**нием коллизий).

Кабель UTP является наиболее дешевым (при обеспечении достаточной скорости передачи данных и простоте монтажа). UTP-кабели категории 1применяются в основном для телефонной разв**о**дки, UTP категории 3 служат для передачи как голоса так и данных при невысокой производительности (диапазон часто до 16 MHz). Для высокоскоростных протоколов при передаче на большие расстояния могут применяться (более дорогие) кабели UTP категорий 6 и 7 (экран вокруг каждой пары и вокруг всех жил соответственно, рабочие частоты до 300 и 600 MHz).

В настоящее время при создании локальных компьютерных сетей практически всегда (для технологий Ethernet, Fast Ethernet и GigabitEthernet) применяют кабель UTP категории 5 (8 попарно скрученных медных жил, активное сопротивление не более 9,4 ом на 100 м, полное волновое сопротивление100 ом на частоте 100 ÷120 MHz, затухание сигнала 0,8 ÷ 22 дБ на частотах от64 kHz до 100 MHz). Каждый провод кабеля UTP маркирован цветом (синий и белый с синими полосками, оранжевый и белый с оранжевыми полосками, зеленый и белый с зелеными полосками, коричневый и белый с коричневыми полосками по скрученным парам соответственно), для UTP-кабеля применяются разъемы RJ-45 (рис.1.1).



Разъем RJ-45: а) — вилка, б) — розетка

Рис.1.1 — Кабель UTPкатегории 5 (слева) и разъем RJ-45, показаны вилка (plug) и розетка (jack).

Отрезок UTP-кабеля (обычно не более 5 метров) со смонтированными него концах вилками RJ-45 называют Patchcord'ом. Вилки RJ-45 являются неразборными, при необходимости кабель просто отрезают около вилки и монтируют новую.

Для технологии Ethernet используется топология «звезда» с концентратором в центре, причем определены порт**ы** типа MDI (*Medium Depended Interface, разъем сетевого адаптера*) и MDIX (*MDI crossing, разъем портов сетевого концентратора*), см. рис.1.2. При соединении MDI-MDIX (подключение конечных узлов сети к портам активного оборудования) используется «прямой» кабель (рис.1.3а), при соединении MDI-MDI (непосредственное соединение адаптеров компьютеров, рис.1.2б) или MDIX-MDIX (соединение двух коммуникационных устройств) используют 'перекрестный' (*кр**о**ссовый*) кабель (рис.1.3б, причем на рис.1.2 'перекрестный' кабель обозначен символом **x**).

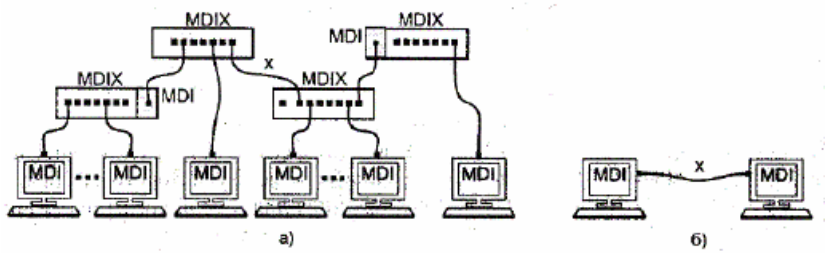


Рис.1.2 — Сеть 10BaseT/100BaseTX: а) – звезда; б) - двухточечное

В GigabitEthernet 1000BaseTX применяют только «прямые» кабели (в случае использования «перекрестного» кабеля скорость связи установится 100Mbit/сек). Впрочем, большинство современных коммутаторов используют функцию автоопределения типа кабеля (MDI или MDIX), что почти исключает вероятность ошибочного подсоединения.

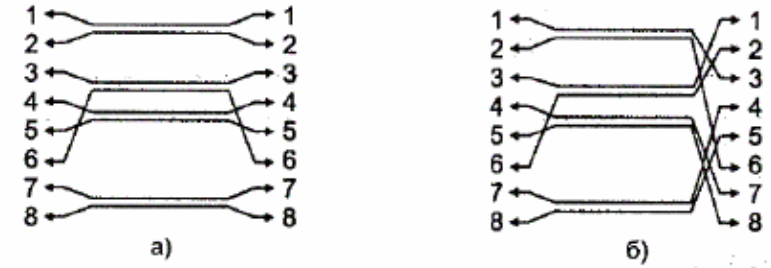


Рис.1.3 — Интерфейсные кабели Ethernet: а) «прямой», б) «перекрестный»

В 10- и 100-мегабитном Ethernet'е (10BaseT/100BaseTX) названия контактов содержат символы **TX** (*transmitter,* передатчик), **RX** (*receiver*, приемник)со знаками '+' и '–' и из 8 жил используется только половина (рис.1.3); для GigabitEthernet (1000BaseTX) используются все 8 медных жил (обмен данными по 4 парам жил в обоих направлениях одновременно), подсоединение соответствует табл.1.1.

Таблица 1.1. — Разъем RJ-45 адаптера Ethernet

Контакт	*10BaseT/100BaseTX*	*1000BaseTX*
1	TX_+	BI_D1+
2	TX_-	BI_D1-
3	RX_+	BI_D2+
4	не подсоединен	BI_D3+
5	не подсоединен	BI_D3-
6	RX_-	BI_D2-
7	не подсоединен	BI_D4+
8	не подсоединен	BI_D4-

Сигналы по каждой двухпроводной линии передаются дифференциальным способом (с противоположной полярностью по линиям '+' и '–'), причем входные и выходные цепи сетевых адаптеров имеют гальваническую развязку (рис.1.4).

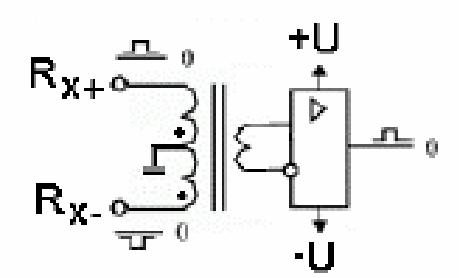


Рис.1.4 – Схема передачи сигнала по сетевому кабелю

Кабель UTP соединяется с вилкой RJ-45 без применения пайки. При монтаже вилки RJ-45 на кабель UTP-5 удаляют внешнюю оболочку кабеля на длинуполудюйма (12,5 мм, см. рис.1.5б); для удаления оболочки на специальном инструменте (рис.1.5а) имеется специальный нож и ограничитель длины удаляемой оболочки. Снимать изоляцию с жил не нужно, однако жилы следует расположить на плоскости в соответствие со схемой заделки (правое изображение из рис.1.5б и нижеследующие схемы).

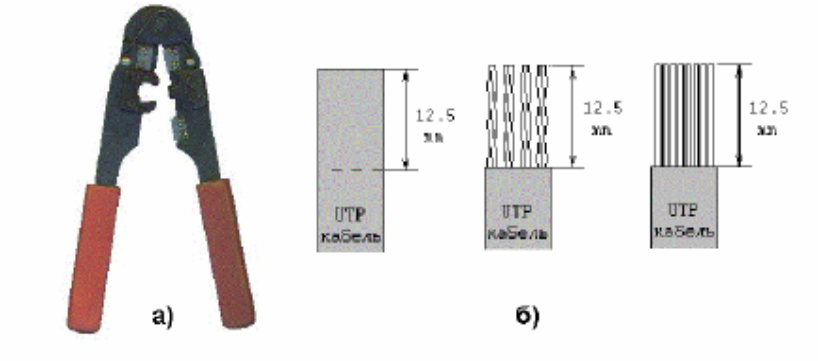


Рис.1.5 — Обжимной инструмент для разделки UTP-кабеля (а) и последовательность снятия внешней оболочки с сетевого кабеля (б).

Варианты заделки проводов (разводка проводов витой пары) показаны ниже (‘прямой’ кабель). В качестве схем заделки для 8-ми жильного кабеля равноценно можно использовать схему 568A или 568B (но одинаковую для данной сети, рекомендуется первая), для 4-х жильного кабеля используется схема согласно последнему из рисунков.

Таблица 1.2. — Стандарт EIA/TIA-586A соответствие контактов

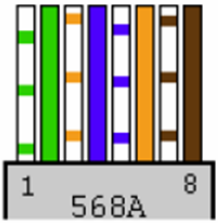
Стандарт EIA/TIA-568A (8-ми жильный ‘прямой’ кабель, схема 568A)		
Номера контактов	*Цвет оболочки провода*	
1	белый с зелеными полосками	
2	зеленый	
3	белый с оранжевыми полосками	
4	синий	
5	белый с синими полосками	
6	оранжевый	
7	белый с коричневыми полосками	
8	коричневый	

Таблица 1.3. — Стандарт EIA/TIA-568B соответствие контактов

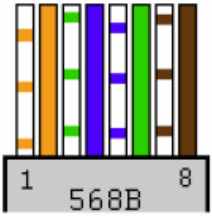
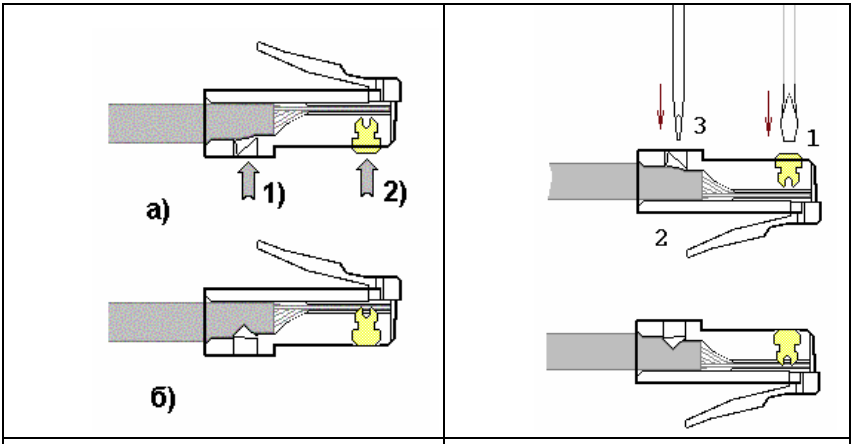
Стандарт EIA/TIA-568B, AT&T 258A (8-ми жильный 'прямой' кабель, схема 568B)		
Номер контактов	*Цвет оболочки провода*	
1	белый с оранжевыми полосками	
2	оранжевый	
3	белый с зелеными полосками	
4	синий	
5	белый с синими полосками	
6	зеленый	
7	белый с коричневыми полосками	
8	коричневый	

Таблица 1.4. — Стандарт 10Base-T/100Base-TX соответствие контактов

Стандарт 10Base-T/100Base-TX (4-х жильный 'прямой' кабель)		
Номер контактов	*Цвет оболочки провода*	
1	белый с оранжевыми полосками	
2	оранжевый	
3	белый с зелеными полосками	
6	синий	



а) б)

Рис.1.6 Последовательность установки разъема RJ-45

После описанного расположения жил на плоскости следует повернуть вилку контактами к себе (как на рис.1.7) и аккуратно надвинуть на кабель до упора, чтобы провода прошли под контактами. Вид вилки с кабелем внутри показан на рис.1.7в.

Последним действием является обж**и**м вилки. На обжимном инструменте имеется специальное гнездо, в которое вставляется вилка с проводами, после чего нажатием на ручки инструмента вилка обжимается (рис. 1.6 б). При этом контакты (на рис.показаны желтым цветом) будут утоплены внутрь корпуса, проре**е**жут изоляцию проводов и обеспечат надежный контакт с жил кабеля с контактами вилки. Фиксатор провода также должен быть утоплен в корпус (нажатие по стрелке 1 на рис.1.6 б).

В крайнем случае (если нет обжимного инструмента) можно обж**а**ть разъем RJ-45 тонкой отверткой (рис.1.6 б). При этом следует утопить все 8 шт.контактов (1) в корпус, а затем утопить и фиксатор провода (3).

Для непосредственного соединения двух компьютеров можно рекомендовать показанное ниже соединение («перекрестный» кабель), приведен вариант 4-х жильного т.н. «нуль-хабного кабеля».

Таблица 1.5 – Вариант монтажа 4-х жильного кабеля

'Cross-over' ('нуль-хабный') кабель (4-х жильный UTP-кабель)

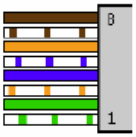
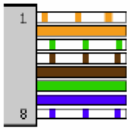
Одна сторона	*Цвет провода*	*Вторая сторона*
1	белый с оранж. полосками	3
2	оранжевый	6
3	белый с синими полосками	1
6	синий	2

Таблица 1.6 – Вариант монтажа 8-ми жильного кабеля (первый)

'Нуль-хабный кабель (8-ми жильный UTP-кабель)

Одна сторона	*Цвет провода*	*Вторая сторона*
1	белый с зелеными полосками	3
2	зеленый	6
3	белый с оранж. полосками	1
4	синий	4
5	белый с синими полосками	5
6	оранжевый	2
7	белый с коричн. полосками	7
8	коричневый	8

Таблица 1.7 – Вариант монтажа 8-ми жильного кабеля (второй)

'Нуль-хабный кабель по варианту 2 (8-ми жильный UTP-кабель)			
	Одна сторона	*Цвет провода*	*Вторая сторона*
	1	белый с зелеными полосками	3
	2	зеленый	6
	3	белый с оранж. полосками	1
	4	синий	7
	5	белый с синими полосками	8
	6	оранжевый	2
	7	белый с коричн. полосками	4
	8	коричневый	5
			

При тщательном выполнении монтажа вилок RJ-45 достигается устойчивый контакт между жилами кабеля и контактами вилки. Вредких случаях (выявляемых обычно уже наэтапе настройки программного обеспечения поддержки сети) требуется проверка физического соединения портов (выполняется с помощью *кабельных тестеров* или просто омметром). В состав ПО сетевых карт некоторых производителей включены утилиты (напр., *Virtual Cable Tester* фирмы 3Com), позволяющие определить место неуверенного контакта в кабеле или разъеме (используется явление отражения сигнала в кабеле).

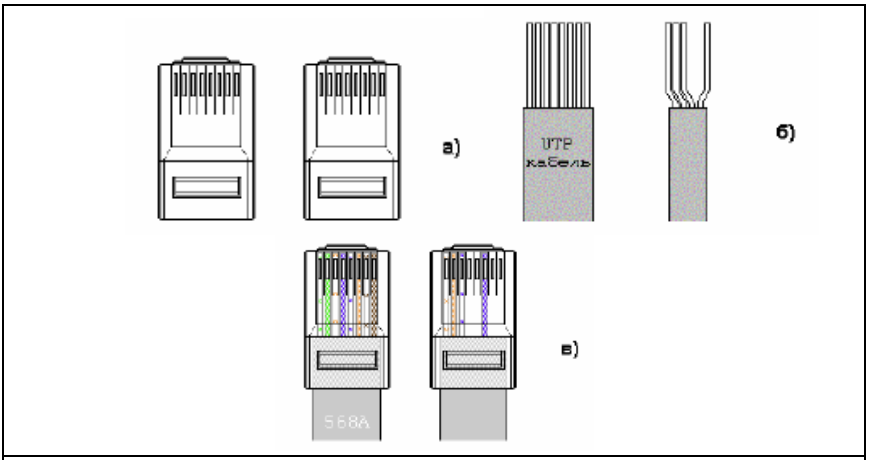


Рис. 1.7 — Расположение вилки RJ-45: а) контактами к себе б) разделанного кабеля UTP; в) вид вилки с кабелем внутри (слева – 8-ми жильный кабель, справа – 4-х жильный).

Сетевые кабели обычно соединяют сетевые карты или карты с сетевыми устройствами. На сетевых картах располагается отв**е**тная часть вилки RJ-45 – гнездо разъема RJ-45. Гнезда устанавливаются в сетевые карты, концентраторы, коммутаторы, трансиверы и другие устройства. Сам разъем представляет собой ряд из 8 пружинящих контактов и выемку для фиксатора вилки. Если смотреть на гнездо со стороны контактов (причем они располагаются сверху), то отсчет идет слева направо (рис.1.1,справа, б).

Розетка представляет собой гнездо (разъем)соединителя с каким-либо приспособлением для крепления кабеля и корпусом для удобства монтажа, обычно в комплекте поставляется и вилка. Внешняя розетка представляет собой небольшую пластмассовую коробочку, к которой прилагается шуруп и двухсторонняя наклейка для монтажа на стену. Такая розетка служит окончанием сетевого кабеля, обычно развод**и**мого по стене помещения и помещенного в коробах. Вт.н. розетках типа KRONE для монтажа кабеля UTP-5 используется специальная пластина с щелью, в которую заталкивается провод, при этом прорезается изоляция и жила кабеля входит в надежный контакт с пластиной (пайка не применяется). Для монтажа проводов имеется специальный инструмент, который помимо заталкивания проводов в щель обрезает лишние его куски. В любом случае настоятельно рекомендуется после тщательного замера длины кабеля оставить по 1 ÷ 1,5 м с каждой стороны для монтажа и укладки части кабеля в непосредственной близи от компьютера (или иного сетевого устройства).

Сетевая карта или сетевой адаптер (NIC, *Network Interface Card*) – плата расширения, обычно вставляемая в разъем системной (материнской) платы (*mainboard*) компьютера; современные системные платы обычно имеют_ встроенную сетевую карту [2,4]. Нарис.1.8 справа показана сетевая карта шины данных PCI: 1 - разъем под витую пару (RJ-45), 2 – светодиодный индикатор активности сети, 3 – шина данных PCI, 4 - панелька под микросхему BootROM (для загрузки операционной системы компьютера не слокального диска, а с сервера сети),5 - микросхема контроллера платы, 6 – коннектор подключения 3-х проводного кабеля к си-

стемной платедля «*пробужде**н**ия» по сети* (RemoteWakeUp; для этого передается специальный кадр MagicPacket, при приеме которого ПЭВМ «просыпается»).

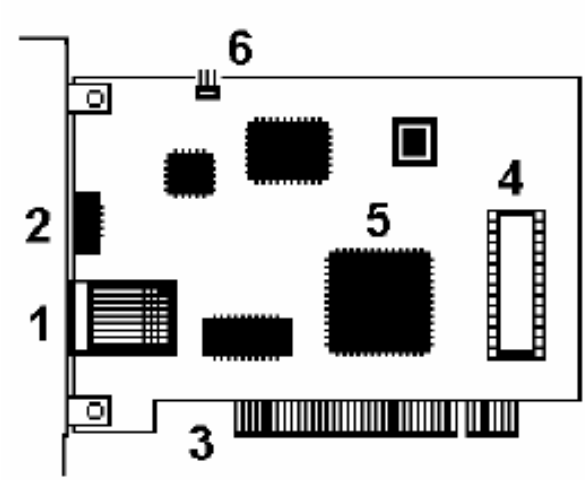


Рис.1.8 – Схема и состав основных элементов сетевого адаптера

Для определения точки назначения пакетов в сети Ethernet используется т.н. MAC (*Media Control Access*)-адрес. Это уникальный серийный номер, присваиваемый каждому сетевому устройству Ethernet для идентификации его в сети. MAC-адрес присваивается адаптеру его производителем, но может быть программно изменен. В обычном режиме работы сетевые адаптеры просматривают весь проходящий сетевой трафик и ищут в каждом пакете свой MAC-адрес. Если такой находится, то устройство (адаптер) обрабатывает этот пакет. MAC-адрес имеет длину 6 байт (48 бит) и обычно записывается в шестнадцатиричном виде, например, 12:34:56:78:90:AB (двоеточия между байтами делают число более читабельным).

Каждый производитель присваивает адреса из принадлежащего ему диапазона адресов. Первые три байта адреса определяют производителя, например:

- 00000CCisco
- 00000EFujitsu
- 00001D Cabletron
- 00004C NEC Corporation
- 000061 Gateway Communications
- 000062 Honeywell
- 0080C8 D-Link
- 00A024 3Com
- 00C049 USRobotics

Обычно все поддерживающие высшие скорости обмена данными сетевые адаптеры работают и на меньших скоростях (если комплементарное устройство не поддерживает данной скорости, но совместимо по стандарту Ethernet). Позволяет это *протокол согласования режимов* (autonegotiation, процесс основан на обмене специальными служебными импульсами), выполняемый каждый раз при установлении соединения после физического подключения (при инициализации портов) и позволяющий выбрать наиболее эффективный из режимов, доступных обоим портам.

Для обеспечения корректной работы каждой сетевой платы необходимо определить для нее *адрес ввода-вывода* (In/Outport) и *номер прерывания*(IRQ). Конфигурирование сетевой платы заключается в настройке ее на свободные адрес и прерывание, которые затем будут использоваться операционной системой. Адрес (In/Outport) и прерывание (IRQ) для каждой сетевой платы должно быть отличным от других устройств компьютера. Современные сетевые карты поддерживают технологию Plug-end-Play и автоматически выполняют эту операцию, при ручной установке полезной оказывается входящая в состав NT-совмест**и**мых версий Windows ут**и**лита WINMSD.EXE(*'Сведения о системе'*). Программная поддержка сетевых карт обеспечивается *драйверами*, для Windows возникновение проблем с драйверами маловероятно.

3. Порядок выполнения работы.

Студент получает задание на выполнение работы; типовыми заданиями являются:

• Смонтировать UTP-кабель для соединения ПЭВМ с сетевым устройством (концентратором, коммутатором).

• Смонтировать UTP-кабель для непосредственного соединения двух ПЭВМ.

Необходимое оборудование – IBM PC-совместимая ЭВМ, сетевая карта(для шины данных PCI) производительностью 10 ÷ 100 Mbit/сек с разъемомRJ-45, кабель UTP категории 5, вилки RJ-45, обжимной инструмент.

Монтаж предполагает разд**е**лку концов кабеля в соответствие с постулируемой целью (причем преподавателем может быть предложен как 4-х, так и8-ми жильный UTP-кабель), обжим вилки RJ-45, проверка контакта осуществляется кабельным тестером или омметром и проверяется преподавателем.

Сетевая карта устанавливается в свободный разъем на системной плате ПЭВМ (если на последней не имеется встроенного сетевого адаптера), при включении ПЭВМ конфигурируется технологией Plug-end-Play. Используемые адреса ввода-вывода (In/Outport) и номер прерывания (IRQ) фиксируются. Сетевой кабель подсоединяется к заданным устройствам, комплексная проверка сетевого соединения проводится с использованием специализированного программного обеспечения (см. описание работы 2 данного пособия).

Оформление отчета по работе.

В отчете указываются параметры выполняемого задания (соединяемые сетевые устройства, тип кабеля, число жил) и выбранные студентом схемы соединения. Приводятся последовательность расположения жил при монтаже карты (при возможности определить MAC-адрес и по нему фирму изготовителя) и поддерживаемые скорости обмена данными, тип шины данных. При возникновении проблем с контактом в кабеле следует привести схему проверки надежности контакта.

Контрольные вопросы

1. Какие сетевые кабели использует технология Ethernet? Что такое кабель UTP? В чем его достоинства и недостатки?
2. Что такое сетевые устройства MDI и MDIX? Для соединения каких устройств необходим ‘перекрестный’ (кроссированный) кабель?
3. Почему при монтаже вилки RJ-45 на кабель нет необходимости снимать изоляцию с отдельных жил кабеля?
4. Что такое «нуль-хабный» кабель и для каких целей он применяется?
5. Каким образом однозначно идентифицируются сетевые адаптеры? С какой целью введена возможность изменения MAC-адреса?
6. В чем суть протокола согласования режимов работы сетевых порт**о**в?
7. В чем заключается процесс конфигурирование сетевой платы? Какие пара метры при этом настраиваются?

Практическая работа №2.

Знакомство со средой Cisco Packet Tracer

1. **Цель работы:** познакомиться с интерфейсом симулятора, изучить режим реального времени, основные операции с устройствами.

2. **Выполнение работы.**

Запускаем среду Cisco Packet Tracer. При запуске программы открывается главное окно симулятора (см.рис.2.1).

2.1 Построение топологии сети

Создаем новую топологию сети, выбираем необходимые устройства и соединения.

Топология сети может быть сконфигурирована из различных устройств и связей. В данной лабораторной работе мы используем простые сетевые устройства: концентратор, коммутатор, конечные устройства (компьютеры).

Network Component Box содержит все представленное оборудование, с помощью которого можно построить сеть (см. рис.2.2). С помощью одного клика по каждой группе устройств и соединений можно отобразить различные их варианты, отличающиеся между собой (рис. 2.2, рис.2.3).

Рис. 2.1 Виды устройств и соединений в программе Cisco Packet Tracer

2.2 Построение топологии, добавление узлов

Для этого требуется сделать клик по конечным устройствам (рис. 2.2).

Рис. 2.2 Виды конечных устройств

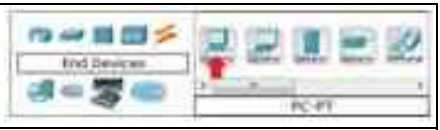


Рис. 2.3 Выбор конечного устройства

Один клик по выбранному устройству, для нашей работы это PC (рис. 2.3). Переместите курсор на рабочую область симулятора. Курсор должен превратиться в знак "+". Щелкните мышью в любом месте на области и выбранное вами устройство скопируется. Проделайте эту процедуру еще три раза, на рабочей области у вас будет 4 PC (рис. 4.4).

Рис. 2.4 – Вид рабочей области

Рис.2.5 – Вид рабочей области

2.3 Подключение к узлам концентратора и коммутатора.

Выберите группу устройств концентраторы (Hubs), из этой группы выберите первую модель (Hub-PT). Разместите концентратор между PC0 и PC1 (рис. 2.5).

Задача концентратора довольно проста: он повторяет пакет, принятый на одном порту на всех остальных портах.

Подключим PC0 к Hub0, выбрав сначала тип подключения. Для этого случая подойдет медный кабель с прямым подключением (рис. 2.6).

Рис. 2.6 Выбор соединения с прямым подключением

Для подключения PC0 к Hub0 выполните следующие действия (рис. 2.7):

1) Один раз щелкните мышью на PC0
2) Выберите тип интерфейса FastEthernet
3) Переместите курсор на Hub0
4) Нажмите на Hub0 один раз и выберите порт 0
5) Обратите внимание на зеленые индикаторы двух устройств на соединении, что значит, оба устройства готовы к работе.

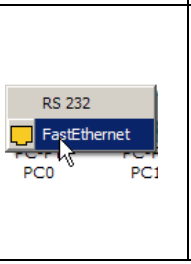
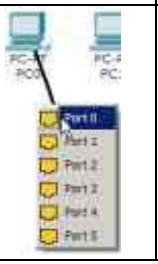
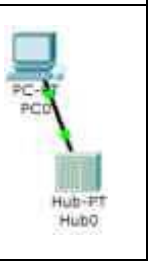
1)	2)	3)	4)	5)
				

Рис. 2.7 Подключение PC0 к Hub0 в программе Cisco Packet Tracer

Повторите описанные выше действия для подключения PC1 к Hub0, выбрав на концентраторе порт 1 (рис.2.8). Фактически номер порта значения не имеет, однако удобнее занимать порты последовательно.

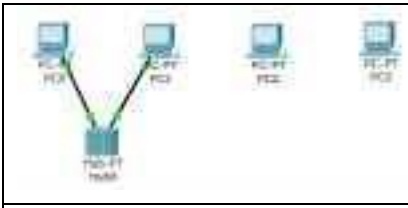
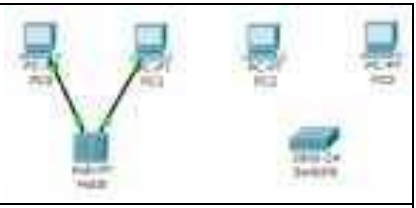
	

Рис. 2.8 Вид рабочей области	Рис. 2.9 Вид рабочей области

Далее размещаем на рабочей области симулятора коммутатор, например, модель 2950-24 (рис. 2.9). Описание семейства коммутаторов серии 2950 можно найти на сайте компании Cisco Systems. [Электронный ресурс]. URL: http://www.cisco.com/web/RU/products/hw/switches/ps628/ps627/index.html.

Коммутаторы - это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор передает пакеты на основании внутренней таблицы коммутации, следовательно, трафик идёт только на тот порт, которому он предназначается, а не повторяется на всех портах, в отличие от концентратора.

Подключим PC2 к Switch0, выбрав тип соединения медный кабель с прямым подключением.

Для подключения выполните следующие действия (рис. 2.10):

1) Щелкните мышью один раз на PC2
2) Выберите тип интерфейса FastEthernet
3) Переместите курсор на Switch0
4) Нажмите один раз на Switch0 и выберите FastEthernet0/1

5) и 6) Обратите внимание, что для правильной работы сети оба подключенных устройства должны быть готовы, о чем свидетельствуют зеленые индикаторы.

В отличие от подключения к концентратору, это может занять некоторое время.

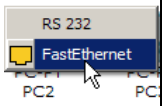
1)	2)	3)	4)	5)	6)
					

Рис. 2.10 Порядок подключения PC2 к Switch0 в программе Cisco Packet Tracer

Повторите описанные выше действия для подключения PC3 к Switch0, выбрав один из его интерфейсов FastEthernet 0/2 (рис. 2.11).

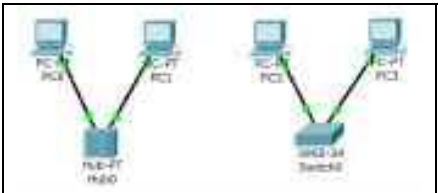
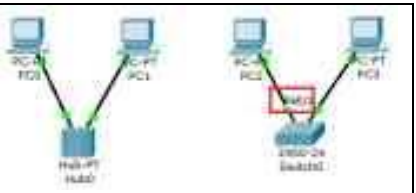
	

Рис. 2.11 Вид рабочей области	Рис. 2.12 Вид рабочей области

Если навести курсор на один из индикаторов, можно посмотреть, какой интерфейс задействован при данном подключении (рис. 2.12).

1. Настройка IP-адреса и маски подсети на хостах

Прежде чем мы сможем общаться между хостами по сети, нам нужно настроить IP-адреса и маски подсети на устройствах. Щелкните мышью один раз на PC0. Откроется окно свойств конечного узла на вкладке Physical (рис. 2.13).

Физический вид устройства мы менять не будем, поэтому сразу переходим к настройке в вкладке Config (рис. 2.14).

Рис. 2.13 Вкладка Physical конечного устройства (компьютера)

Именно здесь вы можете изменить название PC0 (например, ввести IP-адрес этого компьютера, чтобы не подглядывать его каждый раз в настройках). Кроме того, здесь вы можете указать IP-адрес шлюза, также известный как шлюз по умолчанию, и IP-адрес DNS-сервера. Мы обсудим это позже, но это будет IP-адрес локального маршрутизатора. Если вы хотите, вы можете ввести IP-адрес шлюза 192.168.1.1 и IP-адрес DNS-сервера 192.168.1.100, хотя он не будет использоваться в этой лабораторной работе.

Рис. 2.14 Вкладка Config конечного устройства (компьютера)

Кликните мышью на интерфейсе Fast Ethernet (рис. 2.15). Укажите IP-адрес компьютера 192.168.1.10. Нажмите на поле для ввода маски подсети, она определится автоматически 255.255.255.0.

Рис. 2.15 Настройки интерфейса конечного устройства

Информация автоматически сохраняется после ввода. Закройте окно настройки PC0 и повторите указанные выше действия для остальных узлов сети, используя информацию о IP-адресах и маски подсети, представленную в таблице 2.1.

Таблица 2.1 - Информация о IP-адресах и масок подсети

Хост	IP-адрес	Маска подсети
PC0	192.168.1.10	255.255.255.0
PC1	192.168.1.11	255.255.255.0
PC2	192.168.1.12	255.255.255.0
PC3	192.168.1.13	255.255.255.0

После настройки узлов рабочая область симулятора будет выглядеть следующим образом (рис. 2.16).

	
Рис. 2.16 Вид рабочей области	Рис. 2.17 Проверка настроек конечного устройства (компьютера)

Можно проверить введенную вами информацию на узлах (рис. 2.17). Для этого наведите курсор на интересующее вас устройство.

Если при построении сети какие-либо устройства или связи оказались лишними, их можно удалить при помощи инструмента Delete на боковой панели симулятора (Common Tools Bar). Для удаления нужно щелкнуть один раз на инструмент Delete, затем на элемент сети.

2. Соединение концентратора и коммутатора

Для подключения такого типа устройств, как коммутатора и концентратора, используется перекрестный кабель (рис. 2.18).

Рис. 2.18. Выбор соединения

Для подключения Hub0 к Switch0 выполните следующие действия:

1) Щелкните один раз на Hub0, выберите порт 2 (рис. 2.19).

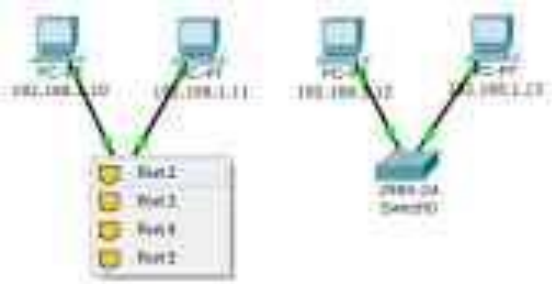


Рис. 2.19 Вид рабочей области

2) Переместите курсор на Switch0, щелкните на нем мышью и выберите интерфейс FastEthernet 0/3 (рис. 2.20).

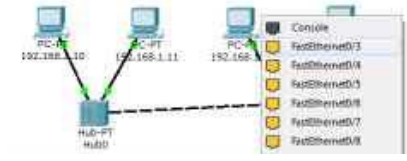


Рис. 2.20. Вид рабочей области

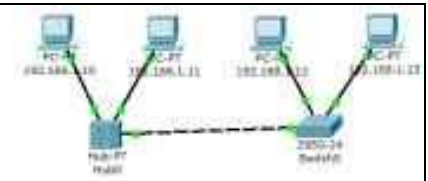


Рис. 2.21. Вид рабочей области

3) Когда оба устройства будут готовы к работе, индикаторы состояния станут зелеными (рис. 2.21).

3. Проверку работоспособности сети в режиме реального времени

Сформируем простой пакет ping-запроса для проверки работы сети, воспользовавшись Add Simple PDU. Нажмите один раз на Add Simple PDU.

Теперь нужно выбрать два узла: источник и приемник ping-запроса. Наведите курсор на PC0 (192.168.1.10) и щелкните на нем мышью (источник ping-запроса), затем переместите курсор на PC3 (192.168.1.13) (приемник ping-запроса) и кликните на нем.

Так как все интерфейсы и связи сети настроены правильно (о чем говорят зеленые индикаторы состояния), то ping-запрос должен пройти успешно. В окне управления пакетами User

Created Packet Window (см. рис. 2.22) появится соответствующая запись (рис. 2.22).

Рис. 4.22 Окно управления пакетами

Важно: измените IP-адрес 192.168.1.13 узла PC3 на IP-адрес 192.168.2.13, с той же маской подсети 255.255.255.0. Выполните ping-запрос от PC0 к PC3. Какой получился результат? Каковы причины?

Чтобы очистить список выполненных операций моделирования, необходимо удалить соответствующий сценарий симуляции. Нажмите на кнопку Delete на панели User Created Packet Window (рис. 2.23). Все записи сценария удалятся.

Рис. 2.23 Окно управления пакетами

4. Сохранение созданной топологии

Выберите в Menu Bar вкладку File, далее Save as. Выберите соответствующую директорию. Все файлы симулятора Cisco Packet Tracer имеют расширение .pkt.

5. Построение топологии сети, состоящей из двух подсетей

В результате первой работы мы изучили основные операции с устройствами. Для подготовки к выполнению следующей

лабораторной работы у нас есть соответствующие знания и навыки для построения топологии сети следующего вида (рис. 2.24):

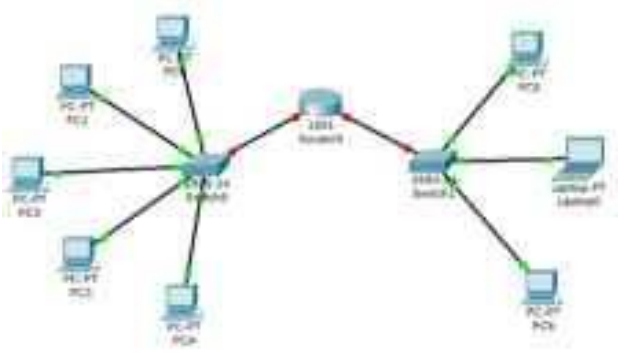


Рис. 2.24. Топология сети для лабораторной работы №2

Созданной топологии нужно добавить в рабочую область симулятора конечные узлы, два коммутатора и маршрутизатор. При добавлении маршрутизатора выберите модель 1841, т.к. она имеет два интерфейса. Описание маршрутизаторов серии 1841 можно найти на сайте компании Cisco Systems. [Электронный ресурс]. URL: http://www.cisco.com /en/US/products/ps5875/index.html. При соединении устройств между собой воспользуйтесь медным кабелем с прямым подключением.

Контрольные вопросы

1. Какие типы топологий сети существуют?
2. Создание топологии сети в программе Cisco Packet Tracer, особенности моделирования.
3. Как осуществляется подключение к конечным узлам сетевых устройств?
4. В чем заключается настройка IP-адресов и масок сети на узлах?
5. Как осуществляется проверка работы сети в режиме реального времени?

Практическая работа №3.

Протоколы ARP и ICMP (программы ping и tracert)

1. **Цель работы:** изучить режим симуляции Cisco Packet Tracer, протоколы ARP и ICMP на примере программ ping и tracert.

2. **Краткие теоретические сведения.**

Протокол ARP. Для определения физического адреса по IP-адресу используется протокол разрешения адреса Address Resolution Protocol (ARP). Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети с возможностью широковещательного доступа одновременно ко всем узлам сети[1]. Протокол ARP позволяет динамически определить MAC-адрес по IP-адресу. MAC-адрес – это уникальный серийный номер, присваиваемый каждому сетевому устройству для идентификации его в сети, так же называется физическим или аппаратным адресом. Протокол локальной сети, поддерживаемый в лабораторной работе – Ethernet. В Ethernet сетях, использующих стек TCP/IP, сетевой интерфейс имеет физический адрес длиной в 48 бит. Кадры, которыми обмениваются на канальном уровне, должны содержать аппаратный адрес сетевого интерфейса. Однако TCP/IP использует собственную схему адресации: 32-битные IP-адреса. Значение IP-адреса приемника недостаточно, чтобы отправить дейтаграмму этому хосту. Драйвер Ethernet должен знать MAC-адрес интерфейса назначения, чтобы послать туда данные.

В задачу ARP входит обеспечение динамического соответствия между 32-битными IP-адресами и 48-битными MAC-адресами, используемыми различными сетевыми технологиями. Протокол ARP работает в пределах одной подсети и автоматически запускается, когда возникает необходимость преобразования IP-адреса в аппаратный адрес. [2].

Рис. 3.1 – ARP-запрос и ARP-ответ

Работа протокола ARP поясняется на рис. 3.1. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

Для того чтобы уменьшить количество посылаемых запросов ARP, каждое устройство в сети, использующее протокол ARP, должно иметь специальную буферную память. В ней хранятся пары адресов (IP-адрес, физический адрес) устройств в сети. Всякий раз, когда устройство получает ARP-ответ, оно сохраняет в буферной памяти соответствующую пару. Если адрес есть в списке пар, то нет необходимости посылать ARP-запрос. Эта буферная память называется ARP-таблицей.

В ARP-таблице могут содержаться как статические, так и динамические записи. Динамические записи добавляются и удаляются автоматически, статические заносятся вручную.

Так как большинство устройств в сети поддерживает динамическое разрешение адресов, то администратору, как правило, нет необходимости вручную указывать записи протокола ARP в таблице адресов.

Каждая запись в ARP-таблице имеет свое время жизни. Политики очистки ARP-таблицы продиктованы используемой операционной системой. При добавлении записи для нее активируется таймер.

Сообщения протокола ARP при передаче по сети инкапсулируются в поле данных кадра. Они не содержат IP-заголовка. В отличие от сообщений большинства протоколов, сообщения ARP не имеют фиксированного формата заголовка. Это объясняется тем, что протокол был разработан таким образом, чтобы он был применим для разрешения адресов в различных сетях [3].

ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети. На рис. 3.2 показана структура пакета запросов и ответов [4].

Рис. 3.2 – Формат пакета ARP

- Network Type – тип канального протокола

Для Ethernet – 1.

- Protocol - протокол сетевого уровня
- HAL - длина канального адреса
- PAL - длина сетевого адреса
- Operation - тип операции (1 – запрос, 2 – ответ)

Узел, отправляющий ARP-запрос, заполняет в пакете все поля, кроме поля искомого локального адреса. Значение этого поля заполняется узлом, опо- знавшим свой IP-адрес.

Протокол ICMP. Протокол ICMP предназначен для передачи управляющих и диагностических сообщений. С его помощью передаются сообщения об ошибках, а также о возникновении ситуаций, требующих повышенного внимания. Протокол относится к сетевому уровню модели TCP/IP. Сообщения ICMP генерируются и обрабатываются протоколами сетевого (IP) и более высоких уровней (TCP или UDP). При появлении некоторых ICMP-сообщений генерируются сообщения об ошибках, которые передаются пользовательским процессам. ICMP-сообщения передаются внутри IP-дейтаграмм (рис. 3.3). [2]

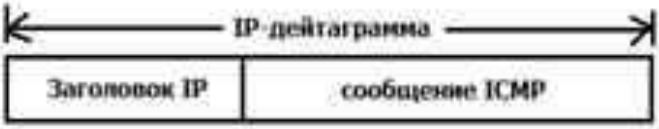


Рис. 3.3 – Инкапсуляция ICMP-сообщений в IP-дейтаграммы

Формат ICMP-сообщения показан на рис. 3.4. Заголовок ICMP включает 8 байт, но только первые 4 байта одинаковы для всех сообщений, остальные поля заголовка и тела сообщения определяются типом сообщения.

Рис. 3.4 – Формат ICMP-сообщения

Поле контрольной суммы охватывает ICMP-сообщение целиком. Тип сообщения определяется значением поля “Тип” заголовка. Некоторые типы ICMP-сообщений имеют внутреннюю детализацию (код), при этом конкретный вид сообщения определяется как типом, так и кодом сообщения. Подробнее с видами типов и кодов ICMP-сообщений можно ознакомиться в специфика-

ции протокола ICMP RFC 792. [Электронный ресурс]. URL: http://tools.ietf.org/html/rfc792.

Программа ping. Программа ping была разработана для проверки доступности удаленного узла. Программа посылает ICMP-эхо-запрос на узел и ожидает возврата ICMP-эхо-отклика. Программа ping является обычно первым диагностическим средством, с помощью которого начинается идентификация какой-либо проблемы в сетях. Помимо доступности, с помощью ping можно оценить время возврата пакета от узла, что дает представление о том, "насколько далеко" находится узел. Кроме этого, Ping имеет опции записи маршрута и временной метки. Сообщения эхо-запроса и эхо-отклика имеют один формат (рис 3.5). [2]

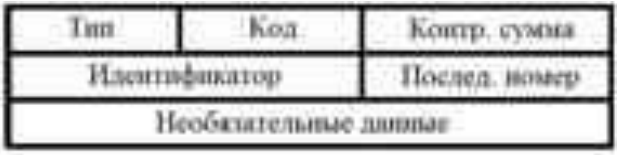


Рис. 3.5 – Формат пакета ICMP-сообщения

- Тип – тип пакета: 8 – запрос эха; 0 – ответ на запрос эха;
- Код – расшифровка назначения пакета внутри типа (в данном случае 0);
- Контрольная сумма вычисляется для всего пакета;
- Идентификатор – номер потока сообщений;
- Последовательный номер – номер пакета в потоке [3].

Так же, как в случае других ICMP-запросов, в эхо-отклике должны содержаться поля идентификатора и номера последовательности. Кроме того, любые дополнительные данные, посланные компьютером, должны быть отражены эхом.

В поле идентификатора ICMP сообщения устанавливается идентификатор процесса, отправляющего запрос. Это позволяет программе ping идентифицировать вернувшийся ответ, если на одном и том же хосте в одно и то же время запущено несколько программ ping.

Номер последовательности начинается с 0 и инкрементируется каждый раз, когда посылается следующий эхо-запрос. Вывод программы показан на рис. 3.6. Первая строка вывода содержит IP-адрес хоста назначения, даже если было указано имя. Поэтому программа ping часто используется для определения IP-адреса удаленного узла [2].

```
C:\>ping yandex.ru

Обмен пакетами с yandex.ru [93.158.134.11] с 32 байтами данных:
Ответ от 93.158.134.11: число байт=32 время=48мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=27мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=29мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=29мс TTL=51

Статистика Ping для 93.158.134.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 27мсек, Максимальное = 48 мсек, Среднее = 33 мсек
```

Рис. 3.6 – Вывод программы ping

Программа tracert. Программа tracert позволяет посмотреть маршрут, по которому двигаются IP-дейтаграммы от одного хоста к другому.

Программа tracert не требует никаких специальных серверных приложений. В ее работе используются стандартные функции протоколов ICMP и IP. Для понимания работы программы следует вспомнить порядок обработки поля TTL в заголовке IP-дейтаграммы.

Каждый маршрутизатор, обрабатывающий дейтаграмму, уменьшает значение поля TTL в ее заголовке на единицу. При получении дейтаграммы с TTL равным 1, маршрутизатор уничтожает ее и посылает хосту, который ее отправил, ICMP-сообщение "время истекло". При этом дейтаграмма, содержащая это ICMP-сообщение, имеет в качестве адреса источника IP-адрес маршрутизатора.

Это и используется в программе tracert. На хост назначения отправляется IP-дейтаграмма, в которой поле TTL, установлено в единицу. Первый маршрутизатор на пути дейтаграммы, уничтожает ее (так как TTL равно 1) и отправляет ICMP-сообщение об истечении вре- мени. Таким образом, опреде-

ляется первый маршрутизатор в маршруте. Затем tracert отправляет дейтаграмму с полем TTL равным 2, что позволяет получить IP-адрес второго маршрутизатора. Аналогичные действия продолжаются до тех пор, пока дейтаграмма не достигнет хоста назначения. При получении ответа от этого узла процесс трассировки считается завершённым. Пример вывода программы показан на рис. 3.7.

Рис. 3.7 Вывод программы tracert

Первая строка, без номера содержит имя и IP адрес пункта назначения и указывает на то, что величина TTL не может быть больше 30.

Следующие строки вывода начинаются с распечатки значения TTL (1, 2, 3 и т.д.) и содержат имя (IP-адрес) хоста или маршрутизатора и время возврата ICMP-сообщения.

Для каждого значения TTL отправляется 3 дейтаграммы. Для каждого возвращенного ICMP-сообщения рассчитывается и печатается время возврата. Если ответ на дейтаграмму не получен в течение пяти секунд, печатается звездочка, после чего отправляется следующая дейтаграмма. [2].

3. Выполнение работы.

3.1 Построение топологии сети

В конце лабораторной работы №2 была создана топология сети, состоящая из конечных узлов (PC), коммутаторов и маршрутизатора (рис. 4.24). Маршрутизатор в ней Router0 имеет два интерфейса и соединяет две подсети. Произведем настройку конечных узлов.

3.2 Настройка конечных узлов

На устройствах PC0-PC4 установим заданные IP-адреса и маску подсети (таблица 3.1). IP-адрес шлюза для всех узлов – 192.168.3.1. IP-адрес DNS-сервера указывать необязательно, т.к. в данной работе он использоваться не будет.

Таблица 3.1 – Параметры конечных узлов

Хост	IP-адрес	Маска подсети
PC0	192.168.3.3	255.255.255.0
PC1	192.168.3.4	255.255.255.0
PC2	192.168.3.5	255.255.255.0
PC3	192.168.3.6	255.255.255.0
PC4	192.168.3.7	255.255.255.0

На устройствах PC5, Laptop0, PC6 установим заданные IP-адреса и маску подсети (таблица 3.2). IP-адрес шлюза для всех узлов – 192.168.5.1. IP-адрес DNS-сервера указывать необязательно.

Таблица 3.2 – Параметры конечных узлов

Хост	IP-адрес	Маска подсети
PC5	192.168.5.3	255.255.255.0
Laptop0	192.168.5.4	255.255.255.0
PC6	192.168.5.5	255.255.255.0

Каждый узел переименуем его же IP-адресом, для наглядности.

3.3 Настройка маршрутизатора

При настройке конечных узлов уже упоминалось о том, что маршрутизатор в данной топологии сети имеет два интерфейса. Произведем настройку интерфейса FastEthernet0/0:

1) Один клик по устройству (маршрутизатору);
2) Выбираем вкладку “Config”;
3) Находим интерфейс FastEthernet0/0, задаем нужный IP-адрес и маску подсети (рис. 3.8).

Важно! Интерфейс маршрутизатора, по умолчанию, отключен; необходимо его включить, кликнув мышкой рядом с "On".

Рис. 3.8 – Настройка интерфейса маршрутизатора

4) Закрываем окно, смотрим на всю топологию сети. Зеленые индикаторы состояния на линии связи между Router0 и Switch0 сигнализируют, что интерфейс подключен правильно (рис. 3.9).

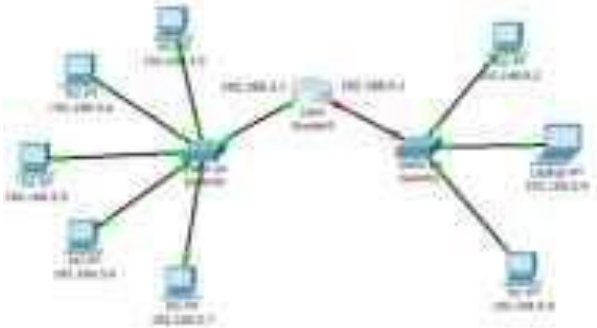


Рис. 3.9 – Вид рабочей области

Аналогично производим настройку интерфейса FastEthernet 0/1 в соответствующем окне (рис. 3.10).

Рис. 3.10 – Настройка интерфейса маршрутизатора

Сделать надписи к интерфейсам маршрутизатора, можно с помощью инструмента Place Note на панели Common Tools  . Необходимо кликнуть на инструмент, затем сделать клик в нужном месте на рабочей области.

3.4 Настройка режима симуляции Cisco Packet Tracer

Убедитесь, что вы находитесь в режиме симуляции. Для этого кликните на иконку симуляции в правом нижнем углу рабочей области симулятора. 

Откроется окно событий, в котором вы увидите список событий, управляющие кнопки, заданные фильтры (рис. 3.11). По умолчанию, фильтруются, т.е. будут отображаться, пакеты всех возможных протоколов, необходимо поправить и ограничить этот список до исследуемых протоколов.

Управляющие кнопки: 1) Back – назад; 2) Auto Capture/Play – автоматический захват пакетов от источника до приемника и обратно;

4) Capture/Forward – захват пакетов только от одного устройства до другого.

	
Рис. 3.11 Окно событий режима симуляции	Рис. 3.12 Добавление фильтров на протоколы ARP и ICMP

В данной лабораторной работе нас интересуют пакету двух типов ARP и ICMP.

Следовательно, нужно поставить фильтр только на сообщения заданного типа (рис. 3.12):

1) Нажимаем на кнопку "Edit Filters"
2) Снимаем метку с "Show All/None"
3) Выбираем ARP и ICMP
4) Убедимся, что заданные протоколы для фильтрации назначены верно.

3.5 Проверка работы сети в режиме симуляции

Отправим тестовый ping-запрос с конечного узла с IP-адресом 192.168.3.3 на хост с IP-адресом 192.168.3.5.

Важно! Оба узла находятся в пределах одного сегмента сети

1) Один клик по выбранному устройству (рис. 3.13)

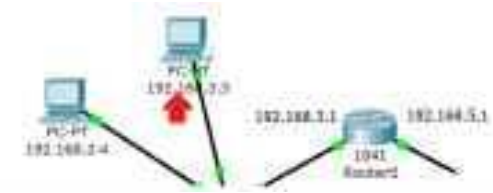


Рис. 3.13 Выбор узла 192.168.3.3

2) Выбираем вкладку Desktop, в которой содержатся симуляторы некоторых программ, доступных на компьютере (см. рис. 3.4).

3) Выбираем "Command Prompt", программу, имитирующую командную строку компьютера.

4) С помощью утилиты ping отправляем ping-запрос (рис. 3.6). (Не забудьте нажать Enter).

На устройстве-источнике формируются два пакета протокола ARP и ICMP (рис. 3.15). ARP-запрос возникает всегда, когда хост пытается связаться с другим хостом.

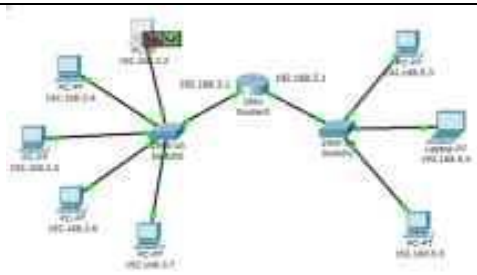


Рис. 3.14 Вид рабочей области

Рис. 3.15 Формат пакета ARP-запроса

Нажимаем на кнопку "Auto Capture/play" или "Capture/Forward", последняя позволит вам управлять движением пакетов от устройства к устройству самим. Видим, что первым отправляется пакет протокола ARP, так как ARP-таблица хоста 192.168.3.3 пуста, и он еще «не знает», кому отправлять ping-запрос. Сделайте один клик по самому пакету (конверту), ознакомьтесь, какие уровни модели OSI задействованы. Перейдите к

вкладке “Inbound PDU Details”, которая содержит структуру пакета (рис. 4.43).

Узел 192.168.3.3 построил запрос и посылает его широковещательным сообщением всем хостам подсети. Помимо IP-адреса назначения, запрос содержит IP-адрес и MAC-адрес отправителя, чтобы приемная сторона могла ответить.

При просмотре прохождения пакетов убедитесь, что на ARP-запрос ответит только хост 192.168.3.5. Каждый хост в подсети получает запрос и проверяет на соответствие свой IP-адрес. Если он не совпадает с указанным адресом в запросе, то запрос игнорируется (рис. 3.16).

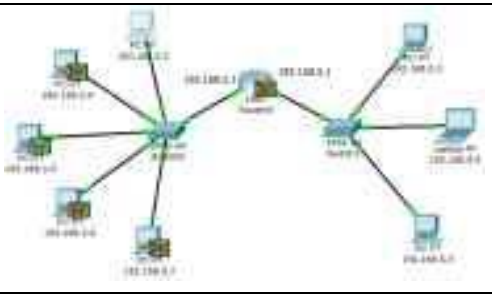


Рис. 3.16 Вид рабочей области

Рис. 3.17 Формат пакета ARP-ответа

Посмотрите содержимое пакета ARP-ответа, пришедшего на хост 192.168.3.3 (рис. 3.18). Узел 192.168.3.5. послал ARP-ответ непосредственно отправителю, используя его MAC-адрес, с указанием собственного MAC-адреса в поле “Target MAC”.

Далее отправляется ICMP-сообщение ping-запроса. Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 3.18).

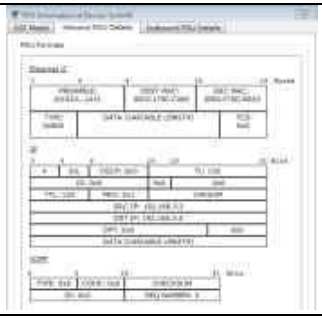


Рис. 3.18 Формат пакета ICMP-эхо-запроса

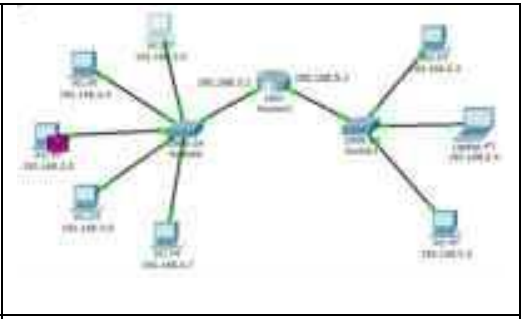


Рис. 3.19 Вид рабочей области

Физические адреса узлов известны. IP-адрес источника – 192.168.3.3. IP-адрес назначения – 192.168.3.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Запрос производится на хост 192.168.3.5 через коммутатор (рис. 4.47). Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.3 (рис. 3.20).

Рис. 3.20 Формат пакета ICMP-эхо-ответа

Рис. 3.21 Окно событий режима симуляции

IP-адрес источника – 192.168.3.5. IP-адрес назначения – 192.168.3.3. Тип ICMP-сообщения – 0 (эхо-ответ).Посмотрите ping-ответ в командной строке хоста 192.168.3.3.

В окне событий так же указаны маршруты запроса ARP и ICMP: через какие устройства прошли пакеты (рис. 4.50).

Удалить сценарий симуляции можно с помощью кнопки "Reset Simulation" или воспользоваться кнопкой "Delete" в области User Created Packet Window.

Теперь ARP-таблицы хостов 192.168.3.3 и 192.168.3.5 не пусты, в них содержится одна запись. Чтобы просмотреть содержимое ARP-таблицы, нужно выполнить команду: "arp –a" в командной строке. Содержимое ARP-таблицы узла 192.168.3.3 (рис. 3.22).

```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.3.5           0002.1790.c065        dynamic
```

Рис. 3.22 ARP-таблица узла 192.168.3.3 в командной строке

Можно воспользоваться другим способом: нажать на кнопку «Inspect»  , нажать на выбранное устройство, выбрать «ARP table» и просмотреть записи ARP-таблицы узла (рис. 3.23).

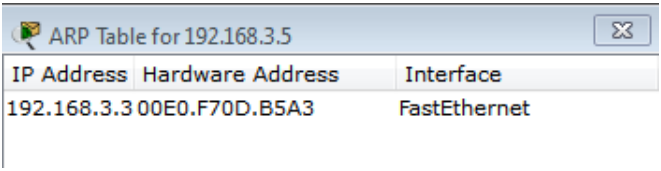


Рис. 3.23 ARP-таблица узла 192.168.3.3, показанная с помощью инструмента «Inspect»

Если снова задать ping-запрос на хост 192.168.3.5, то сразу будет сформирован только один пакет ICMP-сообщения, т.к. в ARP-таблице компьютера-источника уже хранится соответствующий локальный адрес.

3.6 Посылка ping-запроса во внешнюю сеть

Отправим тестовый ping-запрос с конечного узла с IP-адресом 192.168.3.4 на хост с IP-адресом 192.168.5.5.

Важно! *Один узел пытается передать пакет другому узлу, находящемуся с ним в разных сетях.*

В пункте 5 лабораторной работы был рассмотрен случай посылки ARP-запроса внутри локальной сети. Протокол ARP в этом случае определял непосредственно MAC-адрес узла-приемника запроса. Теперь рассмотрим ситуацию, когда узел-источник и узел-приемник находятся в разных сетях. Протокол ARP работает в пределах сегмента сети, поэтому в данном случае он будет использоваться для определения MAC-адреса маршрутизатора. Таким образом, пакет будет передан маршрутизатору для дальнейшей ретрансляции.

Открываем "Command Promt", имитирующую командную строку, на компьютере ***192.168.3.4*** и посылаем на хост ***192.168.5.5.*** ping-запрос.

В этом случае инициируется ARP-запрос маршрутизатору, который пересылает пакеты в сеть назначения. На узле-источнике формируются два пакета протокола ARP и ICMP (рис. 3.24).

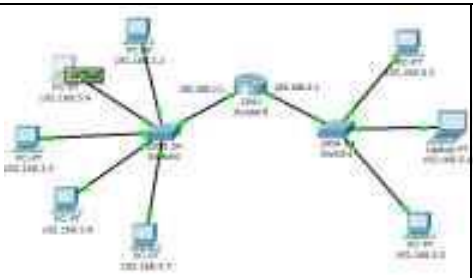


Рис. 3.24 Вид рабочей области

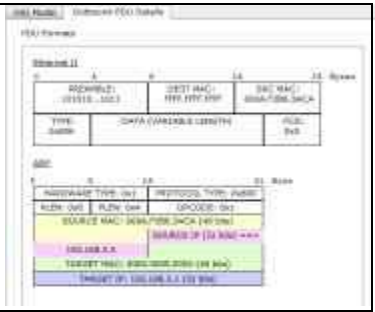


Рис. 3.25 Формат пакета ARP-запроса

Формат пакета ARP-запроса содержит те же сведения, что и для разрешения локального адреса устройства, и рассылается широковещательно всем узлам подсети (рис. 3.25). Все узлы игнорируют пакет, кроме маршрутизатора, для которого пакет предназначался (рис. 3.26).

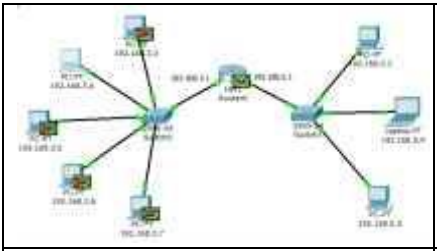


Рис. 3.26 Вид рабочей области

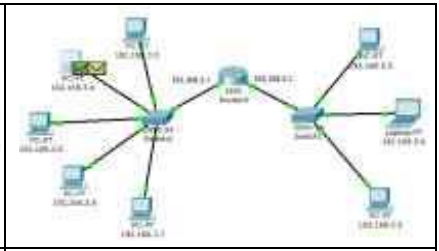


Рис. 3.27 Вид рабочей области

Маршрутизатор формирует ARP-ответ, указывая свой физический адрес, и отправляет его узлу 192.168.3.4 (рис. 3.27). После получения ARP-ответа хост 192.168.3.4 посылает ICMP-сообщение ping-запроса через маршрутизатор в сеть назначения. Посмотрите содержимое пакета, сделав клик по пакету (конверту) (рис. 3.28).

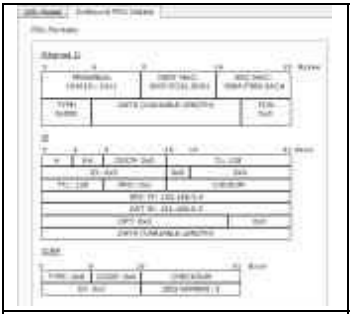


Рис. 3.28 Формат пакета ICMP-эхо-запроса

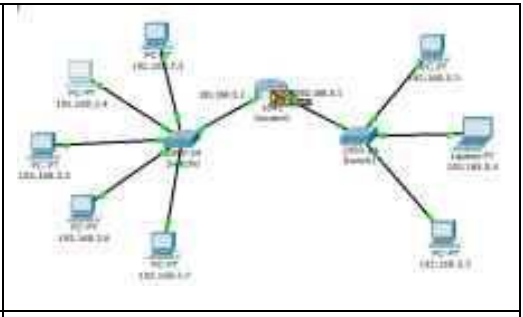


Рис. 3.29 Вид рабочей области

IP-адрес источника – 192.168.3.4. IP-адрес назначения – 192.168.5.5. Тип ICMP-сообщения – 8 (эхо-запрос).

Когда запрос приходит в сеть назначения, то маршрутизатор определяет MAC-адрес получателя, если такового нет в ARP-таблице маршрутизатора. Таким образом, снова решается задача разрешения локального адреса (рис. 3.29).

Маршрутизатор вынужден сперва узнать физический адрес получателя, прежде чем он сможет отправить ping-запрос по назначению, поэтому пакет с ping-запросом, пришедший на маршрутизатор, отклонен.

Новый ARP-запрос отправляется широковещательным сообщением от маршрутизатора, содержит его IP-адрес и MAC-адрес (рис. 3.30). IP-адрес назначения – узел 192.168.5.5.

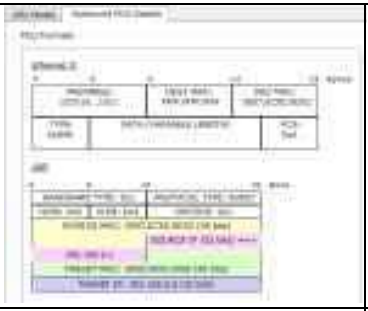


Рис. 3.30 Формат пакета ARP-запроса

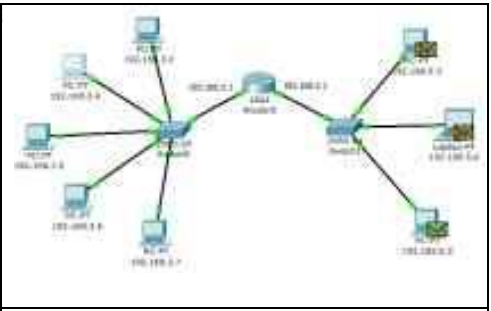


Рис. 3.31 Вид рабочей области

Узлы подсети, которым пакет не предназначен, его игнорируют (рис. 4.61). Узел 192.168.5.5. формирует ARP-ответ и отправляет его обратно маршрутизатору (рис. 3.32), указав свой MAC-адрес, о чем свидетельствует содержимое пакета (рис. 3.33).

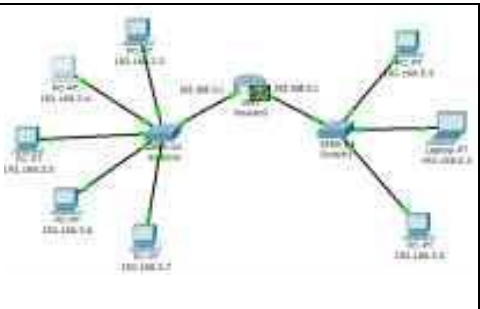


Рис. 3.32 Вид рабочей области

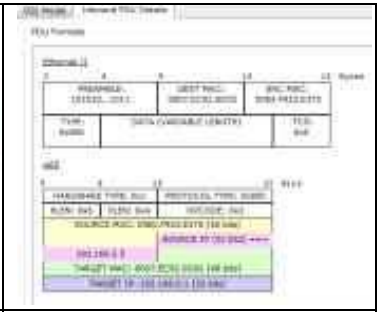


Рис. 3.33 Формат пакета ARP-ответа

После того, как маршрутизатор определил MAC-адрес получателя входящего ping-запроса, он посылает ICMP-ответ маршрутизатору хоста отправителя. (В данном случае это тот же маршрутизатор Router0).

Узел 192.168.3.4. снова пытается отправить ping-запрос во внешнюю сеть узлу 192.168.5.5. Его маршрут должен лежать через коммутатор Switch0, маршрутизатор Router0, коммутатор Switch1 и достигнуть узла назначения (рис. 3.34). Проследите маршрут пакета самостоятельно.

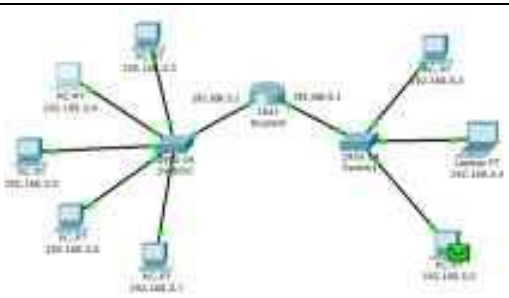


Рис. 3.34 Вид рабочей области

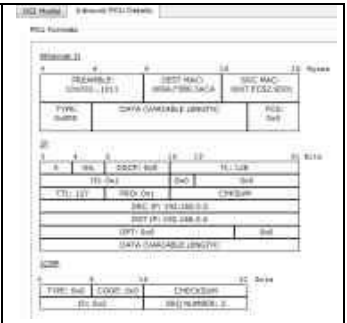


Рис. 3.35 Формат пакета ICMP-эхо-ответа

Узел формирует ping-ответ, который отправляется обратно узлу 192.168.3.4.Посмотрите содержимое пакета ping-ответа, пришедшего на хост 192.168.3.4 (рис. 3.35).

IP-адрес источника – 192.168.5.5. IP-адрес назначения – 192.168.3.4. Тип ICMP-сообщения – 0 (эхо-ответ).

Посмотрите ping-ответ в командной строке хоста 192.168.3.4 (рис. 3.36). Маршрут пакета можно посмотреть с помощью команды tracert. Выполним эту команду, например, в командной строке компьютера 192.168.3.5 (рис. 3.37).

```
PC>ping 192.168.5.5

Pinging 192.168.5.5 with 32 bytes of data:

Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

Рис. 3.36 Вывод программы ping

```
PC>tracert 192.168.5.4

Tracing route to 192.168.5.4 over a maximum of 30 hops:

  1    40 ms      40 ms      40 ms      192.168.3.1
  2    80 ms      70 ms      50 ms      192.168.5.4

Trace complete.
```

Рис. 3.37 Вывод программы tracert

3.7 Посылка ping-запроса на несуществующий хост

Отправим ping-запрос на несуществующий адрес в сеть 192.168.5.0/24. Для этого откроем программу "Command Promt" на узле 192.168.3.7 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом ***192.168.5.6***.

ARP-таблица на узле-источнике не содержит соответствующей записи о MAC-адресе узла 192.168.5.6, поэтому формируется ARP-запрос (рис. 3.38).

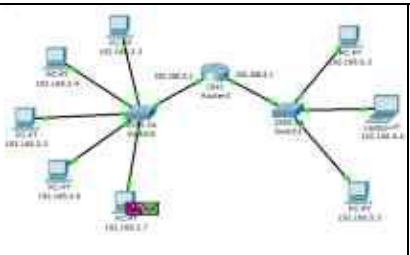


Рис. 3.38 Вид рабочей области

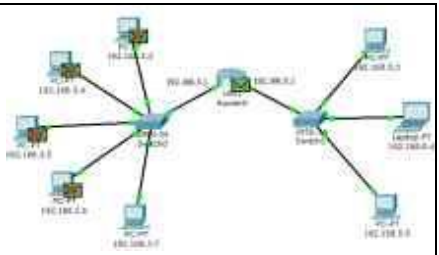


Рис.3.39 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис.3.39). Узел 192.168.3.7 получает ARP-ответ с MAC-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос на узел 192.168.5.6 (рис.3.40).

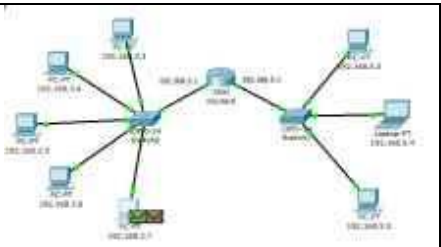


Рис. 3.40 Вид рабочей области

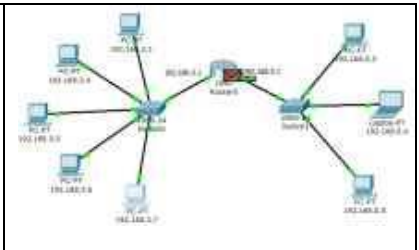


Рис. 3.41 Вид рабочей области

Маршрутизатор пришедший пакет уничтожает, т.к. не может его перенаправить на указанный адрес, потому что соответствующего MAC-адреса он «не знает». В связи с этим маршрути-

затор формирует ARP-запрос по адресу 192.168.5.6 (рис. 3.41).

Все узлы подсети игнорируют пакет, потому что IP-адрес в запросе не соответствует их собственным. Маршрутизатор ни какого ответа ни от кого не получает.

Процедура прохождения пакетов повторяется в течение всего сценария симуляции: маршрутизатор по-прежнему «не знает» MAC-адрес указанного в ping-запросе IP-адреса 192.168.5.6 и продолжает рассылать ARP-запросы. Ни один из узлов подсети на эти запросы не реагирует. Не получив ответа, маршрутизатор и сам «молчит», никак не уведомляя об ошибке хост-источник ping-запроса.

Примечание. *На самом деле в данном случае маршрутизатору следует отправить ICMP-сообщение «хост недостижим»: сообщение типа 3 с кодом 1. Однако проведенный эксперимент с теорией разошелся.*

Посмотрим ответ на ping-запрос в командной строке узла-источника *192.168.3.7*: «превышено время ожидания» (рис.3.42).

```
PC>ping 192.168.5.6

Pinging 192.168.5.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис.3.42 Вывод программы ping

Попробуем отправить ping-запрос, содержащий IP-адрес узла, в сеть, на которую нет маршрута.

Откроем программу “Command Promt” на узле 192.168.3.6 и попробуем отправить ping-запрос на несуществующий хост с IP-адресом: *192.168.6.6.* Так как ARP-таблица узла-источника соответствующей записи не имеет, формируется ARP-запрос на заданный узел с IP-адресом 192.168.6.6 (рис. 3.43).

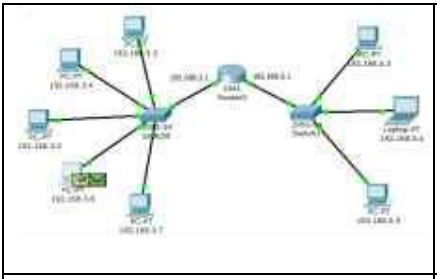


Рис. 3.43 Вид рабочей области

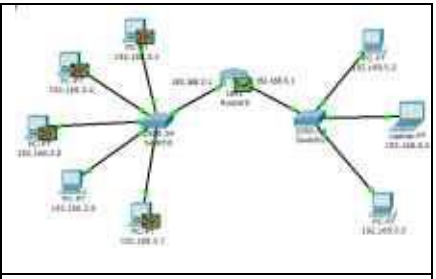


Рис. 3.44 Вид рабочей области

Все узлы игнорируют пакет, кроме маршрутизатора, которому этот пакет предназначался (рис.3.44). Узел 192.168.3.6 получает ARP-ответ с MAC-адресом маршрутизатора. Теперь, зная его аппаратный адрес, хост отправляет ping-запрос.

Когда ping-запрос попадает на маршрутизатор, тот не может его перенаправить не на какой из своих интерфейсов, т.к. IP-адреса его интерфейсов не совпадают с тем адресом, который указан в ping-запросе. Соответственно, этот пакет уничтожается и формируется новое ICMP-сообщение (рис. 3.44).

Посмотрим содержимое пакета, сформированного маршрутизатором (рис. 3.45).

Рис. 3.45 Формат пакета ICMP «хост недостижим»

```
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис. 3.46 Вывод программы ping

IP-адрес источника – 192.168.3.1. IP-адрес назначения – 192.168.3.6. Тип ICMP-сообщения – 3 с кодом 1, что означает «хост недостижим». Этот пакет приходит на узел 192.168.3.6.

Результат ping-запроса в командной строке узла 192.168.3.6: «хост назначения недостижим» (рис. 3.46).

Таким образом, маршрутизатор «ответил» на ping-запрос, для которого у него не было соответствующего маршрута, новым ICMP-сообщением «хост недостижим».

Контрольные вопросы

1. Для чего предназначен протокол протоколы ARP?
2. Для чего предназначен протокол ICMP?
3. Как осуществляется настройка внешних узлов в программе Cisco Packet Tracer?
4. Какие функциональные возможности предоставляет программа ping?
5. Какие функциональные возможности предоставляет программа tracert?
6. Как осуществляется настройка маршрутизатора в программе Cisco Packet Tracer?
7. Назовите какие основные ошибки при посылке ping-запроса могут возникнуть в сети?

Практическая работа №4.

Протоколы SMTP и POP3

1. **Цель работы:** изучить принципы организации взаимодействия прикладных программ с помощью протоколов электронной почты SMTP и POP3 в режиме симуляции Cisco Packet Tracer.

2. **Краткие теоретические сведения.**

2.1 Протоколы SMTP и POP3.

Схема взаимодействия с прикладными почтовыми протоколами представлена на рис. 4.1.

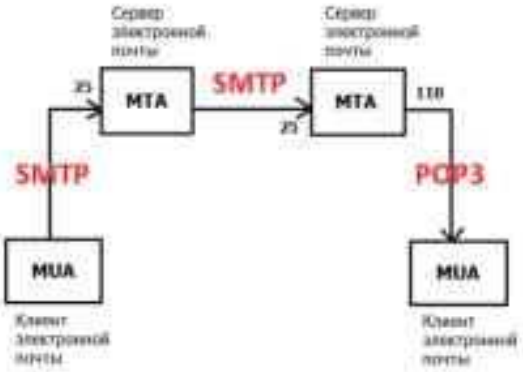


Рис. 4.1 Схема взаимодействия с прикладными почтовыми протоколами

Mail Transfer Agent (MTA) – агент передачи почты, являющийся основным компонентом системы передачи почты, представляет данный компьютер для сетевой системы электронной почты. Обычно пользователи не работают непосредственно с MTA, а используют Mail User Agent (MUA) – клиент электронной почты.

Для передачи сообщений по TCP-соединению большинство почтовых агентов пользуются протоколом Simple Mail Transfer Protocol (SMTP). SMTP принят в качестве стандартного метода передачи электронной почты в сети Internet. Действующий стандарт протокола описан в RFC 2821. В качестве транспортного протокола SMTP использует TCP, соединение устанавливается через порт с номером 25. Для обслуживания этого соединения используется специальная программа, которая именуется почтовым сервером. Для формирования сообщения и установления соединения используется почтовая программа пользователя. После установления соединения обмен информацией происходит посредством команд. Для пользователя эти команды не доступны, если при работе он использует клиент электронной почты [5].

Главной целью протокола SMTP является надежная и эффективная доставка электронных почтовых сообщений. Для реализации протокола требуется только надежный канал связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или же всемирная сеть Internet.

Передача обычно осуществляется непосредственно с хоста отправителя на хост получателя, когда оба хоста используют один транспортный сервис. Если же хосты не подключены к общей транспортной системе, передача осуществляется с использованием одного или нескольких промежуточных серверов SMTP. Сегодня в Internet обычной практикой является представление исходного сообщения промежуточному серверу, который выполняет некоторые дополнительные функции. Промежуточный сервер в таких случаях действует как шлюз в другие среды передачи и выбирается обычно с использованием MX-записей DNS (служба доменных имен).

Протокол SMTP базируется на следующей модели коммуникаций: в ответ на запрос пользователя почтовая программа-отправитель сообщения устанавливает двустороннюю связь с программой-приемником (почтовым сервером). Получателем может быть оконечный или промежуточный адресат. Если необходимо, почтовый сервер может установить соединение с другим сервером и передать сообщение дальше.

Для того чтобы получить сообщение из своего почтового ящика, почтовая программа пользователя соединяется с сервером уже не по протоколу SMTP, а по специальному почтовому протоколу получения сообщений. Такой протокол позволяет работать с почтовым ящиком: забирать сообщения, удалять сообщения, сортировать их и выполнять другие операции. Самым популярным в настоящее время протоколом такого рода является протокол Post Office Protocol v.3 (POP3).

Многие концепции, принципы и понятия протокола POP3 выглядят и функционируют подобно SMTP: взаимодействие происходит посредством команд. Сервер POP3 находится между агентом пользователя и почтовыми ящиками.

Он предусматривает соединение с почтовым сервером на основе транспортного протокола TCP через порт 110. Спецификация POP3 определена в документе RFC 1939. POP3 разработан с учетом специфики доставки почты на персональные компьютеры и имеет соответствующие операции для этого [6].

Конструкция протокола POP3 обеспечивает возможность пользователю обратиться к своему почтовому серверу и изъять накопившуюся для него почту. Пользователь может получить доступ к POP3-серверу из любой точки доступа к Internet. При этом он должен запустить специальный почтовый агент, работающий по протоколу POP3, и настроить его для работы со своим почтовым сервером. Сообщения доставляются клиенту по протоколу POP3, а посылаются при помощи SMTP. То есть на компьютере пользователя существуют два отдельных агента-интерфейса к почтовой системе – доставки (POP3) и отправки (SMTP).

2.2 Служба DNS.

В лабораторной работе будут изучены изучению прикладные протоколов электронной почты SMTP и POP3. Однако взаимодействие с системой электронной почты невозможно без системы доменных имен (DNS). В задачи службы DNS входит:

1. Преобразование символических имен в IP-адреса;
2. Преобразование IP-адресов в символические имена.

Дополнительной функцией DNS является маршрутизация почты. Основная спецификация распределенной службы DNS указана в RFC 1034 и RFC 1035.

Единицами хранения и передачи информации в DNS являются ресурсные записи. Существует множество типов ресурсных записей, каждая из которых состоит из определенного числа полей. Для маршрутизации почты используется запись "MX", при ее отсутствии запись типа "A". Запись "A" (адресная запись) содержит параметры: доменное имя узла, соответствующий IP-адрес.

Пример: *aivt IN A 195.19.212.16, где "IN" – это класс записи* (интернет).

Запись "MX" содержит параметры: имя почтового домена, имя почтового сервера, приоритет.

Пример: aivt IN MX 20 mail.stu.neva.ru, где "IN" – это класс записи (интернет). [4]

При получении письма MTA анализирует его служебную информацию, в частности заголовок письма, определяя домен получателя (см. рис. 4.83). Если он относится к домену, который обслуживается данным MTA, производится поиск получателя и письмо помещается в его ящик.Если домен получателя не обслуживается этим MTA, формируется DNS-запрос, запрашивающий MX-записи для данного домена. MX-запись представляет особый вид DNS-записи, которая содержит имена почтовых серверов, обрабатывающих входящую почту для данного домена. MX-записей может быть несколько, в этом случае MTA пробует последовательно установить соединение, начиная с сервера с наибольшим приоритетом. При отсутствии MX-записи запрашивается A-запись (запись адреса, сопоставляющая доменное имя с IP-адресом) и выполняется попытка доставить почту на указанный там хост. При невозможности отправить сообщение, оно возвращается отправителю (помещается в почтовый ящик пользователя) с сообщением об ошибке.[8]

3. Выполнение работы.

3.1 Построение топологии сети

Для исследования заданных прикладных протоколов построим тестовую топологию сети следующего вида (рис. 4.2):

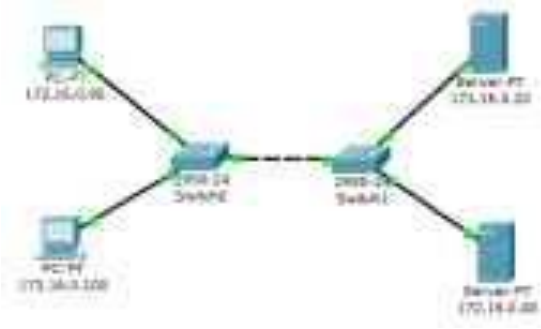


Рис. 4.2 Тестовая топология сети

Производим настройку сетевых устройств согласно заданным параметрам (таблица 4.1, таблица 4.2).

Таблица 4.1 – Параметры узлов тестовой топологии сети

Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.0.90	255.255.0.0	172.16.0.20
PC1	172.16.0.100	255.255.0.0	172.16.0.20

Таблица 4.2 – Параметры серверов тестовой топологии сети

Серверы	IP-адрес	Маска сети	IP-адрес DNS-сервера
Server0	172.16.0.20	255.255.0.0	172.16.0.20
Server1	172.16.0.40	255.255.0.0	172.16.0.20

Все устройства расположены в одном сегменте локальной сети, поэтому маршрутизация пакетов не используется, значит, IP-адрес шлюза по умолчанию указывать необязательно.

3.2 Настройка почтового сервера

В качестве серверов электронной почты выступают сервер 172.16.0.20 и сервер 172.16.0.40. Схема взаимодействия с прикладными почтовыми протоколами применительно к построенной сети представлена на рис. 4.3:

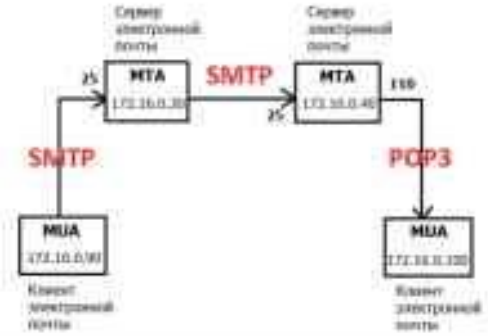


Рис. 4.3 Схема взаимодействия с прикладными почтовыми протоколами в исследуемой сети

На каждом из MTA будет поддерживаться smtp- и pop3-сервер. Подключиться к серверу может любой зарегистрированный пользователь. Чтобы отправить письмо, пользователь на сервере проходит авторизацию, после чего сервер готов отправлять письма от имени пользователя. По адресу назначения письма сервер определяет, кому следует передать его дальше. Нужный адрес сервер определяет с помощью службы DNS, в которой содержится соответствующая ресурсная адресная запись, преобразовывающая имя домена в IP-адрес.

Подключим службу DNS на сервере 172.16.0.20:

1) Один клик по выбранному устройству.
2) Выбираем вкладку Config, Services -> DNS (рис. 4.4).

Заносим данные о новой ресурсной записи: имя домена, IP-адрес, тип ресурсной записи. Симулятор не поддерживает ресурсную запись, предназначенную для почтовых серверов, MX, но ее можно заменить адресной (тип A).

Рис. 4.4 Настройка службы DNS на сервере

Рис. 4.5 Настройка службы DNS на сервере

3) Нажимаем на кнопку “Add” будет добавлена новая запись в службу DNS (рис. 4.5).

Повторим предыдущие действия и добавим еще одну ресурсную запись о почтовом сервере 172.16.0.40 (рис. 4.6).

Рис. 4.6 Настройка службы DNS на сервере

Рис. 4.7 Конфигурация smtp- и pop3-сервера

Теперь сконфигурируем почтовый сервер 172.16.0.20 с поддержкой smtp- и pop3-сервера:

1) Один клик по выбранному устройству.

2) Выбираем вкладку “Config”, Services -> EMAIL

3) Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты. Нажимаем кнопку “Set” (рис. 4.7).

4) Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки “+” (рис. 4.8).

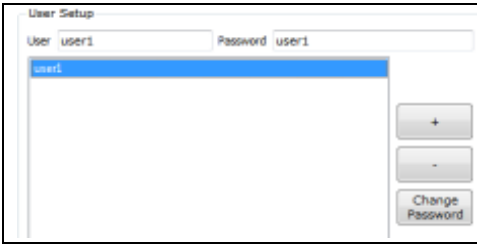


Рис. 4.8 Создание учетной записи

Рис. 4.9 Конфигурация smtp- и pop3-сервера

Smtp-сервер и pop3-сервер на машине 172.16.0.20 сконфигурированы, имеют одного зарегистрированного пользователя. Так же на нем поддерживается служба DNS, в которой есть две ресурсных записи.

На сервере 172.16.0.40 так же необходимо настроить почтовый сервер с поддержкой SMTP и POP3 (рис. 4.9). В качестве DNS для него выступает сервер 172.16.0.20.

1) Один клик по выбранному устройству.
2) Выбираем вкладку "Config", Services -> EMAIL
3) Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты - mail.ru. Нажимаем кнопку "Set".
4) Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки "+".

3.3 Настройка почтовой службы на конечных узлах

Для работы с почтовым smtp- или pop3-сервером на компьютере пользователя должен быть настроен клиент электронной почты, который и будет взаимодействовать с сервером (см. рис. 4.7).

Настроим на хосте 172.16.0.90 клиент электронной почты (рис. 4.92):

1) Один клик на хосте с IP-адресом 172.16.0.90.
2) Выбираем вкладку Desktop, программу "E-mail". Появится окно конфигурации почтового сервиса. Вводим пользовательские данные в форму.

	
Рис. 4.8 Настройка клиента электронной почты	Рис. 4.9 Настройка клиента электронной почты

Нажимаем кнопку “Save”, закрываем окно, конфигурация клиента электронной почты завершена. Теперь для пользователя user1 доступен почтовый сервис в домене server.ru: отправка и получение писем. Настроим почтовый сервис и на хосте 172.16.0.100, выполнив предыдущие действия (рис. 4.8). Вводим следующие пользовательские данные: Теперь для пользователя user2 доступен почтовый сервис в домене mail.ru: отправка и получение писем. Настройка всех устройств и необходимых служб завершена.

3.4 Исследование прикладных почтовых протоколов

Переходим в режим симуляции Cisco Packet Tracer. Добавляем фильтры на 2 протокола: SMTP и POP3 (рис. 4.9). Это значит, что пакеты только фильтруемых протоколов будут отображаться в сети.

Отправим письмо с хоста 172.16.0.90 от user1 на хост 172.16.0.100 user2 (рис. 4.10):

1) Один клик по выбранному узлу (172.16.0.90).
2) Выбираем на вкладке “Desktop” программу “E-mail”.
3) Чтобы написать и отправить письмо, нажимаем на кнопку “Compose”. Появится форма, которую следует заполнить. В поле “To” задается адрес электронной почты, кому вы отправляете письмо. Поле “Subject” содержит заголовок письма. Текст письма можете сочинить самостоятельно.

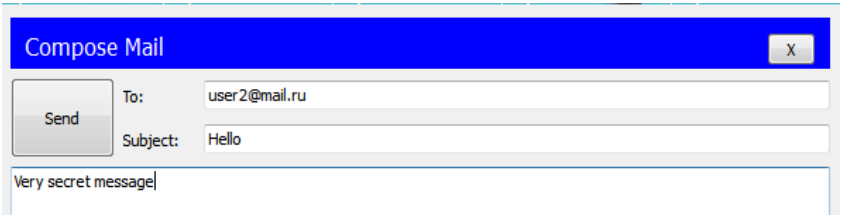


Рис. 4.10 Форма для отправления письма

Нажимаем на кнопку “Send”, начнется отправление письма. Видим, что на хосте 172.16.0.90 сформировался пакет SMTP (рис. 4.11). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

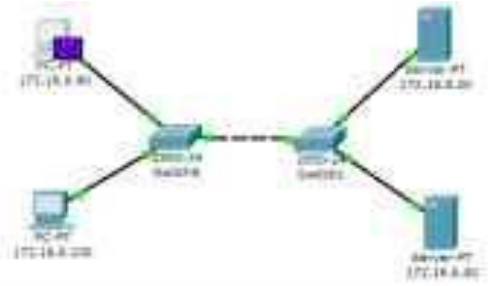


Рис. 4.11 Вид рабочей области

Посмотрим содержимое пакета, сформированного на узле (рис. 4.12).

Пакет адресован почтовому серверу по IP-адресу 172.16.0.20. В заголовке TCP содержится порт назначения – 25. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора (рис. 4.13). Убедитесь, что это так.

Рис. 4.12 Формат пакета SMTP

Когда пакет приходит на сервер, тот, обрабатывая его, определяет, что письмо адресовано домену mail.ru. Сервер 172.16.0.20 обращается к службе DNS за IP-адресом заданного сервера. По указанному адресу письмо перенаправляется на соответствующий почтовый сервер (рис. 4.14).

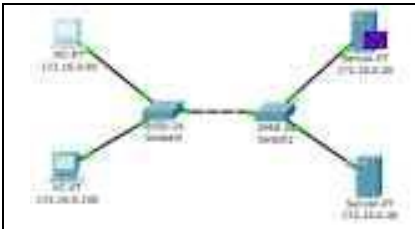


Рис. 4.13 Вид рабочей области

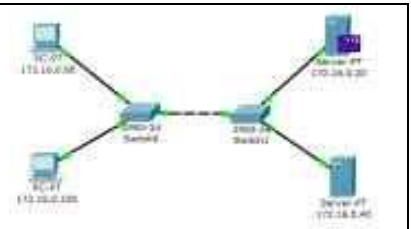


Рис. 4.14 Вид рабочей области

SMTP-пакет, сформированный сервером 172.16.0.20, содержит следующую информацию: IP-адрес назначения – 172.16.0.40, порт назначения – 25 (рис. 4.15).

Рис. 4.15 Формат пакета SMTP

Пакет проходит через коммутатор Switch1 и доставляется серверу 172.16.0.40 (рис. 4.16).

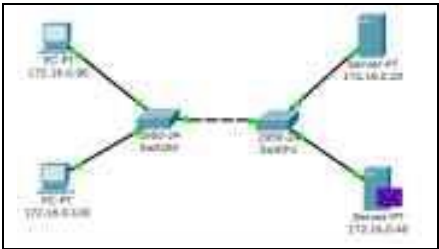


Рис. 4.16 Вид рабочей области

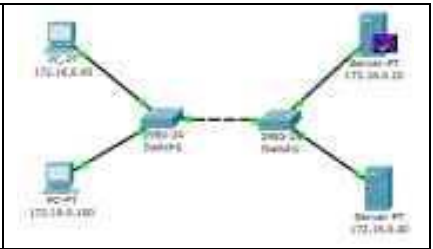
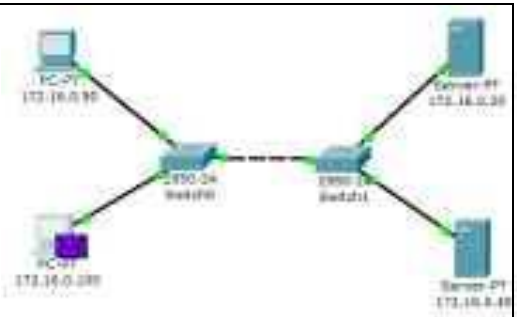


Рис. 4.17 Вид рабочей области

На сервере 172.16.0.40 формируется SMTP-ответ серверу 172.16.0.20 и отправляется на указанный адрес (рис. 4.17).

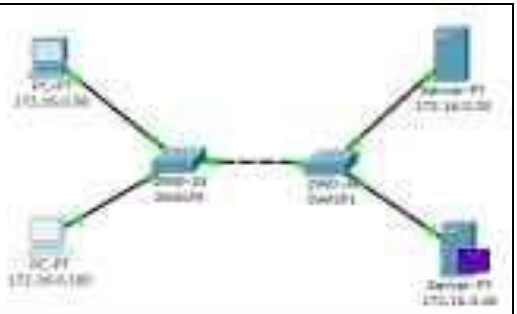
Из содержимого пакета, пришедшего обратно на сервер 172.16.0.20: IP-адрес источника – 172.16.0.40, порт источника – 25 (рис. 4.103). С помощью протокола SMTP мы отправили письмо на сервер mail.ru, теперь оно хранится там. Наш адресат (узел 172.16.0.100) еще не получил отправленное письмо, так как на сервер он еще не обратился по протоколу POP3. Для получения письма необходимо проделать следующие действия:

	
Рис. 4.18 Формат пакета SMTP	Рис. 4.19 Вид рабочей области

1) Один клик по узлу 172.16.0.100.
2) Выбираем на вкладке “Desktop” программу “E-mail”.
3) Нажимаем на кнопку “Receive”, чтобы прочитать письмо.

На хосте формируется пакет протокола POP3 (рис. 4.19). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

Посмотрим содержимое пакета, сформированного на узле (рис. 4.20).

	
Рис. 4.20 Формат пакета POP3	Рис. 4.21 Вид рабочей области

Пакет адресован почтовому серверу по IP-адресу 172.16.0.40. В заголовке TCP содержится порт назначения – 110. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора. Убедитесь, что это так. Когда пакет приходит на сервер, тот обрабатывает его и формирует пакет-ответ (рис. 4.21).

Пакет по тому же маршруту возвращается на узел 172.16.0.100 с ответом (письмом) от сервера. Посмотрим содержимое ответа (рис. 4.22).

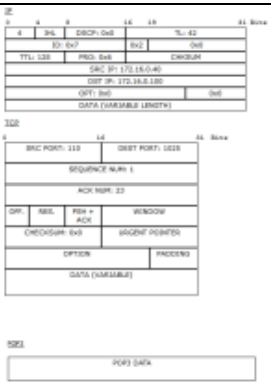


Рис. 4.22 Формат пакета POP3

Рис. 4.23 Форма чтения входящих писем

Порт-источник – 110. Ответ пришел от сервера 172.16.0.40 с некоторыми POP3-данными. С помощью протокола POP3 узел 172.16.0.100 получил письмо с сервера, отправленное туда узлом 172.16.0.90 (рис. 4.23).

Как уже упоминалось в теоретических сведениях, почтовые протоколы SMTP и POP3 обмениваются информацией с помощью команд.

Клиенту электронной почты, чтобы установить соединение с сервером, отправить письмо, разорвать соединение необходимо отправлять серверу соответствующие команды. Сервер электронной почты, в свою очередь, обрабатывает эти команды и формирует отклики для клиента. Отклики smtp-сервера содержат цифровой код ответа: успешно или с ошибкой обработана команда.

Отклики pop3-сервера так же содержат два типа сообщений: успех или ошибка.

Обращая внимание на содержимое пакета SMTP или POP3 протокола, видно, что на прикладном уровне пакет детально не рассматривается.

Поэтому эксперимент посылки письма несуществующему пользователю не является содержательным, т.к. подробно увидеть ответ от smtp-сервера нам не удастся. Для подробного изучения взаимодействия между клиентом и smtp- или pop3-сервером следует обратиться к предложенной спецификации RFC 2821 и RFC 1939.

4. Индивидуальные задания

Исследуйте прикладные протоколы электронной почты SMTP и POP3 самостоятельно. Топологию сети для исследования оставьте прежней. Настройку сетевых устройств проделайте в соответствии с вариантом.

В отчете приведите маршруты пакетов, их содержимое и объясните полученные результаты. Отправителя и получателя определите сами.

Контрольные вопросы:

1. Какова методика построения топологии сети.
2. Объясните параметры настройки сетевых устройств.
3. Какие основные параметры используются для настройки почтового сервера.
4. Каким образом выполняется исследование прикладных почтовых протоколов в режиме симуляции.
5. Как происходит отправка письма по протоколу SMTP на сервер.
6. Как происходит получение письма по протоколу POP3 от сервера.

Практическая работа № 5.

Утилиты протокола TCP/IP.

1. Цель работы: приобретение навыков и умений по работе с утилитами TCP/IP.

2. Краткая теория

2.1 Диагностические утилиты TCP/IP.

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

Таблица 2.1 Описание утилит TCP/IP

Утилита:	**Применение:**
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.

ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

2.2 Проверка правильности конфигурации TCP/IP.

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметры:

all - выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] - обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] - освобождает выделенный DHCP IP-адрес;

adapter - имя сетевого адаптера;

displaydns - выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

• если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;
• если IP-адреса дублируются, то маска сети будет 0.0.0.0;
• если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

2.3 Тестирование связи с использованием утилиты ping.

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда ping проверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение «Request time out» (Пре-

вышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Использование утилиты ping:

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address):

ping 127.0.0.1

Если тест успешно пройден, то вы получите следующий ответ:

Reply from 127.0.0.1
Reply from 127.0.0.1
Reply from 127.0.0.1
Reply from 127.0.0.1

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

ping IP-адрес_локального_хоста

3) Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес_шлюза

4) Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес_удаленного хоста

Синтаксис утилиты ping:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] |

[-k host-list]] [-w timeout] destination-list

Параметры:

-t - выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a - позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count - посылает количество пакетов ECHO, указанное параметром count;

-l length - посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f - посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl - устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos - устанавливает тип поля «сервис» в величину tos;

-r count - записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count - позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list - направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list - направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;

-w timeout - указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);

destination-list - указывает удаленный хост, к которому надо направить пакеты ping.

Пример использования утилиты ping:

C:|Documents and Settings|user>ping www.ya.ru

Обмен пакетами с ya.ru [213.180.204.8] по 32 байт:

Ответ от 213.180.204.8: число байт=32 время=1887мс TTL=53

Ответ от 213.180.204.8: число байт=32 время=1475мс TTL=53

Ответ от 213.180.204.8: число байт=32 время=1094мс TTL=53

Ответ от 213.180.204.8: число байт=32 время=736мс TTL=53

Статистика Ping для 213.180.204.8:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
Минимальное = 736мсек, Максимальное = 1887 мсек, Среднее = 1298 мсек.

2.4 Изучение маршрута между сетевыми соединениями с помощью утилиты tracert.

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP “Time Exeeded” (Время ис-

текло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

Параметры:

-d - указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops - указывает максимальное число хопов для того, чтобы искать цель;

-j host-list - указывает нежесткую статическую маршрутизацию в соответствии с host-list;

-w timeout - указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

Пример использования утилиты tracert:

C:|Documents and Settings|user>tracert www.ya.ru
Трассировка маршрута к ya.ru [213.180.204.8]
с максимальным числом прыжков 30:
1<1 мс<1 мс<1 мсmygateway1.ar7 [192.168.1.1]
216 ms15 ms23 ms192.168.229.9
316 ms16 ms16 ms192.168.224.46
*4***Превышен интервал ожидания для запроса.*
*5***Превышен интервал ожидания для запроса.*
624 ms24 ms25 ms18.224.168.192.in-addr.arpa [192.168.224.18]
7 23 ms 23 ms 23 ms 17.224.168.192.in-addr.arpa [192.168.224.17]
8 2542 ms 2577 ms 2928 ms 18.13.22.172.in-addr.arpa [172.22.13.18]
9 2189 ms 1811 ms 2016 ms 225.126.18.84.in-addr.arpa [84.18.126.225]

10 2354 ms 2193 ms 1653 ms 87.226.230.253
11 1442 ms 1361 ms 1105 ms 87.226.133.38
12 56 ms 55 ms 68 ms 87.226.233.198
13 1715 ms 2206 ms 2579 ms www.ya.ru [213.180.204.8]
Трассировка завершена

2.5 Утилита ARP.

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса (MAC-адреса). Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметры:

-s - занесение в кэш статических записей;

-d - удаление из кэша записи для определенного IP-адреса;

-a - просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;

inet_addr - IP-адрес;

eth_addr - MAC-адрес.

Пример использования утилиты ARP:

C:|Documents and Settings|user>arp -a 169.254.15.2
Интерфейс: 169.254.15.1 --- 0x2
Адрес IP Физический адрес Тип
169.254.15.2 00-19-5b-82-fb-d0 динамический

2.6 Утилита netstat.

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Синтаксис:
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]
Параметры:
-a - выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;
-e - выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);
-n - выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;
-s - выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет просмотреть информацию постранично;
-r - выводит содержимое таблицы маршрутизации.

3. Порядок выполнения работы

1.Ознакомиться с краткой теорией.

2. Выполнить следующие задания используя утилиты:

а) Получение справочной информации по командам.
Выведите на экран справочную информацию по утилитам *ipconfig*, *ping*, *tracert*, *hostname*. Для этого в командной строке введите имя утилиты без параметров или с /?. Изучите ключи, используемые при запуске утилит.
б) Получение имени хоста
Выведите на экран имя локального хоста с помощью команды *hostname*.
в) Изучение утилиты ipconfig

Проверьте конфигурацию TCP/IP с помощью утилиты *ipconfig*.

3.Оформить отчет по лабораторной работе, описав выполнение упражнений и приложив скриншоты к отчету.

Контрольные вопросы

1.Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?

2.Каким образом команда ping проверяет соединение с удаленным хостом?

3.Что такое хост, функциональное назначение?

4.Что такое петля обратной связи?

5.Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?

6.Как работает утилита tracert?

7.Каково назначение протокола ARP?

Практическая работа №6.

Настройка сети в операционной системе Windows

1. Цель работы: экспериментальное исследование сетевого конфигурирования в операционной системе MS Windows**.**

Задачи работы:

1. Ознакомиться с компонентом «Центр управления сетями и общим доступом».
2. Разобраться с понятием «Сетевое расположение».
3. Ознакомиться с компонентом «Карта сети».
4. Ознакомиться с сетевыми компонентами операционной системы, необходимыми для подключения компьютера к локальной или внешней сети.
5. Подготовить отчет о проделанной работе.

2. Краткие теоретические сведения

Зачастую, настройка локальной сети в операционных системах Windows Vista, Windows 7, Windows Server 2008/2008 R2 начинается с такой области конфигурирования сетевых свойств, как компонент «Центр управления сетями и общим доступом». При помощи данного средства конфигурирования сетей можно выбирать сетевое размещение, просматривать карту сети, настраивать сетевое обнаружение, общий доступ к файлам и принтерам, а также настраивать и просматривать состояние ваших текущих сетевых подключений.

2.1 Центр управления сетями и общим доступом

Для того чтобы воспользоваться функционалом средства конфигурирования сетей, нужно для начала его открыть. Чтобы открыть окно «Центр управления сетями и общим доступом», выполните одно из следующих действий:

- В области уведомлений нажмите правой кнопкой мыши на значке «Сеть» и из контекстного меню выберите команду «Центр управления сетями и общим доступом»;
- Нажмите на кнопку «Пуск» для открытия

меню, выделите элемент «Сеть» и нажмите на нем правой кнопкой мыши. Из контекстного меню выберите команду «Свойства»;

- Нажмите на кнопку «Пуск» для открытия меню, откройте «Панель управления», из списка компонентов панели управления выберите категорию «Сеть и Интернет», а затем перейдите по ссылке «Центр управления сетями и общим доступом»;
- Нажмите на кнопку «Пуск» для открытия меню, в поле поиска введите Центр управления и в найденных результатах откройте приложение «Центр управления сетями и общим доступом»;
- Воспользуйтесь комбинацией клавиш +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите %windir%\system32\control.exe /name Microsoft.NetworkAndSharingCenter и нажмите на кнопку «ОК».

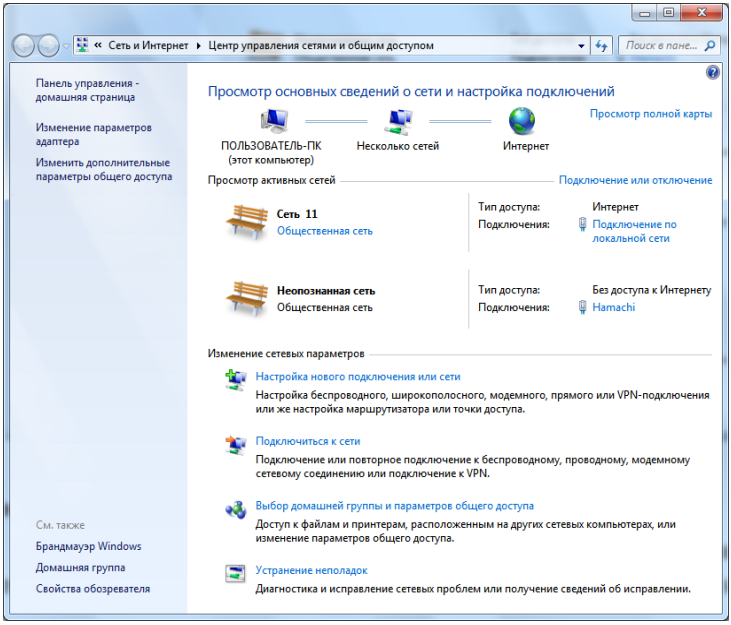


Рис.6.1 – «Центр управления сетями и общим доступом»

2.2 Понятие сетевого расположения

Перед началом работы с данным компонентом, следует разобраться с таким понятием как сетевое расположение. Этот параметр задается для компьютеров при первом подключении к сети и во время подключения автоматически настраивается брандмауэр и параметры безопасности для того типа сети, к которому производится подключение. В отличие от операционной системы Windows Vista, где для всех сетевых подключений используется самый строгий профиль брандмауэра для сетевого размещения, операционная система Windows 7 и более поздние версии поддерживает несколько активных профилей, что позволяет наиболее безопасно использовать несколько сетевых адаптеров, подключенных к различным сетям. Существует четыре типа сетевого расположения (рис.6.2).

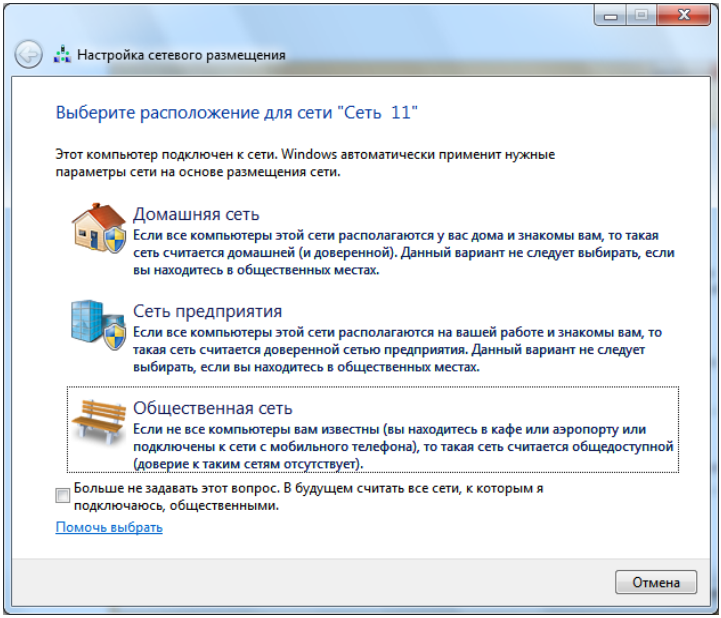


Рис.6.2 – Выбор сетевого расположения

Домашняя сеть. Данное сетевое расположение предназначено для использования компьютера в домашних условиях или в таких сетях, где пользователи очень хорошо знают друг друга.

Такие компьютеры могут создавать и присоединяться к домашним группам. Для домашних сетей автоматически включается обнаружение сети.

Сеть предприятия. Такое сетевое расположение используется в сети малого офиса (SOHO). Для этого сетевого расположения также включено обнаружение сети, но вы не можете ни создавать, ни присоединять компьютер к домашней группе.

Общественная сеть. Это сетевое расположение предназначено для использования компьютера в таких общественных местах, как кафе или аэропорты. Это наиболее строгое размещение, у которого по умолчанию отключены возможности присоединения к домашней группе и сетевое обнаружение.

Доменная сеть. Если компьютер присоединён к домену Active Directory, то существующей сети будет автоматически назначен тип сетевого размещения «Домен». Доменный тип сетевого расположения аналогичен рабочей сети, за исключением того, что в домене конфигурация брандмауэра Windows, сетевого обнаружения, а также сетевой карты определяется групповой политикой. Каким образом связаны компьютеры в сети, можно просматривать с помощью карты сети. Однако этот компонент доступен не для всех типов сетевого расположения.

2.3 Карта сети

Карта сети – это графическое представление расположения компьютеров и устройств, которое позволяет увидеть все устройства вашей локальной сети, а также схему их подключения друг к другу. В окне «Центр управления сетями и общим доступом» отображается только локальная часть сетевой карты, компоновка которой зависит от имеющихся сетевых подключений. Компьютер, на котором выполняется создание карты, отображается в левом верхнем углу. Другие компьютеры подсети отображаются слева. Такие устройства инфраструктуры, как коммутато-

ры, концентраторы и шлюзы в другие сети отображаются справа. Сетевое сопоставление работает в проводных и беспроводных сетях, однако, только в частных и доменных сетях. Просмотреть карту публичной сети невозможно. Протокол LLTD обеспечивает сопоставление только компьютеров в одной подсети, которая является обычной установкой в домашних или малых офисах.

Рис. 6.3 – Пример карты сети

Можно заметить, что некоторые компьютеры и устройства отображаются отдельно в нижней части окна «Карта сети» либо могут вообще отсутствовать. Например, если сервер печати беспроводной сети поддерживает технологию UPnP, а не LLTD, то он будет располагаться в нижней части окна «Карта сети». Подобная ситуация возникает, поскольку не все операционные системы и устройства предполагают поддержку протокола LLTD или вследствие возможной неправильной настройки устройств (рис.1.3).

За работу карты сети в операционных системах отвечают два компонента:

- Обнаружение топологии связи Link Layer (Link Layer Topology Discover Mapper – LLTD Mapper) – компонент, который запрашивает в сети устройства для включения их в карту;
- Отвечающее устройство LLTD (Link Layer Topology Discover Responder – LLTD Responder) – компонент, который отвечает за запросы компонента LLTD Mapper.

По умолчанию, карту сети можно просматривать только для расположений «Домашняя сеть» или «Сеть предприятия». При попытке просмотра сетевой карты для расположений «Доменная сеть» или «Общественная сеть» вы увидите сообщение о невозможности отображения карты.

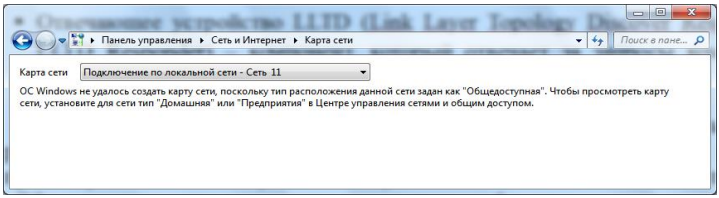


Рис.6.4 – Попытка просмотра карты сети

Для того чтобы включить сетевое сопоставление в доменной сети, вам нужно на контроллере домена выполнить следующие действия:

1. Откройте оснастку «Управление групповой политики»;
2. Выберите объект групповой политики (например, Default Domain Policy, область действия – весь домен), который будет распространяться на компьютер, расположенный в доменной сети, нажмите на нем правой кнопкой мыши и из контекстного меню выберите команду «Изменить»;
3. В оснастке «Редактор управления групповыми политиками» разверните узел Конфигурация компьютера/Политики/Административные шаблоны/Сеть/Обнаружение топологии связи (Link Layer) и выберите политику «Включает драйвер отображения ввода/вывода (LLTDIO)»;
4. В свойствах параметра политики установите переключатель на опцию «Включить» и установите флажок «Разрешить операцию для домена»;
5. Повторите аналогичные действия для параметра политики «Включить драйвер «Ответчика» (RSPNDR)»;
6. Обновите параметры политики на клиентской машине, используя команду gpupdate /force /boot;
7. Обновите карту сети.

2.4 Сетевые подключения

После установки драйвера для каждого сетевого адаптера, операционная система Windows пытается автоматически сконфигурировать сетевые подключения на локальном компьютере. Все доступные сетевые подключения отображаются в окне «Сетевые подключения». Сетевое подключение представляет собой набор данных, необходимых для подключения компьютера к Интернету,

локальной сети или любому другому компьютеру.

Открыть окно «Сетевые подключения» вы можете любым из следующих способов:

- Откройте окно «Центр управления сетями и общим доступом» и перейдите по ссылке «Изменение параметров адаптера»;
- Нажмите на кнопку «Пуск» и в поле поиска введите Просмотр сетевых и в найденных результатах откройте приложение «Просмотр сетевых подключений»;
- Воспользуйтесь комбинацией клавиш +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите ncpa.cpl или control netconnection и нажмите на кнопку «ОК».

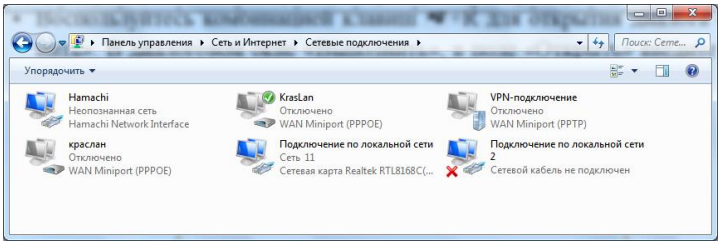


Рис. 6.5 – Окно «Сетевые подключения»

При выборе любого сетевого подключения вы можете выполнить с ним следующие действия:

- **Переименование подключения.** Операционная система по умолчанию назначает всем сетевым подключениям имена «Подключение по локальной сети» или «Подключение к беспроводной сети» и номер подключения в том случае, если у вас существует более одного сетевого подключения. При желании, вы можете переименовать любое сетевое подключение одним из трех следующих способов:
  - Нажмите на клавишу F2, введите новое имя сетевого подключения, после чего нажмите на клавишу Enter;
  - Нажмите правой кнопкой мыши на переименовываемом сетевом подключении и из контекстного меню выберите команду «Переименовать». Введите новое имя сетевого подключения, после чего нажмите на клавишу Enter;

- Выберите сетевое подключение и нажмите на кнопку «Переименование подключения», которая расположена на панели инструментов. После чего введите новое имя сетевого подключения и нажмите на клавишу Enter.

- **Состояние сети.** Используя данное окно, вы можете просмотреть любые данные о состоянии сетевого подключения и такие детали, как IP-адрес, MAC-адрес и прочее. Чтобы открыть диалоговое окно сведений о сетевом подключении, выполните следующие действия:

1. Откройте диалоговое окно «Состояние» одним из следующих способов:
   - Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Состояние»;
   - Выберите сетевое подключение и нажмите на кнопку «Просмотр состояния подключения», которая расположена на панели инструментов;
   - Выберите сетевое подключение и нажмите на клавишу Enter.

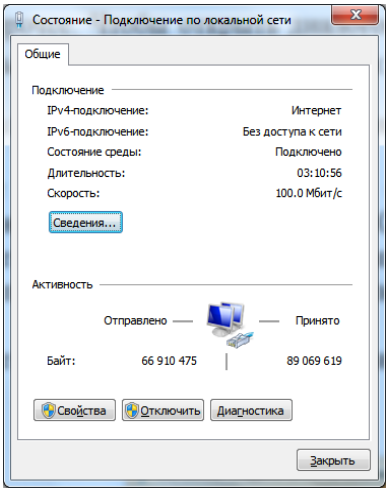


Рис. 6.6 Окно состояния подключения по локальной сети

2. В окне «Состояние – подключение по локальной сети» нажмите на кнопку «Сведения». В диалоговом окне «Сведения о сетевом подключении», отображенном ниже, вы можете просмотреть подробные сведения о текущем сетевом подключении.

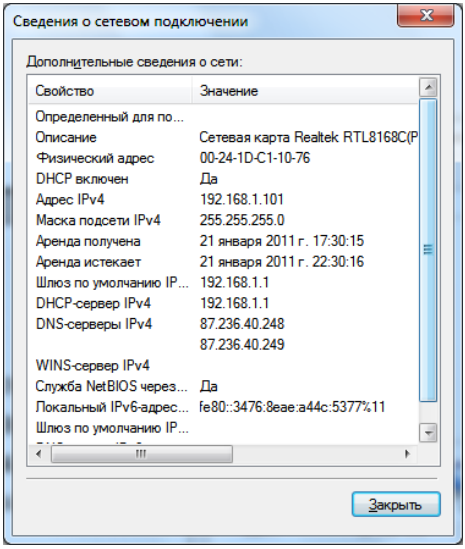


Рис. 6.7 – Сведения о сетевом подключении

- **Диагностика подключения.** В случае обнаружения проблем в работе вашего сетевого подключения, окно «Сетевые подключения» предлагает средство диагностики «Устранение неполадок», которое содержит возможность решения при помощи анализа подключения. Для того чтобы воспользоваться данным средством выполните любое из следующих действий:

    - Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Диагностика».
    - Выберите сетевое подключение и нажмите на кнопку «Диагностика подключения», которая расположена на панели инструментов.

В открывшемся диалоговом окне «Диагностика сетей Windows» для устранения неполадок следуйте действиям мастера.

- **Отключение сетевого устройства.** Иногда проблемы с сетевыми подключениями решаются посредством отключения сетевого адаптера компьютера от сети. Для того чтобы отключить сетевой адаптер выполните одно из следующих действий:
  - Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Отключить»;
  - Выберите сетевое подключение и нажмите на кнопку «Отключение сетевого устройства», которая расположена на панели инструментов.

- **Настройка параметров подключения.** Как таковые, сетевые подключения не позволяют осуществлять коммуникации. Осуществление коммуникаций обеспечивают сетевые клиенты, службы и протоколы, которые привязаны к созданным сетевым подключениям (рис.6.9.).

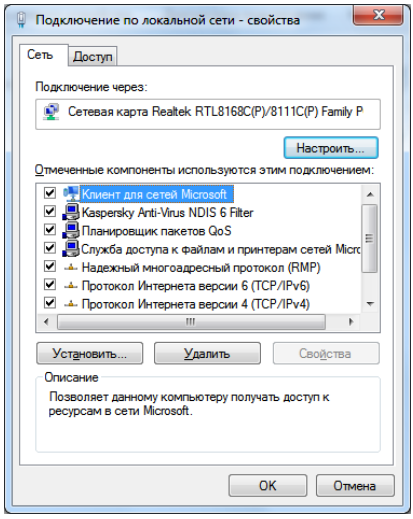


Рис. 6.9 – Диалоговое окно свойств сетевого подключения

Для того чтобы изменить настройки вашего сетевого подключения, вы можете воспользоваться средствами настройки параметров подключения. Для изменения компонентов и настроек сетевого подключения, выполните следующие действия:

- Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Свойства»;
- Выберите сетевое подключение и нажмите на кнопку «Настройка параметров подключения», которая расположена на панели инструментов;
- Выберите сетевое подключение и воспользуйтесь комбинацией клавиш Alt + Enter.

Установленные возле компонентов флажки указывают, что эти компоненты привязаны к подключению. Таким образом, в рамках выполнения данной лабораторной работы были рассмотрены средства конфигурирования сетевых свойств операционных систем Windows – «Центр управления сетями и общим доступом».

Контрольные вопросы

1. Какое назначение у компонента «Центр управления сетями и общим доступом»?
2. Охарактеризуйте типы сетевого расположения.
3. Что представляет собой карта сети, по сути, и по виду?
4. Какие протоколы отвечают за построение карты сети.
5. В каких ситуациях просмотр карты сети будет не возможен?
6. С каким аппаратным сетевым компонентом связываются свойства доступных сетевых подключений?
7. Какие действия пользователь обычно может выполнить по отношению к любому сетевому подключению?
8. Какими способами можно вызвать средства диагностики подключения?
9. Охарактеризуйте компоненты подключения к сети компьютера, за которым вы выполняете лабораторную работу.

Практическая работа №7.

Сетевые клиенты, службы и протоколы

1. Цель работы: исследовать назначение сетевых клиентов, служб и протоколов – компонентов системы, которые привязаны к сетевым подключениям, позволяющие осуществлять коммуникации.

Задачи работы:

1. Получить представление о свойствах клиентов для сетей Microsoft.
2. Разобраться с назначением сетевых служб.
3. Теоретически ознакомиться с протоколами, реализующими сетевое взаимодействие.
4. Подготовить отчет о проделанной работе.

2. Краткие теоретические сведения

2.1 Сетевые клиенты

По определению, сетевой клиент – это компьютер или программное обеспечение, у которого есть доступ к услугам сервера, а также получающее или обменивающееся с ним информацией. В операционных системах Windows сетевые клиенты представляют собой компоненты программного обеспечения, которые позволяют локальному компьютеру подключаться к сетям отдельных операционных систем. Наряду со всеми подключениями по локальным сетям в системах Windows, сетевым клиентом по умолчанию является компонент **«Клиенты для сетей Microsoft»**. Данный компонент позволяет подключаться к общим ресурсам на других компьютерах, оснащенных операционной системой Windows (рис.7.1). По умолчанию, данный сетевой клиент не нуждается в дальнейшей настройке. Однако, если вы захотите изменить настройки клиента для сетей Microsoft, установленные по умолчанию, выполните следующие действия:

1. Откройте диалоговое окно свойств подключения к сети;
2. На вкладке **«Общие»**, в списке **«Отмеченные компоненты используются этим подключением»** выберите службу **«Клиент для сетей Microsoft»** и нажмите на кнопку **«Свойства»** (в случае подключения по виртуальной частной сети (VPN) вам нужно перейти на вкладку **«Сеть»**);
3. В диалоговом окне **«Свойства: Клиент для сетей Windows»** вы можете изменить поставщика службы имен и сетевой адрес для службы удаленного вызова процедур (Remote Procedure Call (RPC)). RPC – это класс технологий, позволяющий компьютерным программам вызывать функции или процедуры в другом адресном пространстве. Идея вызова удалённых процедур состоит в расширении хорошо известного и понятного механизма передачи управления и данных внутри программы, выполняющейся на одной машине, на передачу управления и данных через сеть. Средства удалённого вызова процедур предназначены для облегчения организации распределённых вычислений и создания распределенных клиент-серверных информационных систем. Наибольшая эффективность использования RPC достигается в тех приложениях, в которых существует интерактивная связь между удалёнными компонентами с небольшим временем ответов и относительно малым количеством передаваемых данных.

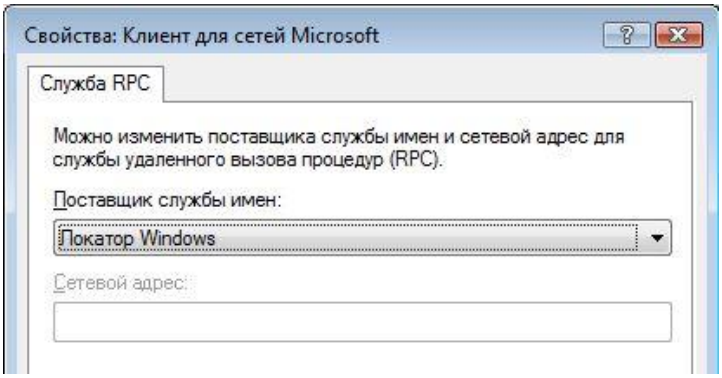


Рис. 7.1. Свойства сетевого клиента «Клиент для сетей Microsoft»

Из раскрывающегося списка **«Поставщик службы имен»** доступны поставщики **«Локатор Windows»**, который является поставщиком служб имен по умолчанию, а также **«Служба каталогов ячеек DCE»**, которую нужно использовать только в том случае, если в сети используется программное обеспечение компании The Open Group, например клиент или сервер DCE (Distributed Computing Environment). В этом случае, вам нужно будет в поле «Сетевой адрес» ввести сетевой адрес поставщика служб имен. Если сетевой клиент вообще не допускает настроек, кнопка **«Свойства»** будет пригашена.

2.2 Сетевые службы

Также как и сетевые клиенты, сетевые службы являются компонентами операционной системы. Сетевые службы операционных систем Windows – это специальные процессы, которые создают прослушивающий сокет и привязывают его к определенному порту, обеспечивающие дополнительную функциональность для сетевых подключений. Системные службы запускаются операционной системой автоматически в процессе загрузки компьютера или по мере необходимости при выполнении стандартных операций. Понятное имя службы отображается в оснастке **«Службы»**, а настоящее имя службы используется в программах с интерфейсом командной строки. По умолчанию в операционных системах Microsoft ко всем локальным подключениям привязаны две сетевые службы:

- **Служба доступа к файлам и принтерам сетей Microsoft**. Данная служба позволяет другим компьютерам, расположенным в одной сети с вами, обращаться к ресурсам данного компьютера по сети.
- **Планировщик пакетов QoS**. Эта служба содержит набор стандартов и механизмов, предназначенных для обеспечения производительности для важных приложений. Обычно механизм QoS используется для настройки приоритетов и управления скоростью отправки исходящего сетевого трафика. Начиная с операционных систем

Windows Vista и Windows Server 2008, службы QoS настраиваются при помощи групповых политик.

2.3 Сетевые протоколы

Основной составляющей коммуникаций сетевых подключений являются протоколы. Протоколами называются 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.

Протоколы TCP/IP — это два протокола нижнего уровня, являющиеся основой связи в сети Интернет. Протокол TCP (Transmission Control Protocol) разбивает передаваемую информацию на порции и нумерует их. С помощью протокола IP (Internet Protocol) все части передаются получателю. Данные протоколы основаны на модели OSI и функционируют на более низком уровне, чем прикладные протоколы. Концепция уровней модели TCP/IP (многослойной сетевой модели) позволяет заменять отдельные протоколы на одном уровне другими протоколами, совместимыми на соседних уровнях протоколами. На рис.2.2 отображен стек (совокупность протоколов) протоколов TCP/IP:

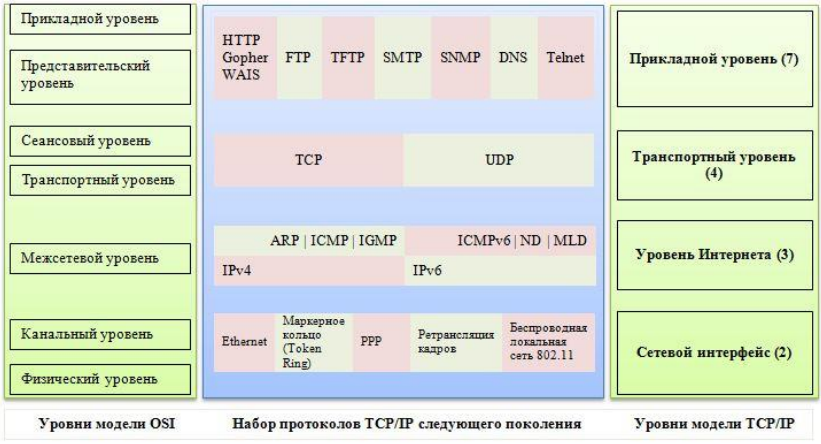


Рис. 7.2. Уровни модели стека TCP/IP

Рассмотрим подробно каждый из четырех уровней модели TCP/IP:

Уровень сетевого интерфейса (уровень 2). Данный уровень содержит протоколы, которые обеспечивают передачу данных между узлами связи, физически напрямую соединенными друг с другом. Другими словами, осуществляют коммуникацию

для сетевых адаптеров и физических (MAC) адресов, которые назначены для этого адаптера, концентраторов, коммутаторов и пр. Существующие стандарты определяют, каким образом должна осуществляться передача данных семейства TCP/IP с использованием этих протоколов. К этому уровню относятся протоколы Ethernet, маркерное кольцо Token Ring, SLIP, PPP и прочее.

Уровень Интернета (уровень 3). Этот уровень обеспечивает доставку информации от сетевого узла отправителя к сетевому узлу получателя без установления виртуального соединения с помощью датаграмм и не является надежным. Основным протоколом данного уровня является IP (Internet Protocol). Вся информация, поступающая к нему от других протоколов, оформляется в виде IP-пакетов данных (IP datagrams). На этом уровне был реализован стек TCP/IP. На уровне 3 в стеке TCP/IP используются две версии протокола Интернета:

- **IPv4**. В современной сети Интернет используется IP четвёртой версии, также известный как маршрутизируемый сетевой протокол IPv4. В протоколе IP этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 32 бита (4 октета). При этом компьютеры в подсетях объединяются общими начальными битами адреса. В связи с тем, что количество адресов ограничено, вскоре может быть дефицит IPv4 адресов.
- **IPv6**. Шестая версия протокола — IPv6 позволяет адресовать значительно большее количество узлов, чем IPv4. Протокол Интернета версии 6 отличается повышенной разрядностью адреса и использует 128-разрядные адреса, и может определить значительно больше адресов.

Также на данном уровне оперирует физическое устройство – маршрутизатор, который блокирует физическое широковещание сообщений сети, вычитывает программный адрес, а затем перенаправляет этот адрес по соответствующему пути.

Транспортный уровень (уровень 4). Транспортный уровень модели TCP/IP предназначен для отправки и получения данных. В набор данного уровня входят два протокола – TCP и UDP. Рассмотрим подробно каждый из них:

- **TCP**. Реализует потоковую модель передачи информации с прикладного уровня, а также ее обработку побайтно. Получившиеся байты группируются TCP в пронумерованные сегменты последовательности для доставки на сетевой хост. Протокол TCP обеспечивает проверку контрольных сумм, передачу подтверждения в случае правильного приема сообщения, повторную передачу пакета данных в случае неполучения подтверждения в течение определенного промежутка времени, правильную последовательность получения информации, полный контроль скорости передачи данных.
- **UDP**. Данный протокол наоборот, является способом связи ненадежным, ориентированным на передачу сообщений (датаграмм). Данный протокол позволяет быстро транспортировать датаграммы, поскольку в нем не предусмотрены такие компоненты надежности, как гарантии доставки и подтверждение последовательности передачи. В связи с этим, данные для приложений доставляются гораздо быстрее.

Прикладной уровень (уровень 7). Данный, последний, уровень модели TCP/IP осуществляет упаковку и передачу данных через порты транспортного уровня. К этому уровню можно отнести протоколы TFTP (Trivial File Transfer Protocol), FTP (File Transfer Protocol), Telnet, SMTP (Simple Mail Transfer Protocol), HTTP, DNS, POP3 (Post Office Protocol 3) и другие, которые поддерживаются соответствующими системными утилитами.

2.4 История стека TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP)- это промышленный стандарт стека протоколов, разработанный для

глобальных сетей. Стандарты TCP/IP опубликованы в серии документов, названных Request for Comment (RFC). Документы RFC описывают внутреннюю работу сети Internet. Некоторые RFC описывают сетевые сервисы или протоколы и их реализацию, в то время как другие обобщают условия применения. Стандарты TCP/IP всегда публикуются в виде документов RFC, но не все RFC определяют стандарты.

Стек был разработан по инициативе Министерства обороны США (Department of Defence, DoD) более 20 лет назад для связи экспериментальной сети ARPAnet с другими сателлитными сетями как набор общих протоколов для разнородной вычислительной среды. Сеть ARPA поддерживала разработчиков и исследователей в военных областях. В сети ARPA связь между двумя компьютерами осуществлялась с использованием протокола Internet Protocol (IP), который и по сей день является одним из основных в стеке TCP/IP и фигурирует в названии стека.

Большой вклад в развитие стека TCP/IP внес университет Беркли, реализовав протоколы стека в своей версии ОС UNIX. Широкое распространение ОС UNIX привело и к широкому распространению протокола IP и других протоколов стека. На этом же стеке работает всемирная информационная сеть Internet, чье подразделение Internet Engineering Task Force (IETF) вносит основной вклад в совершенствование стандартов стека, публикуемых в форме спецификаций RFC.

Лидирующая роль стека TCP/IP объясняется следующими его свойствами:

- Почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP.
- Это метод получения доступа к сети Internet.
- Этот стек служит основой для создания intranet- корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW.
- Все современные операционные системы поддерживают стек TCP/IP.

- Это гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов.
- Это устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.

Контрольные вопросы

1. Дайте определение понятию сетевой клиент.
2. Какими потенциальными возможностями обладает сетевой клиент?
3. Охарактеризуйте служюу удаленного вызова процедур?
4. Задачи Сетевых служб операционных систем Windows?
5. Какие службы в операционных системах Microsoft по умолчанию привязаны ко всем локальным подключениям?
6. Охарактеризуйте модель для сетевых протоколов.
7. Проведите соответствие провести между стеком протоколов TCP/IPи моделью OSI?
8. Выделите различия между адресами IPv4 иIPv6.
9. Какие документы описывают стандарт стека протоколов?
10. Какими свойствами обладает стек TCP/IP?

Практическая работа №8.

Управление параметрами общего доступа

1. Цель работы: научиться настраивать общие папки, для организации общего доступа к файлам и папкам для компьютеров, которые расположены в одной локальной группе или в одном домене.

Задачи работы:

1. Изучить настройки параметров общего доступа.
2. Выполнить настройки параметров общего доступа.
3. Подготовить отчет о проделанной работе.

2. Краткие теоретические сведения

При работе с домашней локальной сетью или с компьютерами интрасети организации вам придется настраивать общие папки, так как, вероятнее всего, что ваши пользователи захотят разрешать сотрудникам просматривать, изменять и создавать файлы и папки для компьютеров, которые расположены в одной локальной группе или в одном домене. В связи с тем, что для открытия общего доступа нужны права администратора, не всем пользователям вашей сети будет предоставлена такая возможность. Но после того как вы настроите на пользовательских компьютерах параметры общего доступа, пользователи смогут самостоятельно предоставлять доступ к своим папкам и файлам.

Для того чтобы ваши пользователи могли просматривать содержимое локальной сети и иметь доступ к компьютерам и устройствам вы можете включить сетевое обнаружение. Если к каждому компьютеру вашей сети не подключен локальный принтер, вам придется открывать общий доступ к принтерам, для того чтобы пользователи могли распечатывать свою документацию. Вы можете предоставлять общий доступ к ресурсам компьютера, как для всех пользователей, так и для тех пользователей, учетные данные которых имеются на компьютере, предоставляющем об-

щий доступ к файлам и папкам. Вы можете разрешить пользователям обмениваться музыкой, видеофайлами и картинками, разрешив общий доступ к потоковому мультимедиа и прочее.

2.1 Дополнительные параметры общего доступа

Для того чтобы открыть окно **«Дополнительные параметры общего доступа»**, окно которого приведено на рис.8.1, выполните любое из следующих действий:

- Откройте компонент **«Центр управления сетями и общим доступом»** и перейдите по ссылке **«Изменить дополнительные параметры общего доступа»**;
- Нажмите на кнопку **«Пуск»** для открытия меню, в поле поиска введите *общего доступа* и в найденных результатах откройте приложение **«Управление расширенными параметрами общего доступа»**;

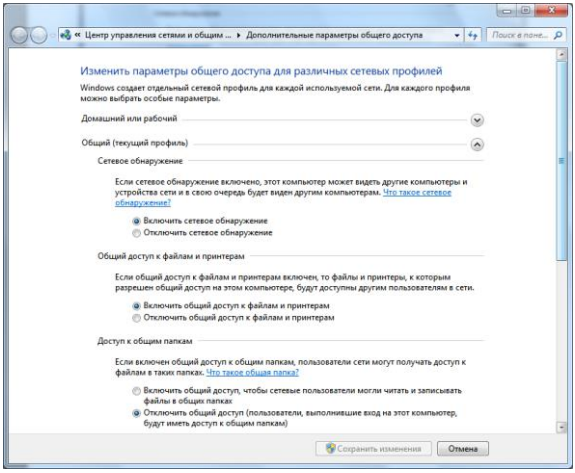


Рис.8.1. Окно «Дополнительные параметры общего доступа»

- Откройте окно **«Изменение параметров домашней группы»** и перейдите по ссылке **«Изменение дополнительных параметров общего доступа»**;

- Воспользуйтесь комбинацией клавиш +R для открытия диалога **«Выполнить»**. В диалоговом окне **«Выполнить»**, в поле **«Открыть»** введите:
  %windir%|system32|control.exe /name Microsoft.NetworkAndSharingCenter /page Advanced
  и нажмите на кнопку **«ОК»**.

2.2 Изменение параметров общего доступа

Операционная система Windows 7 поддерживает несколько активных профилей, что позволяет наиболее безопасно использовать несколько сетевых адаптеров. При помощи окна **«Дополнительные параметры общего доступа»**, вы можете указать разные настройки общего доступа для любого из трех профилей (Домашняя и рабочая сети, Доменный профиль, а также Общий профиль). Указав параметры общего доступа для каждого из профилей, они будут применяться в зависимости от того, какой сетевой интерфейс с профилем активный в данный момент.

Сетевое обнаружение – это функция для сети, которая была реализована в операционной системе Windows Vista и отвечает за параметр, определяющий, могут ли другие компьютеры в сети обнаруживать компьютер пользователя, и может ли он их видеть. Существует два параметра, отвечающих за сетевое обнаружение: **«Включить сетевое обнаружение»**, при помощи которого компьютер становится видимым для других компьютеров пользователей, и **«Отключить сетевое обнаружение»**, который запрещает просматривать другие компьютеры и делает компьютер пользователя невидимым для других компьютеров сети. По умолчанию, для профиля **«Домашний и рабочий»** данный параметр включен. В том случае, когда компьютер подключен к сети в общедоступном месте, например, в аэропорту или в кафетерии, активируется **«Общий»** профиль, в котором сетевое обнаружение по умолчанию отключено.

Для того чтобы изменить настройки сетевого обнаружения, выполните следующие действия:

- Откройте окно **«Дополнительные параметры общего доступа»**;
- Разверните сетевой профиль, для которого будут меняться настройки сетевого обнаружения, например **«Домашний или рабочий»**;
- В группе **«Сетевое обнаружение»** выберите параметр **«Включить сетевое обнаружение»** и нажмите на кнопку **«Сохранить изменения»**.

В доменном окружении по умолчанию также отключен функционал сетевого обнаружения. Для того чтобы его включить, в оснастке **«Управление групповой политикой»** создайте объект GPO, откройте редактор управления групповыми политиками, в узле **Конфигурация компьютера/Политики/Административные шаблоны/Сеть/Обнаружение топологии связи (Link Layer)**.

Выберите политику **«Включает драйвер отображения ввода/вывода (LLTDIO)»**, в ее свойствах установите значение **«Включить»** и установите флажок **«Разрешить операцию для домена»** в дополнительных параметрах свойств политики. Повторите аналогичные действия для параметра политики **«Включить драйвер «Ответчика» (RSPNDR)»**, после чего обновите параметры политики на клиентской машине, используя команду **gpupdate /force /boot**.

2.3 Общий доступ к файлам и принтерам

Если ваш компьютер находится в локальной сети, то, возможно, вы захотите предоставить некоторые файлы или папки для общего просмотра, а также дать возможность использовать ваш принтер остальным членам локальной сети. Если вы хотите, чтобы другие пользователи могли просматривать и выполнять какие-либо действия с файлами, для которых вы предоставляете общий доступ, необходимо включить данный функционал. По умолчанию, для профиля **«Домашний или рабочий»** данная возможность включена, а для профиля **«Общий»** - отключена.

Для того чтобы включить или отключить данную функцию и добавить файлы в общедоступную папку, выполните следующие действия:

1. Откройте окно **«Дополнительные параметры общего доступа»**;
2. Разверните сетевой профиль, для которого будет открыт общий доступ к файлам и принтерам, меню показано на рис.8.2, например **«Домашний или рабочий»**;
3. В группе **«Общий доступ к файлам и принтерам»** выберите параметр **«Включить общий доступ к файлам и принтерам»** и нажмите на кнопку **«Сохранить изменения»;**
4. По умолчанию, общий доступ к файлам или папкам можно предоставлять, скопировав или переместив их в папку **«Общие»**, которая находится в %USERS%\Public (%Пользователи%\Общие).

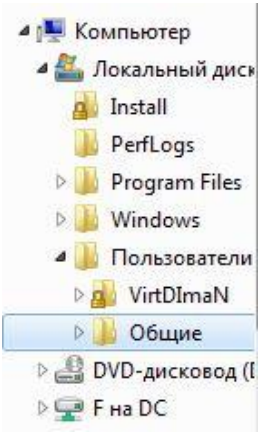


Рис.8.2 – Папка «Общие»

Также вы можете дать доступ для любой папки, расположенной на вашем компьютере и указать пользователей с различными правами, которые будут иметь к ней доступ. Для этого сделайте следующее:

1. Создайте папку, для которой будет предоставлен общий доступ, например, папку Install на диске С;
2. Откройте проводник Windows, выделите ее, нажмите на ней правой кнопкой мыши и из контекстного меню выберите команду **«Свойства»**;
3. В диалоговом окне **«Свойства: Install»** перейдите на вкладку **«Доступ»**;
4. Нажмите на кнопку **«Общий доступ»** для предоставления разрешений пользователя и группам.

Как видно на рис.8.3, в диалоговом окне **«Общий доступ к файлам»** по умолчанию владелец папки имеет к ней полный доступ и называется **«Владелец»**.

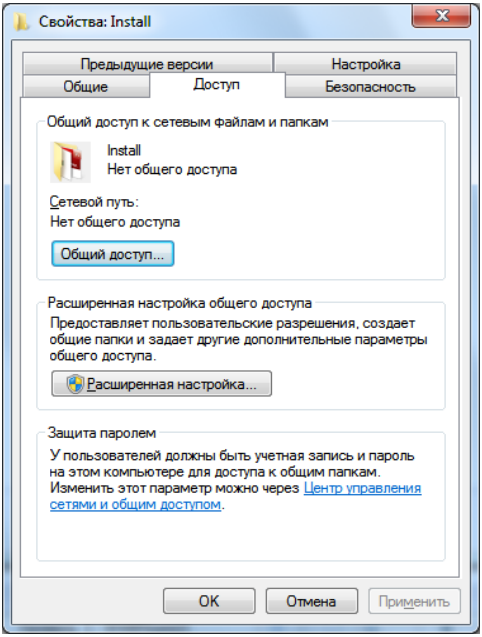


Рис.8.3 – Вкладка «Доступ» диалогового окна свойств папки

Вы можете добавить любого существующего пользователя, которые были созданы на вашем компьютере. Существующих

пользователей вы можете найти в оснастке **«Локальные пользователи и группы»**. Для примера, на компьютере VirtDImaNS был создан пользователь **«Trusted User»**.

Для предоставления пользователю доступа, в раскрывающемся списке диалогового окна **«Общий доступ к файлам»** вы можете ввести имя пользователя или выбрать его из списка и нажать на кнопку **«Добавить»**. Любому добавленному пользователю вы можете присвоить права **«Чтение»** или **«Чтение и запись»**. Если присвоен уровень разрешений **«Чтение»**, то пользователь сможет просматривать файлы из общей папки. Пользователи с правами **«Чтение и запись»** могут не только просматривать, а еще и изменять файлы, расположенные в общей папке.

Выбрав разрешения для пользователей (рис.8.4), нажмите на кнопку **«Общий доступ»**.

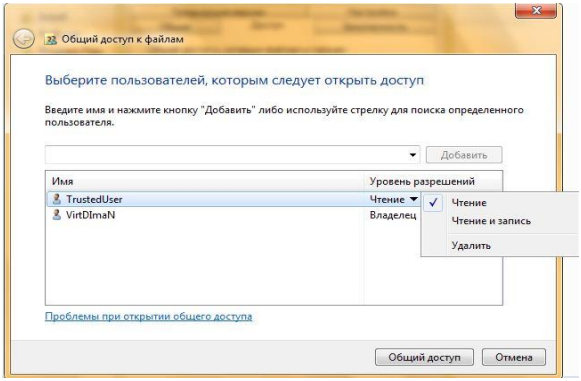


Рис. 8.4 – Диалоговое окно «Общий доступ к файлам»

5. В диалоговом окне «Папка открыта для общего доступа», нажмите на кнопку «Готово»;

6. Для предоставления дополнительных настроек для общедоступной папки, в диалоговом окне «Доступ» свойств папки, нажмите на кнопку «Расширенная настройка».

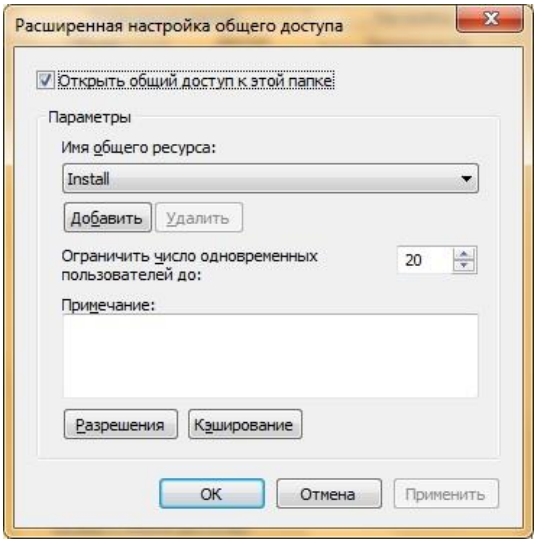


Рис. 8.5 – Расширенная настройка общего доступа папки Install

В этом диалоговом окне вы можете изменять следующие настройки:

- Изменять отображаемое имя общей папки. Для этого выберите из раскрывающегося списка **«Имя общего ресурса»** доступное имя общего ресурса или нажмите на кнопку **«Добавить»**. В диалоговом окне **«Новый общий ресурс»** введите имя и, по желанию, описание ресурса и нажмите на кнопку **«ОК»**. Для того чтобы у подключенных пользователей отображалось только указанное вами имя общего ресурса – из списка выберите оригинальное название папки и нажмите на кнопку **«Удалить»**;
- Ограничивать количество одновременных подключений к вашему общему ресурсу. Значение по умолчанию – 20 подключений. Например, если в вашей локальной сети только пять компьютеров, вы можете изменить количество пользователей, одновременно использующих ресурс;
- Настраивать разрешения для папки и настройки автономного режима.

7. По окончанию настроек общего доступа для папки Install (рис.8.5), нажмите на кнопку «Закрыть»;
8. На другом компьютере локальной сети откройте проводник Windows и в панели навигации выберите «Сеть». Из списка доступных компьютеров, выберите компьютер, папку которого вы открывали для использования общего доступа (в этом примере - VirtDImaNS).

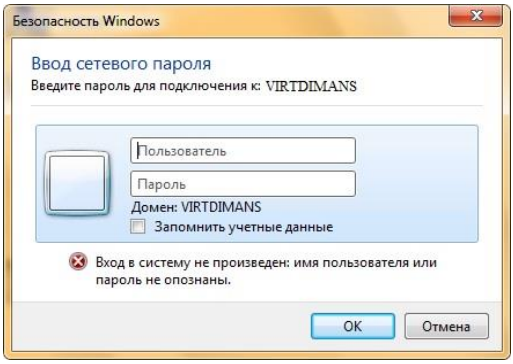


Рис.8.6 – Окно запроса учетных данных

В диалоговом окне «Безопасность Windows» введите имя пользователя и пароль для его учетной записи для доступа к общим папкам компьютера (рис.8.6).

Общие папки будут отображены в проводнике Windows, как показано на рис.8.7.

Рис. 8.7 – Общедоступные папки

2.4 Доступ к общим папкам

Как было указано выше, наряду с папками пользовательских учетных записей, операционная система Windows создает

папку *«Общие»*, общий доступ для которой открыт по умолчанию для профиля *«Домашний и рабочий»*. При помощи окна *«Дополнительные параметры общего доступа»* вы можете запретить доступ к данной папке. Для этого выполните следующие действия:

1. Откройте окно *«Дополнительные параметры общего доступа»*;
2. Разверните сетевой профиль, для которого будет открыт общий доступ к файлам и принтерам, например *«Домашний или рабочий»*;
3. В группе *«Доступ к общим папкам»* выберите опцию *«Отключить общий доступ».*

Следует учесть, что у пользователей, которые уже успели подключиться к данной папке, все еще будет доступ для использования ресурсов, которые в ней расположены.

2.4.1 Потоковая передача мультимедиа

При помощи параметров потоковой передачи мультимедиа для компьютеров и устройств, вы можете устанавливать разрешения для папок с музыкой, видео файлами и изображениями, которые будут доступны для передачи в потоковом режиме на устройства и компьютеры в сети в *«Проигрывателе Windows Media»*. Для настройки данных параметров вам нужно перейти по ссылке *«Выберите параметры потоковой передачи мультимедиа»* в группе *«Потоковая передача мультимедиа»* окна *«Дополнительные параметры общего доступа».*

2.4.2 Подключение общего доступа к файлам

При помощи параметров, расположенных в данной группе, вы можете указать тип шифрования для защиты подключения общего доступа. Шифрование применяется для обеспечения защиты файлов и папок, предоставленных для общего доступа. Операционная система Windows 7 предоставляет два алгоритма для шифрования подключений:

- 40-битное или 56-битное шифрование – DES (Data Encryption Standard). Это симметричный алгоритм шифрования, в котором один ключ используется как для шифрования, так и для расшифрования данных. DES разработан фирмой IBM и утвержден правительством США в 1977 году как официальный стандарт;
- 128-битное шифрование – Advanced Encryption Standard (AES). Это также симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES.

Значение по умолчанию для всех профилей – 128-битное шифрование для защиты подключений общего доступа.

2.4.3 Общий доступ с парольной защитой

В целях безопасности, по умолчанию доступ к общим папкам защищен паролем. Для получения доступа к пользовательским общим папкам и файлам на другом компьютере необходимо ввести соответствующие данные своей учетной записи. Этот метод используется для разрешения доступа лишь к указанному набору ресурсов.

Метод предоставления доступа к файлам и папкам обычно используется в том случае, если одним пользователям разрешен доступ к одному набору общих ресурсов, а другим открыт полный доступ. Для того чтобы отключить доступ с парольной защитой (что в принципе на предприятиях делать крайне не желательно), выполните следующие действия:

1. Откройте окно «Дополнительные параметры общего доступа»;
2. Разверните сетевой профиль, для которого будет открыт общий доступ к файлам и принтерам, например «Домашний или рабочий»;

3. В группе «Общий доступ с парольной защитой» выберите опцию «Отключить общий доступ с парольной защитой» и нажмите на кнопку «Сохранить изменения».

2.5 Подключения домашней группы

Как вам известно, создавать и присоединяться к существующей домашней группе появляется возможность только в том случае, если расположением активного сетевого интерфейса является **«Домашняя сеть»**. Параметры подключения домашней группы в окне настроек дополнительных параметров общего доступа доступны только для профиля **«Домашний и рабочий»**. Для организации общего доступа к файлам в домашней группе существуют два параметра: **«Разрешить Windows управлять подключениями домашней группы»**- при помощи которого, операционная система самостоятельно обеспечивает предоставление общего доступа для компьютеров, которые состоят в данной группе. Не исключена такая ситуация, когда еще до создания домашней группы на ваших компьютерах были созданы разрешения общего доступа, и вам хотелось бы их сохранить для последующего использования в домашней группе. Параметр **«Использовать учетные записи пользователей и пароли для подключения к другим компьютерам»** позволяет отобразить диалог запроса учетных данных при обращении к компьютеру.

Для изменения параметров подключения домашней группы, выполните следующие действия:

1. Откройте окно **«Дополнительные параметры общего доступа»**;
2. Разверните сетевой профиль, для которого будет открыт общий доступ к файлам и принтерам, например **«Домашний или рабочий»**;
3. В группе **«Подключение домашней группы»** выберите опцию соответствующего параметра и нажмите на кнопку **«Сохранить изменения»**.

Таким образом в этом разделе цикла лабораторных работ был описан функционал дополнительных параметров общего доступа. Вы научились изменять сетевое расположение в зависимости от использования сетевого профиля, узнали о способах предоставления общего доступа к файлам и папкам с использованием парольной защиты и без нее, вспомнили о настройках параметров потоковой передачи мультимедиа, немного узнали о методах шифрования сетевых подключений и научились изменять настройки подключения домашней группы. Оперируя полученными знаниями, вы сможете эффективно настраивать общий доступ к файлам и папкам в домашней среде и среде малого офиса.

Контрольные вопросы

1. Опишите функции «Сетевого обнаружения».
2. Какие особенности функционала сетевого обнаружения существуют в доменном окружении?
3. В каком случае доступ к файлам и папкам можно организовать по умолчанию?
4. Приведите примеры различных видов доступа для различных пользователей.
5. Что представляют собой дополнительные настройки для папок открытого доступа?
6. Опишите ситуацию подключения к общим папкам пользователей компьютеров сети.
7. Для чего и каким образом настраивается потоковая передача мультимедиа?
8. Опишите алгоритмы шифрования для подключений, которые предоставляет операционная система Windows 7 .
9. В каких ситуациях целесообразно назначать доступ с парольной защитой, и какие особенности настройки при этом возникают?
10. Каким образом настраивается доступ к файлам и папкам для домашней группы?

Практическая работа №9.

Параметры управления общими папками

1. Цель работы: ознакомиться с системой доступа к папкам в ОС Windows и приобрести навыки по настройке доступа.

Задачи работы:

1. Изучить возможности оснастки «Общие папки».
2. Изучить технологии организации общего доступа к папкам.
3. Рассмотреть ситуации разрешений для общих папок.
4. Подготовить отчет о проделанной работе.

2. Краткие теоретические сведения

Как в домашних условиях, так и в корпоративной среде, на ваших компьютерах может быть предоставлен общий доступ к десяткам папок. Назначив для каждой папки специфические разрешения, вскоре вы можете запутаться в предоставленных правах для своих папок. Целесообразнее управлять общими папками на компьютере при помощи оснастки консоли управления Microsoft **«Общие папки»**. Именно при помощи оснастки **«Общие папки»**, вы можете создавать общие ресурсы, а также устанавливать всевозможные разрешения для таких ресурсов. Помимо этого, вам предоставляется возможность просматривать и отключать открытые файлы и сеансы пользователей, подключенных к вашим общим ресурсам. Также вы можете настраивать доступ к своим папкам в автономном режиме, управлять ограничением числа пользователей, которые могут одновременно получить доступ к вашим ресурсам и многое другое. В этой лабораторной работе вы узнаете не только об интерфейсе оснастки **«Общие папки»**, но и выполнении аналогичных действий средствами командной строки при помощи команд net share, net files и net session.

2.1 Открытие оснастки «Общие папки»

К сожалению, средство управления общими папками нельзя открыть из панели управления. Вы можете открыть оснастку управления общими папками любым из следующих способов:

- Воспользуйтесь комбинацией клавиш +R для открытия диалога **«Выполнить»**. В диалоговом окне **«Выполнить»**, в поле **«Открыть»** введите *fsmgmt.msc* и нажмите на кнопку **«ОК»**.
- Откройте **«Консоль управления ММС»**. Для этого нажмите на кнопку **«Пуск»**, в поле поиска введите mmc (рис.9.1), а затем нажмите на кнопку **«Enter»**.

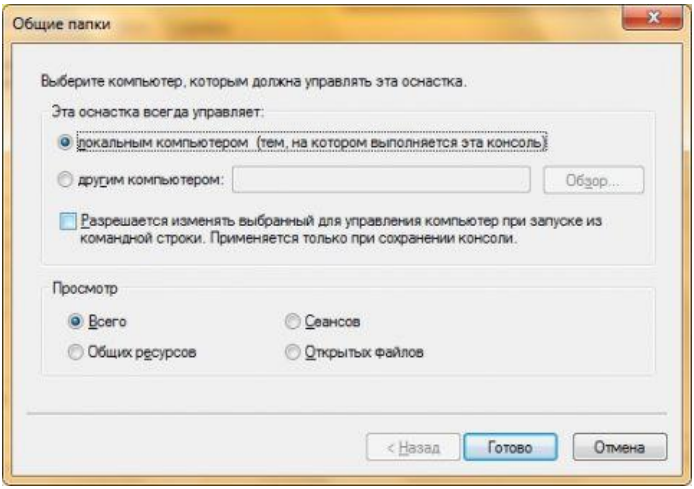


Рис. 9.1. Диалоговое окно «Общие папки» при добавлении оснастки в консоль управления ММС

- Откроется пустая консоль ММС. В меню **«Консоль»** выберите команду **«Добавить или удалить оснастку»** или воспользуйтесь комбинацией клавиш **Ctrl+M**. В диалоге **«Добавление и удаление оснасток»** выберите оснастку **«Общие папки»**. В диалоговом окне **«Общие**

папки», который изображен на следующей иллюстрации, вы можете выбрать компьютер, общими папками которого хотите управлять. По умолчанию вам предлагается выбрать локальный компьютер, но если вы хотите открыть оснастку **«Общие папки»** для другого компьютера – в области **«Эта оснастка всегда управляет»** переместите переключатель на опцию **«другим компьютером»** и введите имя или IP-адрес компьютера. По нажатию на кнопку **«Обзор»** вы можете выбрать компьютер, используя диалоговое окно **«Выбор: Компьютер»**. Также вы можете указать, что будет отображаться в консоли управления Microsoft: только общие ресурсы, только сеансы, только открытые файлы или все три категории сразу.

После того как вы сделаете выбор компьютера и области просмотра нажмите на кнопку **«Готово»**. В диалоге **«Добавление или удаление оснасток»** нажмите на кнопку **«ОК»**;

- Нажмите правой кнопкой мыши на значке **«Компьютер»** и из контекстного меню выберите команду **«Управление»**. В дереве консоли выберите узел **«Общие папки»**;

Оснастка **«Общие папки»** изображена на рис.9.2.

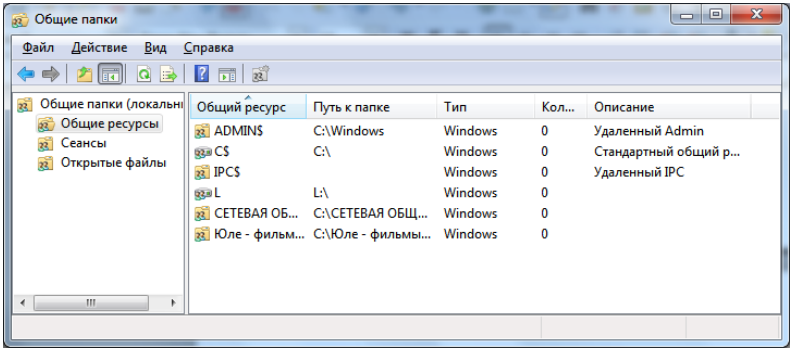


Рис. 9.2 – Оснастка «Общие папки»

2.2 Управление общим доступом папок

Как было сказано выше, вы можете создавать общие ресурсы (предоставлять доступ к папкам или дискам) двумя способами: при помощи оснастки **«Общие папки»**, а также средствами командной строки. Рассмотрим подробно каждое из этих средств.

2.2.1 Создание общего ресурса, используя оснастку «Общие папки»

Для того чтобы создать общий ресурс при помощи оснастки **«Общие папки»**, выполните следующие действия:

1. Откройте оснастку **«Общие папки»**;
2. Перейдите на узел **«Общие ресурсы»** и вызовите **«Мастер создания общих ресурсов»**. Для этого выполните любое из следующих действий:

- В дереве консоли нажмите правой кнопкой мыши на узле **«Общие ресурсы»** и из контекстного меню выберите команду **«Новый общий ресурс»** или команду **«Создать» > «Общий ресурс»**;
- Нажмите правой кнопкой на панели сведений и из контекстного меню выберите команду **«Новый общий ресурс»** или команду **«Создать» > «Общий ресурс»**;
- Если у вас отображается панель действий, то перейдите в ней по ссылке **«Дополнительные действия»** и выберите команду **«Новый общий ресурс»** или команду **«Создать» > «Общий ресурс»**;
- Нажмите на кнопку **«Общий доступ к папке»**, которая расположена на панели инструментов;
- В меню **«Действие»** выберите команду **«Новый общий ресурс»**.

3. В диалоговом окне «Мастер создания общих ресурсов» на первом шаге вы можете прочитать информацию о том, какие действия позволяет выполнить данный мастер. Нажмите на кнопку «Далее»;
4. На шаге «Путь к папке» введите в текстовом поле «Путь к папке:» путь к существующей папке. Вы можете нажать на кнопку «Обзор» и выбрать папку, используя диалоговое окно «Обзор папок» или создать новую. После того как будет выбрана папка для предоставления общего доступа нажмите на кнопку «Далее»;
5. Шаг «Имя, описание и параметры» позволяет задать имя папки, которое будет отображаться на компьютерах, для которых будет предоставлен общий доступ. Для этого в поле «Общий ресурс» задайте имя для данной папки. В поле «Описание» вы можете добавить примечание для данного ресурса. Кнопка «Изменить» вызывает диалоговое окно «Настройка автономного режима», которое позволяет обеспечивать доступ к папке даже при работе в автономном режиме (рис.9.3). После, нажмите «Далее»;

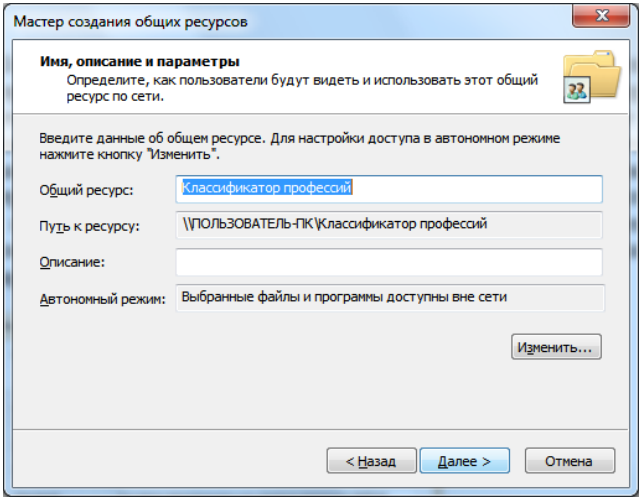


Рис. 9.3 – Настройка описания автономного режима общей папки

6. На предпоследнем шаге мастера создания общих папок вы можете задать разрешения для своей общей папки. Вы можете выбрать любую из трех предоставленных настроек разрешений для общей папки или создать особые разрешения. По умолчанию выбрано разрешение «У всех пользователей доступ только для чтения», что позволяет абсолютно всем пользователям вашей сети просматривать данную папку, но разрешения на изменение файлов будет только у вас. Разрешение «Администраторы имеют полный доступ, остальные – доступ только для чтения» позволяет настроить соответствующие требования. Администраторами являются только те пользователи, которые состоят в группе «Администраторы» только на вашем компьютере (рис.9.4). Если вы хотите, чтобы доступ был только у администраторов – выберите разрешение «Администраторы имеют полный доступ, остальные не имеют доступа».

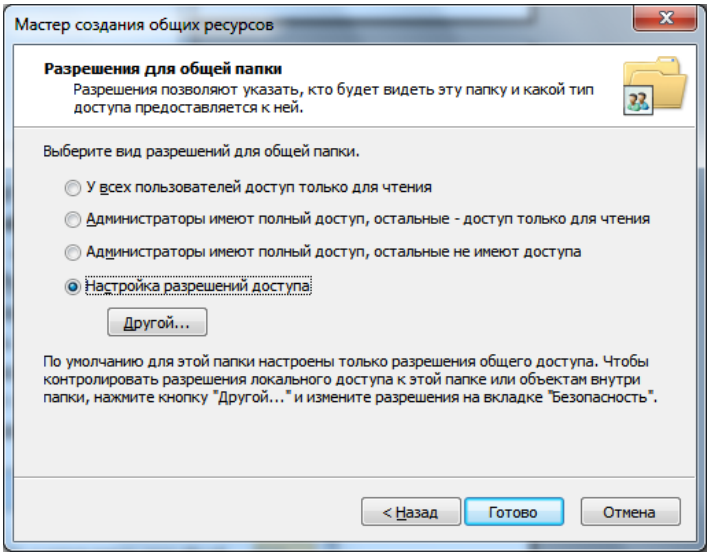


Рис. 9.4 – Назначение разрешений для общей папки

Если вас не устраивает ни один из вышеперечисленных способов разрешений, создайте свои разрешения, установив переключатель на опцию «Настройка разрешений доступа» и нажав на кнопку «Другой». В диалоговом окне «Настройка разрешений доступа» на вкладке «Разрешения для общего доступа» выберите пользователей, которым будет предоставлен доступ к этому общему ресурсу и укажите для этих пользователей разрешения. На вкладке «Безопасность» вы можете указать настройки безопасности для пользователей и групп, которым предоставлен общий доступ. Нажмите на кнопку «ОК» для закрытия диалогового окна настройки разрешений доступа. После выбора требуемого разрешения нажмите на кнопку «Готово»;

7. На последнем шаге вы увидите сводную информацию по созданию общего ресурса. Нажмите на кнопку «Готово» для завершения предоставления общего ресурса (рис.9.5).

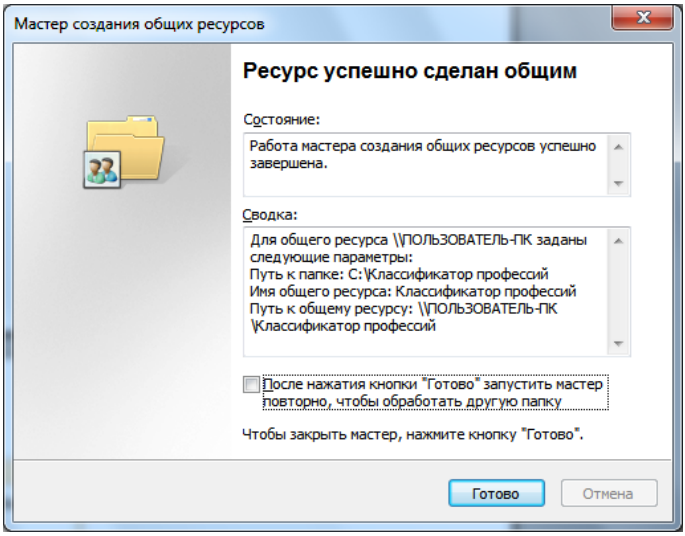


Рис.9.5 – Завершение создания общего ресурса

2.2.2 Создание общего ресурса, используя командную строку

Вы можете предоставлять общий доступ к своим ресурсам без использования графического интерфейса. Утилита командной строки **NET SHARE** позволяет просматривать все общие ресурсы, а также позволяет создавать общий доступ для папок или файлов с идентичными возможностями мастера создания общих ресурсов. Для того чтобы создать общий ресурс, используется следующая команда:

NET SHARE [Имя_общего_ресурса]=Путь /Параметры

где доступны следующие параметры:

- **/GRANT**. При помощи этого параметра вы можете указать пользователей или группы, у которых будет доступ на использование создаваемого общего ресурса. Вместе с этим параметром вы можете указать один из следующих аргументов: **READ**– право только на чтение, **CHANGE**– позволяет пользователю изменять созданные файлы, **FULL**– предоставление полного доступа;
- **/USERS**. Этот параметр позволяет указывать количество одновременно подключаемых пользователей. Доступно числовое значение пользователей. Если вы укажете вместо данного параметра параметр**/UNLINITED**, то количество одновременных подключений к вашему ресурсу не будет лимитированным;
- **/REMARK**. Позволяет добавить примечание для данного ресурса;
- **/CACHE**. Данный параметр позволяет настраивать автономный режим для вашей папки. Все значения данного параметра будут рассмотрены ниже.

В следующем примере (рис.9.6) предоставим общий доступ для папки Temp2, которая расположена в корне диска C:

NET SHARE "Временные файлы 2"=C:\Temp2 /GRANT:TrustedUser,FULL /USERS:5 /REMARK:"Папка, предназначенная для хранения временных файлов, созданная средствами командной строки" /CACHE:Manual

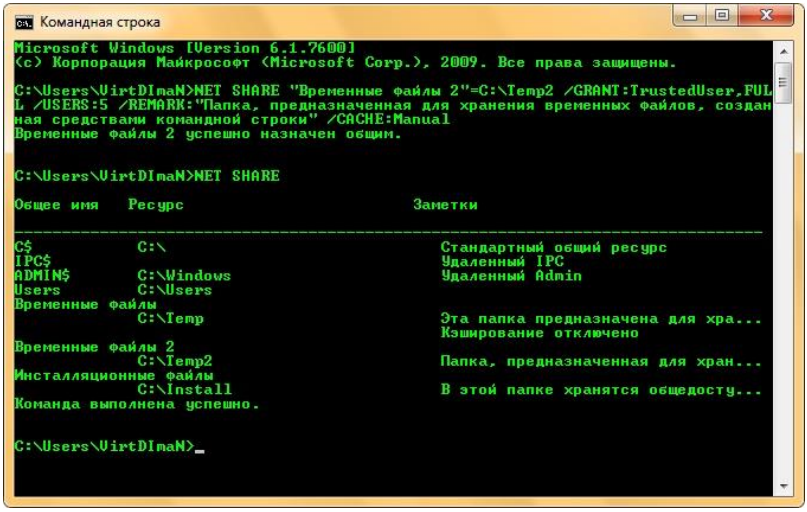


Рис.9.6 – Создание общего доступа при помощи командной строки

2.2.3 Прекращение доступа к общему ресурсу

Так же как и в случае с созданием общих ресурсов, прекратить к ним доступ вы можете при как помощи оснастки **«Общие папки»**, так и средствами командной строки. Перед отключением общего доступа к своему ресурсу следует учесть, что те пользователи, у которых были открыты документы, уже не смогут их сохранить на вашем компьютере. Для того чтобы прекратить общий доступ к своему ресурсы при помощи оснастки **«Общие папки»**, нужно в узле **«Общие ресурсы»** выделить папку, к которой нужно будет прекратить доступ (рис.9.7), нажать на ней правой кнопкой и из контекстного меню выбрать команду **«Прекратить общий доступ»**, как показано ниже:

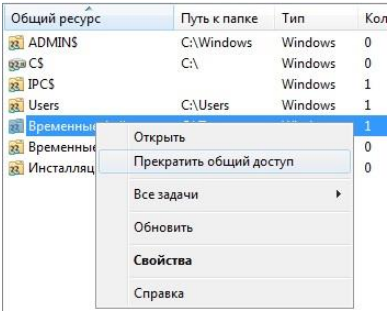


Рис.9.7 – Прекращение общего доступа

При помощи командной строки вы можете прекратить общий доступ к ресурсу при помощи одной команды **NET SHARE**, причем прекратить его даже проще, чем предоставить общий доступ (рис.9.8). Сделать это вы можете следующим образом:

NET SHARE имя_общего_ресурса /DELETE

В данном случае нет необходимости в описании параметра. Перейдем сразу к примеру:

NET SHARE "Временные файлы 2" /DELETE

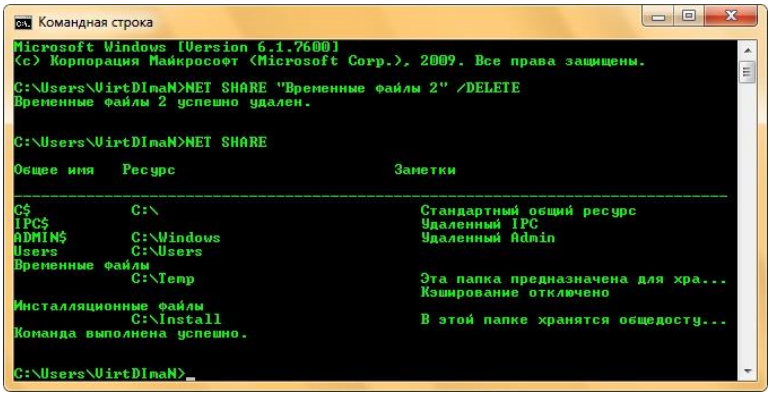


Рис.9.8 – Прекращение общего доступа средствами командной строки

2.3 Разрешения для общих папок

К вашим общим папкам, возможно, будут подключаться десятки, а то и сотни пользователей. У каждого пользователя должны быть назначены свои разрешения на ваши общие ресурсы. При помощи оснастки **«Общие папки»** у вас есть возможность назначения разрешений для пользователей, которые используют ваши общие файлы и папки (рис.9.9). Среди параметров разрешения для общих ресурсов доступны параметры **«Чтение»**, **«Изменение»** и **«Полный доступ»**.

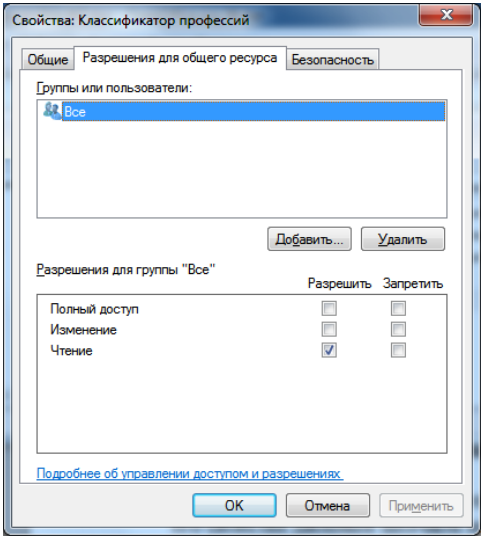


Рис.9.9 – Изменение разрешений для общего ресурса

Если ваш компьютер входит в состав домена Active Directory или если вы хотите указать более строгие разрешения для своих ресурсов, то вам нужно воспользоваться возможностями вкладки **«Безопасность»** свойств общего ресурса. На данной вкладке разрешения задаются на уровне файловой системы NTFS, и вы можете указать более строгие параметры доступа, нежели при использовании возможностей, предоставленных на вкладке **«Разрешения для общего ресурса»**. Для того чтобы изменить разрешения общего доступа, сделайте следующее:

1. Откройте оснастку **«Общие папки»** и в дереве консоли перейдите на узел **«Общие ресурсы»**;
2. Выделите ресурс, разрешения которого вам нужно изменить и откройте его свойства двойным щелчком мыши или выбрав команду **«Свойства»** из контекстного меню;
3. Перейдите на вкладку **«Разрешения общего доступа»**и установите разрешения для выбранных пользователей, как показано ниже:

Помимо оснастки **«Общие папки»** вы можете управлять разрешениями и списком контроля доступа (ACL) при помощи утилит командной строки. Для выполнения этих действий в операционной системе есть две утилиты – ICACLS, а также устаревшая версия данной утилиты CALCS.

Контрольные вопросы

1. Для чего предназначена оснастка «Общие папки», и каким образом можно получить к ней доступ?

2. Что позволяет сделать утилита командной строки NET SHARE**,** и какой формат команды для нее используется?

3. Используя утилиту командной строки NET SHARE**,** продемонстрируйте ситуации создания общего ресурса и прекращения доступа к ресурсу.

4. Какие параметры разрешения доступны общих ресурсов?

Практическая работа №10.

Параметры управления общими папками

1. Цель работы: ознакомиться с системой доступа к ресурсам сети в автономном режиме для ОС Windows и приобрести навыки по настройке доступа.

Задачи работы:

1. Организация работы с общими папками в автономном режиме.
2. Возможности контроля открытых файлов.
3. Технологии просмотра, отключения сеансов пользователей.
4. Подготовить отчет о проделанной работе.

2. Краткие теоретические сведения

Автономные папки позволяют вам и пользователям, которые работают с вашими общими ресурсами, работать с файлами, когда они не подключены к локальной сети при помощи функции кэширования. В операционной системе Windows 7 появился новый метод кэширования автономных файлов – использование функционала BranchCache.

2.1 Работа с общими папками в автономном режиме

В операционных системах, начиная с Windows Vista, за настройки кэширования автономных файлов отвечает диалоговое окно **«Настройка автономного режима»** (рис.10.1). Для того чтобы открыть данное диалоговое окно, выполните следующие действия:

1. Откройте оснастку **«Общие папки»** и в дереве консоли перейдите на узел **«Общие ресурсы»**;
2. Выделите ресурс, разрешения которого вам нужно изменить и откройте его свойства двойным щелчком мыши или выбрав команду **«Свойства»** из контекстного меню;

3. На вкладке **«Общие»** нажмите на кнопку **«Настройка»**.

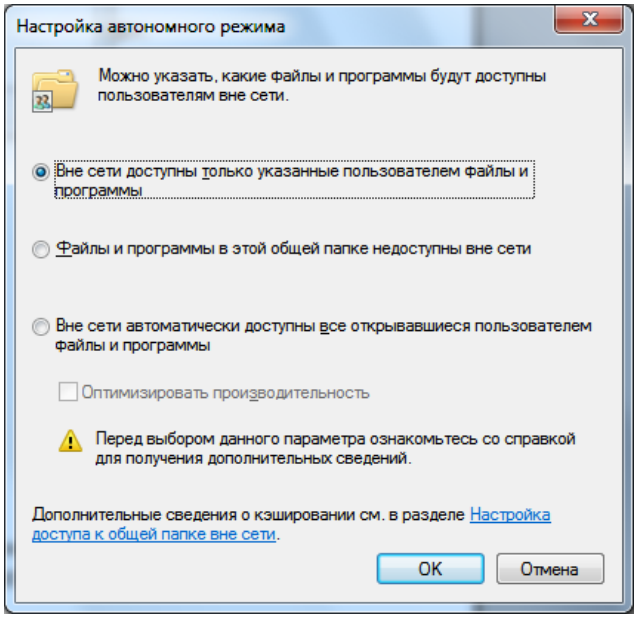


Рис.10.1 – Диалоговое окно настроек автономного режима

Операционная система позволяет вам воспользоваться одним из следующих методов настройки автономных файлов:

- **Вне сети доступны только пользовательские файлы и программы**. Данный параметр указывает на то, что по умолчанию все ваши общие ресурсы будут недоступны в автономном режиме и при необходимости пользователи, подключаемые к вашим ресурсам должны самостоятельно выбрать файлы, которые будут для них доступны при отсутствии подключения к сети;

Если установлен флажок **«Включить Branch Cache»**, то в данном филиале файлы, загружаемые из общей папки, будут кэшироваться, а затем защищенным образом предоставлять эти файлы остальным компьютерам филиала.

- **Файлы и программы в этой общей папке недоступны вне сети**. Указав этот параметр, вы тем самым запрещаете всем пользователям создавать копии файлов вашей общедоступной папки;
- **Вне сети автоматически доступны все открывавшиеся пользователем файлы и программы**. Если вы хотите, чтобы каждый раз после открытия файла, данный файл становился доступным в автономном режиме – укажите этот параметр. Файлы, автоматически ставшие доступными вне сети, останутся в кэше автономных файлов и будут синхронизироваться с версией на сервере, пока кэш не заполнится или пока пользователь не удалит эти файлы;

Опция **«Оптимизировать производительность»** отвечает за то, чтобы при запуске исполняемых файлов или динамических библиотек из общих ресурсов файлы автоматически кэшировались на клиентском компьютере.

Для настройки автономных файлов вы также можете воспользоваться средствами утилиты **NET SHARE** командной строки с параметром**/CACHE** (рис.10.2), у которого доступны следующие значения:

- **Manual**. Данное значение идентично параметру **«Вне сети доступны только пользовательские файлы и программы»**, которое можно установить при помощи графического интерфейса;
- **BranchCache**. Используя это значение, вы можете включить функционал Branch Cache и одновременно указать ручное управление кэшированием документов для общей папки;
- **Documents**. Это значение позволяет включить автономное сохранение файлов на компьютерах пользователей автоматически. Аналогом этого значения в графическом интерфейсе является параметр **«Вне сети автоматически доступны все открывавшиеся пользователем файлы и программы»**;
- **Programs**. Позволяет обеспечить автономное сохранение исполняемых файлов и динамических библиотек (флажок **«Оптимизировать производительность»** из графического интерфейса);

- **None**. При помощи этого параметр вы можете запретить автономное сохранение данных для выбранного ресурса.

Пример показывает, как просто можно настроить автономные файлы для оптимизации производительности при помощи командной строки:

NET SHARE "Временные файлы" /CACHE:Programs

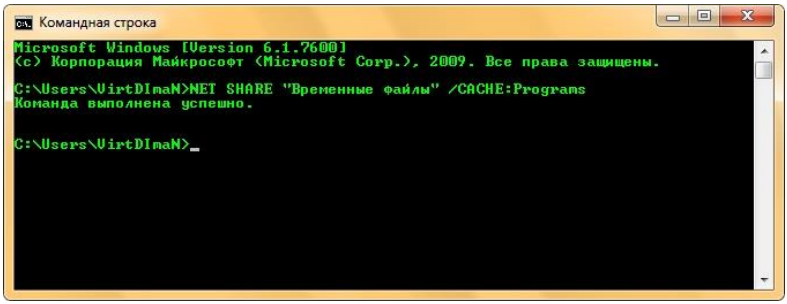


Рис.10.2 – Настройка автономных файлов при помощи командной строки

2.2 Открытые файлы

Используя оснастку «Общие папки» и командную строку вы можете не только управлять общими папками и их настройками, вам также предоставляется возможность просмотра и закрытия открытых файлов, узнать, какие именно файлы просматриваются в данный момент и закрыть данные файлы на компьютере пользователя удаленно без сохранения внесенных изменений.

Для того чтобы закрыть общедоступные файлы при помощи оснастки **«Общие папки»**, выполните следующие действия:

1. В оснастке **«Общие папки»** выберите узел **«Открытые файлы»**;
2. Выберите на панели сведений среди списка открытых файлов тот файл, который вам нужно закрыть;
3. Нажмите на нем правой кнопкой мыши и из контекстного меню (рис.10.3) выберите команду **«Закрыть открытый файл»**, как показано ниже:

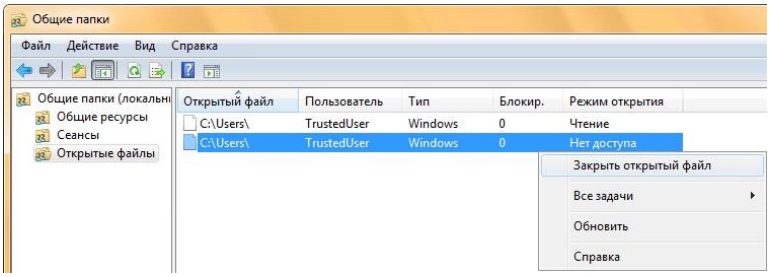


Рис.10.3 – Закрытие открытого общего файла при помощи оснастки *«Общие папки»*

Эти же действия вы можете выполнить из командной строки. Для этого, откройте командную строку от имени администратора и выполните следующие действия, используя утилиту **NET FILE**, при помощи которой вы можете, как просматривать открытые файлы, так и удалять их:

1. Просмотрите открытые файлы. Для этого в командной строке введите **NET FILE**. Как видно на рис.10.4, на данный момент, пользователем TrustedUser два раза открыта общая папка:

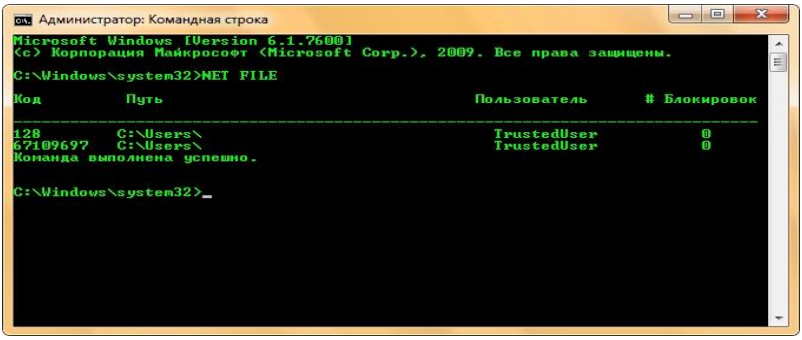


Рис.10.4 – Просмотр открытых общих файлов и папок

2. Как видно на рис.10.4, в столбце код указаны динамически назначаемые идентификаторы общих папок. Теперь, при помощи этой же утилиты нужно закрыть одну папку.

Выполните следующую команду:

NET FILE 67109697 /CLOSE

где: *6710967*–динамически назначаемый идентификатор общих папок;

/CLOSE – параметр, который позволяет закрыть общий файл и папку, а также удалить все блокировки (рис.10.5).

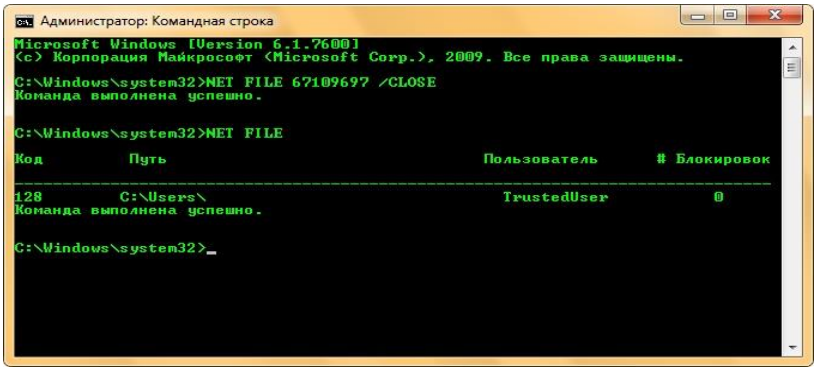


Рис.10.5 – Закрытие общего файла при помощи командной строки

2.3 Настройка сеансов

Оснастка **«Общие папки»** и утилиты командной строки помимо всех вышеперечисленных операций, также позволяют вам отключать пользователя от общедоступного ресурса, который он на данный момент использует.

Для того чтобы отключить пользователя при помощи оснастки **«Общие папки»**, выполните следующие действия:

1. В оснастке **«Общие папки»** выберите узел **«Сеансы»**;
2. На панели сведений из предоставленного списка выберите сеанс пользователя, которого вам нужно отключить;
3. Нажмите на нем правой кнопкой мыши и из контекстного меню (рис.10.6) выберите команду **«Закрыть сеанс»**, как показано ниже:

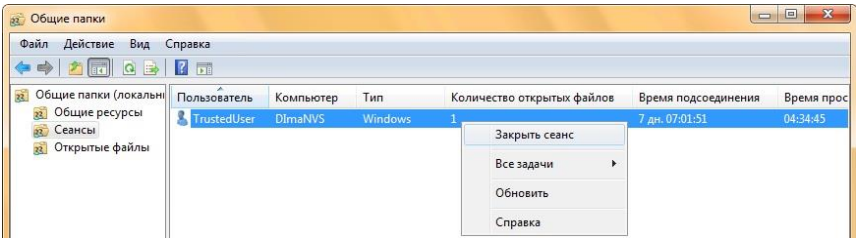


Рис.10.6 – Отключение пользователя при помощи оснастки «Общие папки»

Для командной строки существует еще одна утилита, которая позволяет просматривать сеансы пользователей и отключать их. Для этой цели существует команда **NET SESSION**, которую можно использовать только в командной строке, открытой от имени администратора (рис.10.7). Синтаксис данной команды очень простой и похожий на синтаксис команды **NET FILE**:

NET SESSION /параметр

Для того чтобы просмотреть сеансы, вы можете воспользоваться командой без указания параметров, выводом которой будет таблица с подключенными пользователями. Также вы можете применить данную команду с параметром **/LIST**, который позволяет просмотреть сеансы пользователей в виде списка, отображенного ниже:

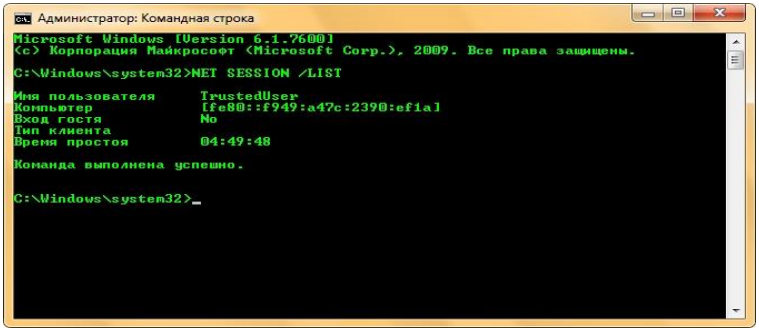


Рис.10.7 – Отображение сеансов пользователей в виде списка

Для того чтобы отключить подключенного к вашим общим ресурсам пользователя, вам нужно воспользоваться данной утилитой со следующими параметрами:

- **\\имя_компьютер**. Необходимый параметр, в котором вам нужно указать имя компьютера или его IP-адрес, с которого выполняется в данный момент доступ к вашим ресурсам. Если не указать данный параметр, то будут отключены все пользователи;
- **/DELETE**. Данный параметр позволяет завершить сеанс (рис.10.8) пользователей и закрыть все файлы, которые открыты на данный момент из вашего ресурса.

Пример использования:

NET SESSION ||VISTA-02 /DELETE

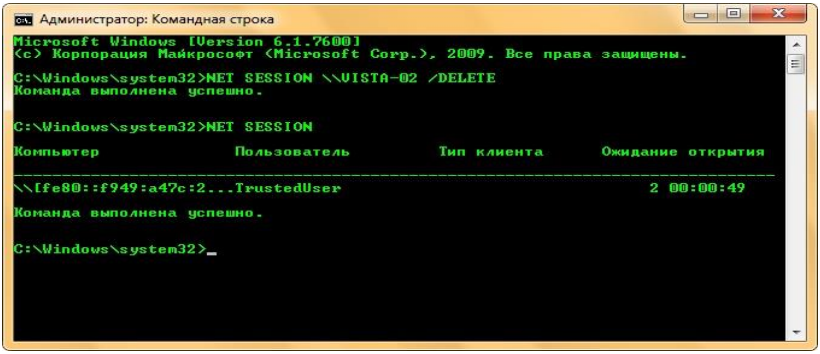


Рис.10.8 – Отключение сеанса пользователя при помощи командной строки

Таким образом, вы познакомились с созданием общих ресурсов, управлением разрешениями, настройкой автономных файлов и прекращением общего доступа при помощи оснастки консоли управления Microsoft **«Общие папки»** и утилит командной строки. Помимо этого вы научились управлять файлами и сессиями общих ресурсов и закрывать их.

Контрольные вопросы

1. Какие параметры разрешения доступны общих ресурсов?
2. Что обеспечивает функционал BranchCache, и каким образом он настраивается через диалоговые окна и командную строку?
3. Каким образом с помощью оснастки *«Общие папки»* и через командную строку закрыть открытые файлы?
4. Каким образом можно управлять сеансами?

РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

1. Баканов В.М. Сети ЭВМ и телекоммуникации: учебно-методическое пособие по выполнению лабораторных работ. —М.: МГУПИ, 2008. – 49 с.
2. Гук М. Аппаратные средства локальных сетей. Энциклопедия. –СПб.: Питер, 2007. -576 с.
3. Максимов Н.В., Попов И.И. Компьютерные сети: Учебное пособие.-М.: ФОРУМ: ИНФРА-М, 2004 г.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд.- СПб.: Питер, 2006 г.
5. Партыка Т.Л., Попов И.И. Информационная безопасность. Уч. пособие для студентов учреждений СПО.- М.: ФОРУМ: ИНФРА-М, 2002 г.
6. Дуглас Э. Камер. Сети TCP/IP. - Вильямс, 2003. -Т.1: Принципы, протоколы и структура.
7. Таненбаум Э. Компьютерные сети. - Питер, 2002.
8. Михаил Гук. Аппаратные средства локальных сетей: Энциклопедия. - СПб.: Питер, 2000.
9. Столингс В. Современные компьютерные сети. - Питер, 2003.
10. Компьютерные сети: Учебный курс. – Microsoft Press: Русская редакция, 1998.
11. Фейт С. TCP/IP. Архитектура, протоколы, реализация. - Лори, 2000.