Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Системы обработки информации и управления

Отчет по лабораторной работе № 5

«WiFi и ограничение трафика»
по дисциплине «Сети и телекоммуникации»

Студент ИУ5-51Б _____ Е.И. Бирюкова
(Группа) (Подпись, дата) (И.О.Фамилия)

Преподаватель _____ А.И. Антонов
(Подпись, дата) (И.О.Фамилия)

Москва

2024

Цель работы

Закрепление теоретических знаний в области конструирования и исследования беспроводных локальных сетей. Изучение программы Cisco Packet Tracer 8.2, а также приобретение практических навыков проектирования и моделирования работы сети, а также оценки принятых проектных решений. Изучение способов организации сети на точках доступа Linksys.

С помощью программы Cisco Packet Tracer 8.2 необходимо построить модель вычислительной сети заданной топологии. Настроить адресацию, методы защиты и шифрования трафика. Задать сетевой трафик между компьютерами и произвести анализ полученных результатов. Добиться безошибочной работы модели.

С помощью точек доступа построить сеть необходимой конфигурации. Добиться передачи данных через нее.

Задание:

Построить сеть из двух сегментов, каждый из которых состоит из D и E рабочих станций соответственно. Каждый сегмент построен на базе точки доступа WRT300N.

Обе точки доступа подключены к маршрутизатору, к которому, в свою очередь, подключен сервер. Необходимо задать IP адреса сетевым интерфейсам маршрутизаторов, сервера и локальных компьютеров согласно следующей логике:

- Диапазон IP-адресов для первого сегмента:
    - 192.1G.F.x (192.151.3.1) – для локальных компьютеров
    - 10.1G.F.1 (10.151.3.1) – для точки доступа
- Диапазон IP-адресов для второго сегмента:
    - 192.1G.(100+F).x (192.151.103.1) – для рабочих станций
    - 10.1G.(100+F).1 (10.151.103.1) – для точки доступа
- Для маршрутизатора:

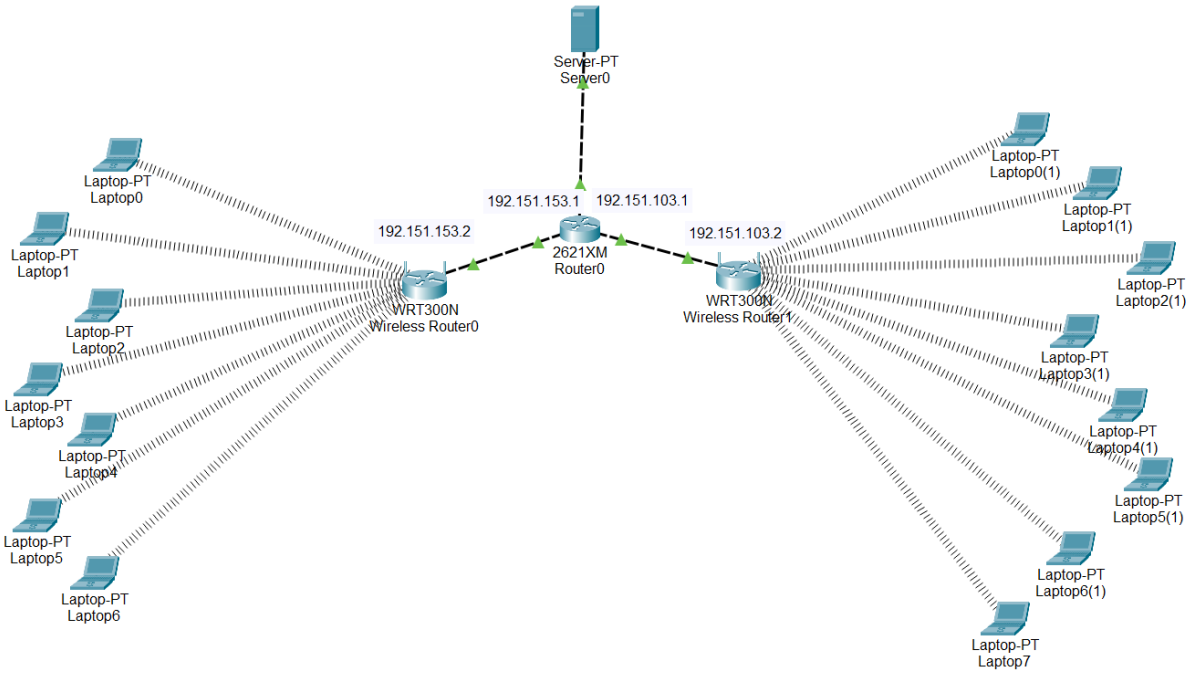
    - 10.1G.(150+F).1 (10.151.153.1)
- Для сервера:
    - 10.1G.(200+F).1 (10.151.203.1)

Первая сеть имеет следующие характеристики: сеть не защищена, идентификатор сети открыт. На точке доступа включена фильтрация Telnet и FTP трафика. Вторая сеть защищена по технологии WPA2-PSK на основе шифрования AES. Идентификатор сети скрыт. На точке доступа включена фильтрация HTTP трафика и включен белый список MAC адресов подключаемых станций. Необходимо добиться возможности пересылки данных по протоколу ICMP между устройствами внутри сетей и сервером.

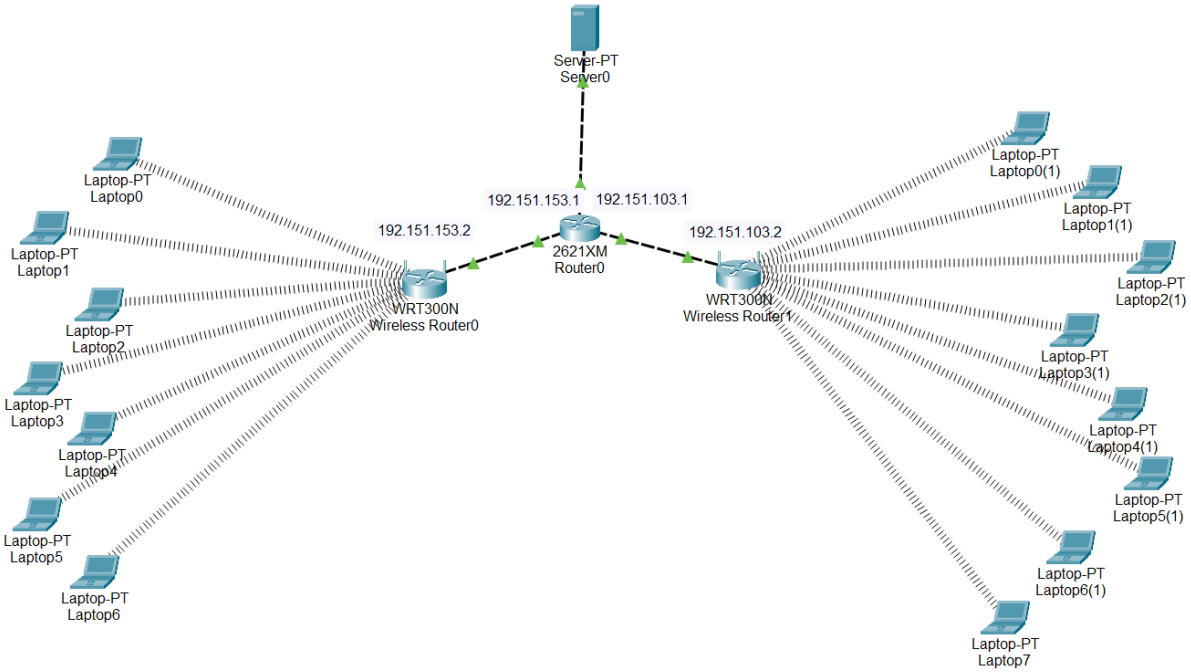
Продемонстрировать невозможность прохождения запрещенного трафика и невозможность подключения станций, не внесенных в белый список.

Ход лабораторной работы

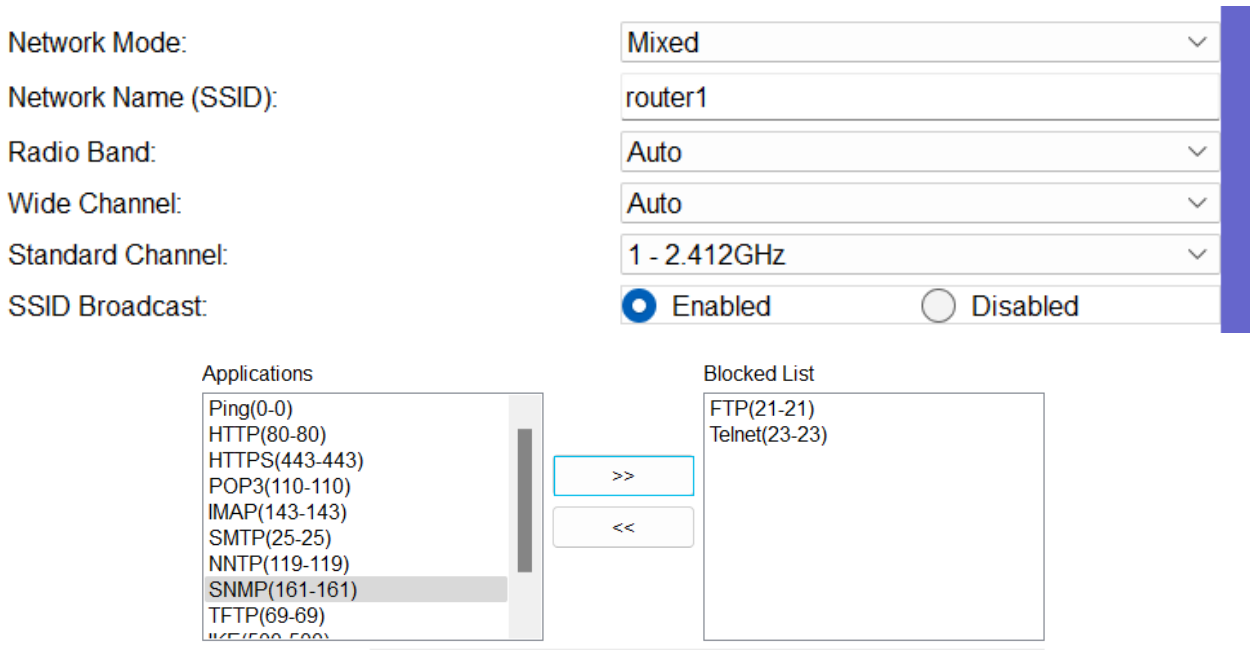
1. Построить сеть из двух сегментов, каждый из которых состоит из 7 и 8 рабочих станций соответственно. Каждый сегмент построен на базе точки доступа WRT300N. Обе точки доступа подключены к маршрутизатору, к которому, в свою очередь, подключен сервер.



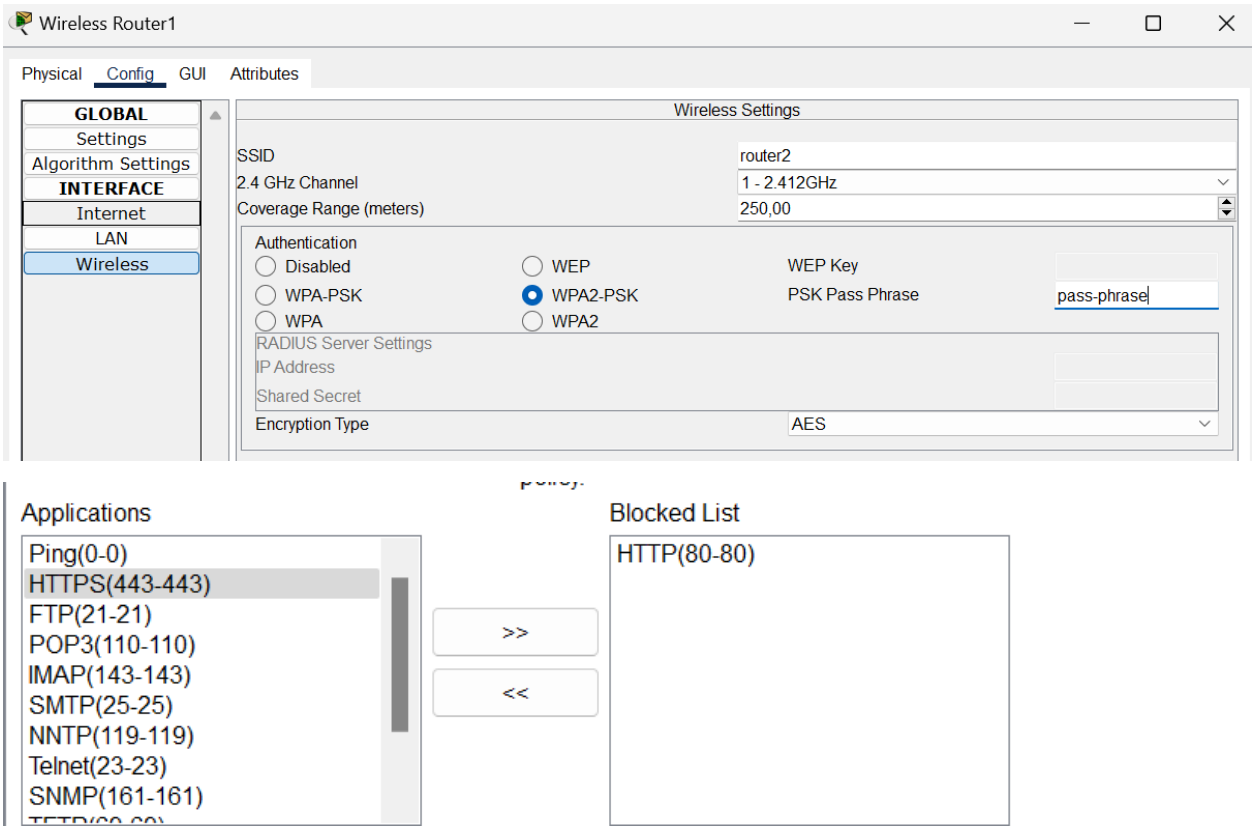
2. Обе точки доступа подключены к маршрутизатору, к которому, в свою очередь, подключен сервер. Необходимо задать IP адреса сетевым интерфейсам маршрутизаторов, сервера и локальных компьютеров согласно следующей логике.

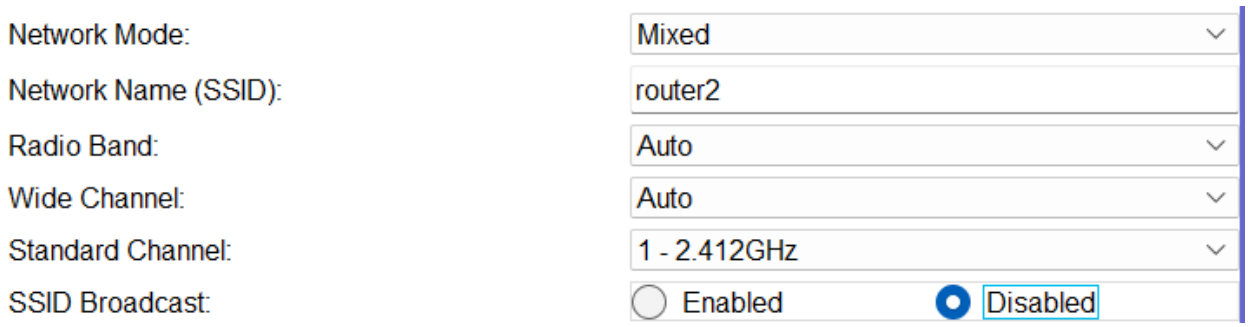


3. Первая сеть имеет следующие характеристики: сеть не защищена, идентификатор сети открыт. На точке доступа включена фильтрация Telnet и FTP трафика.

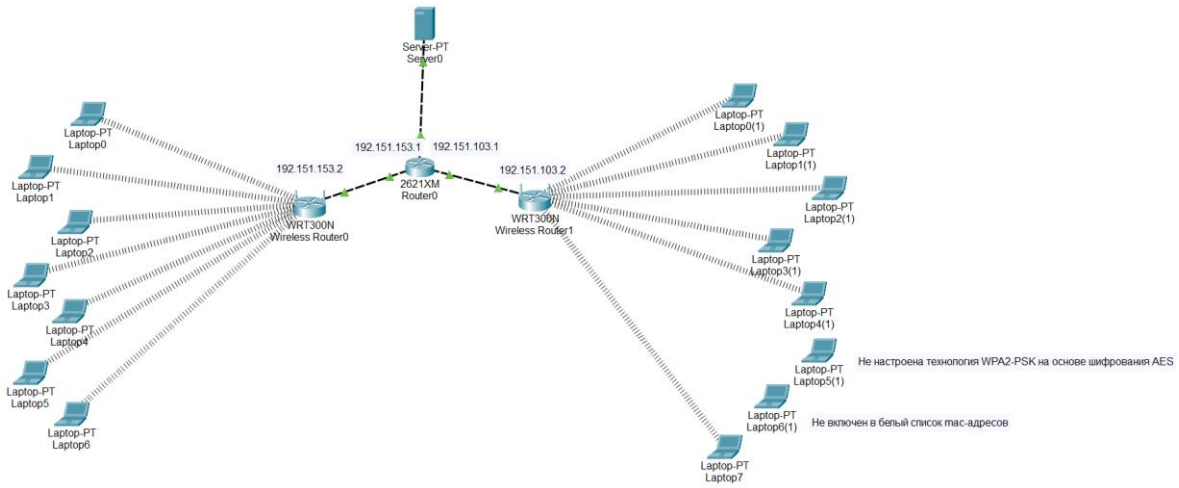


4. Вторая сеть защищена по технологии WPA2-PSK на основе шифрования AES. Идентификатор сети скрыт. На точке доступа включена фильтрация HTTP трафика и включен белый список MAC адресов подключаемых станций. Необходимо добиться возможности пересылки данных по протоколу ICMP между устройствами внутри сетей и сервером.





5. Продемонстрировать невозможность прохождения запрещенного трафика и невозможность подключения станций, не внесенных в белый список.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Laptop0(1)	Server0	ICMP		0.000	N	1	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Laptop5(1)	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	Laptop5(1)	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Failed	Laptop6(1)	Server0	ICMP		0.000	N	2	(edit)	(delete)
	Failed	Laptop6(1)	Server0	ICMP		0.000	N	3	(edit)	(delete)

Контрольные вопросы

1. ***Сети Wi-Fi - основные стандарты и принципы работы.***

Сети Wi-Fi (Wireless Fidelity) — это беспроводные локальные сети, использующие радиоволны для передачи данных между устройствами. Они основаны на стандартах IEEE 802.11, каждый из которых определяет скорость

передачи данных, диапазон частот и другие параметры. Основные стандарты и принципы работы:

Основные стандарты:

- **802.11a:** Работает на частоте 5 ГГц, обеспечивает скорость до 54 Мбит/с. Имеет меньший радиус действия, чем 802.11b/g, но меньше подвержен помехам. Сейчас практически не используется.
- **802.11b:** Работает на частоте 2,4 ГГц, обеспечивает скорость до 11 Мбит/с. Один из первых широко распространенных стандартов. Сейчас устарел.
- **802.11g:** Работает на частоте 2,4 ГГц, обеспечивает скорость до 54 Мбит/с. Совместим с 802.11b. Также устарел, но ещё встречается.
- **802.11n:** Работает на частотах 2,4 ГГц и 5 ГГц (или обеих), использует технологию MIMO (Multiple-Input and Multiple-Output) для увеличения скорости и дальности действия. Обеспечивает скорость до 600 Мбит/с (на практике ниже). Широко распространён.
- **802.11ac:** Работает на частоте 5 ГГц, использует MIMO и более широкий канал связи, обеспечивая скорость до 1,3 Гбит/с (на практике ниже). Более быстрый и менее перегруженный, чем 802.11n на 2,4 ГГц. Широко распространён.
- **802.11ax (Wi-Fi 6):** Работает на частотах 2,4 ГГц и 5 ГГц, использует OFDMA (Orthogonal Frequency-Division Multiple Access) и MU-MIMO (Multi-User MIMO) для повышения эффективности и скорости, особенно в условиях высокой плотности устройств. Обеспечивает скорость до 9,6 Гбит/с (на практике ниже). Становится всё более распространённым.
- **802.11be (Wi-Fi 7):** Новейший стандарт, работающий на более высоких частотах и использующий более совершенные технологии, обеспечивая ещё более высокую скорость передачи данных. Находится на этапе внедрения.

Принципы работы:

- **Радиочастоты:** Wi-Fi использует радиоволны в диапазонах 2,4 ГГц и 5 ГГц (и выше для новых стандартов). 2,4 ГГц имеет большую дальность, но подвержен большему количеству помех (от микроволновок, Bluetooth и др.), 5 ГГц имеет меньшую дальность, но меньше помех.

- **Модуляция:** Для кодирования данных в радиоволны используются различные методы модуляции. Более сложные методы позволяют передавать больше данных за единицу времени.
- **MIMO (Multiple-Input and Multiple-Output):** Эта технология использует несколько антенн как на передающем, так и на принимающем устройствах для увеличения скорости и надежности передачи данных.
- **OFDMA (Orthogonal Frequency-Division Multiple Access) и MU-MIMO (Multi-User MIMO):** Эти технологии, используемые в Wi-Fi 6 и выше, позволяют одновременно передавать данные нескольким устройствам, повышая эффективность сети.
- **Каналы:** Радиодиапазон разделен на каналы, чтобы избежать конфликтов между различными сетями Wi-Fi. Выбор правильного канала важен для обеспечения высокой скорости и стабильности.
- **Аутентификация и шифрование:** Wi-Fi сети используют различные протоколы аутентификации (например, WPA2, WPA3) и шифрования для защиты данных от несанкционированного доступа.
- **Роутеры и точки доступа:** Роутеры и точки доступа являются центральными устройствами в сети Wi-Fi, обеспечивая беспроводной доступ к сети Интернет и другим ресурсам.
- В заключение, Wi-Fi — это сложная технология, которая постоянно развивается, стремясь к большей скорости, дальности действия и эффективности. Понимание основных стандартов и принципов работы поможет вам выбрать оптимальное оборудование и настроить сеть для ваших нужд.

2. Методы доступа к среде в сетях Wi-Fi.

В сетях Wi-Fi используются несколько методов доступа к среде передачи, определяющих, как устройства получают доступ к радиоканалу и передают данные. Основные методы:

- **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance):** Это основной метод доступа к среде в большинстве сетей Wi-Fi, основанных на стандартах 802.11. Он работает по следующему принципу:
    - **Carrier Sense (Прослушивание канала):** Перед передачей данных устройство прослушивает радиоканал, чтобы убедиться, что он свободен.
    - **Multiple Access (Многократный доступ):** Несколько устройств могут пытаться получить доступ к каналу одновременно.
    - **Collision Avoidance (Предотвращение коллизий):** Чтобы избежать коллизий (ситуаций, когда два или более устройств передают данные одновременно, что приводит к потере данных), используется механизм случайного отступа (backoff). Если канал занят, устройство ждет случайное время, прежде чем повторить попытку передачи. Этот механизм помогает уменьшить количество коллизий, но не исключает их полностью.
- **OFDMA (Orthogonal Frequency-Division Multiple Access):** Этот метод доступа используется в стандарте Wi-Fi 6 (802.11ax) и более новых. Он значительно эффективнее CSMA/CA, так как позволяет базовой станции (точке доступа) одновременно передавать данные нескольким устройствам, разделяя канал на ортогональные подканалы. Это позволяет увеличить пропускную способность сети и снизить задержки.
- **MU-MIMO (Multi-User MIMO):** В отличие от OFDMA, который делит частотный спектр, MU-MIMO использует технологию MIMO для одновременной передачи данных нескольким устройствам, используя несколько пространственных потоков. Оба метода (OFDMA и MU-MIMO) могут использоваться вместе для максимальной эффективности.

Сравнение методов:

- **CSMA/CA:** Простой и хорошо работает в сетях с низкой плотностью устройств. Однако, в сетях с высокой плотностью устройств (например, много устройств подключены к одной точке доступа) эффективность CSMA/CA снижается из-за увеличения числа коллизий.
- **OFDMA и MU-MIMO:** Эти методы значительно повышают эффективность сети Wi-Fi в условиях высокой плотности устройств, позволяя одновременно обслуживать большее количество клиентов с меньшими задержками и большей пропускной способностью. Они сложнее в реализации, чем CSMA/CA.

В современных сетях Wi-Fi, особенно в сетях Wi-Fi 6 и выше, используются OFDMA и MU-MIMO для повышения производительности. CSMA/CA, хотя и остается частью стандарта, становится менее важным для обеспечения высокой пропускной способности в условиях высокой плотности подключений. Выбор метода доступа определяется стандартом Wi-Fi и возможностями оборудования.

3. Слот и межкадровый интервал.

1. Слот (Slot)

Определение: Слот — это минимальный временной интервал, в течение которого устройство может начать передачу данных.

Использование: В Wi-Fi устройства слушают канал и, если он свободен, могут начать передачу данных только в начале следующего слота.

Значение: Слот помогает синхронизировать устройства в сети, предотвращая одновременные передачи, которые могут привести к коллизиям.

2. Межкадровый интервал (IFS)

Определение: Межкадровый интервал — это время, которое должно пройти между завершением одной передачи и началом следующей. Он

служит для регулирования порядка передачи и предотвращения коллизий между устройствами.

Типы IFS:

DIFS (Distributed Interframe Space): Основной интервал между кадрами данных в сети.

PIFS (Point Coordination Interframe Space): Используется в точках доступа для управления сетью и организации приоритетной передачи.

SIFS (Short Interframe Space): Кратчайший интервал, используемый для важнейших операций, например, для ответов на кадры управления (ACK).

EIFS (Extended Interframe Space): Применяется в случае ошибок передачи данных (например, при ошибке кадра).

Зачем это нужно:

Слот и IFS помогают координировать действия устройств в сети, чтобы избежать конфликтов при доступе к каналу.

4. Режимы работы сетей Wi-Fi.

1. Инфраструктурный режим

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.

2. Режимы WDS

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.

3. 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.

4. 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.

5. Методы защиты сетей Wi-Fi.

1. Шифрование данных. Шифрование данных помогает предотвратить их перехват и чтение посторонними лицами.
2. Аутентификация пользователей. Для предотвращения несанкционированного доступа, важно правильно настроить аутентификацию.
3. MAC-фильтрация

Принцип: Каждый сетевой адаптер имеет уникальный MAC-адрес. С помощью MAC-фильтрации можно настроить точку доступа так, чтобы разрешать или запрещать подключение только определённым устройствам.

Преимущество: Увеличивает уровень безопасности, так как только устройства с указанными MAC-адресами могут подключаться.

Недостаток: MAC-адрес можно подделать, поэтому этот метод не является абсолютно безопасным.

4. Отключение трансляции SSID

Принцип: SSID (Service Set Identifier) — это имя вашей сети. При отключении трансляции SSID сеть становится невидимой для пользователей, которые не знают её имени.

Преимущество: Скрывает сеть от случайных пользователей.

Недостаток: Сетевые сканеры могут найти скрытую сеть, так что этот метод не даёт полной защиты.

5. Защита с помощью фаервола и NAT

Принцип: Многие маршрутизаторы обеспечивают дополнительную защиту с помощью встроенного фаервола, который контролирует входящий и исходящий трафик, а также использует NAT (Network Address Translation) для скрытия внутренних IP-адресов устройств.

Преимущество: Защищает внутреннюю сеть от внешних атак.

Недостаток: Не предотвращает угрозы внутри сети (например, если злоумышленник уже подключён).

6. Использование VPN

Принцип: VPN (Virtual Private Network) шифрует весь трафик, передаваемый через интернет, и обеспечивает безопасность даже в случае использования открытых или ненадёжных сетей Wi-Fi.

Преимущество: Высокий уровень защиты для передаваемых данных.

Недостаток: Требует дополнительной настройки и ресурсов, как на стороне устройства, так и на сервере VPN.

7. Ограничение доступа по времени

Принцип: В некоторых маршрутизаторах можно настроить ограничения на подключение устройств в определённые временные интервалы.

Преимущество: Обеспечивает дополнительный контроль над доступом, ограничивая использование сети в нерабочие часы.