Содержание

В данном документе все ссылки указывают на разделы и главы в пособие «Управление стендом», если не указано иное пособие.

1. Инфраструктура сетей Wi-Fi

Лабораторная работа № 1.

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).

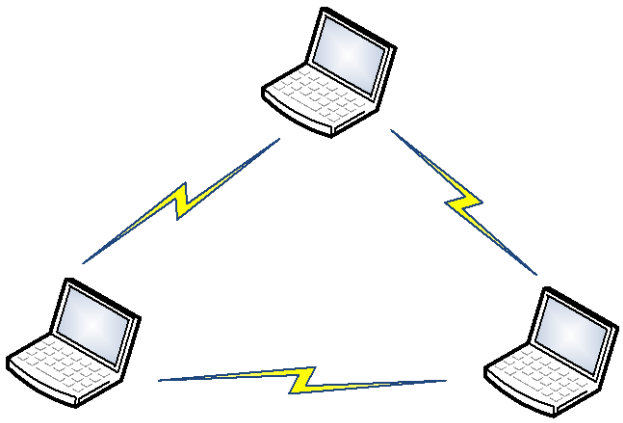

Рисунок 1. Сеть Режим Ad–Hoc.

6. Убедитесь в работоспособности построенной сети.
7. Определите и подпишите на рисунке 1 MAC- и IP-адреса беспроводных адаптеров.

8. Изучите главу «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.

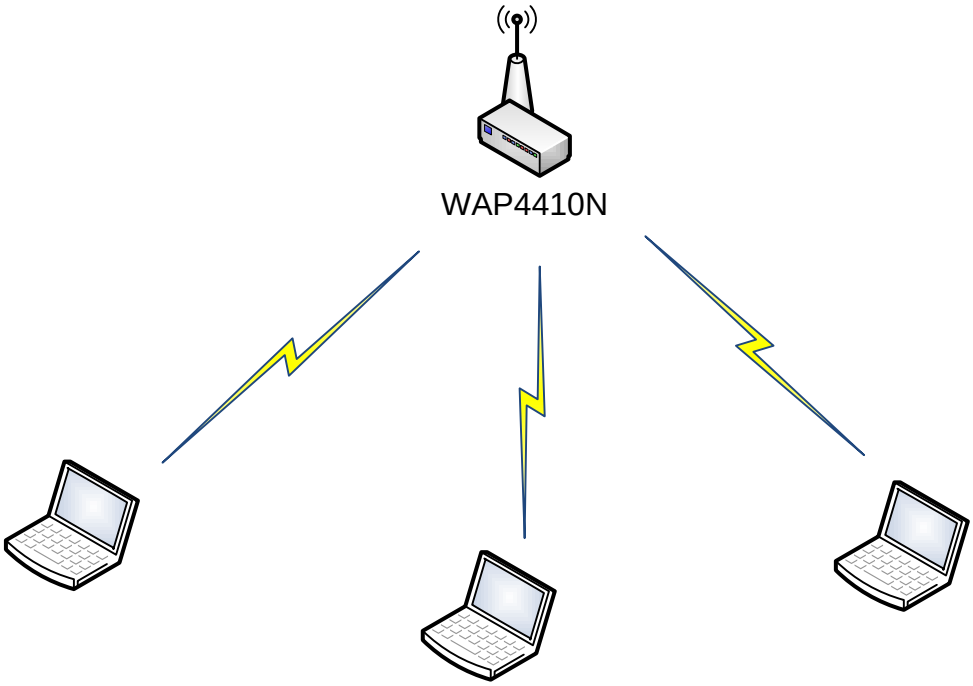

Рисунок 2. Режим инфраструктуры «точка доступа».

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.

Лабораторная работа № 2.

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»).

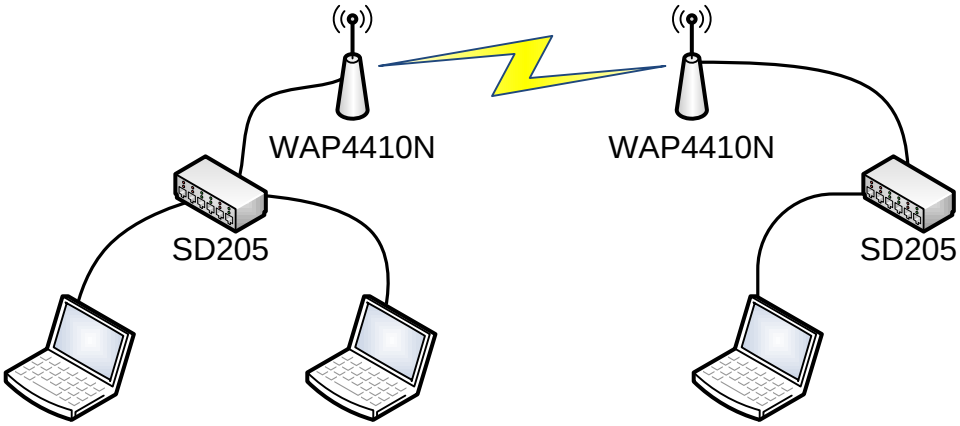

Рисунок 3. Топология сети для режима «моста».

4. Проверьте работоспособность созданной сети.
5. Соберите топологию сети, показанную на рисунке 4.

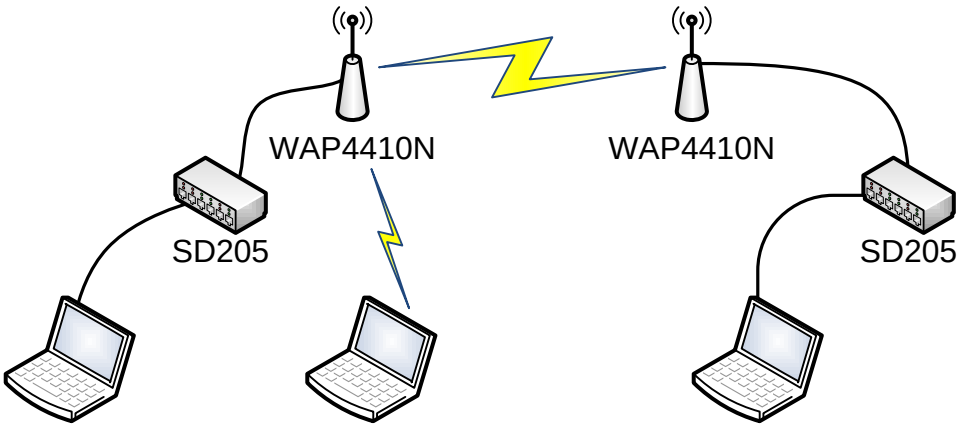

Рисунок 4. Топология сети для режима «моста с точкой доступа».

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.

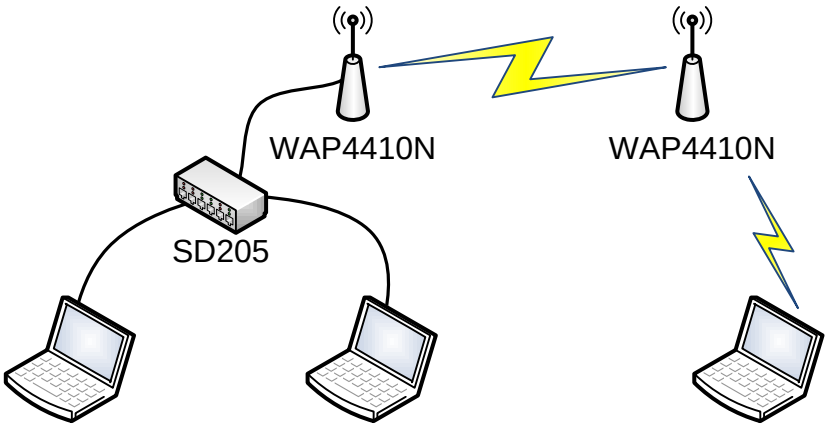

Рисунок 5. Топология сети для режима «повторителя».

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.

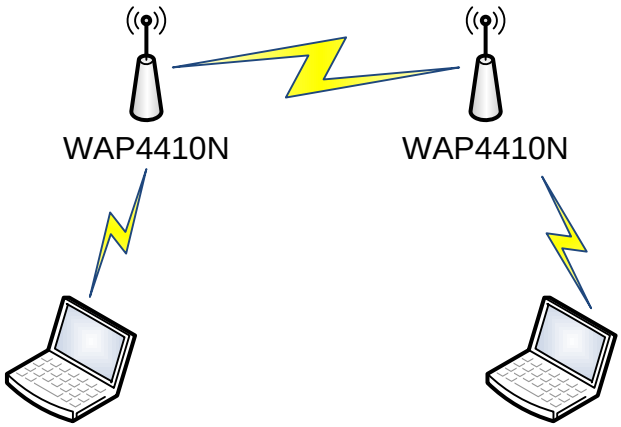

Рисунок 6. Топология сети для режима «клиент точки доступа».

2. Эффективность работы сетей Wi-Fi

Лабораторная работа № 3.

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 GPS-приёмник, 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?

Лабораторная работа № 4.

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.

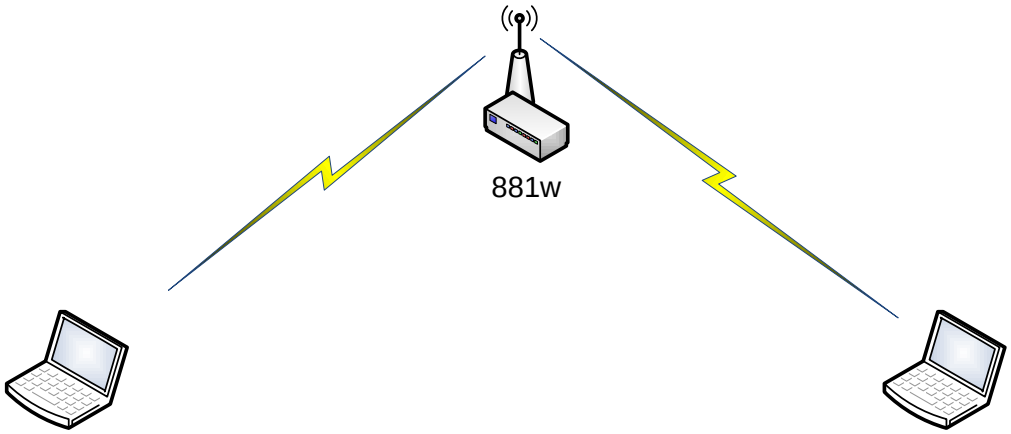

Рисунок 7. Тестирование 881w.

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.

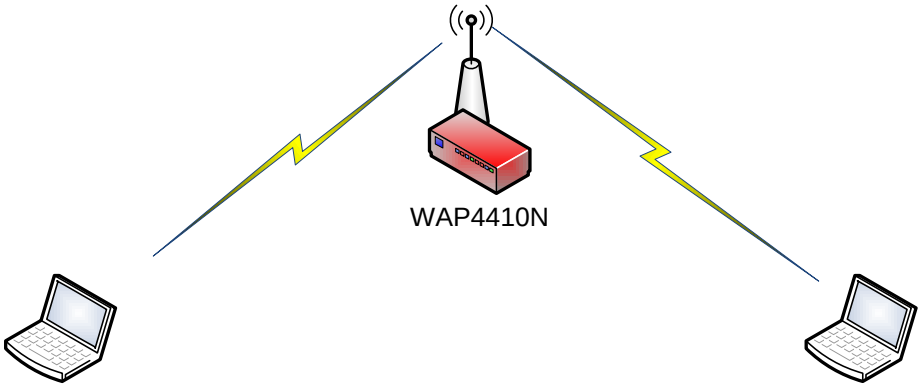

Рисунок 9. Тестирование WAP4410N.

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?

Лабораторная работа № 5.

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 rp-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.

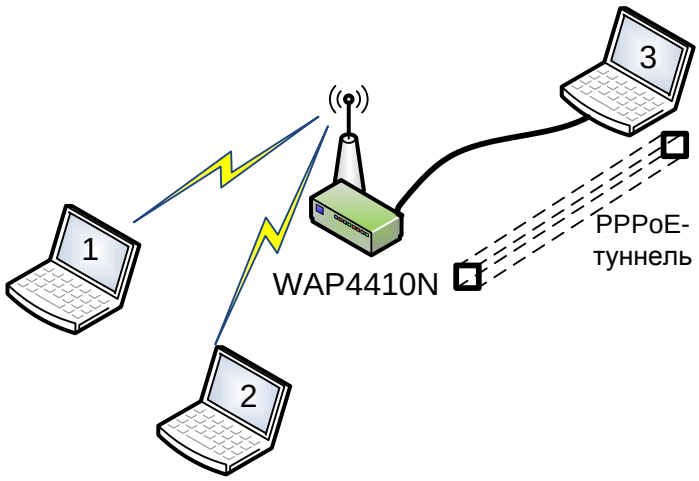

Рисунок 11.Соединение беспроводных сетей с каналом глобальной связи.

3. Безопасность в беспроводных сетях

Лабораторная работа № 6.

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

Цель работы:
Изучение механизмов обеспечения безопасности беспроводной Wi-Fi сети на базе Windows-клиентов.

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.

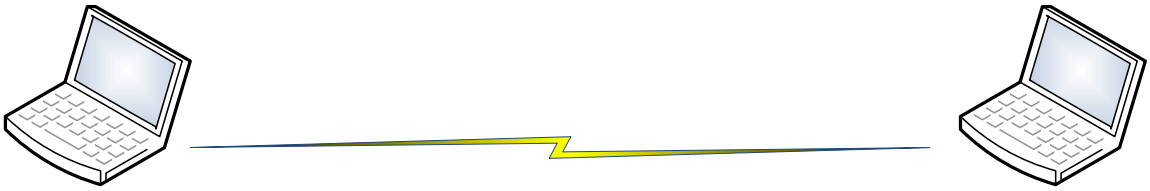

Рисунок 12. Сеть «Ad–Hoc».

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.

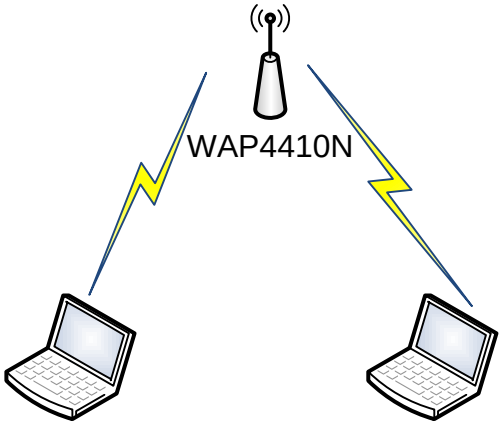

Рисунок 13. Режим «точка доступа».

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 и после 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 и после 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?

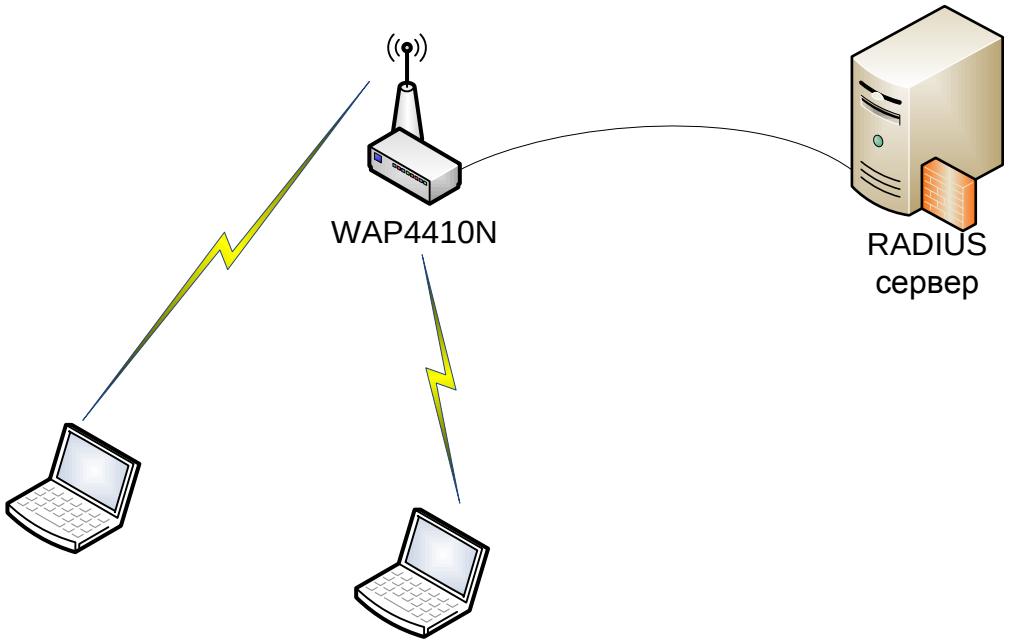

Рисунок 14. Использование RADIUS-сервера.

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.

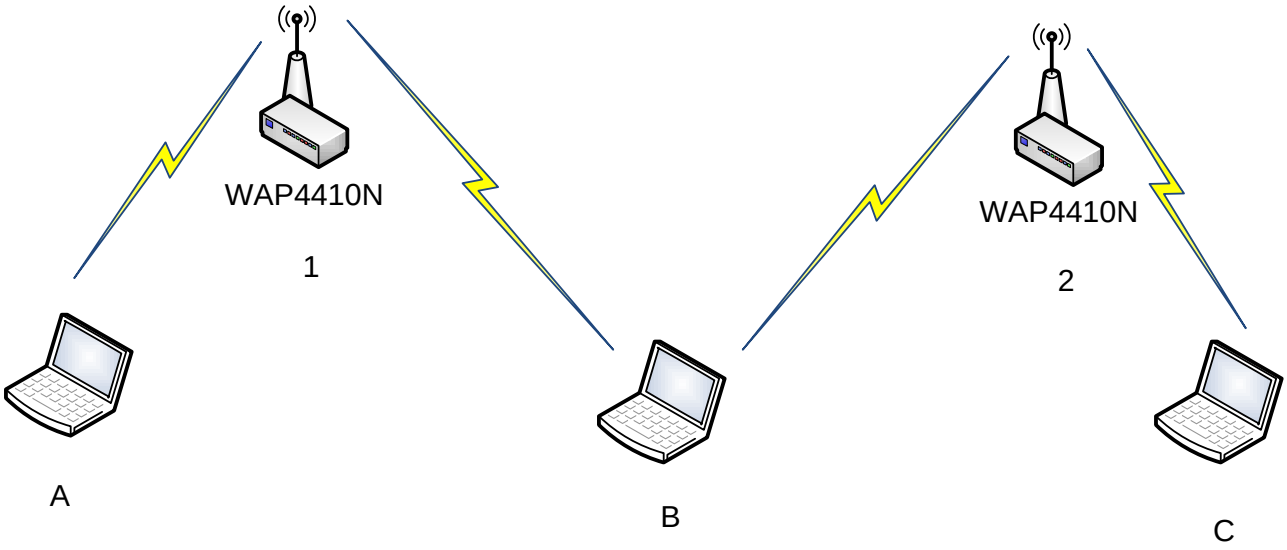

Рисунок 15. Использование фильтрации по MAC-адресам.

Лабораторная работа № 7.

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.

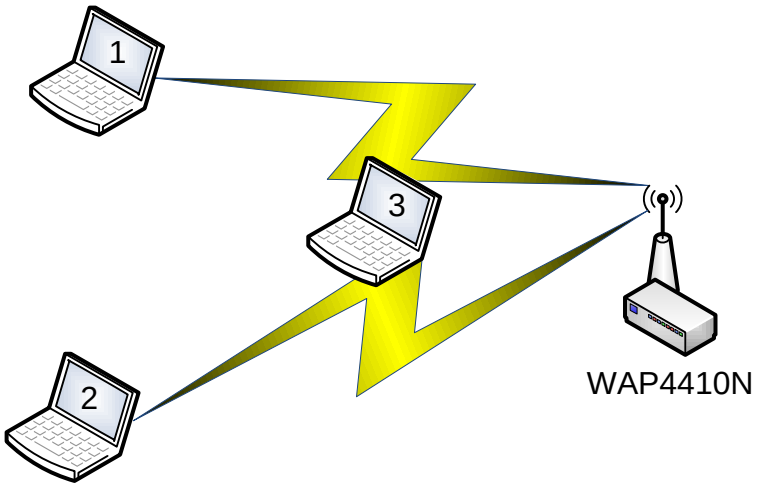

Рисунок 16.

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 DHCP-сервер. 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.

Лабораторная работа № 8.

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.

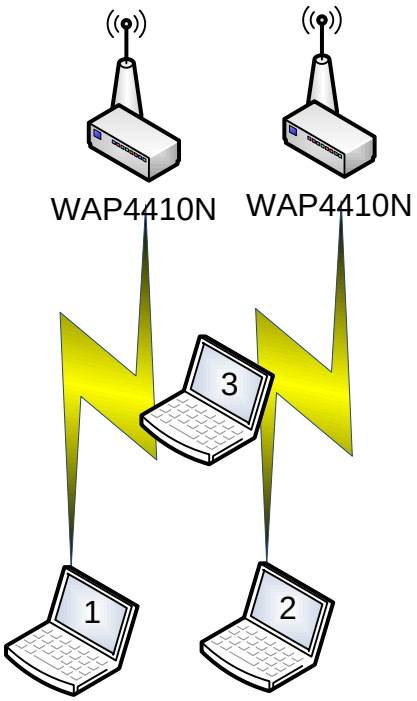

Рисунок 17.

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.