НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДЕНО
педагогическим советом
(протокол № 06-24 от «26» июня 2024)
Председатель педагогического совета
Директор _____ Л.Н. Цой

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине МДК.02.01 Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем

программы подготовки квалифицированных рабочих, служащих среднего профессионального образования

09.01.05 Оператор технической поддержки

Якутск 2024

Комплект ФОС включен в учебно-методическую документацию для аттестации обучающихся на соответствие требованиям образовательной программы по профессии: 09.01.05 Оператор технической поддержки.

Рассмотрено и одобрено на заседании отделения информационных технологий и туризма.

Протокол заседания № 9/1 от 21 мая 2024 г. Председатель: Пронин И.В.

Разработчик: Крымова Олеся Викторовна

СОГЛАСОВАНО: Заместитель директора по МР – Зайцева Д.А. в 2024-2025 учебном году. Протокол № 06-24 от «24» июня 2024 г.

СОДЕРЖАНИЕ

1. Паспорт комплекта фонда оценочных средств

1.1 Область применения

Комплект фонда оценочных средств (ФОС) предназначен для проверки результатов освоения учебной дисциплины МДК.02.01 Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем по профессии 09.01.05 Оператор технической поддержки.

1.2. Объекты оценивания – результаты освоения учебной дисциплины МДК.02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем

Комплекс ФОС позволяет оценивать следующие результаты освоения учебной дисциплины МДК.02.01 Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем в соответствии с ФГОС по профессии 09.01.05 Оператор технической поддержки.

Особое значение дисциплина имеет при формировании и развитии: ПК и ОК, которые актуализируются при изучении профессионального модуля:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1. Вводить в эксплуатацию отдельные устройства инфокоммуникационных систем.

ПК 2.2. Устанавливать и настраивать системное и прикладное ПО, необходимое для функционирования ИС, в том числе сетевое программное обеспечение и программное обеспечение для защиты от несанкционированного доступа.

ПК 2.3. Проверять правильность установки и функционирования устройств после настройки программного обеспечения сетевой инфраструктуры и базовой конфигурации сетевых устройств и программного обеспечения, в том числе – виртуальной сетевой инфраструктуры.

ПК 2.4. Настраивать базовые параметры программного обеспечения для учета конфигураций, слежения за производительностью устройств и защиты их от несанкционированного доступа.

ПК 2.5. Отслеживать производительность устройств и виртуальных вычислительных ресурсов и их защиту от несанкционированного доступа.

1.3. Формы контроля и оценки результатов освоения учебной дисциплины МДК.02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем

Контроль и оценка результатов освоения – это выявление, измерение и оценивание знаний, умений и формирующихся общих и профессиональных компетенций в рамках освоения учебной дисциплины МДК 02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем.

В соответствии с учебным планом профессии 09.01.05 Оператор технической поддержки, рабочей программой учебной дисциплины МДК 02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем, предусматривает текущий и промежуточной контроль результатов освоения.

1.3.1 Формы текущего контроля

Текущий контроль успеваемости представляет собой проверку усвоения учебного материала, регулярно осуществляемую на протяжении курса обучения.

Текущий контроль результатов освоения учебной дисциплины МДК 02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем в соответствии с рабочей

программой и календарно-тематическим планом происходит при использовании следующих обязательных форм контроля:

- выполнение и защита лабораторных работ,
- проверка выполнения самостоятельной работы студентов,

Во время проведения учебных занятий дополнительно используются следующие формы текущего контроля – устный опрос, решение задач, тестирование по темам отдельных занятий.

Проверка выполнения самостоятельной работы. Самостоятельная работа направлена на самостоятельное освоение и закрепление студентами практических умений и знаний, овладение профессиональными компетенциями.

Самостоятельная подготовка студентов по учебной дисциплине МДК 02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем предполагает следующие виды и формы работы:

1. Подключение пользователей к локальной сети;
2. Выбор и подключение коммутатора для локальной сети;
3. Подключение пользователей локальной сети к глобальной сети;
4. Разграничение прав доступа пользователей локальной сети.

Выполнение и защита лабораторных работ. Лабораторные работы проводятся с целью усвоения и закрепления практических умений и знаний, овладения профессиональными компетенциями. В ходе лабораторной работы студенты приобретают умения, предусмотренные рабочей программой учебной дисциплиной МДК 02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем, учатся самостоятельно работать с оборудованием лаборатории, проводить эксперименты, анализировать полученные результаты и делать выводы, подтверждать теоретические положения лабораторным экспериментом.

Список лабораторных работ:

Лабораторное занятие № 1. Подключение пользователей к локальной сети.

Лабораторное занятие № 2. Выбор и подключение коммутатора для локальной сети.

Лабораторное занятие № 3. Подключение пользователей локальной сети к глобальной сети.

Лабораторное занятие № 4. Разграничение прав доступа пользователей локальной сети.

Лабораторное занятие № 5. Настройка проводного подключения.

Лабораторное занятие № 6. Настройка беспроводного подключения.

Лабораторное занятие № 7. Получение таблицы MAC-адресов.

Лабораторное занятие № 8. Настройка режимов и скорости.

Лабораторное занятие № 9. Настройка портов коммутатора.

Лабораторное занятие № 10. Выполнение эхо-запросов.

Лабораторное занятие № 11. Настройка коммутатора.

Лабораторное занятие № 12. Настройка маршрутизатора.

Лабораторное занятие № 13. Выполнение трассировки маршрута и тестирование пути.

Лабораторное занятие № 14. Мониторинг сети с целью выявления типовых инцидентов и угроз безопасности.

Лабораторное занятие № 15. Оценка степени критичности инцидентов при работе согласно инструкции.

Лабораторное занятие № 16. Обнаружение и устранение возникающих типовых инцидентов.

Лабораторное занятие № 17. Сбор информации о сетевом трафике.

Сводная таблица по применяемым формам и методам текущего контроля и оценки результатов обучения

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Освоение умения:	
– применять инструкции по установке и эксплуатации периферийного оборудования; – конфигурировать периферийные устройства; – задавать базовые параметры, в том числе параметры защиты от несанкционированного доступа к операционным системам; – применять методы статической и динамической конфигурации параметров операционных систем; – устанавливать операционные системы; – устанавливать СУБД; – устанавливать прикладное ПО; – применять средства контроля и оценки конфигураций операционных систем; – проверять правильность настройки устройств инфокоммуникационных систем; – использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных	Тест Лабораторная работа Самостоятельная работа Устный и письменный ответ

систем; – идентифицировать типовые инциденты функционирования устройств инфокоммуникационных систем; – устранять возникающие типовые инциденты; – проводить диагностику инцидента согласно инструкции; оценивать степень критичности инцидентов при работе согласно инструкции; – задавать базовые параметры, в том числе параметры защиты от несанкционированного доступа к операционным системам; – применять методы статической и динамической конфигурации параметров операционных систем; – осуществлять текущий контроль и мониторинг производительности устройств и виртуальных вычислительных ресурсов в соответствии с техническим заданием; – осуществлять контроль обеспечения уровня защищенности устройств и виртуальных ресурсов от несанкционированного доступа; – применять средства защиты информации от несанкционированного доступа.	
Усвоенные знания:	
– основы архитектуры аппаратных средств; – принципы функционирования аппаратных средств вычислительной техники; – принципы работы операционных систем; основы современных систем управления базами данных; – основы системного администрирования; модель взаимодействия открытых систем (OSI); – лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; – требования охраны труда при работе с программно-аппаратными средствами инфокоммуникационных систем; – инструкции по установке операционных систем, программного обеспечения; – инструкции по эксплуатации операционных систем, программного обеспечения; – лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения;	Тест Лабораторная работа Самостоятельная работа Устный и письменный ответ

– назначение, виды, последовательность проведения профилактических работ; – основы управления сетевым трафиком; – регламенты проведения профилактических работ для инфокоммуникационных систем; – терминологию и правила чтения технической документации; – требования охраны труда при работе с программно-аппаратными средствами инфокоммуникационных систем; – конфигурирования базовых параметров устройств инфокоммуникационных систем; – регламенты проведения профилактических работ для инфокоммуникационных систем; – терминологию и правила чтения технической документации. – основ законодательства и нормативных правовых актов в области защиты информации; – возможных угроз безопасности информации в инфокоммуникационных системах; – основных средств виртуализации и разграничения уровней доступа к ним; – основных типов технических средств защиты информации от утечки по техническим каналам; – способов защиты информации от несанкционированного доступа; – критерии оценки защищенности инфокоммуникационных систем; – основных методов, алгоритмов, протоколов, используемых для обеспечения защиты информации в ИС.	

Контролируемые разделы / темы	**Код и этапы формирования компетенции (или ее части)**	**Оценочные средства**	
		текущий контроль	**промежуточная аттестация**
Тема 1.1. Активное сетевое оборудование	ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 07, ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	Конспект темы, Устный опрос, Лабораторные работы №1, 2,3,4.	экзамен
Тема 1.2. Сетевой доступ. Ethernet	ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 07, ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	Конспект темы, Устный опрос, Лабораторные работы №5,6,7,8,9	экзамен
Тема 1.3. Настройка	ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 07,	Конспект темы, Устный опрос,	экзамен

маршрутизации	ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	Лабораторные работы №10,11,12,13	
Тема 1.4. Основы эксплуатации и обслуживания сетевых устройств	ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 07, ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5	Конспект темы, Устный опрос, Лабораторные работы №14,15,16,17	экзамен

1.3.1 Форма промежуточной аттестации

Промежуточная аттестация по учебной дисциплине – экзамен, спецификация которого содержится в данном комплекте ФОС.

1.4 Система оценивания комплекта ФОС текущего контроля и промежуточной аттестации

При оценивании лабораторной и самостоятельной работы студента учитывается следующее:

- качество выполнения лабораторной и самостоятельной работы;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

Каждый вид работы оценивается по пяти бальной шкале.

Оценка	Кол-во баллов	Критерии оценки
отлично	91 - 100	студент должен: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; продемонстрировать умения самостоятельной работы с литературой; уметь сделать выводы по излагаемому материалу
хорошо	71 - 90	студент должен: продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; продемонстрировать умение ориентироваться в литературе; уметь сделать достаточно обоснованные выводы по излагаемому материалу
удовлетворительно	51 - 70	студент должен: продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого

		вопроса; показать общее владение понятийным аппаратом дисциплины.
неудовлетворительно	менее 51	ставится в случае: незнания значительной части программного материала; не владения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу.

2. Текущий контроль и оценка результатов обучения учебной дисциплины МДК 02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем

Лабораторное занятие № 1. Подключение пользователей к локальной сети

Задание 1

Зайдите в командную строку. Для этого выполните: Пуск-Поисковая строка-cmd.

В командной строке введите: ping www.vk.com

Запишите в тетрадь полученную информацию и следующую теорию:

PING — одна из базовых и самых полезных CMD-команд. Она отображает качество связи, показывает, может ли ваш компьютер высылать данные по целевому IP-адресу, и если может, то с какой скоростью.

Команда действует по следующему принципу: она высылает определённое количество пакетов данных и определяет, сколько из них вернулось обратно. Если некоторые из них не вернулись, она сообщает о потере. Потеря пакетов ведёт к низкой производительности в играх и интернет-трансляциях. Это отличный способ протестировать ваше интернет-соединение.

По умолчанию команда высылает четыре пакета с тайм-аутом для каждого в четыре секунды.

Задание 2

Продолжите работать в командной строке. Введите команду: getmac

Выпишите полученную информацию и следующую теорию:

Каждое совместимое со стандартами IEEE 802 устройство имеет уникальный MAC-адрес (Media Access Control). Производитель присваивает каждой единице оборудования свой собственный адрес, который прописан в самом устройстве.

Вы можете увидеть несколько MAC-адресов, в зависимости от того, сколько сетевых адаптеров установлено на вашем компьютере. Например, интернет-соединения Wi-Fi и Ethernet будут иметь отдельные MAC-адреса.

Задание 3

Введите в командной строке: nslookup www.google.com

Выпишите команду и полученные 1-2 IP-адреса, а также следующую теорию:

NSLOOKUP означает Name Server Lookup. Потенциал этой утилиты огромен, но большинству людей он не нужен. Для рядовых пользователей важна лишь возможность определить IP-адрес какого-либо доменного имени.

Имейте в виду, что некоторые домены не привязаны к одному IP-адресу, что означает, что вы будете получать разные адреса при каждом новом вводе команды. Это вполне нормально для больших сайтов, потому что они загружаются с огромного количества компьютеров.

Если вы хотите преобразовать IP-адрес в доменное имя, просто введите его в строку браузера и вы увидите, куда он ведёт. Однако не все IP-адреса ведут к доменным именам. Многие из них нельзя достичь через веб-браузер.

Задание 4

Введите в командной строке команду: ipconfig

Выпишите IP-адрес Основного шлюза и следующую теорию:

Узнать свой IP можно зайдя в командную строку и введя команду ipconfig. При разных вариантах подключения к сети, вы можете получить различную информацию с использованием данной команды.

После ее ввода, вы увидите список всех сетевых подключений, используемых вашим компьютером:

Если ваш компьютер подключен к Интернету через Wi-Fi роутер, то основной шлюз в параметрах подключения, используемого для связи с роутером (беспроводное или Ethernet) — это адрес, по которому вы можете зайти в настройки роутера.

Если ваш компьютер находится в локальной сети (если он подключен к роутеру, то он так же находится в локальной сети), то вы можете узнать свой IP адрес в этой сети в соответствующем пункте.

Если на вашем компьютере используется подключение PPTP, L2TP или PPPoE, то вы можете увидеть свой IP адрес в Интернете в параметрах этого подключения (однако лучше воспользоваться каким-либо сайтом для определения своего IP в Интернете, так как в некоторых конфигурациях IP адрес, отображаемый при выполнении команды ipconfig, может не соответствовать ему).

Задание 5.

Описать одноранговую локальную сеть с топологией звезда.

Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в интернет-магазинах и с учётом схемы расположения компьютеров в офисе.

Проанализируйте описание локальной сети и сделайте выводы.

Схема локальной сети		
Недостатки		
Преимущества		
Количество компьютеров в сети		
Оборудование,	Оборудование	Стоимость

необходимое для создания сети и его стоимость		
Общая стоимость создания локальной сети		

Построить схему сети университета и ее модель с указанием топологии сетей и стандартов линий связи. Основными критерием выбора должны быть: экономичность и достаточная пропускная способность. Сделать приблизительный расчет количества материалов и стоимости такой сети с учетом «сетевой» аппаратуры.

Исходные данные приведены в таблице.

№ корпуса	Количество классов	Количество ПК в классе
1	12	15
2	10	
3	6	
4	8	

Объяснить, чем Вы руководствовались при выборе тех или иных элементов сети и указать их преимущества.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

Охарактеризуйте топологию сетей.

Что такое протокол обмена?

Что такое IP-адрес. Для чего они нужны в сети?

Какой самый эффективный кабель при подключении к сети интернет?

Лабораторное занятие № 2. Выбор и подключение коммутатора для локальной сети

1. Изучить состав и назначение основных компонентов сетевого оборудования.

Ответить на контрольные вопросы.

Выяснить состав сетевых компонентов, используемых в составе лаборатории и способ их соединения в ЛВС.

Изучить правила разделки и подключения кабеля типа витая пара по стандартам T568A и T568B.

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

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

Для определения состава оборудования ПК:

Способ 1. Используйте окно «Свойства системы».

Откройте это окно путем ” Мой компьютер” -> ” Свойства” или нажав WIN+Break.

Воспользуйтесь вкладками «Общие» и «Оборудование» -> «Диспетчер устройств».

Способ 2. Откройте окно «Запуск программы» (WIN+R), и введите команду msinfo32.

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

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

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

Отчет: Сохранить значение параметров.

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

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

Откройте окно «Диспетчер устройств»:

Откройте окно «Запуск программы» (”Пуск”->”Выполнить” или WIN+R),

Введите команду devmgmt.msc и нажмите ”ОК”.

В появившемся окне найдите узел дерева «Сетевые адаптеры» и раскройте его.

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

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

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

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

ipconfig /all.

getmac /v /fo list

ping <сетевое имя компьютера>

Отчет: полный протокол выполнения этих команд с вашими пояснениями и выводами.

Анализируете полученный результат, а не сами команды, подробное знакомство с которыми это предмет следующих лабораторных работ.

6. Проверить текущее состояние сетевых подключений Вашего компьютера.

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

Используйте вкладки «Общие» и «Поддержка» (плюс «Подробности») окна «Состояние…».

На этих вкладках познакомьтесь со всеми выводимыми параметрами, нажимая кнопку «?»

и активируя указатель мышки над интересующим параметром.

Проверьте наличие значка сетевого соединения в области уведомлений экрана вашего компьютера. При его наличии ознакомьтесь с параметрами

всплывающего окне над этим значком и действием в ответ на клик мышки на этом значке.

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

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

Откройте окно командной строки и выполните команды:

net view /domain – для просмотра доступных вам рабочих групп.

net view – для просмотра доступных вам компьютеров вашей рабочей группы.

ping <сетевое имя компьютера вашей рабочей группы> - для всех ПК группы.

Сравните результаты с результатами просмотра «Сетевого окружения».

Отчет: полный протокол выполнения этих команд с вашими пояснениями и выводами.

Анализируете полученный результат, а не сами команды, подробное знакомство с которыми это предмет следующих лабораторных работ.

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

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

Дополнительные сведения.

Результаты выполнения из командной строки, описанных выше команд, могут быть просмотрены не только на экране, но и перенаправлены в текстовый файл. Это файл потом может быть просмотрен, сохранен или вставлен в какой-либо документ. Например, отчет по лабораторной работе. Так, команда ping ws1 > d:\student\ping1.txt вызовет формирование текстового файла ping1.txt с результатами работы команды ping.

Совокупность таких команд может составлять командный файл. Запуск на выполнение командного файла позволит получить один текстовый файл, содержащий результаты выполнения сразу нескольких команд. То есть получить один текстовый файл, содержащий все интересующие вас сетевые настройки конкретного компьютера.

Лабораторное занятие № 3. Подключение пользователей локальной сети к глобальной сети

Задание №1.

Создайте на Рабочем столе папку под именем Почта_1 (цифра в имени соответствует номеру вашего компьютера).

С помощью текстового редактора Word или Word Pad создайте письмо к одногруппникам.

Сохраните данный текст в папке Почта_1 своего компьютера в файле письмо1.doc, где 1 – номер компьютера.

Откройте папку другого компьютера, например, Почта_2 и скопируйте в него файл письмо1 из своей папки Почта_1.

В своей папке Почта_1 прочитайте письма от других пользователей, например письмо2. Допишите в них свой ответ.

Переименуйте файл письмо2 .doc в файл письмо2_ответ1.doc

Переместите файл письмо2_ответ1.docв папку Почта _2 и удалите его из своей папки

Далее повторите п.2-4 для других компьютеров.

Прочитайте сообщения от других пользователей в своей папке и повторите для них действия п.5-8.

Задание №2.Ответить на контрольные вопросы:

Укажите основное назначение компьютерной сети.	
Укажите объект, который является абонентом сети.	

Что такое локальная сеть, глобальная сеть?	
Что понимается под топологией локальной сети?	
Какие существуют виды топологии локальной сети?	
Охарактеризуйте кратко топологию «шина», «звезда», «кольцо».	
Что такое протокол обмена?	
Решите задачу. Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов	

Задание №3. Сделать вывод о проделанной лабораторной работе

Лабораторное занятие № 4. Разграничение прав доступа пользователей локальной сети

Задание №1. Определите общий ресурс компьютера. Для этого:

В операционной системе Windows найти на рабочем столе значок Сеть.

Открыть папку, где будут видны все компьютеры, которые подключены в одну сеть.

В данном окне появятся все компьютеры, которые подключены к сети.

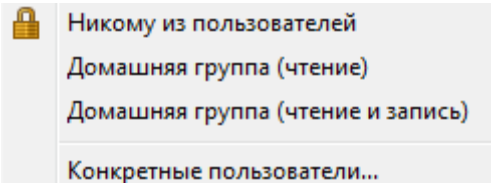
Открыть один из них. Посмотреть ресурсы компьютера, которыми можно воспользоваться. Такие ресурсы называются общими.

Задание № 2. Предоставьте доступ для пользователей локальной сети к папке на своем компьютере, подключенном к локальной сети. Для этого:

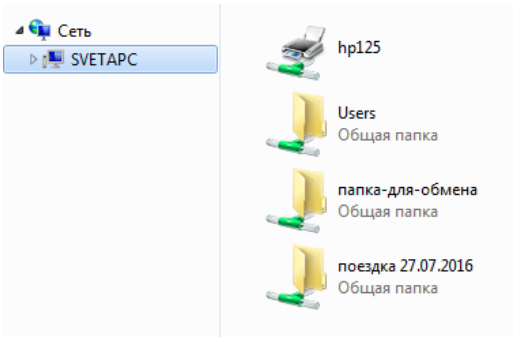
В операционной системе Windows открыть окно папки Компьютер и на диске D: создать свою папку. Назвать ее номером своей группы.

Щелкнуть правой кнопкой мыши по значку папки и в контекстном меню папки выберите команду Общий доступ.

Выбрать нужное подменю: Конкретные пользователи



В списке Сеть внизу появится новая папка: поездка 27.07.2016



Если все правильно сделано, то на диске (у вашей папки) появится значок, который показывает, что папка является общей.

Задание №3. Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов?

Решение:

50*70=3500 символов на страницу.

Так как не указано, сколько символов в алфавите, возьмем 1 байт на символ. Итого 3500 байт или (умножить на 8) 28000 бит.

Теперь делим 100,000,000 на 28,000. Получаем 3571.43 страниц.

Решить самостоятельно по следующим данным:

1 страница текста содержит 70 строк и на каждой строке - 50 символов?

Задание №4. Ответьте на вопросы:

1.Указать основное назначение компьютерной сети.	
2.Указать основную характеристику каналов связи.	
3.Указать объект, который является абонентом сети.	

Лабораторное занятие № 5. Настройка проводного подключения

Открытие компонента «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».

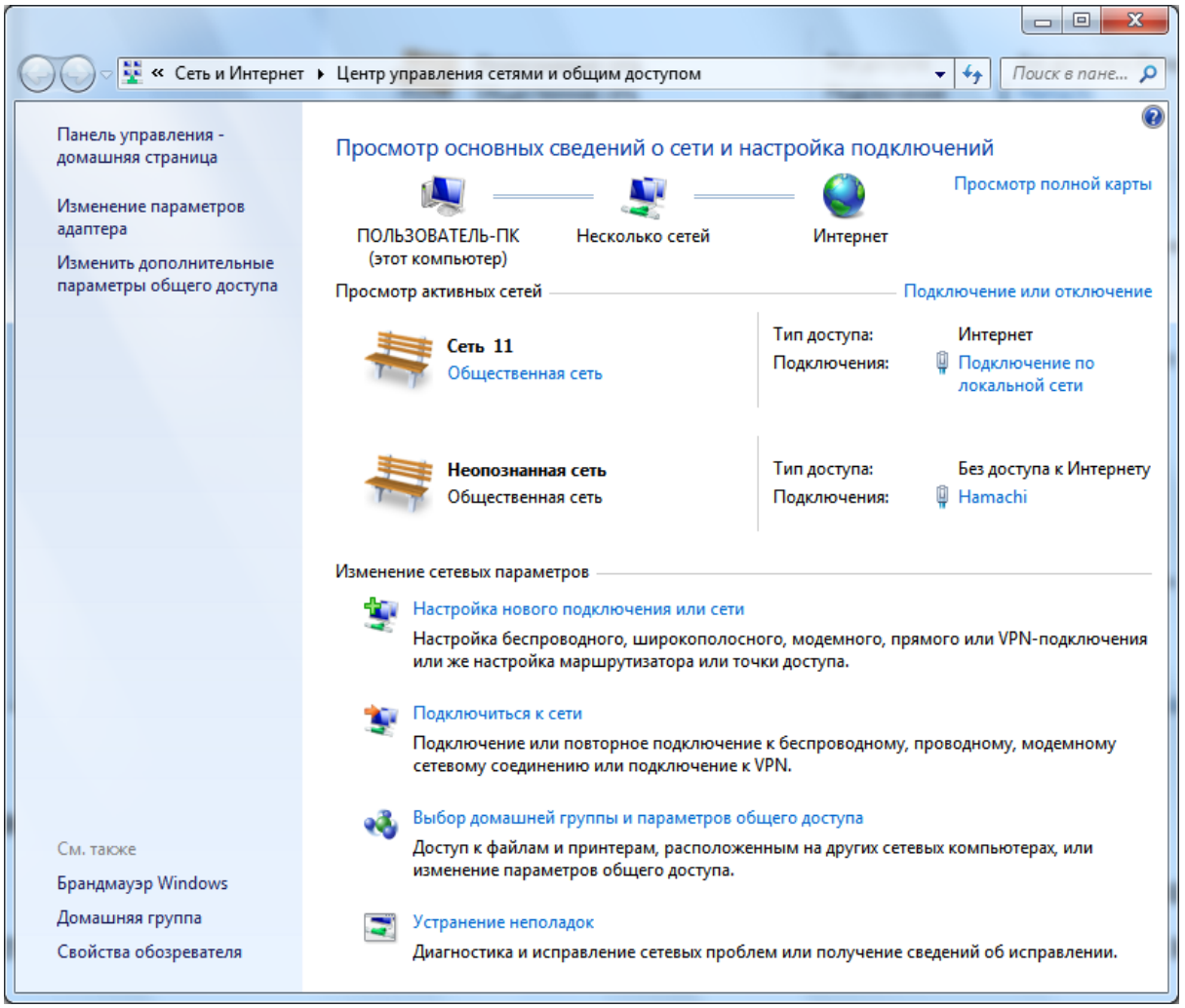


Рис. 1.1. «Центр управления сетями и общим доступом»

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 поддерживает несколько активных профилей, что позволяет наиболее безопасно использовать несколько сетевых адаптеров, подключенных к различным сетям. Существует четыре типа сетевого расположения (рис.1.2).

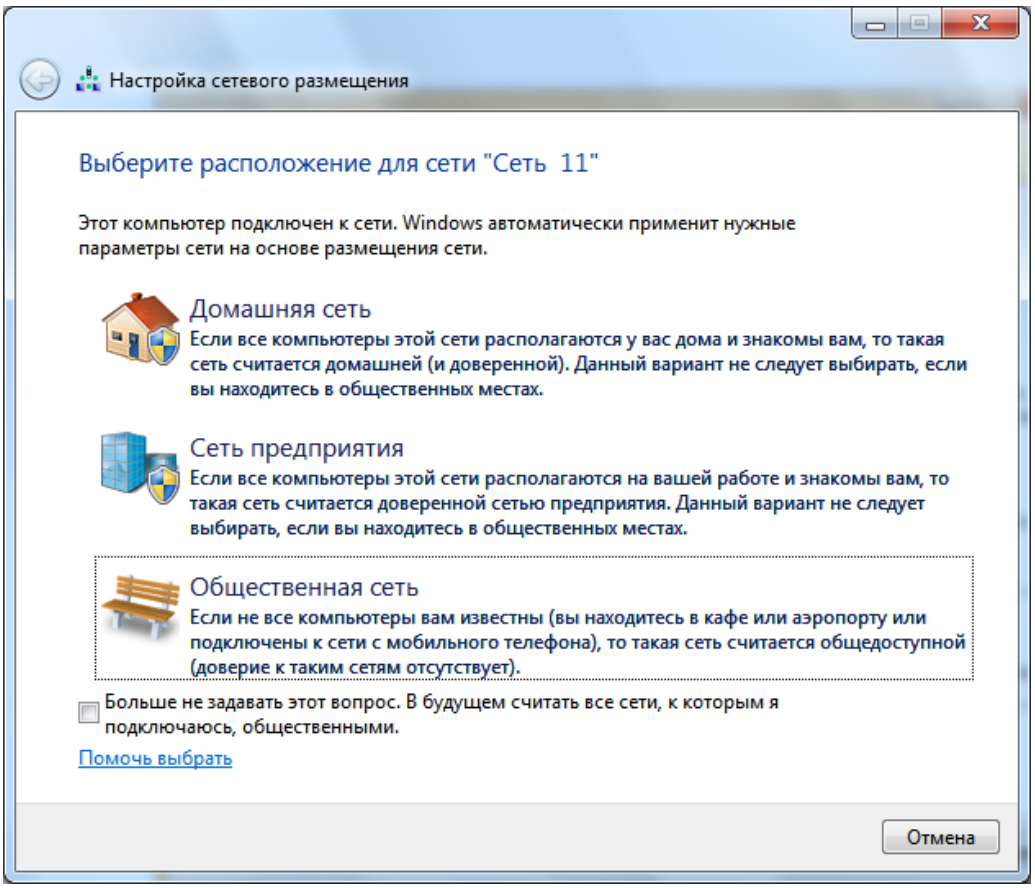


Рис. 1.2. Выбор сетевого расположения

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.

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 коммутаторы, 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.

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. Пример карты сети вы можете увидеть на рис.1.3.

Рис. 1.3. Пример карты сети

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.

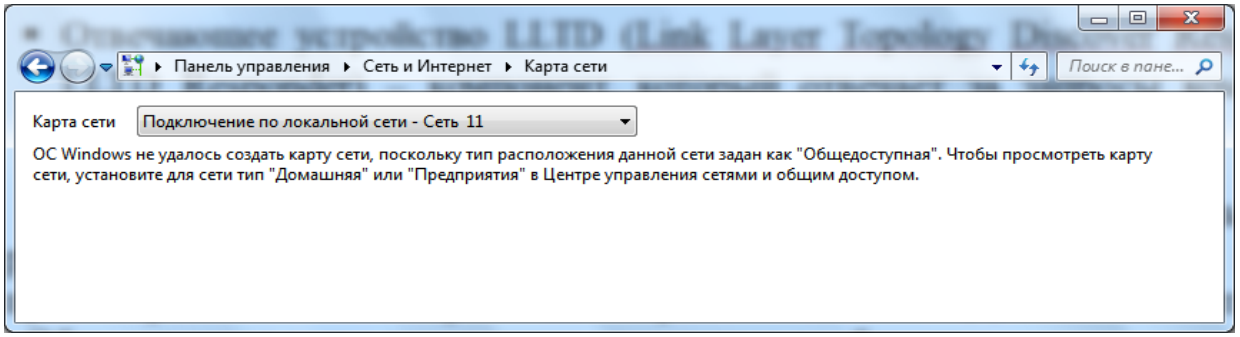


Рис. 1.4. Попытка просмотра карты сети

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

Откройте оснастку «Управление групповой политики»;

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»;

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)»;

В свойствах параметра политики установите переключатель на опцию «Включить» и установите флажок «Разрешить операцию для домена»;

Повторите аналогичные действия для параметра политики «Включить драйвер «Ответчика» (RSPNDR)»;

Обновите параметры политики на клиентской машине, используя команду gpupdate /force /boot;

Обновите карту сети.

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» для открытия меню, 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».

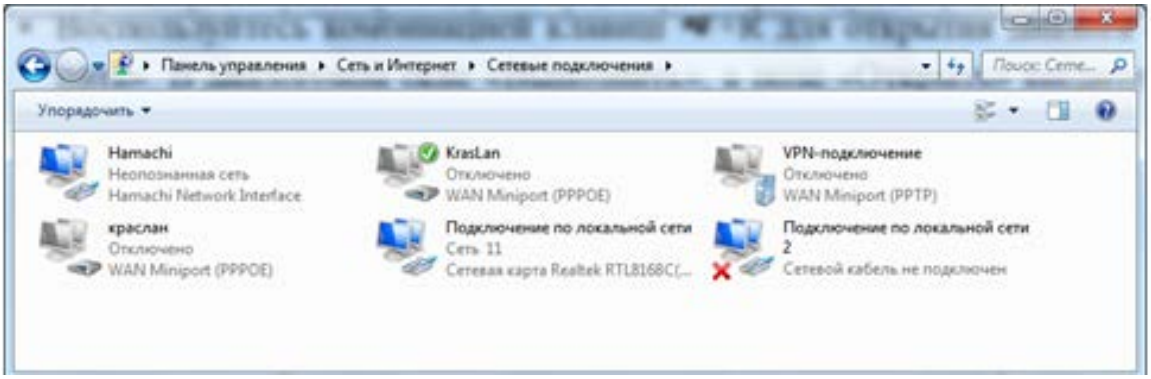


Рис. 1.5. Окно «Сетевые подключения»

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:

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.

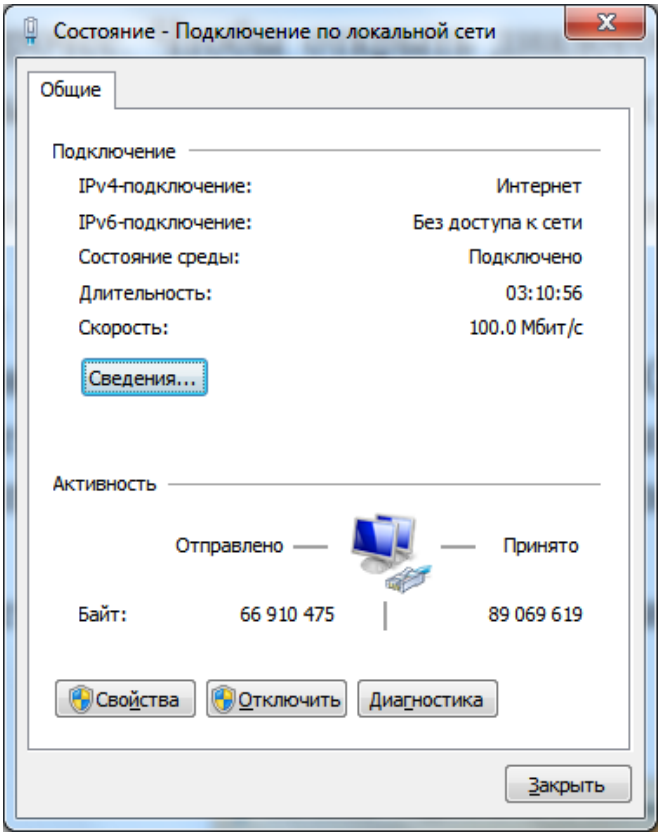


Рис. 1.6. Диалоговое окно состояния подключения по локальной сети

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.

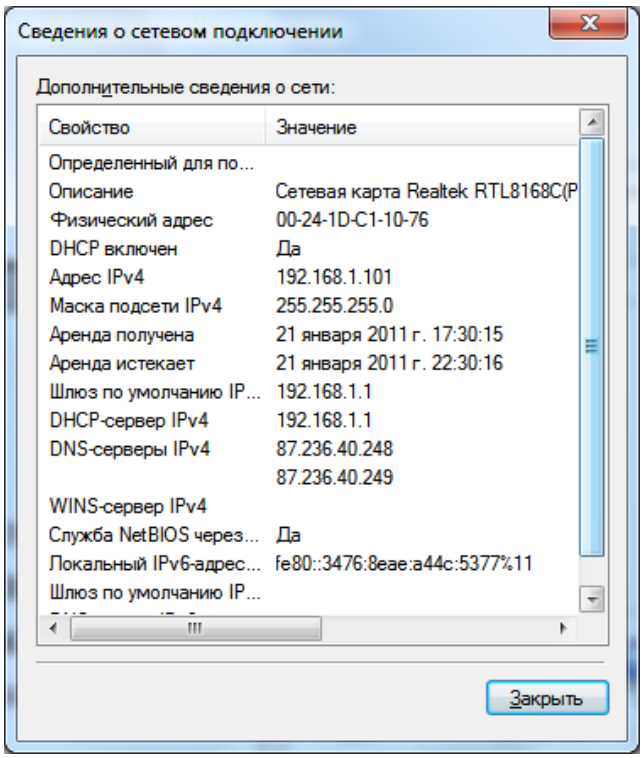


Рис. 1.7. Сведения о сетевом подключении

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.

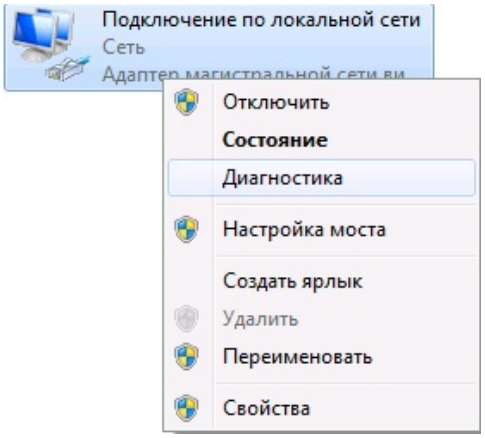


Рис. 1.8. Открытие мастера устранения неполадок подключения по локальной сети

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.1.11.).

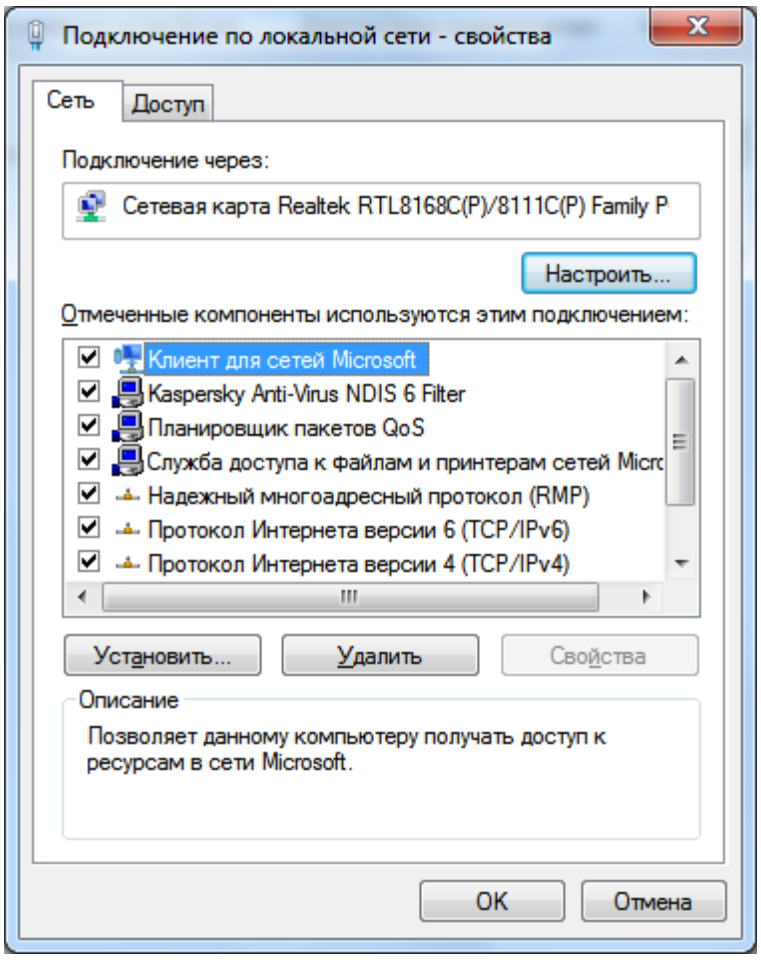


Рис. 1.11. Диалоговое окно свойств сетевого подключения

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». Рассмотрены понятия сетевого расположения, сетевых карт, при помощи которых отображается локальная часть сетевой карты, компоновка которой зависит от имеющихся сетевых подключений. Также вы ознакомились с окном сетевых подключений, которое позволяет конфигурировать сетевые подключения на локальном компьютере. В следующей лабораторной работе вы узнаете о том, как можно настроить клиенты, службы и протоколы сетевых подключений при помощи пользовательского графического интерфейса.

Контрольные вопросы и задания для самоподготовки:

Какое назначение у компонента «Центр управления сетями и общим доступом»?

Продемонстрируйте, какие существуют способы открытия компонента «Центр управления сетями и общим доступом».

Охарактеризуйте типы сетевого расположения.

Что представляет собой карта сети, по сути, и по виду?

Какие протоколы отвечают за построение карты сети.

В каких ситуациях просмотр карты сети будет не возможен?

С каким аппаратным сетевым компонентом связываются свойства доступных сетевых подключений?

Какие существуют способы открытия окна «Сетевые подключения»?

Какие действия пользователь обычно может выполнить по отношению к любому сетевому подключению?

Охарактеризуйте свойства сведений о сетевом подключении для компьютера, на котором вы выполняете лабораторную работу. Объясните значения данных свойств.

Какими способами можно вызвать средства диагностики подключения?

Охарактеризуйте компоненты подключения к сети компьютера, за которым вы выполняете лабораторную работу.

Лабораторное занятие № 6. Настройка беспроводного подключения

Задание:

1. Настроить беспроводной маршрутизатор

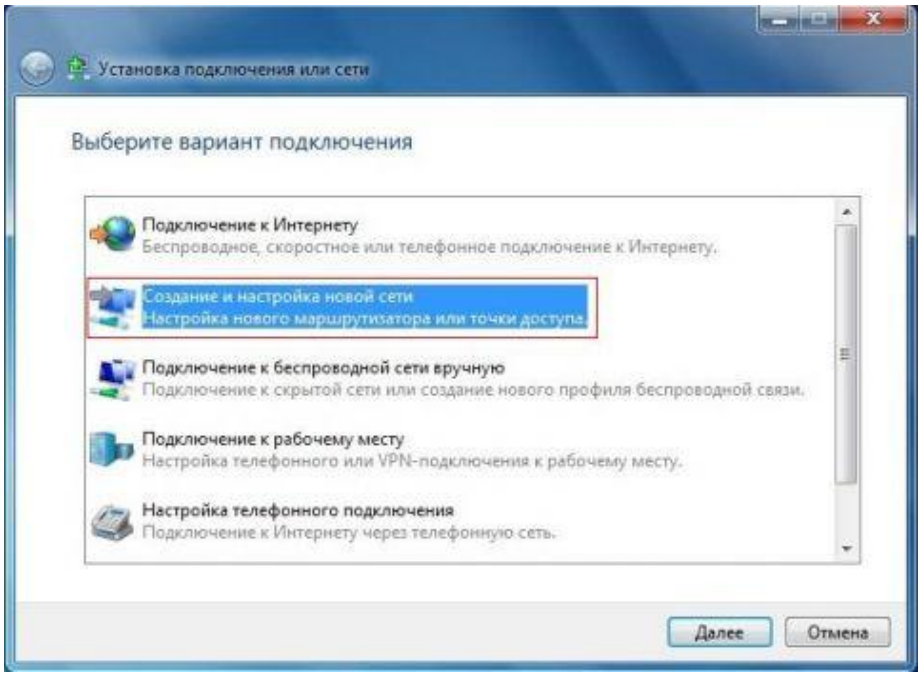
2. Подключиться к точке доступа через Push Button

3. Подключиться к точке доступа через импорт профиля сетевого подключения

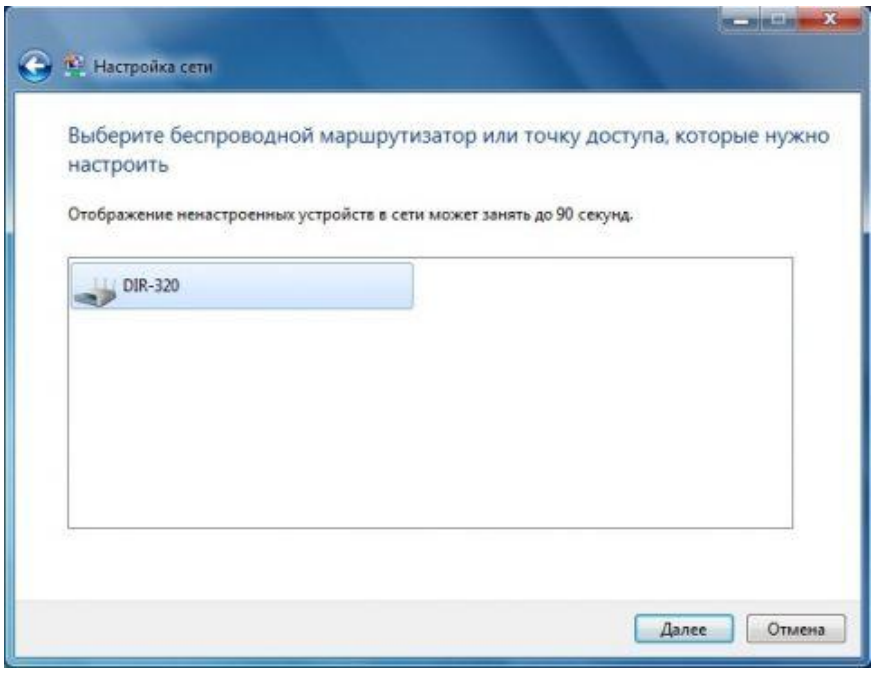
Порядок выполнения работы:

1 Настройка беспроводного маршрутизатора

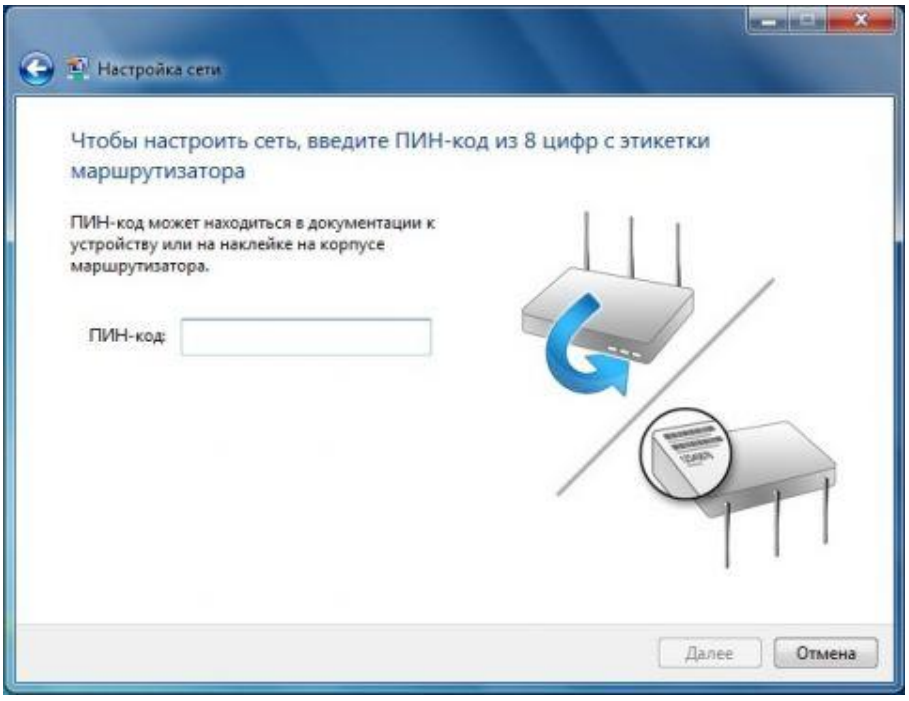
Устройство распаковано и подключено к электросети. Настраивать его можно через Ethernet, используя при этом патчкорд (который входит в комплект поставки) или через WiFi, но от этого никак не зависит сам процесс настройки. На ноутбуке или десктопе нужно зайти в Панель Управления – Центр управления сетями и общим доступом – Настройка нового подключения или сети, где выбрать Создание и настройка новой сети.



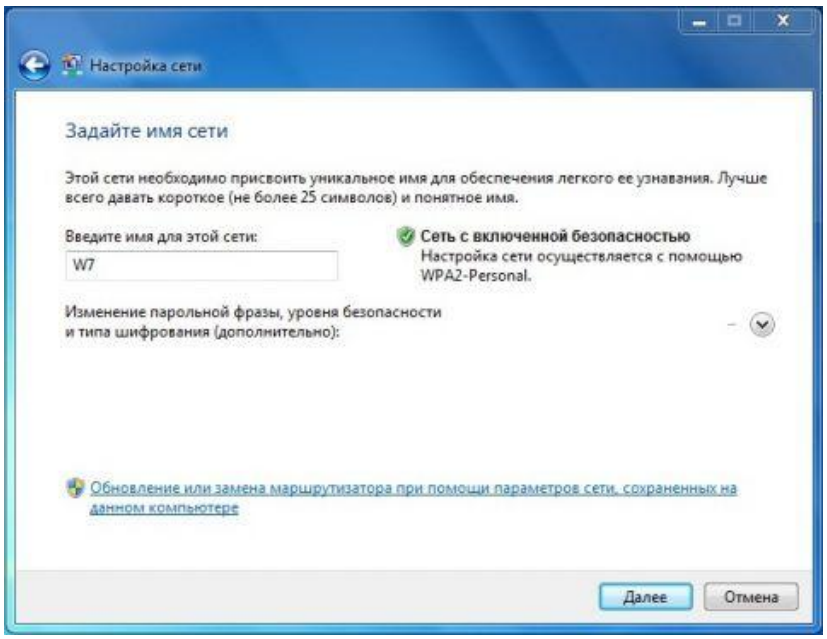
В списке устройств будут видны беспроводные устройства с поддержкой WCN. Выбираем именно нашу точку доступа (беспроводный маршрутизатор).



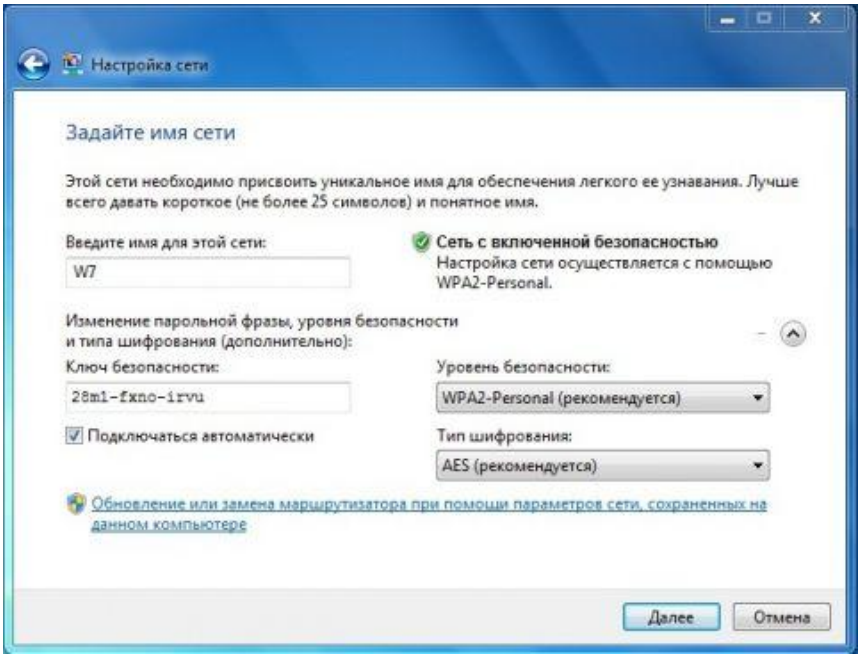
Следующим этапом необходимо вести ПИН-код с этикетки на маршрутизаторе.



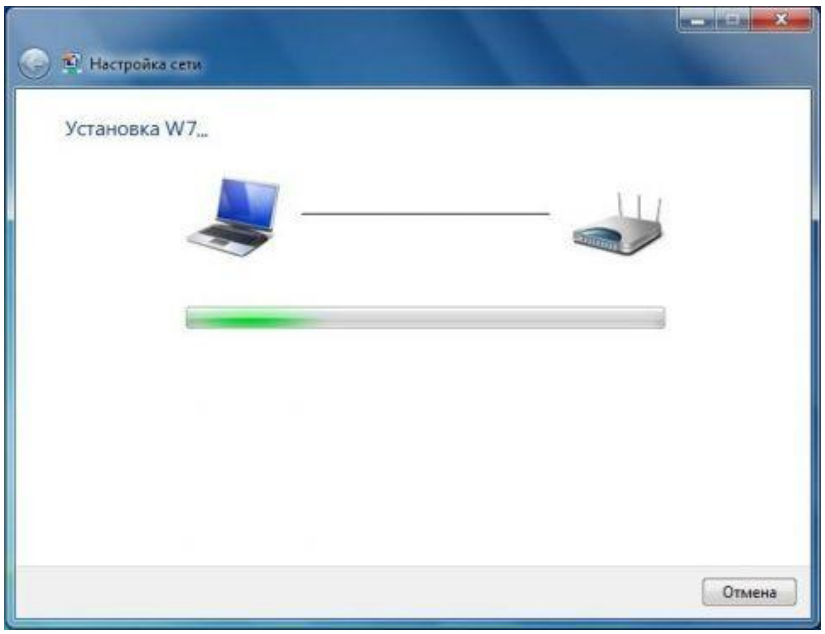
и после нажатия **Далее** согласиться с рекомендуемыми настройками точки доступа

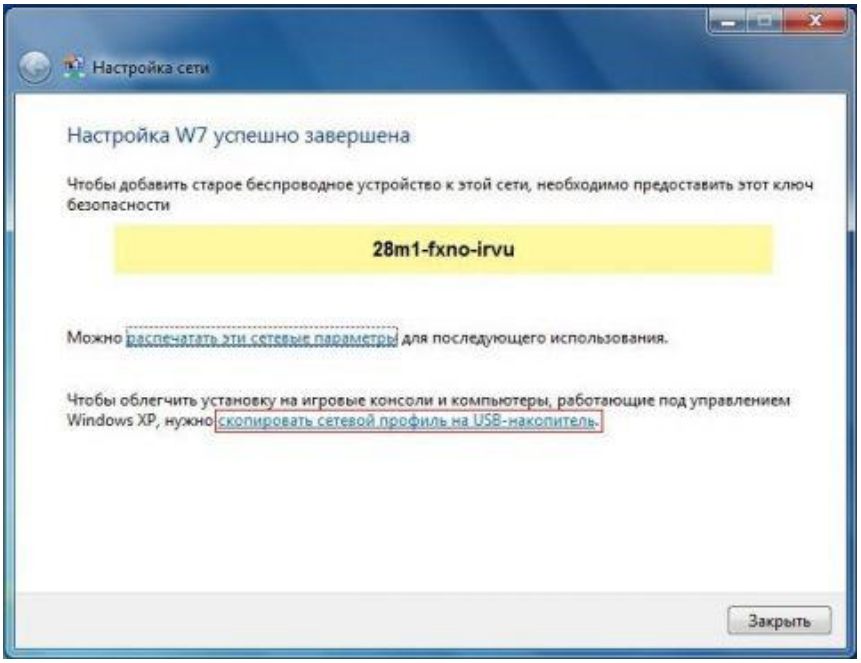


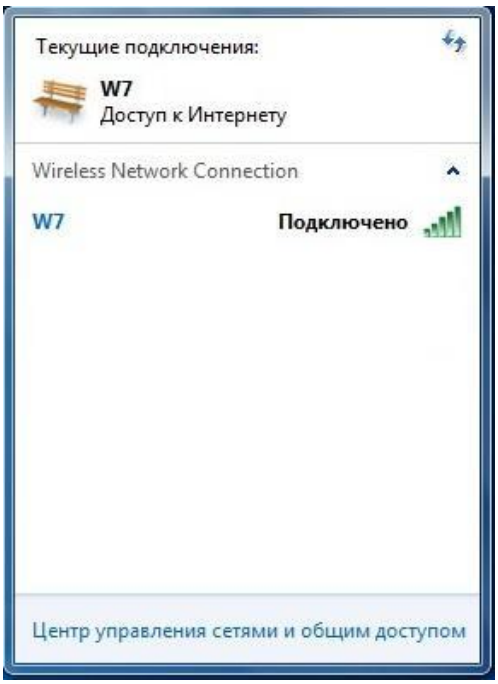
Или задать свои, есть в этом есть необходимость: имя беспроводной сети, пароль для доступа к сети, уровень безопасности и тип шифрования.



После нажатия кнопки **Далее** произойдет настройка точки доступа (беспроводного маршрутизатора) и автоматическое подключение к созданной беспроводной сети.


Настройка сети
Установка W7...
Отмена

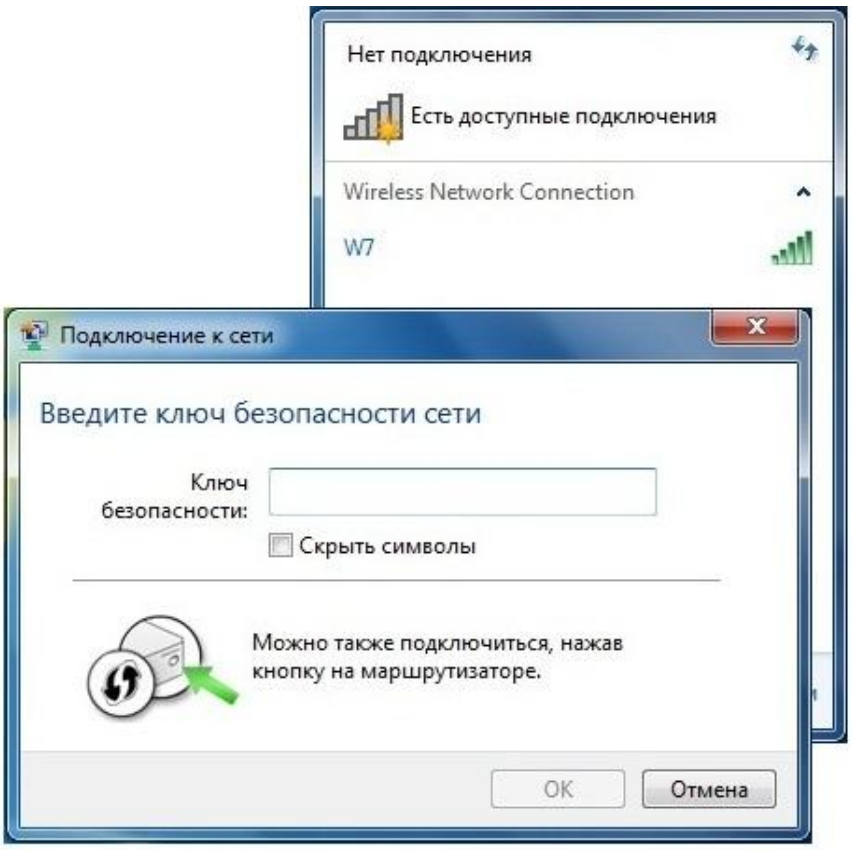

Настройка сети
Настройка W7 успешно завершена
Чтобы добавить старое беспроводное устройство к этой сети, необходимо предоставить этот ключ безопасности
28m1-fxno-irvu
Можно распечатать эти сетевые параметры для последующего использования.
Чтобы облегчить установку на игровые консоли и компьютеры, работающие под управлением Windows XP, нужно скопировать сетевой профиль на USB-накопитель.
Закрыть



По завершении настройки можно распечатать подробную инструкцию для подключения остальных компьютеров к точке доступа (беспроводному маршрутизатору), а также подготовить флешку с настройками для импорта сетевого профиля на другие беспроводные устройства. Если в данный момент в этом нет необходимости, то это можно сделать позже, в свойствах беспроводной сети.

Подключиться к точке доступа через Push Button

При подключении к нашей беспроводной сети с компьютера под управлением Windows 7, можно не вводить ключ безопасности, а нажать кнопку WCN на маршрутизаторе. Подключение к беспроводной сети произойдет автоматически.



На беспроводных устройствах, поддерживающих метод PBC, достаточно нажать кнопку WPS на маршрутизаторе, а потом на беспроводном устройстве, после чего произойдет подключения устройства к беспроводной сети.

На компьютерах, работающих под управлением более старых операционных систем Windows, а также на беспроводных устройствах, не поддерживающих метод Push Button, необходимо воспользоваться импортом профиля сетевого подключения к беспроводной сети.

Лабораторное занятие № 7. Получение таблицы MAC-адресов

Настраиваем устройства и проверяем подключения

Шаг 1. Создаем сеть согласно топологии.

a. Подключаем устройства, показанные в топологии, и кабели соответствующим образом.

b. Включаем все устройства в топологии.

Шаг 2. Настраиваем IPv4-адрес на ПК.

a. Настраиваем IPv4-адрес, маску подсети и адрес шлюза по умолчанию для компьютера PC-A.

b. Из командной строки компьютера PC-A отправляем эхо-запрос на адрес коммутатора.

Вопрос:

Успешно ли выполнена проверка связи? - Нет. Коммутатор еще не настроен.

Шаг 3. Настраиваем базовые параметры коммутатора. (Рис. 11)

a. Подключаемся к коммутатору с помощью консоли и переходим в режим глобальной настройки.

b. Назначаем коммутатору имя узла в соответствии с таблицей адресации.

c. Отключаем поиск DNS.

```
Switch>enable
Switch#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.2 255.255.255.0
S1(config-if)#no shutdown
```

Рис. 11. Шаг 3

Шаг 4. Проверяем подключение к сети.

Посылаем Ping на коммутатор с PC-A. (Рис. 12)

```
S1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/6 ms
```

Рис. 12. Посылаем эхо-запрос

Вопрос:

Успешно ли выполнена проверка связи? - Успешно

Часть 2. Отображаем, описываем и анализируем мас-адресы Ethernet

Шаг 1. Анализируем MAC-адрес сетевой платы компьютера PC-A.

a. Используя результаты выполнения команды ipconfig /all, ответили на следующие вопросы.

Какая часть MAC-адреса этого устройства соответствует OUI? - 5C-26-0A

Какая часть MAC-адреса этого устройства соответствует серийному номеру? - 24-2A-60

В приведенном выше примере определите производителя сетевой платы. - Dell Inc.

b. Вводим команду ipconfig /all в командной строке на компьютере PC-A и

Шаг 2. Анализируем MAC-адрес интерфейса F0/6 коммутатора S1.

a. С помощью консоли подключаемся к коммутатору S1 и выполняем команду show interfaces vlan 1, чтобы найти информацию о MAC-адресе. (Рис. 13)

```
S1>sh interface vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.3ea7.49b4 (bia 0060.3ea7.49b4)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Рис. 13. Выводим интерфейсы

Какой MAC-адрес имеет интерфейс VLAN 1 на коммутаторе S1? – 0060.3EA7.49B4

Назовите производителя оборудования согласно OUI. - Cisco Systems

Что означает bia? - Burned in address

Почему в результатах выполнения команды дважды указан один и тот же MAC-адрес? – MAC-адрес можно изменить с помощью команды

программного обеспечения. Фактический адрес(bia) всё ещё будет там. Он указан в скобках

b. Другой способ отображения MAC-адреса на коммутаторе — это команда show arp. Отображаем MAC-адрес с помощью команды show arp. Она сопоставляет адрес уровня 2 с соответствующим адресом уровня 3.

Какие адреса уровня 2 отображены на коммутаторе S1? - S1 VLAN 1 и MAC-адреса ПК-А

3 уровня? - IP-адреса S1 и PC-A

Шаг 3. Смотрим на MAC-адреса коммутатора.

Выполняем команду show mac address-table на коммутаторе S1.

Является ли коммутатор MAC-адрес компьютера PC-A? Если вы ответили «да», на каком порте он находился? - Да. Порт F0/6. MAC-адрес 5c26.0a24.2a60.

Вопросы для повторения

1. Можете ли вы использовать широковещательную рассылку на уровне 2? Если да, то каким будет ее MAC-адрес? - У вас могут быть широковещательные рассылки на уровне 2. ARP будет использовать широковещательные рассылки для поиска информации о MAC-адресах. Широковещательный адрес: FF:FF:FF:FF:FF:FF.

2. Зачем нужно знать MAC-адрес устройства? - Могут быть самые разные причины. В большой сети может быть проще определить местоположение и идентификацию устройства по его MAC-адресу, а не по IP-адресу. В MAC OUI будет указан производитель, что может помочь сузить поиск. Меры безопасности могут применяться на уровне 2, поэтому необходимо знать допустимые MAC-адреса.

Лабораторное занятие № 8. Настройка режимов и скорости.

Чтобы получить доступ в Internet через модем, необходимо осуществить настройку соединения к серверу удаленного доступа

Провайдера, после чего необходимо осуществить непосредственно само подключение. Для идентификации пользователя, а так же с целью защиты от несанкционированного доступа в сеть других пользователей, каждый абонент имеет свой уникальный логин и пароль доступа, которые вводятся при осуществлении подключения.

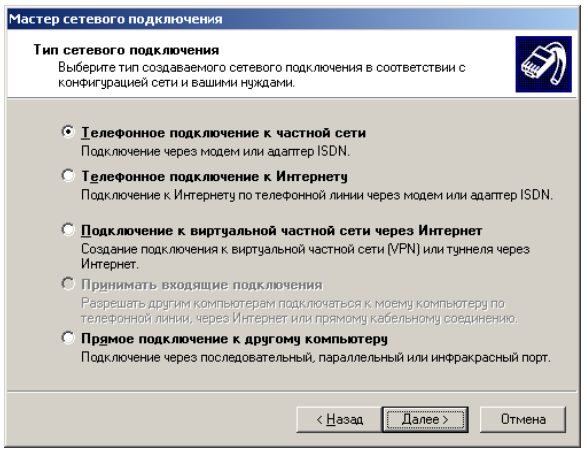
Задание №1. Подключение модема.

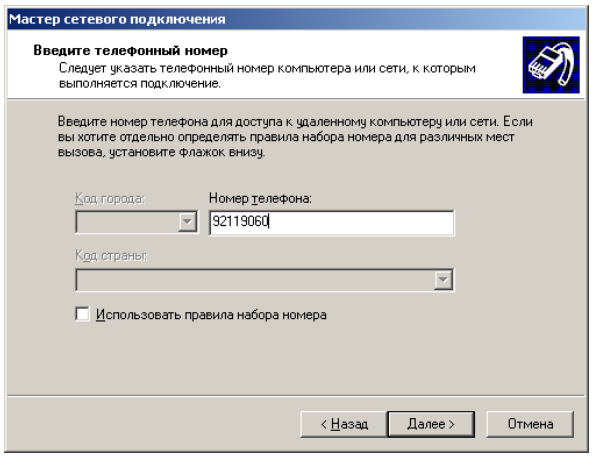
Включите модем.

Выберите в меню кнопки «**Пуск**» пункты «**Настройка - Сеть и удаленный доступ к сети**. После появления окна «Сеть и удаленный доступ» выберите **Создание нового подключения**. Запустится мастер для создания нового подключения. Нажмите кнопку «**Далее**».

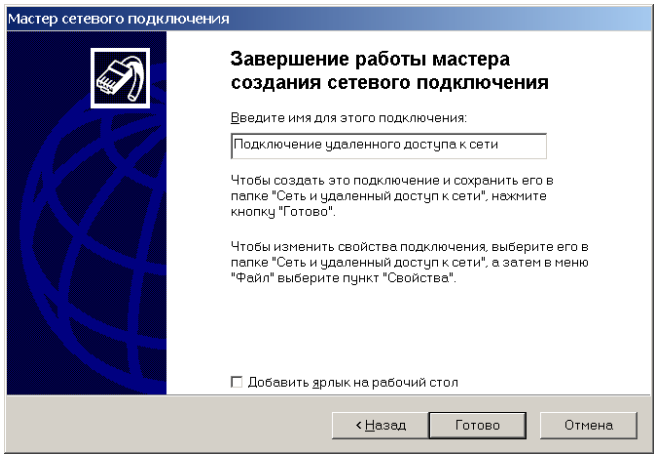
Следуйте указаниям мастера сетевого подключения, приведенным в Приложении 1. При запросе мастера на ввод номера телефона, введите номер, приведенный в Приложении 2. В конце работы мастера нажмите «**Готово**» (Приложение 3). Настройка подключения завершена.

Приложение 1. Приложение 2.





Приложение 3



При выполнении задания необходимо:

1. Сделать копию изображения текущего состояния экрана нажав при этом клавиши Alt+PrintScreen.

2. Установить курсор в то место, куда будет вставлено изображение;

3. Используя контекстное меню команда Вставить, или комбинацию клавиш Ctrl+V вставить изображение на котором будет отражаться ход решения задания.

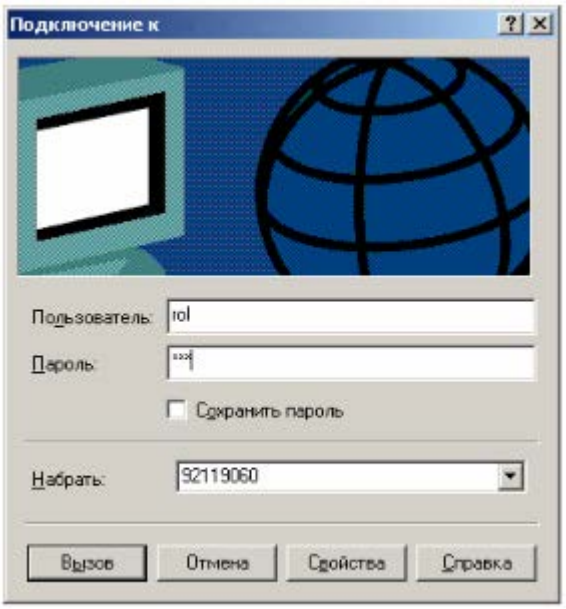
Место вставки изображения

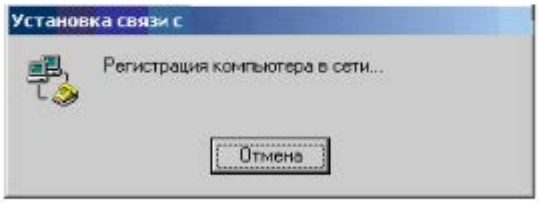
Задание №2. Подключение к Internet.

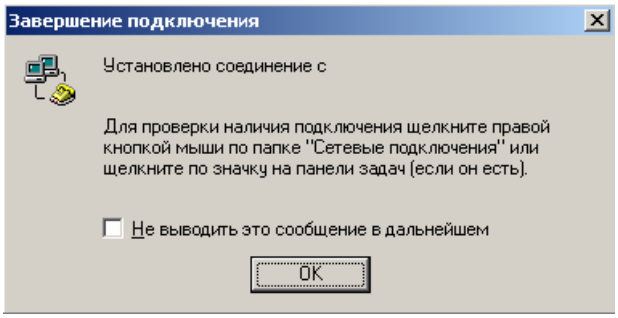
Откройте «Сетевое окружение», щелкнув на соответствующий ярлык на рабочем столе.

Найдите в открывшемся окне ярлык с созданным выше сетевым подключением и имеющий имя, введенное во время настройки, и щелкните его. Откроется окно с вводом логина и пароля.

Введите логин **rol** и пароль **rol**, нажмите кнопку «**Вызов**». Произойдет подключение к серверу удаленного доступа **Провайдера**, во время этого на экране будут появляться следующие сообщения:







1. На последнем сообщении нажмите «**ОК**». Все, компьютер подключен к сети **Internet** через сервер удаленного доступа **Провайдера**. Если во время подключения на экране появится окно с сообщением об ошибке и текстом о том, что телефонная линия занята, нажмите в этом окне кнопку «**Повторный звонок**».

2. Проверьте работу **Internet** на компьютере, для этого запустите обозреватель **Internet Explorer** и в его адресной строке введите адрес **http://try.rol.ru/** . Дождитесь загрузки сайта. Если сайт открывается, значит настройка и подключение к **Internet** осуществлено успешно. Предъявите загруженный сайт try.rol.ru преподавателю!

3. Отключитесь от **Internet**. Для этого дважды нажмите на панели задач значок  (в правом нижнем углу монитора), и нажмите в открывшемся

окне кнопку «**Отключить**». Дождитесь отключения, о чем свидетельствует закрытие окна.

При выполнении задания необходимо:

1. Сделать копию изображения текущего состояния экрана нажав при этом клавиши Alt+PrintScreen.

2. Установить курсор в то место, куда будет вставлено изображение;

3. Используя контекстное меню команда Вставить, или комбинацию клавиш Ctrl+V вставить изображение на котором будет отражаться ход решения задания.

Место вставки изображения

Контрольные вопросы

1. Что такое Модем?

2. Перечислите единицы измерения скорости передачи данных

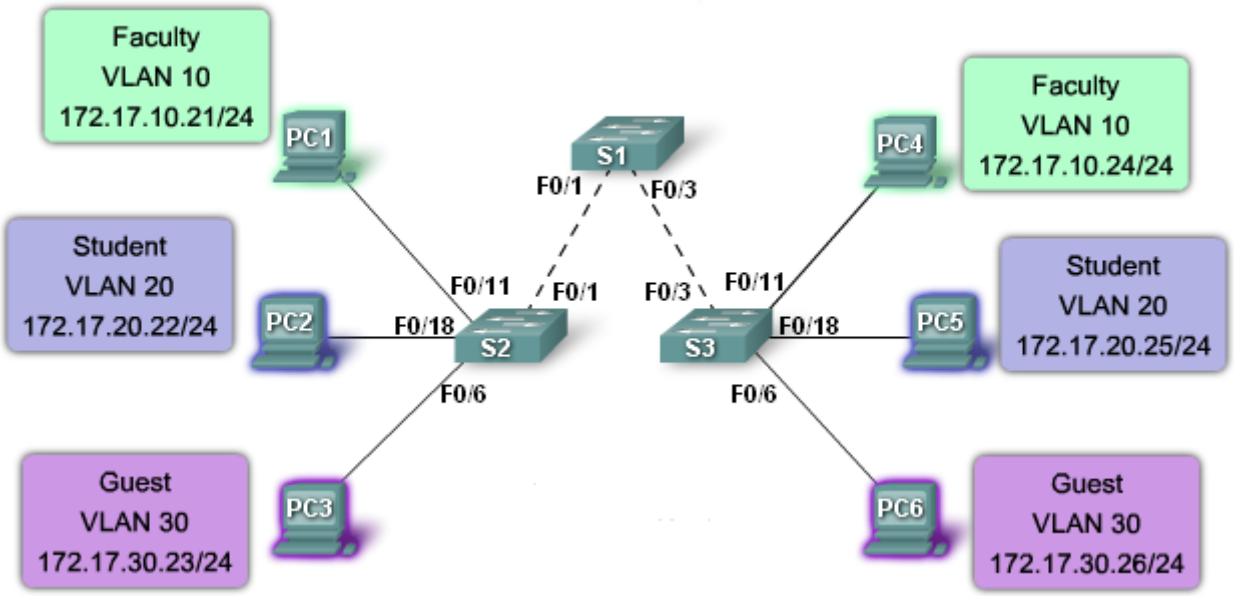
3. Как называются программы размещены программы, показывающие вашу скорость относительно какого-либо сайта

4. Перечислите основные этапы подключения модема

5. Перечислите основные этапы подключения к Internet

Лабораторное занятие № 9. Настройка портов коммутатора

Реализуйте представленную на рисунке ниже топологию и выполните настройку VLAN (используйте коммутаторы 2900 серии).



Лабораторное занятие № 10. Выполнение эхо-запросов

Выполним эхо-запросы от Station1 и Remote1 на все узлы сети:

Station1 -> Station2

Station1 Echo Request Packet Network Created Echo Request packet to 192.168.1.3

Station1 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.3).

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ICMP_packet Network ProtocolStack received packet from local Interface.

Station2 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station2 Echo Reply Packet Network Created Echo Reply packet to 192.168.1.2

Station2 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.1.2

Station2 ARP_packet Network Sending broadcast packet from ProtocolStack.

Station2 Ethernet Packet Link Sending packet from interface 9D:B6:69:19:3A:AE

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ARP_packet Network ProtocolStack received packet from local Interface.

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station1 ARP Response Packet DataLink Created ARP Response packet to 192.168.1.3

Station1 ARP_packet Network Sending packet from ProtocolStack (to 192.168.1.3).

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ARP_packet Network ProtocolStack received packet from local Interface.

Station2 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station2 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.2).

Station2 Ethernet Packet Link Sending packet from interface 9D:B6:69:19:3A:AE

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ICMP_packet Network ProtocolStack received packet from local Interface.

Station1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station1 Echo Reply Packet Network Echo reply packet received from 192.168.1.3

Пакет доставлен корректно и отчет пришел.

Station1 -> Station3

Station1 Echo Request Packet Network Created Echo Request packet to 192.168.1.4

Station1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.1.4

Station1 ARP_packet Network Sending broadcast packet from ProtocolStack.

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ARP_packet Network ProtocolStack received packet from local Interface.

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station3 ARP Response Packet DataLink Created ARP Response packet to 192.168.1.2

Station3 ARP_packet Network Sending packet from ProtocolStack (to 192.168.1.2).

Station3 Ethernet Packet Link Sending packet from interface 20:4E:93:57:1A:B2

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.4).

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ICMP_packet Network ProtocolStack received packet from local Interface.

Station3 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station3 Echo Reply Packet Network Created Echo Reply packet to 192.168.1.2

Station3 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.2).

Station3 Ethernet Packet Link Sending packet from interface 20:4E:93:57:1A:B2

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ICMP_packet Network ProtocolStack received packet from local Interface.

Station1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station1 Echo Reply Packet Network Echo reply packet received from 192.168.1.4

Пакет доставлен корректно и отчет пришел.

Station1 -> Station4

Station1 Echo Request Packet Network Created Echo Request packet to 192.168.1.5

Station1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.1.5

Station1 ARP_packet Network Sending broadcast packet from ProtocolStack.

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ARP_packet Network ProtocolStack received packet from local Interface.

Station4 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station4 ARP Response Packet DataLink Created ARP Response packet to 192.168.1.2

Station4 ARP_packet Network Sending packet from ProtocolStack (to 192.168.1.2).

Station4 Ethernet Packet Link Sending packet from interface 7D:5F:9C:24:56:70

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ARP_packet Network ProtocolStack received packet from local Interface.

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.5).

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ICMP_packet Network ProtocolStack received packet from local Interface.

Station4 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station4 Echo Reply Packet Network Created Echo Reply packet to 192.168.1.2

Station4 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.2).

Station4 Ethernet Packet Link Sending packet from interface 7D:5F:9C:24:56:70

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ICMP_packet Network ProtocolStack received packet from local Interface.

Station1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station1 Echo Reply Packet Network Echo reply packet received from 192.168.1.5

Пакет доставлен корректно и отчет пришел.

Remote1 -> Station1

Remote1 Echo Request Packet Network Created Echo Request packet to 192.168.1.2

Remote1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 99.11.0.10

Remote1 ARP_packet Network Sending broadcast packet from ProtocolStack.

Remote1 Ethernet Packet Link Sending packet from interface 14:53:2F:86:88:13

ADSL Ethernet Packet Link Recieved packet at interface A1:64:94:39:32:31

ADSL ARP_packet Network ProtocolStack received packet from local Interface.

ADSL ARP_packet Network Confirmed Packet is for this Network Layer Device.

ADSL ARP Response Packet DataLink Created ARP Response packet to 99.11.0.11

ADSL ARP_packet Network Sending packet from ProtocolStack (to 99.11.0.11).

ADSL Ethernet Packet Link Sending packet from interface A1:64:94:39:32:31

Remote1 Ethernet Packet Link Recieved packet at interface 14:53:2F:86:88:13

Remote1 ARP_packet Network ProtocolStack received packet from local Interface.

Remote1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Remote1 ICMP_packet Network Sending packet from ProtocolStack (to 99.11.0.10).

Remote1 Ethernet Packet Link Sending packet from interface 14:53:2F:86:88:13

ADSL Ethernet Packet Link Recieved packet at interface A1:64:94:39:32:31

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.0.1

ADSL ARP_packet Network Sending broadcast packet from ProtocolStack.

ADSL Ethernet Packet Link Sending packet from interface 2D:48:66:2B:5B:16

R1 Ethernet Packet Link Recieved packet at interface 86:96:4D:62:BD:97

R1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

R1 ARP Response Packet DataLink Created ARP Response packet to 192.168.0.2

R1 ARP_packet Network Sending packet from ProtocolStack (to 192.168.0.2).

R1 Ethernet Packet Link Sending packet from interface 86:96:4D:62:BD:97

ADSL Ethernet Packet Link Recieved packet at interface 2D:48:66:2B:5B:16

ADSL ARP_packet Network ProtocolStack received packet from local Interface.

ADSL ARP_packet Network Confirmed Packet is for this Network Layer Device.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.1).

ADSL Ethernet Packet Link Sending packet from interface 2D:48:66:2B:5B:16

R1 Ethernet Packet Link Recieved packet at interface 86:96:4D:62:BD:97

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.1.2

R1 ARP_packet Network Sending broadcast packet from ProtocolStack.

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ARP_packet Network ProtocolStack received packet from local Interface.

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station1 ARP Response Packet DataLink Created ARP Response packet to 192.168.1.1

Station1 ARP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.1.2).

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ICMP_packet Network ProtocolStack received packet from local Interface.

Station1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station1 Echo Reply Packet Network Created Echo Reply packet to 99.11.0.11

Station1 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station1 Ethernet Packet Link Sending packet from interface A7:AB:51:BC:C1:A5

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.2).

R1 Ethernet Packet Link Sending packet from interface 86:96:4D:62:BD:97

ADSL Ethernet Packet Link Recieved packet at interface 2D:48:66:2B:5B:16

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 99.11.0.11).

ADSL Ethernet Packet Link Sending packet from interface A1:64:94:39:32:31

Remote1 Ethernet Packet Link Recieved packet at interface 14:53:2F:86:88:13

Remote1 ICMP_packet Network ProtocolStack received packet from local Interface.

Remote1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Remote1 Echo Reply Packet Network Echo reply packet received from 192.168.1.2

Пакет доставлен корректно и отчет пришел.

Remote1 -> Station2

Remote1 Echo Request Packet Network Created Echo Request packet to 192.168.1.3

Remote1 ICMP_packet Network Sending packet from ProtocolStack (to 99.11.0.10).

Remote1 Ethernet Packet Link Sending packet from interface 14:53:2F:86:88:13

ADSL Ethernet Packet Link Recieved packet at interface A1:64:94:39:32:31

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.1).

ADSL Ethernet Packet Link Sending packet from interface 2D:48:66:2B:5B:16

R1 Ethernet Packet Link Recieved packet at interface 86:96:4D:62:BD:97

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.1.3

R1 ARP_packet Network Sending broadcast packet from ProtocolStack.

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ARP_packet Network ProtocolStack received packet from local Interface.

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ARP_packet Network ProtocolStack received packet from local Interface.

Station2 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station2 ARP Response Packet DataLink Created ARP Response packet to 192.168.1.1

Station2 ARP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station2 Ethernet Packet Link Sending packet from interface 9D:B6:69:19:3A:AE

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.1.3).

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ICMP_packet Network ProtocolStack received packet from local Interface.

Station2 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station2 Echo Reply Packet Network Created Echo Reply packet to 99.11.0.11

Station2 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station2 Ethernet Packet Link Sending packet from interface 9D:B6:69:19:3A:AE

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.2).

R1 Ethernet Packet Link Sending packet from interface 86:96:4D:62:BD:97

ADSL Ethernet Packet Link Recieved packet at interface 2D:48:66:2B:5B:16

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 99.11.0.11).

ADSL Ethernet Packet Link Sending packet from interface A1:64:94:39:32:31

Remote1 Ethernet Packet Link Recieved packet at interface 14:53:2F:86:88:13

Remote1 ICMP_packet Network ProtocolStack received packet from local Interface.

Remote1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Remote1 Echo Reply Packet Network Echo reply packet received from 192.168.1.3

Пакет доставлен корректно и отчет пришел.

Remote1 -> Station3

Remote1 Echo Request Packet Network Created Echo Request packet to 192.168.1.4

Remote1 ICMP_packet Network Sending packet from ProtocolStack (to 99.11.0.10).

Remote1 Ethernet Packet Link Sending packet from interface 14:53:2F:86:88:13

ADSL Ethernet Packet Link Recieved packet at interface A1:64:94:39:32:31

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.1).

ADSL Ethernet Packet Link Sending packet from interface 2D:48:66:2B:5B:16

R1 Ethernet Packet Link Recieved packet at interface 86:96:4D:62:BD:97

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.1.4

R1 ARP_packet Network Sending broadcast packet from ProtocolStack.

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ARP_packet Network ProtocolStack received packet from local Interface.

Station3 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station3 ARP Response Packet DataLink Created ARP Response packet to 192.168.1.1

Station3 ARP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station3 Ethernet Packet Link Sending packet from interface 20:4E:93:57:1A:B2

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.1.4).

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ICMP_packet Network ProtocolStack received packet from local Interface.

Station3 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station3 Echo Reply Packet Network Created Echo Reply packet to 99.11.0.11

Station3 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station3 Ethernet Packet Link Sending packet from interface 20:4E:93:57:1A:B2

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.2).

R1 Ethernet Packet Link Sending packet from interface 86:96:4D:62:BD:97

ADSL Ethernet Packet Link Recieved packet at interface 2D:48:66:2B:5B:16

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 99.11.0.11).

ADSL Ethernet Packet Link Sending packet from interface A1:64:94:39:32:31

Remote1 Ethernet Packet Link Recieved packet at interface 14:53:2F:86:88:13

Remote1 ICMP_packet Network ProtocolStack received packet from local Interface.

Remote1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Remote1 Echo Reply Packet Network Echo reply packet received from 192.168.1.4

Пакет доставлен корректно и отчет пришел.

Remote1 -> Station4

Remote1 Echo Request Packet Network Created Echo Request packet to 192.168.1.5

Remote1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 99.11.0.10

Remote1 ARP_packet Network Sending broadcast packet from ProtocolStack.

Remote1 Ethernet Packet Link Sending packet from interface 14:53:2F:86:88:13

ADSL Ethernet Packet Link Recieved packet at interface A1:64:94:39:32:31

ADSL ARP_packet Network ProtocolStack received packet from local Interface.

ADSL ARP_packet Network Confirmed Packet is for this Network Layer Device.

ADSL ARP Response Packet DataLink Created ARP Response packet to 99.11.0.11

ADSL ARP_packet Network Sending packet from ProtocolStack (to 99.11.0.11).

ADSL Ethernet Packet Link Sending packet from interface A1:64:94:39:32:31

Remote1 Ethernet Packet Link Recieved packet at interface 14:53:2F:86:88:13

Remote1 ARP_packet Network ProtocolStack received packet from local Interface.

Remote1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Remote1 ICMP_packet Network Sending packet from ProtocolStack (to 99.11.0.10).

Remote1 Ethernet Packet Link Sending packet from interface 14:53:2F:86:88:13

ADSL Ethernet Packet Link Recieved packet at interface A1:64:94:39:32:31

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.0.1

ADSL ARP_packet Network Sending broadcast packet from ProtocolStack.

ADSL Ethernet Packet Link Sending packet from interface 2D:48:66:2B:5B:16

R1 Ethernet Packet Link Recieved packet at interface 86:96:4D:62:BD:97

R1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

R1 ARP Response Packet DataLink Created ARP Response packet to 192.168.0.2

R1 ARP_packet Network Sending packet from ProtocolStack (to 192.168.0.2).

R1 Ethernet Packet Link Sending packet from interface 86:96:4D:62:BD:97

ADSL Ethernet Packet Link Recieved packet at interface 2D:48:66:2B:5B:16

ADSL ARP_packet Network ProtocolStack received packet from local Interface.

ADSL ARP_packet Network Confirmed Packet is for this Network Layer Device.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.1).

ADSL Ethernet Packet Link Sending packet from interface 2D:48:66:2B:5B:16

R1 Ethernet Packet Link Recieved packet at interface 86:96:4D:62:BD:97

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ARP Discovery Packet DataLink Created ARP discovery packet to source MAC address for IP 192.168.1.5

R1 ARP_packet Network Sending broadcast packet from ProtocolStack.

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ARP_packet Network ProtocolStack received packet from local Interface.

Station4 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station4 ARP Response Packet DataLink Created ARP Response packet to 192.168.1.1

Station4 ARP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station4 Ethernet Packet Link Sending packet from interface 7D:5F:9C:24:56:70

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ARP_packet Network Confirmed Packet is for this Network Layer Device.

Station3 Ethernet Packet Link Recieved packet at interface 20:4E:93:57:1A:B2

Station3 ARP_packet Network ProtocolStack received packet from local Interface.

Station2 Ethernet Packet Link Recieved packet at interface 9D:B6:69:19:3A:AE

Station2 ARP_packet Network ProtocolStack received packet from local Interface.

Station1 Ethernet Packet Link Recieved packet at interface A7:AB:51:BC:C1:A5

Station1 ARP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.1.5).

R1 Ethernet Packet Link Sending packet from interface C4:8E:66:51:BE:A9

Station4 Ethernet Packet Link Recieved packet at interface 7D:5F:9C:24:56:70

Station4 ICMP_packet Network ProtocolStack received packet from local Interface.

Station4 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Station4 Echo Reply Packet Network Created Echo Reply packet to 99.11.0.11

Station4 ICMP_packet Network Sending packet from ProtocolStack (to 192.168.1.1).

Station4 Ethernet Packet Link Sending packet from interface 7D:5F:9C:24:56:70

R1 Ethernet Packet Link Recieved packet at interface C4:8E:66:51:BE:A9

R1 ICMP_packet Network ProtocolStack received packet from local Interface.

R1 ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

R1 ICMP_packet Network Forwarding packet from ProtocolStack(to 192.168.0.2).

R1 Ethernet Packet Link Sending packet from interface 86:96:4D:62:BD:97

ADSL Ethernet Packet Link Recieved packet at interface 2D:48:66:2B:5B:16

ADSL ICMP_packet Network ProtocolStack received packet from local Interface.

ADSL ICMP_packet Network Packet Received: Network Layer Device is Routable forwarding packet.

ADSL ICMP_packet Network Forwarding packet from ProtocolStack(to 99.11.0.11).

ADSL Ethernet Packet Link Sending packet from interface A1:64:94:39:32:31

Remote1 Ethernet Packet Link Recieved packet at interface 14:53:2F:86:88:13

Remote1 ICMP_packet Network ProtocolStack received packet from local Interface.

Remote1 ICMP_packet Network Confirmed Packet is for this Network Layer Device.

Remote1 Echo Reply Packet Network Echo reply packet received from 192.168.1.5

Пакет доставлен корректно и отчет пришел.

Итак, видно, что все пакеты были доставлены корректно и пришли отчеты о доставке.

Таким образом можно сказать, что сеть работает правильно.

Лабораторное занятие № 11. Настройка коммутатора

Цель занятия: Освоить основные навыки настройки коммутатора, включая конфигурирование портов, VLAN и базовых функций безопасности.

Оборудование:

Коммутатор (указать модель)

Кабели Ethernet

ПК с консольным кабелем и программным обеспечением для терминального доступа (например, PuTTY)

(Опционально) дополнительные ПК для тестирования

Ход работы:

Часть 1: Подключение и первичная настройка:

1. Физическое подключение: Подключите консольный кабель от ПК к консольному порту коммутатора. Подключите хотя бы один ПК к одному из портов коммутатора для тестирования.

2. Настройка терминального эмулятора: Откройте терминальный эмулятор (PuTTY) и настройте параметры подключения (скорость передачи данных – обычно 9600 бод, 8 бит данных, 1 стоп-бит, без контроля четности).

3. Вход в режим конфигурирования: После успешного подключения к коммутатору, возможно, потребуется ввести имя пользователя и пароль (по умолчанию – часто `admin` или `cisco` и пустой пароль. Внимательно изучите документацию к вашей модели коммутатора). Затем войдите в режим конфигурирования командой `enable` (или аналогичной, в зависимости от модели).

4. Настройка пароля: Сразу после входа в систему, измените пароль по умолчанию на более безопасный, используя команду `configure terminal` (или аналогичную), а затем `enable secret <новый_пароль>`.

Часть 2: Конфигурирование портов:

1. Настройка порта: Используя команду `interface <номер_порта>`, войдите в режим конфигурирования выбранного порта (например, `interface GigabitEthernet0/1`).

2. Настройка скорости и дуплекса: Установите желаемую скорость и режим дуплекса (например, `speed 100` и `duplex full`). Проверьте совместимость с подключенным оборудованием.

3. Включение/отключение порта: Используйте команды `shutdown` и `no shutdown` для выключения и включения порта соответственно.

4. (Опционально) Настройка Port Security: Настройте ограничения доступа к порту, например, ограничение количества MAC-адресов, которые могут быть подключены к порту.

Часть 3: Создание и настройка VLAN:

1. Создание VLAN: Создайте несколько VLAN с помощью команды `vlan <номер_vlan>` (например, `vlan 10`, `vlan 20`).

2. Наименование VLAN: Дайте VLAN-ам понятные имена, используя команду `name <имя_vlan>` (например, `name Marketing`, `name Sales`).

3. Настройка портов для VLAN: Присвойте портам принадлежность к созданным VLAN, используя команды `interface <номер_порта>` и `switchport access vlan <номер_vlan>`.

4. (Опционально) Настройка Trunking: Настройте trunking для объединения нескольких VLAN на одном физическом порте. Это более продвинутая тема и может потребовать дополнительной информации из документации.

Часть 4: Базовая настройка безопасности:

1. Включение STP (Spanning Tree Protocol): Включите STP для предотвращения сетевых петель. Команда может отличаться в зависимости от модели коммутатора.

2. (Опционально) Конфигурирование SSH: Настройте безопасный доступ к коммутатору по SSH.

Часть 5: Тестирование:

1. Проверка подключения: Проверьте, что ПК могут обмениваться данными между различными VLAN, если VLAN были настроены. Используйте команды `ping` для проверки связи.

2. Проверка работы STP: Создайте временную петлю в сети (подключите два порта коммутатора друг к другу) и убедитесь, что STP правильно предотвращает петлю. Не оставляйте петлю на длительное время.

Отчет:

В отчете необходимо описать все выполненные шаги, настройки, результаты тестирования и возникшие трудности (если таковые были). Включите скриншоты экрана с конфигурацией коммутатора.

Дополнительные задания (опционально):

Настройте более сложную VLAN-архитектуру с несколькими VLAN и trunk-портами.

Настройте QoS (Quality of Service) на коммутаторе.

Настройте более продвинутые функции безопасности, такие как RADIUS-аутентификация.

Примечание: Замените `<номер_порта>`, `<номер_vlan>`, `<новый_пароль>`, `<имя_vlan>` на ваши актуальные значения. Данные команды могут немного отличаться в зависимости от модели коммутатора. Внимательно изучите руководство пользователя вашего коммутатора.

Лабораторное занятие № 12. Настройка маршрутизатора

Цель занятия: Освоить основные навыки настройки маршрутизатора, включая конфигурирование интерфейсов, статических и динамических маршрутов, а также базовых функций безопасности.

Оборудование:

Маршрутизатор (указать модель)

Кабели Ethernet

ПК с консольным кабелем и программным обеспечением для терминального доступа (например, PuTTY)

(Опционально) дополнительные ПК и коммутаторы для построения более сложной сети.

Ход работы:

Часть 1: Подключение и первичная настройка:

Физическое подключение: Подключите консольный кабель от ПК к консольному порту маршрутизатора. Подключите, как минимум, один ПК к одному из Ethernet портов маршрутизатора. Для более сложных сценариев (см. дополнительные задания) потребуются дополнительные ПК и коммутаторы.

Настройка терминального эмулятора: Откройте терминальный эмулятор (PuTTY) и настройте параметры подключения (скорость передачи данных – обычно 9600 бод, 8 бит данных, 1 стоп-бит, без контроля четности). Скорость может варьироваться в зависимости от модели маршрутизатора. Проверьте документацию.

Вход в режим конфигурирования: После успешного подключения к маршрутизатору, введите имя пользователя и пароль (по умолчанию – часто admin или cisco и пустой пароль. Важно: Проверьте документацию к вашей модели маршрутизатора!). Затем войдите в режим привилегированного уровня командой enable (или аналогичной, в зависимости от модели) и в режим конфигурирования глобального уровня командой configure terminal (или аналогичной).

Настройка пароля: Измените пароль по умолчанию на более безопасный, используя команду enable secret <новый_пароль>. Рекомендуется также настроить пароль для доступа пользователя с помощью команды username <имя_пользователя> password <пароль>.

Часть 2: Конфигурирование интерфейсов:

Настройка интерфейса: Используя команду interface <тип_интерфейса> <номер_интерфейса>, войдите в режим конфигурирования выбранного

интерфейса (например, interface GigabitEthernet0/0, interface Serial0/0). Тип интерфейса зависит от используемого подключения (Ethernet, Serial).

Настройка IP-адреса: Настройте IP-адрес, маску подсети и шлюз по умолчанию для каждого интерфейса с помощью команд ip address <IP_адрес> <маска_подсети>, no shutdown.

(Опционально) Настройка DHCP: Настройте DHCP-сервер на одном из интерфейсов, чтобы автоматически назначать IP-адреса клиентам.

Часть 3: Настройка маршрутизации:

Настройка статических маршрутов: Настройте статические маршруты для соединения с другими сетями, используя команду ip route <сеть_назначения> <маска_подсети> <шлюз>.

(Опционально) Настройка динамических маршрутов: Настройте динамические маршруты с помощью протоколов RIP или OSPF. Это более сложная тема и требует дополнительной информации.

Часть 4: Базовая настройка безопасности:

Включение межсетевого экрана (Firewall): Включите межсетевой экран для защиты маршрутизатора от несанкционированного доступа. Команды зависят от модели маршрутизатора. Возможно, потребуется настройка ACL (Access Control List).

(Опционально) Конфигурирование SSH: Настройте безопасный доступ к маршрутизатору по SSH.

Часть 5: Тестирование:

Проверка связи: Проверьте, что ПК могут обмениваться данными между различными сетями. Используйте команды ping для проверки связи.

Проверка маршрутизации: Проверьте, что пакеты данных правильно маршрутизируются между сетями. Используйте трассировку маршрута (traceroute или tracert).

Отчет:

В отчете необходимо описать все выполненные шаги, настройки, результаты тестирования и возникшие трудности (если таковые были). Включите скриншоты экрана с конфигурацией маршрутизатора.

Дополнительные задания (опционально):

Создайте более сложную сеть с несколькими маршрутизаторами и коммутаторами.

Настройте NAT (Network Address Translation) для преобразования адресов.

Настройте VPN-соединение.

Настройте более продвинутые функции безопасности, такие как AAA (Authentication, Authorization, and Accounting).

Примечание: Замените <тип_интерфейса>, <номер_интерфейса>, <новый_пароль>, <IP_адрес>, <маска_подсети>, <шлюз>, <сеть_назначения> на ваши актуальные значения. Команды могут незначительно отличаться в зависимости от модели маршрутизатора и используемой операционной системы (Cisco IOS, Juniper Junos и т.д.). Внимательно изучите руководство пользователя вашего маршрутизатора! Эта инструкция предоставляет лишь общий план, а детали настройки зависят от конкретного оборудования.

Лабораторное занятие № 13. Выполнение трассировки маршрута и тестирование пути

Цель занятия: Научиться использовать утилиты для трассировки маршрута (traceroute/tracert) и тестирования соединения (ping), а также интерпретировать полученные результаты для диагностики сетевых проблем.

Оборудование:

Несколько компьютеров, подключенных к сети (минимум два)

Доступ к интернету (для трассировки удаленных хостов)

Ход работы:

Часть 1: Использование утилиты ping:

Проверка доступности хоста: Используйте команду ping <адрес_хоста> (например, ping google.com, ping 8.8.8.8, ping 192.168.1.1) для проверки доступности удаленного или локального хоста. Обратите внимание на следующие параметры:

Успешные ответы: Показывает, что хост доступен и отвечает на запросы ICMP (Internet Control Message Protocol). Обратите внимание на время ответа (время "туда-обратно"). Большое время ответа может указывать на задержки в сети.

Потеря пакетов: Если часть пакетов теряется (packet loss), это свидетельствует о проблемах в соединении (повреждение кабеля, перегрузка сети, проблемы с маршрутизацией).

Время жизни (TTL): Параметр TTL (Time To Live) уменьшается на каждом маршрутизаторе, через который проходит пакет. По его значению можно косвенно оценить количество маршрутизаторов на пути.

Изменение параметров ping: Попробуйте изменить параметры команды ping, например, количество отправляемых пакетов (-n или -c), размер пакетов (-s или -l), интервал между отправкой пакетов (-i). Это поможет получить более детальную информацию о состоянии соединения.

Часть 2: Использование утилиты traceroute/tracert:

Трассировка маршрута: Используйте команду traceroute <адрес_хоста> (Linux/macOS) или tracert <адрес_хоста> (Windows) для определения пути, по которому пакеты проходят от вашего компьютера до целевого хоста. Обратите внимание на:

Список хостов: Команда отобразит список IP-адресов всех маршрутизаторов и других сетевых устройств на пути к целевому хосту. Это позволяет визуализировать маршрут и идентифицировать потенциальные точки сбоя.

Время ответа: Для каждого хоста указывается время ответа (в миллисекундах). Значительное увеличение времени ответа на каком-либо этапе может указывать на перегруженный или неисправный маршрутизатор.

"*" или "Request timed out": Если вы видите звездочки или сообщение о превышении времени ожидания, это означает, что пакет не смог достичь данного хоста, что может указывать на проблему на данном участке сети.

Анализ результатов: Проанализируйте полученный список IP-адресов. Попробуйте определить, какие устройства находятся на пути (маршрутизаторы провайдера, маршрутизаторы вашей локальной сети и т.д.).

Часть 3: Тестирование пути с помощью различных инструментов (опционально):

Существуют более сложные инструменты для тестирования сетевых путей, такие как:

Wireshark: Для глубокого анализа сетевого трафика.

Network monitoring tools: Различные программы для мониторинга сети (наличие которых зависит от используемой операционной системы и сети).

Часть 4: Диагностика проблем:

На основе результатов ping и traceroute/tracert попытайтесь диагностировать возможные проблемы в сети:

Проблемы с соединением: Потеря пакетов при ping может указывать на поврежденный кабель, неисправное сетевое оборудование или перегрузку сети.

Проблемы с маршрутизацией: Если traceroute/tracert показывает "*“ или "Request timed out" на каком-то этапе, это может быть связано с неправильной настройкой маршрутизации на маршрутизаторах или с неисправностью оборудования.

Проблемы с доступностью хоста: Если ping не отвечает, а traceroute/tracert успешно доходит до целевого хоста, проблема может быть на стороне целевого хоста (например, он выключен или настроен неправильно).

Отчет:

В отчете необходимо указать:

Используемые команды и параметры.

Полученные результаты (ping и traceroute/tracert).

Анализ результатов и выводы о состоянии сети.

Если были обнаружены проблемы, предложите возможные решения.

Дополнительные задания (опционально):

Проведите трассировку маршрута до разных хостов (например, до серверов разных провайдеров).

Сравните результаты traceroute/tracert с разных компьютеров в сети.

Используйте более продвинутые инструменты для анализа сети.

Примечание: Замените <адрес_хоста> на фактический IP-адрес или доменное имя. Результаты traceroute/tracert могут меняться в зависимости от текущей сетевой конфигурации. Не все хосты отвечают на запросы ICMP, поэтому возможно получение неполной информации.

Лабораторное занятие № 14. Мониторинг сети с целью выявления типовых инцидентов и угроз безопасности

Цель занятия: Научиться использовать базовые методы мониторинга сети для выявления типовых инцидентов и угроз безопасности, таких как попытки взлома, DoS-атаки, аномальная активность.

Оборудование:

Компьютер с установленным программным обеспечением для мониторинга сети (например, Wireshark, tcpdump, или инструменты, предоставляемые операционной системой)

Доступ к тестовой сети (виртуальной или реальной)

(Опционально) инструменты для генерации сетевого трафика для симуляции атак

Ход работы:

Часть 1: Использование Wireshark (или аналога):

Запуск Wireshark: Запустите Wireshark и выберите интерфейс для захвата пакетов. Убедитесь, что вы имеете права на захват пакетов на выбранном интерфейсе.

Захват пакетов: Начните захват пакетов. В зависимости от размера сети и интенсивности трафика, захват может длиться от нескольких минут до часов.

Фильтрация пакетов: Используйте фильтры для отображения только интересующих вас типов пакетов. Примеры фильтров:

`ip.addr == 192.168.1.100`: показывает пакеты, связанные с IP-адресом 192.168.1.100.

`port 80`: показывает HTTP-трафик.

`tcp.flags.syn == 1`: показывает SYN-пакеты (часто используются для сканирования портов).

`icmp`: показывает ICMP-трафик (ping).

Анализ пакетов: Изучите захваченные пакеты. Обратите внимание на следующие признаки подозрительной активности:

Многочисленные попытки подключения к нестандартным портам: Может указывать на попытку сканирования портов.

Высокая интенсивность SYN-пакетов от одного IP-адреса: Возможность DoS-атаки.

Необычный объем трафика от неизвестного IP-адреса: Может указывать на вредоносное ПО.

Пакеты с флагом "RST" (Reset): Маршрутизатор сбрасывает соединение в случае проблем. Небольшое число RST пакетов – нормально, большое количество может быть подозрительно.

Часть 2: Использование системных утилит:

Мониторинг активности процессов: Используйте системные утилиты (например, `top` в Linux, `Task Manager` в Windows) для мониторинга активности процессов и выявления подозрительных процессов, потребляющих большое количество ресурсов.

Проверка журналов системы: Проверьте системные журналы (логи) на наличие сообщений об ошибках, предупреждениях и других событиях, которые могут указывать на инциденты безопасности.

Часть 3: Симуляция атак (опционально):

Использование инструментов для генерации трафика: Если доступны инструменты для генерации сетевого трафика, создайте несколько симулированных атак (например, DoS-атаки) и проанализируйте, как они выглядят в Wireshark. Это позволит лучше понять, как распознавать такие атаки в реальных условиях. Важно: Проводите симуляции атак только в контролируемой тестовой среде.

Часть 4: Документация и отчет:

Запись результатов: Задокументируйте все обнаруженные подозрительные события, включая временные метки, IP-адреса, типы пакетов и другие важные детали.

Отчет: Напишите отчет, в котором опишите методику работы, результаты мониторинга, выявленные угрозы и рекомендации по улучшению безопасности сети.

Типовые инциденты и угрозы безопасности:

DoS (Denial-of-Service) атаки: Попытки перегрузить сеть или сервер трафиком, делая его недоступным для легитимных пользователей.

Сканирование портов: Попытки найти уязвимые порты на серверах или других устройствах сети.

Вредоносное ПО: Заражение компьютеров вирусами, троянами и другими вредоносными программами.

Фишинг: Попытки получить конфиденциальную информацию (пароли, номера кредитных карт и т.д.) под видом легитимных организаций.

SQL-инъекции: Атаки на базы данных, используя уязвимости в коде веб-приложений.

Дополнительные задания (опционально):

Используйте расширенные функции Wireshark для анализа протоколов.

Настройте систему мониторинга сети на основе скриптов.

Изучите методы обнаружения и предотвращения более сложных атак.

Примечание: Для проведения данного лабораторного занятия необходимы базовые знания работы с сетевыми утилитами и понимание основных принципов работы сети. Все действия должны проводиться в контролируемой среде, чтобы избежать непредвиденных последствий. Использование инструментов для генерации сетевого трафика следует проводить только в тестовой среде и с разрешения администратора сети.

Лабораторное занятие № 15. Оценка степени критичности инцидентов при работе согласно инструкции

Цель занятия: Научиться оценивать степень критичности различных инцидентов информационной безопасности на основе установленной инструкции и классификатора угроз. Развить навыки анализа ситуаций и принятия взвешенных решений.

Оборудование:

Инструкция по обеспечению информационной безопасности (содержащая классификатор инцидентов и процедуру реагирования). Эта инструкция должна быть разработана заранее и предоставлена студентам. Она должна содержать описание различных типов инцидентов и шкалу их критичности (например, низкая, средняя, высокая, критическая).

Список типовых инцидентов (для оценки, см. ниже примеры).

Бланки для оценки (или электронная таблица).

Ход работы:

Часть 1: Изучение инструкции:

1. Внимательно изучите предоставленную инструкцию по обеспечению информационной безопасности. Обратите особое внимание на классификатор инцидентов и шкалу их критичности. Уясните критерии оценки для каждого уровня критичности.

2. Обратите внимание на процедуры реагирования, описанные в инструкции для каждого уровня критичности.

Часть 2: Оценка степени критичности инцидентов:

Студентам предоставляется список гипотетических инцидентов. Для каждого инцидента необходимо:

1. Квалификация инцидента: Определите тип инцидента (например, утечка данных, несанкционированный доступ, отказ в обслуживании, заражение вредоносным ПО, нарушение целостности данных и т.д.).

2. Оценка воздействия: Оцените потенциальное воздействие инцидента на организацию (финансовые потери, репутационный ущерб, нарушение нормальной деятельности, утечка конфиденциальных данных и т.д.).

3. Оценка вероятности: Оцените вероятность возникновения данного инцидента (низкая, средняя, высокая).

4. Определение уровня критичности: На основе инструкции и классификатора определите уровень критичности инцидента (низкая, средняя, высокая, критическая). Обоснуйте свой выбор, ссылаясь на соответствующие пункты инструкции.

5. Предложение мер реагирования: В соответствии с инструкцией, предложите необходимые меры реагирования на данный инцидент.

Примеры типовых инцидентов:

Несанкционированный доступ к учетной записи сотрудника.

Потеря USB-накопителя с конфиденциальными данными.

Заражение компьютера вирусом-шифровальщиком.

Отказ в обслуживании веб-сервера.

Фишинговая атака, направленная на сотрудников компании.

Выявление подозрительной активности в сети.

Утечка данных клиентов в результате взлома базы данных.

Неисправность сервера базы данных, приведшая к потере данных.

Несанкционированная модификация программного обеспечения.

Часть 3: Обсуждение и анализ:

После того, как студенты оценили все инциденты, проводится обсуждение результатов. Сравните оценки и обоснования разных студентов. Обсудите возможные разногласия и причины для различных интерпретаций.

Часть 4: Отчет:

В отчете необходимо:

Описать используемую инструкцию по информационной безопасности.

Предоставить список оцененных инцидентов и результаты оценки для каждого инцидента (тип инцидента, воздействие, вероятность, уровень критичности, обоснование, предлагаемые меры реагирования).

Сформулировать выводы о своих навыках оценки критичности инцидентов.

Дополнительные задания (опционально):

Разработать собственный классификатор инцидентов.

Разработать сценарий реагирования на наиболее критические инциденты.

Провести анализ эффективности существующей инструкции по информационной безопасности.

Примечание: Для проведения данного лабораторного занятия необходимо заранее подготовить инструкцию по обеспечению информационной безопасности с классификатором инцидентов и процедурами реагирования. Инструкция должна быть достаточно подробной, чтобы студенты могли использовать её для объективной оценки. Качество работы будет зависеть от полноты и ясности этой инструкции.

Лабораторное занятие № 16. Обнаружение и устранение возникающих типовых инцидентов

Цель занятия: Отработать практические навыки обнаружения и устранения типовых инцидентов информационной безопасности в контролируемой среде.

Оборудование и программное обеспечение:

Доступ к виртуальной или физической тестовой сети, включающей серверы, рабочие станции и сетевое оборудование (коммутаторы, маршрутизаторы). Важно: сеть должна быть изолирована от основной сети!

Системы мониторинга (например, Wireshark, системные логи).

Инструменты для симуляции атак (опционально, но желательно для более реалистичного сценария).

Антивирусное программное обеспечение.

Инструкция по реагированию на инциденты (разработанная заранее и предоставленная студентам). Эта инструкция должна содержать четкие инструкции по обнаружению и устранению различных типов инцидентов.

Ход работы:

Часть 1: Подготовка тестовой среды:

Настройка тестовой сети: Создайте тестовую сеть с несколькими виртуальными машинами (или физическими компьютерами). Настройте различные роли для этих машин (серверы баз данных, веб-серверы, рабочие станции и т.д.).

Установка уязвимостей (опционально): Для более реалистичного сценария можно установить уязвимости на некоторых машинах (только в тестовой, изолированной сети!). Это может быть достигнуто путем использования специально разработанных тестовых уязвимостей или путем имитации уже известных уязвимостей. Будьте осторожны и не устанавливайте реальные вредоносные программы!

Настройка мониторинга: Настройте системы мониторинга для наблюдения за сетевым трафиком и системными логами.

Часть 2: Симуляция и обнаружение инцидентов:

Инициирование инцидентов: Симулируйте различные инциденты безопасности, используя инструменты для симуляции атак или вручную, например:

DoS-атака: Используйте инструмент для отправки большого количества запросов на веб-сервер.

Сканирование портов: Используйте инструмент для сканирования портов на сервере.

Попытка несанкционированного доступа: Попытайтесь войти в систему с использованием неправильных учетных данных.

Заражение вредоносным ПО: (Только в контролируемой, виртуальной среде!) Запустите специально подготовленный, безопасный тестовый вирус или запустите процесс, имитирующий вредоносное ПО.

Утечка данных: Создайте сценарий имитирующий утечку данных.

Обнаружение инцидентов: Используя системы мониторинга, выявите симулированные инциденты. Зафиксируйте время обнаружения и признаки каждого инцидента.

Часть 3: Устранение инцидентов:

Анализ инцидентов: Проанализируйте обнаруженные инциденты. Определите их природу, масштаб и потенциальное воздействие.

Устранение инцидентов: Следуя инструкции по реагированию на инциденты, предпримите необходимые действия для устранения каждого инцидента. Это может включать:

Блокировку подозрительных IP-адресов.

Удаление вредоносного ПО.

Восстановление поврежденных данных.

Изменение паролей.

Усиление безопасности системы.

Документация: Задокументируйте все предпринятые действия, включая время, описание проблемы и принятые решения.

Часть 4: Отчет:

В отчете необходимо:

Описать конфигурацию тестовой сети.

Перечислить симулированные инциденты и время их обнаружения.

Описать признаки каждого инцидента и методы его обнаружения.

Подробно описать действия по устранению каждого инцидента, ссылаясь на используемые инструменты и инструкции.

Сделать выводы о результатах работы и эффективности используемых методов обнаружения и устранения инцидентов.

Оценить эффективность инструкции по реагированию на инциденты.

Дополнительные задания (опционально):

Симуляция более сложных, многоэтапных атак.

Разработка собственной инструкции по реагированию на инциденты.

Изучение и применение автоматизированных систем обнаружения и реагирования на инциденты.

Меры предосторожности:

Все действия должны проводиться в контролируемой тестовой среде, полностью изолированной от основной сети.

Не используйте реальные вредоносные программы, за исключением специально подготовленных безопасных тестовых образцов.

При возникновении трудностей обращайтесь за помощью к инструктору.

Эта лабораторная работа требует внимательности и точности. Хорошо подготовленная инструкция по реагированию на инциденты и использование инструментов симуляции сделают занятие более эффективным.

Лабораторное занятие № 17. Сбор информации о сетевом трафике

Цель занятия: Научиться собирать и анализировать информацию о сетевом трафике с использованием различных инструментов и методик. Цель – понять, как извлекать полезную информацию из сетевого трафика для диагностики, мониторинга безопасности и анализа производительности сети.

Оборудование и программное обеспечение:

Доступ к тестовой сети (виртуальная или физическая, изолированная от производственной сети).

Программное обеспечение для захвата и анализа пакетов (Wireshark, tcpdump, или аналогичные инструменты).

(Опционально) инструменты для генерации сетевого трафика (для создания тестовых сценариев).

Текстовый редактор для анализа полученных данных.

Ход работы:

Часть 1: Захват пакетов с помощью Wireshark:

Выбор интерфейса: Запустите Wireshark и выберите сетевой интерфейс для захвата пакетов. Убедитесь, что у вас есть необходимые права доступа. Важно выбрать правильный интерфейс, чтобы не захватывать весь трафик сети, если это не требуется.

Запуск захвата: Начните захват пакетов. Определите продолжительность захвата в зависимости от цели. Для анализа кратковременных событий достаточно нескольких минут, для анализа долговременных трендов – более длительный период.

Фильтрация пакетов: Во время или после захвата используйте фильтры для сужения области анализа. Примеры фильтров:

ip.addr == 192.168.1.100: отображает пакеты, связанные с IP-адресом 192.168.1.100.

port 80: отображает HTTP-трафик.

tcp.port == 443: отображает HTTPS-трафик.

http.request.method == GET: отображает HTTP GET запросы.

dns: отображает DNS запросы.

Анализ пакетов: Изучите захваченные пакеты. Обратите внимание на следующие параметры:

IP-адреса источника и назначения: Идентифицируйте участвующие в коммуникации устройства.

Порты источника и назначения: Определите используемые приложения и сервисы.

Протоколы: Определите используемые протоколы (TCP, UDP, ICMP и т.д.).

Размер пакетов: Проанализируйте размер пакетов и возможные отклонения от нормы.

Время: Определите временные характеристики трафика.

Часть 2: Захват пакетов с помощью tcpdump (или аналогичных утилит командной строки):

Запуск tcpdump: Используйте команду `tcpdump` (или аналогичную) для захвата пакетов. Например, `tcpdump -i eth0 -w capture.pcap` запишет трафик с интерфейса `eth0` в файл `capture.pcap`. Используйте опции `-i` для выбора интерфейса, `-w` для записи в файл.

Анализ файла: После захвата используйте Wireshark или другую утилиту для анализа записанного файла `.pcap`.

Часть 3: Анализ собранной информации:

Определение наиболее активных устройств: Определите устройства, генерирующие наибольший объем трафика.

Идентификация приложений: Определите, какие приложения генерируют трафик.

Поиск аномалий: Выявите любые аномалии в трафике, которые могут указывать на проблемы или угрозы безопасности.

Анализ производительности: Проанализируйте производительность сети на основе собранных данных.

Часть 4: Отчет:

В отчете необходимо:

Описать используемые инструменты и методики.

Предоставить примеры собранных данных (скриншоты, выдержки из логов).

Проанализировать полученную информацию, указав наиболее активные устройства, используемые приложения и обнаруженные аномалии.

Сделать выводы о состоянии сети на основе анализа трафика.

Дополнительные задания (опционально):

Изучение расширенных фильтров в Wireshark.

Использование скриптов для автоматизации анализа трафика.

Использование других инструментов для анализа сетевого трафика.

Моделирование различных сценариев сетевой активности (например, симуляция атаки) и анализ полученных данных.

Меры предосторожности:

Все действия должны проводиться в контролируемой тестовой среде.

При работе с реальными сетями необходимо получить разрешение администратора. Несанкционированный захват трафика может быть нарушением закона.

Данное лабораторное занятие требует базовых знаний о сетевых протоколах и работе с сетевыми утилитами. Умение использовать фильтры в Wireshark значительно ускорит анализ данных.

3. Промежуточная аттестация по учебные дисциплины МДК 02.01. Настройка и сопровождение аппаратно-программного обеспечения сетевых устройств инфокоммуникационных систем

1. Общие сведения о локальных компьютерных сетях, их назначении и области использования;
2. Топология локальных сетей, физическая структура, способы соединения компьютеров в сеть, виды интерфейсов, кабелей и коннекторов;
3. Типы инструментов, используемых для монтажа и диагностики кабельных систем компьютерных сетей;
4. Состав аппаратных ресурсов локальных сетей;
5. Виды активного и пассивного сетевого оборудования;
6. Логическая организация сети;
7. Определение конфигурация сервера;
8. Подключение к удаленному рабочему столу через консоль;
9. Управление компьютером;
10. Управление файлами на рабочих станциях и сервере;
11. Telnet – путь поиска файлов в сети;
12. Проверка наличия физической связи. Способы тестирования;
13. Тестирование сети с использованием тестеров. Варианты тестеров;
14. Проверка настройки протокола TCP/IP;
15. Тестирование сети с использованием программного способа;
16. Монтаж активного оборудования;
17. Проведение пуско-наладочных работ;
18. Тестирование компьютерной сети после монтажа, проверка ее работоспособности и соответствие стандартам;
19. Составление инструкции по эксплуатации;
20. Архитектура Клиент - сервер. Серверной ОС. Виды серверной ОС;
21. Microsoft Windows Server. Преимущества и недостатки;

22. Роли и компоненты MS Windows Server;

23. Установка и настройка роли контролер домена AD;

24. Установка и настройка роли Файловый сервер. Управление квотами и разрешениями;

25. Управление квотами и разрешениями. Создание общего сетевого ресурса;

26. Освоение методов установки первого контроллера в домене (лесе);

27. Установки второго контроллера домена с помощью репликации БД active directory с первого контроллера домена;

28. Установка второго контроллера домена из резервной копии БД ActiveDirectory первого контроллера домена;

29. Управление пользователями и группами;

30. Режимы функционирования домена;

31. Организационные подразделения (ОП);

32. Делегирование административных полномочий;

33. Управление приложениями с помощью групповых политик;

34. Организация работы с провайдерами;

35. Классификация провайдеров Интернета по видам оказываемых услуг;

36. Организация сети Интернет на физическом уровне;

37. Организация выхода в Интернет двух объединенных в сеть компьютеров;Изучение разных способов подключения;

38. Изучение варианта использования маршрутизатора;

39. Изучение варианта использования коммутатора. Изучение варианта построения сети с использованием сервера;

40. Изучение варианта построения сети с использованием сервера, но без маршрутизатора;

41. Протоколы почтовых соединений. Использование протоколов pop3, imap, smtp;

42. Использование почтовых программ для обработки почтовых сообщений;

43. Понятие глобальной компьютерной сети. Использование ключевых слов для поиска информации в Интернет. Язык поисковых запросов;

44. Коммуникационные средства интернета. Использование облачных сервисов;

45. Настройка FTP – сервиса. Права доступа к ресурсу, назначение, ограничении и фильтрация трафика;

46. Использование FTP-сервиса с помощью web-обозревателя. Настройка и использование программ FTP-клиента;

47. Информационная безопасность. Основные понятия ИБ;

48. Информационные угрозы. Цели и объекты защиты информации;

49. Юридические меры защиты информации;

50. Классификация помещений для составления карты информационной безопасности.

51. Способы защиты информации;

52. Средства безопасности операционных систем семейства;

53. Вредоносные программы. Классификация вредоносных программ;

54. Источники и основные признаки заражения. Способы защиты;

55. Средства защиты от вредоносных программ. Антивирусные и антиспамовые программы;

56. Защита от потерь информации;

57. Виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них;

58. Требования безопасности к локальным сетям;

59. Аппаратное обеспечение для безопасности ЛВС;

60. Методы обеспечения защиты компьютерных сетей от несанкционированного доступа;

61. Специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.