Билеты для экзамена по M2M
Автор конспекта - Мячин Данил

Содержание

1. Билет 1

1.1. Понятие протокола. Понятие архитектуры сети. Эталонная модель TCP/IP

1.1.1. Из расписки билетов

Протокол передачи данных — набор соглашений интерфейса логического уровня, которые определяют обмен данными между различными программным и аппаратным обеспечением. Под архитектурой сети обычно подразумевается схема взаимодействия сетевых и конечных устройств между собой и с внешним миром. Модель TCP/IP является основной моделью на которой построен Интернет включает в себя 4 уровня - канальный (физический и канальный из классической модели OSI, сетевой (Используется протокол IP), транспортный (Используется протокол TCP), а также уровень приложения, все остальные уровни опущены. Зачастую TCP/IP называют стеком протоколов.

1.1.2. Попытка нарыть самому

1.1.2.1. Протокол. Лично моё понимание - **протокол это способ согласовать как данные выглядят** t.

Пример: в школьном журнале учителя ведут не запись построчную вида "Поставил ученику А оценку Б дата В а есть таблица, размером (количество учеников × количество уроков), где учитель в нужной ячейке заполняет оценку ученика. Это конкретно определённый протокол для оценок.

Ещё пример: на пропускных пунктах такое было бы делать неудобно - людей очень много. Вот там протокол такой, что в каждой строке пишется кто когда пришёл, ушёл, кто пустил, номер пропуска за день итд.

Если брать очень упрощённую модель - вы можете сказать, что для передачи чисел с устройства на другое могут быть такие протоколы:

- Каждую секунду по кабелю подаётся ток, где подача напряжения соответствует биту 1, отсутствие биту 0. Каждые 8 секунд мы можем прочитать одно беззнаковое двоичное число.
- Каждую секунду по кабелю подаётся ток, где подача напряжения соответствует биту 1, отсутствие биту 0. Каждые 16 секунд мы можем прочитать одно беззнаковое двоичное число.

Интерфейс тут один и тот же - провод. Но вот протоколы различны, и если устройства используют разные протоколы, то в итоге получим фигню.

Протокол - это соглашение о том, как устройства должны обмениваться данными. В компьютерных сетях, протокол определяет формат данных и правила их передачи между устройствами. Кроме того, протокол может также включать правила для обработки ошибок и механизмы управления доступом к ресурсам.

Примерами протоколов в компьютерных сетях могут быть: TCP/IP, HTTP, FTP, SMTP и другие. Каждый из этих протоколов определяет, как данные должны быть структурированы, как они передаются между устройствами и какие действия должны быть предприняты, если возникают проблемы с передачей данных.

Протоколы используются для обмена информацией не только в компьютерных сетях, но и в других областях, таких как телекоммуникации, транспорт, электронная коммерция и многие другие. Они позволяют различным устройствам и системам работать вместе и обмениваться информацией, несмотря на различия в их аппаратном и программном обеспечении.

1.1.2.2. Архитектура сети. Архитектура сети - это концептуальное представление о том, как устройства и компоненты сети связаны и как они взаимодействуют друг с другом. Она включает в себя физическую структуру сети, протоколы, используемые для обмена данными, и правила, которым должны следовать устройства, чтобы обеспечить эффективную и безопасную передачу данных.

Одним из ключевых элементов архитектуры сети является физическая топология - описание физических связей между устройствами в сети. Это может быть дерево, кольцо, звезда, сетка или другая конфигурация, которая определяет, как устройства связаны друг с другом.

Другим важным аспектом архитектуры сети являются протоколы, которые используются для передачи данных между устройствами в сети. Протоколы определяют, как данные структурированы, как они передаются между устройствами, как обрабатываются ошибки и какие механизмы используются для управления доступом к ресурсам.

Также в архитектуру сети входят устройства, которые составляют сеть, такие как маршрутизаторы, коммутаторы, хабы, серверы, клиентские устройства и другие. Важно, чтобы эти устройства были совместимы и могли взаимодействовать друг с другом, чтобы обеспечить эффективную и безопасную передачу данных.

Наконец, архитектура сети включает в себя правила, которые определяют, как устройства в сети должны взаимодействовать друг с другом. Эти правила могут включать в себя правила безопасности, механизмы управления доступом к ресурсам и другие параметры, которые должны быть определены и настроены для обеспечения правильной работы сети.

Таким образом, архитектура сети - это основополагающий элемент любой компьютерной сети, который определяет, как устройства связаны друг с другом и как они обмениваются данными. Это позволяет эффективно использовать ресурсы сети и обеспечить безопасность передачи данных.

1.1.2.3. Эталонная модель TCP/IP. Эталонная модель TCP/IP - это сетевая модель, используемая для описания и стандартизации протоколов передачи данных в компьютерных сетях. Она состоит из четырех уровней:

1. Уровень доступа к сети (Network Access Layer) - определяет методы передачи данных через конкретную среду передачи (например, Ethernet или Wi-Fi) и включает в себя протоколы, такие как Ethernet, Wi-Fi, PPP и другие.

2. Уровень интернета (Internet Layer) - обеспечивает маршрутизацию и доставку пакетов данных через несколько сетей. Этот уровень использует IP-адресацию и включает в себя протоколы, такие как IP, ICMP, ARP и другие.

3. Транспортный уровень (Transport Layer) - обеспечивает установление соединения и передачу данных между конечными узлами сети. На этом уровне работают протоколы TCP и UDP.

4. Прикладной уровень (Application Layer) - обеспечивает приложениям доступ к сетевым службам и протоколам для передачи данных. На этом уровне работают протоколы, такие как HTTP, FTP, SMTP, DNS и другие.

Эталонная модель TCP/IP является основой для сетевых протоколов Интернета и является наиболее широко используемой сетевой моделью в мире.

1.2. Особенности протокола LoRa. Базовый стек протоколов LoRa.

Особенности протокола LoRa проявляются на 2ом уровне модели OSI, т.к. в данном протоколе используется свой аналог протокола MAC, который ранее даже назывался LoRaMAC. Принцип работы LoRa состоит в линейно-частоной модуляции сигнала (CSS) и имеет такие параметры как коэффициент расширения спеткра, ширину полосы и коэффицент коррекции ошибок. Также в LoRa можно менять чувствительность и скорость приемника (обратно-пропорциональны друг-другу). Базовый стек протоколов состоит из физического, MAC (канального) и уровня приложения (`https://itechinfo.ru/content/%D0%BE%D0%B1%D0%B7%D0%BE%D1%80-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8-lora`).

1.2.1. Мои попытки нарыть

1.2.1.1. Особенности протокола LoRa LoRa (от англ. Long Range) - это беспроводной протокол передачи данных с низким энергопотреблением, который используется для создания IoT-сетей на больших расстояниях. Особенности протокола LoRa включают:

- Дальность передачи: LoRa обеспечивает дальность передачи данных на расстояние до 15 км в открытом пространстве, что делает его идеальным для создания сетей IoT в городах и сельской местности.

- Низкое энергопотребление: благодаря своей конструкции, LoRa использует очень мало энергии для передачи данных, что обеспечивает долгую жизнь батареи устройств, работающих на его основе.

- Широкий диапазон частот: LoRa может работать на частотах от 433 МГц до 928 МГц, что делает его доступным для использования в разных странах и регионах.

- Высокая степень проникновения сигнала: благодаря своей низкочастотной модуляции, LoRa-сигнал может проникать сквозь стены и другие препятствия, что делает его идеальным для использования в густонаселенных городах и зданиях.

- Возможность использования в сетях с большим количеством устройств: LoRa обеспечивает множественный доступ к среде передачи, что позволяет использовать его в сетях с большим количеством устройств.

- Поддержка двунаправленной связи: LoRa поддерживает как однонаправленную, так и двунаправленную связь, что позволяет устройствам отправлять данные и получать ответы.

- Безопасность: LoRa использует различные методы шифрования данных, что обеспечивает безопасную передачу информации.

В целом, эти особенности делают LoRa привлекательным для создания сетей IoT на больших расстояниях с низким энергопотреблением и высокой степенью проникновения сигнала.

1.2.1.2. Базовый стек протоколов LoRa. Базовый стек протоколов LoRa включает в себя два уровня: физический (PHY) и медиа-доступовый контроль (MAC).

Физический уровень определяет параметры передачи данных по радиоканалу, такие как скорость передачи данных, ширина спектра сигнала и т.д. LoRa PHY использует характеристики Лоренца (Lorenzian) для достижения дальней и более эффективной передачи данных.

MAC уровень управляет доступом к радиоканалу, управлением энергопотреблением и маршрутизацией данных. LoRa MAC использует два режима работы: класс A и класс C.

Класс A - это наиболее распространенный режим, который позволяет передавать данные в обе стороны, то есть от устройства к сети и наоборот. Устройство может передавать данные только после принятия данных от сети. Таким образом, время доступа к каналу передачи данных устройства ограничено. Класс A также имеет низкое энергопотребление.

Класс C позволяет устройству быть всегда готовым к приему данных от сети, в отличие от класса A, который переключается на прием только после передачи данных. Это увеличивает время доступа к каналу передачи данных, но позволяет устройству быстро получать данные от сети.

Кроме того, LoRa поддерживает различные протоколы верхнего уровня, такие как LoRaWAN, который предоставляет функции сетевого управления, такие как авторизация устройств, шифрование данных и маршрутизация пакетов данных.

2. Билет 2

2.1. 1.Многоуровневый подход проектированя сетей. Эталонная модель OSI. 2.Сети операторов связи. Программно-определяемые сети.

2.1.1. Из расписки билетов.

1. Многоуровневый подход Декомпозиция задачи сетевого взаимодействия

Организация взаимодействия между устройствами сети является сложной задачей. Как известно, для решения сложных задач используется универсальный прием — декомпозиция, то есть разбиение одной задачи на несколько задач-модулей. Декомпозиция состоит в четком определении функций каждого модуля, а также порядка их взаимодействия (интерфейсов). В результате достигается логическое упрощение задачи, а, кроме того, появляется возможность модификации отдельных модулей без изменения остальной части системы. При декомпозиции часто используют многоуровневый подход. Он заключается в следующем:

- все множество модулей, решающих частные задачи, разбивают на группы и упорядочивают по уровням, образующим иерархию ;
- в соответствии с принципом иерархии для каждого промежуточного уровня можно указать непосредственно примыкающие к нему соседние вышележащий и нижележащий уровни;
- группа модулей, составляющих каждый уровень, должна быть сформирована таким образом, чтобы все модули этой группы для выполнения своих задач обращались с запросами только к модулям соседнего нижележащего уровня;
- , с другой стороны, результаты работы всех модулей, отнесенных к некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня.

Важно различать модель OSI и стек протоколов OSI. В то время как модель OSI является концептуальной схемой взаимодействия открытых систем, стек OSI представляет собой набор спецификаций конкретных протоколов. В отличие от других стеков протоколов, стек OSI полностью соответствует модели OSI, включая спецификации протоколов для всех семи уровней взаимодействия, определённых в этой модели: На физическом и канальном уровнях стек OSI поддерживает протоколы Ethernet, Token ring, FDDI, а также протоколы LLC, X.25 и ISDN, то есть использует все разработанные вне стека популярные протоколы нижних уровней, как и большинство других стеков. Сетевой уровень включает сравнительно редко используемые протоколы Connection-oriented Network Protocol (CONP) и Connectionless Network Protocol (CLNP). Как следует из названий, первый из них ориентирован на соединение (connection-oriented), второй — нет (connectionless). Более популярны протоколы маршрутизации стека OSI: ES-IS (End System — Intermediate System) между конечной и промежуточной системами и IS-IS (Intermediate System — Intermediate System) между промежуточными системами. Транспортный уровень стека OSI в соответствии с функциями, определёнными для него в модели OSI, скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают требуемое качество обслуживания независимо от нижележащего сетевого уровня. Чтобы обеспечить это, транспортный уровень требует, чтобы пользователь задал нужное количество обслуживания. Службы прикладного уровня обеспечивают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее популярными являются служба каталогов (стандарт X.500), электронная почта (стандарт X.400), протокол виртуального терминала (VTP), протокол передачи, доступа и управления файлами (FTAM), протокол пересылки и управления работами (JTM). Стек протоколов TCP/IP — набор сетевых протоколов, на которых базируется Интернет. Обычно в стеке TCP/IP верхние 3 уровня (прикладной, представления и сеансовый) модели OSI объединяют в один — прикладной. Поскольку в таком стеке не предусматривается унифицированный протокол передачи данных, функции по определению типа данных передаются приложению. Уровни стека TCP/IP: Канальный уровень описывает каким образом передаются пакеты данных через физический уровень, включая кодирование (то есть специальные последовательности битов, определяющих начало и конец пакета данных). Сетевой уровень изначально разработан для передачи данных из одной (под)сети в другую. Примерами такого протокола является X.25 и IPC в сети ARPANET. С развитием концепции глобальной сети в уровень были внесены дополнительные возможности по передаче из любой сети в любую сеть, независимо от протоколов нижнего уровня, а также возможность запрашивать данные от удалённой стороны. Протоколы транспортного уровня могут решать проблему негарантированной доставки сообщений («дошло ли сообщение до адресата?»), а также гарантировать правильную последовательность прихода данных. На прикладном уровне работает большинство сетевых приложений. Эти программы имеют свои собственные протоколы обмена информацией, например, HTTP для WWW, FTP (передача файлов), SMTP (электронная почта), SSH (безопасное соединение с удалённой машиной),

DNS (преобразование символьных имён в IP-адреса) и многие другие. Существуют разногласия в том, как вписать модель TCP/IP в модель OSI, поскольку уровни в этих моделях не совпадают. Упрощённо интерпретацию стека TCP/IP можно представить так:

2.1.2. Из попыток самому нарыть

2.1.2.1. Многоуровневый подход проектированя сетей. Многоуровневый подход проектирования сетей предполагает разбиение функциональности сети на несколько уровней, каждый из которых выполняет свою задачу и обеспечивает определенный уровень абстракции. Этот подход используется для упрощения проектирования и разработки сетей, а также для обеспечения совместимости и интероперабельности различных сетевых устройств.

Обычно многоуровневая модель включает в себя три основных уровня:

- Уровень прикладных протоколов (Application Layer)
- Транспортный уровень (Transport Layer)
- Уровень сетевого управления (Network Management Layer)

На уровне прикладных протоколов определяются способы обмена данными между приложениями, которые работают в сети. Здесь определяются форматы данных, протоколы и методы доступа к приложениям.

Транспортный уровень обеспечивает передачу данных между узлами сети и включает в себя протоколы, такие как TCP и UDP. TCP обеспечивает надежную доставку данных, тогда как UDP используется для передачи данных в реальном времени, когда небольшая задержка не критична.

Уровень сетевого управления обеспечивает управление и контроль сетью, включая маршрутизацию, контроль доступа и безопасность. Здесь определяются протоколы, такие как IP, ICMP, ARP, которые обеспечивают передачу данных и управление в сети.

Многоуровневый подход позволяет сделать сеть более гибкой, управляемой и масштабируемой. Каждый уровень может быть проектирован независимо, что позволяет использовать различные технологии и протоколы в каждом уровне, в зависимости от требований сети.

2.1.2.2. Эталонная модель OSI. Эталонная модель OSI (Open Systems Interconnection) - это семиуровневая модель, используемая для описания взаимодействия различных устройств в компьютерных сетях. Каждый уровень модели OSI выполняет определенные функции и предоставляет определенные услуги для последующего уровня.

Ниже перечислены семь уровней модели OSI (от низшего к высшему):

1. Физический уровень (Physical layer) - обеспечивает передачу битовых потоков по физической среде связи, например, по кабелю, радиоволнам или оптическим волокнам.
2. Канальный уровень (Data Link layer) - обеспечивает доставку данных между двумя соседними устройствами в сети, управляет ошибками в канале связи, контролирует доступ к среде передачи данных и управляет потоком данных.
3. Сетевой уровень (Network layer) - обеспечивает маршрутизацию пакетов данных через несколько устройств, управляет трафиком в сети и определяет кратчайший маршрут для доставки пакета данных.
4. Транспортный уровень (Transport layer) - обеспечивает надежную передачу данных между приложениями на разных устройствах, управляет потоком данных, обеспечивает сегментацию и сборку данных и контролирует ошибки в передаче данных.
5. Сеансовый уровень (Session layer) - устанавливает, поддерживает и завершает соединение между приложениями на разных устройствах, контролирует синхронизацию и управляет обменом данными между приложениями.
6. Уровень представления (Presentation layer) - обеспечивает преобразование данных в формат, понятный приложениям, поддерживает кодирование и декодирование данных, обеспечивает конфиденциальность и целостность данных.
7. Прикладной уровень (Application layer) - предоставляет интерфейс для приложений, которые используют сеть, обеспечивает доступ к различным приложениям и сервисам, таким как электронная почта, веб-браузеры и файловые серверы.

Каждый уровень модели OSI взаимодействует с соответствующим уровнем на другом устройстве с помощью протоколов и предоставляет определенные услуги для следующего уровня. Благодаря этой структуре, устройства разных производителей могут работать в одной сети, при этом каждое устройство будет использовать свои протоколы на своих уровнях, но при этом они будут совместимы друг с другом.

Также модель OSI позволяет разделять задачи на различные уровни, что упрощает разработку и отладку протоколов. Каждый уровень может быть изменен независимо от других уровней, что улучшает гибкость и эффективность работы сети. Однако, этот подход также может привести к избыточности данных, так как каждый уровень добавляет свои заголовки и протоколы для обеспечения своих функций, что увеличивает объем передаваемых данных.

2.1.2.3. Сети операторов связи. Сети операторов связи - это инфраструктуры, которые обеспечивают передачу информации между абонентами, используя различные технологии связи. Они могут включать в себя проводные и беспроводные сети, такие как сотовые сети, сети фиксированной связи, спутниковые сети, оптические сети и т.д.

Операторы связи предоставляют различные услуги связи, такие как голосовая связь, передача данных, интернет-соединения, видеосвязь и другие. Для обеспечения этих услуг операторы используют различные технологии и стандарты связи.

Одним из важных аспектов сетей операторов связи является обеспечение качества обслуживания (Quality of Service - QoS). QoS позволяет гарантировать, что различные типы трафика (например, голосовой, видео или данных) будут передаваться с разной приоритетностью, чтобы обеспечить оптимальную производительность и удовлетворительное качество обслуживания.

Операторы связи также заботятся о безопасности своих сетей и данных пользователей, используя различные методы и технологии, такие как шифрование данных и аутентификация пользователей. Они также должны соблюдать законодательные и регуляторные требования, связанные с обеспечением безопасности и защитой личных данных пользователей.

2.1.2.4. Программно-определяемые сети. Программно-определяемые сети (Software-Defined Networking, SDN) - это сетевая архитектура, в которой управление сетью и передача данных разделены друг от друга. В SDN, управление сетью осуществляется централизованным контроллером, который использует программное обеспечение для управления коммутаторами и маршрутизаторами.

В SDN, основным принципом является абстрагирование управления сетью от устройств, которые обеспечивают передачу данных. Это позволяет сети быть более гибкой и масштабируемой, так как изменения в управлении сетью могут быть быстро и легко внедрены на централизованном контроллере, без необходимости вносить изменения в каждый коммутатор и маршрутизатор.

SDN также позволяет программировать сеть для решения конкретных задач. Например, администратор сети может настроить определенные политики для маршрутизации трафика в зависимости от его типа, и эти политики будут применяться ко всей сети.

SDN имеет большое значение для развития технологий облачных вычислений, IoT и других сетевых приложений.

3. Билет 3

3.1. 1.Протоколы распределенных вычислительных сетей. Протокол MPLS. 2.Технологии узкополосной передачи данных NB-IoT сетей доступа LTE/LTE Advanced (4G).Особенности построения радиоинтерфейса технологии NB-IoT.

3.1.1. Из расписки билетов

"MPLS: https://ru.wikipedia.org/wiki/MPLS NB-IoT: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82_NB-IoT_Low-Power_and_Wide-Area,_LPWAN_(%D0%AD%D0%BD%D0%B5%D1%80%D0%B3%D0%BE%D1%8D%D1%84%D1%84%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C_%D0%B4%D0%B0%D0%BB%D1%8C%D0%BD%D0%B5%D0%B3%D0%BE_%D1%80%D0%B0%D0%B4%D0%B8%D1%83%D1%81%D0%B0_%D0%B4%D0%B5%D0%B9%D1%81%D1%82%D0%B2%D0%B8%D1%8F)"

3.1.2. Мои попытки нарыть

3.1.2.1. Протоколы распределенных вычислительных сетей. Протоколы распределенных вычислительных сетей предназначены для организации обмена данными между различными узлами сети и обеспечения ее работоспособности. Эти протоколы должны учитывать особенности сети и способы передачи данных, а также гарантировать надежность, целостность и конфиденциальность передаваемых данных.

Некоторые из распространенных протоколов распределенных вычислительных сетей включают в себя:

- Transmission Control Protocol (TCP) - протокол управления передачей данных, который гарантирует надежность и целостность передачи данных между узлами сети.
- User Datagram Protocol (UDP) - более быстрый и менее надежный протокол, чем TCP, который используется в приложениях, где скорость передачи данных более важна, чем точность.
- Hypertext Transfer Protocol (HTTP) - протокол передачи гипертекста, который используется для обмена данными между веб-сервером и веб-браузером.
- Simple Network Management Protocol (SNMP) - протокол управления сетями, который позволяет администраторам мониторить и управлять устройствами в сети.
- Domain Name System (DNS) - протокол, который преобразует доменные имена в IP-адреса, используемые для идентификации узлов в сети.
- Remote Procedure Call (RPC) - протокол, который позволяет удаленно вызывать процедуры на других узлах сети.
- Lightweight Directory Access Protocol (LDAP) - протокол, который используется для доступа к каталогам информации, таким как каталоги пользователей и групп в сетях.

Каждый из этих протоколов имеет свои особенности и предназначен для решения определенных задач в распределенных вычислительных сетях.

3.1.2.2. Протокол MPLS. MPLS (Multi-Protocol Label Switching) - это протокол коммутации пакетов, который используется в IP-сетях для оптимизации и ускорения передачи данных. Он работает на уровне сетевого интерфейса OSI модели и позволяет определить оптимальный путь для передачи данных между узлами сети.

Принцип работы MPLS заключается в добавлении специальной метки (label) в заголовок каждого пакета данных, которая идентифицирует его маршрут в сети. Роутеры в сети используют эту метку для быстрой коммутации пакетов и выбора оптимального пути.

Одной из основных преимуществ MPLS является возможность создания виртуальных частных сетей (VPN), которые позволяют группе узлов совместно использовать сетевые ресурсы и обмениваться данными, при этом изолируясь от других групп узлов в сети.

Кроме того, MPLS поддерживает качество обслуживания (QoS), что позволяет обеспечивать приоритетную обработку для определенных видов трафика, например, для голосового и видео-трафика, чтобы гарантировать их бесперебойную передачу.

В целом, MPLS является широко используемым протоколом в сетях провайдеров и корпоративных сетях, где требуется высокая производительность и надежность передачи данных.

3.1.2.3. Технологии узкополосной передачи данных NB-IoT сетей доступа LTE/LTE Advanced (4G). NB-IoT (Narrowband Internet of Things) - это технология для передачи данных в интернете вещей (IoT), которая позволяет устройствам соединяться с сетью оператора связи и обмениваться данными, используя существующую инфраструктуру сотовых сетей.

NB-IoT использует сеть доступа LTE/LTE Advanced (4G), но для передачи данных использует узкую полосу частот, что позволяет использовать ее для соединения устройств, которые требуют низкой скорости передачи данных, низкой задержки и низкого энергопотребления. Например, это могут быть устройства для умного дома, умных счетчиков, системы безопасности и другие устройства IoT.

Технология NB-IoT имеет следующие особенности:

- Узкая полоса частот: NB-IoT использует полосу частот в 200 кГц, что в несколько раз меньше, чем полоса частот, используемая в обычной сотовой связи.
- Низкое энергопотребление: NB-IoT использует механизмы энергосбережения, чтобы устройства потребляли меньше энергии при передаче данных и оставались в спящем режиме, когда не используются.
- Широкий охват: NB-IoT позволяет соединять устройства в отдаленных и труднодоступных местах, таких как земельные участки, горные районы и т.д.
- Высокая степень надежности: NB-IoT использует механизмы коррекции ошибок и повтора передачи, что позволяет обеспечивать высокую степень надежности передачи данных.
- Низкая задержка: NB-IoT позволяет достигать низкой задержки при передаче данных, что важно для устройств, требующих реакции в реальном времени, например, систем безопасности.
- Совместимость с существующей инфраструктурой: NB-IoT может использоваться в существующей сотовой сети LTE/LTE Advanced (4G), что позволяет использовать ее без дополнительных инвестиций в инфраструктуру.

Протоколы, используемые в NB-IoT, включают в себя протоколы связи для установления соединения, передачи данных и управления соединением, а также протоколы безопасности и управления энергопотр

3.1.2.4. Особенности построения радиоинтерфейса технологии NB-IoT. Особенности построения радиоинтерфейса технологии NB-IoT включают в себя использование узкополосной модуляции, которая позволяет передавать данные на очень длинные расстояния и снижает влияние помех. Другая важная особенность - это использование разных режимов передачи данных, таких как энергосберегающий режим, который позволяет устройствам работать на батарейках в течение нескольких лет.

Кроме того, в технологии NB-IoT используются специальные механизмы для повышения качества связи и улучшения эффективности передачи данных, такие как управление мощностью передатчика, автоматическое переключение между частотными каналами и повторная передача данных в случае потери пакета информации.

Для обеспечения более надежной связи между устройствами и базовыми станциями NB-IoT использует алгоритмы коррекции ошибок, такие как Turbo-кодирование, для повышения скорости и точности передачи данных.

Кроме того, в технологии NB-IoT используется различные механизмы управления ресурсами сети, такие как динамическое выделение ресурсов и мультиплексирование во времени, что позволяет улучшить эффективность использования частотного ресурса и повысить пропускную способность сети.

4. Билет 4

4.1. 1.Протоколы ЛВС. Сети Fast Ethernet, Gigabit Ethernet. 2.Характеристики оборудования Zigbee и Z-Wave.

4.1.1. Из расписки билетов

ЛВС: `http://project.net.ru/others/article7/net4_2.html`
Fast Ethernet: `https://ru.wikipedia.org/wiki/Fast_Ethernet`
Gigabit Ethernet: `https://ru.wikipedia.org/wiki/Gigabit_Ethernet`
Zigbee и Z-Wave: `https://superhome.pro/z-wave-vs-zigbee-wifi-thread-bluetooth-ble-vybiraem-protokol-up`

4.1.2. Мои раскопки

4.1.2.1. Протоколы ЛВС Протоколы локальных вычислительных сетей (ЛВС) - это набор правил и процедур, которые определяют способ, которым устройства в ЛВС общаются между собой. Протоколы ЛВС используются для управления передачей данных между устройствами в сети, управления доступом к среде передачи и обеспечения безопасности и целостности данных.

Существует множество протоколов ЛВС, каждый из которых предназначен для решения определенных задач. Рассмотрим некоторые из них:

- Ethernet - наиболее распространенный протокол ЛВС, используемый для соединения компьютеров и других сетевых устройств. Ethernet работает на физическом и канальном уровнях модели OSI и определяет способы доступа к среде передачи, формат кадра и методы обнаружения ошибок.
- Wi-Fi - протокол беспроводной ЛВС, используемый для соединения устройств посредством радиоволн. Wi-Fi работает на физическом и канальном уровнях модели OSI и определяет способы передачи данных по радиоканалу, формат кадра и методы обнаружения ошибок.
- Token Ring - протокол ЛВС, в котором передача данных осуществляется с помощью "жетонов". Устройство может передавать данные только при наличии у него жетона, который передается по кольцу вместе с данными. Этот протокол больше не используется, однако его идеи в части управления доступом к среде передачи применяются в других протоколах.
- FDDI - протокол ЛВС, используемый для построения кольцевых сетей с двойной степенью избыточности. Он работает на физическом и канальном уровнях модели OSI и предназначен для высоконадежных сетей с высокой пропускной способностью.
- ATM - протокол, используемый для передачи данных в высокоскоростных сетях. ATM работает на канальном и сетевом уровнях модели OSI и предназначен для обеспечения высокой скорости передачи данных и гарантированной доставки.
- TCP/IP - протоколы, используемые в Интернете и на сетях, построенных на его основе. TCP/IP работает на сетевом, транспортном и прикладном уровня

4.1.2.2. Сети Fast Ethernet, Gigabit Ethernet. Fast Ethernet и Gigabit Ethernet - это два поколения технологий Ethernet, которые используются для передачи данных в компьютерных сетях.

Fast Ethernet - это первое поколение технологии Ethernet, которое было разработано для увеличения скорости передачи данных в локальных сетях (LAN). Fast Ethernet работает на скорости 100 Мбит/с, что в 10 раз быстрее, чем оригинальная Ethernet-технология, которая работала на скорости 10 Мбит/с. Fast Ethernet использует тот же протокол доступа к среде передачи данных (CSMA/CD), что и оригинальная Ethernet-технология. Fast Ethernet быстро стал широко распространенной технологией для построения локальных сетей.

Gigabit Ethernet - это следующее поколение технологии Ethernet, которое было разработано для увеличения скорости передачи данных еще в 10 раз, до 1 Гбит/с. Gigabit Ethernet использует тот же протокол доступа к среде передачи данных, что и Fast Ethernet, но с более высокой скоростью передачи данных. Gigabit Ethernet также добавляет новые функции, такие как Jumbo Frame, которые позволяют передавать более большие блоки данных, что увеличивает эффективность передачи данных в сети.

Обе технологии используют UTP-кабель (Unshielded Twisted Pair), который может быть проложен на расстоянии до 100 метров без использования усилителей сигнала. Однако для достижения максимальной скорости передачи данных на больших расстояниях (до 2 км) могут использоваться другие типы кабеля, например оптоволокно.

Fast Ethernet и Gigabit Ethernet являются важными технологиями для построения современных компьютерных сетей. Они позволяют передавать данные на высоких скоростях и обеспечивать быстрый доступ к ресурсам в сети.

4.1.2.3. Характеристики оборудования Zigbee и Z-Wave. Zigbee и Z-Wave - это две различные технологии беспроводной связи, которые широко используются в области умного дома и Интернета вещей (IoT).

Zigbee - это технология беспроводной сети на основе стандарта IEEE 802.15.4, которая использует малоэнергетические радиочастоты (2,4 ГГц) для передачи данных. Zigbee работает на расстояниях до 100 метров и обеспечивает высокую пропускную способность до 250 кбит/с. Кроме того, Zigbee обладает высокой степенью надежности и безопасности, что делает его идеальным для применения в умном доме и IoT.

Оборудование Zigbee состоит из нескольких компонентов, включая устройства передачи данных (узлы), координаторы сети и серверы сетевого управления. Узлы обеспечивают подключение к сети и передачу данных, координаторы управляют сетью и узлами, а серверы управления позволяют пользователям управлять сетью и узлами.

Z-Wave - это другая технология беспроводной связи, которая использует радиочастоты (908,42 МГц в США и 868,42 МГц в Европе) для передачи данных. Z-Wave работает на расстояниях до 100 метров и обеспечивает скорость передачи данных до 100 кбит/с. Z-Wave также обладает высокой степенью надежности и безопасности.

Оборудование Z-Wave включает в себя устройства управления, устройства передачи данных (узлы) и контроллеры сети. Устройства управления позволяют пользователям управлять сетью и узлами, узлы обеспечивают подключение к сети и передачу данных, а контроллеры сети управляют сетью и узлами.

Одной из главных различий между Zigbee и Z-Wave является то, что Zigbee поддерживает большее количество устройств в сети, чем Z-Wave. Кроме того, Zigbee имеет более широкий диапазон частот, чем Z-Wave, что делает его более гибким в использовании. Однако, Z-Wave более надежен в условиях большой плотности сети и предлагает более простой способ управления сетью.

5. Билет 5

5.1. 1.Множественный доступ с контролем несущей и обнаружением конфликтов. Маркерные методы доступа. 2.Обзор технологии Zigbee. Обзор технологии Z-Wave.

5.1.1. Из расписки билетов

https://ru.wikipedia.org/wiki/CSMA/CD
https://it-wr.ru/support/spravochnik/technology/marker-access

5.1.2. Мои поиски по инетам

5.1.2.1. Множественный доступ с контролем несущей и обнаружением конфликтов. Множественный доступ с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) - это метод доступа к среде передачи данных, который используется в Ethernet-сетях для разрешения конфликтов при одновременном доступе нескольких устройств к среде передачи.

CSMA/CD работает следующим образом: каждое устройство, желающее передать данные в сеть, проверяет занятость среды передачи (контроль несущей) и если среда свободна, то начинает передачу данных. Если в процессе передачи данных происходит конфликт (несколько устройств начинают передачу одновременно), то происходит обнаружение коллизии и устройства, участвующие в конфликте, прекращают передачу и начинают процедуру повторной передачи через случайное время.

CSMA/CD обеспечивает эффективное использование среды передачи данных и снижает количество коллизий при одновременном доступе нескольких устройств к среде. Однако, данный метод имеет свои ограничения в скорости передачи данных и не может использоваться в сетях высокой скорости, таких как Gigabit Ethernet.

В настоящее время в Ethernet-сетях вместо CSMA/CD используется метод множественного доступа с контролем несущей и определением столкновения (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) с использованием протокола Ethernet over TCP/IP.

5.1.2.2. Маркерные методы доступа. Маркерные методы доступа являются одним из способов реализации множественного доступа к среде передачи данных в компьютерных сетях. Они используют механизм передачи маркера по среде, который позволяет управлять доступом устройств к сети и предотвращать конфликты при передаче данных.

Существуют два основных типа маркерных методов доступа: маркерный метод доступа с контролем обмена и маркерный метод доступа с контролем передачи.

Маркерный метод доступа с контролем обмена (Token Passing) основан на передаче маркера по кольцевой топологии сети. В этом методе маркер перемещается по кольцу и устройство, которое получило маркер, имеет право на передачу данных. После передачи данных устройство освобождает маркер, и он перемещается дальше по кольцу к следующему устройству. Маркерный метод доступа с контролем обмена используется, например, в технологии Token Ring.

Маркерный метод доступа с контролем передачи (Token Bus) основан на передаче маркера в линейной топологии сети. В этом методе устройство может передавать данные только после того, как получит маркер. Устройство, которое получило маркер, передает данные и передает маркер следующему устройству в сети. Маркерный метод доступа с контролем передачи используется, например, в технологии ARCnet.

Маркерные методы доступа обеспечивают более эффективное использование пропускной способности среды передачи данных, чем методы доступа с обнаружением несущей и с контролем доступа по расписанию. Однако они также имеют недостатки, связанные с потерей маркера, задержками при передаче данных и необходимостью сложной логики управления доступом к среде передачи данных.

5.1.2.3. Обзор технологии Zigbee. Zigbee - это беспроводная технология, которая используется для управления устройствами на коротких расстояниях. Она использует малую энергию, что позволяет ей работать дольше от батареи, и подходит для создания сетей, которые могут включать сотни или даже тысячи устройств.

Основные характеристики технологии Zigbee:

- Использует частотный диапазон 2,4 ГГц, 868 МГц или 915 МГц.
- Поддерживает множество топологий сетей, включая звезду, дерево и сети меш.
- Обеспечивает высокий уровень безопасности с помощью шифрования AES-128.

- Имеет низкую скорость передачи данных (от 20 до 250 кбит/сек), что позволяет снизить энергопотребление и увеличить дальность передачи сигнала.
- Поддерживает многоканальную передачу данных, что повышает надежность связи и позволяет избежать помех.
- Обеспечивает высокую масштабируемость, что позволяет добавлять новые устройства и расширять сеть без необходимости перестраивать ее с нуля.

Технология Zigbee используется в различных областях, таких как домашняя автоматизация, умный город, управление освещением и т.д. Zigbee может работать с различными типами устройств, включая датчики, переключатели, мониторы и устройства управления.

5.1.2.4. Обзор технологии Z-Wave. Z-Wave - это технология беспроводной связи для сетей управления умным домом (home automation). Она работает в диапазоне частот 800-900 МГц и 2,4 ГГц и обеспечивает беспроводную связь между устройствами умного дома, такими как датчики движения, дверные замки, термостаты, освещение и другие.

Основными характеристиками технологии Z-Wave являются:

- Низкая потребляемая мощность: устройства, использующие Z-Wave, потребляют очень мало энергии, что позволяет им работать на батарейках дольше.
- Безопасность: протокол Z-Wave использует шифрование AES-128 для обеспечения безопасности передачи данных между устройствами.
- Простота установки: устройства на базе Z-Wave очень легко устанавливаются и настраиваются благодаря использованию беспроводной связи и простому интерфейсу управления.
- Стандартизация: технология Z-Wave является стандартом для устройств умного дома и обеспечивает совместимость между различными устройствами.
- Надежность: протокол Z-Wave использует механизм повтора сигнала (repeater) для обеспечения надежности передачи данных между устройствами.
- Масштабируемость: технология Z-Wave позволяет легко добавлять новые устройства в сеть управления умным домом, что обеспечивает ее масштабируемость и гибкость.
- Дальность действия: устройства на базе Z-Wave могут работать на расстоянии до 100 метров в открытом пространстве и до 30 метров в помещении.

Технология Z-Wave позволяет создавать различные сценарии управления умным домом, включая автоматическое управление освещением, термостатами, замками и другими устройствами на основе времени суток, датчиков движения и других параметров.

6. Билет 6

6.1. 1.Архитектура сетей и радиопокрытие сетей LoRa. Безопасность в сетях LoRa. 2.Базовая концепция облачных платформ в интернете вещей. Обзор основных платформ на рынке AWS, Microsoft, Google Cloud

6.1.1. Из расписки билетов

1. https://itechinfo.ru/content/%D0%BE%D0%B1%D0%B7%D0%BE%D1%80-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8-lora
   https://www.iksmedia.ru/articles/5573226-Set-LoRaWAN-bezopasnost-obespechiva.html

6.1.2. Мои поиски по инету

6.1.2.1. Архитектура сетей и радиопокрытие сетей LoRa. Архитектура сетей LoRa построена на основе сетей с ячеистой топологией, где каждый узел (устройство) может быть как узлом передачи, так и узлом приема данных. Устройства в LoRa-сети могут также действовать как ретрансляторы, что позволяет увеличить дальность передачи данных.

Радиопокрытие сетей LoRa определяется несколькими факторами, включая используемые частоты, мощность передатчиков, чувствительность приемников и физическую окружающую среду. Частоты, используемые в LoRa-сетях, обычно находятся в диапазоне от 433 МГц до 928 МГц, что обеспечивает относительно большую дальность передачи данных на открытом пространстве. Однако, дальность передачи может сильно зависеть от препятствий на пути сигнала, таких как стены, здания и другие объекты.

Для обеспечения стабильной связи в условиях переменной окружающей среды, LoRa использует технологию адаптивной скорости передачи данных, которая автоматически выбирает оптимальную скорость передачи данных в зависимости от качества канала связи и уровня шума. Это обеспечивает стабильную передачу данных на большие расстояния, при этом сохраняя энергопотребление устройств на минимальном уровне.

Для организации LoRa-сетей используются различные архитектуры, включая централизованные и децентрализованные. В централизованных сетях управление передачей данных осуществляется центральным узлом, который контролирует передачу данных между устройствами. В децентрализованных сетях каждое устройство является самостоятельным и может передавать данные непосредственно другим устройствам.

В целом, архитектура сетей и радиопокрытие сетей LoRa обеспечивают высокую дальность передачи данных, надежность связи и энергоэффективность, что делает их привлекательными для применения в различных IoT-решениях.

6.1.2.2. Безопасность в сетях LoRa. Безопасность в сетях LoRa основана на криптографических протоколах и механизмах обеспечения конфиденциальности, целостности и аутентификации данных.

Один из основных протоколов безопасности в сетях LoRa - это AES (Advanced Encryption Standard) с длиной ключа 128 бит, который используется для шифрования передаваемых данных. Для обеспечения целостности данных используется HMAC (Hash-based Message Authentication Code), который вычисляет код аутентификации сообщения на основе хэш-функции и секретного ключа.

В сетях LoRa также применяются механизмы аутентификации, которые позволяют проверять подлинность устройств и защищают сеть от поддельных устройств. Для этого используется протокол MIC (Message Integrity Code), который проверяет целостность сообщения, а также протокол симметричной аутентификации, который проверяет, что устройство имеет доступ к секретному ключу.

Кроме того, в сетях LoRa используются различные механизмы контроля доступа к сети, такие как MAC (Medium Access Control) и ADR (Adaptive Data Rate), которые позволяют обеспечивать эффективное использование ресурсов сети и предотвращать атаки с перегрузкой сети.

Таким образом, в сетях LoRa применяются различные механизмы безопасности, которые обеспечивают конфиденциальность, целостность и аутентификацию данных, а также защиту от атак на сеть.

6.1.2.3. Базовая концепция облачных платформ в интернете вещей. Базовая концепция облачных платформ в интернете вещей (IoT) заключается в том, что устройства собирают данные и отправляют их в облако для анализа, хранения и дальнейшей обработки. Это позволяет организациям эффективно использовать данные, собранные с большого количества устройств, для улучшения бизнес-процессов и повышения производительности.

Одной из ключевых особенностей облачных платформ IoT является возможность удаленного управления и мониторинга устройств через интернет. Облачные платформы могут предоставлять различные

сервисы, такие как управление устройствами, сбор данных, аналитику, машинное обучение и другие функции, которые помогают организациям извлекать максимальную пользу из данных IoT.

В облачных платформах IoT используются различные технологии и протоколы, такие как MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), HTTP (Hypertext Transfer Protocol) и другие. Эти протоколы обеспечивают передачу данных между устройствами и облачными серверами.

Облачные платформы IoT также могут использоваться для управления безопасностью и конфиденциальностью данных. Они могут обеспечить защиту данных, передаваемых между устройствами и облачными серверами, а также между облачными серверами и приложениями.

Также важно отметить, что облачные платформы IoT могут быть использованы как для коммерческих, так и для некоммерческих целей. Они могут быть использованы в различных отраслях, таких как здравоохранение, сельское хозяйство, промышленность, транспорт и др.

6.1.2.4. Обзор основных платформ на рынке AWS, Microsoft, Google Cloud. На рынке облачных платформ существует несколько крупных игроков, которые предоставляют услуги для разработки, развертывания и управления приложениями Интернета вещей. Некоторые из них включают:

- Amazon Web Services (AWS) - это облачная платформа Amazon, которая предоставляет широкий спектр услуг, таких как хранение, вычисления, базы данных, аналитика, Интернет вещей и многие другие. В контексте Интернета вещей, AWS предоставляет различные сервисы, такие как AWS IoT Core, AWS IoT Greengrass и AWS IoT Analytics. AWS IoT Core - это облачный сервис, который позволяет управлять миллионами подключенных устройств, собирать и обрабатывать данные, отправлять уведомления и автоматически реагировать на события.

- Microsoft Azure - это облачная платформа Microsoft, которая предоставляет услуги, такие как вычисления, хранение, базы данных, аналитика, Интернет вещей и многие другие. Azure IoT Hub - это сервис, который позволяет управлять миллионами подключенных устройств, собирать и анализировать данные, отправлять уведомления и автоматически реагировать на события. Azure IoT Edge - это сервис, который позволяет развернуть облачные сервисы на локальных устройствах для обработки данных ближе к источнику.

- Google Cloud - это облачная платформа Google, которая предоставляет услуги, такие как вычисления, хранение, базы данных, аналитика, Интернет вещей и многие другие. Google Cloud IoT Core - это сервис, который позволяет управлять миллионами подключенных устройств, собирать и обрабатывать данные, отправлять уведомления и автоматически реагировать на события. Google Cloud IoT Edge - это сервис, который позволяет развернуть облачные сервисы на локальных устройствах для обработки данных ближе к источнику.

Все три платформы предоставляют широкий набор сервисов, которые могут быть использованы для разработки и управления приложениями Интернета вещей. Каждая из них имеет свои сильные и слабые стороны, поэтому выбор конкретной платформы зависит от конкретных потребностей и требований проекта.

7. Билет 7

7.1. 1.Каналы передачи данных.Среда передачи данных. Передача данных на физическом и канальном уровнях. 2.MQTT протокол: Сильные/слабые стороны. Принципы работы.

7.1.1. Из расписки билетов

2. MQTT – это основанный на стандартах протокол, или набор правил, обмена сообщениями, используемый для взаимодействия между компьютерами. Интеллектуальные датчики, носимые устройства и другие устройства Интернета вещей (IoT) обычно передают и получают данные по сетям с ограниченными ресурсами и пропускной способностью. Эти устройства IoT используют MQTT для передачи данных, поскольку он прост в реализации и может эффективно передавать данные IoT. MQTT поддерживает передачу сообщений от устройств в облако и в обратном направлении. Преимущества : MQTT нейтрален к содержимому пакета. Поле данных протокола MQTT может содержать данные любого типа, такие как двоичные файлы, текст ascii и т.д. Приемник должен уметь интерпретировать и декодировать в соответствии с форматом, используемым передатчиком. Он использует пакет небольшого размера и может использоваться для приложений с низкой пропускной способностью. Он обеспечивает более низкое энергопотребление батареи. Это надежный протокол, поскольку он использует параметры QoS для обеспечения гарантированной доставки. Предназначен для доставки сообщений в соответствии с шаблонами максимум один раз, минимум один раз и ровно один раз Масштабируемость благодаря своей модели публикации/подписки. Он предлагает несвязанную конструкцию, так как легко разделить устройство и сервер. Идеально подходит для распределенных коммуникаций один ко многим и для отдельных приложений. Устройство публикации может отправлять данные на сервер в любое время, независимо от его состояния. Оснащен функцией LWT (“Последняя воля” и “Завещание”) для уведомления сторон о ненормальном отключении клиента. Полагается на TCP/IP для основных задач связи. Недостатки: MQTT не поддерживает потоковую передачу видео. Проблемы с задержкой. MQTT имеет более медленные циклы передачи. Безопасность не встроена. MQTT не зашифрован. Вместо этого он использует TLS/SSL (Уровень безопасности транспортного уровня/Уровень защищенных сокетов) для шифрования безопасности. Централизованный брокер может привести к сбою, поскольку клиентские соединения с брокерами постоянно открыты. Принцип работы : Протокол MQTT работает по модели «издатель-подписчик». При традиционном взаимодействии по сети клиенты и серверы связываются между собой напрямую. Клиенты запрашивают у сервера ресурсы или данные, сервер обрабатывает запрос и возвращает ответ. Но MQTT использует шаблон «издатель-подписчик», чтобы отделить отправителя сообщения (издателя) от получателя (подписчика). Взаимодействием между издателями и подписчиками управляет третий компонент – брокер сообщений. Задача брокера – отфильтровать все входящие сообщения от издателей и отправить их соответствующим подписчикам.

7.1.2. Из моих поисков

7.1.2.1. Каналы передачи данных. Канал передачи данных - это физический или логический канал, используемый для передачи информации между двумя устройствами. Каналы передачи данных могут быть различными в зависимости от типа сети, протокола передачи и других факторов. Некоторые из наиболее распространенных каналов передачи данных включают в себя:

- Кабельная линия: Это один из наиболее распространенных каналов передачи данных, используемый для соединения компьютеров, серверов и других устройств в локальной сети (LAN) или метрополитенской сети (MAN). Кабельные линии могут быть витой пары, коаксиальными, оптическими или другими типами кабелей.
- Беспроводные сети: Беспроводные сети позволяют передавать данные между устройствами без необходимости использования физических кабелей. Типичные примеры беспроводных сетей включают в себя Wi-Fi, Bluetooth, NFC и Zigbee.
- Спутниковые связи: Спутниковые связи используют спутники, находящиеся в космическом пространстве, для передачи данных между устройствами. Этот метод часто используется в глобальных сетях связи и мобильных сетях.
- Линии связи: Линии связи используются для передачи данных на большие расстояния между устройствами. Они могут быть физическими (например, оптоволоконные кабели) или логическими (например, VPN-туннели).

- Линии связи: Линии связи используются для передачи данных на большие расстояния между устройствами. Они могут быть физическими (например, оптоволоконные кабели) или логическими (например, VPN-туннели).

- Локальный обмен данными: Локальный обмен данными (LAN) - это группа связанных устройств, которые используются для передачи данных между ними. Локальные сети обычно используются в офисах или домах для обеспечения связи между компьютерами и другими устройствами.

- Каналы спутниковой связи - это системы связи, использующие искусственные спутники, находящиеся в космическом пространстве, для передачи данных. Они широко используются в телекоммуникациях, транспорте, геодезии, метеорологии и других областях, где требуется дальнейшая передача данных через большие расстояния. Существуют различные виды спутниковых систем связи, включая геостационарные, низкоорбитальные и среднеорбитальные системы.

- Каналы оптоволоконной связи - это каналы передачи данных, использующие оптоволоконные кабели для передачи световых сигналов. Они представляют собой один из наиболее быстрых и надежных способов передачи данных на длинные расстояния. Оптоволоконные кабели широко используются в телекоммуникационных системах, компьютерных сетях, медицинских приборах, научных исследованиях и других областях.

- Каналы радиорелейной связи - это системы связи, использующие радиоволны для передачи данных между двумя точками через воздух. Радиорелейная связь широко используется в телекоммуникационных системах, где требуется быстрое и надежное соединение между удаленными точками. Системы радиорелейной связи могут использоваться для передачи данных между зданиями, на больших расстояниях и в труднодоступных местах.

- Каналы мобильной связи - это системы связи, использующие сотовые технологии для передачи данных между мобильными устройствами и базовыми станциями. Они широко используются в мобильных телефонах, планшетах и других устройствах, которые позволяют пользователю подключаться к интернету и обмениваться данными с другими устройствами через мобильные сети.

- Каналы кабельной связи - это каналы передачи данных, использующие провода и кабели для передачи сигналов между двумя или более устройствами. Кабельная связь широко используется в домашних и офис

7.1.2.2. Среда передачи данных. Среда передачи данных - это физическая среда, в которой передаются данные между устройствами в компьютерных сетях. Среда передачи данных может быть проводной (например, медный или оптоволоконный кабель) или беспроводной (например, радиоволны или инфракрасный свет).

Проводная среда передачи данных представляет собой физический кабель, по которому проходят сигналы данных. Такие кабели могут быть сделаны из различных материалов, включая медь, стекловолокно и оптические волокна. Кабели делятся на два типа: коаксиальные и витые пары.

Коаксиальные кабели используются для передачи аналоговых сигналов высокой частоты, например, в кабельном телевидении. Они состоят из медного провода, окруженного слоями изоляции и экрана. Витые пары используются для передачи цифровых сигналов. Они состоят из двух или более проводников, скрученных вместе для уменьшения влияния электромагнитных помех.

Беспроводная среда передачи данных использует радиоволны, инфракрасный свет или другие методы для передачи данных между устройствами. Такие среды передачи данных широко используются в мобильных сетях и Wi-Fi-сетях.

Выбор среды передачи данных зависит от ряда факторов, включая требования к скорости передачи данных, расстояние между устройствами и наличие помех в среде передачи данных.

7.1.2.3. Передача данных на физическом и канальном уровнях Передача данных на физическом и канальном уровнях включает в себя передачу сигналов по физической среде связи. Физический уровень занимается преобразованием битов информации в электрические, оптические или радиочастотные сигналы, а также передачей этих сигналов по среде связи.

Передача данных на канальном уровне включает в себя управление доступом к среде передачи данных и обеспечение надежной передачи данных между устройствами. Для этого используются различные протоколы и алгоритмы, такие как протоколы MAC (Media Access Control) и LLC (Logical Link Control).

Протокол MAC определяет правила доступа к среде передачи данных и контролирует коллизии (столкновения сигналов), которые могут возникнуть при одновременной передаче данных несколькими устройствами. Протокол LLC обеспечивает надежность передачи данных на канальном уровне путем проверки целостности данных и управления потоком данных между устройствами.

Оба уровня взаимодействуют между собой и образуют канальный уровень модели OSI. Канальный уровень является промежуточным между физическим и сетевым уровнями и обеспечивает надежную передачу данных внутри сети.

7.1.2.4. MQTT протокол: Сильные/слабые стороны. Протокол MQTT (Message Queuing Telemetry Transport) - это легковесный протокол передачи сообщений, который используется в интернете вещей для обмена данными между устройствами и приложениями. Вот некоторые из сильных и слабых сторон этого протокола:

- Легковесность: MQTT - это легковесный протокол, который требует минимальных ресурсов для работы, что делает его идеальным для использования на устройствах с ограниченными ресурсами.
- Эффективность передачи данных: благодаря минимальным накладным расходам MQTT-сообщения передаются быстро и эффективно.
- Гибкость: MQTT поддерживает различные уровни качества обслуживания (QoS), что позволяет пользователю настраивать уровень доставки сообщений в зависимости от их важности.
- Надежность: MQTT-сообщения сохраняются в буфере на сервере брокера, что позволяет их доставить, когда устройство становится доступным.

Слабые стороны:

- Нет встроенной безопасности: MQTT не имеет встроенных механизмов безопасности, таких как аутентификация и шифрование, и должен использоваться в сочетании с другими протоколами и методами безопасности, такими как TLS/SSL.
- Ограниченные возможности маршрутизации: MQTT-сообщения передаются через брокер, и нет возможности отправлять сообщения напрямую на другое устройство.
- Отсутствие стандартизации: наличие нескольких вариантов протокола MQTT, которые не всегда полностью совместимы друг с другом, может привести к некоторым проблемам при обмене данными между устройствами, использующими разные варианты протокола.

8. Билет 8

8.1. 1.Количество информации. Энтропия. Коэффициент избыточности сообщения. 2.Производители оборудования LoRa. Характеристики оборудования LoRa.

8.1.1. Из расписок билетов

"1. Количество информации в теории информации – это количество информации в одном случайном объекте относительно другого. Тут формулки красивые, поэтому лучше на сайте глянуть. Также здесь довольно понятно приводят пример того, зачем это нужно.

Информационная энтропия — мера неопределённости некоторой системы (в статистической физике или теории информации), в частности, непредсказуемость появления какого-либо символа первичного алфавита. В последнем случае при отсутствии информационных потерь энтропия численно равна количеству информации на символ передаваемого сообщения. Например, в последовательности букв, составляющих какое-либо предложение на русском языке, разные буквы появляются с разной частотностью, поэтому неопределённость появления для некоторых букв меньше, чем для других. Если же учесть, что некоторые сочетания букв (в этом случае говорят об энтропии n-го порядка, см. ниже) встречаются очень редко, то неопределённость уменьшается еще сильнее. Более подробное определение, свойства и вариации здесь.

Избыточность информации — термин из теории информации, означающий превышение количества информации, используемой для передачи или хранения сообщения, над его информационной энтропией. Для уменьшения избыточности применяется сжатие данных без потерь, в то же время контрольная сумма применяется для внесения дополнительной избыточности в поток, что позволяет производить исправление ошибок при передаче информации по каналам, вносящим искажения (спутниковая трансляция, беспроводная передача и т. д.). Коэффициент избыточности сообщения A определяется по формуле

$$r = \frac{(I_{max} - I)}{I_{max}}$$

где I - количество информации в сообщении A, I_{max} - максимально возможное количество информации в сообщении той же длины, что и A. Пример избыточности дают сообщения на естественных языках, так, у русского языка r находится в пределах 0,3...0,5. Наличие избыточности позволяет ставить вопрос о сжатии информации без ее потери в передаваемых сообщениях.

2. Список части самых известных производителей LoRa Основыне характеристики:

- Радиус действия
- Скорость
- Диапазон частот

Также более подробная информация тут, тут и тут"

8.1.2. Из поисков в интернете

8.1.2.1. Количество информации. Энтропия. Количество информации - это мера количества знаний, которые сообщает какой-то источник информации. Это понятие связано с теорией информации, которая занимается изучением свойств, ограничений и процессов передачи информации.

Энтропия является ключевым понятием в теории информации и является мерой неопределенности или неизвестности в системе. Она используется для описания степени хаоса или неопределенности в системе и может рассматриваться как мера количества информации, которое может быть передано в системе.

В контексте теории информации, энтропия обычно выражается в битах и определяется формулой:

$$H = -\sum p(x) \log_2 p(x)$$

где H - энтропия, $p(x)$ - вероятность того, что случайная переменная X примет значение x, и log_2 - логарифм по основанию 2.

Чем более неопределенная система, тем выше ее энтропия. Например, если у нас есть монета, которая может выпасть либо орлом, либо решкой, то энтропия этой системы будет равна 1 биту, так как мы можем передать один бит информации, сообщая результат подбрасывания монеты. Если же у нас есть кубик, который может выпасть одной из шести граней, то энтропия этой системы будет равна примерно 2,58 бита.

Сильные стороны MQTT протокола включают в себя его легковесность, простоту и эффективность в передаче данных между устройствами, а также поддержку публикации-подписки (publish-subscribe), которая упрощает реализацию систем взаимодействия IoT-устройств. Кроме того, MQTT может работать в надежных и ненадежных сетевых условиях, обеспечивая гарантированную доставку сообщений с помощью подтверждений и повторной передачи в случае потери.

Слабые стороны MQTT включают ограниченную поддержку безопасности, что может быть проблемой в случае передачи чувствительной информации, а также ограниченные возможности масштабирования в случае большого количества устройств, так как каждое устройство подключается напрямую к брокеру MQTT.

8.1.2.2. Коэффициент избыточности сообщения. Коэффициент избыточности сообщения (англ. redundancy ratio) - это отношение количества бит информации в сообщении к общему количеству бит, передаваемых в сообщении. Он показывает, насколько сообщение содержит дополнительную информацию, которая не является необходимой для передачи основного содержания сообщения.

Например, рассмотрим сообщение "мама мыла раму". Для передачи этого сообщения требуется 56 бит (8 бит на символ). Однако если мы будем использовать кодирование Хаффмана, то можно сократить количество бит, не потеряв информацию. В результате количество бит для передачи сообщения будет меньше 56, и коэффициент избыточности будет меньше 1.

В целом, чем меньше коэффициент избыточности, тем более эффективно используется пропускная способность канала связи. Однако слишком низкий коэффициент может привести к тому, что при возникновении ошибок в передаче данных будет сложно восстановить исходное сообщение. Поэтому оптимальный коэффициент избыточности зависит от конкретного случая и может быть различным.

8.1.2.3. Производители оборудования LoRa. На рынке существует множество производителей оборудования, поддерживающего технологию LoRa. Некоторые из них:

- Semtech - компания, разработавшая технологию LoRa и предоставляющая чипы для устройств на ее основе.
- Microchip - производитель микроконтроллеров и радиомодулей на основе LoRa.
- STMicroelectronics - производитель микроконтроллеров и радиомодулей на основе LoRa.
- Murata - производитель радиомодулей и устройств на основе LoRa.
- Laird Connectivity - производитель радиомодулей и устройств на основе LoRa.
- Adeunis - производитель устройств на основе LoRa для различных применений, включая умный город и промышленность.
- Kerlink - производитель сетевых устройств и оборудования на основе LoRa для умных городов, сельской местности и других применений.
- Dragino - производитель различных устройств на основе LoRa для домашнего использования, а также для умных городов и промышленности.
- Link Labs - производитель промышленных радиомодулей и сетевых устройств на основе LoRa для различных применений.
- Multitech Systems - производитель промышленных устройств на основе LoRa для умных городов, сельской местности и других применений.

8.1.2.4. Характеристики оборудования LoRa. Оборудование для сетей LoRa включает в себя несколько компонентов:

- Устройства сбора данных (LoRa-устройства): это устройства, которые собирают данные от датчиков и передают их через LoRa-радиоинтерфейс в сеть LoRaWAN. Эти устройства могут быть разных типов: от небольших датчиков температуры и влажности до устройств слежения за расположением и состоянием объектов.
- Шлюзы LoRa: это устройства, которые получают данные от LoRa-устройств и передают их в сеть LoRaWAN через сеть интернет. Шлюзы могут быть различных типов и форм-факторов: от небольших устройств для домашнего использования до больших серверных решений для промышленных сетей.

- Серверы LoRaWAN: это серверы, которые управляют сетью LoRaWAN и обрабатывают данные, полученные от LoRa-устройств. Они также отвечают за безопасность сети и управление доступом к ней.

Характеристики оборудования LoRa:

- Частотный диапазон: Обычно используются частоты 433, 868 и 915 МГц, в зависимости от региона и страны.
- Дальность передачи: Дальность передачи может достигать до 15 км в открытой местности и до 2 км в городской застройке, в зависимости от используемой мощности передатчика и условий окружающей среды.
- Скорость передачи данных: Обычно скорость передачи данных составляет от 0,3 кбит/с до 50 кбит/с, в зависимости от конфигурации и настроек устройства.
- Потребляемая мощность: Одним из главных преимуществ LoRa является низкое энергопотребление. Многие устройства могут работать на батареях в течение нескольких лет.
- Взаимодействие с другими протоколами: Устройства, основанные на LoRa, могут работать с другими беспроводными технологиями, такими как Bluetooth, Wi-Fi и Zigbee, что позволяет создавать комплексные системы интернета вещей.
- Стоимость: Цена оборудования LoRa снизилась в последнее время, что делает его доступным для многих производителей устройств интернета вещей.
- Надежность: LoRa обеспечивает высокую надежность передачи данных за счет использования технологии расширенного спектра и физических свойств радиоволн.
- Стандартизация: LoRa является стандартизированной технологией, поддерживаемой LoRa Alliance, что гарантирует совместимость и взаимодействие различных устройств и систем.
- Возможности расширения: Устройства, основанные на LoRa, могут быть легко интегрированы с облачными сервисами и другими системами управления данными, что делает их идеальным выбором для различных приложений интернета вещей.

9. Билет 9

9.1. 1. Аналоговая модуляция. Цифровое кодирование. 2.Бюджет канала связи. Помехи в городских условиях. Наличие препятствий и соответствующие потери.

9.1.1. Из расписки билетов

1. http://solidstate.karelia.ru/p/tutorial/informatics/chapter4/9/3.html
2. https://wl.unn.ru/materials/courses/wlnet/Lect/2_Lect_1_2.pdf

Страницы:

Бюджет канала связи - 4-7.

Помехи в городскиъ условиях - 13. (в принципе помехой является любое другое устройство, вещающее на той же частоте)

Наличие препятсвий и соответстующие потери - 20-25.

9.1.2. Из поисков в интернете

9.1.2.1. Аналоговая модуляция. Аналоговая модуляция - это процесс изменения параметров непрерывного аналогового сигнала (например, звуковой волны), чтобы он мог передаваться через канал связи, который обычно предназначен для передачи других типов сигналов (например, электромагнитных волн).

Существует несколько типов аналоговой модуляции, включая амплитудную модуляцию (АМ), частотную модуляцию (ЧМ) и фазовую модуляцию (ФМ).

Амплитудная модуляция (АМ) изменяет амплитуду высокочастотного несущего сигнала в соответствии с изменением амплитуды модулирующего сигнала. Это позволяет кодировать информацию модулирующего сигнала в высокочастотном несущем сигнале. Приемник демодулирует высокочастотный несущий сигнал и восстанавливает информацию модулирующего сигнала.

Частотная модуляция (ЧМ) изменяет частоту высокочастотного несущего сигнала в соответствии с изменением амплитуды модулирующего сигнала. Это также позволяет кодировать информацию модулирующего сигнала в высокочастотном несущем сигнале. Приемник демодулирует высокочастотный несущий сигнал и восстанавливает информацию модулирующего сигнала.

Фазовая модуляция (ФМ) изменяет фазу высокочастотного несущего сигнала в соответствии с изменением амплитуды модулирующего сигнала. Это также позволяет кодировать информацию модулирующего сигнала в высокочастотном несущем сигнале. Приемник демодулирует высокочастотный несущий сигнал и восстанавливает информацию модулирующего сигнала.

Аналоговая модуляция широко используется в радиосвязи, телевизионном вещании, аудиозаписи и других областях передачи сигналов. Однако она имеет ряд ограничений, включая ограниченный диапазон частот и подверженность помехам и искажениям в канале связи.

9.1.2.2. Цифровое кодирование. Цифровое кодирование – это процесс преобразования аналогового сигнала в цифровой вид с целью передачи или хранения данных. Для этого аналоговый сигнал дискретизируется, т.е. разбивается на отдельные отсчеты (сэмплы) с определенным интервалом, и каждый отсчет кодируется в цифровой код.

Существует несколько типов цифрового кодирования, включая двоичное, кватернионное, восьмеричное, шестнадцатеричное и другие. Для большинства цифровых приложений наиболее распространенным является двоичное кодирование, в котором каждый отсчет представлен битом со значением 0 или 1.

Одним из основных преимуществ цифрового кодирования является его устойчивость к помехам. Цифровой сигнал можно восстановить после передачи или хранения с намного меньшими ошибками, чем аналоговый сигнал, который подвержен влиянию шумов и искажений. Кроме того, цифровое кодирование позволяет использовать более эффективные методы сжатия данных, что может существенно сократить объем передаваемой информации.

Однако цифровое кодирование также имеет некоторые недостатки. Во-первых, его реализация требует дополнительных вычислительных ресурсов и более сложной техники, чем аналоговое кодирование. Во-вторых, цифровой сигнал более чувствителен к задержкам, вызываемым обработкой данных, что может привести к задержкам при передаче или обработке сигнала.

9.1.2.3. Бюджет канала связи. Бюджет канала связи - это оценка эффективности передачи сигнала от передатчика к приемнику, учитывающая все потери и усиления сигнала на пути передачи. Она включает в себя несколько параметров, таких как мощность передачи, чувствительность приемника, уровень шума и потери сигнала в кабелях и антеннах.

Общий бюджет канала связи рассчитывается как разность между мощностью передатчика и суммарными потерями сигнала на пути передачи до момента приема сигнала приемником. Чем выше бюджет канала связи, тем лучше будет качество передачи и меньше вероятность ошибок приема.

Одним из основных факторов, влияющих на бюджет канала связи, является аттенюация сигнала, которая происходит при прохождении сигнала через различные среды передачи, такие как воздух, кабели, препятствия и т.д. Другими факторами являются уровень шума, качество антенн, мощность передатчика и чувствительность приемника.

Для обеспечения эффективной передачи сигнала необходимо учитывать все параметры, влияющие на бюджет канала связи, и выбирать соответствующее оборудование и настройки для оптимальной передачи сигнала в конкретных условиях.

9.1.2.4. Помехи в городских условиях. Городские условия являются одними из самых сложных для передачи данных из-за большого количества помех, которые могут возникнуть. Некоторые из основных видов помех, которые могут возникнуть в городских условиях, включают в себя:

- Многолучевое распространение (multipath propagation) - это явление, при котором сигналы, излучаемые передатчиком, могут достигать приемника несколькими различными путями, что может привести к интерференции и снижению качества сигнала.
- Шумы и помехи от электронного оборудования - городские условия могут быть очень шумными из-за большого количества электронного оборудования, такого как сигналы от сотовых телефонов, микроволновых печей, электрических линий передачи и т.д. Это может вызывать помехи на сигнале.
- Препятствия на пути распространения сигнала - здания, стены, деревья и другие препятствия могут вызвать ослабление и рассеивание сигнала.
- Интерференция сигналов от других устройств - если в окрестности находятся другие устройства, которые работают на той же частоте, что и ваше устройство, это может привести к интерференции и снижению качества сигнала.

Для борьбы с этими помехами и повышения надежности передачи данных в городских условиях используются различные технологии, такие как алгоритмы коррекции ошибок, многолучевая передача с разнесением по времени, антенны с узкой направленностью и другие техники.

9.1.2.5. Наличие препятствий и соответствующие потери. Наличие препятствий на пути распространения радиоволн может привести к значительным потерям сигнала. Типы препятствий могут включать в себя здания, деревья, горы, металлические конструкции и т.д.

Возможные потери связаны с различными факторами, такими как дифракция, отражение, поглощение, рассеяние и интерференция.

Дифракция возникает, когда волна проходит вокруг угла объекта и огибает его. Это приводит к излучению волн в разных направлениях и снижению уровня сигнала на приемнике.

Отражение происходит, когда волна отражается от поверхности и направляется к приемнику. В этом случае могут возникать отраженные волны, которые могут привести к интерференции и дополнительным потерям сигнала.

Поглощение связано с поглощением энергии волны материалом на ее пути, таким образом, уровень сигнала уменьшается.

Рассеяние включает в себя случайное изменение направления движения волны из-за рассеяния на поверхности препятствия. Это может привести к уменьшению уровня сигнала и ухудшению качества связи.

Интерференция возникает, когда два или более сигналов пересекаются в точке приема и могут взаимодействовать между собой, что может привести к ухудшению качества связи.

Все эти факторы могут привести к снижению уровня сигнала и ухудшению качества связи в городских условиях. Поэтому важно учитывать потери при проектировании и строительстве сетей связи.

10. Билет 10

10.1. 1.Транспортные и сетевые протоколы. Назначение коммутаторов, маршрутизаторов, шлюзов. 2.Классификация технологий передачи данных в IoT.

10.1.1. Из расписок билетов

"1. Протоколы транспортного уровня: DCCP (подпротокол), RUDP (подпротокол), SCTP (подпротокол), TCP (основной), UDP (основной), UDP Lite (подпротокол) (нужны для транспортировки пакетов от источника к получаетлю Протоколы сетевого уровня: IPv4/IPv6, Internet Protocol DVMRP, Distance Vector Multicast Routing Protocol, ICMP, Internet Control Message Protocol IGMP, Internet Group Management Protocol , PIM-SM, Protocol Independent Multicast Sparse Mode, IPsec, Internet Protocol Security, IPX, Internetwork Packet Exchange, RIP, Routing Information Protocol,DDP, Datagram Delivery Protoco. Позволябт достигнуть сетевой связности и маршрутизации

Коммутаторы объединяют устройства в рамках подсети, при этом ведя таблицу MAC адресов и адресуя пакеты от источника к получателю (если они известны). Маршрутизаторы позволяют объединить несколько подсетей и передавать пакеты между ними, также позволяют достигнуть связи с внешним миром. Шлюзы нужны для объединения с внешним миром, на данный момент практически не используются

2. (да, когда мне прислали ссылку с комментарием смотрите, на слайд из вашей лекции ссылаются , я сразу же решил уточнить - на первый или все-таки на второй) (и еще комментарий - могу примерно половину вопросов тут гораздо более грамотно заполнить, но мне лень)

* LPWAN, Low-power Wide Area Network

I Скорость передачи не важна (сотни, редко тысячи бит/с), требуется большая зона покрытия

I UNB-сети (Sigfox, NB-Fi и подобные), LoRa/LoRaWAN, в некоторой степени — NB-IoT

I Частотный диапазон Sub 1-GHz (433 или 868/915 МГц)

I LR-WPAN, Low-rate Wireless Personal Area Network

I Скорость передачи относительно мала (до 250 кбит/с)

I IEEE 802.15.4, BLE, IEEE 802.11ah

I Частотный диапазон ISM (2,4 ГГц) или Sub 1-GHz

I «Вне зачета» — традиционные беспроводные технологии: WiFi

(IEEE 802.11), Bluetooth, Bluetooth Low Energy, сотовая связ"

10.1.2. Из поисков в интернете

10.1.2.1. Транспортные и сетевые протоколы. Транспортные и сетевые протоколы являются ключевыми элементами в построении сетевой инфраструктуры. Они обеспечивают передачу данных от источника к назначению, выполняя различные функции на разных уровнях сетевой модели OSI.

Один из основных транспортных протоколов - это TCP (Transmission Control Protocol), который обеспечивает надежную передачу данных между двумя приложениями, используя механизмы управления потоком и обнаружения ошибок. TCP работает на транспортном уровне модели OSI и является основным протоколом для передачи данных в Интернете.

Еще один транспортный протокол - UDP (User Datagram Protocol), который также работает на транспортном уровне модели OSI. UDP не обеспечивает надежную передачу данных, но обладает меньшей задержкой передачи и использование его возможно в случаях, когда небольшие задержки являются критическими.

Сетевые протоколы, в свою очередь, используются для передачи данных между узлами сети и обеспечивают правильную адресацию и маршрутизацию данных. Наиболее распространенным сетевым протоколом является IP (Internet Protocol), который работает на сетевом уровне модели OSI и обеспечивает адресацию и маршрутизацию пакетов данных в Интернете.

Также существует множество других протоколов, в том числе протоколы маршрутизации (например, OSPF и BGP), протоколы динамической конфигурации сети (например, DHCP) и протоколы управления сетью (например, SNMP). Все они выполняют свои специфические функции, необходимые для эффективной работы сети.

10.1.2.2. Назначение коммутаторов, маршрутизаторов, шлюзов. Коммутаторы, маршрутизаторы и шлюзы - это сетевые устройства, которые выполняют разные функции в компьютерных сетях.

Коммутаторы, также называемые сетевыми переключателями, обычно используются в локальных сетях (LAN) для соединения компьютеров и других сетевых устройств, таких как принтеры, серверы и хранилища данных. Коммутаторы работают на канальном уровне OSI-модели и используют адресацию

MAC для доставки данных внутри сети. Они обеспечивают передачу данных только тем устройствам, которые являются получателями, что снижает загрузку сети и повышает ее производительность.

Маршрутизаторы, с другой стороны, обычно используются для соединения разных сегментов сети и позволяют устройствам из разных сетей общаться друг с другом. Маршрутизаторы работают на сетевом уровне OSI-модели и используют IP-адресацию для доставки данных. Они выбирают оптимальный маршрут для передачи данных между разными сетями и могут выполнять различные функции, такие как фильтрация трафика и управление пропускной способностью.

Шлюзы - это сетевые устройства, которые используются для соединения разных сетей, которые могут работать с разными протоколами. Например, шлюз может соединять локальную сеть с сетью Интернет, или две локальные сети, использующие разные протоколы. Шлюзы работают на прикладном уровне OSI-модели и могут выполнять функции, такие как преобразование протоколов, обеспечение безопасности и фильтрация трафика.

В целом, коммутаторы, маршрутизаторы и шлюзы выполняют разные функции, но вместе они обеспечивают эффективную работу сети и обеспечивают передачу данных между разными устройствами и сетями.

10.1.2.3. Классификация технологий передачи данных в IoT. Существует несколько классификаций технологий передачи данных в IoT, одна из них основана на дальности передачи данных, а другая - на используемой технологии связи.

Классификация по дальности передачи данных:

- WPAN (Wireless Personal Area Network) - беспроводные сети персональной области. Эти сети предназначены для обмена данными на небольших расстояниях (до 10 метров) и используются, например, для соединения устройств, расположенных внутри одного помещения. Примеры технологий WPAN: Bluetooth, Zigbee, Z-Wave.

- WLAN (Wireless Local Area Network) - беспроводные локальные сети. Эти сети предназначены для обмена данными на средних расстояниях (до нескольких сотен метров) и используются, например, для подключения устройств к Интернету в зданиях и на территориях, охватываемых одной точкой доступа. Примеры технологий WLAN: Wi-Fi.

- WMAN (Wireless Metropolitan Area Network) - беспроводные городские сети. Эти сети предназначены для обмена данными на больших расстояниях (до нескольких километров) и используются, например, для организации беспроводного доступа в Интернет в городах. Примеры технологий WMAN: WiMAX.

- WWAN (Wireless Wide Area Network) - беспроводные сети широкой области покрытия. Эти сети предназначены для обмена данными на больших расстояниях (до нескольких десятков километров) и используются, например, для организации беспроводного доступа в Интернет в областях с низкой плотностью населения. Примеры технологий WWAN: 2G/3G/4G/LTE, NB-IoT, LoRa, Sigfox.

Классификация по используемой технологии связи:

- Беспроводные технологии связи - используются радиоволны для передачи данных. Примеры технологий: Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, Sigfox.

- Сети мобильной связи - используются мобильные сети операторов связи для передачи данных. Примеры технологий: 2G/3G/4G/LTE, NB-IoT.

- Кабельные технологии связи - используются кабели для передачи данных. Примеры технологий: Ethernet, USB, HDMI, RS-485.

Классификация по типу соединения:

- Прямое соединение - устройства подключаются друг к другу непосредственно с помощью кабеля или беспроводного соединения, без участия других устройств.

- Соединение через центральный узел - устройства подключаются к центральному узлу (коммутатору, маршрутизатору, контроллеру), который обеспечивает передачу данных между ними.

Классификация по масштабу:

- Локальные сети (LAN) - используются для связи устройств внутри ограниченной территории, например, в здании или на территории предприятия.

- Глобальные сети (WAN) - используются для связи устройств на больших расстояниях, включают в себя Интернет и сети операторов связи.
- Персональные сети (PAN) - используются для связи устройств вблизи пользователя, например, между смартфоном и наушниками или между планшетом и клавиатурой.

Классификация по топологии сети:

- Звездообразная - все устройства подключены к центральному узлу (коммутатору, маршрутизатору, контроллеру).
- Шина - все устройства подключены к одной линии связи, которая является шиной.
- Кольцо - устройства подключены последовательно в кольцо.
- Смешанная - сочетание нескольких типов топологий в одной сети.

11. Билет 11

11.1. 1.Алгоритмы маршрутизации Беллмана-Форда и OSPF. Протоколы маршрутизации глобальных компьютерных сетей. 2.Стандарты IEEE 802.11, IEEE 802.15, IEEE 802.16, условно закрытые и условно открытые стандарты передачи данных Интернета вещей.

11.1.1. Из расписки билетов

"1. Алгоритм Беллмана — Форда — алгоритм поиска кратчайшего пути во взвешенном графе, в маршрутизации он используется под названием RIP и является одним из самых простых и старых протоколов маршрутизации. RIP - это дистанционно-векторный протокол, а это значит, что маршрутизаторы в сети периодически широковещательно рассылают информацию о расстоянии от данного маршратизатора до других. Максимальное количество транзитных участков (переходов) равно 15, что достаточно мало, поэтому протокол если где-то и используется, то только для небольших компьютерных сетей. Первая версия протокола считается устаревшей и вместо её используется RIPv2, которая позволяет передавать дополнительную муршрутную информацию и в целом более безопасна. Более современным по сравнению с RIP является протокол OSPF. Он более оптимален в плане использования пропускной способности для построения кратчайших путей, максимальное количество транзитных участков намного больше 15, а также поддерживает бесклассовую адресацию (это когда маска подсети имеет переменную длину).

2. IEEE 802 — группа стандартов семейства IEEE, касающихся локальных вычислительных сетей (LAN) и сетей мегаполисов (MAN).

- 802.11 - WIFI.
- 802.15 - WPAN (Беспроводные персональные сети), используется для Bluetooth, ZigBee, 6loWPAN.
- 802.16 - WMAN (беспроводные сети масштаба города. Предоставляют широкополосный доступ к сети через радиоканал.)"

11.1.2. Из поисков в интернете

11.1.2.1. Алгоритмы маршрутизации Беллмана-Форда и OSPF. Алгоритм Беллмана-Форда и протокол OSPF (Open Shortest Path First) - это два разных подхода к маршрутизации в компьютерных сетях.

Алгоритм Беллмана-Форда - это алгоритм динамической маршрутизации, который используется для нахождения кратчайшего пути между двумя узлами в графе, в котором ребра могут иметь отрицательные веса. Алгоритм Беллмана-Форда на каждой итерации обновляет расстояние от начальной точки до каждой вершины в графе, используя информацию о расстояниях до всех соседних вершин. Алгоритм выполняется до тех пор, пока расстояния до вершин перестают изменяться.

Протокол OSPF - это протокол маршрутизации для IP-сетей, который использует алгоритм Dijkstra для нахождения кратчайшего пути между узлами. OSPF работает на уровне сети и обеспечивает быстрое переключение на новый маршрут в случае обрыва существующего. OSPF также обеспечивает поддержку различных типов сервиса качества обслуживания (QoS) и различных путей маршрутизации для разных типов трафика.

Основное отличие между алгоритмом Беллмана-Форда и протоколом OSPF заключается в том, что OSPF использует более сложный алгоритм маршрутизации, который обеспечивает более эффективную и надежную работу в сети. Однако алгоритм Беллмана-Форда может быть использован в сетях с более простой топологией, где нет необходимости в более сложных алгоритмах маршрутизации.

11.1.2.2. Протоколы маршрутизации глобальных компьютерных сетей. Существует несколько протоколов маршрутизации для глобальных компьютерных сетей, которые обеспечивают маршрутизацию между различными автономными системами (AS).

Один из наиболее распространенных протоколов - это Border Gateway Protocol (BGP). BGP является протоколом, используемым для обмена маршрутной информацией между различными AS, чтобы определить наилучший путь для передачи данных между ними. BGP также обеспечивает возможность балансировки нагрузки и предотвращения возможных петель маршрутизации.

Еще одним протоколом маршрутизации глобальных компьютерных сетей является Open Shortest Path First (OSPF). OSPF также используется для определения наилучшего маршрута между различными AS. Однако, в отличие от BGP, OSPF работает только внутри одной AS и обычно используется для определения наилучшего маршрута между различными узлами внутри AS. OSPF также предоставляет более

эффективную маршрутизацию и балансировку нагрузки, чем стандартные протоколы маршрутизации, такие как RIP и IGRP.

Другим протоколом маршрутизации глобальных компьютерных сетей является Intermediate System-to-Intermediate System (IS-IS). Этот протокол, как и OSPF, также используется для маршрутизации внутри одной AS, но он предлагает более высокую скорость передачи данных и меньшие задержки, чем OSPF. IS-IS также обеспечивает более эффективное использование сетевых ресурсов и предоставляет возможность балансировки нагрузки между различными узлами внутри AS.

В целом, эти протоколы маршрутизации обеспечивают эффективную передачу данных между различными узлами внутри и между различными автономными системами, что делает их важными для глобальных компьютерных сетей.

11.1.2.3. Стандарты IEEE 802.11, IEEE 802.15, IEEE 802.16, условно закрытые и условно открытые стандарты передачи данных Интернета вещей. IEEE 802.11, IEEE 802.15 и IEEE 802.16 - это стандарты передачи данных по беспроводным сетям, которые также могут использоваться для передачи данных в Интернете вещей.

Стандарт IEEE 802.11, также известный как Wi-Fi, используется для передачи данных в беспроводных локальных сетях. Он поддерживает скорости передачи данных от 1 Мбит/с до 10 Гбит/с и работает в диапазоне частот от 2,4 ГГц до 5 ГГц. Wi-Fi также имеет множество различных стандартов, таких как 802.11b, 802.11g, 802.11n, 802.11ac и 802.11ax, которые имеют различные скорости передачи данных и диапазоны частот.

Стандарт IEEE 802.15, известный как Zigbee, используется для создания маломощных беспроводных сетей с низкой скоростью передачи данных. Он работает на частоте 2,4 ГГц и использует малоэнергетичную технологию передачи данных, что позволяет устройствам работать на батарейной энергии в течение длительного времени. Zigbee может использоваться для передачи данных в различных областях, таких как домашняя автоматизация, умный город и промышленность.

Стандарт IEEE 802.16, известный как WiMAX, используется для передачи данных в беспроводных глобальных сетях. Он работает на частоте от 2 ГГц до 66 ГГц и поддерживает скорости передачи данных до 1 Гбит/с на расстоянии до 50 км. WiMAX используется в различных областях, таких как широкополосный доступ в Интернет, мобильная связь и транспорт.

Условно закрытые стандарты передачи данных - это стандарты, которые разработаны и поддерживаются определенными компаниями и могут использоваться только с их оборудованием. Например, стандарты Thread и HomeKit разработаны компанией Apple для использования в своих устройствах умного дома.

Условно открытые стандарты передачи данных - это стандарты, которые разработаны сообществом и открыты для использования любыми компаниями и устройствами. Например, стандарты MQTT и CoAP открыты для использования в любых устройствах IoT.

12. Билет 12

12.1. 1.Криптография. Симметричный ключ. Ассиметричный ключ. Криптографический хеш (аутентификация и цифровая подпись). 2.Роль консорциумов(промышленные) и сообществ в IoT. Отраслевые стандарты.

12.1.1. Расписка из билета

А не расписали, а всё

12.1.2. Мои поиски в интернете

12.1.2.1. Криптография. Симметричный ключ. Ассиметричный ключ. Криптографический хеш (аутентификация и цифровая подпись). Криптография - это наука о методах защиты информации. Криптография включает в себя различные методы и технологии, которые позволяют защищать данные от несанкционированного доступа, подделки и внесения изменений.

Симметричный ключ - это метод криптографии, при котором для шифрования и расшифровки информации используется один и тот же ключ. Такой метод шифрования называется симметричным, потому что ключ, используемый для шифрования, такой же, как и ключ, используемый для расшифровки.

Асимметричный ключ - это метод криптографии, при котором используются два ключа: открытый и закрытый. Открытый ключ известен всем, кто хочет отправить сообщение, а закрытый ключ известен только получателю. Шифрование происходит с помощью открытого ключа, а расшифровка - с помощью закрытого.

Криптографический хеш - это математический алгоритм, который принимает входные данные любой длины и генерирует выходные данные фиксированной длины. Криптографический хеш используется для обеспечения аутентификации и целостности данных. Хеш может быть использован для создания цифровой подписи или для проверки целостности данных.

Аутентификация - это процесс проверки подлинности участника коммуникации. Цифровая подпись - это метод аутентификации, при котором используется криптографический хеш, который создается отправителем данных с использованием его закрытого ключа. Получатель данных может проверить подлинность данных, используя открытый ключ отправителя и проверяя цифровую подпись, созданную отправителем.

12.1.2.2. Роль консорциумов(промышленные) и сообществ в IoT. В области IoT консорциумы и сообщества играют важную роль в разработке стандартов, регулировании рынка и продвижении новых технологий.

Промышленные консорциумы объединяют компании из разных отраслей, чтобы совместно работать над развитием стандартов, решений и продуктов в области IoT. Это позволяет ускорить разработку и внедрение новых технологий, а также обеспечить совместимость между разными устройствами и системами. Примеры промышленных консорциумов в области IoT: Industrial Internet Consortium, LoRa Alliance, Open Connectivity Foundation, Zigbee Alliance.

Сообщества также играют важную роль в развитии IoT, особенно в отношении открытых исходных кодов и проектов. Они объединяют людей, увлеченных технологиями IoT, для обмена опытом, разработки новых решений и продвижения открытых стандартов. Примеры сообществ в области IoT: Eclipse IoT, OpenSensors, The Things Network.

Кроме того, консорциумы и сообщества также являются платформами для общественной дискуссии и регулирования рынка IoT. Они могут способствовать разработке правил и стандартов для обеспечения безопасности, конфиденциальности и защиты потребителей.

12.1.2.3. Отраслевые стандарты. Отраслевые стандарты в Интернете вещей (IoT) являются набором правил, рекомендаций и спецификаций, которые разрабатываются отраслевыми организациями и регуляторными органами для обеспечения совместимости и безопасности устройств и приложений IoT. Они определяют требования к устройствам, протоколам связи, безопасности и другим аспектам IoT.

Вот некоторые известные отраслевые стандарты в области IoT:

- Zigbee: Zigbee Alliance разрабатывает стандарт Zigbee для беспроводной сети датчиков и управления устройствами на коротких расстояниях. Этот стандарт использует радиочастоты на диапазоне 2,4 ГГц для связи устройств.
- Z-Wave: Z-Wave Alliance разрабатывает стандарт Z-Wave для беспроводной сети домашней автоматизации на коротких расстояниях. Этот стандарт использует радиочастоты на диапазоне 900 МГц для связи устройств.

- Bluetooth: Bluetooth Special Interest Group (SIG) разрабатывает стандарт Bluetooth для беспроводной связи на коротких расстояниях. Этот стандарт использует радиочастоты на диапазоне 2,4 ГГц для связи устройств.
- LoRaWAN: LoRa Alliance разрабатывает стандарт LoRaWAN для беспроводной сети на длинные расстояния с низким энергопотреблением. Этот стандарт использует радиочастоты на диапазоне 868 МГц и 915 МГц для связи устройств.
- MQTT: OASIS разрабатывает стандарт MQTT для протокола передачи сообщений на машинном уровне. Этот стандарт используется для передачи данных в IoT и других приложениях машинного обучения.
- OPC-UA: Организация OPC Foundation разрабатывает стандарт OPC-UA для промышленной автоматизации и контроля. Этот стандарт используется для передачи данных между устройствами и системами в промышленных приложениях.
- KNX: KNX Association разрабатывает стандарт KNX для домашней автоматизации и управления зданиями. Этот стандарт используется для управления освещением, отоплением, вентиляцией и другими системами в зданиях.
- 6LowPAN: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) - это стандарт, разработанный IETF (Internet Engineering Task Force) для использования протокола IPv6 в беспроводных сенсорных сетях, которые обладают ограниченным ресурсом памяти и процессора. Он позволяет устройствам в беспроводной сети обмениваться данными с другими устройствами, которые находятся в локальной или глобальной сети IPv6.
- Thread: Thread Group разрабатывает стандарт Thread для беспроводной сети домашней автоматизации. Он представляет собой стандартный протокол связи между устройствами IoT и смарт-домами, обеспечивающий совместимость между различными производителями устройств и сетей.
- Sigfox: Sigfox - это условно закрытый стандарт, который использует радиочастотный диапазон ISM для передачи небольших объемов данных на большие расстояния, используя минимальное энергопотребление. Sigfox может быть использован для передачи данных, таких как местоположение, температура, влажность и другие параметры, с помощью множества устройств.
- NB-IoT: Narrowband IoT - это стандарт, разработанный 3GPP (3rd Generation Partnership Project) для передачи данных в IoT по сети мобильной связи. NB-IoT использует радиочастотный диапазон, который обычно используется для GSM и LTE сетей, что обеспечивает обширное покрытие и низкое энергопотребление.

Это лишь некоторые из отраслевых стандартов, которые используются в IoT. Каждый стандарт имеет свои особенности и применяется в определенных сферах.

13. Билет 13

13.1. 1.Ассиметричная криптография (с открытым ключом). Протокол защиты транспортного уровня TLS. 2.Ограниченный протокол приложений (CoAP). Ключевые особенности, сравнение с HTTP (стек протоколов/-технологий по уровням).

13.1.1. Расписка из билета

"1. Криптографическая система с открытым ключом — система, при которой открытый ключ передаётся по открытому, незащищенному каналу и используется для шифрования сообщения, а закрытый ключ остается сохранным и используется для расшифровки сообщения. При такой системе сам механизм генерации и механизмы шифрования остаются общеизвестными, но при этом вычислить за разумный срок закрытый ключ, зная открытый, не представляется возможным.

TLS (англ. transport layer security — Протокол защиты транспортного уровня) — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

2. CoAP, полное название Constrained Application Protocol - протокол ограниченного приложения, разработан для устройств с ограниченными ресурсами (такие как узлы датчиков) и для простейших сетей (таких как NB-loT и LoRa). CoAP разработан на основе HTTP. CoAP работает в режиме запрос / ответ. По сравнению с HTTP, CoAP учитывает как оптимизацию длины пакета данных, так и надежность связи. coAP имеет простой формат пакета, сжатый заголовок и очень короткое сообщение"

13.1.2. Из поисков интернете

13.1.2.1. Ассиметричная криптография (с открытым ключом). Асимметричная криптография (или криптография с открытым ключом) — это метод шифрования, при котором используется пара ключей: открытый и закрытый. Открытый ключ может быть распространен в открытом доступе, в то время как закрытый ключ должен быть известен только владельцу ключа.

Открытый ключ используется для шифрования сообщений, а закрытый ключ — для их расшифровки. Таким образом, при использовании асимметричной криптографии открытый ключ может быть использован безопасным образом для передачи данных, так как никакая третья сторона не сможет расшифровать данные без знания соответствующего закрытого ключа.

Асимметричная криптография широко используется для решения задач аутентификации и цифровой подписи, а также для создания защищенных каналов связи в интернете и других сетях передачи данных. Примерами популярных алгоритмов асимметричной криптографии являются RSA, DSA и ECC.

13.1.2.2. Протокол защиты транспортного уровня TLS. Протокол защиты транспортного уровня (Transport Layer Security, TLS) является криптографическим протоколом, который обеспечивает безопасность передачи данных между двумя узлами в компьютерной сети. TLS используется для защиты веб-трафика, электронной почты, FTP-передач и других приложений, использующих сетевой протокол TCP.

Протокол TLS был разработан на основе его предшественника SSL (Secure Sockets Layer) и включает в себя такие функции, как шифрование данных, аутентификация и цифровые сертификаты. TLS использует симметричную и асимметричную криптографию для обеспечения конфиденциальности, целостности и аутентификации передаваемых данных.

В процессе установки соединения по протоколу TLS, клиент и сервер обмениваются сообщениями для согласования параметров безопасности и аутентификации. Затем они соглашаются на сеансовый ключ, который используется для шифрования данных, передаваемых между ними во время сеанса.

Протокол TLS также поддерживает использование цифровых сертификатов, которые выдаются удостоверяющими центрами и используются для аутентификации серверов и клиентов. Цифровые сертификаты позволяют клиентам убедиться, что они связываются с правильным сервером, а также обеспечивают конфиденциальность передаваемых данных, так как они шифруются с использованием открытого ключа сервера.

В целом, протокол TLS является важным средством обеспечения безопасности в Интернете и используется многими веб-сайтами и приложениями для защиты конфиденциальных данных пользователей.

13.1.2.3. Ограниченный протокол приложений (CoAP). Ограниченный протокол приложений (CoAP) - это протокол прикладного уровня, который используется в Интернете вещей для передачи данных между устройствами и серверами. Он был разработан с целью оптимизации использования сетевых

ресурсов, таких как энергия и пропускная способность, что делает его идеальным для использования в устройствах с ограниченными ресурсами, таких как датчики и устройства умного дома.

CoAP работает поверх протокола UDP, что обеспечивает низкую задержку и минимальную нагрузку на сеть. Протокол поддерживает методы запросов GET, POST, PUT и DELETE, а также определяет специальные параметры и заголовки, которые могут использоваться для передачи дополнительной информации и управления процессом передачи данных.

CoAP также поддерживает аутентификацию и безопасность данных с помощью протокола DTLS (Datagram Transport Layer Security). Это обеспечивает защиту данных в процессе их передачи и предотвращает несанкционированный доступ к устройствам.

Протокол CoAP широко используется в Интернете вещей, включая устройства умного дома, системы автоматизации зданий, медицинские устройства, транспортные системы и другие приложения.

13.1.2.4. Ключевые особенности, сравнение с HTTP (стек протоколов/технологий по уровням). CoAP (Constrained Application Protocol) - это протокол прикладного уровня, который разработан для использования в сетях интернета вещей (IoT). Его основная цель - обеспечение эффективной передачи данных на устройствах с ограниченными ресурсами, таких как датчики и микроконтроллеры.

Основные ключевые особенности CoAP:

- Протокол CoAP использует упрощенную модель запроса-ответа, подобную HTTP, что делает его более легковесным по сравнению с HTTP.
- Он работает поверх протокола UDP (User Datagram Protocol), который является более легковесным, чем TCP (Transmission Control Protocol), используемый HTTP.
- CoAP поддерживает механизмы обнаружения устройств и ресурсов, что позволяет устройствам находить друг друга в сети.
- Он использует формат сообщений, который позволяет передавать данные в упакованном виде, сокращая тем самым объем передаваемых данных.
- CoAP поддерживает управление кешем, что позволяет сократить нагрузку на сеть и уменьшить время задержки при передаче данных.

Сравнение с HTTP:

- HTTP использует протокол TCP, который обеспечивает надежную передачу данных, но затратен по ресурсам и неэффективен для устройств с ограниченными ресурсами.
- CoAP использует протокол UDP, который является более легковесным, чем TCP, и обеспечивает более быструю передачу данных, но менее надежную, чем TCP.
- HTTP использует более сложную модель запроса-ответа, чем CoAP, что делает его более громоздким и неэффективным для устройств с ограниченными ресурсами.
- CoAP поддерживает механизмы обнаружения устройств и ресурсов, что не поддерживается в HTTP.
- CoAP позволяет передавать данные в упакованном виде, что позволяет сократить объем передаваемых данных и снизить нагрузку на сеть.
- HTTP не поддерживает управление кешем, что делает его менее эффективным для передачи данных в сетях с большим количеством устройств.

14. Билет 14

14.1. 1.Топология облачных и туманных вычислений. Модель облачных сервисов (XaaS, NaaS, SaaS, IaaS). 2.RFID и NFC технологии. Ключевые особенности, принципы.

14.1.1. Расписка билетов

Как облачные, так и туманные вычисления предоставляют конечным пользователям возможность хранения данных и управление ими с помощью приложений. Тем не менее, туманные вычисления находятся «ближе» к конечным пользователям и имеют более широкое географическое распространение. Само определение «туманные вычисления» призвано указать на дополнительный уровень архитектуры сети данных, который расположен структурно «ниже» облачных вычислений, по аналогии с облаками и туманом, явление которого можно наблюдать близко к земле.

«Облачные вычисления» — это практика использования сети удаленных серверов, размещенных в Интернете, для хранения, управления и обработки данных, а не локальных сервисов или персональных компьютеров. Облачные вычисления, в ряде случаев, отличаются большей вычислительной мощностью и максимальной плотностью обрабатываемых потоков данных.

Туманные вычисления облегчают работу сервисов обработки и хранения информации, а также сетевых служб, осуществляющих взаимосвязь между конечными устройствами и дата-центрами, использующими облачные технологии; они выступают в качестве дополнительного уровня сбора и обработки информации. Обычно туманные вычисления рассматривают как дополнительную часть инфраструктуры облачных вычислений.

SaaS (англ. Software-as-a-Service) – ПО как сервис, подразумевает использование клиентом приложений, развернутых на платформе провайдера. Пользователь SaaS получает готовое решение, которое остается только применить. Многие примеры SaaS-решений вам наверняка будут знакомы: Gmail, Jira, Bitrix, WordPress.

IaaS (англ. Infrastructure-as-a-Service) – модель облачных вычислений, которая включает в себя все основы: серверную инфраструктуру, коммуникации, хранилища и т.д. В эту услугу входит сама облачная инфраструктура и обслуживание аппаратуры - поддержкой занимается IaaS-провайдер. В рамках модели IaaS клиент получает вычислительные мощности облака; на базе этой инфраструктуры строятся программные решения.

XaaS - anything-as-a-Service - общее определение для моделей облачных технологий, которые предоставляются пользователю в аренду; разница между ними заключается в уровне решаемых задач. В него входят все из вышеперечисленных вариантов моделей.

2. Технологии ближней бесконтактной связи (NFC) и радиочастотной идентификации (RFID) используются для обмена данными с помощью радиоволн. RFID метки (теги) содержат антенну и чип в котором хранятся данные. RFID-технология представляет собой метод идентификации с использованием радиоволн разного диапазона (от средних до сверхвысоких), в то время как NFC – это специализированный подвид RFID, работающий только на высоких частотах. Он разработан для эффективной связи на очень маленьком расстоянии и лежит в основе бесконтактных платежей, совершаемых с помощью смартфона. RFID-метки (теги) содержат антенну и чип, в котором хранятся данные. Чтобы увидеть данные, потребуется RFID считыватель.

14.1.2. Из поисков в интернете

14.1.2.1. Топология облачных и туманных вычислений. Облачные вычисления и вычисления тумана (fog computing) представляют собой различные модели обработки данных и вычислений, используемые в современных сетевых системах.

Топология облачных вычислений предполагает наличие удаленного облачного центра обработки данных, к которому могут подключаться клиенты через Интернет. Этот центр хранит и обрабатывает данные, а клиенты получают к ним доступ через сеть. В топологии облачных вычислений обычно используется модель клиент-сервер, где клиенты обращаются к серверу для получения необходимых данных.

С другой стороны, топология вычислений тумана предполагает наличие распределенной инфраструктуры для обработки данных и вычислений. Эта инфраструктура может включать в себя устройства IoT, локальные серверы и облачные центры, которые работают вместе для обработки и анализа данных. Вычисления тумана предоставляют возможность обработки данных ближе к их источникам, что уменьшает задержки и улучшает отзывчивость системы.

Топология вычислений тумана также может использоваться для решения проблем, связанных с ограниченной пропускной способностью сети и большим количеством данных. В этом случае, данные могут

обрабатываться на локальных устройствах, а только необходимая информация отправляется на удаленный сервер для дальнейшей обработки.

Сравнение топологий облачных вычислений и вычислений тумана показывает, что вычисления тумана предоставляют более децентрализованную и гибкую инфраструктуру для обработки данных и вычислений, в то время как облачные вычисления предоставляют более централизованный подход, с высокой масштабируемостью и отказоустойчивостью. Обе топологии имеют свои преимущества и недостатки, и могут использоваться в зависимости от требований конкретного приложения.

14.1.2.2. Модель облачных сервисов (XaaS, NaaS, SaaS, IaaS) Модель облачных сервисов - это способ предоставления различных уровней информационных технологий через интернет, используя облачные вычисления. Она включает в себя несколько типов облачных сервисов, которые могут быть предоставлены пользователям в зависимости от их потребностей. Ниже приведены основные типы облачных сервисов:

- IaaS (Infrastructure-as-a-Service) - это модель, при которой пользователи получают доступ к облачной инфраструктуре, такой как серверы, хранилища данных, виртуальные машины, сетевые устройства и т.д. Пользователи могут управлять этой инфраструктурой, устанавливать и настраивать операционные системы и приложения, а также масштабировать ресурсы по мере необходимости.

- PaaS (Platform-as-a-Service) - это модель, при которой пользователи получают доступ к облачной платформе для разработки, тестирования и развертывания приложений. Платформа может включать в себя такие сервисы, как языки программирования, средства разработки, базы данных, веб-серверы, хостинг и т.д. Пользователи могут разрабатывать и развертывать свои приложения на платформе, не беспокоясь о инфраструктуре, на которой они работают.

- SaaS (Software-as-a-Service) - это модель, при которой пользователи получают доступ к облачным приложениям через интернет. Это могут быть программы для офисных задач, системы управления отношениями с клиентами, учетные системы, веб-сервисы и т.д. Пользователи могут использовать приложения без необходимости устанавливать их на своих устройствах или управлять инфраструктурой, на которой они работают.

- NaaS (Network-as-a-Service) - это модель, при которой пользователи получают доступ к облачной сетевой инфраструктуре через интернет. Это могут быть такие сервисы, как виртуальные частные сети, брандмауэры, балансировщики нагрузки, маршрутизаторы и т.д. Пользователи могут настраивать и управлять сетевыми ресурсами, используя облачную платформу.

- XaaS (Anything-as-a-Service) - это модель, при которой предоставляются другие типы облачных сервисов, такие как DaaS (Data-as-a-Service), FaaS (Function-as-a-Service), CaaS (Container-as-a-Service), DBaaS (Database-as-a-Service), и т.д. Каждый из этих сервисов предоставляет управляемый доступ к определенному типу данных, функциональности или ресурсам, которые могут быть использованы на основе потребностей пользователей.

- DaaS (Data-as-a-Service) - это модель, при которой предоставляется доступ к облачным хранилищам данных и инструментам для управления данными. Пользователи могут загружать, хранить, обрабатывать и анализировать данные, используя облачные сервисы.

- FaaS (Function-as-a-Service) - это модель, при которой предоставляется возможность разработки и выполнения кода функций в облачной среде. Пользователи могут разрабатывать и загружать функции в облачную среду, а облачный провайдер автоматически масштабирует ресурсы для выполнения функций.

- CaaS (Container-as-a-Service) - это модель, при которой предоставляется возможность разработки, управления и развертывания контейнеров в облачной среде. Пользователи могут использовать контейнеры для запуска приложений в изолированной среде, а облачный провайдер управляет инфраструктурой, необходимой для выполнения контейнеров.

- DBaaS (Database-as-a-Service) - это модель, при которой предоставляется управляемый доступ к облачным базам данных. Пользователи могут создавать и управлять базами данных, а облачный провайдер управляет инфраструктурой, необходимой для хранения и обработки данных.

В сравнении с IaaS, PaaS и SaaS, XaaS модель более гибкая и адаптивная к различным потребностям пользователей, так как она предоставляет широкий спектр сервисов, которые могут быть использованы в зависимости от конкретных требований. Однако, эта гибкость также может привести к большей сложности в выборе и управлении различными сервисами.

14.1.2.3. RFID и NFC технологии. Ключевые особенности, принципы. RFID (Radio-Frequency Identification) и NFC (Near Field Communication) - это беспроводные технологии, которые используются для идентификации и обмена данными между устройствами. Обе технологии используют радиочастотную связь, но имеют некоторые различия в принципах работы и применении.

Основные принципы работы RFID:

- RFID-метка (тег) содержит микросхему и антенну, которые позволяют ей принимать и передавать радиосигналы на определенной частоте.
- Радиочастотные считыватели считывают данные с метки, используя радиочастотную связь.
- RFID-системы могут использоваться для автоматической идентификации объектов, контроля инвентаризации, управления складом и логистики, а также для безопасности и аутентификации.

Основные принципы работы NFC:

- NFC-технология использует магнитное поле для передачи данных между устройствами.
- Устройства должны быть на расстоянии не более 4 см друг от друга для передачи данных.
- NFC-технология может использоваться для мобильных платежей, передачи данных между устройствами, идентификации и аутентификации, а также для управления умным домом.

Несмотря на то, что обе технологии используют беспроводную связь, они имеют некоторые различия в применении. RFID-технология, как правило, используется для автоматизации бизнес-процессов и управления логистикой, тогда как NFC-технология используется для удобства пользователей, таких как мобильные платежи и передача данных между устройствами.

Однако, NFC также может быть использована в бизнес-процессах, например, для облегчения взаимодействия между устройствами и проведения быстрого обмена данными между ними.