УДК 004.89

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ В БЕСПРОВОДНЫЕ СЕТИ

Жуматаев Рустем Жумабекович
indira.bukenova11@gmail.com
Студент 3 курса образовательной программы «Информационные системы»
Алматинский технологический университет, г.Алматы, Республика Казахстан
Научный руководитель, м.т.н., лектор – **Букенов Г.С.**

Технология передачи данных в беспроводных сетях является важной отраслью современных коммуникаций и оборудования, обеспечивающей мобильность и гибкость передачи данных в отличие от проводных сетей. Беспроводные сети используют различные типы электромагнитных волн, таких как радиоволны, микроволны и инфракрасные лучи, для передачи данных между устройствами.

Беспроводные сети включает в себя изучение различных типов беспроводных технологий, их преимуществ и недостатков, стандартов и протоколов передачи данных [1]. Это также включает в себя исследование проблем беспроводных сетей, таких как безопасность, шумы и помехи, пропускная способность и масштабируемость. Кроме того, введение в беспроводные сети предполагает изучение методов оптимизации и улучшения производительности беспроводных сетей, включая различные виды мультиплексовции и форм модуляции.

Основная цель работы состоит в том, чтобы предоставить основные знания и основные понятия для понимания и разработки беспроводных систем передачи данных, кроме того, введение в беспроводные сети должно способствовать пониманию последствий использования беспроводных технологий и их влияния на общество и инфраструктуру. В целом, позволяет читателю приобрести необходимые знания для работы в этой области и участвовать в разработке новых методов и технологий для передачи данных.

Материалы и методы. Основная проблема, которую будет решать исследование -это улучшение производительности беспроводных сетей, повышение безопасности, уменьшение помех и шумов, или другие проблемы, связанные с беспроводными сетями.

Сбор данных. Собраны данные, необходимые для тестирования. Это включает экспериментальные данные, данные из литературного обзора, данные полученные из других источников.

Анализ данных. Собранные данные проанализированы. Анализ включает статистический анализ, моделирование и другие методы анализа данных.

Интерпретация результатов. Результаты анализа данных интерпретированы и сделаны выводы относительно гипотезы.

Технологии беспроводных сетей имеют разнообразные приложения и методы, которые позволяют создавать сети для передачи данных без использования проводов. Вот некоторые из основных типов беспроводных сетей:

Беспроводные локальные сети (WLAN): Эти сети позволяют создавать беспроводные соединения в небольших областях, таких как дома, офисы или кафе [2]. Они используют стандарты, такие как Wi-Fi, для обеспечения связи между устройствами.

Беспроводные широкополосные сети (WWAN): WWAN обеспечивает доступ к интернету широкополосным каналом для ноутбуков, планшетных ПК и мобильных устройств. Они работают через мобильные сети связи, такие как 4G или 5G.

Беспроводные метрополитенские сети (WMAN): WMAN предоставляет широкополосный доступ к интернету для крупных областей, таких как города или регионы. Они используют безлинейное оборудование, такое как микроволновые или спутниковые антенны.

Беспроводные глобальные сети (WWGN): Эти сети предоставляют широкополосный доступ к интернету для пользователей в разных странах [3]. Они основаны на спутниковых системах связи, таких как GPS или спутниковое телевидение.

Беспроводные сети для умных домов: Эти сети позволяют устройствам в доме или офисе взаимодействовать между собой через беспроводные соединения. Это может включать в себя умные устройства для управления освещением, отоплением, безопасностью и другими системами.

Беспроводные сети играют ключевую роль в современном мире, обеспечивая удобство и гибкость в подключении к сети в любом месте и в любое время.

Динамическая маршрутизация. OSPF (Open Shortest Path First) - протокол динамической маршрутизации, использующий алгоритм SPF (Shortest Path First) для определения наилучших маршрутов в IP-сетях. Он поддерживает иерархию областей, обмен маршрутной информацией через LSA (Link State Advertisement), безопасность через механизмы аутентификации и поддержку IPv6. OSPF широко используется благодаря эффективности и надежности [4].

Для настройки динамической маршрутизации с OSPF в компьютерной сети, сначала нужно начать с настройки маршрутизаторов под названием AR1 – AR2 – AR3 – AR4
Динамическую маршрутизацию можно увидеть на рисунке 1.

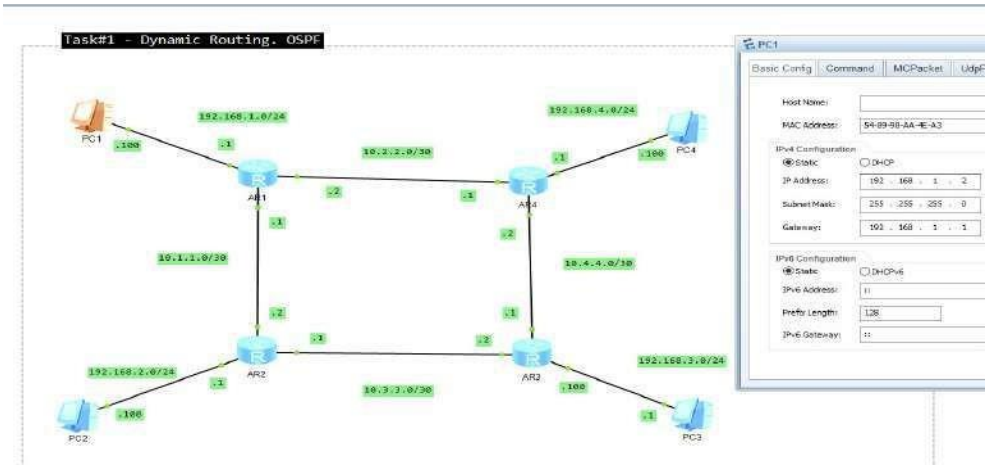

Рисунок 1. Настраивание PC.

Написана общая конфигурация поэтому нужно записать Айпи адрес: 192.168.1.2, маску: 255.255.255.0, и шлюз:192.168.1.1.

Аналогичную конфигурацию мы проводим и с остальными тремя компьютерами.

Далее мы переходим к настройке роутеров. По стандарту через system-view мы задаем имя и для каждого порта(GE 00,01,02) задаем свой айпи (рисунок 2).

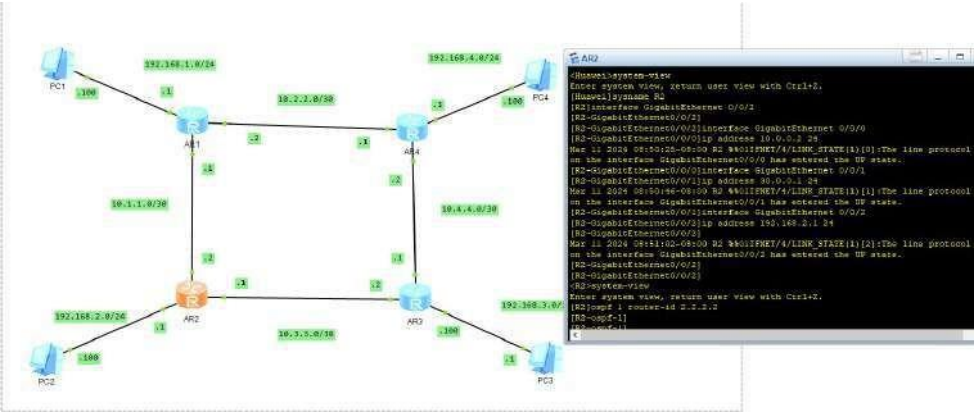

Рисунок 2. Настраивание маршрутизаторов.

Далее мы создаем процесс OSPF, используя команду «ospf-process-id»:

<R1> system-view

[R1] ospf 1 router-id 1.1.1.1[R1-ospf-1]

Далее проводим аналогичную операцию с R2, R3 и R4

Далее мы настраиваем OSPFv2 для одной области OSPF, точнееобласти 0.

[R1-ospf-1] area 0

[R1-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255

[HR1-ospf-1-area-0.0.0.0] network 20.0.0.0 0.0.0.255

[R1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255

С помощью этих команд мы подключаем соединения области 0 дляайпи наших портов.

Остальные 3 роутера настраиваем через те же команды меняя только соединения айпи(IP)

После настройки в задании написано проверить работоспособность пропинговав PC2, PC3 и PC4 через PC1(рисунок 3, 4).

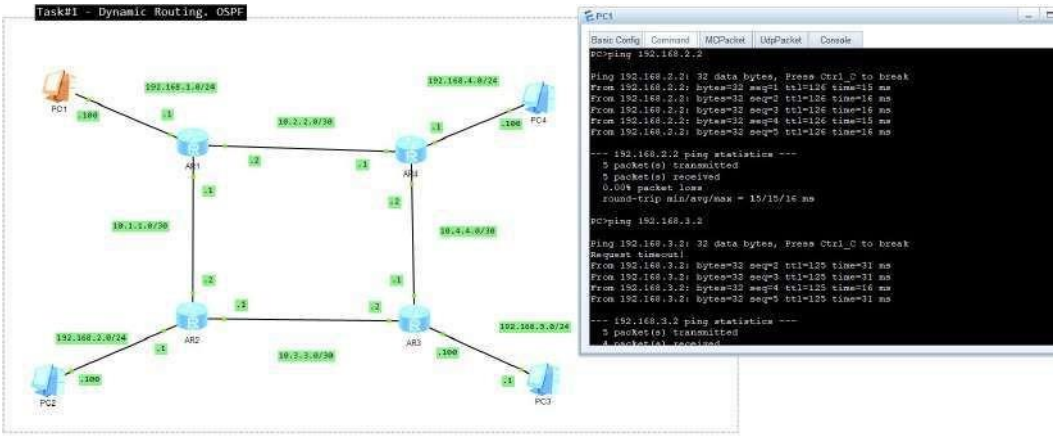

Рисунок 3. С персонального компьютера пингуем на остальные части ПК.

Все это делаем через команды:

ping 192.168.2.2

ping 192.168.3.2

ping 192.168.4.2

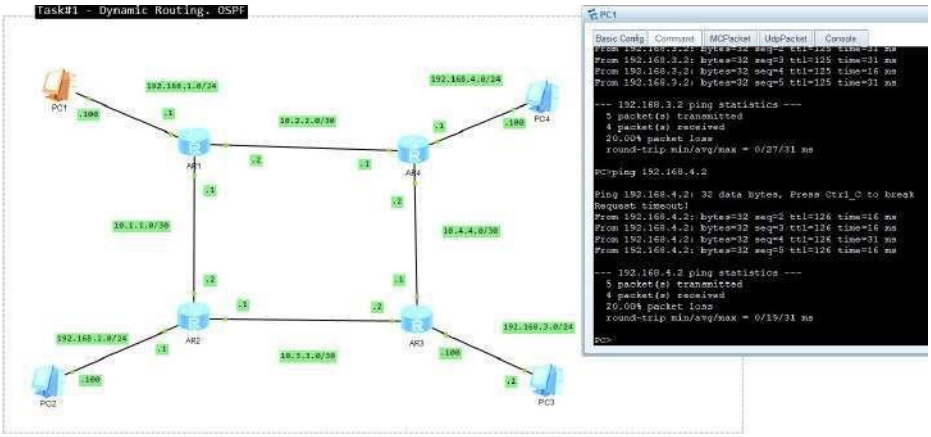

Рисунок 4. С персонального компьютера пингуем на остальные части ПК.

Как видим по всем командам есть обратный отклик значитподключение заработало.

Статическая маршрутизация. Производим стандартную настройку роутеров входим в system-view, меняем имя на R1 через sysname. После переходим к настройке айпи адресов как показано в рисунке 5.

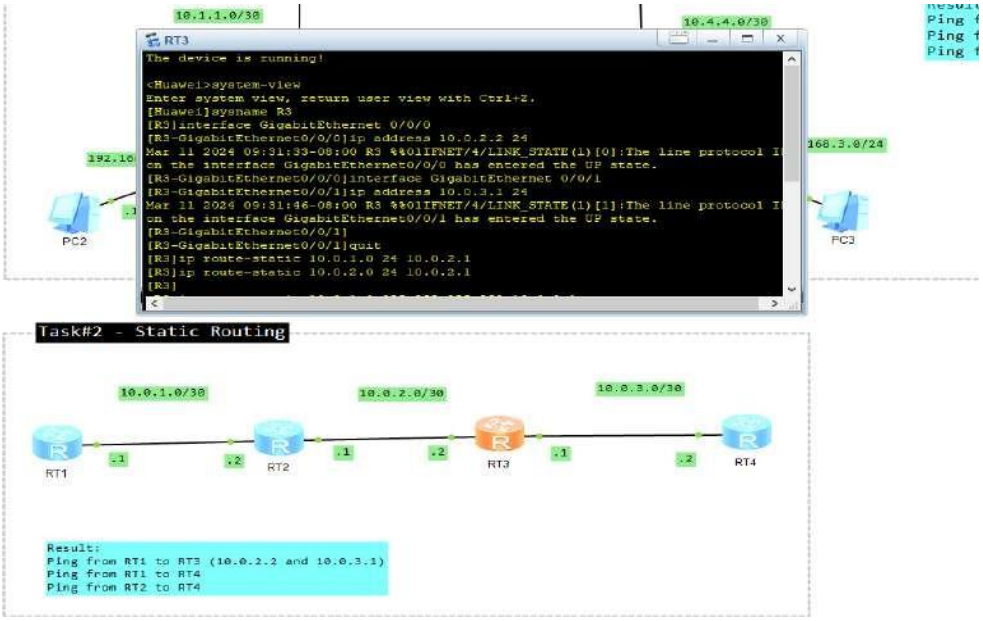

Рисунок 5. Настраивание статический айпи.

Записываем все по условию, пример R3:

interface GigabitEthernet 0/0/0ip address 10.0.2.2/24 interface GigabitEthernet 0/0/1ip address 10.0.3.1/24

Производим аналогичные операции для оставшихся трех роутеров (рисунок 6).

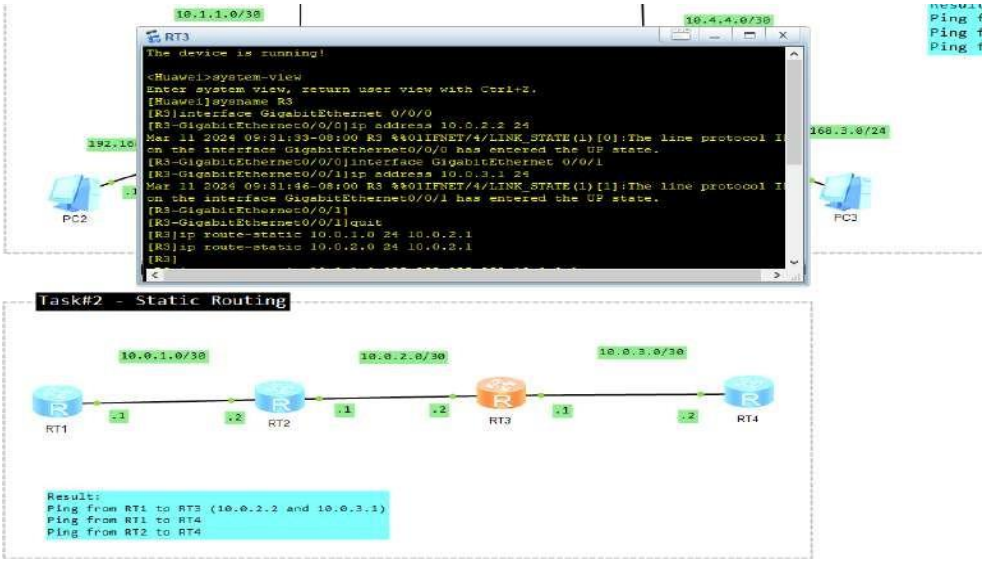

Рисунок 6. Настраивание статический айпи.

Далее мы конфигурируем статические роутеры через: ip route-static 10.0.1.0 255.255.255.252 10.0.2.1

ip route-static 10.0.2.0 255.255.255.252 10.0.2.1

После конфигурации оставшихся трех роутеров производим проверкупо условию Ping from RT1 to RT3 (10.0.2.2 and 10.0.3.1). Это можно увидеть на рисунке 7, 8.

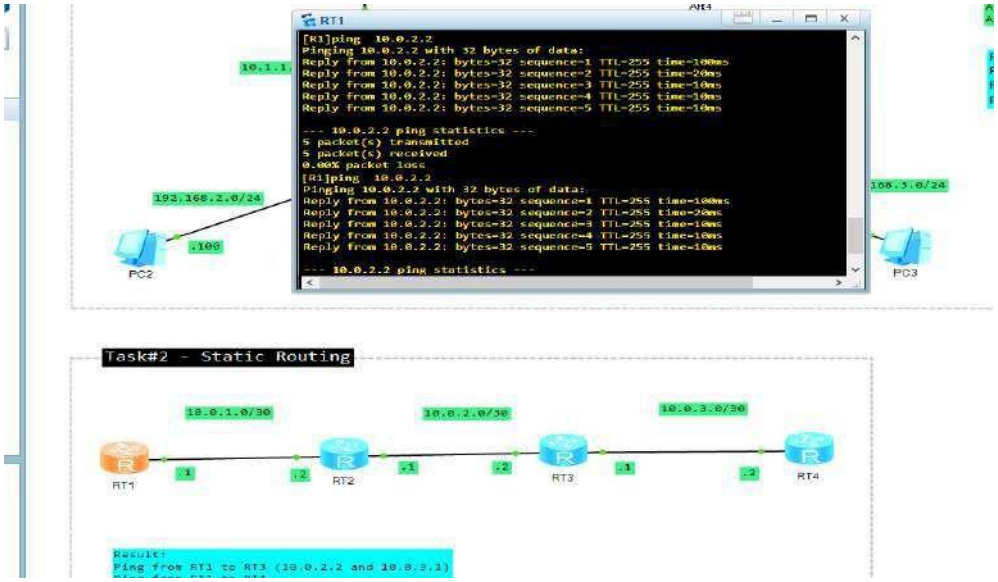

Рисунок 7. Пингуем систему Ping from RT1 to RT4.

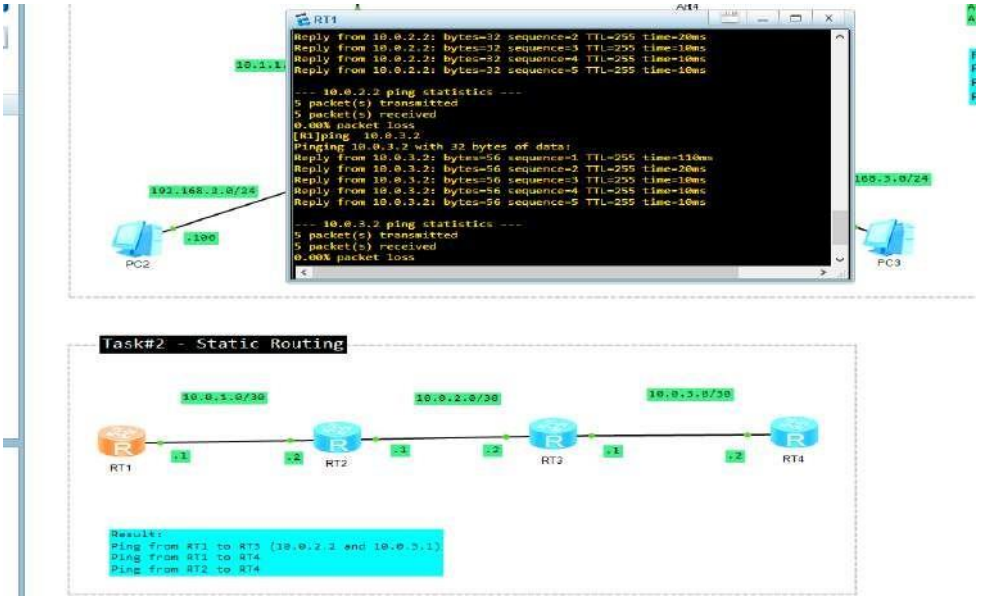

Рисунок 8. Пингуем систему Ping from RT2 to RT4.

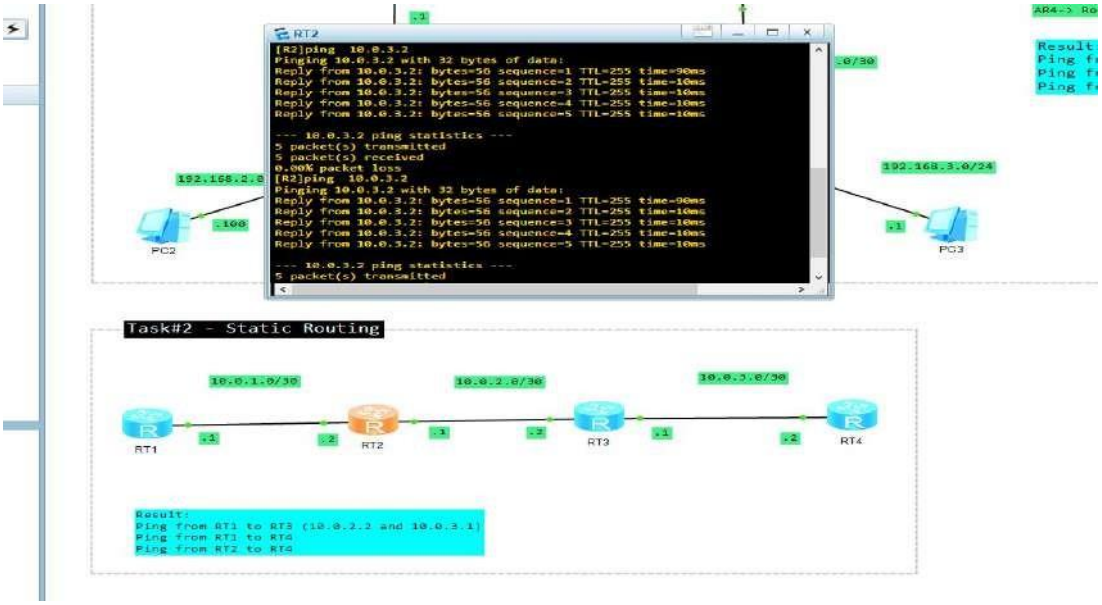

Рисунок 9. Пингуем систему.

Возвратный ответ получен, значит все работает.

Скорости передачи данных. На рисунке 10 можно увидеть виды беспроводных технологий.

Рисунок 10. Виды беспроводных технологий.

Технология беспроводных метрополитенских сетей (WMAN) предоставляет широкополосный доступ в интернет на расстоянии около 50 км и призвана заменить или дополнить проводную инфраструктуру городских коммуникационных сетей, обеспечивая высокоскоростной доступ в интернет и телефонию через "последнюю милю" [5]. Эти сети, такие как WiMAX (стандарты IEEE 802.16), поддерживают различные скорости передачи данных, разделенные на поддиапазоны: SIR, MIR, FIR, VFIR, UFIR.

SIR (Serial Infrared) обеспечивает скорости передачи данных, аналогичные стандарту RS232 (COM-порт), от 9.6 Кбит/с до 115.2 Кбит/с.

MIR (Medium Infrared) поддерживает скорости 0.576 Мбит/с и 1.152 Мбит/с.

FIR (Fast Infrared) включает устаревшие скорости до 4 Мбит/с и современно используемую скорость 4 Мбит/с.

VFIR (Very Fast Infrared) поддерживает скорости до 16 Мбит/с.

UFIR (Ultra Fast Infrared), находящийся в разработке, ожидается поддерживать скорости до 100 Мбит/с.

Технология GPRS (General Packet Radio Service), использующаяся в мобильной связи GSM, предоставляет пакетную передачу данных и позволяет пользователям обмениваться информацией с другими устройствами и внешними сетями, включая интернет [6]. GPRS использует различные кодовые схемы для обеспечения качественной передачи данных в зависимости от качества радиосигнала.

Опишем основные методы разделения доступа к радиоканалу. Использование этих методов доступа в современных протоколах передачи информации по беспроводным каналам связи вызвано необходимостью передавать большие объемы информации за короткий промежуток времени, поддерживать связь с несколькими абонентами в узких диапазонах частот [7].

В современных протоколах передачи данных предусматривается три основных метода разделения доступа устройств связи к радиоканалу — CDMA, FDMA, TDMA. Также существует ряд их модификаций.

CSMA. Carrier Sense Multiple Access (CSMA) — вероятностный сетевой протокол канального (MAC) уровня. Узел, желающий передать пакет данных, выполняет процедуру оценки чистоты канала, то есть в течение заранее заданного времени определяет уровень шума в передающей среде. Если передающая среда оценивается как чистая, узел может передать пакет данных. В противном случае, если выполняется другая передача, узел «отстраняется», то есть,

прежде чем опять предпринять процедуру отправки пакета, узел ждёт определённое время.

На практике более распространена модификация этой технологии — CSMA/CD, предусматривающая контроль коллизий. Существует также технология CSMA/CA, в которой предпринимаются меры по исключению коллизий. На рисунке 11 представлен один кадр для метода доступа устройств в сеть CSMA.

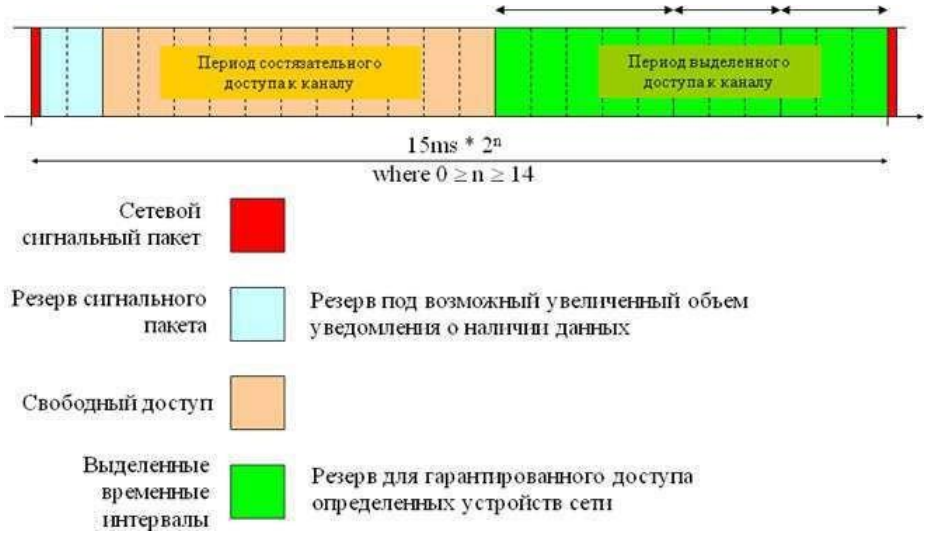

Рисунок 11. Система синхронизации и обеспечения множественного доступа к каналу CSMA.

OFDM. Frequency-division multiplexing — ортогональное частотное разделение каналов с мультиплексированием является цифровой схемой модуляции, которая использует большое количество близко расположенных ортогональных поднесущих. Каждая поднесущая модулируется по обычной схеме модуляции (например, квадратурная амплитудная модуляция) на низкой символьной скорости, сохраняя общую скорость передачи данных, как и у обычных схем модуляции одной несущей в той же полосе пропускания. На практике сигналы OFDM получаются путем использования БПФ (быстрое преобразование Фурье).

Все приведенные методы разделения доступа к каналу применяются в беспроводных сетях с множественным доступом. При этом сети могут иметь разную топологию.

Шифрование является одним из ключевых аспектов технологии передачи данных в беспроводных сетях, поскольку оно обеспечивает конфиденциальность, целостность и аутентификацию данных, передаваемых по беспроводным каналам.

Шифрование в беспроводных сетях может быть реализовано на нескольких уровнях:

- шифрование на прикладном уровне. Шифрование на прикладном уровне выполняется приложениями, которые передают данные по беспроводным сетям. Этот вид шифрования обеспечивает конфиденциальность данных, но не предотвращает атаки на сеть.

- шифрование на транспортном уровне. Шифрование на транспортном уровне выполняется протоколами транспортного уровня, такими как SSL/TLS. Этот вид шифрования обеспечивает конфиденциальность, целостность и аутентификацию данных, но требует дополнительных ресурсов.

- шифрование на сетевом уровне. Шифрование на сетевом уровне выполняется протоколами сетевого уровня, такими как IPsec. Этот вид шифрования обеспечивает конфиденциальность, целостность и аутентификацию данных, а также защищает сеть от атак.

- шифрование на канальном уровне. Шифрование на канальном уровне выполняется протоколами канального уровня, такими как WPA/WPA2. Этот вид шифрования обеспечивает конфиденциальность, целостность и аутентификацию данных, а также защищает беспроводную сеть от не санкционированного доступа в сеть (рисунок 12).

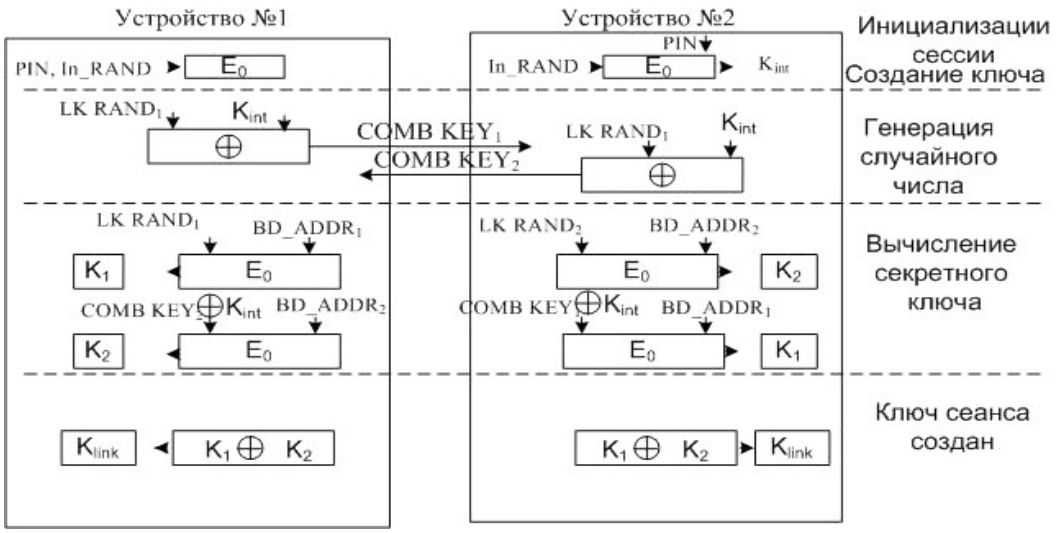

Рисунок 12. Схема соединения двух устройств Bluetooth для генерации общего ключа.

Протокол Bluetooth использует алгоритм потокового шифрования E0, основанный на линейном рекуррентном регистре (ЛРР). Этот алгоритм генерирует ключ потока, который смешивается с открытым текстом через операцию XOR и передается на приемное устройство. Ключ потока формируется с использованием главного идентификатора, случайного числа, номера слота и ключа шифрования. Размер ключа шифрования определяется в ходе установления сеанса между устройствами и может варьироваться от 8 до 128 бит. Протокол SSP включает в себя алгоритм Диффи-Хеллмана на эллиптических кривых для генерации пары безопасных ключей. На данный момент нет эффективных известных атак на алгоритмы Bluetooth, однако возможны реализации программных или аппаратных атак

Результаты и обсуждения. В ходе исследования технологии передачи данных в беспроводных сетях были изучены различные методы и протоколы, используемые для обеспечения безопасности и эффективности передачи данных в беспроводных сетях.

Было установлено, что существует несколько типов беспроводных сетей, таких как беспроводные локальные сети (WLAN), беспроводные широкополосные сети (WWAN), беспроводные метаполитенские сети (WMAN), беспроводные глобальные сети (WWGN) и беспроводные сети смарт-домов. Каждая из этих сетей имеет свои особенности и использование в зависимости от требований к передаче данных.

Было также выявлено, что существует несколько топологий беспроводных сетей, таких как звезда, кольцо, линия, метка, дерево и меш. Каждая топология имеет свои преимущества и недостатки, и выбор топологии зависит от требований к сети.

В ходе исследования было установлено, что шифрование является одним из ключевых аспектов беспроводных сетей, поскольку оно обеспечивает конфиденциальность, целостность и аутентификацию данных, передаваемых по беспроводным каналам. Были изучены различные методы шифрования, такие как шифрование на прикладном уровне, транспортном уровне, сетевом уровне и канальном уровне, и было выявлено, что каждый из этих методов имеет свои преимущества и недостатки.

Выводы. Исследования показывают непрерывное развитие технологий, таких как Wi-Fi, Bluetooth, Zigbee, 5G и других, что приводит к улучшению скорости передачи данных, дальности покрытия и надежности связи.

Благодаря использованию более эффективных методов модуляции, широких каналов и улучшенных алгоритмов управления ресурсами, пропускная способность в беспроводных сетях постоянно растет.

Такие технологии, как OFDM (Orthogonal Frequency Division Multiplexing) и MIMO (Multiple Input Multiple Output), обеспечивают эффективное использование спектра и увеличивают пропускную способность и надежность беспроводных сетей.

Исследования в области управления интерференцией, QoS (Quality of Service), адаптивной модуляции и т. д., способствуют повышению эффективности и стабильности передачи данных в беспроводных сетях.

С развитием технологий шифрования, аутентификации и контроля доступа к сети уровень безопасности беспроводных сетей постоянно повышается, что делает их более защищенными от угроз.

Разработка новых алгоритмов маршрутизации и протоколов управления сетью, таких как маршрутизация на основе контекста или алгоритмы машинного обучения, может улучшить эффективность и адаптивность беспроводных сетей.

Список использованных источников:

1. ISO/IEC 26907 Information technology — Telecommunications and information exchange between systems — High-rate ultra-wideband PHY and MAC standard.

2. IEEE 802.15.4 IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements.

3. Buttyгan L., Czap L., Vajda I. Securing coding based distributed storage in wireless sensor networks // Proceedings of the IEEE Workshop on Wireless and Sensor Network Security (WSNS), Atlanta, USA, 2020.

4. Lima L., Vilela J., Oliveira P., Barros J., Filiz I., Guo X., Morton J., Sturmfels B., Mungan M., Ramasco J. [et al.] Network Coding Security Attacks and Countermeasures. 2019.

5. Jaggi S., Langberg M., Katti S., Ho T., Katabi D., Mredard M. Resilient network coding in the presence of byzantine adversaries // Proceedings of the Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, Alaska, USA, 2021. P. 616-624.

6. Buttyгan Levente, ro Czap Lraszl, Vajda Istvгan. Pollution Attack Defense for Coding Based Sensor Storage Proceedings of the Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, Alaska, USA, 2019.

7. Dong J., Curtmola R., Nita-Rotaru C. Practical defenses against pollution attacks in intra- flow network coding for wireless mesh networks, in WiSec ’09 // Proceedings of the second.