Инфа для меня

Каждый уровень модели OSI взаимодействует с другими уровнями для того, чтобы воспользоваться представляемыми ими **службами**. Эти службы дают возможность определённому уровню OSI взаимодействовать с таким же уровнем другой компьютерной системы. Говоря о службах уровней, необходимо дать определение трем базовым элементам: пользователь службы, провайдер службы и точка доступа к службе.

**Пользователь службы** – это уровень OSI, который запрашивает службы смежного уровня OSI. **Провайдер службы** – это уровень OSI, предоставляющий пользователю доступ к службе. Уровни OSI могут предоставлять службы нескольким пользователям.

**Точка доступа к службе** является тем уровнем, на котором один уровень OSI может запрашивать службы другого уровня.

Актуалочка:

**Эталонная модель OSI. Эталонная модель TCP/IP. Критика эталонных моделей OSI и TCP/IP. Гибридная модель.**

**Перечислите уровни эталонной модели OSI. Поясните, для чего предназначен каждый уровень.**

**Изложите принципы организации уровней эталонной модели OSI.**

**Определите службы физического уровня модели OSI. Изложите принципы кодирования сигналов: уровнем, амплитудная, частотная, амплитудно-частотная модуляция, манчестерское кодирование.**

**Определите службы канального уровня модели OSI. Изложите принципы, лежащие в основе методов обнаружения и исправления ошибок в кодовых комбинациях.**

**Изложите принципы фрагментации и сборки дейтаграмм в протоколе IP версии 4.**

**Изобразите схему внутреннего устройства маршрутизатора. (Схемы нет но есть описание)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Эталонная модель OSI**  Эталонная модель OSI представляет собой сетевую модель передачи данных, представленных в цифровом формате, описывающую способ передачи данных от источника информации к получателю. Модель описывает различные уровни, через которые проходит информация, каждый из которых описывается некоторым правилом или протоколом передачи.   |  |  |  | | --- | --- | --- | | Прикладной | HTTP, SMTP, DNS, FTP, SSH, итд | обеспечивает взаимодействие пользовательских приложений с сетью. | | Уровень представления | MIME, XDR, ASN.1, ASCII, PGP. | структурирует информацию для прикладного уровня. | | Сеансовый | NetBIOS, SAP,PPTP RTP, SOCKS | установление, управление и разрыв соединения между двумя хостами | | Транспортный | TCP, UDP | Обеспечивает сквозную доставку пакетов (датаграм), подтверждение успешной передачи, контроль ошибок. | | Сетевой | IP,ICMP | Определяет маршрутизацию и связь между сетями | | Канальный | PPP, IEEE 802.22, Ethernet, DSL, ARP, сетевая карта. | берет на себя задачу адресации в пределах локальной сети, обнаруживает ошибки, проверяет целостность данных. LLC, MAC-адрес и Ethernet. | | Физический | Среда | Установка и поддержка физического соединения, работа с физической средой | |
| **Эталонная модель TCP/IP**  Эталонная модель TCP/IP представляет собой сетевую модель передачи данных, представленных в цифровом формате, описывающую способ передачи данных от источника информации к получателю. Модель описывает различные уровни, через которые проходит информация, каждый из которых описывается некоторым правилом или протоколом передачи.   |  |  |  | | --- | --- | --- | | Уров. приложений | HTTP, SMTP, DNS, FTP, SSH, итд | установление, управление и разрыв соединения между двумя хостами, обеспечение взаимодействия пользовательских приложений с сетью | | Транспортный | TCP,UDP | Обеспечивает сквозную доставку пакетов (датаграм), подтверждение успешной передачи, контроль ошибок. | | Сетевой | IP,ICMP | - передача данных из одной сети в другую, независимо от протоколов нижнего уровня | |  | ARP,DHCP |  | | Уров. Доступа к сети | Ethernet,WIFI,DSL | описывает способы кодирования данных для передачи в физической среде. | |
| **Критика эталонных моделей OSI и TCP/IP.**  Недостатки модели OSI:  - избыточное количество уровней, два из которых не востребованы в реальных сетях; - неудачная реализация;  - сложность модели и протоколов; - неэффективность.  Недостатки модели TCP/IP:  - нет четкого разграничения служб, интерфейсов и протоколов;  - не является общей (например, не опишет Bluetooth (IEEE 802.15));  - не различает физический уровень и уровень передачи данных.  На практике используется **гибридная модель**:  1) Физический уровень  2) Канальный уровень  3) Сетевой уровень  4) Транспортный уровень  5) Прикладной уровень - объединяет в себя (прикладной, представления,  сеансовый). |
| **Дайте определение физической и логической инфраструктур сети** Физическая инфраструктура сети - топология сети, со всем её оборудованием.  Элементы: кабели, маршрутизаторы, коммутаторы, мосты, концентраторы, серверы, узлы.  Логическая инфраструктура сети - множество программ, для связи и управления узлами сети; обеспечивает связь между компьютерами. Элементы: система доменных имен DNS, сетевые протоколы, сетевые клиенты, маршрутизация, служба инфраструктуры открытого ключа, службы каталогов и др. |
| **Изобразите схему внутреннего устройства маршрутизатора. Функция маршрутизатора** – чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту, и перенаправление пакета по его сетевому адресу, включающему, номер сети и номер узла.  **Основные компоненты маршрутизатора**:  − **Входные порты**. Они функционируют на физическом уровне, подключая к маршрутизатору физическую среду. Входной порт также выполняет функции сетевого уровня, требуемые для взаимодействия с сетевым уровнем на другой стороне входящего соединения.  − **Коммутирующая матрица**. Она соединяет входные порты маршрутизатора с выходными портами. Матрица маршрутизатора работает только в его пределах. Именно в этом компоненте маршрутизатор сверяется с таблицей перенаправления и определяет выходной порт, в который прибывший пакет будет перенаправлен через коммутирующую матрицу. Управляющие пакеты (например, содержащие информацию о протоколе маршрутизации) передаются из входного порта в процессор маршрутизации.  − **Выходные порты**. Выходной порт хранит пакеты, полученные от коммутирующей матрицы, и передаёт их в исходящий канал, выполняя функции сетевого и физического уровней. Когда связь двунаправленная, выходной порт будет, спарен с входным портом того же канала.  − **Процессор маршрутизации**. Он выполняет протоколы маршрутизации, обрабатывает таблицы маршрутизации и прилагаемую информацию о состоянии соединения, а также составляет таблицу перенаправления для маршрутизатора. Кроме того, он выполняет функции управления сетью. |
| **Электронная почта** — текстовый сервис обмена сообщениями.  Протокол SMTP (Simple Mail Transfer Protocol): Протокол SMTP используется для транспортировки электронной почты на почтовый  сервер. Работает поверх TCP. Посылка почты осуществляется в 3 этапа: 1. приветствие (рукопожатие); 2. пересылка писем; 3. закрытие сессии.  Обмен сообщениями:  POP и IMAP (Internet Message Access Protocol) — наиболее распространенные Интернет-протоколы для извлечения почты. Практически все современные клиенты и серверы электронной почты поддерживают оба стандарта.  Протокол IMAP представляет собой, в основном, альтернативу POP3 с зачаточными способностями по отправке.  IMAP предоставляет пользователю обширные возможности для работы с почтовыми ящиками, находящимися на центральном сервере. |
| **Прикладной уровень (уровень приложений**) — верхний уровень модели OSI, обеспечивает взаимодействие пользовательских приложений с сетью  Позволяет приложениям использовать сетевые службы: удалённый доступ к файлам и базам данных, пересылка электронной почты; отвечает за передачу служебной информации; предоставляет приложениям информацию об ошибках; формирует запросы к уровню представления.  **Примеры протоколов**: HTTP для WWW, FTP, SMTP, SSH, DNS, etc.  **Сетевые службы прикладного уровня**: удалённый доступ к файлам и базам данных, пересылка электронной почты; отвечает за передачу служебной информации; предоставляет приложениям информацию об ошибках; формирует запросы к уровню представления; Служба имён DNS; Электронная почта; Потоковая передача аудио и видео.  Всемирная паутина (World Wide Web), представляет собой архитектуру, связывающую информацию из миллиардов машин по всему миру.  **Протоколы прикладного уровня**  HTTP (HyperText Transfer Protocol ) – протокол передачи данных, с помощью которого браузер взаимодействует с веб сервером.  FTP (File Transfer Protocol, протокол передачи файлов) –протокол для передачи файлов.  NFS (Network File System) – протокол сетевого доступа к файловым системам, разработанный в 1984 году.  SMTP (Simple Mail Transfer Protocol) – это широко используемый протокол, предназначенный для передачи электронной почты в сетях.  POP3 (Post Office Protocol Version 3 – протокол почтового отделения, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению. |
| **Представления уровень**  Этот уровень сопрягает сеансовый и прикладной уровни. По этой причине уровень представления также называют уровнем перевода. Другими словами, уровень 6 представляет данные в понятном человеку и машине виде, включая текст, изображения и аудио видеоданные.  **Протоколы** MIME, XDR, ASN.1, ASCII, PGP.  **Функции уровня представления**  • Перевод - Уровень представления переводит текст из одной кодировки в другую.  • Шифрование/дешифрование - Шифрование означает использование ключа для преобразования обычного текста в зашифрованный текст и использование того же ключа для расшифровки сообщения.  • Сжатие - используется функция для удаления нескольких битов из сообщения, чтобы сделать передачу более плавной. |
| **Сеансовый уровень** отвечает за безопасность, аутентификацию, обслуживание сеанса и установление соединения.  **Протоколы** NetBIOS, SAP, PPTP, RTP, SOCKS и т.д.  **Функции сеансового уровня:**  • Установка и завершение сеанса - Сеансовый уровень сообщает двум сторонам (отправителю и получателю), как взаимодействовать, а также как устанавливать и завершать связь.  • Синхронизация - Механизм контроля ошибок сеансового уровня позволяет процессу добавлять контрольные точки (флаги) в передачу, чтобы идентифицировать и исправлять любые несоответствия по метке.  • Диалоговое управление - Сеансовый уровень может «заставить» процесс передавать сообщения в полудуплексном или полнодуплексном режиме. |

|  |
| --- |
| **Транспортный уровень.** Принимает данные от сеансового уровня, разбивает их при необходимости на небольшие части, называемые сегментами, передать их сетевому уровню и гарантирует, что эти части в правильном виде прибудут по назначению.  **Функции транспортного уровня:** • контроль ошибок: потери, изменение порядка следования, дублирование; • контроль потока данных; • сегментирует и повторно собирает данные в один поток; • обеспечивает совместное использование канала различными программами (каждой присваивается число – «номер порта»)  **Протоколы: TCP, UDP**.  **Службы транспортного уровня** смотри **Протокол UDP** и **Протокол TCP и Борьба с перегрузками** |
| **(Транспорт)идентификации двух процессов в сетевом взаимодействии.** Для обмена сообщениями между процессами на разных хостах, необходимо, чтобы они могли идентифицировать друг друга. Идентификация требует наличия следующей информации о процессе: • Имя или адрес хоста; • Идентификатор процесса внутри хоста.  **Адрес хоста**: в интернет-приложениях хосты идентифицируются с помощью IP-адресов,  представляющих собой 32-разрядное двоичное число, уникальное для каждого хоста сети (говоря  точнее для каждого интерфейса, с помощью которого осуществляется подключение хоста к сети).  **Идентификация процесса** производится с помощью уникального для каждого процесса хоста номера порта. Популярные Интернет-протоколы прикладного уровня имеют стандартные значения номеров портов. Например, процесс протокола HTTP, получает порт номер 80 |
| **(Транспорт)Протокол UDP**  UDP (User Datagram Protocol) — один из ключевых элементов TCP/IP и набора сетевых протоколов. С UDP приложения могут посылать сообщения (дейтаграммы) другим хостам по IP­сети без необходимости предварительной установки специальных каналов передачи данных. Таким образом, UDP предоставляет ненадёжный сервис, и датаграммы могут прийти не по порядку, дублироваться или вовсе не дойти. UDP подразумевает, что проверка ошибок и исправление либо не нужны,  либо должны исполняться в приложении.  Структура пакета UDP: |
| **(Транспорт)Протокол TCP и Борьба с перегрузками**  TCP (transmission control protocol — протокол управления передачей) — один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных. Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери и устраняет дублирование, гарантируя, в отличие от UDP, целостность данных и уведомление отправителя о результатах передачи.  **Управление перегрузкой в TCP** контролирует наличие перегрузки из-за конечных систем. Подход заключается в задании ограничений каждому отправителю на скорость, с которой он отсылает трафик, с оглядкой на загруженность сети.  Если TCP-отправитель понимает, что загруженность на пути до удалённого хоста невелика, то он увеличивает скорость отправки; если на пути соединения сеть перегружена, то снижает скорость отправки. |
| **Сетевой уровень** занимается разработкой маршрутов доставки пакетов от отправителя до получателя. Для  достижения этих целей сетевой уровень должен обладать информацией о топологии сети и выбирать нужный путь по этой сети. При выборе маршрутизаторов он должен обеспечивать равномерную нагрузку на линии связи. Если источник и приемник находятся в различных сетях, сетевой уровень обеспечит их взаимодействие.  **Функции сетевого уровня:** 1. Установка соединения 2. Определение пути 3. Продвижение пакетов (дейтаграмм, данных)  Модель сетевого обслуживания определяет характеристики сквозной передачи данных между двумя  периферийными устройствами сети, т.е. между передающей и принимающей системами. Наиболее важной  абстракцией, предоставляемой сетевым уровнем более высоким уровням, является виртуальный канал.  **Модели сетевого обслуживания**  Модель обслуживания на основе виртуальных каналов подразумевает:  1) Установку виртуального канала. (Отправитель связывается с сетевым уровнем, указывая адрес получателя и ждет, пока сеть установит виртуальный канал. Сетевой уровень определяет путь от отправителя до получателя)  2) Передачу данных по виртуальному каналу.  3) Разрыв виртуального канала. В случае информирования одним из узлов сети о желании разорвать канал.  Модель **на основе дейтаграмм** - каждый раз, когда система хочет послать пакет, она указывает в нем адрес получающей системы. |
| **(Сетевой)Сетевые устройства-концентраторы, коммутаторы, мосты**  • Концентратор – работает на физическом уровне OSI, ретранслируя входящий сигнал с одного из портов в сигнал на все остальные подключённые порты, реализуя, свойственную Ethernet топологию общая шина, c разделением пропускной способности сети между устройствами в режиме полудуплекса.  • Сетевой мост – работает на канальном уровне, делит среду передачи сети на части, передавая информацию из одного сегмента в другой только в том случае, если адрес компьютера назначения принадлежит другой подсети. Тем самым мост изолирует трафик одной подсети от трафика другой, повышая общую производительность и безопасность.  • Сетевой коммутатор (switch) — устройство, предназначенное для соединения нескольких узлов в пределах одного или нескольких сегментов сети. Коммутаторы часто рассматриваются как многопортовые мосты. Коммутаторы подразделяются на управляемые и неуправляемые. |
| **(Сетевой)Интернет-протокол (IP)** – протокол сетевого уровня, который определяет адресацию сетевого уровня, формат дейтаграмм и действия над ними, предпринимаемые маршрутизаторами и конечными системами. Получение IP-адреса: 1) Ручная конфигурация; 2) Автоматическая: • DHCP (Dynamic Host Configuration Protocol); • APIPA (Automatic Private IP Addressing).  **Адресация в протоколе IPv4** использует 32-битные адреса, ограничивающие адресное пространство 4 294 967 296 (232) возможными уникальными адресами. Традиционной формой записи IPv4 адреса является запись в виде четырёх десятичных чисел от 0 до 255), разделённых точками. Через дробь указывается длина маски подсети. При этом компьютеры в подсетях объединяются общими начальными битами адреса. Количество этих бит, общее для данной подсети, называется маской подсети. |
| **(Сетевой)Принципы фрагментации и сборки дейтаграмм в IPv4.**Формат дейтаграммы IPv4   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Версия | IHL | Тип обслуживания | | Длина Пакета | | | Идентификатор | | | | Флаги | Смещение фрагмента | | Время жизни (TTL) | | | Протокол | Контрольная сумма заголовка | | | IP адрес отправителя | | | | | | | IP адрес получателя | | | | | | | Опции | | | | Смещение | | | Данные | | | | | |   Процедура фрагментации - разбивка дейтаграммы на несколько частей, которые позже будут собраны вместе.  Каждый из фрагментов должен быть снабжён заголовком IP. Некоторые из полей заголовка (идентификатор, TTL, флаги DF и MF, смещение) предназначены для сборки фрагментов в исходное сообщение.  − Идентификатор пакета – одинаковый для всех частей одного пакета должны иметь одинаковое значение этого поля, уникальное по отношению к другим пакетам. Это позволяет отличать части одного пакета от частей другого.  − Поле времени жизни (TTL) определяет предельный срок, в течение которого пакет может перемещаться по сети.  − Смещение фрагмента – какой фрагмент по порядку относительно других фрагментов (первый или не разбитый будут иметь 0).  − Флаг MF (More Fragments) 1 - данный пакет не последний. 0 - последний или не фрагментированный.  − Флаг DF (Do not Fragment), если 1, маршрутизатору запрещено фрагментировать пакет. Если помеченный пакет не может быть доставлен без фрагментации, то модуль IP его уничтожает, а узлу-отправителю посылается диагностическое сообщение. |

|  |
| --- |
| **(Сетевой)Основы маршрутизации**  Задачей сетевого уровня является маршрутизация – передача пакетов между двумя узлами в сети. В сложных составных сетях почти всегда существует несколько маршрутов для передачи пакетов между двумя конечными узлами. **Маршрут** – это последовательность маршрутизаторов, который должен пройти пакет от отправителя до пункта назначения. Задачу выбора маршрута решают маршрутизаторы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также указанного критерия выбора маршрута. Обычно в качестве критерия выступает пропускная способность маршрута, также используется критерий, количества пройденных промежуточных маршрутизаторов. Чтобы по адресу сети назначения можно было бы выбрать рациональный маршрут дальнейшего следования пакета, каждый конечный узел и маршрутизатор анализируют специальную информационную структуру, которая называется таблицей маршрутизации. Она хранится на маршрутизаторе и содержит записи, представляющие собой список наилучших маршрутов в соответствующие сети. В том случае, если к сети назначения имеется несколько путей, в таблицу маршрутизации будет помещён маршрут, у которого наилучшая метрика, определяемая на основании загрузки, полосы пропускания, задержки, стоимости или надёжности канала связи. **Алгоритмы маршрутизации: Статические** - распределение таблиц маршрутизации производится администратором. **Динамические** - маршрутизации подстраиваются к изменяющимся обстоятельствам сети в масштабе реального времени путем анализа поступающих сообщений об обновлении маршрутизации. - **Одномаршрутные или многомаршрутные**. Данные типы алгоритмов устанавливают число маршрутов к одному и тому же узлу сети. В случае одномаршрутного – 1 к 1; многомаршрутного – 1 ко много. - **Одноуровневые или иерархические.** В одноуров- невой все маршрутизаторы равны. В иерархической часть маршрутизаторов создает основу(backbone) маршрутизации. **- Внутридоменные или междоменные.** Некоторые алгоритмы действуют только в пределах доменов; другие и между ними тоже. **- Глобальные или децентрализованные.** Глобальные нужна информация о структуре всей сети для построения маршрута - LSA (Line State Algorithm). Децентрализованные – определение маршрутов происходит итерационно(DistanceVector Algorithm). |
| **(Сетевой) Бесклассовая адресация, Маска подсети, Разбиение на подсети**  **Бесклассовая** (Classless Inter-Domain Routing) — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткую классовую адресацию. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.  Количество адресов в подсети не равно количеству возможных узлов. Нулевой адрес IP резервируется для идентификации подсети, а последний — в качестве широковещательного адреса, таким образом в реально действующих сетях возможное количество узлов на два меньшее количества адресов.  **Маска подсети** —Благодаря маске можно узнать, какая часть IPадреса узла относится к адресу сети, а какая — к адресу самого узла в этой сети. Такое разбиение упрощает маршрутизацию. **Привести примеры.**  **Разбиение на подсети** Разбиение одной крупной сети на несколько мелких позволяет: рационально использовать адресное пространство, повысить безопасность и управляемость сети.  Исходную сеть можно разбить на подсети применяя маски, а точнее удлиняя маску, тем самым расширяя сетевую часть адреса. Это позволяет создавать подсети. Однако при этом уменьшается количество узлов доступных в каждой подсети, и не стоит забывать, что два адреса уходит на саму подсеть и её широковещательный адрес. |
| **(Сетевой) Классы сетей**  Класс А (Первые биты “0…”, начальный адрес 0.0.0.0, конечный адрес 127.255.255.255) Предназначен для крупных сетей.  Класс B (Первые биты “10…”, начальный адрес 128.0.0.0, конечный адрес 191.255.255.255) Предназначен для сетей средних масштабов.  Класс C (Первые биты “110…”, начальный адрес 192.0.0.0, конечный адрес 223.255.255.255) Предназначен для малых сетей.  Класс D (Первые биты “1110…”, начальный адрес 224.0.0.0, конечный адрес 239.255.255.255) Предназначен для Многоадресной рассылки.  Класс E (Первые биты “1111…”, начальный адрес 240.0.0.0, конечный адрес 255.255.255.255) Зарезервировано для использования в будущем.  Маски подсетей всегда фиксированной длинны. |
| **(Сетевой) Алгоритмы динамической маршрутизации**  **на основе вектора расстояний и на основе состояния канала**. Внутришлюзовыепротоколы делятся на 2 класса: дистанционно-векторные и учитывающие пропускную способность канала.  • Дистанционно-векторные основаны на вычислении количества узлов, которые необходимо пройти пакету до сети назначения Векторный алгоритм не учитывает скорость и надежность канала.  К таким протоколам относятся: RIP, IGRP.  • протоколы, которые учитывают пропускную способность канала, а не число узлов. В отличие от векторных протоколов они обладают быстрой сходимостью и могут использоваться в больших сетях.  К таким протоколам относятся: OSPF, IS-IS. |
| **(Сетевой) Протоколы маршрутизации RIP, OSPF**  **RIP** (протокол маршрутной информации). Протокол RIP является дистанционно-векторным протоколом маршрутизации, использующим в качестве приоритета (метрики) при выборе маршрута число переходов – чем оно меньше, тем выше приоритет маршрута. RIP-1 - классовый протокол маршрутизации; RIP-2 бесклассовый, может переносить доп. информацию о маршрутизации и механизм аутентификации для обеспечения безопасного обновления таблиц маршрутизации и поддержку масок подсетей;  **OSPF** (протокол прохождения по кратчайшему пути). Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры. OSPF обладает высокой скоростью сходимости в сравнении с дистанционно-векторными протоколами маршрутизации, поддержкой сетевых масок переменной длины и оптимальным использованием пропускной способности с построением дерева кратчайших путей; |
| **(Сетевой) Алгоритм построения таблицы маршрутизации RIP.** Рассмотрим действия одного маршрутизатора:  • Этап 1 – создание минимальной таблицы маршрутизации в маршрутизаторе, в которой учитываются только непосредственно подсоединённые сети.  • Этап 2 – рассылка минимальных таблиц маршрутизаторам, находящимся в тех же сетях что рассматриваемый маршрутизатор (соседям). RIP-сообщения передаются в пакетах протокола UDP и для каждой сети включают её IP-адрес и расстояние до неё от рассматриваемого маршрутизатора.  • Этап 3 – получение RIP-сообщений от соседей и обработка полученной информации. После, маршрутизатор наращивает каждое полученное поле метрики на единицу и запоминает, из какой сети и от какого маршрутизатора получена новая информация.  Сравнивая новую информацию с той, которая хранится в его таблице, маршрутизатор находит кратчайший маршрут, сохраняя его в таблицу (оставляя всегда только одну запись).  • Этап 4 – рассылка обновленной таблицы соседям. В которой содержится информация и о соседних, и об удаленных маршрутизаторах.  • Этап 5 – повторение с этапа 3, маршрутизаторы принимают RIP-сообщения, обрабатывают информацию и корректируют свои таблицы. |
| **Канальный уровень**. Из пересылаемых данных создаются кадры (пакеты) добавлением к ним заголовка со служебной информацией, и кода CRC, обеспечивающего целостность данных в кадре. На уровне DLC(Data link control) выполняется управление каналом.  Примеры протоколов: PPP, IEEE 802.22, Ethernet, DSL (Data link control), ARP, сетевая карта.  **Оборудование**: Коммутатор, точка доступа, и другие сетевые адаптеры. (Сетевой адаптер относится к периферийному устройству компьютера, взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами).  **Функции** уровня: а) Получение доступа к среде передачи; б) Выделение границ кадра; в) Аппаратная адресация; г) Обеспечение достоверности принимаемых данных; д) Адресация протокола верхнего уровня;  **Службы**: 1) Формирование кадра. 2) Доступ к линиям связи. 3) Надежность доставки. 4) Управления потоками данных (Скорость, буфер). 5) Обнаружение ошибок. 6) Исправление ошибок. 7) Дуплексная и полудуплексная передача. |
| **(Канальный) Обнаружение ошибок** в технике связи, помогает сохранять целостность данных или при передаче по линиям связи. **Исправление ошибок** — это восстановление информации после чтения её из канала связи. Для обнаружения используют коды обнаружения ошибок, для исправления - корректирующие коды (коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды). **Стратегии борьбы с ошибками:**  • обнаружение ошибок и запрос повторной передачи повреждённых блоков — этот подход применяется, в основном, на канальном и транспортном уровнях;  • обнаружение ошибок и отбрасывание повреждённых блоков — иногда применяется в системах потокового мультимедиа, где важна задержка передачи и нет времени на повторную передачу;  • исправление ошибок, применяется на физическом уровне.  **Корректирующие коды** — коды, служащие для обнаружения или исправления ошибок, возникающих при передаче информации под влиянием помех. • Блоковые коды. • Коды Хемминга. • Линейные циклические коды. • Коды CRC (Циклический избыточный код) • Коды БЧХ. • Коды Рида. |
| **(Канальный) Протоколы разделения канала** используют идеологию коммутации каналов и разделяют общий канал на столько частей, каково число компьютеров в сети. Если обозначить общую пропускную способность канала, как 𝑅, то при использовании TDM- и FDM- мультиплексирования, каждое устройство может передавать данные со скоростью 𝑅/𝑁 , где 𝑁 – число устройств.  1) TDMA (Time-Division Multiple Access) – мультиплексирование с временным разделением. Пакеты от разных абонентов передаются по очереди. Передача осуществляется на одной частоте.  2) FDMA (Frequency Division Multiple Access) – мультиплексирование с частотным разделением. Все абоненты передают информацию на разных частотах.  3) CDMA (Code Division Multiple Access) – множественный доступ с кодовым разделением Пакеты от разных абонентов имеют идентификационный код  4) Комбинирование. |

|  |
| --- |
| **(Канальный)ПротоколыПроизвольногоДоступа**  узел всегда передает данные в канал с максимальной скоростью. Когда возникает коллизия, каждый вовлеченный узел, выжидает в течение случайного интервала времени, а затем передает свой кадр повторно, повторяя эту процедуру пока ему не удастся пройти без коллизий. Благодаря разной длительности задержек времени существует вероятность того, что интервал, выбранный одним из узлов, окажется меньше, чем у других вовлеченных в коллизию узлов, и он успеет отправить свой кадр.  1) ALOHA - протокол разрешает пользователям передачу, как только у них появляются данные для отсылки. При этом столкнувшиеся кадры будут разрушены.  2) CSMA - протокол, в котором станции прослушивают среду передачи данных, перед отправкой (протоколы с контролем несущей). Типы CSMA: • 1-настойчивый CSMA. Перед отправкой, станция прослушивает канал, проверяя, свободен он или занят.  • Ненастойчивый СSMA. Перед отправкой, станция опрашивает канал. Если нет передач в данный момент, станция начинает передачу сама, иначе ждет в течение случайного интервала времени, а затем снова прослушивает линию.  • p-настойчивый CSMA. Когда станция готова передавать, она опрашивает канал. Если канал свободен, она с вероятностью p начинёт передачу. С вероятностью q = 1 – p она отказывается и ждет начала следующего такта. 2.1) CSMA/CD новая реализация – CSMA (с обнаружением коллизий). Если во время передачи кадра рабочая станция обнаруживает другой сигнал, она останавливает передачу, посылает сигнал помехи и ждёт в течение случайного времени backoff delay, перед тем как снова отправить кадр. Преимущество перед ALOHA - прекращение передачи сразу после обнаружения коллизии, быстрее освобождая канал. |
| **(Канальный)Протоколы последовательного доступа**  Двумя желательными свойствами протокола коллективного доступа являются возможность единственного активного узла передавать свои данные с максимальной пропускной способностью канала 𝑅 бит/сек и  возможность для каждого из 𝑀 активных узлов передавать свои данные со скоростью 𝑅/𝑀 бит/сек.  Наиболее важные протоколы последовательного доступа:  1) Протокол опроса. Один из узлов назначается управляющим, который поочередно опрашивает узлы и разрешает им передавать данные. Недостаток –затраты на оправку разрешений, а также система зависнет в случае поломки главного узла;  2) Протокол передачи маркера. Не существует главного узла, но есть специальный кадр – маркер, который передается от одного узла к другому и наличие которого разрешает передавать им данные. Недостаток – требуются специальные алгоритмы (обработка потери маркера, итд). |
| **Физический уровень +** **Носители**  Описывает физическую среду, необходимую для передачи необработанных двоичных данных между узлами.  **Компоненты**: характеристика кабеля; повторитель; сетевой адаптер; адаптер главной шины; контроллер сетевого интерфейса (сетевая плата); беспроводные технологии.  **Протоколы**: RS-232, PON, DSL, Bluetooth, USB, Ethernet, ИК-порт и т. д.  **Носители**  Управляемые (Проводные): • Витая пара (UTP) – несколько пар медных проводов, перекрученных друг с другом, в одной оболочке. В зависимости от категории, полоса пропускания у них разная. • Коаксиальный кабель – лучше экранирован, чем неэкранированная витая пара, поэтому может обеспечить передачу данных на более дальние расстояния с более высокими скоростями.• Волоконная оптика – оптоволоконная система состоит из трех основных компонентов: источника света, носителя, по которому распространяется световой сигнал, и приемника сигнала, или детектора. Не подвержены ЭМ помехам.  Неуправляемые (Беспроводные) – это сети, связь в которых обеспечиваются с помощью передачи-приема электромагнитных волн или передачи света напрямую (луч лазера). |
| **(Физический) принципы кодирования сигналов:**  • Кодирование уровнем, Физическое кодирование – самое простое кодирование, когда 0 и 1 кодируют разными уровнями напряжения. В чистом виде в Ethernet не используется.  • Амплитудная и частотная модуляции происходят на какой-то установленной частоте, при этом логические уровни сигнала кодируются изменением амплитуды сигнала или частотой сигнала соответственно. Амплитудно-частотная модуляция совмещает в себе оба принципа кодирования.  • В манчестерском кодировании единица кодируется перепадом от высокого уровня сигнала к низкому, а ноль - обратным перепадом. В начале такта может происходить служебный перепад сигнала (при передаче несколько единиц или нулей подряд). Сигнал, закодированный манчестерским кодом, является самосинхронизирующимся, для передачи данных не требуется дополнительная линия передачи тактовых импульсов за счет того, что за время передачи одного бита данных, независимо от того, 1 это или 0, обеспечивается один переход с одного уровня на другой |

**Канальный уровень**

Отдельно, т.к. ни в каких вопросах не было:

- MAC-адрес — уникальный идентификатор, присваиваемый каждой единице активного оборудования или

некоторым их интерфейсам в компьютерных сетях Ethernet.

- Ethernet — семейство технологий пакетной передачи данных между устройствами для компьютерных и

промышленных сетей.

<https://www.securitylab.ru/analytics/533599.php?clear_cache=Y>