

Архитектура, параметры и организация беспроводных сетей.

Доклад

Юсупова Ксения Равиловна

Содержание

1	Введение	3
2	Архитектура беспроводных сетей	5
2.1	Классификация архитектур беспроводных сетей:	5
2.2	Ключевые компоненты беспроводных сетей:	7
3	Параметры беспроводных сетей	9
3.1	Частотные диапазоны	9
3.2	Стандарты беспроводной связи (IEEE 802.11):	10
3.3	Пропускная способность (Bandwidth)	10
3.4	Дальность связи (Range)	11
3.5	Мощность сигнала (Signal Strength)	11
3.6	Уровень шума (Noise Level)	12
3.7	Отношение сигнал/шум (Signal-to-Noise Ratio, SNR)	12
3.8	Безопасность (Security)	12
4	Организация беспроводных сетей	14
4.1	Планирование сети	14
4.2	Развертывание сети	15
4.3	Управление сетью	15
4.4	Программно-определяемые беспроводные сети (Software-Defined Wireless Networking, SDWN)	16
4.5	Вопросы безопасности	16
5	Новейшие тенденции в беспроводных сетях	17
6	Заключение	19
7	Список литературы	20

1 Введение

В современном цифровом мире беспроводные сети стали неотъемлемой частью нашей повседневной жизни, оказывая глубокое влияние на все сферы деятельности – от личного использования и бизнеса до образования и промышленности. Обеспечивая повсеместный доступ к информации и ресурсам, они трансформировали способы коммуникации, работы и потребления контента. Актуальность изучения архитектуры, параметров и организации беспроводных сетей обусловлена следующими ключевыми факторами:

- Растущая зависимость от беспроводных технологий: Количество беспроводных устройств, подключенных к сети, стремительно увеличивается (Интернет вещей, мобильные устройства, датчики и т.д.), что создает потребность в высокопроизводительных, надежных и безопасных беспроводных решениях.
- Критическая инфраструктура: Беспроводные сети используются в критически важных областях, таких как здравоохранение, транспорт, энергетика и общественная безопасность. Надежность и безопасность этих сетей имеют первостепенное значение.
- Потребность в оптимизации: Оптимизация параметров беспроводных сетей (пропускная способность, дальность связи, энергоэффективность) является важной задачей для повышения производительности, снижения затрат и улучшения пользовательского опыта.
- Постоянное развитие технологий: Беспроводные технологии непрерывно развиваются (Wi-Fi 6/6E/7, 5G, Li-Fi), что требует постоянного обновления знаний и навыков для эффективного использования новых возможностей.
- Проблемы безопасности: Беспроводные сети подвержены различным угрозам безопасности (несанкционированный доступ, перехват тра-

фика, DoS-атаки), что требует разработки и внедрения эффективных механизмов защиты.

В контексте архитектуры компьютера, понимание принципов функционирования беспроводных сетей позволяет разрабатывать более эффективные и интегрированные вычислительные системы, способные использовать преимущества беспроводной связи для расширения функциональности и повышения производительности. Этот доклад представляет собой всестороннее исследование архитектуры, параметров и организации беспроводных сетей, предоставляя необходимую базу знаний для специалистов в области архитектуры компьютера и смежных дисциплин.

2 Архитектура беспроводных сетей

Архитектура беспроводной сети описывает её общую структуру и компоненты, обеспечивающие беспроводную связь. Существуют различные архитектурные модели, каждая из которых подходит для определенных сценариев использования.

2.1 Классификация архитектур беспроводных сетей:

1. Инфраструктурный режим (Infrastructure Mode):

• Описание: В инфраструктурном режиме беспроводные устройства (клиенты) подключаются к центральной точке доступа (Access Point, AP). AP служит мостом между беспроводной и проводной сетью, обеспечивая доступ в Интернет или другие сетевые ресурсы. • Преимущества: * Централизованное управление и безопасность. * Поддержка большего количества устройств и дальности связи. * Оптимизация энергопотребления клиентских устройств. • Недостатки: * Зависимость от AP: отказ AP приводит к отключению всех клиентов. * Необходимость развертывания и обслуживания AP. • Пример: Домашняя Wi-Fi сеть, офисная сеть предприятия.

2. Режим “Точка-точка” (Ad-hoc Mode):

• Описание: В режиме “точка-точка” беспроводные устройства общаются напрямую друг с другом, без использования AP. Каждое устройство функционирует

как клиент и AP одновременно. • Преимущества: * Простая настройка и развертывание. * Не требует наличия инфраструктуры. • Недостатки: * Ограниченная дальность связи. * Сложность масштабирования. * Отсутствие централизованного управления и безопасности. * Более высокое энергопотребление (по сравнению с инфраструктурным режимом). • Пример: Временная сеть для обмена файлами между ноутбуками, соединение двух устройств в полевых условиях.

3. Mesh-сети (Mesh Networks):

• Описание: Mesh-сети представляют собой децентрализованную архитектуру, в которой узлы (nodes) сети связаны друг с другом, образуя ячеистую структуру. Данные передаются от узла к узлу, пока не достигнут назначения. Некоторые узлы могут быть подключены к проводной сети. • Протоколы маршрутизации в Mesh-сетях: Ключевым аспектом Mesh-сетей является выбор протокола маршрутизации, определяющего, как данные передаются от одного узла к другому. Примеры: * AODV (Ad-hoc On-demand Distance Vector Routing): Протокол реактивного маршрутизирования, который создает маршруты только по мере необходимости. * DSDV (Destination-Sequenced Distance-Vector Routing): Протокол проактивного маршрутизирования, который поддерживает таблицу маршрутов для всех узлов в сети. * OLSR (Optimized Link State Routing): Протокол оптимизированного состояния канала, который использует мультиточечную ретрансляцию (MPR) для уменьшения объема передаваемой информации. • Типы Mesh-сетей: * Инфраструктурные Mesh-сети: Некоторые узлы подключены к проводной сети, обеспечивая доступ в Интернет или другие сетевые ресурсы. * Ad-hoc Mesh-сети: Все узлы являются беспроводными и общаются друг с другом без подключения к проводной сети. • Преимущества: * Высокая отказоустойчивость: при отказе одного узла данные могут быть перенаправлены по другим маршрутам. * Расширенная зона покрытия: легко расширяется добавлением новых узлов. * Самовосстановление: сеть динамически адаптируется к изменениям топологии. • Недостатки: * Более сложная настройка и управление. * Потенциальные задержки из-за многошаговой передачи данных. * Более высокая стоимость оборудования (обычно).

* Проблемы масштабируемости: С ростом числа узлов в Mesh-сети сложность маршрутизации и управления возрастает. Необходимы эффективные алгоритмы и протоколы для обеспечения масштабируемости. • Пример: Беспроводные сети в масштабе города, сети для мониторинга окружающей среды, системы “умный дом”.

4. Беспроводные сети персональной зоны (Wireless Personal Area Networks, WPAN):

• Описание: WPAN используются для связи на небольших расстояниях (обычно до 10 метров) между устройствами, принадлежащими одному пользователю. • Примеры технологий: Bluetooth, Zigbee, Z-Wave. • Применение: Подключение наушников, мышей, клавиатур, фитнес-трекеров, устройств “умного дома”.

5. Беспроводные сенсорные сети (Wireless Sensor Networks, WSN):

• Описание: Специализированный тип беспроводных сетей, состоящий из большого количества небольших, недорогих сенсорных узлов. Эти узлы собирают данные об окружающей среде (температура, влажность, давление и т.д.) и передают их на центральный узел или шлюз. • Применение: Мониторинг окружающей среды, сельское хозяйство, здравоохранение, промышленность. • Особенности: Ограниченные ресурсы (энергия, вычислительная мощность, память), строгие требования к энергоэффективности. • Протоколы: Zigbee, IEEE 802.15.4, LoRaWAN.

2.2 Ключевые компоненты беспроводных сетей:

• Беспроводные адаптеры (Wireless Adapters): Устройства, позволяющие компьютерам и другим устройствам подключаться к беспроводной сети (например, Wi-Fi адаптер в ноутбуке). • Точки доступа (Access Points, AP): Устройства, обеспечивающие доступ беспроводных клиентов к проводной сети. AP выполняют

функции моста между беспроводным и проводным сегментами сети. • Беспроводные маршрутизаторы (Wireless Routers): Устройства, объединяющие в себе функции маршрутизатора и точки доступа. Они управляют трафиком между различными сетями (например, домашней сетью и Интернетом) и обеспечивают беспроводной доступ для клиентских устройств. • Антенны (Antennas): Устройства, излучающие и принимающие радиоволны. Различные типы антенн (например, всенаправленные и направленные) используются для оптимизации покрытия и производительности сети.

3 Параметры беспроводных сетей

Производительность и функциональность беспроводной сети определяются рядом ключевых параметров.

3.1 Частотные диапазоны

- 2.4 ГГц: Широко используемый диапазон, предлагающий хорошее покрытие, но подверженный интерференции от других устройств (микроволновые печи, Bluetooth-устройства). Используется в стандартах 802.11b/g/n.
- 5 ГГц: Менее загруженный диапазон, предлагающий более высокую скорость передачи данных и меньшую подверженность интерференции. Используется в стандартах 802.11a/n/ac/ax.
- 6 ГГц (Wi-Fi 6E): Новейший диапазон, обеспечивающий еще большую пропускную способность и меньшую интерференцию. Требуется поддержки Wi-Fi 6E со стороны устройств и AP.
- Спектральная эффективность: Мера того, насколько эффективно используется доступный частотный спектр. Более высокая спектральная эффективность позволяет передавать больше данных при той же ширине полосы.
- Регулирование: Использование частотных диапазонов регулируется национальными и международными организациями (например, FCC в США, ETSI в Европе). Разные страны могут иметь разные правила и ограничения.
- Динамическое частотное распределение (DFS): Механизм, позволяющий беспроводным устройствам избегать использования частот, занятых другими службами (например, радары).

3.2 Стандарты беспроводной связи (IEEE 802.11):

- 802.11b: Старый стандарт, обеспечивающий скорость до 11 Мбит/с.
- 802.11g: Более быстрый стандарт, обеспечивающий скорость до 54 Мбит/с.
- 802.11a: Стандарт, работающий в диапазоне 5 ГГц, обеспечивающий скорость до 54 Мбит/с.
- 802.11n (Wi-Fi 4): Использует технологии MIMO (Multiple-Input Multiple-Output) для повышения скорости и дальности связи. Обеспечивает скорость до 600 Мбит/с (в теории).
- 802.11ac (Wi-Fi 5): Улучшенный стандарт, использующий более широкие каналы и более эффективную модуляцию для достижения скорости до нескольких гигабит в секунду.
- 802.11ax (Wi-Fi 6/6E): Новейший стандарт, разработанный для повышения эффективности и производительности в условиях высокой плотности устройств. Использует технологии OFDMA (Orthogonal Frequency-Division Multiple Access) и MU-MIMO (Multi-User MIMO) для одновременного обслуживания большего количества клиентов.
- MIMO (Multiple-Input Multiple-Output): Технология, использующая несколько антенн на передатчике и приемнике для повышения пропускной способности и дальности связи. Различают SU-MIMO (Single-User MIMO) и MU-MIMO (Multi-User MIMO).
- OFDM (Orthogonal Frequency-Division Multiplexing): Технология, разбивающая канал на множество поднесущих частот, что позволяет уменьшить влияние многолучевого распространения сигнала.
- OFDMA (Orthogonal Frequency-Division Multiple Access): Расширение OFDM, позволяющее одновременно обслуживать несколько пользователей, выделяя им различные поднесущие частоты.
- Target Wake Time (TWT): Механизм, позволяющий устройствам договариваться с точкой доступа о времени пробуждения для передачи данных, что позволяет существенно снизить энергопотребление.

3.3 Пропускная способность (Bandwidth)

- Максимальная скорость передачи данных в беспроводной сети. Зависит от используемого стандарта, частотного диапазона, ширины канала и других факто-

ров. • Агрегация кадров: Механизм, позволяющий объединять несколько небольших кадров в один большой кадр для уменьшения накладных расходов и повышения пропускной способности. • Протоколы качества обслуживания (QoS): Механизмы, позволяющие приоритизировать трафик в беспроводной сети для обеспечения гарантированной пропускной способности и задержки для критически важных приложений (например, VoIP, видеоконференции). Примеры: WMM (Wi-Fi Multimedia).

3.4 Дальность связи (Range)

• Максимальное расстояние, на котором беспроводное устройство может поддерживать надежное соединение с точкой доступа. Зависит от мощности передатчика, чувствительности приемника, используемого стандарта, типа антенны и наличия препятствий. • **Влияние окружающей среды на дальность связи:** * **Затухание сигнала:** Сила сигнала уменьшается с увеличением расстояния от передатчика. * **Отражение:** Сигнал отражается от объектов (стены, мебель и т.д.), что может приводить к многолучевому распространению и интерференции. * **Поглощение:** Сигнал поглощается материалами (вода, бетон и т.д.), что также приводит к уменьшению силы сигнала. * **Дифракция:** Сигнал огибает препятствия, но при этом теряет часть своей энергии.

3.5 Мощность сигнала (Signal Strength)

• Измеряется в dBm (децибел-милливатт). Более высокое значение указывает на более сильный сигнал и более надежное соединение.

3.6 Уровень шума (Noise Level)

- Измеряется в dBm. Более низкое значение указывает на меньшее количество помех и более чистый сигнал.

3.7 Отношение сигнал/шум (Signal-to-Noise Ratio, SNR)

- Разница между мощностью сигнала и уровнем шума. Более высокое значение SNR указывает на более надежное соединение.

3.8 Безопасность (Security)

- **WEP (Wired Equivalent Privacy):** Устаревший и небезопасный протокол шифрования. Не рекомендуется к использованию.
- **WPA (Wi-Fi Protected Access):** Более безопасный протокол, использующий TKIP (Temporal Key Integrity Protocol) для шифрования данных.
- **WPA2 (Wi-Fi Protected Access 2):** Использует более надежный алгоритм шифрования AES (Advanced Encryption Standard) и является рекомендуемым протоколом для защиты беспроводных сетей.
- **WPA3 (Wi-Fi Protected Access 3):** Новейший стандарт безопасности, предлагающий улучшенные функции защиты, такие как SAE (Simultaneous Authentication of Equals) для защиты от атак методом подбора пароля.
- **802.1X Authentication:** Протокол аутентификации, использующий сервер RADIUS (Remote Authentication Dial-In User Service) для проверки подлинности пользователей. Обеспечивает более высокий уровень безопасности, чем аутентификация на основе PSK (Pre-Shared Key).
- **Wi-Fi Protected Setup (WPS):** Упрощенный метод настройки безопасности беспроводной сети, но подверженный уязвимостям. Рекомендуется отключать WPS.
- **Скрытый SSID:** Скрытие SSID (Service Set Identifier) не является эффективной мерой безопасности, так как SSID может быть обнаружен с помощью анализа беспроводного трафика.
- **Мониторинг беспроводного трафика:** Использование инструментов для мониторинга беспроводного трафика позволяет обнаруживать

несанкционированный доступ и другие подозрительные действия. • **WIDS/WIPS (Wireless Intrusion Detection System/Wireless Intrusion Prevention System):** Системы обнаружения и предотвращения вторжений в беспроводную сеть.

4 Организация беспроводных сетей

Организация беспроводной сети включает в себя планирование, развертывание, настройку и управление сетью для обеспечения оптимальной производительности, безопасности и надежности.

4.1 Планирование сети

- **Определение потребностей:** Определение количества пользователей, требуемой пропускной способности, зоны покрытия и других требований к сети.
- **Выбор оборудования:** Выбор точек доступа, маршрутизаторов, антенн и других компонентов сети, соответствующих определенным требованиям.
- **Обследование радиочастотного спектра (Site Survey):** Проведение анализа радиочастотного спектра для выявления источников интерференции и определения оптимальных мест размещения точек доступа.
- **Инструменты для обследования радиочастотного спектра (Site Survey):**
 - * Программные инструменты: NetSpot, Ekahau HeatMapper, VisiWave Site Survey.
 - * Аппаратные инструменты: Спектроанализаторы.
 - * Параметры, измеряемые во время обследования: Уровень сигнала, уровень шума, отношение сигнал/шум (SNR), интерференция.
- **Цель обследования:** Определение оптимального размещения точек доступа, выбор каналов, настройка мощности передатчика.
- **Проектирование топологии сети:** Разработка плана размещения точек доступа и организации сетевых соединений для обеспечения оптимального покрытия и производительности.

4.2 Развертывание сети

- **Установка оборудования:** Установка и настройка точек доступа, маршрутизаторов и других компонентов сети.
- **Настройка параметров сети:** Настройка SSID (Service Set Identifier), каналов, режимов безопасности и других параметров сети.
- **Тестирование сети:** Проверка покрытия, пропускной способности и безопасности сети.

4.3 Управление сетью

- **Мониторинг производительности:** Мониторинг использования пропускной способности, уровня сигнала, количества подключенных клиентов и других параметров сети.
- **Устранение неисправностей:** Выявление и устранение проблем, связанных с производительностью, безопасностью и надежностью сети.
- **Обновление программного обеспечения:** Регулярное обновление программного обеспечения точек доступа, маршрутизаторов и других компонентов сети для исправления ошибок и улучшения безопасности.
- **Управление доступом:** Настройка прав доступа для различных пользователей и групп пользователей.
- **Оптимизация сети:** Регулярная оптимизация параметров сети для улучшения производительности и эффективности.
- **Управление радиоресурсами (Radio Resource Management, RRM):**
 - * **Автоматический выбор канала (Automatic Channel Selection, ACS):** Механизм, позволяющий точкам доступа автоматически выбирать наименее загруженный канал.
 - * **Управление мощностью передатчика:** Регулировка мощности передатчика точек доступа для оптимизации покрытия и уменьшения интерференции.
 - * **Балансировка нагрузки (Load Balancing):** Перенаправление клиентов на менее загруженные точки доступа для повышения производительности сети.

4.4 Программно-определяемые беспроводные сети (Software-Defined Wireless Networking, SDWN)

• **Описание:** Архитектура, позволяющая централизованно управлять беспроводной сетью с помощью программного контроллера. • **Преимущества:** Гибкость, масштабируемость, автоматизация, возможность внедрения новых функций и услуг.

4.5 Вопросы безопасности

• **Использование сильных паролей:** Использование сложных и уникальных паролей для защиты доступа к сети и оборудованию. • **Включение шифрования:** Использование WPA2 или WPA3 для шифрования беспроводного трафика. • **Фильтрация MAC-адресов:** Ограничение доступа к сети только для зарегистрированных устройств. • **Гостевая сеть (Guest Network):** Предоставление доступа к сети для гостей с использованием отдельной сети с ограниченными правами доступа. • **Регулярные проверки безопасности:** Проведение регулярных проверок безопасности сети для выявления и устранения уязвимостей.

5 Новейшие тенденции в беспроводных сетях

• **Wi-Fi 6/6E (802.11ax):** Разработан для повышения эффективности и производительности в условиях высокой плотности устройств. Использует технологии OFDMA и MU-MIMO для одновременного обслуживания большего количества клиентов. • **Wi-Fi 7 (802.11be):** Следующее поколение Wi-Fi, обещающее еще более высокую скорость передачи данных и меньшие задержки. Будет использовать более широкие каналы, более высокую модуляцию и новые технологии для улучшения производительности. • **6 GHz Spectrum:** Открытие 6 ГГц спектра для нелицензируемого использования позволило расширить возможности Wi-Fi и снизить перегрузку сети. • **Open Roaming:** Инициатива, направленная на упрощение подключения к Wi-Fi сетям в общественных местах. • **Беспроводные сети 5G:** Развертывание сетей 5G предоставляет альтернативный способ доступа к интернету с высокой скоростью и низкой задержкой. 5G также используется для построения частных беспроводных сетей для промышленных предприятий. • **IoT и беспроводные сети:** Интернет вещей (IoT) приводит к увеличению количества беспроводных устройств, требующих подключения к сети. Разрабатываются новые технологии и протоколы для поддержки IoT устройств с низким энергопотреблением и ограниченной пропускной способностью. • **Wi-Fi Sensing:** Использование Wi-Fi сигналов для обнаружения движения, определения местоположения и других приложений. • **Li-Fi (Light Fidelity):** Использование видимого света для передачи данных. Обладает потенциалом для более высокой скоро-

сти и безопасности, чем Wi-Fi. • **Terahertz (THz) Communication:** Использование терагерцового излучения для сверхвысокоскоростной беспроводной связи. Находится на стадии исследований и разработок. • **Edge Computing в беспроводных сетях:** Обработка данных ближе к источнику (на краю сети) позволяет уменьшить задержки и повысить производительность приложений, требующих низкой задержки (например, AR/VR).

6 Заключение

Беспроводные сети продолжают играть все более важную роль в современной вычислительной инфраструктуре. Этот доклад предоставил углубленный анализ архитектуры, параметров и организации беспроводных сетей, охватывая как фундаментальные принципы, так и передовые технологии. Понимание этих аспектов необходимо для разработки эффективных, безопасных и масштабируемых беспроводных решений. По мере развития технологий, беспроводные сети будут продолжать преобразовывать способы взаимодействия с информацией и окружающим миром. Непрерывное изучение и адаптация к новым тенденциям позволит вам оставаться на передовой в этой динамичной области.

7 Список литературы

1. <https://www.wi-fi.org/>
2. <https://www.cisco.com/c/en/us/products/wireless/index.html>
3. <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/wifi/wifi-overview>
4. <https://www.coursera.org/learn/computernetworks>
5. Таненбаум Э., Уэзеролл Д. “Компьютерные сети”
6. Олифер В.Г., Олифер Н.А. “Компьютерные сети. Принципы, технологии, протоколы”