

Информационные сети

Лекция 2.

Физический и канальный
уровень

Физический уровень

- Физический уровень в модели OSI служит основой для построения всей модели передачи данных между компьютерными системами.
- Физический уровень определяет электрические, механические, процедурные и функциональные спецификации для активизации, поддержания и деактивизации физической связи между конечными системами.
- Назначение физического уровня – передача данных. Процесс передачи данных – *кодирование* – выполняется с помощью *среды передачи данных* (кабели, разъемы и т.п.).

Среда передачи данных

- Средой передачи данных называют физическую среду, используемую для прохождения сигнала.
- Для обеспечения обмена кодированной информацией, среда должна обеспечить физическое соединение компьютеров друг с другом.
- Информация в локальных сетях чаще всего передается в последовательном коде, то есть бит за битом. Такая передача медленнее и сложнее, чем при использовании параллельного кода.
- Однако надо учитывать то, что при более быстрой параллельной передаче (по нескольким кабелям одновременно) увеличивается количество соединительных кабелей в число раз, равное количеству разрядов параллельного кода (например, в 8 раз при 8-разрядном коде).

Среда передачи данных

- Промышленностью выпускается огромное количество типов кабелей, например, только одна крупнейшая кабельная компания Belden предлагает более 2000 их наименований.
- Все кабели можно разделить на три большие группы:
 - электрические (медные) кабели на основе *витых пар* проводов (twisted pair), которые делятся на экранированные (shielded twisted pair, STP) и неэкранированные (unshielded twisted pair, UTP);
 - электрические (медные) *коаксиальные кабели* (coaxial cable);
 - *оптоволоконные кабели* (fiber optic).
- Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию.

Параметры кабельных систем

- Можно выделить следующие основные параметры кабелей, принципиально важные для использования в локальных сетях:
 - *Полоса пропускания* кабеля (частотный диапазон сигналов, пропускаемых кабелем) и *затухание сигнала* в кабеле. Два этих параметра тесно связаны между собой, так как с ростом частоты сигнала растет затухание сигнала. *Затухание* измеряется в децибелах и пропорционально длине кабеля.
 - **Помехозащищенность** кабеля и обеспечиваемая им **секретность** передачи информации. Эти два взаимосвязанных параметра показывают, как кабель взаимодействует с окружающей средой, то есть, как он реагирует на внешние помехи, и насколько просто прослушать информацию, передаваемую по кабелю.
 - **Скорость распространения сигнала** по кабелю или, обратный параметр – *задержка сигнала* на метр длины кабеля. Этот параметр имеет принципиальное значение при выборе длины сети. Типичные величины скорости распространения сигнала – от 0,6 до 0,8 от скорости распространения света в вакууме. Соответственно типичные величины *задержек* – от 4 до 5 нс/м.
 - Для электрических кабелей очень важна величина **волнового сопротивления** кабеля. Волновое сопротивление важно учитывать при согласовании кабеля для предотвращения отражения сигнала от концов кабеля. Волновое сопротивление зависит от формы и взаиморасположения проводников, от технологии изготовления и материала диэлектрика кабеля. Типичные значения волнового сопротивления – от 50 до 150 Ом.

Кабели на основе витых пар

- *Витые пары* проводов используется в дешевых и сегодня, пожалуй, самых популярных кабелях. Кабель на основе **витых пар** представляет собой несколько пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке.
- Кабель гибкий и удобный для прокладки. Скручивание проводов позволяет свести к минимуму индуктивные наводки кабелей друг на друга и снизить влияние переходных процессов.
- Обычно в кабель входит две или четыре *витые пары*.



Кабели на основе витых пар

- Неэкранированные *витые пары* характеризуются слабой защищенностью от внешних электромагнитных помех, а также от подслушивания, которое может осуществляться с целью, например, промышленного шпионажа. Причем перехват передаваемой по сети информации возможен как с помощью контактного метода (например, посредством двух иголок, воткнутых в кабель), так и с помощью бесконтактного метода, сводящегося к радиоперехвату излучаемых кабелем электромагнитных полей. Причем действие помех и величина излучения вовне увеличивается с ростом длины кабеля. Для устранения этих недостатков применяется экранирование кабелей.

Кабели на основе витых пар

- В случае экранированной *витой пары* STP каждая из *витых пар* помещается в металлическую оплетку-экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга (crosstalk – перекрестные наводки).
 - Для того чтобы экран защищал от помех, он должен быть обязательно заземлен.
- Основные достоинства неэкранированных *витых пар* – простота монтажа разъемов на концах кабеля, а также ремонта любых повреждений по сравнению с другими типами кабеля. Все остальные характеристики у них хуже, чем у других кабелей.
- В настоящее время *витая пара* используется для передачи информации на скоростях до 1000 Мбит/с.

Коаксиальный кабель

- **Коаксиальный кабель** представляет собой электрический кабель, состоящий из центрального медного провода и металлической оплетки (экрана), разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку.
- Коаксиальный кабель до недавнего времени был очень популярен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), более широкими, чем в случае витой пары, полосами пропускания (свыше 1ГГц), а также большими допустимыми расстояниями передачи (до километра).
- К нему труднее механически подключиться для несанкционированного прослушивания сети, он дает также заметно меньше электромагнитных излучений вонне.
 - Монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше (он дороже примерно в 1,5 – 3 раза).
- Сейчас его применяется реже, чем витая пара.

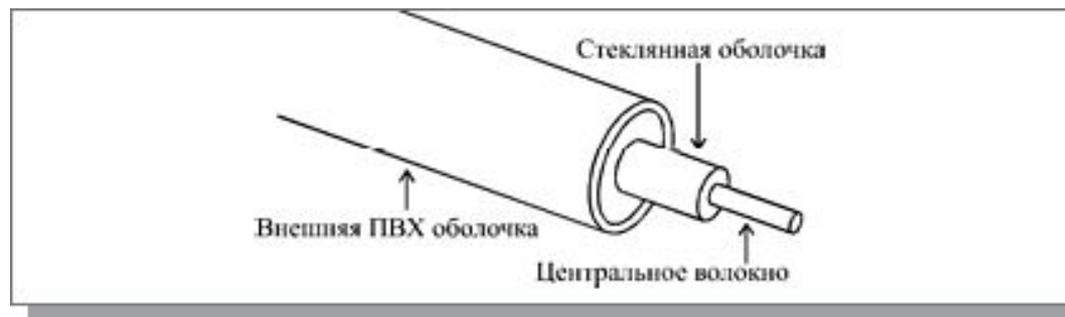


Коаксиальный кабель

- Основное применение *коаксиальный кабель* находит в сетях с топологией типа шина. При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один (и только один!) из терминаторов должен быть заземлен.
 - В отсутствие заземления металлическая оплетка не защищает сеть от внешних электромагнитных помех и не снижает излучение передаваемой по сети информации во внешнюю среду. При заземлении оплетки в двух или более точках из строя может выйти не только сетевое оборудование, но и компьютеры, подключенные к сети.
- Терминаторы должны быть обязательно согласованы с кабелем, необходимо, чтобы их сопротивление равнялось волновому сопротивлению кабеля.
- Существует два основных типа *коаксиального кабеля* для организации локальных сетей:
 - тонкий (thin) кабель, имеющий диаметр около 0,5 см, более гибкий;
 - толстый (thick) кабель, диаметром около 1 см, значительно более жесткий. Он представляет собой классический вариант *коаксиального кабеля*, который уже почти полностью вытеснен современным тонким кабелем.

Оптоволоконный кабель

- **Оптоволоконный (он же волоконно-оптический) кабель** – это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля.
- Информация передается не электрическим сигналом, а световым. Главный его элемент – это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.
- Структура *оптоволоконного кабеля* очень проста и похожа на структуру *коаксиального электрического кабеля*.
- Металлическая оплетка кабеля применяется для механической защиты от окружающей среды (такой кабель иногда называют *броневым*, он может объединять под одной оболочкой несколько *оптоволоконных кабелей*).



Оптоволоконный кабель

- *Оптоволоконный кабель* обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации.
 - Внешние электромагнитные помехи не способны исказить световой сигнал, а сам сигнал не порождает внешних электромагнитных излучений. Подключение к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как при этом нарушается целостность кабеля.
 - Стоимость *оптоволоконного кабеля* постоянно снижается и сейчас примерно равна стоимости тонкого *коаксиального кабеля*.
 - Типичная величина *затухания сигнала* в *оптоволоконных кабелях* на частотах, используемых в локальных сетях, составляет от 5 до 20 дБ/км, что примерно соответствует показателям электрических кабелей на низких частотах.
 - В случае *оптоволоконного кабеля* при росте частоты передаваемого сигнала *затухание* увеличивается очень незначительно, и на больших частотах (особенно свыше 200 МГц) его преимущества перед электрическим кабелем неоспоримы, у него просто нет конкурентов.

Оптоволоконный кабель

- Однако *оптоволоконный кабель* имеет и некоторые недостатки.
 - Высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит *затухание* в разьеме).
 - Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего такой же коэффициент преломления света, что и стекловолокно. Некачественная установка разъема резко снижает допустимую длину кабеля, определяемую *затуханием*.
 - Использование *оптоволоконного кабеля* требует специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что увеличивает стоимость сети в целом.

Оптоволоконный кабель

- *Оптоволоконные кабели* допускают разветвление сигналов (для этого производятся специальные пассивные **разветвители** (couplers) на 2—8 каналов), но, как правило, их используют для передачи данных только в одном направлении между одним передатчиком и одним приемником.
- *Оптоволоконный кабель* менее прочен и гибок, чем электрический. Типичная величина допустимого радиуса изгиба составляет около 10 – 20 см, при меньших радиусах изгиба центральное волокно может сломаться. Плохо переносит кабель и механическое растяжение, а также раздавливающие воздействия.
- Чувствителен *оптоволоконный кабель* и к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, то есть увеличивается *затухание сигнала*. Резкие перепады температуры также негативно сказываются на нем, стекловолокно может треснуть.
- Применяют *оптоволоконный кабель* только в сетях с топологией звезда и кольцо. Кабель обеспечивает идеальную гальваническую развязку компьютеров сети.

Типы оптоволоконного кабеля

- Существуют два различных типа *оптоволоконного кабеля*:
 - **многомодовый** или **мультимодовый** кабель, более дешевый, но менее качественный;
 - **одномодовый** кабель, более дорогой, но имеет лучшие характеристики по сравнению с первым.

Беспроводные системы передачи данных

- Главное преимущество беспроводных систем состоит в том, что не требуется никакой прокладки проводов.
- *Радиоканал* использует передачу информации по радиоволнам, поэтому теоретически он может обеспечить связь на многие десятки, сотни и даже тысячи километров.
- Скорость передачи достигает десятков мегабит в секунду (здесь многое зависит от выбранной длины волны и способа кодирования).

Беспроводные системы передачи данных

- Особенность *радиоканала* состоит в том, что сигнал свободно излучается в эфир, он не замкнут в кабель, поэтому возникают проблемы совместимости с другими источниками радиоволн (радио- и телевещательными станциями, радарам, радиоловительскими и профессиональными передатчиками и т.д.).
- В *радиоканале* используется передача в узком диапазоне частот и модуляция информационным сигналом несущей частоты.
- Главным недостатком *радиоканала* является его плохая защита от прослушивания, так как радиоволны распространяются неконтролируемо. Другой большой недостаток *радиоканала* – слабая помехозащищенность.
- *Радиоканал* широко применяется в глобальных сетях как для наземной, так и для спутниковой связи. В этом применении у *радиоканала* нет конкурентов, так как радиоволны могут дойти до любой точки земного шара.

Беспроводные системы передачи данных

- Для локальных беспроводных сетей (WLAN – Wireless LAN) в настоящее время применяются подключения по *радиоканалу* на небольших расстояниях (обычно до 100 метров) и в пределах прямой видимости.
- Используются два частотных диапазона – 2,4 ГГц и 5 ГГц. Скорость передачи – до 54 Мбит/с. Распространен вариант со скоростью 11 Мбит/с.
- Сети WLAN позволяют устанавливать беспроводные сетевые соединения на ограниченной территории (обычно внутри офисного или университетского здания или в таких общественных местах, как аэропорты).
- Технология Wi-Fi (Wireless Fidelity) позволяет организовать связь между компьютерами числом от 2 до 15 с помощью концентратора (называемого точка доступа, Access Point, AP), или нескольких концентраторов, если компьютеров от 10 до 50.

Беспроводные системы передачи данных

- Инфракрасный канал также не требует соединительных проводов, так как использует для связи инфракрасное излучение (подобно пульту дистанционного управления домашнего телевизора). Главное его преимущество по сравнению с *радиоканалом* – нечувствительность к электромагнитным помехам, что позволяет применять его, например, в производственных условиях, где всегда много помех от силового оборудования.
- Скорости передачи информации по инфракрасному каналу обычно не превышают 5–10 Мбит/с, но при использовании инфракрасных лазеров может быть достигнута скорость более 100 Мбит/с. Секретность передаваемой информации, как и в случае *радиоканала*, не достигается, также, требуются сравнительно дорогие приемники и передатчики. Все это приводит к тому, что применяют инфракрасные каналы в локальных сетях довольно редко. В основном они используются для связи компьютеров с периферией (интерфейс IrDA).
- Инфракрасные каналы делятся на две группы:
 - Каналы прямой видимости.
 - Каналы на рассеянном излучении.

Выбор типа среды передачи данных

- Для определения наиболее подходящего типа среды передачи данных могут использоваться различные критерии, например, скорость передачи данных, стоимость, проблемы обеспечения конфиденциальности.

Канальный уровень

- Протоколы канального уровня обеспечивают интерфейс между физической сетью и стеком протоколов компьютера.
- Протокол канального уровня, обычно, включает три элемента:
 - *Кадр* специального формата, который инкапсулирует данные протокола сетевого уровня;
 - Механизма, регулирующего доступ к совместно используемой сетевой среде;
 - Принципов, которые должны быть реализованы при разработке физического уровня.

Адресация

- Заголовок канального уровня содержит адрес компьютера, отправившего сообщения, и адрес компьютера, который должен данное сообщение получить.
- На этом уровне используются адреса среды передачи данных – аппаратные (MAC) адреса.
- Данные адреса часто «прошиваются» производителем в сетевом контроллере.
- В сетях Ethernet и Token Ring используются адреса длиной 6 байт.

Доставка кадров

- Протоколы канального уровня заботятся о доставке пакета конечному адресату, только если он находится в той же локальной сети, что и отправитель.
- Если получатель находится в другой вычислительной сети, протокол канального уровня отвечает за доставку кадра маршрутизатору, обеспечивающему доступ к следующей сети следования кадра.
- Таким образом, адрес получателя в заголовке протокола канального уровня всегда относится к устройству, расположенному в локальной сети.

Управление доступом к среде

- Управление доступом к среде – набор правил посредством которых протокол канального уровня разрешает спорные ситуации, связанные с попытками одновременного использования среды передачи данных.
- Для функционирования в сетевой среде рабочая станция должна иметь возможность передавать информацию.
- Для контроля доступа к среде передачи данных используются два метода:
 - Метод доступа с передачей маркера;
 - Множественный доступ с контролем несущей и обнаружением коллизий.

Способы контроля доступом к среде передачи данных

- *Метода доступа с передачей маркера* используется в сетях Token Ring и FDDI.
- Метод основан на передаче от одной рабочей станции к другой специального кадра, называемого *маркером*.
- Только система, овладевшая кадром, имеет право отправлять свои сообщения. Рабочая станция, захватившая кадр, передает свои данные и освобождает маркер для других станций.
- Пока в сети перемещается один маркер, передача данных одновременно двумя системами невозможна.

Способы контроля доступом к среде передачи данных

- Метод *множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD)* состоит в том, что рабочая станция прослушивает сетевой кабель и передает информацию только в том случае, если сетевая среда свободна.
- В CSMA/CD сетях возможна ситуация, когда несколько станций начнут передавать данные одновременно. Результат – появление *коллизий*.
- Для исправления данной ситуации система имеет механизм, позволяющий выявить возникшие коллизии и повторно передать потерянные данные.
- Данный метод используется в сетях Ethernet.

Индикатор протокола

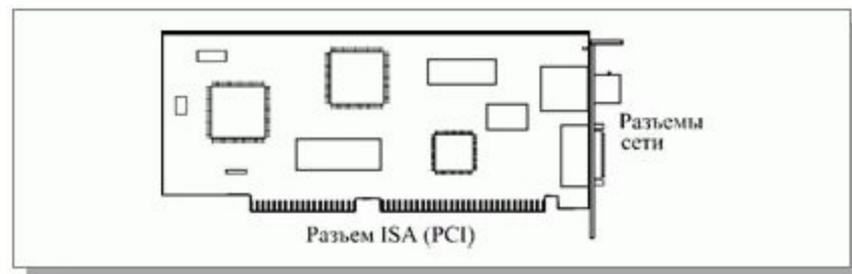
- Большинство реализаций канального уровня разрабатываются для поддержки нескольких протоколов сетевого уровня.
- Для осуществления возможности использования множества протоколов сетевого уровня, заголовок канального уровня должен содержать указатель, определяющий тип использующего протокола сетевого уровня.
- Например, в сети включающей серверы под управлением Windows 2000 и NetWare, одни кадры переносят IP-датаграммы, другие – пакеты IPX протокола. Чтобы различать два эти протокола в спецификации Ethernet определено поле заголовка, идентифицирующего протокол.

Выявление ошибок

- В большинстве протоколов канального уровня используется специальный участок информации, идущий за собственно данными пакета сетевого уровня (трейлер кадра).
- Эта информация содержит поле *контрольной последовательности кадра (FCS)*. Данное поле применяется для выявления ошибок, возникающих в процессе передачи данных. При нарушении целостности пакета принимающая сторона его отвергает.
- Канальный уровень не предполагает, что принимающая сторона предпримет действия при отбраковывании пакетов. В модели OSI данные функции возложены на протоколы более высокого уровня.

Сетевые адаптеры

- Сетевые адаптеры (они же контроллеры, карты, платы, интерфейсы, NIC – Network Interface Card) – это основная часть аппаратуры локальной сети.
- Назначение сетевого адаптера – сопряжение компьютера (или другого абонента) с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена.
- Сетевые адаптеры реализуют функции двух нижних уровней модели OSI.
- Как правило, сетевые адаптеры выполняются в виде платы, вставляемой в слоты расширения системной магистрали (шины) компьютера (чаще всего PCI, ISA или PC-Card). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.



Сетевые адаптеры

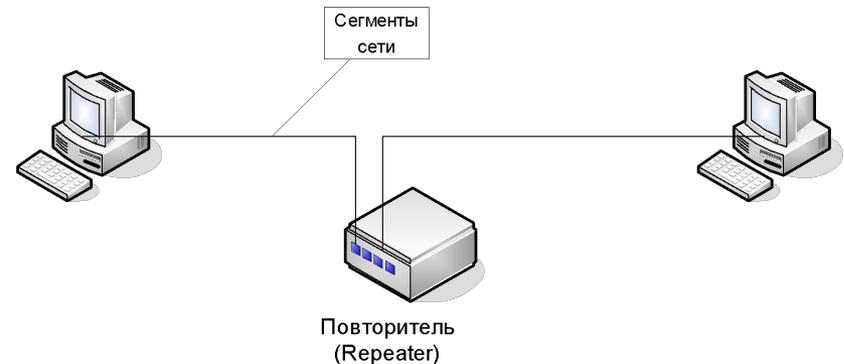
- Функции сетевого адаптера делятся на магистральные и сетевые.
- К **магистральным** относятся те функции, которые осуществляют взаимодействие адаптера с магистралью (системной шиной) компьютера (то есть опознание своего магистрального адреса, пересылка данных в компьютер и из компьютера, выработка сигнала прерывания компьютера и т.д.).
- **Сетевые** функции обеспечивают общение адаптера с сетью.

Основные функции сетевых адаптеров

- К основным сетевым функциям адаптеров относятся:
 - гальваническая развязка компьютера и кабеля локальной сети (для этого обычно используется передача сигналов через импульсные трансформаторы);
 - преобразование логических сигналов в сетевые (электрические или световые) и обратно;
 - кодирование и декодирование сетевых сигналов, то есть прямое и обратное преобразование сетевых кодов передачи информации (например, манчестерский код);
 - опознание принимаемых пакетов (выбор из всех входящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно);
 - преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
 - буферирование передаваемой и принимаемой информации в буферной памяти адаптера;
 - организация доступа к сети в соответствии с принятым методом управления обменом;
 - подсчет контрольной суммы пакетов при передаче и приеме.

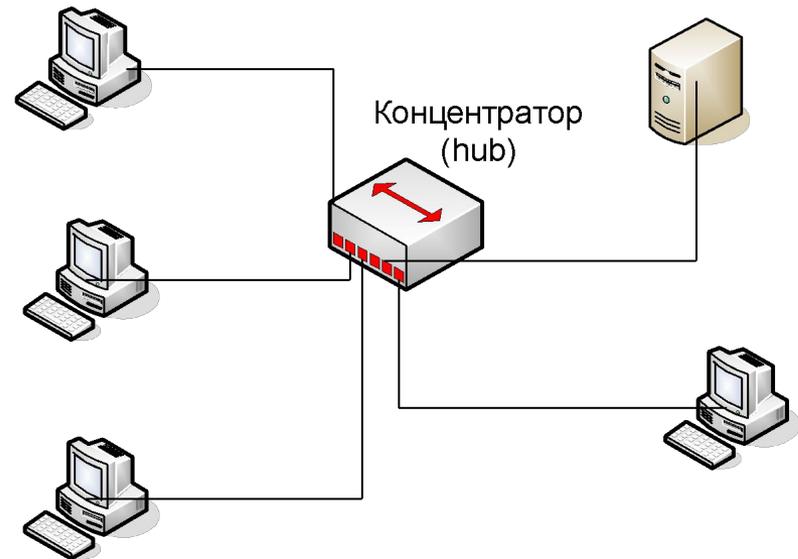
Повторители

- При передачи по кабелю сигнал постепенно слабеет. Данное ослабление сигнала называется **затуханием**. Эффект затухания зависит от типа кабеля и приводит к ограничению длины отдельного сегмента кабеля.
- Для продолжения кабеля используются специальные устройства – повторители (repeater), которые усиливают сигнал. Благодаря усилению сигнал распространяется на большие расстояния.



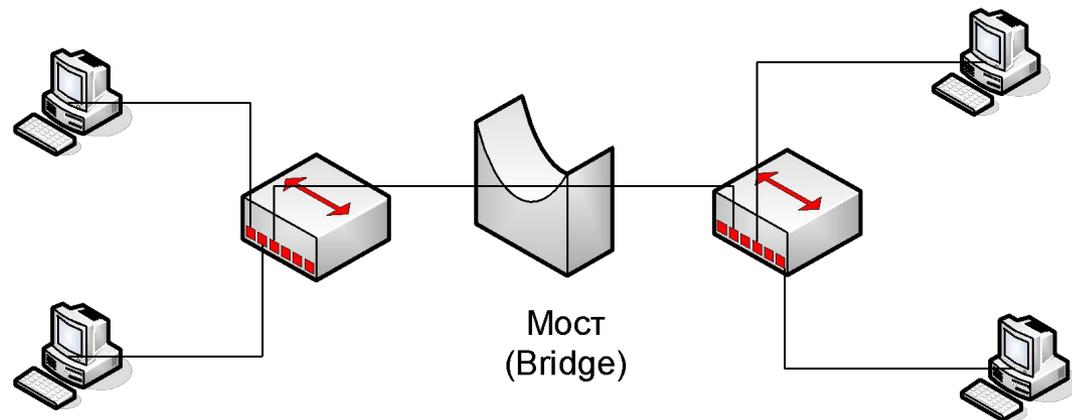
Концентраторы

- Концентратор (hub) – устройство, выполняющее функции связующего отдельные сегменты сети и усиливающего сигнал в сетях с топологией типа «звезда».
- Термин концентратор используется для технологии Ethernet, в сетях Token Ring аналогичное устройство называется *модулем множественного доступа*.
- Ретранслирующие концентраторы обеспечивают усиление сигнала.
- Ограничение на число концентраторов между точками подключения составляет – 4 устройства.



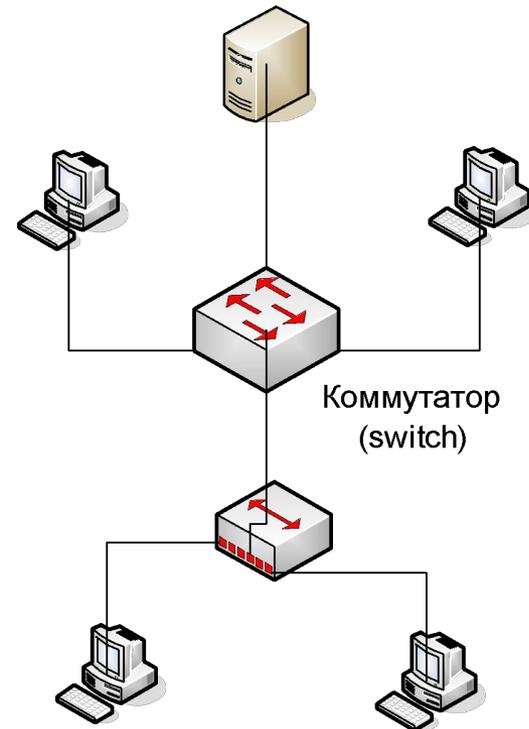
МОСТЫ

- Мост (bridge) – устройство, используемое для объединения сегментов кабеля ЛВС, но в отличие от концентраторов функционирующее на физическом и канальном уровнях.
- Мост позволяет осуществлять фильтрацию передаваемых пакетов по физическому адресу. Мост не изменяет содержимое кадров и не учитывает данные протоколов сетевого и более высокого уровней.



Коммутаторы

- Коммутатор ЛВС (switch) – многопортовое устройство, каждый порт которого связан со своим сегментом сети.
- Внешне похож на концентратор, но в отличие от последнего коммутатор направляет входящий трафик на один порт, необходимый для достижения места назначения.
- Коммутатор функционирует на 2 уровне модели OSI, поддерживая различные протоколы сетевого уровня.



Литература

- 1. В. Амато. Основы организации сетей Cisco.
- 2. В.Г. Олифер, Н.А. Олифер. Основы сетей передачи данных.
- Ю.В. Новиков, С.В. Кондратенко. Основы локальных сетей.
- К. Закер. Компьютерные сети. Модернизация и поиск неисправностей.