РОСЖЕЛДОР
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ростовский государственный университет путей сообщения»
(ФГБОУ ВО РГУПС)
Филиал РГУПС в г. Воронеж

Утверждаю:
Заместитель директора по УПР филиала
РГУПС в г. Воронеж
_____ Гуленко П.И
«01» сентября 2023 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 56e04e82f2d91c396292d43d4b4c48071
Владелец: Гуленко Петр Игоревич
Действителен: с 06.06.2023 по 29.08.2024

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по МДК 05.02 Беспроводная передача данных и IP-телефония

Специальность: 09.02.01. Компьютерные системы и комплексы

Профиль: технический

Квалификация выпускника: техник по компьютерным системам

Форма обучения: очная

Воронеж 2023 г.

Авторы-составители преподаватели высшей категории
Толубаева Л.А., Русинова Е.С.
предлагают методические указания по выполнению практических работ
по МДК 05.02 Беспроводная передача данных и IP-телефония
Протокол № 04 от 01.09.2023 г.
Председатель цикловой комиссии_____ Русинова Е.С.

(подпись) (Ф.И.О.)

СОДЕРЖАНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания для проведения практических занятий составлены в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, учебным планом и рабочей программой ПМ.05 Компьютерные и телекоммуникационные сети. Методические указания предназначены для студентов и преподавателей средних профессиональных учебных заведений, изучающих МДК 05.02 Беспроводная передача данных и IP-телефония.

Данные указания содержат необходимый теоретический материал, задания, необходимые для выполнения практических работ.

Целью изучения МДК 05.02 Беспроводная передача данных и IP-телефония является освоение следующих компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 5.1. Проектировать и администрировать локально-вычислительные сети.

ПК 5.2. Проводить контроль, диагностику и восстановление работоспособности компьютерных и вычислительных сетей.

ПК 5.3. Определять методы и основные принципы защиты информации от несанкционированного доступа.

ПК 5.4. Настраивать виды соединений в IP - телефонии и взаимодействие с компьютерной сетью.

В результате выполнения практических работ обучающийся должен

уметь:

– участвовать в проектировании, монтаже и эксплуатации и диагностике компьютерных сетей;

– правильно выявлять и оценивать угрозы безопасности информации;

– категорировать информацию в соответствии с действующим законодательством;

– определять сферу действия и использовать законодательство в области инфор-

мационной безопасности;

– реализовывать технологии VPN и VLAN;

– правильно выбирать программные и/или аппаратные средства защиты информации от всех видов угроз по различным критериям;

– использовать оснастки политик безопасности различных операционных систем;

знать:

– типы сетей, серверов, сетевую топологию;

– типы передачи данных, стандартные стеки коммуникационных протоколов;

– установку и конфигурирование сетевого оборудования;

– принципы построения телекоммуникационных вычислительных сетей (ТВС);

– принципы построения беспроводного соединения;

– основы технологии IP – телефонии;

– технологию виртуальных частных сетей VPN;

– технологию виртуальных сетей;

– методы и средства обеспечения информационной безопасности;

– защиту от несанкционированного доступа, основные принципы защиты информации;

– технические методы и средства защиты информации.

2 ТЕМАТИЧЕСКИЙ ПЛАН

№№ п/п	Наименование темы	Количество часов
1	2	**3**
1.	Настройка беспроводной сети с помощью Wi-Fi роутера	2
2.	Настройка SHDSL модема	2
3.	Исследование возможностей коммутаторов	2
4.	Построение сложной гибридной сети	2
5.	Построение сложной гибридной сети	2
6.	Организация беспроводной связи по стандарту Bluetooth	2
7.	Методы и средства обеспечения безопасности сети Wi-Fi	2
8.	Изучение характеристик системы GPS	2
9.	Изучение видов соединений в IP-телефонии	2
10.	Изучение видов соединений в IP-телефонии	2
11.	Изучение сигнализация на основе протокола SIP	2
12.	Изучение сигнализация на основе протокола SIP	2
13.	Изучение процедур обработки речи в IP-телефонии	2
14.	Изучение процедур обработки речи в IP-телефонии	2
15.	Беспроводные Ad-Hoc сети. Инфраструктура "точка доступа"	2
16.	Беспроводные Ad-Hoc сети. Инфраструктура "точка доступа"	2
17.	Основные инфраструктуры беспроводных сетей IEEE 802.11.	2
18.	Определение радиуса действия беспроводной сети и применение способов, увеличивающих данный показатель.	2
19.	Измерение скорости передачи данных сетей Wi-Fi.	2
20.	Использование беспроводных маршрутизаторов	2
21.	Использование беспроводных маршрутизаторов	2
22.	Изучение механизмов безопасности сетей Wi-Fi с использованием Windows XP.	2
23.	Изучение механизмов безопасности сетей Wi-Fi с использованием Windows XP.	2
24.	Аудит безопасности сетей, шифруемых с использованием WEP, с использованием ОС Linux.	2
25.	Аудит безопасности сетей, шифруемых с использованием WEP, с использованием ОС Linux.	2
26.	Обнаружение атак диссоциации с использованием ОС Linux.	2
27.	Обнаружение атак диссоциации с использованием ОС Linux.	2
	Итого:	**54**

Практическая работа № 1
Настройка беспроводной сети с помощью Wi-Fi роутера.
Цель работы:
Научиться настраивать Wi-Fi точку доступа через Web-интерфейс.
Необходимое оборудование:
-Wi-Fi точка доступа
-Компьютер
-Кабель Ethernet
Задание.
Подключить Wi-Fi роутер к одному из компьютеров сети.
Настроить протокол (TCP/IP) на компьютере
Настроить Wi-Fi роутер через WEB-интерфейс
Порядок выполнения работы:
1 Прочитайте приложение
2 Настройте протокол интернета (TCP/IP)
-Пуск → "Настройка" → "Панель управления" → "Сетевые подключения" → Подключение по локальной сети →"Свойства" →Протокол Интернета (TCP/IP) → Свойства.

-в свойствах подключения по локальной сети установите IP адрес 192.168.0.2 и маску подсети 255.255.255.0; основной шлюз 192.168.0.1; (смотри рис. 1)
Пуск → "Настройка" → "Панель управления" → "Сетевые подключения" → Подключение по локальной сети →"Свойства" →Протокол Интернета (TCP/IP) → Свойства. Нажмите «ОК».

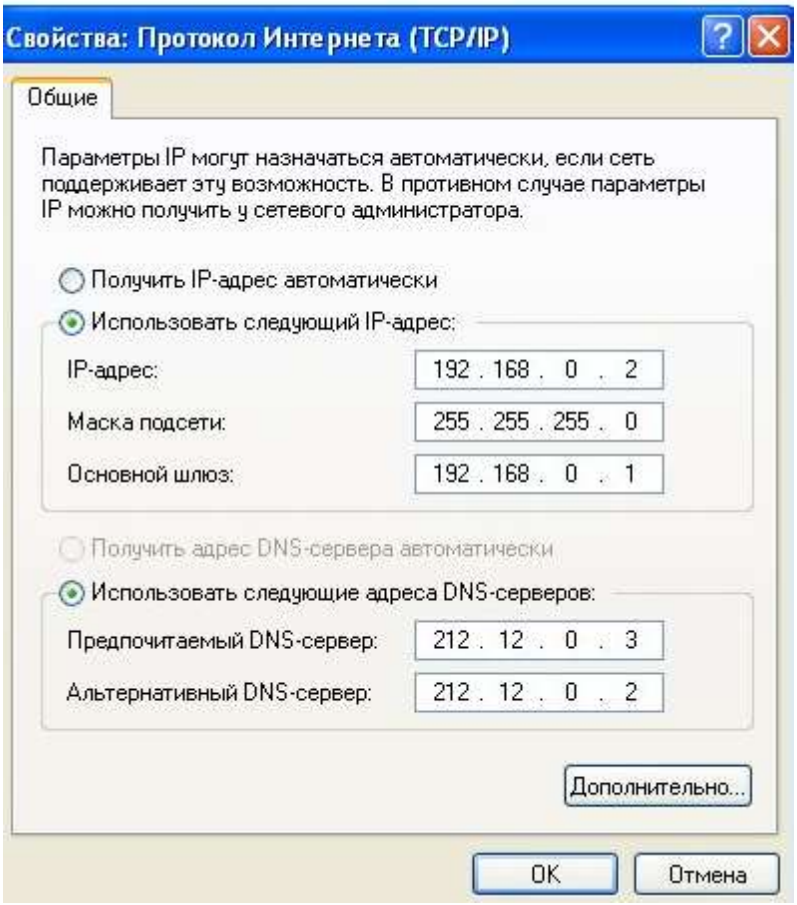


Рис.1 Протокол Интернета (TCP/IP)

3 Настройка Статического IP адреса на роутере

-Чтобы приступить к настройке нужно набрать в адресной строке вашего интернет браузера 192.168.0.1 и нажать клавишу "Enter".

В появившемся окне наберите имя пользователя admin и нажмите кнопку "Log In".

- Войдите в раздел «Manual Internet connection Setup» во вкладке «Internet setup». Для настройки интернета по статическому IP адресу необходимо в ниспадающем меню окна internet connection type выбрать пункт «Static IP»

В появившемся ниже окне в строке IP адрес, Subnet mask Gateway address введите данные 2222222 и нажмите «Save settings»

4 Настройка Wi-Fi сети в роутере

- Войдите в раздел «Manual Wireless connection Setup» во вкладке «Wireless setup»(рис.4) для установки названия и пароля wi fi соединения.

Оставьте галку Enable Wireless для включения радиотракта. В поле SSID введите название беспроводной сети. (Примечание: В дальнейшем сеть будет отображаться под этим именем. Необходимо использовать только латинские буквы и/или цифры. В данном примере имя сети: «Skyline»).

-выбрать страну, для России это RUSSIAN FEDERATION. После внесения всех изменений нажать кнопку Save/Apply для сохранения параметров.

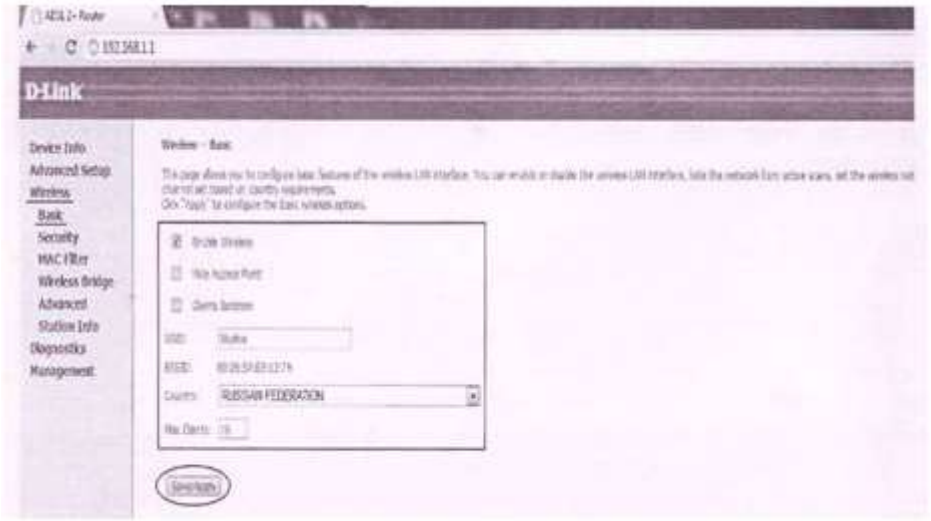


Рис. 3 Начало настройки сети

-Для настройки Шифрования данных необходимо зайти в раздел Wireless далее Security (рис. 4). В списке Select SSID выберите имя беспроводной сети «Skyline». Выберите тип сетевой аутентификации Network Authentication, например WPA2-PSK.

Наиболее стойкую защиту беспроводного канала даёт совместная работа точки доступа и RADIUS сервера (для аутентификации беспроводных клиентов). Это режимы «WPA-2 EAP» и «WPA EAP». При отсутствии возможности установки RADIUS сервера (домашние сети и сети малого офиса), используются режимы «WPA-2 PSK» и «WPA PSK». Менее всех защищен режим «WEP» («Shared Key»). При отсутствии необходимости защиты беспроводной сети (например, общедоступный Hot Spot), используется режим открытого доступа без шифрования «Open System»). В поле WPA Pre-Shared Key введите ключ сети.

(Примечание: Ключ должен быть не менее 8 символов в длину, необходимо использовать только латинские буквы и/или цифры без пробелов, регистр имеет значение).

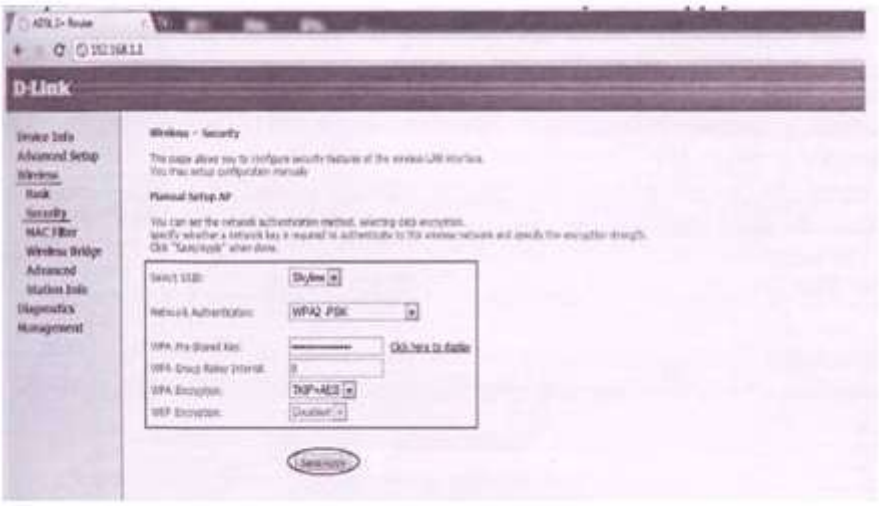


Рис.4 Настройки шифрования данных

-настроить частотный канал беспроводной сети и мощность передатчика. Для этого необходимо зайти в раздел Wireless далее Advanced (рис. 5). После задания настроек нажать кнопку Save/Annlv.

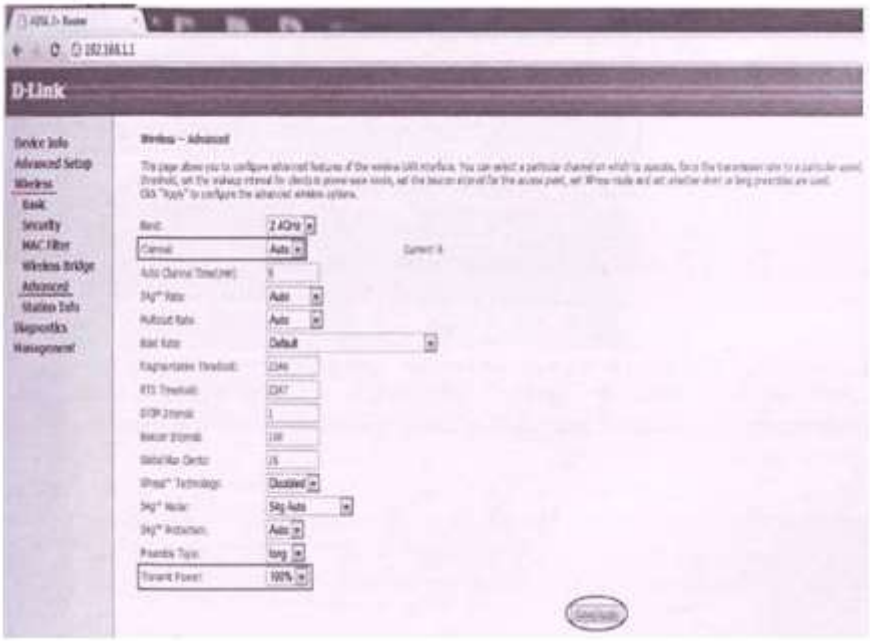


Рис.5 Настройка частотного канала

-сохранить настройки модема и перезагрузить модем (перезагрузка пройдет автоматически). Для этого необходимо зайти в раздел Management далее Save/Reboot и сверху по центру нажать на кнопку Save/Reboot (рис. 6). Модем сохранит настройки и сам перезагрузится.

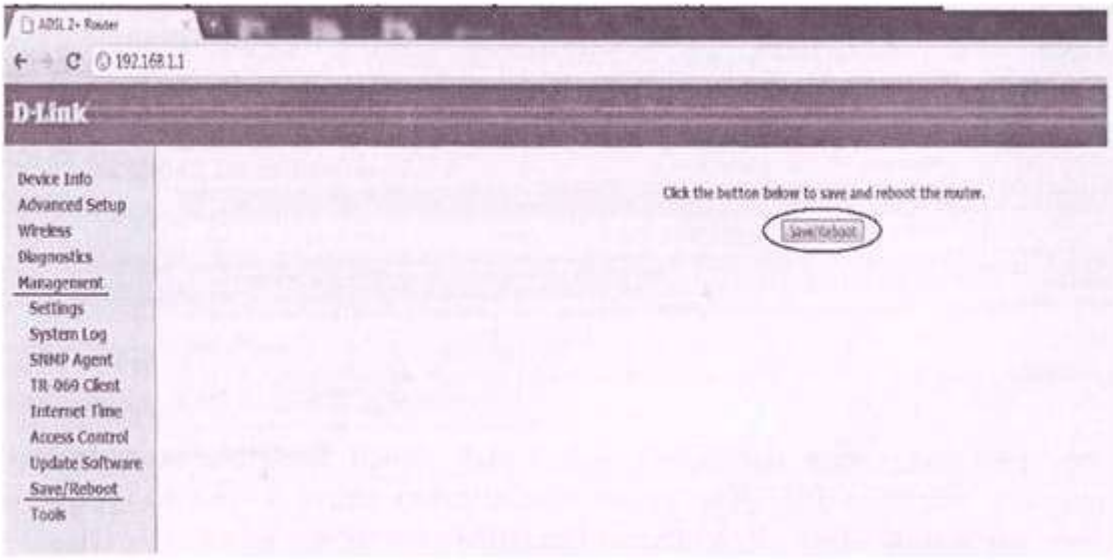


Рис.6 Сохранение и перезапуск WI-FI

Контрольные вопросы:

1. Какой IP адрес нужно прописать в адресной строке обозревателя, чтобы зайти в WEB интерфейс Wi-Fi роутера?
2. Какую маску подсети нужно вводить при настройке сетевого протокола TCP/IP?
3. В какой раздел нужно зайти при настройке беспроводной сети?
4. Что даёт стойкую защиту беспроводного канала?
5. Какой вид имеет предпочитаемый DNS-сервер?
6. Какой вид имеет альтернативный DNS-сервер?
7. Какие действия необходимо выполнить после того как ввели все настройки?
8. Как сбросить настройки Wi-Fi роутера?

Практическая работа №2
Настройка SHDSL модема
Цель работы:
1.Изучение способов подключения SHDSL модема к ПК.
2.Получить настроике пары модемов P-791R для объединения двух \
разных подсетей
Необходимое оборудование:
-SHDSL модем
-компьютер
-кабель Ethernet
-телефонный кабель
Задание:
1Выполнить настройку сетевой платы
2Подключить модем к одному из компьютеров сети
3Настройка SHDSL-модема через «Telnet»
Порядок выполнения работы:
1 Прочитайте приложение
2 Настройте сетевую плату
-Ввести следующие значения
подключения по локальной сети установите IP адрес 192.168.1.2 и
маску подсети 255.255.255.0; основной шлюз 192.168.1.1; Нажмите «ОК».

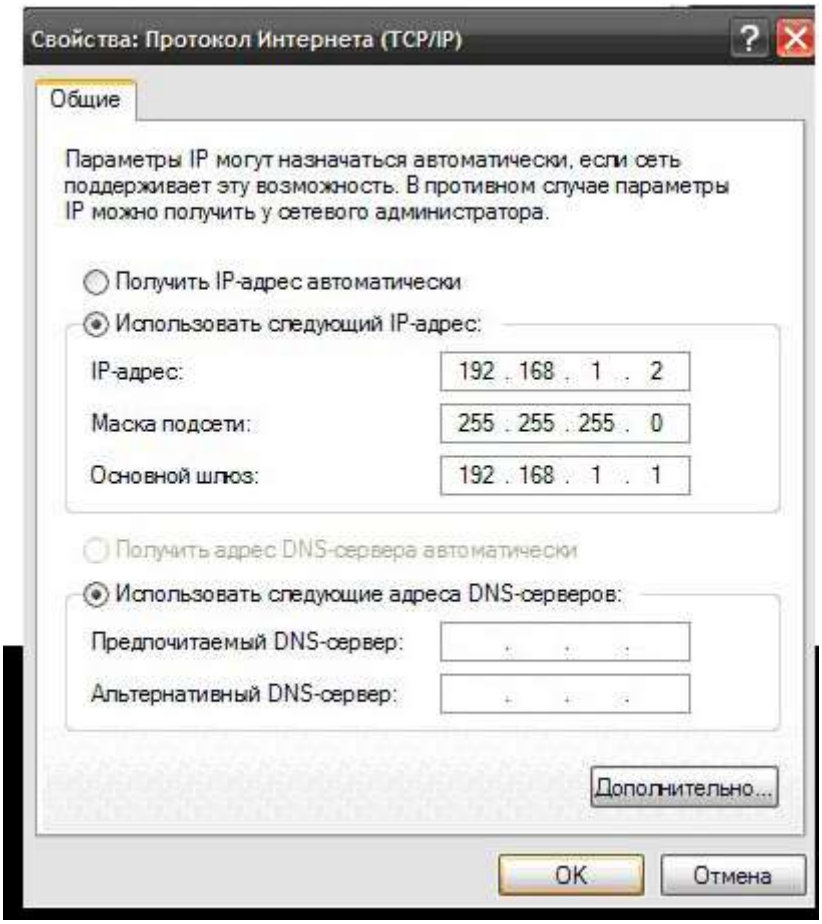


Рис.1 Протокол Интернета (TCP/IP)

7.3 Подключение модема к компьютеру

Включите модем в розетку 220В, подключите патч-корд Ethernet к разъему модема Zyxel P791 до разъема на ПК.
Через некоторое время должен заморгать и потом загореться ровным светом индикатор POWER.
Нажмите (например, стержнем от ручки) и удерживайте утопленную кнопку на задней стенке модема Zyxel P791. Дождитесь, пока на модеме изменится индикация, после этого отпустите кнопку. Это сбросит ДСЛ модем Zyxel P791 в заводские настройки по умолчанию.
7.4 Настройка SHDSL модема через «Telnet»
-Для начала настройки модема Zyxel P791 , выполните «Пуск»- «Выполнить» и наберите окне на латинице «cmd». После чего должно появиться следующее окно
- Наберите в открывшемся окне: «telnet 192.168.1.1» и нажмите ввод.
Появится окошко с запросом пароля. Введите пароль «1234»
Нажмите ввод.
Если все верно, то после ввода пароля вы увидите следующее окно:

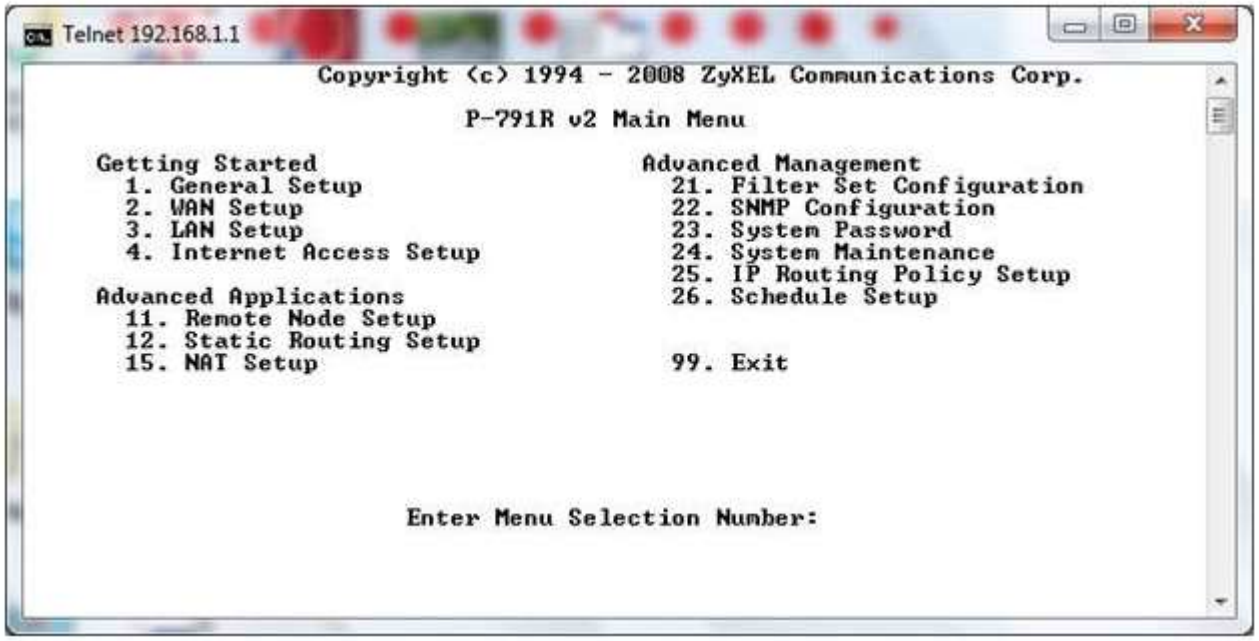


Рис.3 Главное меню

-Введите цифру «1» в строке приглашения и нажмите ввод для входа в пункт основных настроек модема.
В открывшемся окне нужно установить:
Route IP= No
Bridge= Yes
Для чего нажимая « Enter» или стрелками вверх вниз переместите курсор до необходимой строки затем, нажимая пробел, измените до указанных значении.
По окончанию изменении на строке сохранения или отмены изменении нажмите « Enter» для сохранения и выхода в главное меню.
- Введите цифру «2» в строке приглашения и нажмите ввод для входа в пункт WAN настроек. В открывшемся окне нужно установить тип модема. Если настраиваемый модем, будет станционной частью, то изменить значение

«Service Type» на «Server». В случае абонентской частью - «Client».
По завершению настроек на строке сохранения или отмены изменении нажмите « Enter» для сохранения и выхода в главное меню.
- Введите цифру «4» в строке приглашения и нажмите ввод для входа в пункт Internet access setup. В открывшемся окне нужно изменить параметр «Encapsulation» на «RFC 1483»
По завершению настроек на строке сохранения или отмены изменении нажмите « Enter» для сохранения и выхода в главное меню.

- Для настроики профиля удаленного узла Введите цифру «11» в строке приглашения и нажмите ввод для входа в
настройки удаленного доступа.
В 1 пунке нужно изменить с
Route= IP
Bridge= No
на
Route= None
Bridge= Yes.
Затем сохранить изменения.
Выити в главное меню нажатием «Esc»

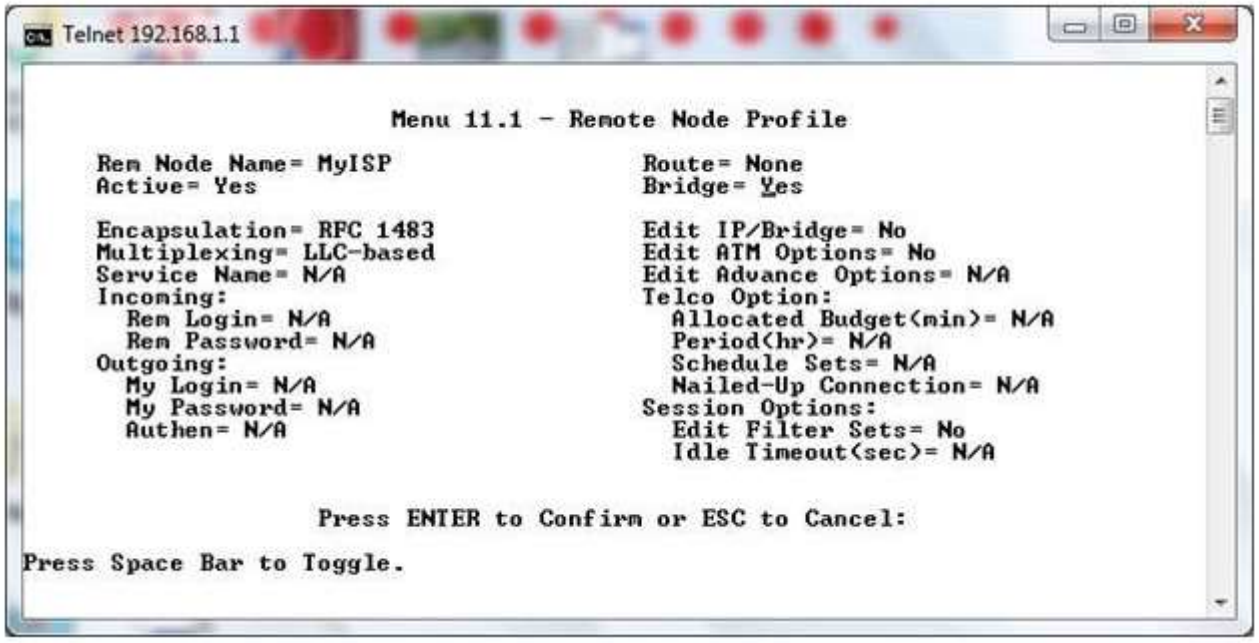


Рис.8 Окно профиля удаленного узла

- Введите цифру «21» в строке приглашения и нажмите ввод для входа в пункт фильтров. В открывшемся окне нужно поочередно удалить все имеющиеся фильтры

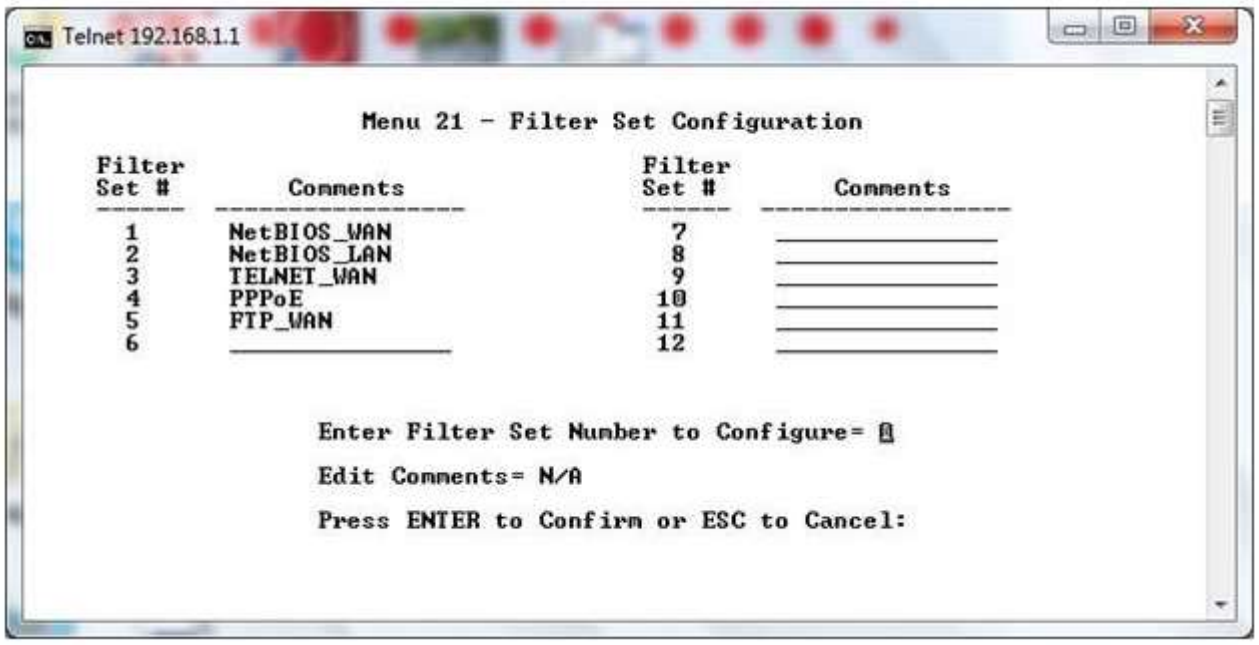


Рис.9 Окно установки фильтров

Для чего в строке приглашения войти в настройки фильтра, нажав ввод предварительно указав его номер по списку. После чего в строке «Edit Comments» высветится название фильтра.
Рис.10 Окно фильтра NetBIOS

Для удаления фильтра, нужно нажимая пробел удалить один два символа названия, после чего появится приглашения удаления пункта.
Затем нажать ввод для подтверждения. После повторения действии для всех 5 фильтров окно фильтров должно выглядеть следующим образом

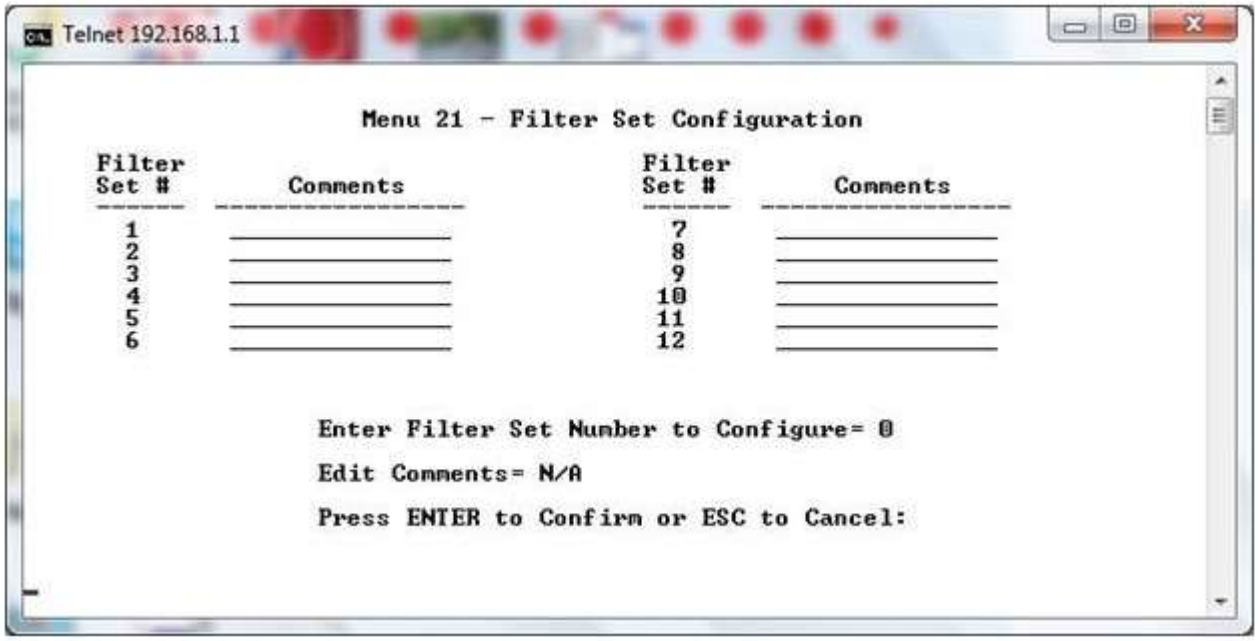
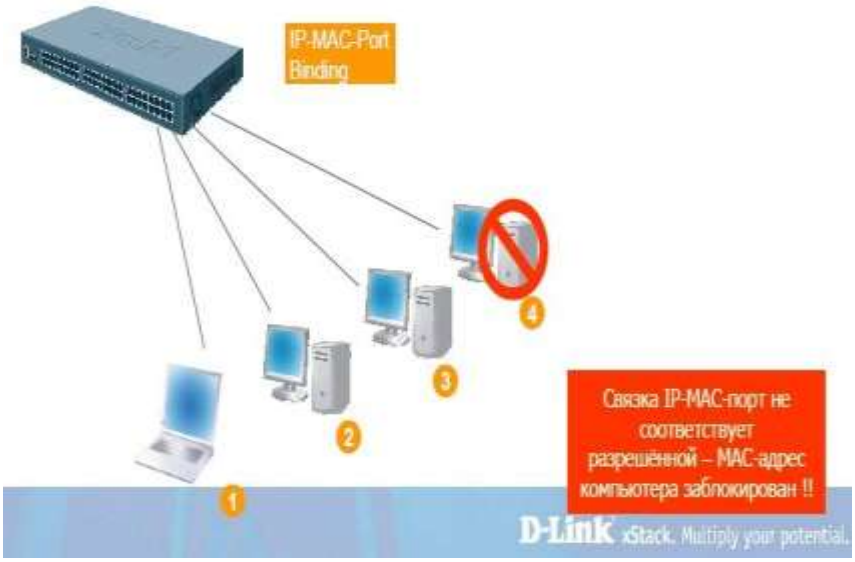


Рис.11 Окно фильтров

Выйти в главное меню нажатием «Esc»
Для завершения сеанса введите 99 и нажмтие «Enter»

Контрольные вопросы:
1. Как расшифровывается SHDSL?
2. В чём преимущества и недостатки этой технологии?
3. Можно ли соединить два SHDSL-модема между собой?
Если да то как их надо настроить?
4. Что является средой передачи данных для технологии SHDSL?
5. По скольким парам может работать SHDSL модем?
6. Какова максимальная скорость передачи данных SHDSL?
7. Может ли работать SHDSL модем с телефонным аппаратом вместе?

Практическая работа №3
Исследование возможностей коммутаторов
Базовые механизмы безопасности коммутаторов
Цель работы
Изучение технологии Trusted Hosts, IP-MAC Binding и Hjst security.
Теоретический материал
Настройка безопасности индивидуального порта
Данная функция позволяет
1. Заблокировать дальнейшее обновление таблицы коммутаторов. Если конфигурация вашей сети больше не изменится таблица коммутаторов блокируется и поступающие пакеты с неизвестных адресов будут отбрасываться.
2. Задать максимальное количество MAC-адресовдля привязки к конкретному порту.
Технология фильтрации IP-MAC Binding
Проверка подлинности компьютеров в сети
Функция IP-MAC-Port Binding в коммутаторах D-Link позволяет контролировать доступ компьютеров в сеть на основе их IP и MAC-адресов, а также порта подключения. Если какая-нибудь составляющая в этой записи меняется, то коммутатор блокирует данный MAC-адрес с занесением его в блок-лист.
Привязка IP-MAC-порт (IP-MAC-Port Binding)
Эта функция специально разработана для управления сетями ETTH/ ETTB и офисными сетями



Для чего нужна функция IP-MAC-Port binding?
D-Link расширил популярную функцию IP-MAC binding до более удобной в использовании IP-MAC-Port binding с целью повышения гибкости аутентификации пользователей в сети.
IP-MAC-Port binding включает два режима работы: ARP (по умолчанию) и ACL.
Сравнение этих двух режимов показано в таблице ниже:

	ARP режим	ACL режим
Плюсы	Простота в использовании и независимость от ACL	Позволяет предотвратить несанкционированное подключение даже если нарушитель использует статический MAC-адрес

Минусы	Невозможность фильтрации в случае если hacker/sniffer присвоит себе статический MAC-адрес для спуфинга коммутатора	Тратится профиль ACL, а также необходимо продумывать целиком всю стратегию ACL

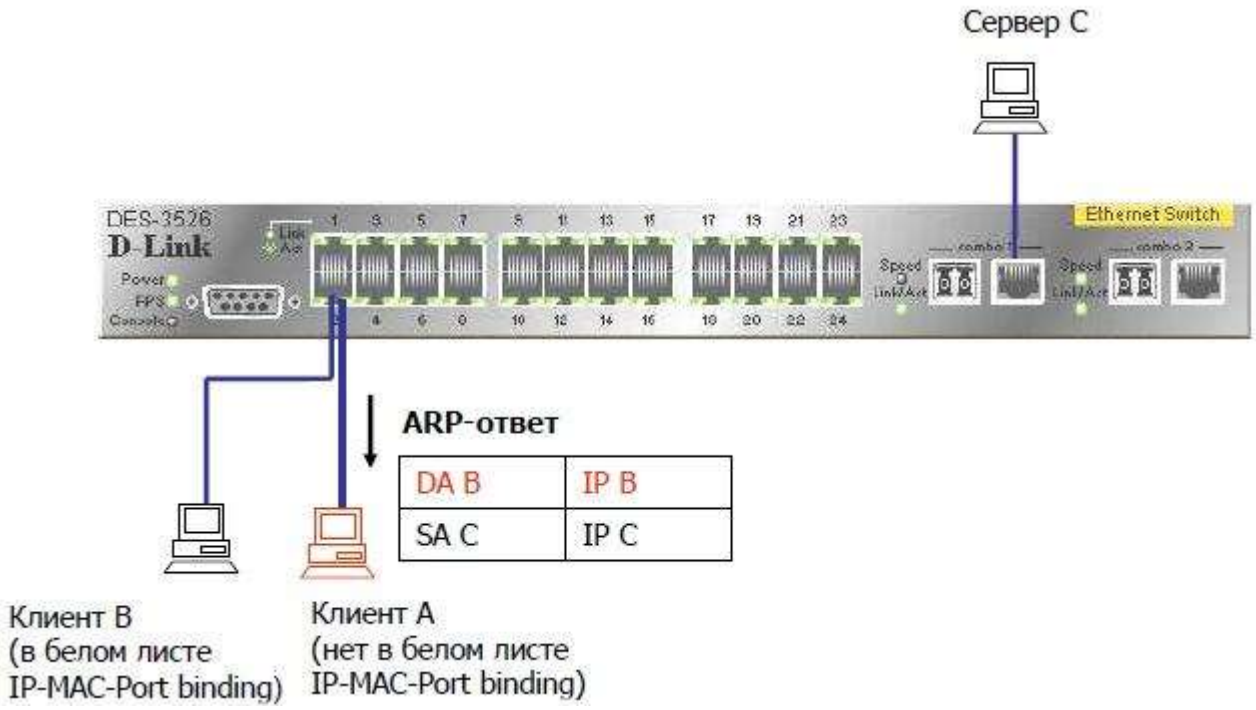
IP-MAC-Port будет поддерживаться коммутаторами L2 серии xStack - DES-3500 (R4 – ACL Mode), DES-3800 (R3), and DGS-3400 (R2). На данный момент IP-MAC-Port Binding поддерживается коммутатором DES-3526.

Данный документ описывает примеры настройки IP-MAC-Port binding, например, против атак ARP Poison Routing.

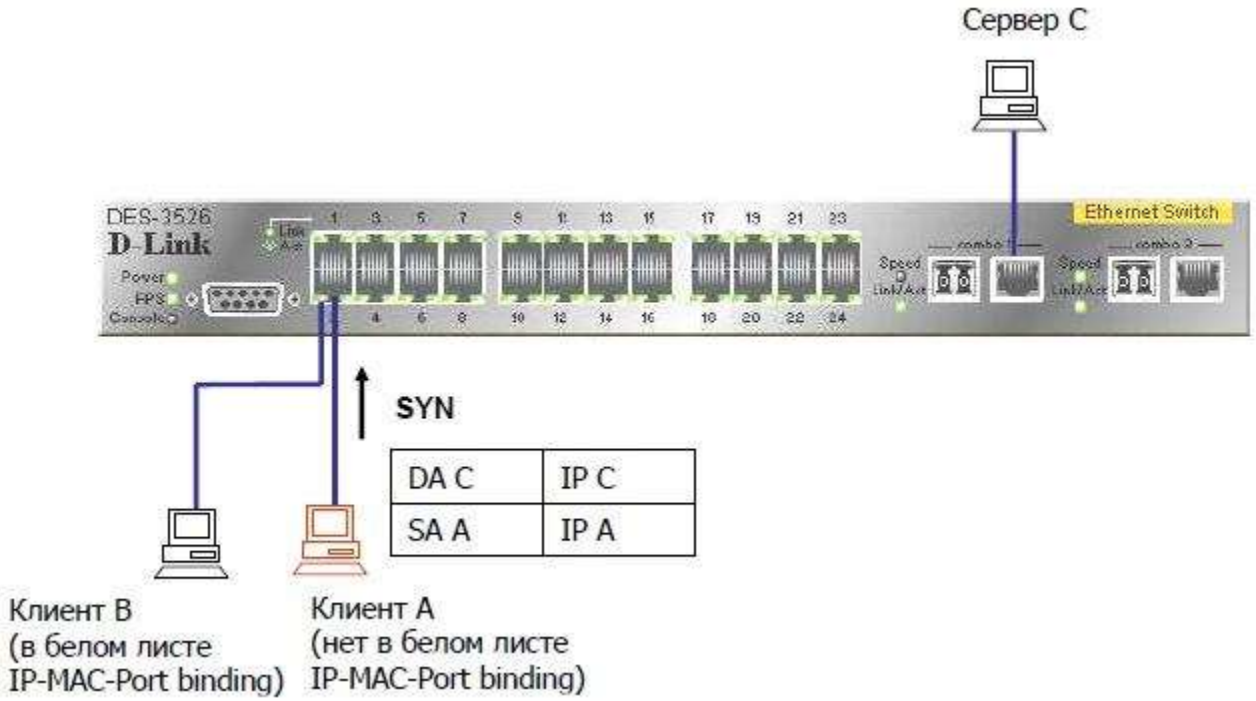
Пример 1. Использование режима ARP или ACL для блокирования снифера

Шаг 1: Клиенты A и B подключены к одному порту коммутатора, клиент A (sniffer) шлет поддельные ARP

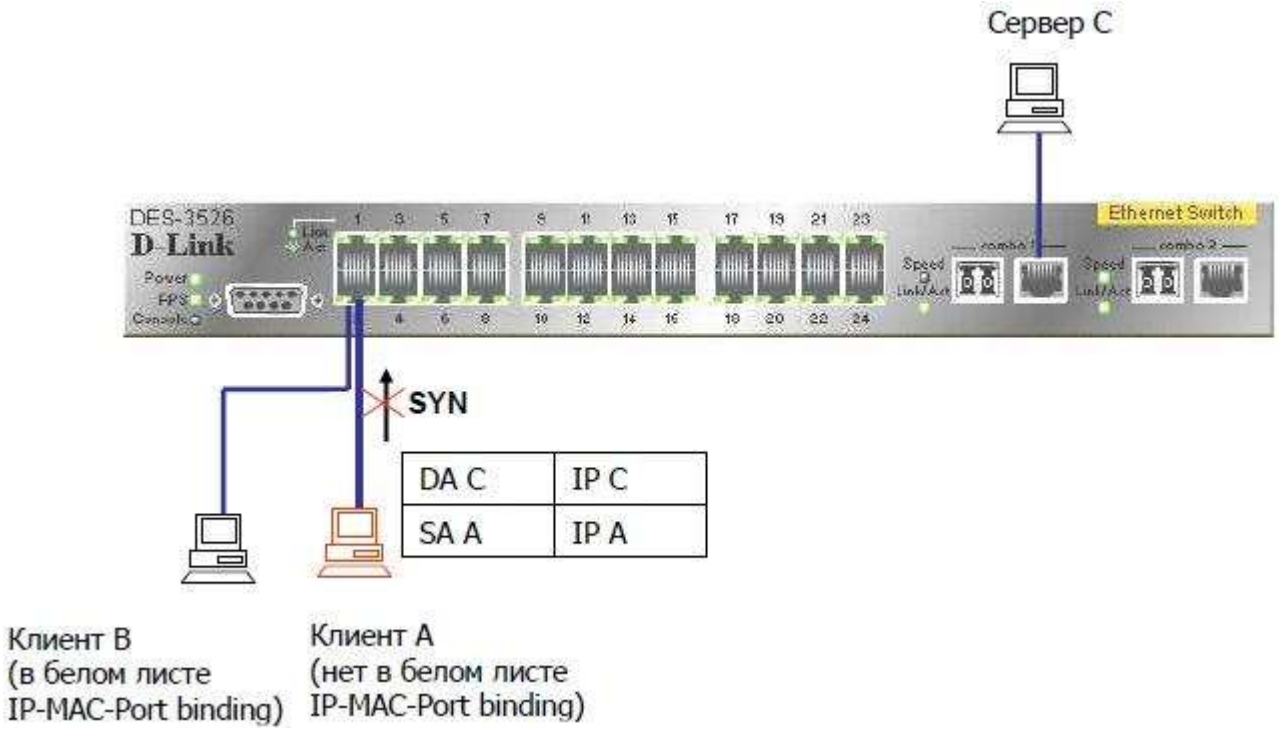
Шаг 2: Сервер C отвечает на запрос и изучает поддельную связку IP/MAC.



Шаг 3:Клиент A хочет установить TCP соединение с сервером C

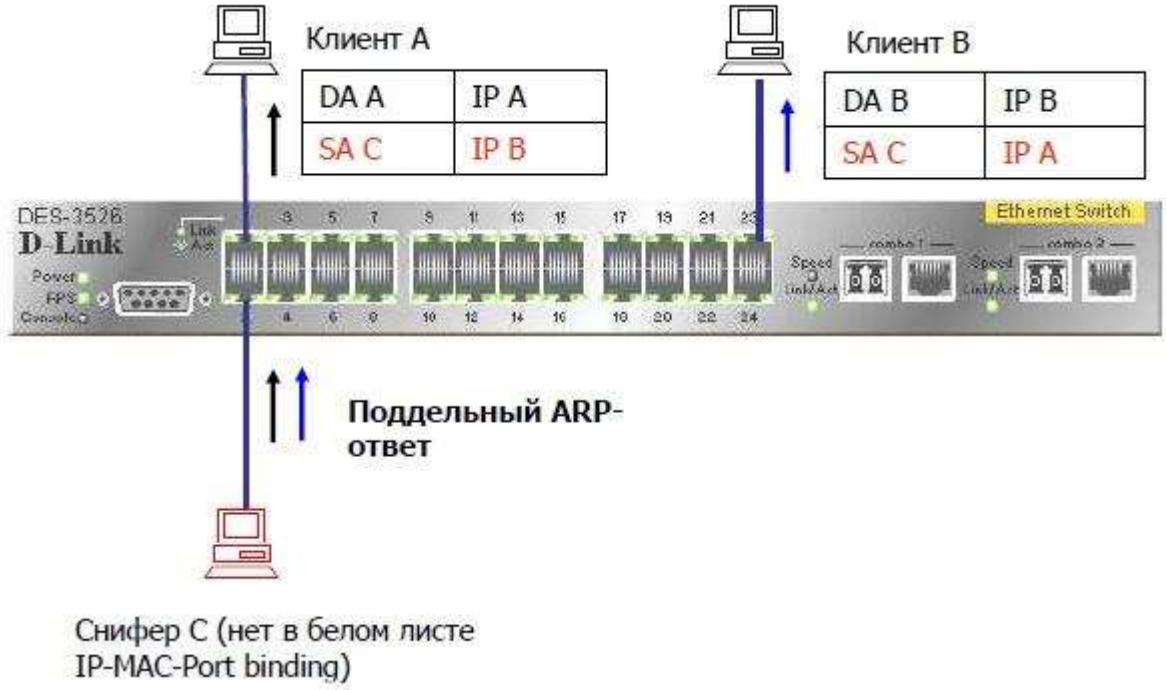


Шаг 4: Т.к. клиент A не в белом листе, DES-3526 блокирует пакет, поэтому, соединение не сможет быть установлено



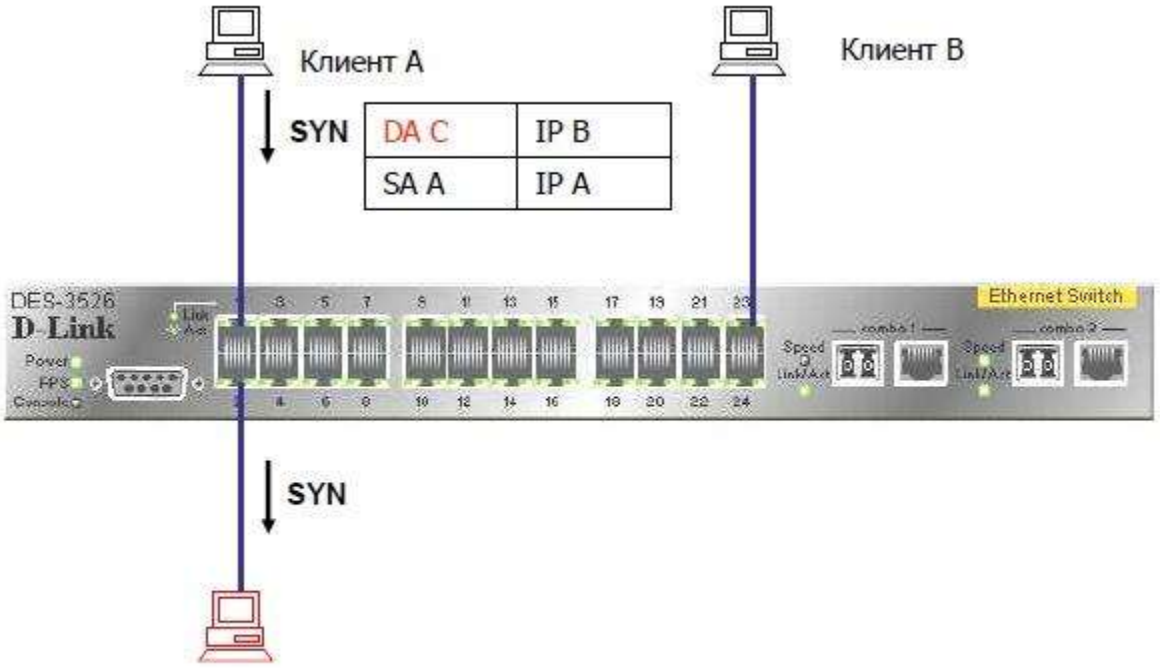
Пример 2. Использование режима ACL для предотвращения ARP атаки Man-in-the-Middle

Шаг 1: Sniffer C (Man in the middle) отсылает поддельный пакет ARP-Reply клиентам A и

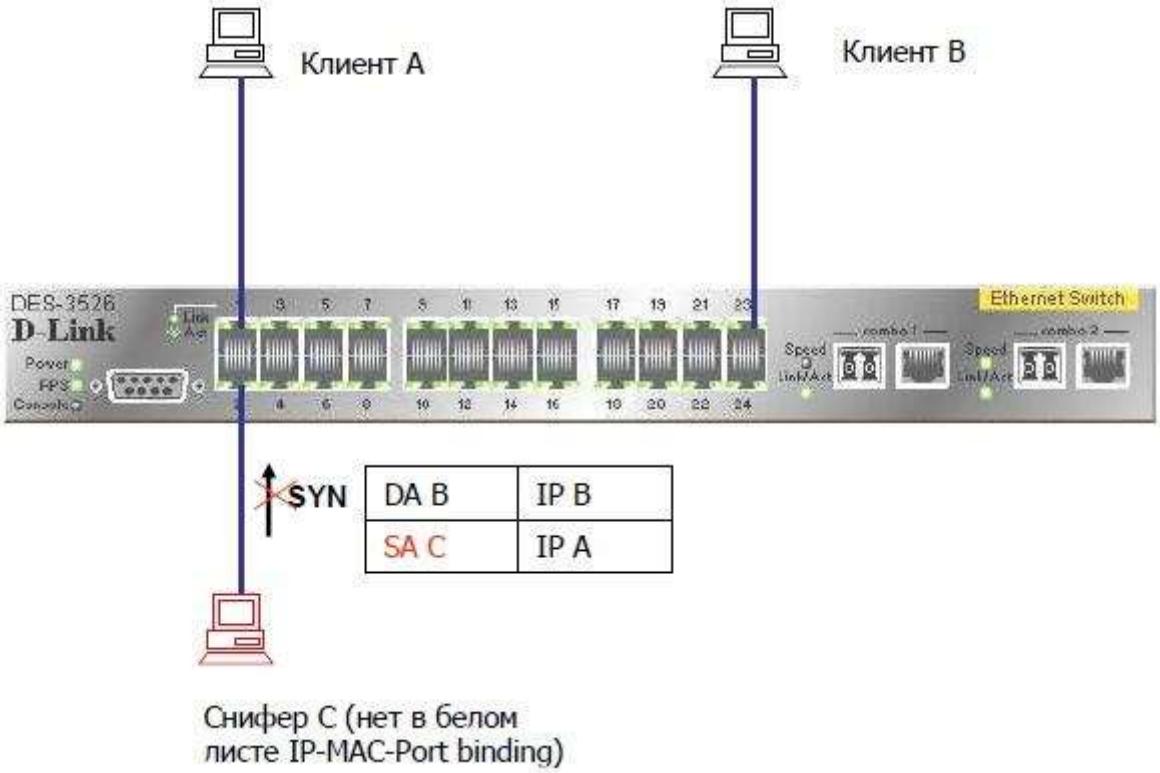


В

Шаг 2: Клиент А хочет установить TCP соединение с клиентом



В Шаг 3: Т.к. C не в белом листе, DES-3526 блокирует пакет, поэтому, соединение не сможет быть установлено



Советы по настройке IP-MAC-Port binding ACL Mode

ACL обрабатываются в порядке сверху вниз (см. рисунок 1). Когда пакет «соответствует» правилу ACL, он сразу же отбрасывается (если это запрещающее, правило, deny) либо обрабатывается (если это разрешающее правило, permit)

При использовании IP-MAC-Port binding в режиме ACL автоматически создаются 2 профиля (и правила для них) в первых двух доступных номерах профилей.

- Любое запрещающее правило после IP-MAC-Port binding становится ненужным, поэтому рекомендуется располагать все остальные ACL в более приоритетном порядке. - Нельзя включать одновременно функции IP-MAC-Port ACL mode и ZoneDefense. Т.к. правила привязки IP-MAC-Port создаются первыми, и правила, создаваемые ZoneDefense автоматически после этого, могут быть неправильными.

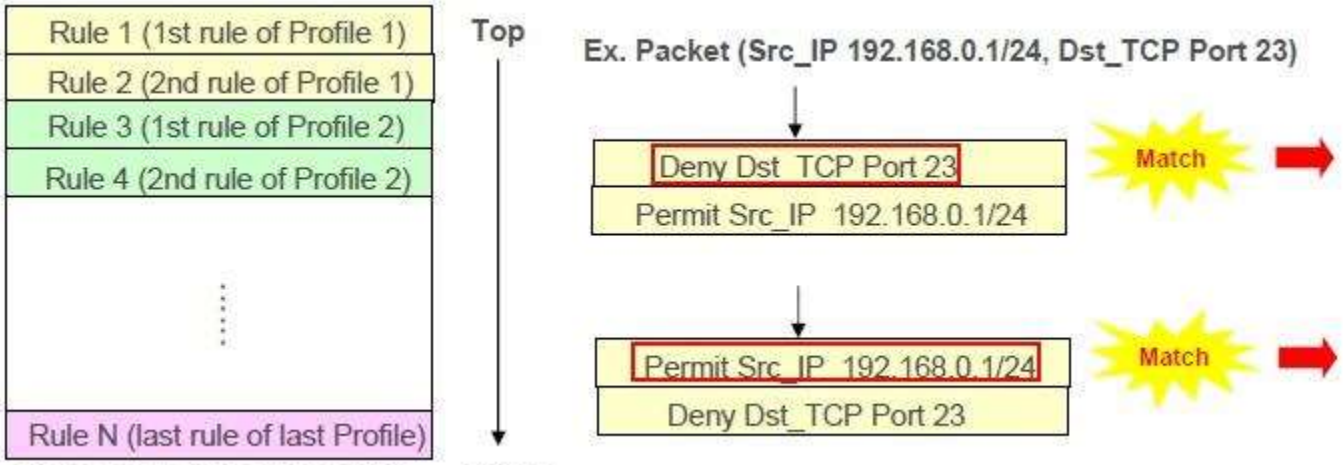


Рисунок 1. Обработка ACL

Вопрос: Что делать, если необходимо создать еще один профиль, когда режим ACL уже включен (рисунок 2)?

– Нужно использовать команды "disable address_binding acl_mode” (Рисунок 3) и затем "enable address_binding acl_mode” (Рисунок 4)

Рисунок 2 Рисунок 3 Рисунок 4

IP-MAC-Port Binding (пример)

Раздел «Security». Меню «Port Security»

См. Руководство пользователя. Управляемые коммутаторы 10/100Мбит/с Fast Ethernet СЕРИЯ I. D-Link ™ DES-3028/DES-3028P/DES-3052/DES-3052P

Данное меню предназначено для настройки безопасности на уровне индивидуального порта. Внешний вид меню представлен на рисунке 61.

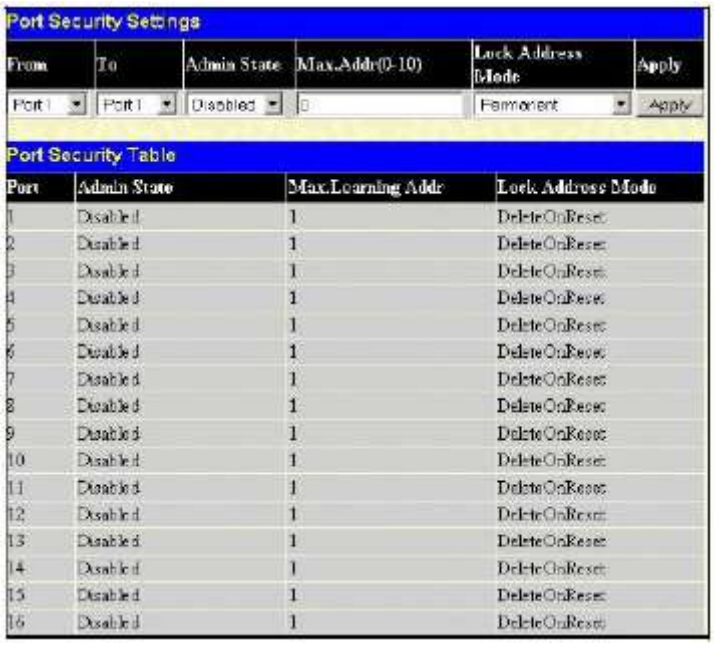


Рисунок 61. Окно раздела «Security» меню «Port Security»

Могут быть выставлены следующие параметры:

- From/To – задаѐт диапазон портов, для которых выполняются настройки;
- Admin State – активирует (Enabled) или деактивирует (Disabled) функцию безопасности, то есть блокирует таблицу коммутации для выбранных портов;
- Max. Addr (0-10) – задаѐт максимальное количество аппаратных адресов, которые будут занесены в таблицу коммутации для выбранной группы портов;
- Lock Address Mode – режим блокировки – позволяет выбрать, каким образом будет реализовано блокирование таблицы коммутации:

-- Permanent – заблокированные адреса НЕ будут устаревать (удаляться) по прошествии таймаута (времени их жизни);

-- DeleteOnTimeout – заблокированные адреса будут устаревать (удаляться) по прошествии таймаута, то есть как и обычно;

-- DeleteOnReset – заблокированные адреса будут удаляться только после перезагрузки коммутатора.

Задание

1. Соберите топологию сети, представленную на рисунке 1.

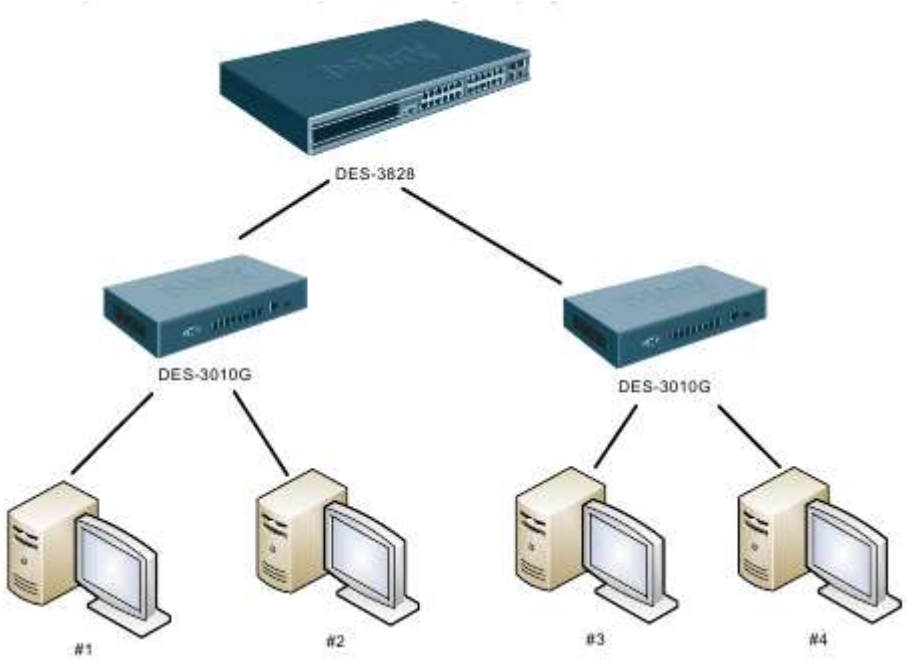


Рисунок 1. Топология коммутируемой сети.

Вопросы для самоконтроля.

1. Какие настройки можно организовать с помощью меню «Port Security»?
2. Чем отличаются возможности настройки коммутаторов 1 и 2 уровня?
3. Как определите MAC-адрес коммутатора?
4. Какие настройки можно организовать с помощью меню «IP-MAC Binding»?
5. Какие настройки можно организовать с помощью меню «Trusted Hosts»?
6. Перечислите достоинства используемого метода?

Практическая работа №4-5

Построение сложной гибридной сети

Цели:

-объединять сегменты сети, использующие стандарты Ethernet 10Base-2 и 10Base-T, как друг с другом, так и с сегментами, построенными на базе Fast-или Gigabit Ethernet;

-настраивать и подключать к сети Ethernet сегменты, в которых используются беспроводные точки доступа и беспроводные устройства.

Оборудование

Для проведения лабораторной работы понадобятся:

– компьютеры с комбинированным сетевым адаптером Ethernet стандартов 10Base-2/10Base-T и с установленной ОС Windows 2000 Professional или Windows XP Professional;

– компьютеры с беспроводными сетевыми адаптерами стандарта 802.11b или 802.11g и с установленной ОС Windows 2000 Professional или Windows XP Professional;

– один или несколько отрезков коаксиального кабеля RG-58 с заделанными обычными BNC-коннекторами;

– Т-коннекторы (по одному на каждое сетевое устройство стандарта 10Base-2) и два терминатора;

– гибридный концентратор 10Base-2/10Base-T с портами BNC и RJ-45;

– один концентратор или коммутатор Ethernet;

– набор кабелей «витая пара» с коннекторами RJ-45 (по одному кабелю на каждый компьютер и сетевое устройство);

– подключаемая к сети Ethernet беспроводная точка доступа, работающая по стандарту 802.11b или 802.11g.

Результаты

После выполнения работы учащиеся должны уметь:

– строить отдельные участки сети, в которых будут использоваться различные стандарты Ethernet (10Base-2, 10Base-T, Fast- или Gigabit Ethernet), а затем соединять эти участки в единую сеть;

– подключать к сети Ethernet беспроводную точку доступа, работающую по одному из стандартов Wi-Fi, и проверять работоспособность объединенной сети.

В итоге учащиеся должны убедиться в высокой совместимости разных стандартов Ethernet и увидеть, как с помощью шлюзов обеспечивается подключение к сети Ethernet устройств, использующих другие сетевые архитектуры.

Задание 1.

Построение сложной сети Ethernet

Цель работы

В этом задании вы должны познакомиться с принципами объединения в единую сеть сегментов, использующих оборудование различных стандартов Ethernet.

Предварительные условия

Для успешного выполнения этого задания необходимо, чтобы вы настроили компьютеры для работы в сети, как описано в задании 1 лабораторной работы 1, и установили на один из компьютеров сетевой адаптер стандарта 10Base-2, как описано в задании 2 лабораторной работы 3.

Создание сегмента сети, использующего стандарты 10Base-2 и 10Base-T

Подключите к BNC-разъему вашего сетевого адаптера Т-коннектор, терминатор и коаксиальный кабель.

Примечание. Пункты 1 и 2 этого задания выполняются на компьютерах с сетевыми адаптерами 10Base-2/10Base-T.

Другой конец коаксиального кабеля с Т-коннектором и терминатором соедините с BNC-разъемом гибридного концентратора, имеющего порты BNC и RJ-45.

Примечание. Если у вас есть несколько компьютеров, объединенных коаксиальным кабелем, то подключение к гибридному концентратору можно осуществить в любом месте сегмента, а не обязательно в его конце. Один из терминаторов желательно заземлить, а затем проверить возможности взаимодействия и убедиться, что сеть работает.

Используя прямой кабель на основе «витой пары», подключите компьютер вашего партнера к порту RJ-45 гибридного концентратора. Получившаяся сеть должна выглядеть, как показано на рис. 5.1.

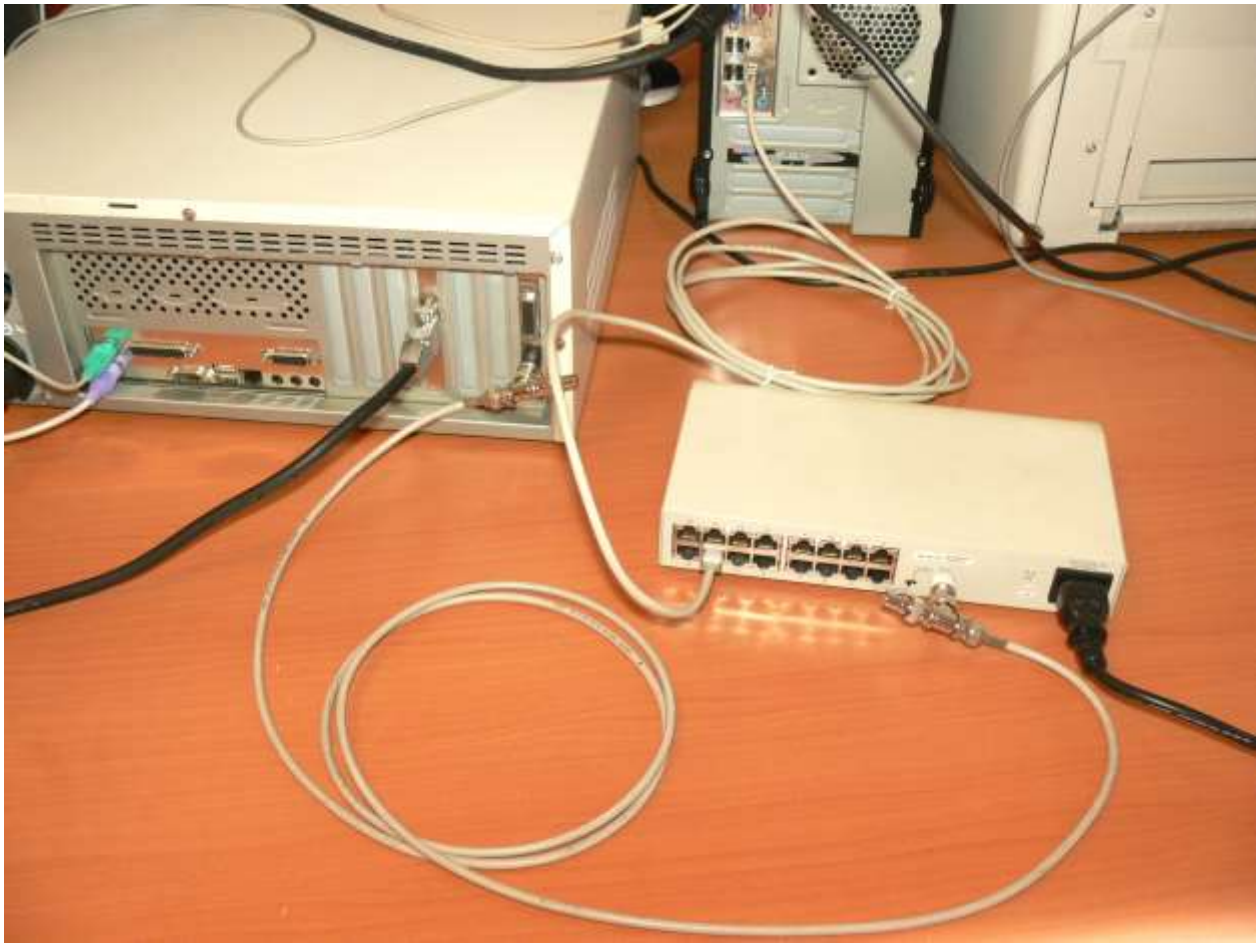


Рис. 1. Сеть, объединяющая сегменты 10Base-2 и 10Base-T

Примечание. Пункт 3 этого задания выполняется на компьютерах, оборудованных сетевыми адаптерами 10Base-T или Fast Ethernet. Если есть возможность, то подключите к концентратору несколько компьютеров, чтобы проверить взаимодействие в объединенной сети.

Включите компьютеры, подключенные к коаксиальному кабелю и гибридному концентратору, и войдите в систему.

Попытайтесь обратиться к общим ресурсам на компьютере вашего партнера и на других компьютерах в сети.

Удалось ли вам обратиться к ресурсам какого-либо из компьютеров сети?

Успешное обращение к общим ресурсам означает, что взаимодействие между сегментами 10Base-2 и 10Base-T установлено.

Закройте все окна.

Подключение сегмента сети, использующего стандарты 10Base-2 и 10Base-T, к коммутатору Fast Ethernet

Возьмите *прямой* кабель на основе «витой пары». Помня о правилах каскадирования концентраторов (коммутаторов), подключите один из его концов к перекрестному порту (Uplink) гибридного концентратора.

Если используется прямой кабель, то в какой порт другого концентратора (коммутатора) — обычный или перекрестный — следует вставить второй коннектор RJ-45?

Возьмите коммутатор Fast- или Gigabit Ethernet и подключите второй конец кабеля к одному из его портов. Получившаяся сеть должна выглядеть, как показано на рис. 5.2.

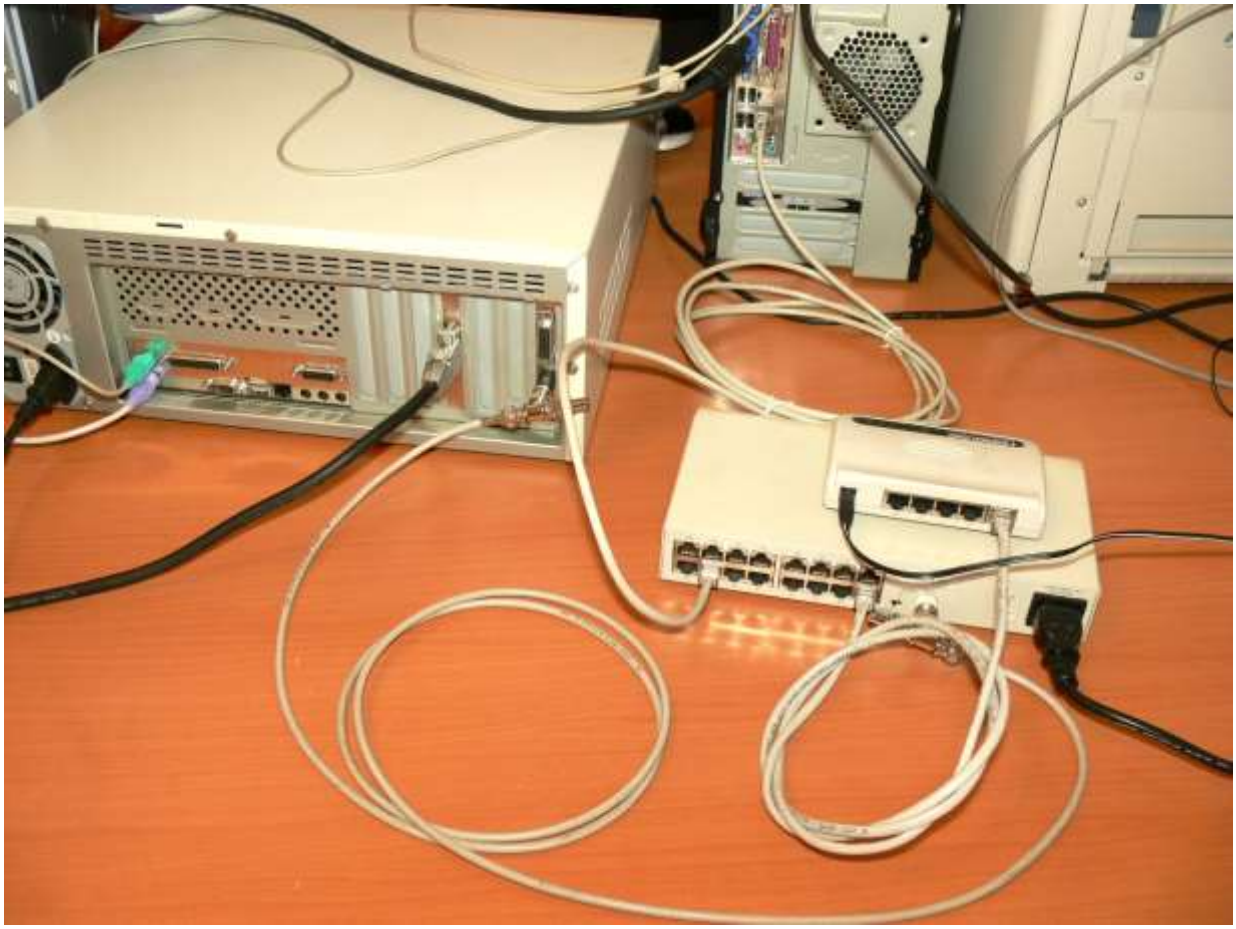


Рис. 2. Сеть, объединяющая сегменты 10Base-2, 10Base-T и Fast Ethernet

Включите компьютеры, подключенные к коммутатору Fast Ethernet.

Примечание. Эта часть задания выполняется на компьютерах, оборудованных сетевыми адаптерами 10Base-T или Fast Ethernet. Если есть возможность, то подключите к коммутатору несколько компьютеров, чтобы проверить взаимодействие в объединенной сети.

Попытайтесь обратиться к общим ресурсам компьютеров, подключенных к концентратору 10Base-T, и компьютеров, подключенных с помощью коаксиального кабеля.

Удалось ли вам обратиться к ресурсам компьютеров, подключенных к концентратору и коаксиальному кабелю?

Успешное обращение к общим ресурсам означает, что взаимодействие между сегментами 10Base-2, 10Base-T и Fast Ethernet установлено.

Закройте все окна.

Задание 2.

Построение беспроводного участка сети и его подключение к сети Ethernet

Цель работы

В этом задании вы должны познакомиться с принципами подключения к сети Ethernet беспроводной точки доступа, работающей по одному из стандартов Wi-Fi, и настроить сетевое взаимодействие между проводными и беспроводными клиентами.

Настройка беспроводной точки доступа

Примечание. Эта часть задания выполняется на одном из компьютеров, с помощью которого будет настроена точка доступа. Поскольку настройка беспроводной точки доступа обычно осуществляется через веб-интерфейс с использованием стандартного сетевого Ethernet-соединения, выбранный компьютер нужно подключить к точке доступа, а затем правильно сконфигурировать параметры протокола IP на этом компьютере.

Возьмите беспроводную точку доступа и, используя разъем для коннектора RJ-45, соедините с помощью кабеля «витая пара» точку доступа с одним из компьютеров класса.

Примечание. Как правило, точки доступа имеют порты с автоопределением MDI/MDI-X, поэтому тип кабеля (прямой или перекрестный) обычно не имеет значения. Однако желательно проверить, поддерживает ли ваша точка доступа эту функцию, в ее руководстве пользователя.

Включите компьютер и войдите в систему с учетной записью, входящей в локальную группу «Администраторы».

В меню Пуск щелкните правой кнопкой мыши на пункте Сетевое окружение и в появившемся контекстном меню выберите пункт Свойства.

В открывшемся окне Сетевые подключения щелкните правой кнопкой мыши на значке Подключение по локальной сети и в появившемся контекстном меню выберите пункт Свойства.

В окне свойств сетевого подключения щелкните мышью на строке Протокол Интернета (TCP/IP) в списке Компоненты, используемые этим подключением, а затем щелкните мышью на кнопке Свойства.

В окне настройки параметров протокола IP выберите радиокнопку Использовать следующий IP-адрес и введите следующие параметры:

IP-адрес — 192.168.1.200;

маска подсети — 255.255.255.0.

Примечание. Как правило, точка доступа имеет предварительно установленный IP-адрес в сети 192.168.1.0 (обычно 192.168.1.1 или 192.168.1.254). Желательно проверить в руководстве пользователя, какой IP-адрес и пароль входа настроены изготовителем для вашей точки доступа.

Дважды щелкните мышью на кнопках OK, чтобы закрыть окна настройки сетевого подключения. Закройте окно Сетевые подключения.

В меню Пуск выберите пункт Интернет.

В открывшемся окне программы Microsoft Internet Explorer в поле Адрес введите строку http://*IP-адрес вашей точки доступа* (например, http://192.168.1.1) и щелкните мышью на значке Переход.

В окне авторизации введите пароль, указанный в документации к вашей точке доступа.

Примечание. Дальнейшие действия зависят от конкретной точки доступа, поэтому ниже приведены лишь общие шаги настройки, позволяющие добиться сетевого взаимодействия с беспроводными клиентами. Следует обратить внимание, что для упрощения подключения здесь приведены такие параметры настройки, которые не рекомендуется применять в реальной работе (в частности, здесь включается режим оповещения и отключается защита при беспроводном доступе).

Найдите в меню управления точкой доступа раздел Wireless Settings («настройки беспроводного взаимодействия») или аналогичный и настройте следующие (или аналогичные) параметры:

Channel («канал») — оставьте установленным по умолчанию;

SSID («идентификатор») — введите название вашей точки доступа, например, ClassAP;

SSID Broadcast («оповещение») — для упрощения обнаружения вашей точки доступа беспроводными клиентами этот режим лучше включить (Enable);

Wireless Mode («стандарт, используемый точкой доступа») — для совместимости лучше указать смешанный режим 802.11b/g.

Щелкните мышью на кнопке Apply («применить»). Перейдите к разделу Encryption («шифрование») или аналогичному и выберите следующий (или аналогичный) параметр:

Security Mode («режим защиты») — отключен (Disabled).

Внимание! Отключение защиты производится в этом задании только для упрощения настройки! На практике такие параметры беспроводного взаимодействия применять нельзя.

Щелкните мышью на кнопке Apply («применить») и закройте окно программы Internet Explorer.

Настройка беспроводного адаптера и подключение к точке доступа

Примечание. Эта часть задания выполняется на компьютере, не имеющем проводного подключения к сети.

Возьмите беспроводной сетевой адаптер и установите его в один из компьютеров сети.

Примечание. Если это PCI-совместимый адаптер, то процедуру установки адаптера в разъем следует проводить, как описано в задании 2 лабораторной работы 3. Если это USB-адаптер, его можно подключить к любому порту USB работающего компьютера.

Включите компьютер и войдите в систему с учетной записью, входящей в локальную группу «Администраторы».

Примечание. Поскольку ОС Windows XP Professional пока не имеет в своем комплекте драйверов для большинства беспроводных адаптеров, после входа в систему или подключения USB-адаптера должен запуститься Мастер нового оборудования. Если этого не произошло, то проверьте в Диспетчере устройств: возможно, ваш адаптер автоматически определен ОС и драйверы для него уже установлены. В этом случае соответствующие пункты этого раздела можно пропустить.

На странице Мастер нового оборудования выберите радиокнопку Нет, не в этот раз и щелкните мышью на кнопке Далее.

На странице Если с устройством поставляется установочный диск, вставьте его убедитесь, что выбрана радиокнопка Автоматическая установка (рекомендуется), вставьте компакт- или флоппи-диск (из комплекта беспроводного адаптера) с драйвером и щелкните мышью на кнопке Далее.

Примечание. Если после установки диска запустится какая-либо программа, то закройте ее.

Мастер нового оборудования должен найти на диске подходящий для вашего адаптера драйвер. На странице Выберите наиболее подходящее программное обеспечение для вашего оборудования щелкните мышью на кнопке Далее.

Примечание. Если появится предупреждение, что устанавливаемое программное обеспечение не тестировалось на совместимость с Windows XP, щелкните мышью на кнопке Все равно продолжить.

На странице Мастер завершил установку программ для щелкните мышью на кнопке Готово.

Примечание. Если все операции выполнены правильно, то в Панели задач появится значок беспроводного сетевого подключения.

Щелкните правой кнопкой мыши на значке Беспроводное сетевое соединение в Панели задач и выберите в меню пункт Просмотр доступных беспроводных сетей.

На странице Выберите беспроводную сеть выберите сеть с названием, указанным в поле SSID при настройке вашей точки доступа (например, ClassAP), и щелкните мышью на кнопке Подключить.

Примечание. Если появится предупреждение, что сеть является незащищенной, то щелкните мышью на кнопке Подключить. Подключение к беспроводной сети должно установиться, однако оно корректно не заработает, пока не будут настроены совместимые IP-адреса.

Выполните двойной щелчок мышью на значке Беспроводное сетевое соединение (ClassAP) в Панели задач.

В окне Состояние Беспроводное сетевое соединение щелкните мышью на кнопке Свойства.

В окне свойств беспроводного сетевого подключения щелкните мышью на строке Протокол Интернета (TCP/IP) в списке Компоненты, используемые этим подключением, а затем щелкните мышью на кнопке Свойства.

В окне настройки параметров протокола IP выберите радиокнопку Использовать следующий IP-адрес и введите параметры:

IP-адрес — 192.168.1.150;

маска подсети — 255.255.255.0.

Дважды щелкните мышью на кнопках ОК и закройте все окна.

Подключение точки доступа к сети Ethernet и проверка взаимодействия в гетерогенной сети

Примечание. Эта часть задания выполняется на компьютерах, подключенных к сети Ethernet, построенной в ходе выполнения задания 1 данной лабораторной работы.

Используя кабель «витая пара», подключите беспроводную точку доступа к порту RJ-45 коммутатора Fast Ethernet.

Настройте на компьютерах сети параметры протокола IP, совместимые с теми, которые вы использовали при настройке беспроводной точки доступа и компьютера с беспроводным адаптером, например, следующие:

IP-адрес — 192.168.1.10*x*, где *x* — номер компьютера в классе;

маска подсети — 255.255.255.0.

То есть, первый компьютер должен иметь IP-адрес, равный 192.168.1.101, второй — 192.168.1.102 и т. д.

Попытайтесь обратиться к общим ресурсам на компьютерах сети (особенно интересно проверить, работает ли обращение к ресурсам компьютеров с беспроводными адаптерами).

Удалось ли вам обратиться к ресурсам какого-либо из компьютеров сети?

Закройте все окна и завершите работу с компьютером.

Практическая работа №6
Организация беспроводной связи по стандарту Bluetooth
Цель:
- обобщение и систематизация знаний по теме «Базовые технологии локальных сетей»;
- изучение концепции беспроводных сетевых технологий, классификации беспроводных сетей;
- исследование характеристик беспроводной персональной сети стандарта IEEE 802.15.
Задание 1. Соединение телефона и компьютера.
Задание 2. Соединение двух компьютеров.
Задания к работе
Задание 1. Соединение телефона и компьютера.
1) Соединение и синхронизация осуществляются с помощью программы BlueSoleil.
2) Вторым необходимым элементом является наличие Bluetooth-адаптера. В телефоне он является встроенным, а установка адаптера на компьютер не вызывает проблем, т. к. осуществляется с помощью Мастера установки нового оборудования Windows XP.

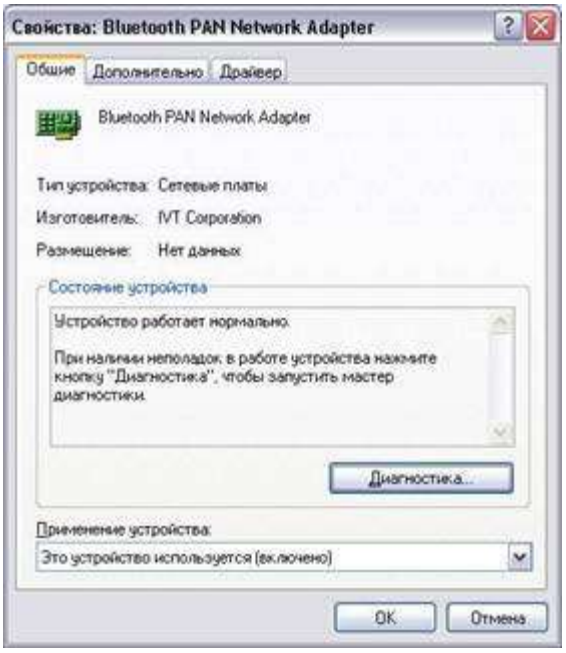


Рисунок 1. Настройка адаптера Bluetooth
3) Теперь необходимо раскрыть окно «Bluetooth-окружение» и выбрать в верхнем меню раздел Bluetooth, щелкнуть пункт «Дополнительные настройки» и в открывшемся окне нажать на «Локальные службы». Далее нужно указать и запомнить COM-порт для организации соединения.

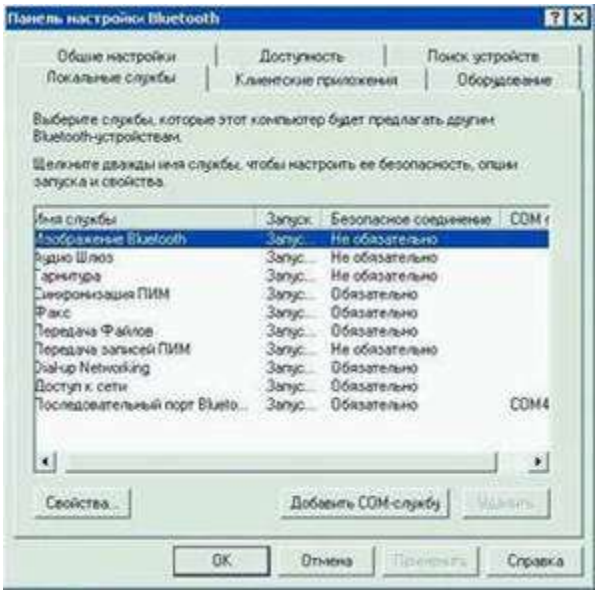


Рисунок. 2 Панель настройки Bluetooth

4) В меню Bluetooth телефона активируем одноименную функцию. Аппарат найдет все Bluetooth-устройства, находящиеся в радиусе его действия. Нам остается только выбрать имя нашего компьютера и нажать Next. После - на экране возникнет требование ввести код; вводим 0000. Переходим к экрану компьютера и также указываем 0000. Вовсе не обязательно использовать именно эту комбинацию - главное, чтобы пароль по обе стороны подключения был одинаков.

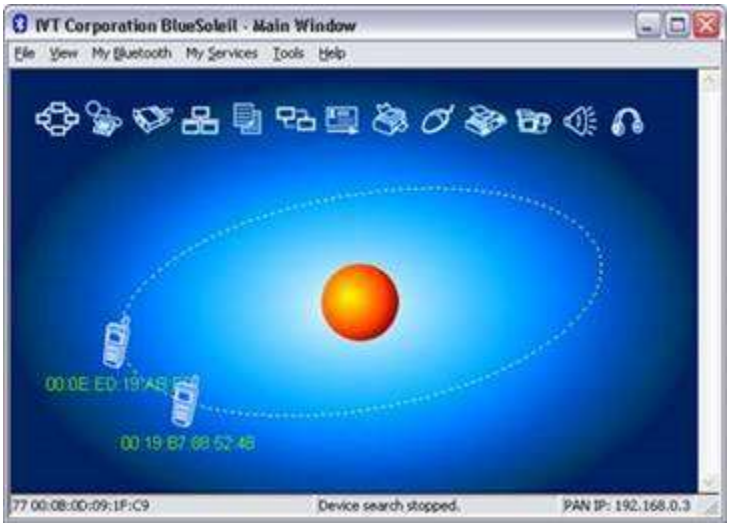


Рисунок 3. Окно диалога, в котором отображаются телефоны с активным Bluetooth

5) После окончания синхронизации в проводнике становится возможным доступ к содержимому памяти устройства. Данная функция очень удобна для установки новых программ и копирования важной информации.

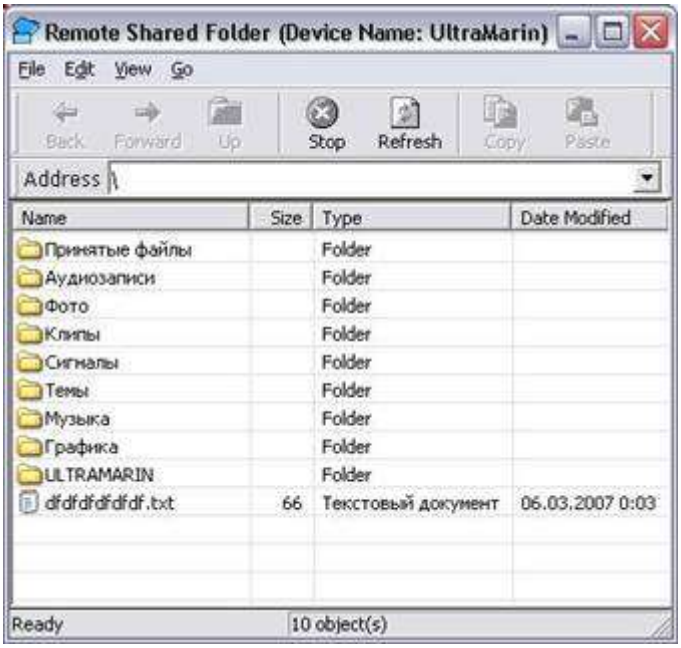


Рисунок 4. Содержимое телефона отображено на компьютере

Полученные в результате проведения двух опытов данные представить в таблицах 1 и 2.

Таблица 1 - Передача данных по Bluetooth (с компьютера на телефон)

Тип файла	Размер файла Кб	Время передачи,с	Скорость передачи Кбит/с

Таблица 2 - Передача данных по Bluetooth (с компьютера на телефон)

Тип файла	Размер файла Кб	Время передачи,с	Скорость передачи Кбит/с

Задание 2. Соединение двух компьютеров.

Если нужно соединить два компьютера между собой с помощью технологии Bluetooth, нужно использовать Bluetooth-адаптер. После объединения двух компьютеров при помощи Bluetooth на экране появится диалоговое окно, изображенное на рисунке 5.

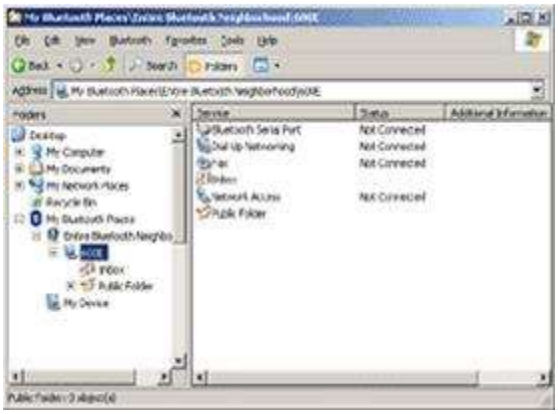


Рисунок 5. Объединение компьютеров с помощью Bluetooth.

Операционная система видит соединение Bluetooth, как достаточно быстрый последовательный порт (он примерно в пять раз быстрее, чем обычный COM или IrDA), и, при желании, даже можно организовать сетевое подключение Windows через него. Далее следует настроить подключение Bluetooth в папке «Сетевые подключение»

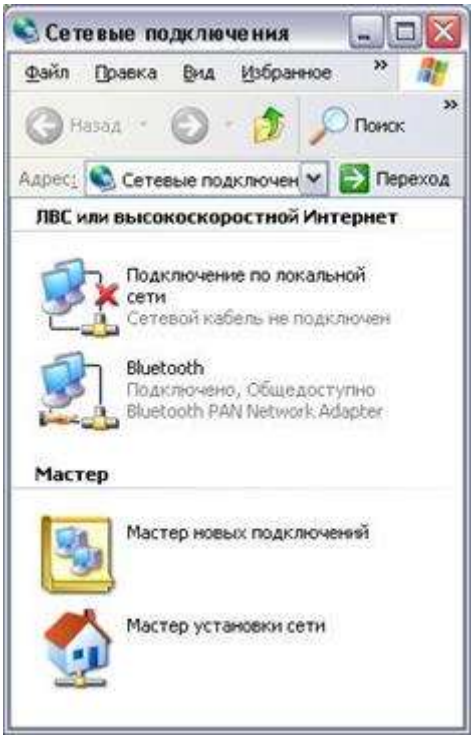


Рисунок 6. Активное подключение Bluetooth

Для этого нужно выбрать доступные этому подключению компоненты.

Рисунок 7. Настройка Bluetooth

Записать в таблицу данные, полученные в результате выполнения четырех опытов по передаче файлов разного размера и формата.

Таблица 3 - Передача данных по Bluetooth (с компьютера на компьютер)

№ опыта	Размер файла, МБ	Формат	Время передачи, с	Скорость передачи, Кбит/с	Средняя скорость передачи, Кбит/с
1.	1.				
2.					

3.					
2.	1.				
2.					
3.					
3.	1.				
2.					
3.					
4.	1.				
2.					
3.					

Контрольные вопросы:

1. В чем заключаются концепции беспроводных сетевых технологий?
2. Приведите классификацию беспроводных сетей.
3. Каковы характеристики беспроводной персональной сети стандарта IEEE 802.15.

Практическая работа №7

Методы и средства обеспечения безопасности сети WI-FI

Цель работы: изучить специфику задач обеспечения безопасности сети Wi-Fi, стандарты, протоколы и средства аутентификации и шифрации, выполнить настройку сети на разные уровни безопасности.

Ход работы:

1. Изучить средства обеспечения безопасности, поддерживаемые Wi-Fi адаптером DLink DWL-G520 и точкой доступа DLink DI-724P+ по стандарту 802.11

Сравнить методы аутентификации и шифрации WEP.

Выполнить настройки в сети Wi-Fi на варианты:

- открытая аутентификация,
- аутентификация с общим ключом,
- аутентификация по MAC-адресу,
- сокрытие SSID.

Аутентификация в беспроводных сетях

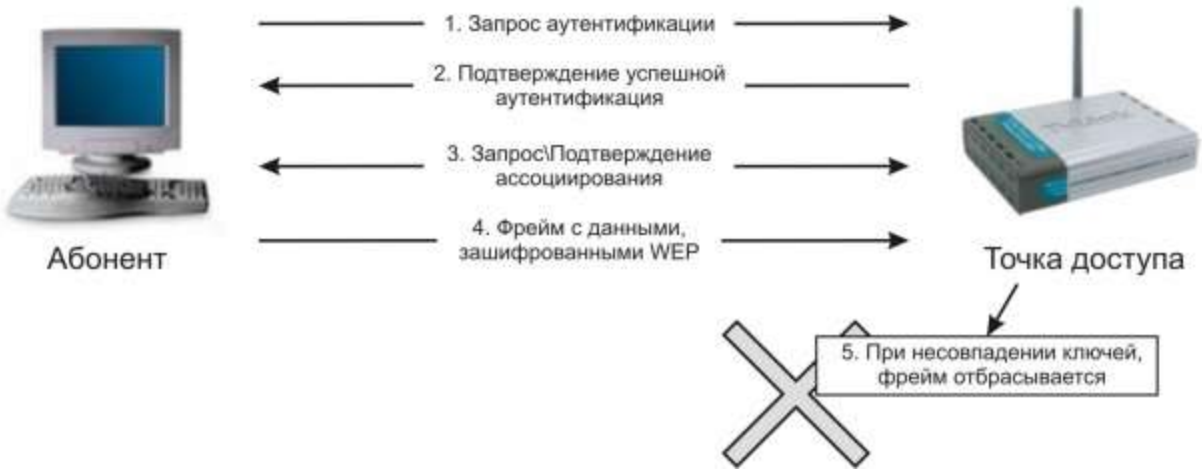
1) Открытая аутентификация

Открытая аутентификация, по сути, не является алгоритмом аутентификации в привычном понимании. Точка радиодоступа удовлетворит любой запрос открытой аутентификации. На первый взгляд использование этого алгоритма может показаться бессмысленным, однако следует учитывать, что разработанные в 1997 году методы аутентификации IEEE 802.11 ориентированы на быстрое логическое подключение к беспроводной локальной сети. Вдобавок к этому многие IEEE 802.11-совместимые устройства представляют собой портативные блоки сбора информации (сканеры штрих-кодов и т. п.), не имеющие достаточной процессорной мощности, необходимой для реализации сложных алгоритмов аутентификации.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:

- запрос аутентификации (Authentication Request);
- подтверждение аутентификации (Authentication Response).

Таким образом, при открытой аутентификации возможен доступ любого абонента к беспроводной локальной сети. Если в беспроводной сети шифрование не используется, любой абонент, знающий идентификатор SSID точки радиодоступа, получит доступ к сети. При использовании точками радиодоступа шифрования WEP сами ключи шифрования становятся средством контроля доступа. Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку радиодоступа, ни расшифровывать данные, переданные точкой радиодоступа.



Уязвимость открытой аутентификации

Открытая аутентификация не позволяет точке радиодоступа определить, является абонент легитимным или нет. Это становится заметной брешью в системе безопасности в том случае, если в беспроводной локальной сети не используется шифрование WEP

D-Link не рекомендует эксплуатацию беспроводных сетей без шифрования WEP В тех случаях, когда использование шифрования WEP не требуется или невозможно (например, в беспроводных локальных сетях публичного доступа), методы аутентификации более высокого уровня могут быть реализованы посредством Internet-шлюзов.

2) Аутентификация с общим ключом

Можно вводить интерактивно или в свойствах адаптера.

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP.

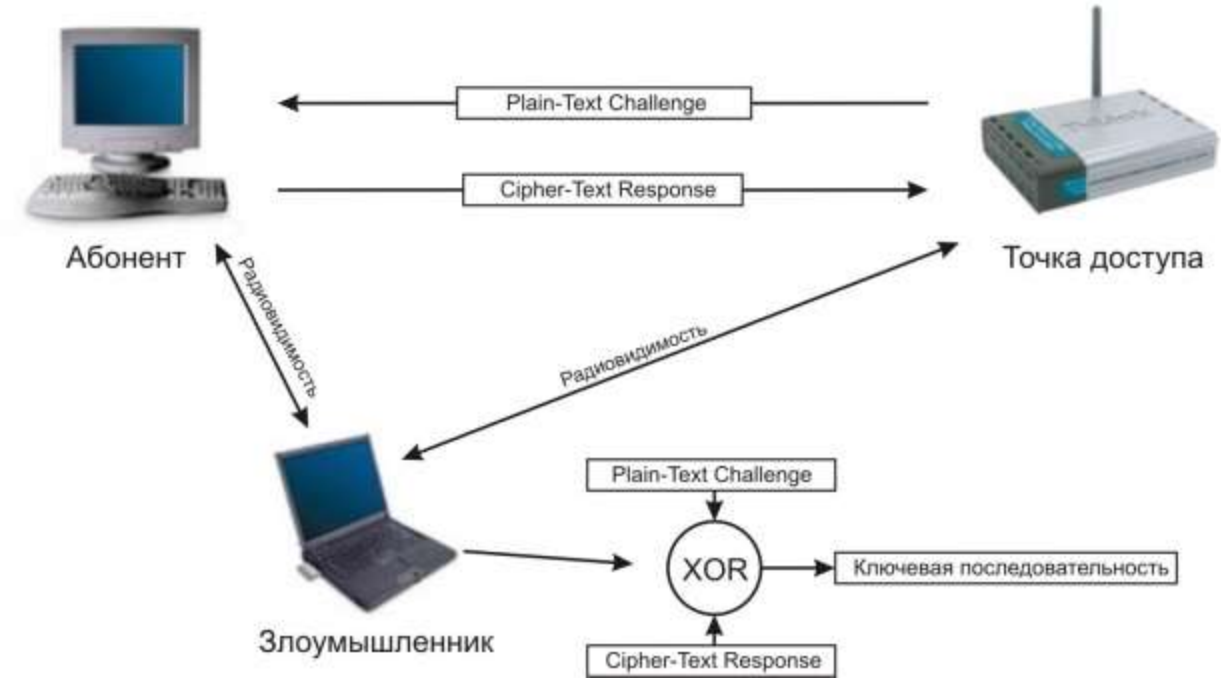
Процесс аутентификации:

1. Абонент посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.
2. Точка радиодоступа посылает подтверждение аутентификации, содержащее Challenge Text.
3. Абонент шифрует Challenge Text своим статическим WEP-ключом и посылает точке радиодоступа запрос аутентификации.
4. Если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем Challenge Text, она посылает абоненту подтверждение аутентификации, таким образом предоставляя доступ к сети.

Уязвимость аутентификации с общим ключом

Аутентификация с общим ключом требует настройки у абонента статического WEP-ключа для шифрования Challenge Text, отправленного точкой радиодоступа. Точка радиодоступа аутентифицирует абонента посредством дешифрации его ответа на Challenge и сравнения его с отправленным оригиналом. Обмен фреймами, содержащими Challenge Text, происходит по

открытому радиоканалу, а значит, подвержен атакам со стороны наблюдателя (Man in the middle Attack). Наблюдатель может принять как нешифрованный Challenge Text, так и тот же Challenge Text, но уже в шифрованном виде. Шифрование WEP производится путем выполнения побитовой операции XOR над текстом сообщения и ключевой последовательностью, в результате чего получается зашифрованное сообщение (Cipher-Text). Важно понимать, что в результате выполнения побитовой операции XOR над зашифрованным сообщением и ключевой последовательностью мы имеем текст исходного сообщения. Таким образом, наблюдатель может легко вычислить сегмент ключевой последовательности путем анализа фреймов в процессе аутентификации абонента.



3) Аутентификация по MAC-адресу

Аутентификация абонента по его MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями оборудования для беспроводных сетей, в том числе D-Link. При аутентификации по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации. Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних абонентов.

Уязвимость аутентификации по MAC-адресу

Стандарт IEEE 802.11 требует передачи MAC-адресов абонента и точки радиодоступа в открытом виде. В результате в беспроводной сети, использующей аутентификацию по MAC-адресу, злоумышленник может обмануть метод аутентификации путем подмены своего MAC-адреса легитимным. Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Злоумышленник может воспользоваться анализатором трафика протокола IEEE 802.11 для выявления MAC-адресов легитимных абонентов.

Практическая работа №8

Изучение характеристик системы GPS

Цель работы: изучить характеристики навигационного поля GPS, получить практические навыки имитации навигационных сигналов.

Указания к выполнению Теоретические сведения о принципах работы и функциональных возможностях используемого оборудования и программных средств содержатся в теоретической части, а также в руководстве по программной среде SimGEN.

Порядок выполнения

1. Изучить характеристики навигационного поля в зоне видимости для заданного географического расположения потребителя, в т.ч.: — подготовить оборудование для имитации навигационного поля, соответствующего заданной эфемеридной информации и заданному географическому расположению потребителя; — запустить оборудование для имитации навигационного поля; — определить количество и размещение навигационных спутников в зоне видимости; — зафиксировать уровни сигналов, поступающих от различных НКА; — оценить геометрический фактор, соответствующий заданной конфигурации НКА и заданному географическому расположению потребителя; — оценить погрешность определения координат навигационным приемником.

2. Определить влияние географического расположения потребителя на характеристики навигационного поля в зоне видимости, в т.ч.: — изменить географическое расположение потребителя по широте и повторить перечисленные выше действия; — построить зависимости геометрического фактора и погрешности определения координат от широты потребителя; — выполнить описанные действия, сменив информацию об альманахе и эфемеридах, отметить произошедшие изменения.

Контрольные вопросы

1. Какое минимальное количество навигационных спутников необходимо иметь в зоне видимости пользователя для определения его местоположения?

2. Как зависит точность определения местоположения пользователя от количества навигационных спутников в зоне его видимости?

3. Объяснить влияние расположения навигационных спутников на небосводе на точность определения местоположения пользователя.

4. Объяснить влияние уровня сигналов от навигационных спутников на точность навигации.

5. Что характеризует геометрический фактор?

6. От чего зависит геометрический фактор и влияет ли на его величину географическое расположение потребителя? 7. Как можно улучшить геометрический фактор?

Практическая работа №9-10

Изучение видов соединений в IP-телефонии

Цель работы

Изучить виды соединений в сетях IP-телефонии

Изучить принципы организации соединений в сетях IP-телефонии

Освоить принципы построения сетей IP-телефонии

Задание

Ознакомиться с видами соединений

Зарисовать схемы организации связи

Ответить на контрольные вопросы

Контрольные вопросы:

1. Как работает схема IP-телефонии «компьютер-телефон»?
2. Какое терминальное оборудование используется в схеме связи «компьютер-компьютер»?
3. Как АЦП и ЦАП влияют на связь в процессе разговора между абонентами?
4. Для чего предназначен H.323 терминал?
5. Что такое ТФОП?
6. Что определяет формат E.164?
7. Какие услуги связи организуются при подключении абонентом IP-телефонии?
8. Для чего предназначен шлюз?
9. Что такое VoIP?
10. Какую функцию выполняет протокол H.245?

Практическая работа №11-12
Изучение сигнализация на основе протокола SIP

Цель работы
1 Изучить назначение сигнализации SIP
2 Изучить виды сигнальных сообщений SIP
2 Освоить принципы организации сигнального канала по протоколу SIP
Задание
1 Ознакомиться с назначением протокола SIP
2 Зарисовать схемы организации связи по протоколу SIP
3 Ответить на контрольные вопросы
Контрольные вопросы:
1. Для чего предназначен протокол SIP?
2. По какой схеме работает протокол SIP?
3. С помощью какого транспортного протокола переносятся сигнальные сообщения SIP?
4. Какие команды запросов использует SIP?
5. Какие команды ответов использует SIP?
6. Для чего предназначен сервер переадресации в схеме построения SIP сети?
7. Какие услуги связи организуются при подключении абонентом IP-телефонии?
8. Что представляет собой команда INVITE?
9. Какой сигнальный порт используется для обмена служебными сообщениями SIP?
10. Чем протокол SIP отличается от протокола H.323?

Практическая работа №13-14

Изучение процедур обработки речи в IP-телефонии

Цель работы

1 Изучить процедуры обработки речи в IP-телефонии

2 Произвести расчет полосы пропускания IP-телефонии

3 Освоить принципы построения сетей IP-телефонии

Задание

1 Ознакомиться с процедурами обработки речи в IP-телефонии

2 Произвести расчет полосы пропускания в расчете на один канал IP-телефонии для всех типов кодеков (таблица 2.1.1)

3 Ответить на контрольные вопросы

Контрольные вопросы:

1. Какие существуют процедуры обработки речи в IP-телефонии?
2. Как происходит обработка речи в соответствии с кодеком PCM?
3. Как происходит обработка речи в соответствии с кодеком CELP?
4. От каких параметров зависит полоса пропускания в IP-телефонии?
5. Какой объем составляют заголовки в общей полосе пропускания IP-канала?

Практическая работа №15-16 Беспроводные Ad-Hoc сети. Инфраструктура "точка доступа"

Цель работы:

Изучение структуры стенда, способов коммутации его составляющих. Получение навыков использования базовых утилит мониторинга беспроводной сети. Изучение основных принципов беспроводной связи.

Изучаемые технологии:

Сети Ad-Hoc. Инфраструктура «точка доступа».

Порядок выполнения работы:

Работа ориентирована на использование ОС MS Windows XP

1.Изучите раздел 1.1 «Описание комплекта». Найдите все описанные элементы комплекта.

2.Изучите главы 3 «Основные элементы сети Wi-Fi» и 4 «Архитектура IEEE 802.11» теоретического пособия.

3.Изучите раздел 2.1 «Настройка сетевых параметров в ОС MS Windows XP».

4.Включите рабочие ноутбуки и зарегистрируйтесь на них.

5.Постройте топологию, показанную на рисунке 1 (соединение в режиме Ad – Hoc).

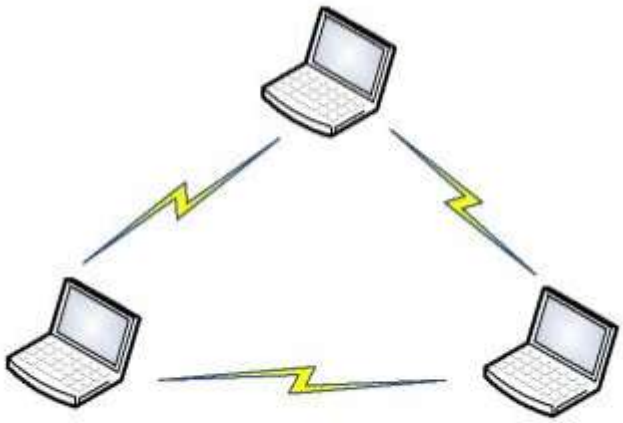


Рисунок 1. Сеть Режим Ad–Hoc.

6.Убедитесь в работоспособности построенной сети.

7.Определите и подпишите на рисунке 1 MAC- и IP-адреса беспроводных адаптеров.

8.Изучите главу 4.2. «Управление Cisco WAP4410N».

9.Постройте топологию, показанную на рисунке 2 (режим инфраструктуры).

10.После включения точки доступа восстановите заводские настройки.

11.Используя меню настройки включите режим «точка доступа» (Mode: Access point).

12.С помощью утилиты ping проверьте связь каждой рабочей станции со остальными.

13.Определите параметры узлов созданной сети. На рисунке 2 отметьте IP- и MAC-адреса машин и точки доступа.

14.С помощью утилиты настройки точки доступа определите идентификатор сети SSID. Запишите его под рисунком.

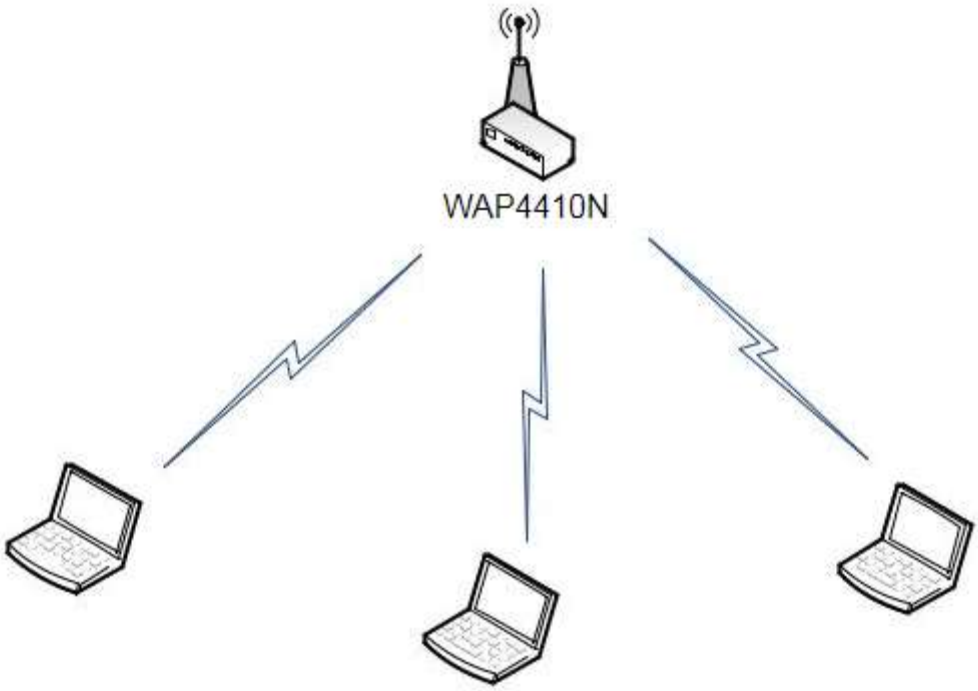


Рисунок 2. Режим инфраструктуры «точка доступа».

15.Установите для точки доступа 10 канал передачи данных. Все устройства в одной и той же сети должны использовать один и тот же канал передачи.

16.Изучить параметры на вкладке Wireless→Advanced. Поясните смысл каждого параметра преподавателю.

Практическая работа № 17.

Основные инфраструктуры беспроводных сетей IEEE 802.11.

Цель работы:

Изучение режимов работы беспроводного оборудования (на примере Cisco WAP4410N).

Изучаемые технологии:

Инфраструктура «мост», «мост с точкой доступа», «повторитель», «клиент точки доступа».

Порядок выполнения работы:

Работа ориентирована на использование ОС MS Windows XP

1.Изучите главу 6 «Режимы работы беспроводного оборудования» теоретического пособия.

2.Соберите топологию сети, показанную на рисунке 3.

3.Настройте обе точки доступа для работы в режиме моста («Bridge»).

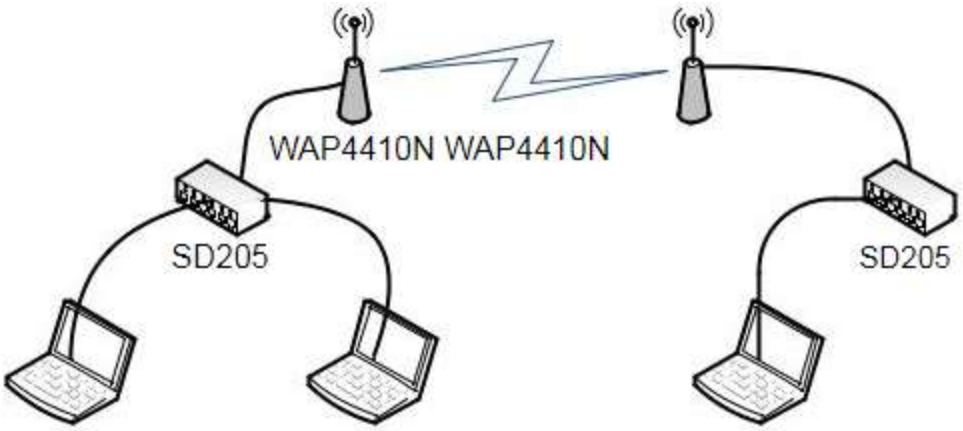


Рисунок 3. Топология сети для режима «моста».

4.Проверьте работоспособность созданной сети.

5.Соберите топологию сети, показанную на рисунке 4.

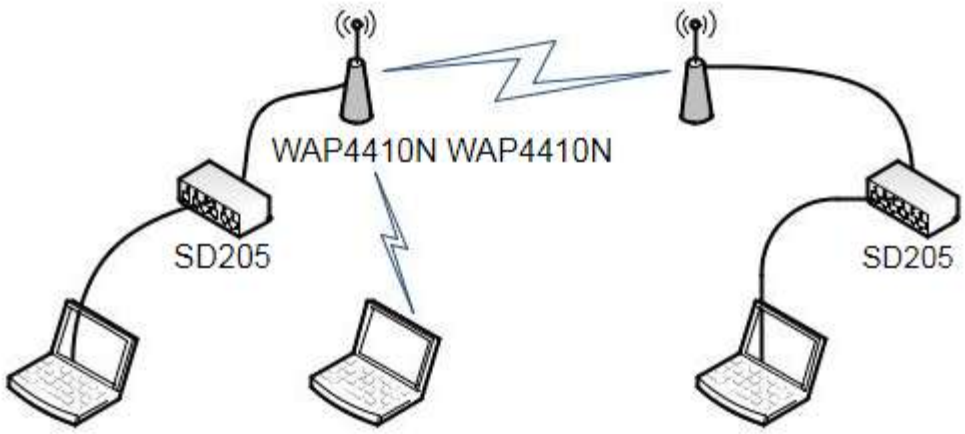


Рисунок 4. Топология сети для режима «моста с точкой доступа».

6.Настройте обе точки доступа для работы в режиме моста с точкой доступа (настроить мостовое соединение с возможностью точки доступа).

7.Проверьте работоспособность созданной сети.

8.Соберите топологию сети, показанную на рисунке 5.

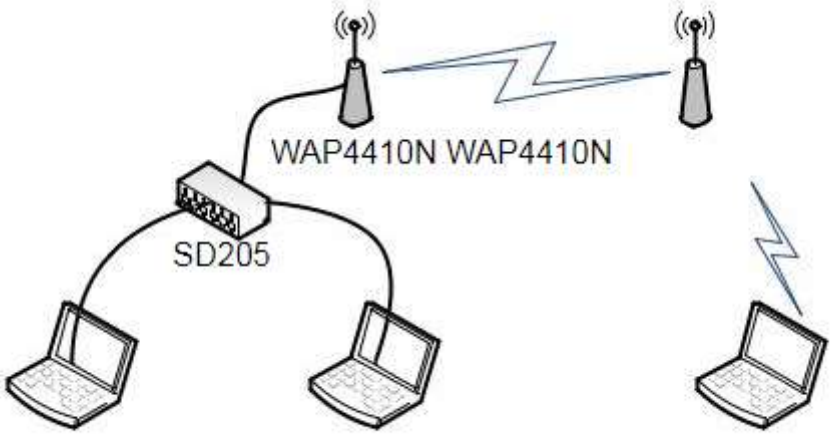


Рисунок 5. Топология сети для режима «повторителя».

9.Установить первую точку доступа в режим точки доступа, а вторую – в режим повторителя.

10.Проверьте работоспособность созданной сети.

11.Соберите топологию сети, показанную на рисунке 6.

12.Настройте соединение таким образом, чтобы вторая точка доступа являлась клиентом первой точки доступа.

13.Проверьте работоспособность созданной сети.

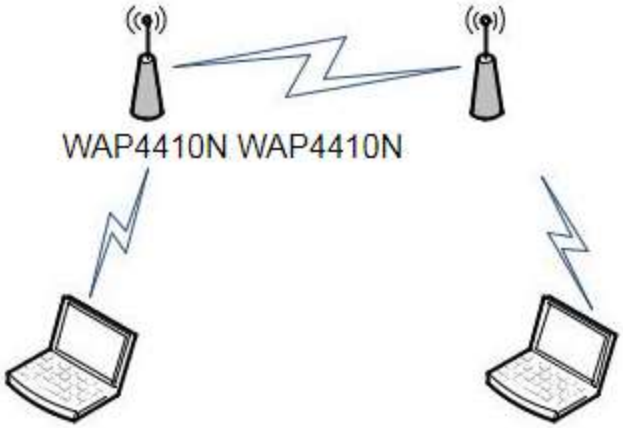


Рисунок 6. Топология сети для режима «клиент точки доступа».

Практическая работа № 18.
Определение радиуса действия беспроводной сети и применение способов, увеличивающих данный показатель.
Цель работы:
Определение радиуса действия (территории покрытия) беспроводной сети и применение способов, увеличивающих данный показатель.
Изучаемое оборудование: Антенны.

Порядок выполнения работы:
Работа ориентирована на использование ОС MS Windows XP
Внимание: данную работу могут выполнять одновременно две бригады.
1.Изучите главу 5 «Стандарты IEEE 802.11» теоретического пособия.
2.Настроите соединение (режим инфраструктуры), используя ноутбук и точку доступа WAP4410N.
3.Изучите раздел 2.2 «Утилита NetStumbler».
4.На ноутбуке запустите утилиту NetStumbler.
5.Далее возможны два варианта выполнения ЛР (на открытой местности и в здании).
6.*Открытая местность*. Используя карту местности, утилиту NetStumbler и GPSприѐмник, обозначьте зону покрытия Wi-Fi сети.
7.Используйте увеличитель радиуса сети Cisco WRE54G
8.Повторите действия пункта 6.
9.Сравните результаты, полученные в пунктах 6 и 8. Насколько увеличился радиус действия сети?
10.*Здание*. Используя план этажа и утилиту NetStumbler, обозначьте зону покрытия Wi-Fi сети.
11.Используйте увеличитель радиуса сети Cisco WRE54G
12.Повторите действия пункта 10.
13.Сравните результаты, полученные в пунктах 10 и 12. Насколько увеличился радиус действия сети?
14.Одновременно включите точки доступа маршрутизатора 881w и WAP4410N и настройте их в режиме работы «Access Point» следующим образом:
✓WAP4410N: номер канала – 6, SSID – cisco1;
✓881w: номер канала – 11, SSID – cisco2.
15.Все точки доступа должны работать.
16.На удаленности 30-50 метров, используя утилиту NetStumbler, зафиксируйте уровень сигнала всех точек доступа. Какие результаты вы получили?

Практическая работа № 19.
Измерение скорости передачи данных сетей Wi-Fi.
Цель работы:
Измерение скорости передачи данных по сетям Wi-Fi.
Порядок выполнения работы:

Работа ориентирована на использование ОС MS Windows XP
Внимание: данную работу могут выполнять одновременно две бригады. Для её выполнения понадобятся дополнительные внешние беспроводные интерфейсы Cisco WUSB600N.
1. Соберите топологию, представленную на рисунке 7.

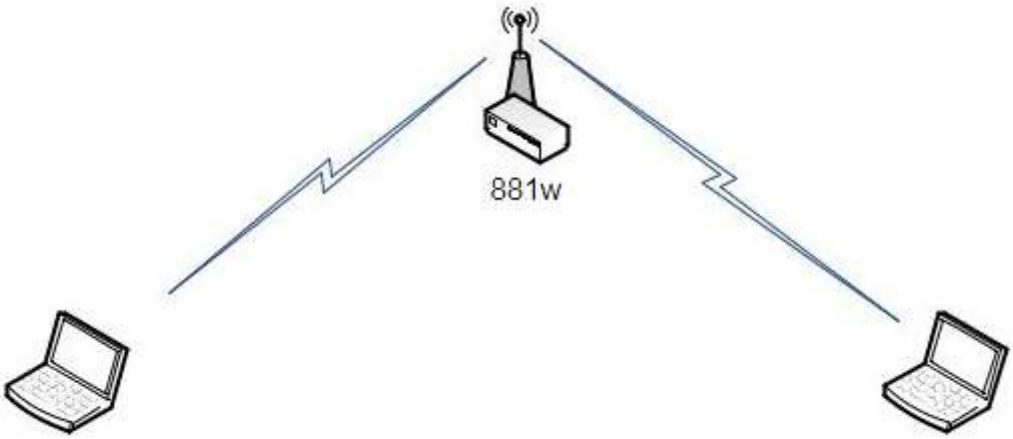


Рисунок 7. Тестирование 881w.

2.На одном из компьютеров запустите утилиту «Speed Test».
3.Осуществите передачу файла, размером не менее 100 Мб, с одного ноутбука на другой.
4.Установите полезную пропускную способность канала передачи данных.
5.Соберите топологию, представленную на рисунке 9.

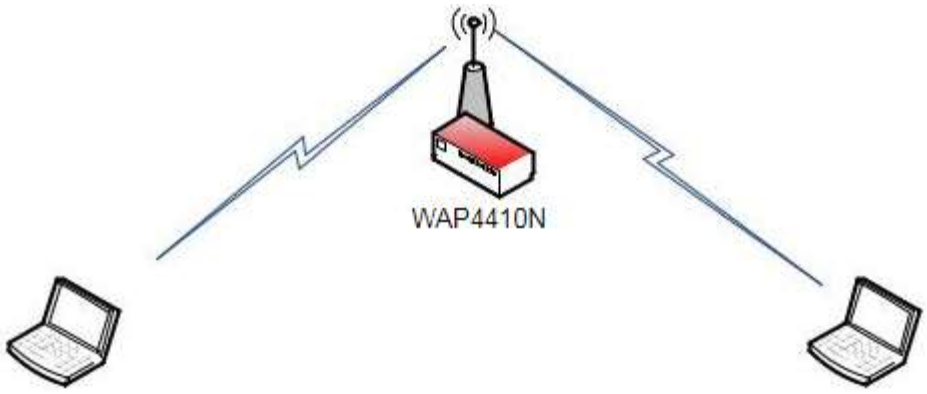


Рисунок 9. Тестирование WAP4410N.

6.Удостоверьтесь, что скорость подключения к сети ноутбуков составляет 300 Мбит/с.
7.Осуществите передачу файла, размером не мене 100 Мб, с одного ноутбука на другой.
8.Установите полезную пропускную способность канала передачи данных.
9.Ответьте на вопрос: насколько в среднем отличается полезная пропускная способность от пропускной способности канала, заявленной в стандартах?

Практическая работа № 20-21.
Использование беспроводных маршрутизаторов.
Цель работы:
Получение практических навыков предоставления доступа в Интернет клиентам беспроводной сети (офисные работники) через проводной выделенный канал.
Изучаемое оборудование и технологии:
Беспроводной маршрутизатор Cisco 881w. Протокол построения виртуальных частных сетей PPPoE.
Порядок выполнения работы:
1.Соберите топологию сети, показанную на рисунке 11 (ноутбук 3 необходимо подсоединять к 881w через WAN-интерфейс).
2.На ноутбуках 1 и 2 загрузите ОС MS Windows XP, на ноутбуке 3 загрузите Linux.
3.Ноутбуки 1 и 2 включите в подсеть 192.168.1.0/24., ноутбук 3 и WAN-интерфейс маршрутизатора включите в подсеть 192.168.2.0/24.
4.Используя утилиту гр-pppoe, настройте и запустите PPPoE-сервер на ноутбуке 3.
5.Настройте PPPoE-клиента на маршрутизаторе 881w.
6.Установите туннель между маршрутизатором и ноутбуком 3.
7.Проверьте возможность выхода в Интернет (то есть возможность доступа до ноутбука 3) с ноутбуков 1 и 2.

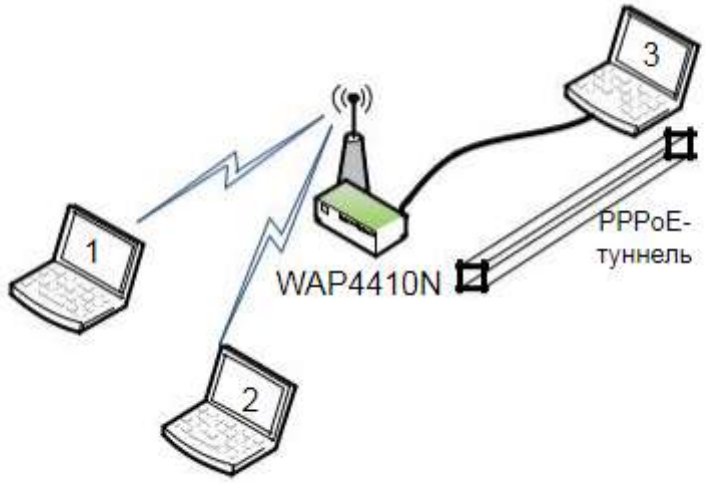


Рисунок 11.Соединение беспроводных сетей с каналом глобальной связи.

Практическая работа №22-23.

Изучение механизмов безопасности сетей Wi-Fi с использованием Windows XP.

Цель работы:

Изучение механизмов обеспечения безопасности беспроводной Wi-Fi сети на базе Windowsклиентов.

Изучаемые технологии:

Шифрование WEP/WPA/WPA2/AES. Фильтрация MAC-адресов. Запрет широковещания SSID.

Порядок выполнения работы:

1.Изучите главу 7 «Защита информации в беспроводных сетях» теоретического пособия.

2.Соберите топологию сети, представленную на рисунке 12.

Рисунок 12. Сеть «Ad–Hoc».

3.Настройте сеть в режиме Ad-Hoc, используя два ноутбука, на основе WEP– шифрования.

4.Используя утилиту «Speed Test» сравните полезную пропускную способность канала до и после использования WEP шифрования.

5.Соберите топологию, представленную на рисунке 13.

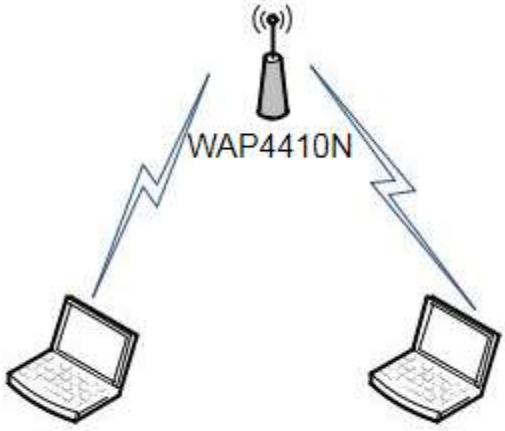


Рисунок 13. Режим «точка доступа».

6.Настройте защищенную беспроводную сеть (режим инфраструктуры) с использованием WEP шифрования.

7.Используя утилиту «Speed Test» сравните полезную пропускную способность канала до и после использования WEP шифрования.

8.Используя утилиту «Wireshark» осуществите перехват пакетов. Изучите содержимое перехваченных пакетов до и после применения шифрования. Расскажите о результатах преподавателю.

9.Используя сеть, представленную на рисунке 13, настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA и алгоритмом шифрования TKIP.

10.Используя утилиту «Speed Test», сравните полезную пропускную способность канала до

ипосле использования WPA.
11.Используя утилиту «Wireshark» осуществите перехват пакетов. Изучите содержимое перехваченных пакетов до и после применения WPA. Сравните с результатами, полученными с использованием WEP шифрования. Расскажите о результатах преподавателю.
12.Используя сеть, представленную на рисунке 13, настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA2/PSK и системой шифрования TKIP.
13.Используя утилиту «Speed Test», сравните полезную пропускную способность канала до ипосле использования WPA2/PSK.
14.Используя сеть, представленную на рисунке 13, настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA2/PSK и системой шифрования AES.
15.Используя утилиту «Speed Test», сравните полезную пропускную способность канала с использованием системы шифрования TKIP с системой шифрования AES.
16.Постройте сеть, топология которой представлена на рисунке 14.
17.Настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA2/EAP и системой шифрования TKIP.
18.Используя утилиту freeradius, настройте RADIUS-сервер таким образом, чтобы только абоненты, занесенные в базу данных пользователей смогли пройти процедуру аутентификации.
19.Чем хорош этот метод и в чем его недостатки?

Рисунок 14. Использование RADIUS-сервера.
20.Постройте сеть согласно рисунку 13.
21.Отключите в настройках точки доступа широковещание SSID.
22.На клиентских машинах настройте встроенные беспроводные адаптеры средствами ОС Windows. В параметрах настройки укажите в поле SSID имя сети, указанное в настройках точки доступа. Проверьте работоспособность вашей сети.
23.Как ведет себя точка доступа при отключении SSID? Для чего нужна эта функция?
24.Соберите топологию, представленную на рисунке 15.

25.К точке доступа 1 разрешить подключение ноутбуков A и B с помощью разрешенных списков MAC-адресов. К точке доступа 2 запретить подключение с ноутбука A с помощью запрещенных списков MAC-адресов.
26.Проверьте правильность выполненных настроек.

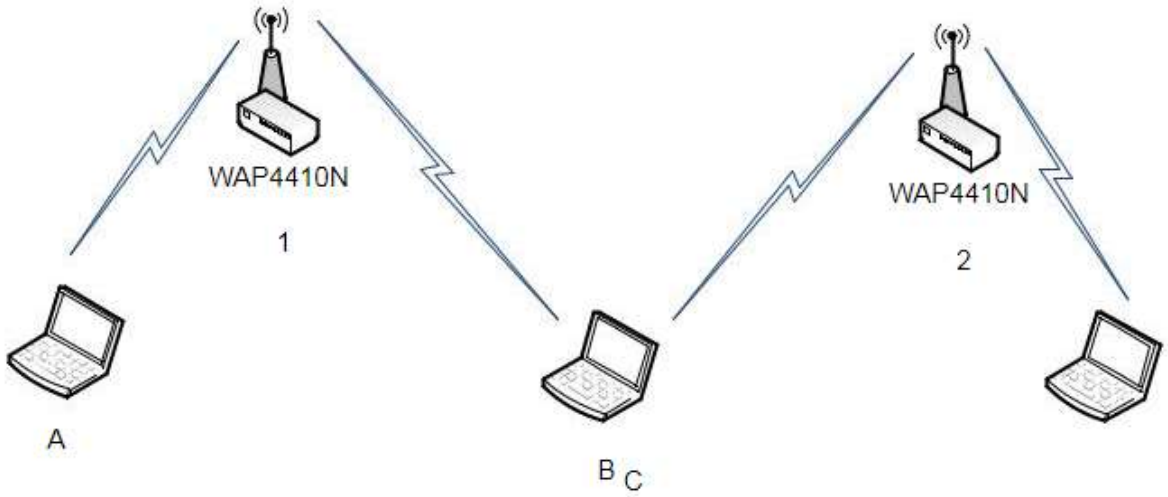


Рисунок 15. Использование фильтрации по MAC-адресам.

Практическая работа № 24-25.

Аудит безопасности сетей, шифруемых с использованием WEP, с использованием ОС Linux.

Цель работы:

Получение навыков аудита безопасности механизмов шифрования WEP.

Изучаемые технологии: Шифрование WEP.

Порядок выполнения работы:

1. Постройте сеть, топология которой представлена на рисунке 16.

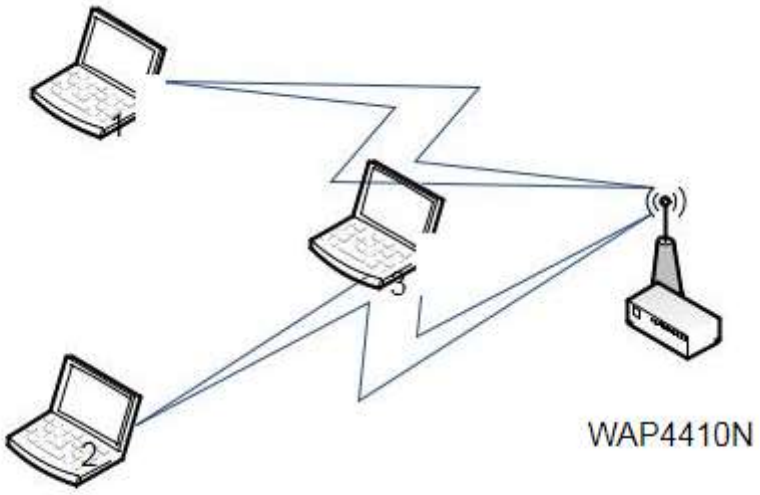


Рисунок 16.

2.Изучите главу 7 «Защита информации в беспроводных сетях» теоретического пособия.

3.Изучите раздел 2.8 «Утилита WepAttack».

4.Включите точку доступа, настройте канал и имя сети. Включите внутренний DHCPсервер. Включите шифрование WEP, используя 40-битный ключ.

5.Ассоциируйте 2 ноутбука с этой точкой доступа.

6.Запустите на третьем ноутбуке утилиту «Airodump-ng» для перехвата пакетов.

7.Выполните взаимодействие между ноутбуками 1 и 2.

8.Убедитесь (по экрану airodump-ng), что несколько пакетов с данными было перехвачено.

9.Используя скрипт keygen в каталоге «/root/Desktop/Scripts/», сгенерируйте файл словаря, содержащий несколько произвольных ключей и добавьте в конец файла заданный ключ. Длина словаря должна быть не меньше 10000 записей.

10.Используя полученный словарь и перехваченные пакеты выполните атаку на файл с перехваченными пакетами с помощью утилиты «WepAttack».

11.Выполните эти же действия, изменяя длину ключа и используя в качестве перехватчика Kismet вместо airodump. Варьируйте размер файла словаря, добавляя или удаляя записи. Сделайте вывод о влиянии длины ключа и размера словаря на скорость атаки.

Практическая работа № 26-27.

Обнаружение атак диссоциации с использованием ОС Linux.

Цель работы:

Изучение работы и возможностей утилиты Kismet.

Порядок выполнения работы:

1.Постройте сеть, топология которой представлена на рисунке 17.

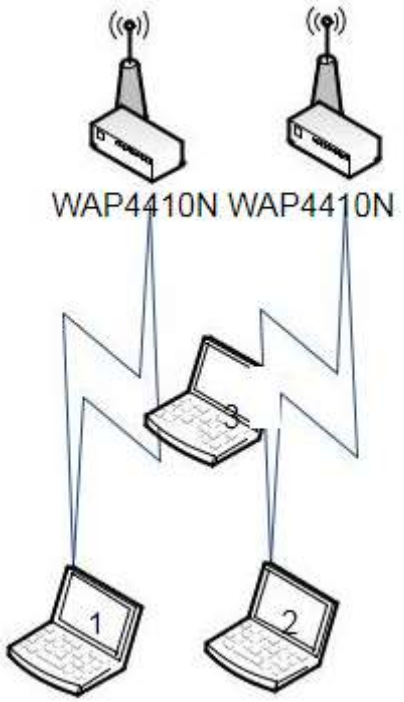


Рисунок 17.

2.Изучите главу 7 «Защита информации в беспроводных сетях» теоретического пособия.

3.Изучите раздел 2.5 «Утилита Kismet» и раздел 2.6 «Утилита MDK3».

4.Включите и настройте 2 точки доступа на разные каналы и имена сетей. Включите внутренний DHCP-сервер точки доступа.

5.Подключите 2 ноутбука к разным сетям, как показано на рисунке 17.

6.Запустите Kismet на 3 ноутбуке. Просмотрите обнаруженные сети.

7.Определите каналы, на которых располагаются точки доступа.

8.Посмотрите, какие типы пакетов перехватываются, когда ноутбуки ассоциированы, но не активны. Наблюдайте за графиком количества перехваченных пакетов в секунду

9.Подключите к ноутбуку 3 дополнительный беспроводной интерфейс DWA-120 и ассоциируйте его с одной из точек доступа.

10.Выполните взаимодействие между 2 ноутбуками, находящимися в одной сети (например, скопируйте файл с одного ноутбука на другой с помощью scp). Какие типы пакетов появились в эфире? Как изменился график?

11.Определите клиентов обнаруженных сетей.

12.Запустите на одном из 2 ноутбуков, подключенных к одной сети, непрерывную атаку диссоциации на вторую сеть (с помощью MDK или с помощью aireplay).

13.Посмотрите на реакцию Kismet.

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

1. Гагарина Л. Г. Разработка и эксплуатация автоматизированных информационных систем : учеб. пособие — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 384 с. — (Среднее профессиональное образование). - ISBN 978-5-16-106202-9. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1003025

2. Дибров М. В. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2019. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/

3.Партыка Т. Л., Попов, И.И. Информационная безопасность: учебное пособие – 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2019. - 432 с.: 60х90 1/16. - (Профессиональное образование) - Текст : электронный. - URL: https://new.znanium.com/