**9. Опишите сетевой уровень модели OSI.**

Открытая сетевая модель OSI (Open Systems Interconnection model) является эталонной. Эталонная она потому, что полное название модели выглядит как «Basic Reference Model Open Systems Interconnection model», где Basic Reference Model означает «эталонная модель».

Сетевая модель OSI состоит из семи уровней.

1. Прикладной уровень – обеспечивает доступ пользователей к окружению OSI а также предоставляет распределенные информационные службы.
2. Уровень представления – обеспечивает прикладному процессу независимость от различий в представлении данных (синтаксисе).
3. Сеансовый уровень – предоставляет структуру управления для взаимодействия приложений, устанавливает и разрывает соединения (сеансы) между приложениями, а также управляет соединениями.
4. Транспортный уровень - обеспечивает надежный и прозрачный процесс переноса данных между конечными точками, обеспечивает сквозное восстановление после ошибок и управление потоком.
5. Сетевой уровень – обеспечивает независимость верхних уровней от технологий передачи данных и коммутации, применяемых для соединения систем, отвечает за установку и разрыв соединений, а также за управление соединениями.
6. Уровень передачи данных – обеспечивает надежную передачу информации по физической линии, посылает блоки (кадры) с необходимой синхронизацией, контролем ошибок и управлением потоком.
7. Физический уровень – обеспечивает передачу неструктурированного потока битов по физическому носителю, имеет дело с механическими, функциональными и процедурными характеристиками доступа к физическому носителю.

В процессе передачи данных всегда участвуют устройство-отправитель, устройство-получатель, а также сами данные, которые должны быть переданы и получены. Все, что происходит при отправке и приеме данных, детально описывает семиуровневая модель OSI.

На седьмом уровне информация представляется в виде данных, на первом — в виде бит. Процесс, когда информация отправляется и переходит из данных в биты, называется инкапсуляцией. Обратный процесс, когда информация, полученная в битах на первом уровне, переходит в данные на седьмом, называется декапсуляцией. На каждом из семи уровней информация представляется в виде блоков данных протокола — PDU (Protocol Data Unit).

Рассмотрим на примере: пользователь 1 отправляет картинку, которая обрабатывается на седьмом уровне в виде данных, данные должны пройти все уровни до самого нижнего (первого), где будут представлены как биты (инкапсуляция). Компьютер пользователя 2 принимает биты, которые должны снова стать данными (декапсуляция).

Начнем с самого нижнего уровня. Он отвечает за обмен физическими сигналами между физическими устройствами - «железом». Компьютерное «железо» не понимает, что такое картинка или что на ней изображено, «железу» картинка понятна только в виде набора нулей и единиц, то есть бит. В данном случае бит является блоком данных протокола, сокращенно PDU (Protocol Data Unit).

Каждый уровень имеет свои PDU, представляемые в той форме, которая будет понятна на данном уровне и, возможно, на следующем до преобразования. Работа с чистыми данными происходит только на уровнях с пятого по седьмой.

Устройства физического уровня оперируют битами. Они передаются по проводам (например, через оптоволокно) или без проводов (например, через Bluetooth или IRDA, Wi-Fi, GSM, 4G и так далее).

Когда два пользователя находятся в одной сети, состоящей только из двух устройств — это идеальный случай. Но что, если этих устройств больше?

Второй уровень (уровень передачи данных) решает проблему адресации при передаче информации. Канальный уровень получает биты и превращает их в кадры (frame, также «фреймы»). Задача здесь — сформировать кадры с адресом отправителя и получателя, после чего отправить их по сети.

У канального уровня есть два подуровня — это MAC и LLC. MAC (Media Access Control, контроль доступа к среде) отвечает за присвоение физических MAC-адресов, а LLC (Logical Link Control, контроль логической связи) занимается проверкой и исправлением данных, управляет их передачей.

На втором уровне OSI работают коммутаторы, их задача — передать сформированные кадры от одного устройства к другому, используя в качестве адресов только физические MAC-адреса.

На третьем уровне (сетевом) появляется новое понятие — маршрутизация. Для этой задачи были созданы устройства третьего уровня — маршрутизаторы (их еще называют роутерами). Маршрутизаторы получают MAC-адрес от коммутаторов с предыдущего уровня и занимаются построением маршрута от одного устройства к другому с учетом всех потенциальных неполадок в сети.

На сетевом уровне активно используется протокол ARP (Address Resolution Protocol — протокол определения адреса). С помощью него 64-битные MAC-адреса преобразуются в 32-битные IP-адреса и наоборот, тем самым обеспечивается инкапсуляция и декапсуляция данных.

Все семь уровней модели OSI можно условно разделить на две группы:

Media layers (уровни среды), Host layers (уровни хоста).

Уровни группы Media Layers (L1, L2, L3) занимаются передачей информации (по кабелю или беспроводной сети), используются сетевыми устройствами, такими как коммутаторы, маршрутизаторы и т.п. Уровни группы Host Layers (L4, L5, L6, L7) используются непосредственно на устройствах, будь то стационарные компьютеры или портативные мобильные устройства.

Четвертый уровень (транспортный) - это посредник между Host Layers и Media Layers, относящийся скорее к первым, чем к последним, его главной задачей является транспортировка пакетов. Естественно, при транспортировке возможны потери, но некоторые типы данных более чувствительны к потерям, чем другие. Например, если в тексте потеряются гласные, то будет сложно понять смысл, а если из видеопотока пропадет пара кадров, то это практически никак не скажется на конечном пользователе. Поэтому, при передаче данных, наиболее чувствительных к потерям на транспортном уровне используется протокол TCP, контролирующий целостность доставленной информации.

Для мультимедийных файлов небольшие потери не так важны, гораздо критичнее будет задержка. Для передачи таких данных, наиболее чувствительных к задержкам, используется протокол UDP, позволяющий организовать связь без установки соединения.

При передаче по протоколу TCP, данные делятся на сегменты. Сегмент — это часть пакета. Когда приходит пакет данных, который превышает пропускную способность сети, пакет делится на сегменты допустимого размера. Сегментация пакетов также требуется в ненадежных сетях, когда существует большая вероятность того, что большой пакет будет потерян или отправлен не тому адресату. При передаче данных по протоколу UDP, пакеты данных делятся уже на датаграммы. Датаграмма (datagram) — это тоже часть пакета, но ее нельзя путать с сегментом.

Главное отличие датаграмм в автономности. Каждая датаграмма содержит все необходимые заголовки, чтобы дойти до конечного адресата, поэтому они не зависят от сети, могут доставляться разными маршрутами и в разном порядке. Датаграмма и сегмент — это два PDU транспортного уровня модели OSI. При потере датаграмм или сегментов получаются «битые» куски данных, которые не получится корректно обработать.

Первые четыре уровня — специализация сетевых инженеров, но с последними тремя они не так часто сталкиваются, потому что пятым, шестым и седьмым занимаются разработчики.

Пятый уровень (сеансовый) оперирует чистыми данными; помимо пятого, чистые данные используются также на шестом и седьмом уровне. Сеансовый уровень отвечает за поддержку сеанса или сессии связи. Пятый уровень оказывает услугу следующему: управляет взаимодействием между приложениями, открывает возможности синхронизации задач, завершения сеанса, обмена информации.

Службы сеансового уровня зачастую применяются в средах приложений, требующих удаленного вызова процедур, т.е. чтобы запрашивать выполнение действий на удаленных компьютерах или независимых системах на одном устройстве (при наличии нескольких ОС).

Примером работы пятого уровня может служить видеозвонок по сети. Во время видеосвязи необходимо, чтобы два потока данных (аудио и видео) шли синхронно. Когда к разговору двоих человек прибавится третий — получится уже конференция. Задача пятого уровня — сделать так, чтобы собеседники могли понять, кто сейчас говорит.

О задачах уровня представления вновь говорит его название. Шестой уровень занимается тем, что представляет данные (которые все еще являются PDU) в понятном человеку и машине виде. Например, когда одно устройство умеет отображать текст только в кодировке ASCII, а другое только в UTF-8, перевод текста из одной кодировки в другую происходит на шестом уровне.

Шестой уровень (уровень представления) также занимается представлением картинок (в JPEG, GIF и т.д.), а также видео-аудио (в MPEG, QuickTime). Помимо перечисленного, шестой уровень занимается шифрованием данных, когда при передаче их необходимо защитить.

Седьмой уровень иногда еще называют уровень приложений (прикладной), но, чтобы не запутаться можно использовать оригинальное название — application layer. Прикладной уровень — это то, с чем взаимодействуют пользователи, своего рода графический интерфейс всей модели OSI, с другими он взаимодействует по минимуму.

Все услуги, получаемые седьмым уровнем от других, используются для доставки данных до пользователя. Протоколам седьмого уровня не требуется обеспечивать маршрутизацию или гарантировать доставку данных, когда об этом уже позаботились предыдущие шесть. Задача седьмого уровня — использовать свои протоколы, чтобы пользователь увидел данные в понятном ему виде.

Протоколы на седьмом уровне используют UDP (например, DHCP, FTP) или TCP (например, HTTP, HTTPS, SFTP (Simple FTP), DNS). Прикладной уровень является самым верхним по иерархии, но при этом его легче всего объяснить.

Семиуровневая модель была принята в качестве стандарта ISO/IEC 7498, действующего по сей день, однако, модель имеет свои недостатки. Среди основных недостатков говорят о неподходящем времени, плохой технологии, поздней имплементации, неудачной политике.

Первый недостаток — это неподходящее время. На разработку модели было потрачено неоправданно большое количество времени, но разработчики не уделили достаточное внимание существующим в то время стандартам. В связи с этим модель обвиняют в том, что она не отражает действительность. В таких утверждениях есть доля истины, ведь уже на момент появления OSI другие компании были больше готовы работать с получившей широкое распространение моделью TCP/IP.

Вторым недостатком называют плохую технологию. Как основной довод в пользу того, что OSI — это плохая технология, приводят распространенность стека TCP/IP. Протоколы OSI часто дублируют другу друга, функции распределены по уровням неравнозначно, а одни и те же задачи могут быть решены на разных уровнях.

Разделение на семь уровней было скорее политическим, чем техническим. При построении сетей в реальности редко используют уровни 5 и 6, а часто можно обойтись только первыми четырьмя. Даже изначальное описание архитектуры в распечатанном виде имеет толщину в один метр.

Кроме того, в отличие от TCP/IP, OSI никогда не ассоциировалась с UNIX. Добиться широкого распространения OSI не получилось потому, что она проектировалась как закрытая модель, продвигаемая Европейскими телекоммуникационными компаниями и правительством США. Стек протоколов TCP/IP изначально был открыт для всех, что позволило ему набрать популярность среди сторонников открытого программного кода.

Даже несмотря на то, что основные проблемы архитектуры OSI были политическими, репутация была запятнана и модель не получила распространения. Тем не менее, в сетевых технологиях, при работе с коммутацией даже сегодня обычно используют модель OSI.

На каждом из семи уровней модели выполняется своя задача. В действительности архитектура OSI сложнее, чем описано. Существуют и другие уровни, например, сервисный, который встречается в интеллектуальных или сотовых сетях, или восьмой — так называют самого пользователя.

Как упоминали выше, оригинальное описание всех принципов построения сетей в рамках этой модели, если его распечатать, будет иметь толщину в один метр. Но компании активно используют OSI как эталон. Перечислили только основную структуру.

Модель OSI служит инструментом при диагностике сетей. Если в сети что-то не работает, то гораздо проще определить уровень, на котором произошла неполадка, чем пытаться перестроить всю сеть заново.

Зная архитектуру сети, гораздо проще ее строить и диагностировать. Как нельзя построить дом, не зная его архитектуры, так невозможно построить сеть, не зная модели OSI. При проектировании важно учитывать все. Важно учесть взаимодействие каждого уровня с другими, насколько обеспечивается безопасность, шифрование данных внутри сети, какой прирост пользователей выдержит сеть без обрушения, будет ли возможно перенести сеть на другую машину и т.д. Каждый из перечисленных критериев укладывается в функции одного из семи уровней.

**46. Опишите методы доступа к среде передачи данных.**

Методы доступа к среде передачи (media access method) делятся на конфликтные и неконфликтные.

Конфликтные методы доступа предполагают возможность конфликта (коллизии) – одновременной передачи по одной линии двумя или более устройствами.

При этом методе доступа узел, желающий послать кадр в сеть, прослушивает линию. Если линия занята или обнаружена коллизия, попытка передачи откладывается на некоторое время. Основные разновидности:

CSMA/CA - множественный доступ с прослушиванием несущей и избеганием коллизий.

CSMA/CD - множественный доступ с опознаванием несущей и обнаружением коллизий.

При неконфликтном методе узлы получают доступ к среде в предопределенном порядке. Последовательность определяется контроллером сети, который может быть централизованным (его функции может выполнять, например, сервер) или/и распределенным (функции выполняются оборудованием всех узлов).

Основные типы:

-доступ с передачей маркера (token passing), применяемый в сетях ARCnet, Token Ring, FDDI;

-доступ по приоритету;

-поллинг (polling) - опрос готовности, применяемый в больших машинах (mainframes) и технологии 100VG-AnyLAN, так же polling применяется в широкополосных беспроводных технологиях (WiMax). Основное преимущество метода - ограниченное время прохождения кадра, мало зависящее от нагрузки.

В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD). Этот метод используется исключительно в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме коллективного доступа (multiply access).

Алгоритм работы: Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он начинает передачу кадра, одновременно контролируя состояние линии. При обнаружении коллизии передача прекращается, и повторная попытка откладывается на случайное время. Коллизии - нормальное, хотя и не очень частое явление для CSMA/CD. Их частота связана с количеством и активностью подключенных узлов. Нормально коллизии могут начинаться в определенном временном окне кадра, запоздалые коллизии сигнализируют об аппаратных неполадках в кабеле или узлах. CSMA/CD эффективнее, чем CSMA/CA, но требует более сложных и дорогих схем цепей доступа. Применяется во многих сетевых архитектурах: Ethernet, EtherTalk (реализация Ethernet фирмы Apple), G-Net, IBM PC Network, AT&T StarLAN.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - множественный доступ с прослушиванием несущей и избежанием коллизий Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он посылает короткий сигнал запроса па передачу (RTS) и определенное время ожидает ответа (CTS) от адресата назначения. При отсутствии ответа (подразумевается возможность коллизии) попытка передачи откладывается, при получении ответа в линию посылается кадр. При запросе на широковещательную передачу (RTS содержит адрес 255) CTS не ожидается. Метод не позволяет полностью избежать коллизий, но они обрабатываются на вышестоящих уровнях протокола. Метод применяется в сети Apple LocalTalk, характерен простотой и низкой стоимостью цепей доступа.

Метод доступа с маркером.

Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения - маркер.

Получив маркер, станция анализирует его и при отсутствии у нее данных для передачи обеспечивает его продвижение к следующей станции. Станция, которая имеет данные для передачи, при получении маркера изымает его из кольца, что дает ей право доступа к физической среде для передачи своих данных. Затем эта станция выдает в кольцо кадр данных установленного формата последовательно по битам. Переданные данные проходят по кольцу всегда в одном направлении от одной станции к другой. Кадр снабжен адресом назначения и адресом источника.

Все станции кольца ретранслируют кадр побитно, как повторители. Если кадр проходит через станцию назначения, то, распознав свой адрес, эта станция копирует кадр в свой внутренний буфер и вставляет в кадр признак подтверждения приема. Станция, выдавшая кадр данных в кольцо, при обратном его получении с подтверждением приема изымает этот кадр из кольца и передает в сеть новый маркер, давая другим станциям сети возможность передавать данные.

Время удержания одной станцией маркера ограничивается тайм-аутом удержания маркера, после истечение которого станция обязана передать маркер далее по кольцу. Каждая станция имеет механизмы обнаружения и устранения неисправностей сети, возникающих в результате ошибок передачи или переходных явлений (например, при подключении и отключении станции). Не все станции в кольце равны. Одна из станций обозначается как активный монитор,что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление тайм-аутом в кольце, порождает новые маркеры (если необходимо), чтобы сохранить рабочее состояние, и генерирует диагностические кадры при определенных обстоятельствах. Активный монитор выбирается, когда кольцо инициализируется, и в этом качестве может выступить любая станция сети. Если монитор отказал по какой-либо причине, существует механизм, с помощью которого другие станции (резервные мониторы) могут договориться, какая из них будет новым активным монитором.

Метод доступа по приоритету.

Доступ по приоритету запроса - относительно новый метод доступа, разработанный для стандарта сети Еthernet со скоростью передачи данных 100 Мбит/с - 100VG-AnyLAN. Он стандартизован IЕЕЕ в категории 802.12. Этот метод доступа основан на том, что все сети 100VG-AnyLAN строятся только из концентраторов и оконечных узлов. Концентраторы управляют доступом к кабелю, последовательно опрашивая все узлы в сети и выявляя запросы на передачу. Концентратор должен знать все адреса, связи и узлы и проверять их работоспособность. Оконечным узлом, в соответствии с определением 100VG-AnyLAN, может быть компьютер, мост, маршрутизатор или коммутатор. Как и при СSМА/СD, при доступе по приоритету запроса два компьютера могут бороться за право передать данные. Однако только последний метод реализует схему, по которой определенные типы данных - если возникло состязание, - имеют соответствующий приоритет. Получив одновременно два запроса, концентратор вначале отдаст предпочтение запросу с более высоким приоритетом. Если запросы имеют одинаковый приоритет, они будут обслужены в произвольном порядке. В сетях с использованием доступа по приоритету запроса каждый компьютер может одновременно передавать и принимать данные, поскольку для этих сетей разработана специальная схема кабеля. В них применяется восьмипроводной кабель, по каждой паре проводов сигналы передаются с частотой 25 МГц. В сетях, где реализован доступ по приоритету запроса, связь устанавливается только между компьютером-отправителем, концентратором и компьютером-получателем.

**84. Охарактеризуйте сети с коммутацией пакетов.**

Коммутация пакетов – это техника коммутации абонентов, которая была специально разработана для эффективной передачи компьютерного трафика.

Эксперименты по созданию первых компьютерных сетей на основе техники коммутации каналов показали, что этот вид коммутации не позволяет достичь высокой общей пропускной способности сети. Суть проблемы заключается в пульсирующем характере трафика, который генерируют типичные сетевые приложения. Коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может составлять 1:50 или 1:100. Если для описанной сессии организовать коммутацию канала между компьютером пользователя и сервером, то большую часть времени канал будет простаивать. В то же время коммутационные возможности сети будут использоваться нерационально — часть тайм-слотов или частотных полос коммутаторов будет занята и недоступна другим пользователям сети.

При коммутации пакетов все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. Напротив, пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения. Пакеты транспортируются в сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге - узлу назначения.

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета. В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта, а когда до него дойдет очередь, то он передается следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсации трафика на магистральных связях между коммутаторами и тем самым использовать их наиболее эффективным образом для повышения пропускной способности сети в целом.

Так, общий объем передаваемых сетью компьютерных данных в единицу времени при технике коммутации пакетов будет выше, чем при технике коммутации каналов.

Описанный выше режим передачи пакетов между двумя конечными узлами сети предполагает независимую маршрутизацию каждого пакета. Такой режим работы сети называется дейтаграммным, и при его использовании коммутатор может изменить маршрут какого-либо пакета в зависимости от состояния сети - работоспособности каналов и других коммутаторов, длины очередей пакетов в соседних коммутаторах и т. п.

Существует и другой режим работы сети - передача пакетов по виртуальному каналу (virtual circuit или virtual channel*)*. В этом случае, перед тем как начать передачу данных необходимо установить виртуальный канал, который представляет собой единственный маршрут, соединяющий эти конечные узлы. Виртуальный канал может быть динамическим или постоянным. Динамический виртуальный канал устанавливается при передаче в сеть специального пакета - запроса на установление соединения. Этот пакет проходит через коммутаторы и «прокладывает» виртуальный канал. Коммутаторы запоминают маршрут для данного соединения и при поступлении последующих пакетов данного соединения отправляют их всегда по проложенному маршруту. Постоянные виртуальные каналы создаются администраторами сети путем ручной настройки коммутаторов.

При отказе коммутатора или канала на пути виртуального канала соединение разрывается, и виртуальный канал нужно прокладывать заново.

Каждый режим передачи пакетов имеет свои преимущества и недостатки. Дейтаграммный метод не требует предварительного установления соединения и поэтому работает без задержки перед передачей данных. Это особенно выгодно для передачи небольшого объема данных, когда время установления соединения может быть соизмеримым со временем передачи данных. Кроме того, дейтаграммный метод быстрее адаптируется к изменениям в сети.

При использовании метода виртуальных каналов время, затраченное на установление виртуального канала, компенсируется последующей быстрой передачей всего потока пакетов. Коммутаторы распознают принадлежность пакета к виртуальному каналу по специальной метке - номеру виртуального канала, а не анализируют адреса конечных узлов, как в предыдущем случае.

Одним из отличий метода коммутации пакетов от метода коммутации каналов является неопределенность пропускной способности соединения между двумя абонентами. В методе коммутации каналов после образования составного канала пропускная способность сети при передаче данных между конечными узлами известна - это пропускная способность канала.

Неопределенная пропускная способность сети с коммутацией пакетов - это плата за ее общую эффективность при некотором ущемлении интересов отдельных абонентов.

На эффективность работы сети существенно влияют размеры пакетов, которые передает сеть. Слишком большие размеры пакетов приближают сеть с коммутацией пакетов к сети с коммутацией каналов, поэтому эффективность сети при этом падает. Слишком маленькие пакеты заметно увеличивают долю служебной информации, так как каждый пакет несет с собой заголовок фиксированной длины, а количество пакетов, на которые разбиваются сообщения, будет резко расти при уменьшении размера пакета. Существует некоторая золотая середина, которая обеспечивает максимальную эффективность работы сети, однако ее трудно определить точно, так как она зависит от многих факторов, некоторые из них к тому же посто­янно меняются в процессе работы сети. Поэтому разработчики протоколов для сетей с коммутацией пакетов выбирают пределы, в которых может находиться длина пакета, а точнее его поле данных, так как заголовок, как правило, имеет фиксированную длину. Обычно нижний предел поля данных выбирается равным нулю, что разрешает передавать служебные пакеты без пользовательских данных, а верхний предел не превышает 4-х килобайт. Приложения при передаче данных пытаются занять максимальный размер поля данных, чтобы быстрее выполнить обмен данными, а небольшие пакеты обычно используются для квитанций о доставке пакета.

При выборе размера пакета необходимо учитывать также и интенсивность битовых ошибок канала. На ненадежных каналах необходимо уменьшать размеры пакетов, так как это уменьшает объем повторно передаваемых данных.

**94. Опишите классы протокола IP.**

IP-адрес - это уникальная 32-разрядная последовательность двоичных цифр, с помощью которой компьютер однозначно идентифицируется в IP-сети.

Для удобства работы с IP-адресами 32-разрядную последовательность обычно разделяют на 4 части по 8 бит (на октеты), каждый октет переводят в десятичное число и при записи разделяют эти числа точками.

В таком виде (это представление называется «dotted-decimal notation») IP-адреса занимают гораздо меньше места и намного легче запоминаются.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP-адрес в  32-разрядном виде | 11000000 10101000 00000101 11001000 | | | |
| IP-адрес, разбитый на октеты | 11000000 | 10101000 | 00000101 | 11001000 |
| Октеты в десятичном представлении | 192 | 168 | 5 | 200 |
| IP-адрес в виде десятичных чисел, разделённых точками | 192.168.5.200 | | | |

Чтобы определить какая именно часть IP-адреса принадлежит к номеру сети, а какая - к номеру хоста, определяется значениями первых бит адреса. Также, первые биты IP-адреса используются для того, чтобы определить к какому классу относится тот или другой IP-адрес.

IP-адреса разделяются на 5 классов: A, B, C, D, E.

Адреса классов A, B и C делятся на две логические части: номер сети и номер узла.

Идентификатор сети, также называемый адресом сети, обозначает один сетевой сегмент в более крупной объединенной сети (сети сетей), использующей протокол TCP/IP. IP-адреса всех систем, подключенных к одной сети, имеют один и тот же идентификатор сети. Этот идентификатор также используется для уникального обозначения каждой сети в более крупной объединенной сети.

Идентификатор узла, также называемый адресом узла, определяет узел TCP/IP (рабочую станцию, сервер, маршрутизатор или другое TCP/IP-устройство) в пределах каждой сети. Идентификатор узла уникальным образом обозначает систему в том сегменте сети, к которой она подключена.

На рисунке показана структура IP-адреса разных классов.



Если адрес начинается с 0, то сеть относят к классу А и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) Сетей класса А немного, зато количество узлов в них может достигать 224, то есть 16 777 216 узлов.

Если первые два бита адреса равны 10, то сеть относится к классу В. В сетях класса В под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса В является сетью средних размеров с максимальным числом узлов 216, что составляет 65 536 узлов.

Если адрес начинается с последовательности 110, то это сеть класса С. В этом случае под номер сети отводится 24 бита, а под номер узла — 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено 28, то есть 256 узлами.

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес — multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.

Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу Е. Адреса этого класса зарезервированы для будущих применений.

В таблице приведены диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей.



Большие сети получают адреса класса А, средние — класса В, а маленькие — класса С.

**125. Опишите сеть Token Ring**

Сеть Token-Ring (маркерное кольцо) была предложена компанией IBM в 1985 году (первый вариант появился в 1980 году). Она предназначалась для объединения в сеть всех типов компьютеров, выпускаемых IBM. Token-Ring является в настоящее время международным стандартом IEEE 802.5 (хотя между Token-Ring и IEEE 802.5 есть незначительные отличия). Это ставит данную сеть на один уровень по статусу с Ethernet.

 Разрабатывалась Token-Ring как надежная альтернатива Ethernet, но сейчас Ethernet вытеснил все остальные сети, и Token-Ring можно считать безнадежно устаревшей. Уже в 1999 году большинством производителей оборудования было прекращено производство новых устройств для сетей Token-Ring

 Сеть Token-Ring имеет топологию кольцо, хотя внешне она больше напоминает звезду. Это связано с тем, что отдельные абоненты (компьютеры) присоединяются к сети не напрямую, а через специальные концентраторы или многостанционные устройства доступа (MSAU или MAU – Multistation Access Unit). Физически сеть образует звездно-кольцевую топологию. В действительности же абоненты объединяются все-таки в кольцо, то есть каждый из них передает информацию одному соседнему абоненту, а принимает информацию от другого.

Концентратор (MAU) при этом позволяет централизовать задание конфигурации, отключение неисправных абонентов, контроль работы сети и т.д. Никакой обработки информации он не производит.

Для каждого абонента в составе концентратора применяется специальный блок подключения к магистрали (TCU – Trunk Coupling Unit), который обеспечивает автоматическое включение абонента в кольцо, если он подключен к концентратору и исправен. Если абонент отключается от концентратора или же он неисправен, то блок TCU автоматически восстанавливает целостность кольца без участия данного абонента. Срабатывает TCU по сигналу постоянного тока (так называемый «фантомный» ток), который приходит от абонента, желающего включиться в кольцо. Абонент может также отключиться от кольца и провести процедуру самотестирования. «Фантомный» ток никак не влияет на информационный сигнал, так как сигнал в кольце не имеет постоянной составляющей.

 Существуют как пассивные, так и активные концентраторы MAU. Активный концентратор восстанавливает сигнал, приходящий от абонента (то есть работает, как концентратор Ethernet). Пассивный концентратор не выполняет восстановление сигнала, только перекоммутирует линии связи.

 Концентратор в сети может быть единственным, в этом случае в кольцо замыкаются только абоненты, подключенные к нему. Внешне такая топология выглядит, как звезда. Если же нужно подключить к сети большое число абонентов, несколько концентраторов соединяют магистральными кабелями и образуют звездно-кольцевую топологию.

 Как уже отмечалось, кольцевая топология очень чувствительна к обрывам кабеля кольца. Для повышения живучести сети, в Token-Ring предусмотрен режим так называемого сворачивания кольца, что позволяет обойти место обрыва.

В нормальном режиме концентраторы соединены в кольцо двумя параллельными кабелями, но передача информации производится при этом только по одному из них.

В случае одиночного повреждения (обрыва) кабеля сеть осуществляет передачу по обоим кабелям, обходя тем самым поврежденный участок. При этом даже сохраняется порядок обхода абонентов, подключенных к концентраторам, но увеличивается суммарная длина кольца.

В случае множественных повреждений кабеля сеть распадается на несколько частей (сегментов), не связанных между собой, но сохраняющих полную работоспособность. Максимальная часть сети остается при этом связанной, как и прежде. Конечно, это уже не спасает сеть в целом, но позволяет при правильном распределении абонентов по концентраторам сохранять значительную часть функций поврежденной сети.

 Несколько концентраторов может конструктивно объединяться в группу, кластер (cluster), внутри которого абоненты также соединены в кольцо. Применение кластеров позволяет увеличивать количество абонентов, подключенных к одному центру.

 В качестве среды передачи в сети IBM Token-Ring сначала применялась витая пара, как неэкранированная (UTP), так и экранированная (STP), но затем появились варианты аппаратуры для коаксиального кабеля, а также для оптоволоконного кабеля в стандарте FDDI.

 Основные технические характеристики классического варианта сети Token-Ring:

* максимальное количество концентраторов типа IBM 8228 MAU - 12;
* максимальное количество абонентов в сети - 96;
* максимальная длина кабеля между абонентом и концентратором - 45 метров;
* максимальная длина кабеля между концентраторами - 45 метров;
* максимальная длина кабеля, соединяющего все концентраторы - 120 метров;
* скорость передачи данных - 4 Мбит/с и 16 Мбит/с.

Все приведенные характеристики относятся к случаю использования неэкранированной витой пары. Если применяется другая среда передачи, характеристики сети могут отличаться. Например, при использовании экранированной витой пары (STP) количество абонентов может быть увеличено до 260 (вместо 96), длина кабеля - до 100 метров (вместо 45), количество концентраторов - до 33, а полная длина кольца, соединяющего концентраторы - до 200 метров. Оптоволоконный кабель позволяет увеличивать длину кабеля до двух километров.

 Больший допустимый размер передаваемых данных в одном пакете по сравнению с сетью Ethernet сильно позволяет увеличить производительность сети: теоретически для скоростей передачи 16 Мбит/с и 100 Мбит/с длина поля данных может достигать даже 18 Кбайт, что принципиально при передаче больших объемов данных. Но даже при скорости 4 Мбит/с благодаря маркерному методу доступа сеть Token-Ring часто обеспечивает большую фактическую скорость передачи, чем сеть Ethernet (10 Мбит/с). Особенно заметно преимущество Token-Ring при больших нагрузках (свыше 30—40%), так как в этом случае метод CSMA/CD требует много времени на разрешение повторных конфликтов.

 Сеть Token-Ring в классическом варианте уступает сети Ethernet как по допустимому размеру, так и по максимальному количеству абонентов. Также по сравнению с аппаратурой Ethernet аппаратура Token-Ring заметно дороже, так как используется более сложный метод управления обменом. По скорости передачи - хотя и имеются версии Token-Ring на скорость 100 Мбит/с (High Speed Token-Ring, HSTR) и на 1000 Мбит/с (Gigabit Token-Ring), однако еще в 1999 году все производители оборудования, изначально поддержавшие эту инициативу, отказались от нее.

 В сети Token-Ring используется классический маркерный метод доступа, то есть по кольцу постоянно циркулирует маркер, к которому абоненты могут присоединять свои пакеты данных. Отсюда следует такое важное достоинство данной сети, как отсутствие конфликтов, но есть и недостатки, в частности необходимость контроля целостности маркера и зависимость функционирования сети от каждого абонента (в случае неисправности абонент обязательно должен быть исключен из кольца).

 Каждый абонент сети (его сетевой адаптер) должен выполнять следующие функции:

* выявление ошибок передачи;
* контроль конфигурации сети (восстановление сети при выходе из строя того абонента, который предшествует ему в кольце);
* контроль многочисленных временных соотношений, принятых в сети.

Большое количество функций, конечно, усложняет и удорожает аппаратуру сетевого адаптера.

 Для контроля целостности маркера в сети используется один из абонентов (так называемый активный монитор). При этом его аппаратура ничем не отличается от остальных, но его программные средства следят за временными соотношениями в сети и формируют в случае необходимости новый маркер.

 Активный монитор выполняет следующие функции:

* запускает в кольцо маркер в начале работы и при его исчезновении;
* регулярно (раз в 7 с) сообщает о своем присутствии специальным управляющим пакетом (AMP – Active Monitor Present);
* удаляет из кольца пакет, который не был удален пославшим его абонентом;
* следит за допустимым временем передачи пакета.

Активный монитор выбирается при инициализации сети, им может быть любой компьютер сети, но, как правило, становится первый включенный в сеть абонент. Абонент, желающий передавать пакет, ждет прихода свободного маркера и захватывает его. Захваченный маркер превращается в обрамление информационного пакета. Затем абонент передает информационный пакет в кольцо и ждет его возвращения. После этого он освобождает маркер и снова посылает его в сеть.

 В сети Token-Ring предусмотрено также использование мостов и коммутаторов. Они применяются для разделения большого кольца на несколько кольцевых сегментов, имеющих возможность обмена пакетами между собой. Это позволяет снизить нагрузку на каждый сегмент и увеличить долю времени, предоставляемую каждому абоненту.

 В результате можно сформировать распределенное кольцо, то есть объединение нескольких кольцевых сегментов одним большим магистральным кольцом или же звездно-кольцевую структуру с центральным коммутатором, к которому подключены кольцевые сегменты

Существует большое количество аппаратуры для сетей Token Ring, которая улучшает некоторые стандартные характеристики этих сетей: максимальную длину сети, расстояние между концентраторами, надежность (путем использования двойных колец).