1) Физическая инфраструктура сети.

Под физической инфраструктурой сети подразумевают её топологию, то есть физическое строение сети со всем её оборудованием: кабелями, маршрутизаторами, коммутаторами, мостами, концентраторами, серверами и узлами. К физической инфраструктуре также относятся транспортные технологии: Ethernet 802.11b, коммутируемая телефонная сеть общего пользования (PSNT), ATM – в совокупности они определяют, как осуществляется связь на уровне физических подключений.

2) Логическая инфраструктура сети.

Логическая – множество программных элементов, служащих для связи, управления и безопасности узлов сети, обеспечивающие связь между компьютерами с использованием коммуникационных каналов, определенных в физической топологии. Примеры элементов логической инфраструктуры сети: DNS, различные сетевые протоколы (стек TCP/IP), а также сетевые службы.

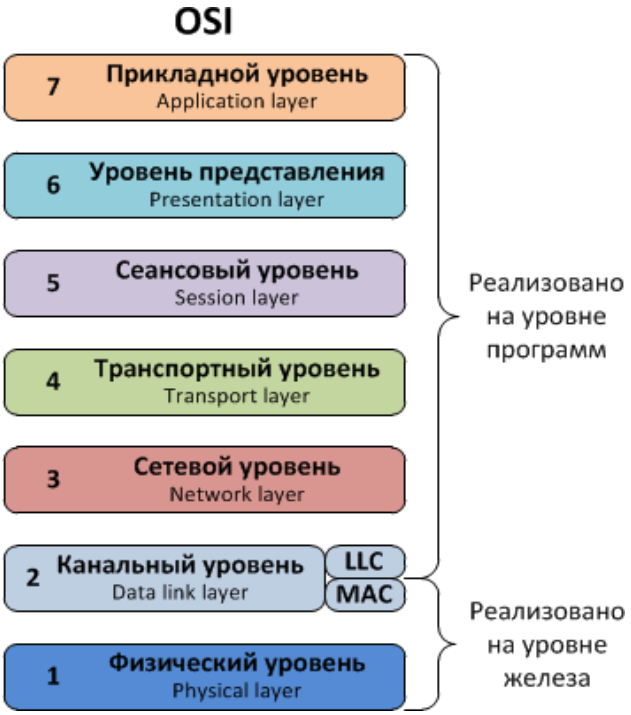
Логическую структуризацию производят при помощи следующих устройств:

а) Сетевой коммутатор и сетевой мост предназначены для объединения нескольких сегментов сети в единую сеть. Главное различие – в принципе работы: мост в каждый момент времени может осуществлять передачу пакетов только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами.

б) Маршрутизатор используется для пересылки пакетов между различными сегментами сети на основе правил и таблиц маршрутизации.

в) Шлюз также может соединять отдельные части сети. Обычно, основной причиной его использования в сети может стать необходимость объединить сети с разными типами системного и прикладного ПО, а нежелание локализовать трафик.

3) Эталонная модель OSI.



Эталонная модель OSI представляет собой многоуровневую модель сетевого взаимодействия, созданную Международной организацией по стандартизации ISO. Модель определяет различные уровни взаимодействия сетевых систем друг с другом и каждый из уровней выполняет определенные функции при таком взаимодействии.

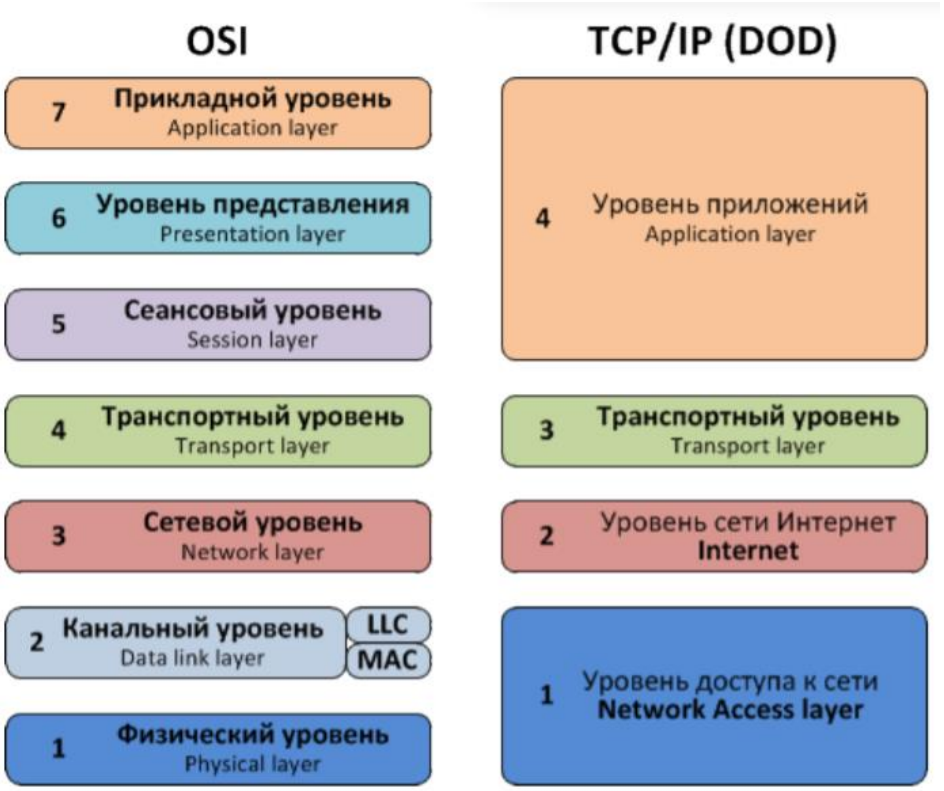
Любые данные, предназначенные для передачи по сети оборачиваются в протоколы каждого уровня сверху вниз (Например, HTTP → TCP → IPv4 → Ethernet) при этом заголовки протокола верхнего уровня являются данными для протокола нижнего уровня. При получении данных из сети клиент производит обратные действия.

Уровни:

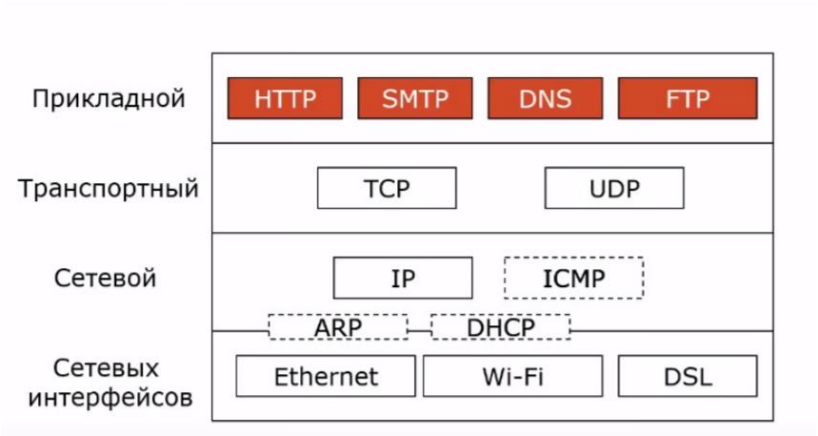
1) Физический — определяет метод передачи данных, какая среда используется (передача электрических сигналов, световых импульсов или радиоэфир), уровень напряжения, метод кодирования двоичных сигналов.
2) Канальный — берет на себя задачу адресации в пределах локальной сети, обнаруживает ошибки, проверяет целостность данных. MAC-адрес и Ethernet.
3) Сетевой — берет на себя объединения участков сети и выбор оптимального пути. Каждое сетевое устройство должно иметь уникальный сетевой адрес в сети. Протоколы IPv4 и IPv6.
4) Транспортный — берет на себя функцию транспорта. На этом уровне работают протоколы TCP и UDP.
5) Сеансовый — роль этого уровня в установлении, управлении и разрыве соединения между двумя хостами.
6) Уровень представления — структурирует информацию в читабельный вид для прикладного уровня.
7) Прикладной — обеспечивает взаимодействие пользовательских приложений с сетью. E-mail, браузеры по протоколу HTTP, FTP и остальное.

4) 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.



Три верхних уровня OSI: прикладной, представления и сеансовый объединены у TCP/IP в один, под названием прикладной. Сетевой уровень сменил название и называется — уровень сети Интернет. Транспортный остался таким же и с тем же названием. А два нижних уровня OSI: канальный и физический объединены у TCP/IP в один с названием — уровень доступа к сети.



1) Уровень сетевых интерфейсов или доступа к сети - описывает способ кодирования данных для передачи пакета данных на физическом уровне.

2) Сетевой или уровень сети Интернет - разработан для передачи данных из одной сети в другую. На этом уровне работают маршрутизаторы, что перенаправляют пакеты в нужную сеть путем расчета адреса сети по ее маске. Кроме того, обладает возможностями по передаче из любой сети в любую сеть независимо от протоколов нижнего уровня, а также возможность запрашивать данные от удаленной стороны, например ICMP или IGMP;

3) Транспортный уровень - решает проблему негарантированной доставки сообщений, а также гарантирует правильную последовательность прихода данных.

4) Прикладной или уровень приложений - на этом уровне работает большинство сетевых приложений, имеющих свои собственные протоколы обмена информацией, например HTTP для WWW, FTP, SMTP, SSH, DNS, etc.

5) Критика эталонных моделей ISO 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, невозможно описать работу Bluetooth с помощью TCP/IP);
- не различает физический уровень и уровень передачи данных.

6) Гибридная модель

На практике используется гибридная эталонная модель, использующая в качестве протоколов взаимодействия между уровнями стек протоколов TCP/IP и состоящая из следующих уровней:

1) Физический уровень
2) Канальный уровень
3) Сетевой уровень
4) Транспортный уровень
5) Прикладной уровень - объединяет в себя три верхних уровня (прикладной, представления, сеансовый).

7) Физический уровень

Назначением физического уровня сети является передача необработанного потока битов от одной машины к другой. Для передачи могут использоваться различные физические носители информации, называемые также средой распространения сигнала. Каждый из них имеет характерный набор полос пропускания, задержек, простоты установки и использования. Носители можно разделить на две категории: управляемые носители,

такие, как медный провод и оптоволоконный кабель, и неуправляемые, например, радиосвязь и передача по лазерному лучу без кабеля. (Или проводные и беспроводные).

8) Физические носители

Управляемые носители. (Проводные)

- Витая пара (UTP) – несколько пар медных проводов, перекрученных друг с другом, в одной оболочке. В зависимости от категории, полоса пропускания у них разная. Витая пара категории 5 (наиболее широко распространенная в локальных сетях) имеет полосу пропускания 100 мегагерц.

- Коаксиальный кабель – лучше экранирован, чем неэкранированная витая пара, поэтому может обеспечить передачу данных на более дальние расстояния с более высокими скоростями. Современные кабели имеют полосу пропускания около 1 гигагерца.

- Волоконная оптика – оптоволоконная система состоит из трех основных компонентов: источника света, носителя, по которому распространяется световой сигнал, и приемника сигнала, или детектора. Способны передавать данные со скоростью 50 Гбит/с на расстояния до 100 км.

Неуправляемые носители

Беспроводные сети – это сети, каналы связи в которых обеспечиваются с помощью передачи-приема электромагнитных волн. Частоты при этом могут использоваться самые разнообразные.

9) Канальный уровень

Из пересылаемых данных создаются кадры (пакеты) путем добавления к ним служебной информации – заголовка (состоящего из начального флага или преамбулы и адресной информации) и 32-х разрядного кода CRC, помещаемого в конце кадра и обеспечивающего целостность пересылаемых по физическому носителю данных. На уровне DLC выполняется управление каналом. Код CRC защищает данные от искажения во время передачи в физическом сегменте сети или сегментах, связанных повторителями;

Примеры: PPP, IEEE 802.22, Ethernet, DSL, ARP, сетевая карта.

Оборудование: Коммутатор, точка доступа.

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

___

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.

___

10) Службы канального уровня

1) Формирование кадра.
2) Доступ к линиям связи.
   MAC – media access control (Определяется правило передачи кадра в линию связи).
3) Надежность доставки.
4) Управления потоками данных (Скорость, буфер).
5) Обнаружение ошибок.
6) Исправление ошибок.
7) Дуплексная и полудуплексная передача.

11) Сетевые адаптеры

Реализуют функциональность канального уровня.

Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами.

Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи.

Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы, и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

12) Обнаружение и исправление ошибок

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления - корректирующие коды (коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

В системах связи возможны несколько стратегий борьбы с ошибками:

- обнаружение ошибок в блоках данных и автоматический запрос повторной передачи повреждённых блоков — этот подход применяется, в основном, на канальном и транспортном уровнях;

- обнаружение ошибок в блоках данных и отбрасывание повреждённых блоков — такой подход 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, а также при её хранении.

- Блоковые коды.
- Коды Хемминга.
- Линейные циклические коды.
- Коды CRC (Циклический избыточный код)
- Коды БЧХ.
- Коды Рида.

13) Протоколы разделения канала

Протоколы разделения каналов 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. Информация от каждого абонента делится на пакеты (блоки), и 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. На одной фиксированной частоте все абоненты передают информацию одновременно.

4) Комбинирование.

14) Протоколы произвольного доступа

В протоколе произвольного доступа передающий узел всегда передает данные в канал с максимальной скоростью. Когда возникает коллизия, каждый вовлеченный в нее узел передает свой кадр повторно до тех пор, пока ему не удастся пройти по каналу без коллизий.

Однако, испытав коллизию, узел, как правило, не повторяет передачу тут же, а выжидает в течение случайного интервала времени. Благодаря разной длительности случайных интервалов времени существует ненулевая вероятность того, что интервал, выбранный одним из узлов, окажется меньше, чем у других вовлеченных в коллизию узлов, и он успеет «пропихнуть» свой кадр в канал без коллизии.

1) ALOHA

В основе системы ALOHA лежит простая идея: разрешить пользователям передачу, как только у них появляются данные для отсылки. Конечно, при этом будут коллизии, и столкнувшиеся кадры будут разрушены. Отправителям необходимо уметь обнаруживать такие ситуации.

2) CSMA и CSMA/CD

Протоколы, в которых станции прослушивают среду передачи данных и действуют в соответствии с этим, называются протоколами с контролем несущей. Одними из протоколов с контролем несущей являются протоколы CSMA (множественный доступ с контролем несущей) и CSMA/CD.

Типы CSMA:

1) 1-настойчивый CSMA.

Когда у станции появляются данные для передачи, она сначала прослушивает канал, проверяя, свободен он или занят.

2) Ненастойчивый CSMA.

Прежде чем начать передачу, станция опрашивает канал. Если никто не передает в данный момент по каналу, станция начинает передачу сама, а если канал занят, станция не ждет освобождения канала, а ждет в течение случайного интервала времени, а затем снова прослушивает линию.

3) p-настойчивый CSMA.

Когда станция готова передавать, она опрашивает канал. Если канал свободен, она с вероятностью начинает передачу. С вероятностью q = 1 – p она отказывается от передачи и ждет начала следующего такта.

В дальнейшем, протокол получил новую реализацию – CSMA/CD (множественный доступ с контролем несущем и обнаружением коллизий). Данный протокол работает на канальном уровне модели OSI.

Если во время передачи кадра рабочая станция обнаруживает другой сигнал, занимающий передающую среду, она останавливает передачу, посылает сигнал преднамеренной помехи и ждёт в течение случайного промежутка времени (известного, как «backoff delay»), перед тем как снова отправить кадр.

CSMA/CD обладает преимуществом перед ALOHA – прекращая передачу сразу после обнаружения коллизии, мы тем самым быстрее освобождаем канал для дальнейшей попытки передачи.

15) 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. Протоколы CSMA и ALOHA удовлетворяют первому требованию, но не удовлетворяют второму, вследствие чего были созданы протоколы последовательного доступа.

Наиболее важные протоколы последовательного доступа:

1) Протокол опроса.

Один из узлов назначается главным (управляющим), который поочередно опрашивает узлы и разрешает им передавать данные. Недостаток – дополнительные затраты на оправку разрешений и то, что все «встанет» 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 – требуется наличие специальных алгоритмов для экстраординарных случаев, наподобие «потери» маркера.

16) Сетевые устройства: концентраторы, коммутаторы, мосты.

Концентратор работает на первом (физическом) уровне сетевой модели OSI, ретранслируя входящий сигнал с одного из портов в сигнал на все остальные (подключённые) порты, реализуя, таким образом, свойственную Ethernet топологию общая шина, с разделением пропускной способности сети между всеми устройствами и работой в режиме полудуплекса

Сетевой мост делит разделяемую среду передачи сети на части, передавая информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, то есть если адрес компьютера назначения принадлежит другой подсети. Тем самым мост изолирует трафик одной подсети от трафика другой, повышая общую производительность передачи данных в сети. Локализация трафика не только экономит пропускную способность, но и уменьшает возможность несанкционированного доступа к данным, так как кадры не выходят за пределы своего сегмента, и злоумышленнику сложнее перехватить их. Сетевой мост работает на канальном уровне модели OSI.

Сетевой коммутатор (switch) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Коммутаторы подразделяются на управляемые и неуправляемые. Коммутатор работает на канальном уровне модели OSI.

17) Сетевой уровень

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 также заботиться о том, чтобы нагрузка на маршрутизаторы и линии связи была равномерной. Наконец, если источник и приемник находятся в различных сетях, именно сетевой уровень должен уметь решать проблемы, связанные с различиями в сетях.

Функции сетевого уровня:

1. Установка соединения
2. Определение пути
3. Продвижение пакетов (дейтаграмм, данных)

18) Модели сетевого обслуживания

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.

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. Как только виртуальный канал будет установлен, данные могут начать перемещаться по нему;

3) Разрыв виртуального канала. В случае информирования одним из узлов сети о желании разорвать канал, происходит разрыв.

При использовании же модели обслуживания на основе дейтаграмм (дейтаграммного сетевого уровня) каждый раз, когда оконечная система хочет послать пакет, она указывает в нем адрес получающей системы, а, затем, передает этот пакет в сеть (канальному уровню).

19) Службы сетевого уровня

В системе-отправителе, когда пакет передаётся с транспортного уровня на сетевой, тот может предоставить следующие службы (функции):

− Гарантированная доставка;

− Гарантированная доставка с ограниченной задержкой.

Существуют также службы, предназначенные для организации потока пакетов по пути от источника до места назначения:

− Упорядоченная доставка пакетов;

− Гарантированная минимальная пропускная способность;

− Гарантированный максимальный джиттер (интервалы времени между последовательной передачей двух пакетов отправителем будут равняться интервалам между их приёмом, либо интервалы могут отличаться в пределах указанного значения);

− Службы безопасности. Используя секретный сеансовый ключ, известный только системе-отправителю и системе-получателю, сетевой уровень отправителя может шифровать содержимое всех дейтаграмм, посылаемых в пункт назначения. Сетевой уровень получателя будет отвечать за расшифровку содержимого.

Данная служба обеспечивает конфиденциальность всех сегментов транспортного уровня между источником и получателем, а также целостность данных и работу служб аутентификации).

20) Интернет-протокол

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: 1. DHCP (Dynamic Host Configuration Protocol);
   2. APIPA (Automatic Private IP Addressing).

21) Адресация в протоколе IPv4

IPv4 использует 32-битные четырёхбайтные) 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.

Формат дейтаграммы IPv4: (МНЕ КАЖЕТСЯ, НЕ НУЖНО)

22) Фрагментация дейтаграмм

Процедура фрагментации заключается в разбивке единой дейтаграммы на несколько частей, которые позже будут собраны вместе. Каждый из фрагментов должен быть снабжён полноценным заголовком IP. Некоторые из полей заголовка (идентификатор, TTL, флаги DF и MF, смещение) непосредственно предназначены для последующей сборки фрагментов в исходное сообщение.

− Идентификатор пакета используется для распознавания пакетов, образовавшихся путём деления на части исходного пакета. Все части одного пакета должны иметь одинаковое значение этого поля, уникальное по отношению к другим пакетам.

− Поле времени жизни (Time To Live - TTL) занимает один байт и определяет предельный срок, в течение которого пакет может перемещаться по сети.

− Поле смещения фрагмента предоставляет получателю информацию о положении фрагмента относительно начала поля данных исходного нефрагментированного пакета. (первый или не разбитый будут иметь нулевое значение). Смещение в байтах кратно 8.

− Флаг MF (More Fragments – больше фрагментов) в 1 говорит о том, что данный пакет является промежуточным (не последним). 0 – последний или нефрагментированный.

− Флаг DF (Do not Fragment – не фрагментировать), установленный в единицу, запрещает маршрутизатору фрагментировать данный пакет. Если помеченный таким образом пакет не может достигнуть получателя без фрагментации, то модуль IP его уничтожает, а узлу-отправителю посылается диагностическое сообщение.

23) Основы маршрутизации

Важнейшей задачей сетевого уровня является маршрутизация – передача пакетов между двумя конечными узлами в составной сети.

В сложных составных сетях почти всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами. Маршрут – это последовательность маршрутизаторов, который должен пройти пакет от отправителя до пункта назначения.

Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также на основании указанного критерия выбора маршрута. Обычно в качестве критерия выступает задержка прохождения маршрута отдельным пакетом или средняя пропускная способность маршрута для последовательности пакетов. Часто также используется критерий, учитывающий только количество пройденных в маршруте промежуточных маршрутизаторов (хопов).

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.

24) Классификация алгоритмов маршрутизации

Алгоритмы маршрутизации можно классифицировать по следующим типам:

- Статические или динамические.

Распределение статических таблиц маршрутизации производится администратором до начала маршрутизации и оно не меняется до тех пор, пока администратор его не изменит.

Динамические алгоритмы маршрутизации подстраиваются к изменяющимся обстоятельствам сети в масштабе реального времени путем анализа поступающих сообщений об обновлении маршрутизации. В случае поступления сообщении об обновлении, маршруты пересчитываются и таблица маршрутизации обновляется;

- 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 одноуровневой системе маршрутизации все маршрутизаторы равны по отношению друг к другу. В иерархической системе маршрутизации некоторые маршрутизаторы формируют то, что составляет основу (backbone - базу) маршрутизации.

- Внутридоменные или междоменные.

Некоторые алгоритмы маршрутизации действуют только в пределах доменов; другие - как в пределах доменов, так и между ними.

- Глобальные или децентрализованные

Глобальные используют информацию о структуре всей сети для построения маршрута - LSA (Line State Algorithm).

Децентрализованные – определение маршрутов происходит итерационно – DVA (DistanceVector Algorithm).

25) Алгоритмы динамической маршрутизации: на основе вектора расстояний и на основе состояния канала.

Внутришлюзовые протоколы делятся на 2 класса: дистанционно-векторные и по состоянию канала.

Принцип дистанционно-векторных протоколов основан на вычислении метрики - расстояния до сети назначения. Под расстоянием понимают количество узлов (участков сети), которые необходимо пройти пакету до сети назначения. Векторный алгоритм не учитывает скорость и надежность канала. Механизм векторных протоколов позволяет балансировать нагрузку в случае, если до сети назначения будут найдены несколько маршрутов.

К таким протоколам относятся: RIP, IGRP.

Другим типом протоколов маршрутизации являются протоколы, которые учитывают пропускную способность канала. То есть при выборе наилучшего маршрута они руководствуются не количеством промежуточных узлов, а скоростью канала. В отличие от векторных протоколов они обладают быстрой конвергенцией (сходимостью) и могут использоваться в больших сетях.

К таким протоколам относятся: OSPF, IS-IS.

26) Протоколы маршрутизации RIP, OSPF

1) RIP (протокол маршрутной информации). Протокол RIP является дистанционно-векторным протоколом маршрутизации, использующий в качестве метрики (по сути, приоритета) при выборе маршрута число переходов – чем оно меньше, тем выше приоритет маршрута при выборе. С течением времени он претерпел изменения: от классового (RIP-1) протокола маршрутизации к бесклассовому (RIP-2). RIP-2 в отличие от RIP-1 имеет способность переносить дополнительную информацию о маршрутизации пакетов, механизм аутентификации для обеспечения безопасного обновления таблиц маршрутизации и поддержку масок подсетей;

2) OSPF (протокол прохождения по кратчайшему пути). OSPF – протокол динамическом 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;

27) Алгоритмы построения таблицы маршрутизации RIP

Этап 1 – создание минимальных таблиц.

В исходном состоянии в каждом маршрутизаторе автоматически создаётся минимальная таблица маршрутизации, в которой учитываются только непосредственно подсоединённые сети.

Этап 2 – рассылка минимальных таблиц соседям.

Маршрутизатор начинает посылать своим соседям сообщения протокола RIP, в которых содержится его минимальная таблица. RIP-сообщения передаются в пакетах протокола UDP и включают два параметра для каждой сети: её IP-адрес и расстояние до неё от передающего сообщения маршрутизатора. Соседями являются те маршрутизаторы, которым данный маршрутизатор непосредственно может передать IP-пакет по какой-либо своей сети, не пользуясь услугами промежуточных маршрутизаторов.

Этап 3 – получение RIP-сообщений от соседей и обработка полученной информации.

После получения аналогичных сообщений от соседей, маршрутизатор наращивает каждое полученное поле метрики на единицу и запоминает, через какой порт и от какого маршрутизатора получена новая информация. Затем начинает сравнивать новую информацию с той, которая хранится в его таблице маршрутизации. Если новая информация имеет лучшую метрику (расстояние в хопах меньше), чем имеющаяся, протокол RIP замещает запись. В результате в таблице маршрутизации о каждой сети остаётся только одна запись.

Аналогичные операции с новой информацией выполняют и остальные маршрутизаторы сети.

Этап 4 – рассылка новой, уже не минимальной таблицы соседям.

Каждый маршрутизатор отсылает новое RIP-сообщение всем своим соседям. В этом сообщении он помещает данные о всех известных ему сетях – как непосредственно подключённых, так и удалённых, о которых маршрутизатор узнал из RIP-сообщений.

Этап 5 - получение RIP-сообщений от соседей и обработка полученной информации.

Этап 5 повторяет этап 3 – маршрутизаторы принимают RIP-сообщения, обрабатывают содержащуюся в них информацию и на её основании корректируют свои таблицы маршрутизации.

28) Устройство маршрутизаторов

Основная функция маршрутизатора – чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому парту, и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номер сети и номер узла.

Основные компоненты маршрутизатора:

− Входные порты. Они выполняют несколько ключевых функций. Они функционируют на физическом уровне, завершая входящую физическую связь в маршрутизаторе. Входной порт также выполняет функции сетевого уровня, требуемые для взаимодействия с сетевым уровнем на другой стороне входящего соединения. Функции поиска и выбора. 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, пакеты, содержащие информацию о протоколе маршрутизации) передаются из входного пора в процессор маршрутизации.

− Коммутирующая матрица. Она соединяет входные порты маршрутизатора с выходными портами. Матрица конкретного маршрутизатора работает только в его пределах, создавая условную сеть внутри сетевого маршрутизатора.

− 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, как правило, спарен с входным портом того же канала на интерфейсной плате.

− 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.

29) Классы сетей

Первые 3 класса – A, B и C используются для индивидуальной адресации сетей и узлов.

Классовая адресация

Класс	Первые биты	Начальный адрес	Конечный адрес
A	0	0.0.0.0	127.255.255.255
B	10	128.0.0.0	191.255.255.255
C	110	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Класс A
Маска класса A — 255.0.0.0. Предназначено для крупных сетей.
Класс B
Маска у B класса — 255.255.0.0.
Класс C
Маска у него — 255.255.255.0.
Классы D
Маска у него — 255.0.0.0. Предназначен для многоадресной рассылки.
Классы E
Маска у него — 255.0.0.0. Зарезервировано для использования в будущем.
Маски подсетей должны быть одинаковой длины.

30) CIDR

Бесклассовая адресация (Classless Inter-Domain Routing, англ. CIDR) — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. 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, последний — в качестве широковещательного адреса, таким образом в реально действующих сетях возможное количество узлов на два меньшее количества адресов.

30) Маска подсети

Маска подсети — битовая маска для определения по IP-адресу адреса подсети и адреса узла (хоста, компьютера, устройства) этой подсети. Благодаря маске можно узнать, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети. Такое разбиение упрощает маршрутизацию.

32) Разбиение на подсети

Разбиение одной крупной сети на несколько мелких позволяет:

− Рационально использовать адресное пространство;

− Повысить безопасность и управляемость сети.

С появлением трёхуровневой иерархии IPv4-адреса потребовались дополнительные методы, которые позволяли бы определить, какая часть IPv4-адреса указывает на идентификатор

подсети, а какая – на идентификатор узла. Было предложено использовать битовую маску (bit mask), которая отделяла бы часть адресного пространства идентификаторов узлов от адресного пространства идентификатора подсети. Такая битовая маска называется маской подсети.

Чтобы получить адрес сети, зная IPv4-адрес и маску подсети, необходимо применить к ним операцию логического «И». Другими словами, в тех позициях IPv4-адреса, в которых в маске подсети стоят двоичные единицы, находится идентификатор сети, где двоичные 0 – идентификатор узла.

Для сетей класса A, B, C определены фиксированные маски подсети, которые жёстко определяют количество возможных IPv4-адресов и механизм маршрутизации.

При применении масок подсети сети можно разделять на меньшие по размеру подсети путём расширения сетевой части адреса и уменьшения узловой части. Технология разделения сетей даёт возможность создавать большее число сетей с меньшим количеством узлов в них, что позволяет эффективно использовать адресное пространство.

33) Транспортный уровень

Транспортный (Transport Layer) Доставляет данные непосредственно от программы-отправителя к программе-получателю с определёнными гарантиями (на сохранность информации, порядок передачи сообщений и др.), не имеет дела с узлами сети.

Функции транспортного уровня:

- контроль ошибок: искажения пакетов, 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.

Основная функция транспортного уровня — принять данные от сеансового уровня, разбить их при необходимости на небольшие части, называемые сегментами, передать их сетевому уровню и гарантировать, что эти части в правильном виде прибудут по назначению.

34) Службы транспортного уровня

UDP (User Datagram Protocol — протокол пользовательских датаграмм) — один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.

TCP (англ. 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 данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи.

Мультиплексирование сеансов представляет собой операцию, в которой отдельный компьютер с одним IP-адресом может работать с несколькими сеансами одновременно.

35) Механизмы идентификации двух процессов в сетевом взаимодействии

Для успешного обмена сообщениями между процессами, выполняющимися на двух различных хостах, необходимо, чтобы они могли идентифицировать друг друга. Идентификация требует наличия следующей информации о процессе:

– Имя или адрес хоста, которому принадлежит процесс;

– 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 внутри хоста производится с помощью уникального для каждого процесса хоста номера порта. Популярные Интернет-протоколы прикладного уровня имею стандартизированные (хорошо известные) значения номеров портов. Так, процесс, использующий протокол HTTP, получает порт номер 80, а процесс, использующий протокол, - порт номер 25.

36) Протокол UDP

UDP (User Datagram Protocol — протокол пользовательских датаграмм) — один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.

UDP использует простую модель передачи, без неявных «рукопожатий» для обеспечения надёжности, упорядочивания или целостности данных. Таким образом, UDP предоставляет ненадёжный сервис, и датаграммы могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа. UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении.

Структура пакета UDP:

Биты	0 - 15	16 - 31
0-31	Порт отправителя (Source port)	Порт получателя (Destination port)
32-63	Длина датаграммы (Length)	Контрольная сумма (Checksum)
64-...	Данные (Data)	

37) Протокол TCP

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 данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи.

38) Борьба с перегрузками в протоколе TCP

Для управления перегрузкой протокол TCP должен использовать контроль перегрузки конечными системами. Подход протокола TCP заключается в задании ограничений каждому отправителю на скорость, с которой он отсылает трафик по соединению, как функции, зависящей от загруженности сети. Если TCP-отправитель понимает, что загруженность на пути до удалённого хоста невелика, то он увеличивает скорость отправки; если отправитель определяет, что на пути соединения сеть перегружена, то снижает скорость отправки.

39) Прикладной уровень

Прикладной уровень (уровень приложений; от англ. application layer) — верхний уровень модели OSI, обеспечивающий 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.

В массе своей эти протоколы работают поверх TCP или UDP.

40) Протоколы прикладного уровня

HTTP (HyperText Transfer Protocol – протокол передачи гипертекста) – протокол прикладного уровня передачи данных, с помощью которого браузер взаимодействует с веб-сервером.

FTP (File Transfer Protocol, протокол передачи файлов) – стандартный протокол, предназначенный 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, версия 3) – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению.

41) Сетевые службы прикладного уровня

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.

- Служба имён доменов DNS, суть которой заключается в иерархической схеме имён, основанной на доменах, и распределённой базе данных, реализующих эту схему имён. В первую очередь эта система используется для преобразования имён хостов в IP-адреса.

- Электронная почта

- Всемирная паутина (WWW, World Wide Web) представляющая собой архитектуру, являющуюся основой для доступа к связанному контенту, находящемуся на миллионах машин по всему Интернету.

- Потоковая передача аудио и видео.

- Доставка контента.

42) Электронная почта

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.