Лабораторная работа № 4

Тема: Настройка беспроводной сети (WI-FI)

Цель: научиться настраивать компьютеры для работы в беспроводных сетях по стандарту 802.11: обнаруживать точку доступа и программно настраивать ПК для работы.

Средства для выполнения работы:

аппаратные: компьютер с установленным сетевым адаптером; точка доступа (AccessPoint (AP), подключенная к локальной сети, беспроводной сетевой адаптер USB, соединительные кабели.

программные: ОС WindowsXP/Vista/7, *анализатор беспроводных сетей*

Теоретические сведения

WI-FI - это современная беспроводная технология соединения компьютеров в локальную сеть и подключения их к Internet. Именно благодаря этой технологии Internet становится мобильным и дает пользователю свободу перемещения не то что в пределах комнаты, но и по всему миру.

Под аббревиатурой "Wi-Fi" (от английского словосочетания "Wireless Fidelity", которое можно дословно перевести как "высокая точность беспроводной передачи данных") в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

- WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:
- WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорость современных сетей довольно высока (до 300 Мб/с), что позволяет использовать их для решения очень широкого спектра задач;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, все-таки меньшая скорость, подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации.

Сегмент Wi-Fi сети может использоваться как самостоятельная сеть, либо в составе более сложной сети, содержащей как беспроводные, так и обычные проводные сегменты.

Самый популярный стандарт беспроводных локальных сетей - *IEEE 802.11*.Институт инженеров по электротехнике и электронике IEEE (Institute of *Electrical*and *Electronics Engineers*) сформировал рабочую группу по

стандартам для беспроводных локальных сетей 802.11 в 1990 году. Работы по созданию стандарта были завершены через 7 лет, и в июне 1997 года была ратифицирована первая спецификация 802.11. Стандарт *IEEE 802.11* являлся первым стандартом для продуктов *WLAN* от независимой международной организации, разрабатывающей большинство стандартов для проводных сетей.

Один из первых высокоскоростных стандартов беспроводных сетей — IEEE 802.11a — определяет скорость передачи уже до 54 Мбит/с. Рабочий диапазон стандарта 5 ГГц.

Принятый, в 1999 году стандарт IEEE 802.11b не является совместимым со стандартом 802.11a, поскольку стандарт предусматривает использование не лицензируемого диапазона частот 2,4 ГГц. Скорость передачи до 11 Мбит/с.

Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией Wireless Ethernet Compatibility Alliance (WECA), которая в настоящее время больше известна под названием Wi-Fi Alliance. Совместимые беспроводные продукты, прошедшие испытания по программе «Альянса Wi-Fi», могут быть маркированы знаком Wi-Fi.

Долгое время IEEE 802.11b был распространённым стандартом, на базе которого было построено большинство беспроводных локальных сетей. Сейчас его место занял стандарт IEEE 802.11g, постепенно вытесняемый высокоскоростным IEEE 802.11n.

Проект стандарта IEEE 802.11g был утверждён в октябре 2002 г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость соединения до 54 Мбит/с и превосходя, таким образом, стандарт IEEE 802.11b, который обеспечивает скорость соединения до 11 Мбит/с. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b.

802.11 — Изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997)
802.11a — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001)
802.11b — Улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999)
802.11d — Интернациональные роуминговые расширения (2001)
802.11e — Улучшения: QoS, включение packet bursting (2005)
802.11g — 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003)
802.11h — Распределенный по спектру 802.11a (5 GHz) для совместимости в Европе (2004)
802.11n — Увеличение скорости передачи данных (600 Мбит/с). 2,4-2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g . Особенно распространён на рынке в США в устройствахD-Link, Cisco и Apple. (сентябрь 2009)
802.11p — WAVE — Wireless Access for the Vehicular Environment (Беспроводной Доступ для Транспортной Среды, такой как машины скорой помощи или пассажирский транспорт)
802.11ac — Новый, разрабатываемый IEEE стандарт. Скорости передачи данных до 1.3 Гбит/с, энергопотребление по сравнению с 802.11n снижено до 6

раз. Обратная совместимость с 802.11a/b/g/n. Финальная версия стандарта ожидается к концу 2012 года, а устройства, реализующие новый стандарт уже представлены.

802.11ad — Модификация стандарта 802.11ac, работающая в 60Ghz (частота не требует лицензирования). Скорость передачи данных до 7 Гбит/с.

Существует множество технологий безопасности, и все они предлагают решения для важнейших компонентов политики в области защиты данных: аутентификации, поддержания целостности данных и активной проверки. Мы определяем аутентификацию как аутентификацию пользователя или конечного устройства (клиента, сервера, коммутатора, маршрутизатора, межсетевого экрана и т. д.) и его местоположения с последующей авторизацией пользователей и конечных устройств.

Целостность данных включает такие области, как безопасность сетевой*инфраструктуры, безопасность* периметра и конфиденциальность данных. Активная проверка помогает удостовериться в том, что установленная политика в области безопасности соблюдается, и отследить все аномальные случаи и попытки несанкционированного доступа.

WEP

WiredEquivalentPrivacy (WEP) — алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания. Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. В настоящее время данная технология является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут. Тем не менее, она продолжает широко использоваться. Для безопасности в сетях Wi-Fi рекомендуется использовать WPA. WEP часто неправильно называют WirelessEncryptionProtocol.

Спецификация WPA

До мая 2001 г. стандартизация средств информационной безопасности для беспроводных сетей *802.11* относилась к ведению рабочей группы IEEE 802.11e, но затем эта проблематика была выделена в самостоятельное подразделение. Разработанный стандарт 802.11i призван расширить возможности протокола *802.11*, предусмотрев средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Основные производители Wi-Fi оборудования в лице организации *WECA* (*Wireless Ethernet* Compatibility Alliance), иначе именуемой Wi-Fi Alliance анонсировали спецификацию Wi-Fi Protected Access (*WPA*), соответствие которой обеспечивает совместимость оборудования различных производителей.

Новый стандарт безопасности *WPA* обеспечивает уровень безопасности куда больший, чем может предложить *WEP* Он перебрасывает мостик между

стандартами *WEP* и 802.11i и имеет немаловажное преимущество, которое заключается в том, что микропрограммное обеспечение более старого оборудования может быть заменено без внесения аппаратных изменений.

IEEE предложила *временный протокол целостности ключа* (*Temporal* Key Integrity Protocol, *TKIP*).

Основные усовершенствования, внесенные протоколом *TKIP*:

Пофреймовое изменение ключей шифрования. *WEP*-ключ быстро изменяется, и для каждого фрейма он другой;

Контроль целостности сообщения. Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения скрытых манипуляций с фреймами и воспроизведения фреймов;

Усовершенствованный механизм управления ключами.

В июне 2004 г. IEEE ратифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях - 802.11i.

Абсолютно новая система безопасности, лишенная недостатков *WEP*, представляет собой лучшее долгосрочное и к тому же расширяемое решение для безопасности беспроводных сетей. С этой целью комитет по стандартам принял решение разработать систему безопасности с нуля. Это новый стандарт 802.11i, также известный как *WPA2* и выпущенный тем же Wi-Fi Alliance.

802.11i (*WPA2*) - это наиболее устойчивое, расширяемое и безопасное решение, предназначенное в первую очередь для крупных предприятий, где управление ключами и администрирование доставляет множество хлопот.

Стандарт 802.1x/EAP (Enterprise-режим)

Проблемы, с которыми столкнулись разработчики и пользователи сетей на основе стандарта *802.11*, вынудили искать новые решения защиты беспроводных сетей. Были выявлены компоненты, влияющие на системы безопасности беспроводной локальной сети:

- Архитектура аутентификации.
- Механизм аутентификации.
- Механизм обеспечения конфиденциальности и целостности данных.
- Архитектура аутентификации IEEE 802.1x - стандарт IEEE 802.1x описывает единую архитектуру контроля доступа к портам с использованием разнообразных методов аутентификации абонентов.

Алгоритм аутентификации Extensible *Authentication Protocol* или *EAP* (расширяемый протокол идентификации) поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и ее пользователей с возможностью динамической *генерации ключей* шифрования.

Архитектура IEEE 802.1x

Архитектура IEEE 802.1x включает в себя следующие обязательные логические элементы (Рис. 1):

Клиент (Supplicant) - находится в операционной системе абонента;

Аутентификатор (Authenticator) - находится в программном обеспечении точки радиодоступа;

Сервер аутентификации (*Authentication Server*) - находится на RADIUS-сервере.

IEEE 802.1x предоставляет абоненту беспроводной локальной сети лишь средства передачи атрибутов серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является поддержка разрешенных политикой сетевой *безопасности методов* аутентификации.

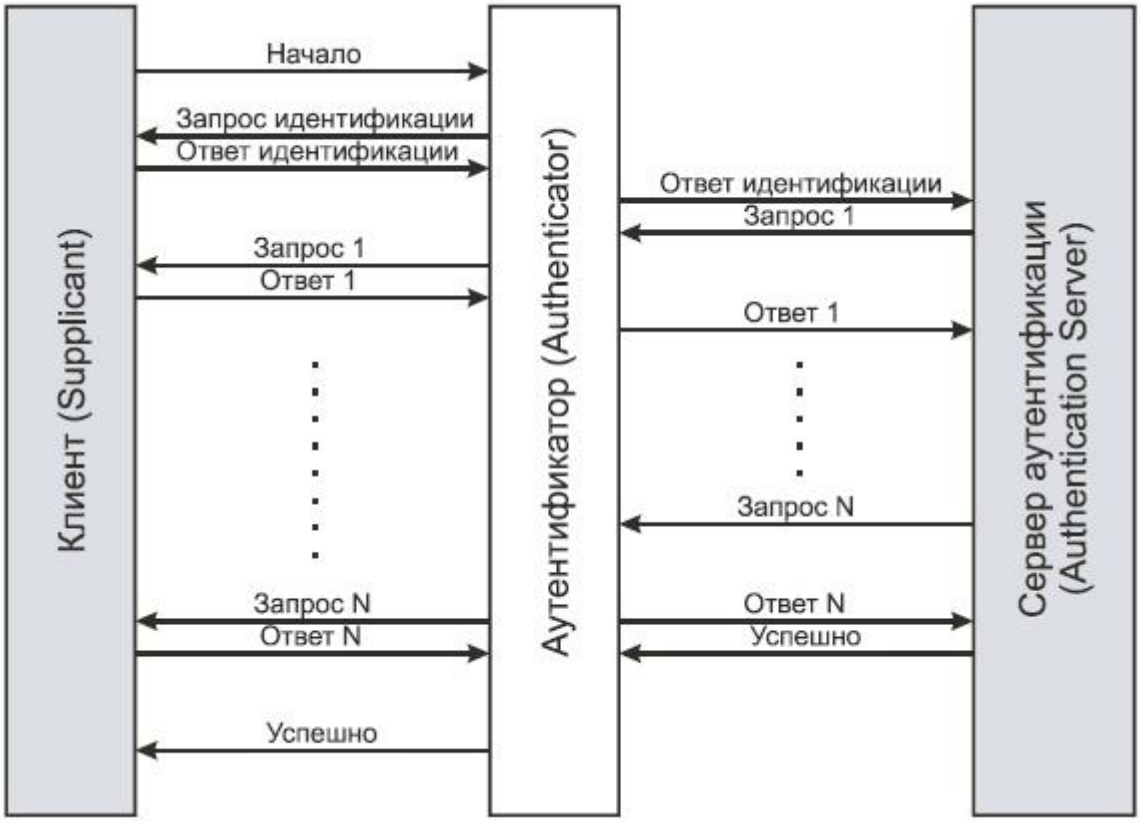


Рисунок 1 – Архитектура IEEE 802.1x

Режимы работы точек доступа.

Ad Hoc

В режиме *Ad Hoc* клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу "точка-точка", и компьютеры взаимодействуют напрямую без применения точек доступа. При этом создается только одна зона обслуживания, не имеющая интерфейса для подключения к проводной локальной сети.

Основное достоинство данного режима - простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.

Однако необходимо иметь в виду, что режим Ad Hoc позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость обмена данными будет ниже и составит не более 11/N Мбит/с, где N - число устройств в сети. Дальность связи

составляет не более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.

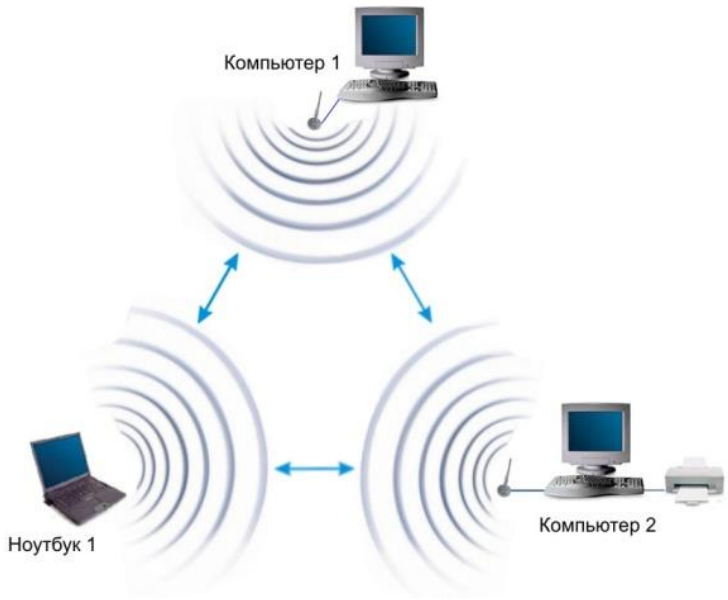


Рисунок 2 – Режим Ad Hoc

AP

В этом режиме точки доступа обеспечивают связь клиентских компьютеров. Точку доступа можно рассматривать как беспроводной коммутатор. Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам.

Точка доступа имеет порт Ethernet, через который базовая зона обслуживания подключается к проводной или смешанной сети - к сетевой *инфраструктуре*.

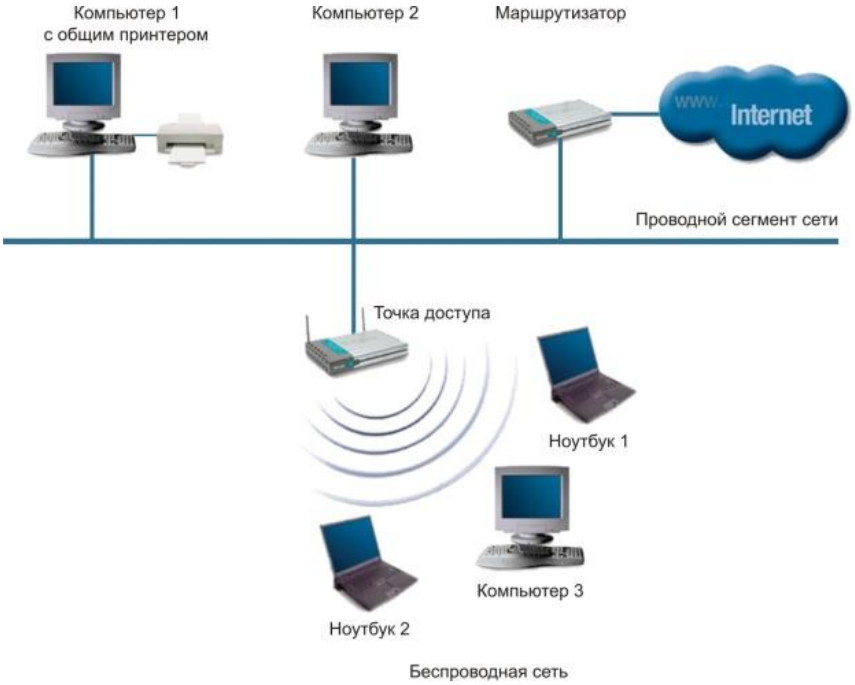


Рисунок 3 – Инфраструктурный режим

Режимы WDS и WDS WITH AP

Термин *WDS* (Wireless Distribution System) расшифровывается как "распределенная беспроводная система". В этом режиме точки доступа соединяются только между собой, образуя мостовое соединение. При этом каждая точка может соединяться с несколькими другими точками. Все точки в этом режиме должны использовать один и тот же канал, поэтому количество точек, участвующих в образовании моста, не должно быть чрезмерно большим. Подключение клиентов осуществляется только по проводной сети через *uplink*-порты точек.

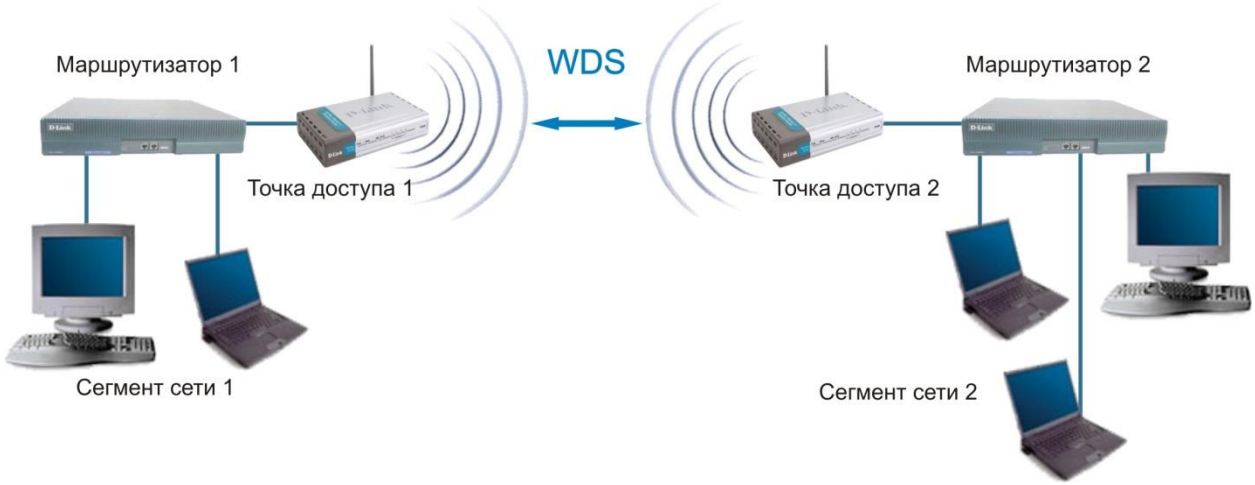


Рисунок 4 – Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов можно объединять проводные LAN, находящиеся как в соседних зданиях, так и на расстоянии до нескольких километров. Это позволяет объединить в сеть филиалы и центральный офис, а также подключать клиентов к сети провайдера Internet.

Беспроводной мост может использоваться там, где прокладка кабеля между зданиями нежелательна или невозможна. Данное решение позволяет достичь значительной экономии средств и обеспечивает простоту настройки и гибкость конфигурации при перемещении офисов.

К точке доступа, работающей в режиме моста, подключение беспроводных клиентов невозможно. Беспроводная связь осуществляется только между парой точек, реализующих мост.

Термин WDS with AP (WDS with Access Point) означает "распределенная беспроводная система, включающая точку доступа", т.е. с помощью этого режима можно не только организовать мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры. Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

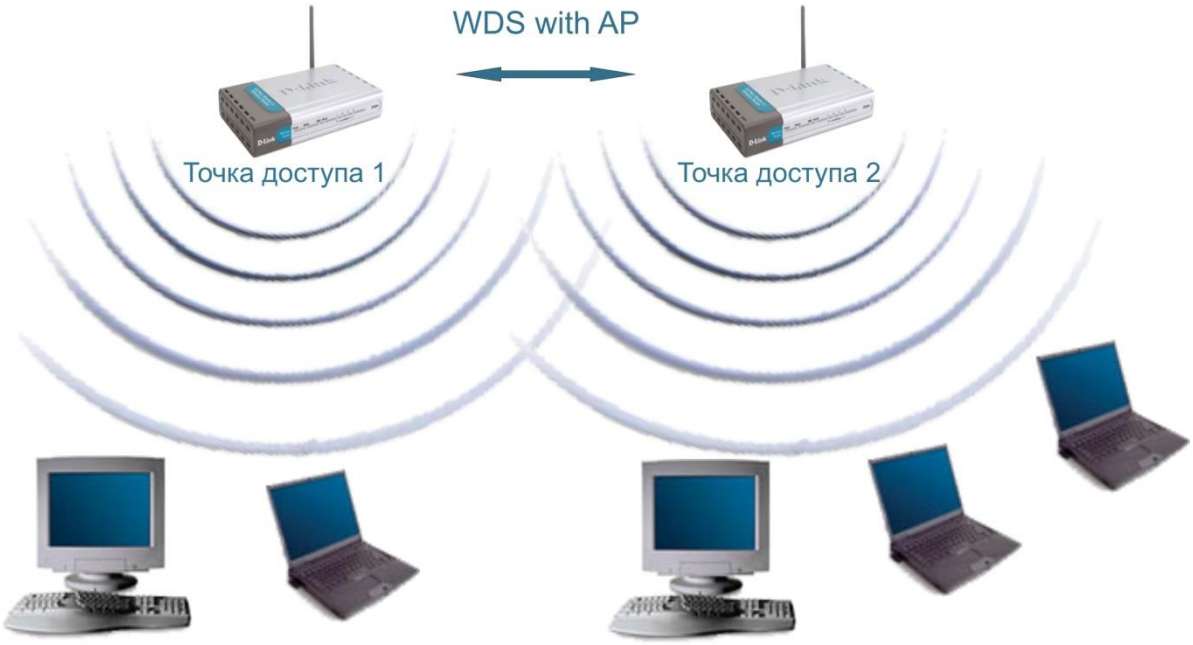


Рисунок 5 – Режим WDS with AP

Тем не менее, необходимо помнить, что все устройства в составе одной *WDS* with AP работают на одной частоте и создают взаимные помехи, что ограничивает количество клиентов до 15-20 узлов. Для увеличения количества подключаемых клиентов можно использовать несколько *WDS*-сетей, настроенных на разные неперекрывающиеся каналы и соединенные проводами через *uplink*-порты.

Топология организации беспроводных сетей в режиме *WDS* аналогична обычным проводным топологиям.

Выполнение работы

Задание 1. Настройка точки доступа беспроводной сети.

1) Подключите точку доступа (Access Point, AP) к компьютеру с помощью патч-корда.
2) На сетевой плате компьютера, с помощью сетевой утилиты netsh укажите IP-адрес - 192.168.0.51 и маску подсети - 255.255.255.0
3) Проверьте связь между компьютером и точкой доступа. Если связь отсутствует, то следует произвести сброс настроек AP путем нажатия кнопки reset (держать около 10 с.)
4) Откройте Internet Explorer и наберите в строке адреса: 192.168.0.50, если web интерфейс не открывается, то необходимо отключить прокси сервер – Свойство обозревателя – Подключения – Настройка сети

Подключение по беспроводной связи к устройству или попытка открытия настроек через любой другой Интернет- браузер не всегда могут быть успешными.

Login: admin
Password: (по умолчанию пароль отсутствует)

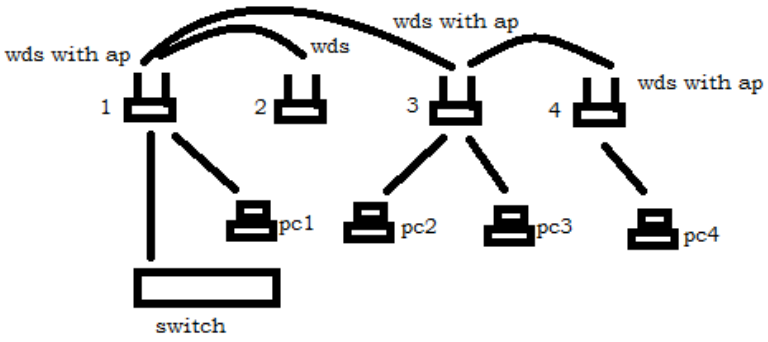
5) На AP устанавливаем ip-адрес 10.1.30.101 - 10.1.30.108 с маской подсети 255.255.255.0.
6) На компьютере с помощью утилиты netsh устанавливаем ip-адреса 10.1.30.201 - 10.1.30.208
7) На AP установить свой логин и пароль для входа на web-интерфейс.
8) Создать на AP сеть по шаблону:

SSID: AP_X, где X номер компьютера.
Канал: X, где X номер компьютера.
Шифрование: Отсутствует.

9) Подключите AP с помощью патч корда, идущего из розетки в ваш компьютер.
10) Подключится к беспроводной сети.
11) Проверить выполненное задание пропинговав все компьютеры в аудитории.
12) На AP выставить тип шифрования WPA-Personal и повторить шаг 11.

Задание 2. Настроить AP в соответствии с одной из схем. С каждого компьютера должен идти пинг на любой другой компьютер, любую точку и интернет сайты. Проверить правильность собранной конфигурации, выполнив указанные действия.

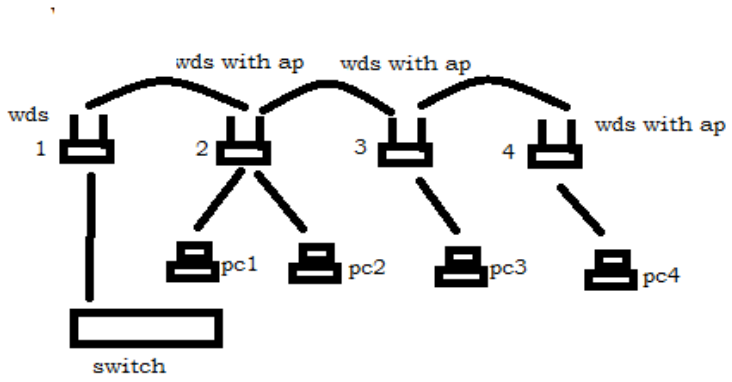
а)



Если отключить первую точку, то пинг перестанет идти с первого компьютера на остальные, вторая точка доступа станет недоступна. Компьютеры 2, 3, 4 пингуются между собой, как и 3 и 4 точки.

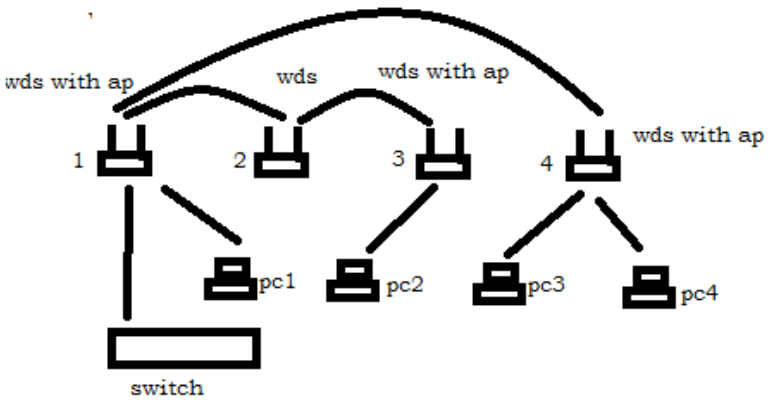
Если отключить 3 точку, то 1 компьютер пропингует свитч, 1 и 2 точки. 2 и 3 компьютеры не увидят остальные элементы. 4 компьютер будет видеть только 4 точку.
Если отключить 4 точку, то 4 компьютер перестанет видеть остальные элементы.

b)



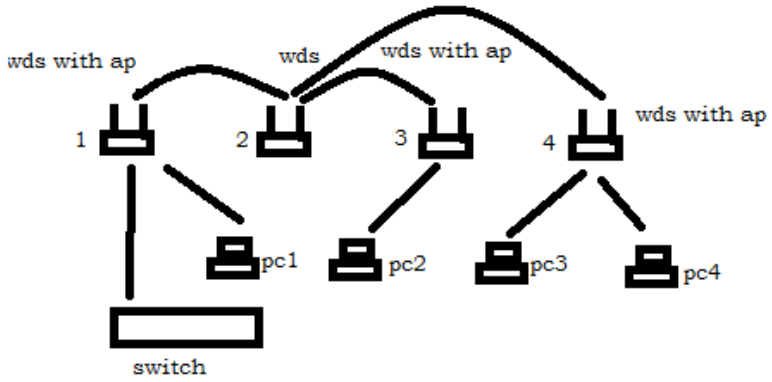
Если отключить 1 точку, пропадет связь со свитчем и интернетом.
Если отключит 2 точку, пропадет связь с первой точкой и первым и вторым компьютерами.
Если отключить 3 точку, то 3 компьютер перестанет видеть основные элементы конфигурации, 4 компьютер увидит только 4 точку, 1 и 2 компьютеры будут видеть 1 и 2 точки с интернетом.

c)



Если отключить 1 точку, то 1 компьютер потеряет связь с остальными элементами. 2 компьютер увидит только 2 и 3 точки, 3 и 4 компьютеры будут пинговать себя и 4 точку.
Если отключить 2 точку, второй компьютер будет пинговать только 3 точку.
При отключении 3 точки, второй компьютер потеряет связь с остальными элементами конфигурации, а 2 точка будет пинговаться с остальных компьютеров.

d)



Если отключить 1 точку, то 1 компьютер потеряет связь с с остальными элементами.
Если отключить 2 точку, пинг перестанет идти со 2 компьютера на остальные и на 4 и 1 точки. 1 компьютер увидит только 1 точку. 3 и 4 компы пропингуют друг друга и 4 точку.
Если отключить 3 точку, то связь прервется между 2 компьютером и остальными элементами.
Если отключить 4 точку, то 3 и 4 комп перестанут видеть остальные элементы, в том числе и друг друга.