Вопросы к экзамену «Компьютерные сети»

1. Назначение сетей. Основные определения и термины. Преимущества использования сетей.

Сеть – это совокупность объектов, образуемых устройствами передачи и обработки данных. Международная организация по стандартизации определила компьютерную сеть *как последовательную бит-ориентированную передачу информации между связанными друг с другом независимыми устройствами*.

В общем случае различают два понятия сети: коммуникационная сеть и информационная сеть.

Коммуникационная сеть предназначена для передачи данных, также она выполняет задачи, связанные с преобразованием данных. Коммуникационные сети различаются по типу используемых физических средств соединения.

Информационная сеть предназначена для хранения информации и состоит из ***информационных систем***. На базе коммуникационной сети может быть построена группа информационных сетей.

Под ***информационной системой*** следует понимать систему, которая является поставщиком или потребителем информации.

Вычислительная сеть – это одна из разновидностей распределенных систем, предназначенная для распараллеливания вычислений, за счет чего может быть достигнуто повышение производительности и отказоустойчивости системы.

В общем, компьютерная сеть состоит из информационных систем и каналов связи.

Под ***информационной системой*** в данном случае следует понимать объект, способный осуществлять хранение, обработку или передачу информации. В состав информационной системы входят: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных. В дальнейшем информационная система, предназначенная для решения задач пользователя, будет называться – ***рабочая станция*** (***client***). Рабочая станция в сети отличается от обычного персонального компьютера (ПК) наличием ***сетевой карты*** (***сетевого адаптера***), канала для передачи данных и сетевого программного обеспечения.

Под ***каналом связи*** следует понимать путь или средство, по которому передаются сигналы. Средство передачи сигналов называют ***физическим каналом .Абонентский канал*** – это физический канал, соединяющий коммуникационную сеть с абонентской системой. Параметры и характеристики абонентского канала в точке подключения системы определяется абонентским интерфейсом.

Каналы связи создаются по ***линиям связи*** при помощи сетевого оборудования и физических средств связи. Физические средства связи построены на основе витых пар, коаксиальных кабелей, оптических каналов или эфира. Между взаимодействующими информационными системами через физические каналы коммуникационной сети и узлы коммутации устанавливаются *логические каналы*.

Логический канал – это путь для передачи данных от одной системы к другой. Логический канал прокладывается по маршруту в одном или нескольких физических каналах. Логический канал можно охарактеризовать, как маршрут, проложенный через физические каналы и узлы коммутации.

Информация в сети передается ***блоками данных*** по процедурам обмена между объектами. Эти процедуры называют ***протоколами передачи данных.***

Протокол – это совокупность правил, устанавливающих формат и процедуры обмена информацией между двумя или несколькими устройствами.

Интерфейс – совокупность средств и методов взаимодействия между элементами или устройствами системы. Интерфейсы являются основой взаимодействия всех современных информационных систем. Если интерфейс какого-либо объекта (рабочей станции, сетевой карты, программы и т.д.) не изменяется (стандартизирован), это даёт

возможность модифицировать сам объект, не перестраивая принципы его взаимодействия с другими объектами.

Загрузка сети характеризуется параметром, называемым трафиком.

Трафик – это поток сообщений в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящих блоков данных и их длины, выраженное в битах в секунду.

Существенное влияние на характеристику сети оказывает метод доступа.

Метод доступа – это способ определения того, как сеть управляет доступом к каналу связи (кабелю), существенно влияет на ее характеристики. В сети все рабочие станции физически соединены между собою каналами связи по определенной структуре, называемой топологией.

Топология – это описание физических соединений в сети, указывающее какие рабочие станции могут связываться между собой. Тип топологии определяет производительность, работоспособность и надежность эксплуатации рабочих станций, а также время обращения к файловому серверу. В зависимости от топологии сети используется тот или иной метод доступа.

Состав основных элементов в сети зависит от ее архитектуры.

Архитектура – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети. Она предусматривает логическую, функциональную и физическую организацию технических и программных средств сети. Архитектура определяет принципы построения и функционирования аппаратного и программного обеспечения элементов сети.

Основные преимущества сетей вытекают из их принадлежности к распределенным системам.

Концептуальным преимуществом распределенных систем (а значит, и сетей) перед централизованными системами является их способность выполнять параллельные вычисления. За счет этого в системе с несколькими обрабатывающими узлами в принципе может быть достигнута производительность, превышающая максимально возможную на данный момент производительность любого отдельного, сколь угодно мощного процессора. Распределенные системы потенциально имеют лучшее соотношение производительность-стоимость, чем централизованные системы.

Еще одно очевидное и важное достоинство распределенных систем – это их принципиально более высокая отказоустойчивость. Основой повышенной отказоустойчивости распределенных систем является ***избыточность***. Избыточность обрабатывающих узлов (процессоров в многопроцессорных системах или компьютеров в сетях) позволяет при отказе одного узла переназначать приписанные ему задачи на другие узлы. С этой целью в распределенной системе могут быть предусмотрены процедуры динамической или статической реконфигурации. В вычислительных сетях некоторые наборы данных могут дублироваться на внешних запоминающих устройствах нескольких компьютеров сети, так что при отказе одного их них данные остаются доступными.

Для пользователя, кроме выше названных, распределенные системы дают еще и такие преимущества, как возможность совместного использования данных и устройств, а также возможность гибкого распределения работ по всей системе. Такое разделение дорогостоящих периферийных устройств – таких как дисковые массивы большой емкости, цветные принтеры, графопостроители, модемы, оптические диски – во многих случаях является основной причиной развертывания сети на предприятии.

В последнее время стал преобладать другой побудительный мотив развертывания сетей, гораздо более важный в современных условиях, чем экономия средств за счет разделения между сотрудниками корпорации дорогой аппаратуры или программ. Этим мотивом стало стремление обеспечить сотрудникам оперативный доступ к обширной корпоративной информации. В условиях жесткой конкурентной борьбы в любом секторе рынка выигрывает, в конечном счете, та фирма, сотрудники которой могут быстро и

правильно ответить на любой вопрос клиента: о возможностях их продукции, об условиях ее применения, о решении любых возможных проблем и т. п. В большой корпорации вряд ли даже хороший менеджер может знать все тонкости каждого из выпускаемых фирмой продуктов, тем более что их номенклатура обновляется сейчас каждый квартал, если не месяц. Поэтому очень важно, чтобы менеджер имел возможность со своего компьютера, подключенного к корпоративной сети, скажем в Минске, передать вопрос клиента на сервер, расположенный в центральном отделении предприятия в Жодино, и оперативно получить качественный ответ, удовлетворяющий клиента. В этом случае клиент не обратится к другой фирме, а будет пользоваться услугами данного менеджера и впредь.

Этот аспект сетевой работы всегда был узким местом в организации доставки информации сотрудникам – даже при существовании мощных СУБД информация в них попадала не самая «свежая» и не в том объеме, который был нужен. В последнее время в этой области наметился некоторый прогресс, связанный с использованием гипертекстовой информационной службы WWW – так называемой технологии ***intranet***. Эта технология поддерживает достаточно простой способ представления текстовой и графической информации в виде гипертекстовых страниц, что позволяет быстро поместить самую свежую информацию на WWW-серверы корпорации. Кроме того, она унифицирует просмотр информации с помощью стандартных программ – Web-*браузеров*, работа с которыми несложна даже для неспециалиста.

2. Архитектура терминал – главный компьютер.

Архитектура «терминал – главный компьютер» (terminal–host computer architecture) – это концепция информационной сети, в которой вся обработка данных осуществляется одним или группой главных компьютеров.

Рассматриваемая архитектура предполагает два типа оборудования:

– главный компьютер, где осуществляется управление сетью, хранение и обработка данных;

– терминалы, предназначенные для передачи главному компьютеру команд на организацию сеансов и выполнения заданий, ввода данных для выполнения заданий и получения результатов.

Главный компьютер через *мультиплексоры* передачи данных (МПД) взаимодействуют с терминалами, как представлено на рис. 2.1. Классический пример архитектуры сети с главными компьютерами –системная сетевая архитектура (System Network Architecture – SNA).

3. Одноранговая архитектура. Архитектура клиент – сервер.

Одноранговая архитектура (peer-to-peer architecture) – это концепция информационной сети, в которой ее ресурсы рассредоточены по всем взаимодействующим между собой системам (рис. 2.2). Данная архитектура характеризуется тем, что в ней все системы равноправны.

К одноранговым сетям относятся малые сети, где любая рабочая станция может выполнять одновременно функции файлового сервера и рабочей станции. В одноранговых ЛВС дисковое пространство и файлы на любом компьютере могут быть общими. Чтобы ресурс стал общим, его необходимо отдать в общее пользование, используя службы удаленного доступа сетевых одноранговых операционных систем. В зависимости от того, как будет установлена защита данных, другие пользователи смогут пользоваться файлами сразу же после их создания. Одноранговые ЛВС достаточно хороши только для небольших рабочих групп.

Одноранговые ЛВС являются наиболее легким и дешевым типом сетей для установки. Они требуют на компьютере, кроме сетевой карты и сетевого носителя, наличие пользовательской операционной системы. При соединении компьютеров, пользователи могут предоставлять ресурсы и информацию в совместное пользование.

Одноранговые сети имеют следующие преимущества:

– они легки в установке и настройке;

– отдельные ПК не зависят от выделенного сервера;
– пользователи в состоянии контролировать свои ресурсы;
– малая стоимость и легкая эксплуатация;
– минимум оборудования и программного обеспечения;
– нет необходимости в администраторе;
– хорошо подходят для сетей с количеством пользователей, не превышающим десяти.

Проблемой одноранговой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают виды сервиса, которые они предоставляли. Сетевую безопасность одновременно можно применить только к одному ресурсу, и пользователь должен помнить столько паролей, сколько сетевых ресурсов. При получении доступа к разделяемому ресурсу ощущается падение производительности компьютера. Существенным недостатком одноранговых сетей является отсутствие централизованного администрирования.

Использование одноранговой архитектуры не исключает применения в той же сети также архитектуры «терминал – главный компьютер» или архитектуры «клиент – сервер».

Архитектура клиент–сервер (client-server architecture) – это концепция информационной сети, в которой основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов (рис. 2.3). Рассматриваемая архитектура определяет два типа компонентов: серверы и клиенты.

Сервер – это объект, предоставляющий сервис другим объектам сети по их запросам. ***Сервис*** – это процесс обслуживания клиентов.

Сервер работает по заданиям клиентов и управляет выполнением их заданий. После выполнения каждого задания сервер посылает полученные результаты клиенту, пославшему это задание.

Сервисная функция в архитектуре клиент–сервер описывается комплексом прикладных программ, в соответствии с которым выполняются разнообразные прикладные процессы.

Процесс, который вызывает сервисную функцию с помощью определенных операций, называется клиентом. Им может быть программа или пользователь. На рис. 2.4 приведен перечень сервисов в архитектуре клиент – сервер.

Клиенты – это рабочие станции, которые используют ресурсы сервера и предоставляют удобные интерфейсы пользователя. ***Интерфейсы пользователя*** – это процедуры взаимодействия пользователя с системой или сетью.

Клиент является инициатором и использует электронную почту или другие сервисы сервера. В этом процессе клиент запрашивает вид обслуживания, устанавливает сеанс, получает нужные ему результаты и сообщает об окончании работы.

В ***сетях с выделенным файловым сервером*** на выделенном автономном ***ПК*** (персональном компьютере) устанавливается серверная сетевая операционная система. Этот ПК становится сервером. Программное обеспечение (***ПО***), установленное на рабочей станции, позволяет ей обмениваться данными с сервером. Наиболее распространенные сетевые операционная системы:

– NetWare фирмы Novel;
– Windows фирмы Microsoft;
– UNIX фирмы AT&T;
– Linux.

Помимо сетевой операционной системы необходимы сетевые прикладные программы, реализующие преимущества, предоставляемые сетью.

Сети на базе серверов имеют лучшие характеристики и повышенную надежность. Сервер владеет главными ресурсами сети, к которым обращаются остальные рабочие станции.

В современной клиент-серверной архитектуре выделяется четыре группы объектов: клиенты, серверы, данные и сетевые службы. Клиенты располагаются в системах на рабочих местах пользователей. Данные в основном хранятся в серверах. Сетевые службы являются совместно используемыми серверами и данными. Кроме того службы управляют процедурами обработки данных.

Сети клиент-серверной архитектуры имеют следующие преимущества:

– позволяют организовывать сети с большим количеством рабочих станций;

– обеспечивают централизованное управление учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;

– эффективный доступ к сетевым ресурсам;

– пользователю нужен один пароль для входа в сеть и для получения доступа ко всем ресурсам, на которые распространяются права пользователя.

Наряду с преимуществами сети клиент – серверной архитектуры имеют и ряд недостатков:

– неисправность сервера может сделать сеть неработоспособной, как минимум потерю сетевых ресурсов;

– требуют квалифицированного персонала для администрирования;

– имеют более высокую стоимость сетей и сетевого оборудования.

4. Топология вычислительной сети. Виды топологий. Топология общая шина.

Понятие ***топологии*** широко используется при создании сетей. Одним из подходов к классификации топологий ЛВС является выделение двух основных классов топологий: широковещательные и последовательные.

В ***широковещательных топологиях*** ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: общая шина, дерево, звезда.

В ***последовательных топологиях*** информация передается только одному ПК. Примерами таких топологий являются: произвольная (произвольное соединение ПК), кольцо.

При выборе оптимальной топологии преследуются три основных цели:

– обеспечение *альтернативной маршрутизации* и максимальной надежности передачи данных;

– выбор *оптимального маршрута* передачи блоков данных;

– предоставление приемлемого *времени ответа* и нужной *пропускной способности*.

При выборе конкретного типа сети важно учитывать ее топологию. Основными сетевыми топологиями являются: шинная (линейная) топология, звездообразная, кольцевая и древовидная.

Например, в конфигурации сети ArcNet используется одновременно и линейная, и звездообразная топология. Сети Token Ring физически выглядят как звезда, но логически их пакеты передаются по кольцу. Передача данных в сети Ethernet происходит по линейной шине, так что все станции видят сигнал одновременно.

Существуют пять основных топологий:

– *общая шина* (Bus);

– *кольцо* (Ring);

– звезда (Star);

– *древовидная* (Tree);

– *ячеистая* (Mesh).

Также возможны комбинации нескольких различных топологий.

Общая шина – это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля, называемого *сегментом*.

Топология «*общая шина*» предполагает использование одного кабеля, к которому подключаются все компьютеры сети. В случае топологии «общая шина» кабель используется всеми станциями по очереди. Для уменьшения зашумленности среды

отраженными сигналами, мешающим передаче данных, используют так называемые «*терминаторы*» – специальные резистры на концах кабеля, предотвращающие появление «отраженной волны».

Все сообщения, посылаемые отдельными компьютерами, принимаются и прослушиваются всеми остальными компьютерами, подключенными к сети. Рабочая станция отбирает адресованные ей сообщения, пользуясь ***адресной информация***" информацией. Надежность здесь выше, так как выход из строя отдельных компьютеров не нарушит работоспособность сети в целом. Поиск неисправности в сети затруднен. Кроме того, так как используется только один кабель, в случае обрыва нарушается работа всей сети. Шинная топология – это наиболее простая и наиболее распространенная топология сети.

Примерами использования топологии общая шина является сеть 10Base-5 (соединение ПК толстым коаксиальным кабелем) и 10Base-2 (соединение ПК тонким коаксиальным кабелем).

5. Топология кольцо.

«Кольцо» – это топология ЛВС, в которой каждая рабочая станция соединена с двумя другими рабочими станциями, образуя кольцо. Данные передаются от одной рабочей станции к другой в одном направлении (по кольцу).

Каждая рабочая станция выполняет роль *повторителя*, ретранслируя сообщения к следующей рабочей станции, т. е. данные, передаются от одного компьютера к другому как бы по эстафете. Если компьютер получает данные, предназначенные для другого компьютера, он передает их дальше по кольцу, в ином случае они дальше не передаются.

Основная проблема при кольцевой топологии заключается в том, что каждая рабочая р станция должна активно участвовать в пересылке информации, и в случае выхода из строя хотя бы одной из них, вся сеть парализуется. Подключение новой рабочей станции требует краткосрочного выключения сети, так как во время установки кольцо должно быть разомкнуто. Топология «кольцо» имеет хорошо предсказуемое время отклика, определяемое числом рабочих станций.

Чистая кольцевая топология используется редко. Вместо этого кольцевая топология играет транспортную роль в схеме метода доступа. Кольцо описывает логический маршрут, а пакет передается от одной станции к другой, совершая в итоге полный круг.

В сетях ***Token Ring*** кабельная ветвь из центрального концентратора называется MAU (Multiple Access Unit). MAU имеет внутреннее кольцо, соединяющее все подключенные к нему станции, и используется как альтернативный путь, когда оборван или отсоединен кабель одной рабочей станции. Когда кабель рабочей станции подсоединен к MAU, он просто образует расширение кольца: сигналы поступают к рабочей станции, а затем возвращаются обратно во внутреннее кольцо.

6. Топология звезда.

«Звезда» – это топология ЛВС (рис. 2.7), в которой все рабочие станции присоединены к центральному узлу (например, к концентратору), который устанавливает, поддерживает и разрывает связи между рабочими станциями.

Преимуществом такой топологии является возможность простого исключения неисправного узла. Однако, если неисправен центральный узел, вся сеть выходит из строя. В этом случае каждый компьютер через специальный сетевой адаптер подключается отдельным кабелем к объединяющему устройству.

При необходимости можно объединять вместе несколько сетей с топологией «звезда», при этом получаются разветвленные конфигурации сети. В каждой точке ветвления необходимо использовать специальные соединители (распределители, повторители или устройства доступа).

Примером звездообразной топологии является топология **Ethernet** с кабелем типа ***витая пара*** 10BASE-T, 100BASE-T и т. д. ***Центром*** «звезды» обычно является *Hub* (***хаб, концентратор***).

Звездообразная топология обеспечивает защиту от разрыва кабеля. Если кабель рабочей станции будет поврежден, это не приведет к выходу из строя всего сегмента сети. Она позволяет также легко диагностировать проблемы подключения, так как каждая рабочая станция имеет свой собственный кабельный сегмент, подключенный к концентратору. Для диагностики достаточно найти разрыв кабеля, который ведет к неработающей станции. Остальная часть сети продолжает нормально работать.

Однако звездообразная топология имеет и недостатки. Во-первых, она требует много кабеля. Во-вторых, концентраторы довольно дороги. В-третьих, кабельные концентраторы при большом количестве кабеля трудно обслуживать. Однако в большинстве случаев в такой топологии используется недорогой кабель типа *витая пара*. В некоторых случаях можно даже использовать существующие телефонные кабели. Кроме того, для диагностики и тестирования выгодно собирать все кабельные концы в одном месте. По сравнению с концентраторами **ArcNet** концентраторы Ethernet и MAU Token Ring достаточно дороги. Новые подобные концентраторы включают в себя средства тестирования и диагностики, что делает их еще более дорогими.

7. Древовидные топологии.

Кроме трех рассмотренных базовых топологий нередко применяется также сетевая топология «***дерево***» (tree), которую можно рассматривать как комбинацию нескольких звезд. Причем, как и в случае «звезды», «дерево» может быть активным или истинным (рис. 2.8).

Также «дерево» может быть пассивным (рис. 2.9). При ***активном «дереве»*** в центрах объединения нескольких линий связи находятся центральные компьютеры, а при ***пассивном*** – концентраторы (хабы).

В отличие от классической топологии дерево, в которой все связи между узлами одинаковы, связи в утолщенном дереве становятся более широкими (производительными по пропускной способности) с каждым уровнем по мере приближения к корню дерева. Часто используют удвоение пропускной способности на каждом уровне. Сети с топологией fat tree являются предпочтительными для построения кластерных межсоединений

8. Ячеистые топологии.

В *сеточной* (*ячеистой топология*") (mesh) топологии компьютеры связываются между собой не одной, а многими линиями связи, образующими сетку.

В *полной сеточной топологии* каждый компьютер напрямую связан со всеми остальными компьютерами. В этом случае при увеличении числа компьютеров резко возрастает количество линий связи. Кроме того, любое изменение в конфигурации сети требует внесения изменений в сетевую аппаратуру всех компьютеров, поэтому полная сеточная топология не получила широкого распространения.

Частичная сеточная топология предполагает прямые связи только для самых активных компьютеров, передающих максимальные объемы информации. Остальные компьютеры соединяются через промежуточные узлы. Сеточная топология позволяет выбирать маршрут для доставки информации от абонента к абоненту, обходя неисправные участки. С одной стороны, это увеличивает надежность сети, с другой же – требует существенного усложнения сетевой аппаратуры, которая должна выбирать маршрут.

В заключение несколько слов о ***решетчетой*** топологии, в которой узлы образуют регулярную многомерную решетку. При этом каждое ребро решетки параллельно ее оси и соединяет два смежных узла вдоль этой оси.

Одномерная «решётка» – это цепь, соединяющая два внешних узла (имеющие лишь одного соседа) через некоторое количество внутренних (у которых по два соседа – слева и справа). При соединении обоих внешних узлов получается топология «кольцо». Двух- и трехмерные решетки используются в архитектуресуперкомпьютеров. Многомерная решётка, соединенная циклически в более чем одном измерении, называется «тор».

Основным достоством топологии «решетка» является высокая надежность, а недостатком – сложность реализации.

9. Комбинированные топологии.

Довольно часто применяются комбинированные топологии, среди которых наиболее распространены *звездно-шинная* (star-bus) (рис. 2.11) и *звездно-кольцевая*(star-ring) (рис. 2.12).

В звездно-шинной топологии используется комбинация шины и пассивной «звезды». К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. На самом деле реализуется физическая топология шина, включающая все компьютеры сети. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. К каждому из концентраторов при этом подключаются отдельные компьютеры или шинные сегменты. В результате получается звездно-шинное «дерево». Таким образом, пользователь может гибко комбинировать преимущества шинной и звездной топологий, а также легко изменять количество компьютеров, подключенных к сети. С точки зрения распространения информации данная топология равноценна классической шине.

В случае звездно-кольцевой топологии в кольцо объединяются не сами компьютеры, а специальные концентраторы (изображенные на рис. 2.11 в виде прямоугольников), к которым в свою очередь подключаются компьютеры с помощью звездообразных двойных линий связи. В действительности все компьютеры сети включаются в замкнутое кольцо, так как внутри концентраторов линии связи образуют замкнутый контур. Данная топология дает возможность комбинировать преимущества звездной и кольцевой топологий. Например, концентраторы позволяют собрать в одно место все точки подключения кабелей сети. Если говорить о распространении информации, данная топология равноценна классическому кольцу.

10. Метод доступа CSMA/CD.

Множественный доступ с прослушиванием несущей и разрешением коллизий (Carrier Sense Multiple Access with Collision Detection – CSMA/CD).

устанавливает следующий порядок: если рабочая станция «хочет» воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала: начинать передачу рабочая станция может, если канал свободен.

В процессе передачи рабочая станция продолжает прослушивание сети для обнаружения возможных конфликтов (коллизий). Если возникает конфликт из-за того, что два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата соответствующего компьютера выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу. Принимающая рабочая станция отбрасывает частично принятое сообщение, а все рабочие станции, желающие передать сообщение, в течение некоторого, случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

Все сетевые интерфейсные платы запрограммированы на разные псевдослучайные промежутки времени ожидания. Если конфликт возникнет во время повторной передачи сообщения, этот промежуток времени будет увеличен.

Стандарт типа ***Ethernet*** определяет сеть с конкуренцией, в которой несколько рабочих станций должны конкурировать друг с другом за право доступа к сети.

В некоторых сетях применяется метод доступа ***Demand Priority***, который является развитием метода доступа CSMA/CD и обеспечивает более справедливое распределение пропускной способности сети. Этот метод доступа поддерживает приорететный доступ для синхронных приложений.

Метод доступа Demand Priority основан на передаче концентратору функций арбитра, решающего проблему доступа к разделяемой среде. Концентратор циклически выполняет опрос портов. Рабочая станция, желающая передать пакет, посылает специальный низкочастотный сигнал концентратору, запрашивая передачу кадра и указывая его

приоретет (низкий, высокий). Низкий уровень приоритета соответствует обычным данным (файловая служба, служба печати и т. п.), а высокий приоритет соответствует данным, чувствительным к временным задержкам (например, мультимедиа).

11. Метод доступа TPMA.

Множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод с передачей *маркера.*

Метод с передачей маркера – это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения.

При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. Каждая рабочая станция между передающей станцией и принимающей видит это сообщение, но только станция – адресат принимает его. При этом она создает новый маркер.

Маркер (token), или ***полномочие,*** – уникальная комбинация битов, позволяющая начать передачу данных.

Каждый узел принимает пакет от предыдущего, восстанавливает уровни сигналов до номинального (требуемого) уровня и передает дальше. Передаваемый пакет может содержать данные или являться маркером. Когда рабочей станции необходимо передать пакет, ее адаптер дожидается поступления маркера, а затем преобразует его в пакет, содержащий данные, отформатированные по протоколу соответствующего уровня, и передает результат далее по ЛВС. Пакет распространяется по ЛВС от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь в ЛВС. После чего пакет возвращается в узел, из которого был отправлен. Здесь после проверки безошибочной передачи пакета узел освобождает ЛВС, генерируя новый маркер. Таким образом, в ЛВС с передачей маркера не возможны ***коллизии*** (конфликты).

Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

– гарантирует время доставки блоков данных в сети;

– дает возможность предоставления различных *приоритетов передачи данных*.

Вместе с тем он имеет существенные недостатки:

– в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу;

– включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

12. Метод доступа TDMA.

Множественный доступ с разделением во времени (Time Division Multiple Access – TDMA).

-основан на распределении времени работы канала между системами.

Доступ TDMA основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Каждый из циклов начинается *сигналом-разграничителем*. Цикл включает *n* пронумерованных временных интервалов, называемых *ячейками*. Интервалы предоставляются для загрузки в них блоков данных.

Данный способ позволяет организовать передачу данных с *коммутацией пакетов* и с *коммутацией каналов*.

Первый (простейший) вариант использования интервалов заключается в том, что их число (*n*) делается равным количеству абонентских систем, подключенных к рассматриваемому каналу. Тогда во время цикла каждой системе предоставляется один интервал, в течение которого она может передавать данные. При использовании рассмотренного метода доступа часто оказывается, что в одном и том же цикле одним

системам нечего передавать, а другим не хватает выделенного времени. В результате – неэффективное использование пропускной способности канала.

Второй, более сложный, но высокоэкономичный вариант заключается в том, что система получает интервал только тогда, когда у нее возникает необходимость в передаче данных, например при асинхронном способе передачи. Для передачи данных система может в каждом цикле получать интервал с одним и тем же номером. В этом случае передаваемые системой блоки данных появляются через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. Это режим передачи данных с имитацией коммутации каналов. Способ особенно удобен при передаче речи.

13. Метод доступа FDMA.

Множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или *множественный доступ с разделением длины волны*(Wavelength Division Multiple Access – WDMA).

-основан на разделении *полосы пропускания* канала на группу полос частот, образующих*логические каналы*.

Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными.

При использовании FDMA, именуемого также ***множественным доступом с разделением волны*** WDMA, широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать *шум* в соседнем логическом канале.

В *оптических* каналах разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При осуществлении этого мультиплексирования в один световод излучает свет большое число лазеров (на различных частотах). Через световод излучение каждого из них проходит независимо от другого. На приемном конце разделение частот сигналов, прошедших физический канал, осуществляется путем фильтрации выходных сигналов.

Метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах.

14. Назначение пакетов и их структура. Адресация пакетов.

Информация в локальных сетях, как правило, передается отдельными порциями, кусками, называемыми в различных источниках ***пакетами*** (packets), ***кадрами*** (frames) или ***блоками***. Причем предельная длина этих пакетов строго ограничена (обычно величиной в несколько килобайт). Ограничена длина пакета и снизу (как правило, несколькими десятками байт). Выбор пакетной передачи связан с несколькими важными соображениями.

Локальная сеть, как уже отмечалось, должна обеспечивать качественную, прозрачную связь всем абонентам (компьютерам) сети.

Важнейшим параметром является так называемое ***время доступа к сети*** (access time), которое определяется как временной интервал между моментом готовности абонента к передаче (когда ему есть, что передавать) и моментом начала этой передачи. Это время ожидания абонентом начала своей передачи. Естественно, оно не должно быть слишком большим, иначе величина реальной, интегральной скорости передачи информации между приложениями сильно уменьшится даже при высокоскоростной связи.

Ожидание начала передачи связано с тем, что в сети не может происходить несколько передач одновременно (во всяком случае, при топологиях шина и кольцо). Всегда есть только один передатчик и один приемник (реже – несколько приемников). В противном

случае информация от разных передатчиков смешивается и искажается. В связи с этим абоненты передают свою информацию по очереди. И каждому абоненту, прежде чем начать передачу, надо дождаться своей очереди. Вот это время ожидания своей очереди и есть *время доступа*.

Если бы вся требуемая информация передавалась каким-то абонентом сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети этим абонентом на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут (например, при копировании содержимого целого жесткого диска). С тем чтобы уравнять в правах всех абонентов, а также сделать примерно одинаковыми для всех них величину времени доступа к сети и интегральную скорость передачи информации, как раз и применяются пакеты (кадры) ограниченной длины.

Важно также и то, что при передаче больших массивов информации *вероятность ошибки* (передана «1» – принимается «0» или наоборот) из-за помех и сбоев довольно высока. Например, при характерной для локальных сетей величине вероятности одиночной ошибки в 10^{-8} (в среднем одна ошибка приходится на 100 мегабайт переданных двоичных символов) пакет длиной 10 Кбит будет искажен с вероятностью 10^{-4}, а массив длиной 10 Мбит – уже с вероятностью 10^{-1}. К тому же выявить ошибку в массиве из нескольких мегабайт намного сложнее, чем в пакете из нескольких килобайт, а при обнаружении ошибки придется повторить передачу всего большого массива. Но и при повторной передаче большого массива снова высока вероятность ошибки, и процесс этот при слишком большом массиве может повторяться до бесконечности.

С другой стороны, сравнительно большие пакеты имеют преимущества перед очень маленькими пакетами, например, перед побайтовой (8 бит) или пословной (16 бит или 32 бита) передачей информации.

Дело в том, что каждый пакет помимо собственно данных, которые требуется передать, должен содержать некоторое количество *служебной информации*. Прежде всего, это адресная информация, которая определяет, от кого и кому передается данный пакет (как на почтовом конверте – адреса получателя и отправителя). Если порция передаваемых данных будет очень маленькой (например, несколько байт), то доля служебной информации станет непозволительно высокой, что резко снизит интегральную скорость обмена информацией по сети.

Существует некоторая оптимальная длина пакета (или оптимальный диапазон длин пакетов), при которой *средняя скорость обмена информацией* по сети будет максимальна. Эта длина не является неизменной величиной, она зависит от уровня помех, метода управления обменом, количества абонентов сети, характера передаваемой информации, и от многих других факторов. Имеется диапазон длин, который близок к оптимуму.

Таким образом, процесс информационного обмена в сети представляет собой чередование пакетов, каждый из которых содержит информацию, передаваемую от абонента к абоненту.

В частном случае все эти пакеты могут передаваться одним абонентом (когда другие абоненты «не хотят» передавать). Но обычно в сети чередуются пакеты, посланные разными абонентами.

Структура и размеры пакета в каждой сети жестко определены стандартом на данную сеть и связаны, прежде всего, с аппаратными особенностями (аппаратной платформой) данной сети, выбранной топологией и типом среды передачи информации. Кроме того, эти параметры зависят от используемого протокола (порядка обмена информацией).

Но существуют некоторые общие принципы формирования структуры пакета, которые учитывают характерные особенности обмена информацией по любым локальным сетям.

Чаще всего пакет содержит в себе следующие основные *поля* или части.

Стартовая комбинация битов или ***преамбула***, которая обеспечивает предварительную настройку аппаратуры адаптера или другого сетевого устройства на прием и обработку пакета. Это поле может полностью отсутствовать или же сводиться к единственному стартовому биту.

Сетевой адрес (идентификатор) принимающего абонента, то есть индивидуальный или групповой номер, присвоенный каждому принимающему абоненту (компьютеру) в сети. Этот адрес (или *IP-адрес*) позволяет приемнику распознать пакет, адресованный ему лично, группе, в которую он входит, или всем абонентам сети одновременно (при широком вещании).

Сетевой адрес (идентификатор) передающего абонента, то есть индивидуальный номер, присвоенный каждому передающему абоненту. Этот адрес информирует принимающего абонента, откуда пришел данный пакет. Включение в пакет адреса передатчика необходимо в том случае, когда одному приемнику могут попеременно приходить пакеты от разных передатчиков.

Служебная информация, которая может указывать на тип пакета, его номер, размер, формат, маршрут его доставки, на то, что с ним надо делать приемнику и т. д.

Данные (поле данных) – это та информация, ради передачи которой используется пакет. В отличие от всех остальных полей пакета поле данных имеет переменную длину, которая, собственно, и определяет полную длину пакета. Существуют специальные управляющие пакеты, которые не имеют поля данных. Их можно рассматривать как сетевые команды. Пакеты, включающие поле данных, называются информационными пакетами. Управляющие пакеты могут выполнять функцию начала и конца сеанса связи, подтверждения приема информационного пакета, запроса информационного пакета и т. д.

Контрольная сумма пакета – это числовой код, формируемый передатчиком по определенным правилам и содержащий в свернутом виде информацию обо всем пакете. Приемник, повторяя вычисления, сделанные передатчиком, с принятым пакетом, сравнивает их результат с контрольной суммой и делает вывод о правильности или ошибочности передачи пакета. Если пакет ошибочен, то приемник запрашивает его повторную передачу. Обычно используется циклическая контрольная сумма (CRC).

Стоповая комбинация служит для информирования аппаратуры принимающего абонента об окончании пакета, обеспечивает выход аппаратуры приемника из состояния приема. Это поле может отсутствовать, если используется самосинхронизирующийся код, позволяющий определять момент окончания передачи пакета.

Нередко в структуре пакета выделяют всего три поля:

– начальное управляющее поле пакета (или заголовок пакета), то есть поле, включающее в себя стартовую комбинацию, сетевые адреса приемника и передатчика, а также служебную информацию;

– поле данных пакета;

– конечное управляющее поле пакета (заключение, трейлер), куда входят контрольная сумма и стоповая комбинация, а также, возможно, служебная информация.

Структура и вид отдельных полей зависят от применяемой технологии (Ethernet, Token Ring, Arcnet, FDDI и т.д.) и будут рассмотрены в главе 9.

Как уже упоминалось, помимо термина «*пакет*» (packet) в литературе также нередко встречается термин «*кадр*» (frame). Иногда под этими терминами имеется в виду одно и то же. Но иногда подразумевается, что кадр и пакет различаются: кадр вложен в пакет. В этом случае все перечисленные поля пакета, кроме преамбулы и стоповой комбинации, относятся к кадру (рис. 3.4). Например, в описаниях сети Ethernet говорится, что в конце преамбулы передается признак начала кадра.

В других, напротив, поддерживается мнение о том, что пакет вложен в кадр. И тогда под пакетом подразумевается только информация, содержащаяся в кадре, который передается по сети и снабжен служебными полями.

В процессе сеанса обмена информацией по сети между передающим и принимающим абонентами происходит обмен информационными и управляющими пакетами по установленным правилам, называемым протоколом обмена. Это позволяет обеспечить надежную передачу информации при любой интенсивности обмена по сети.

Пример простейшего протокола показан на рис. 3.5.

Сеанс обмена начинается с запроса передатчиком готовности приемника принять данные. Для этого используется управляющий пакет «*Запрос*». Если приемник не готов, он отказывается от сеанса специальным управляющим пакетом. В случае, когда приемник готов, он посылает в ответ управляющий пакет «*Готовность*». Затем начинается собственно передача данных. При этом на каждый полученный информационный пакет приемник отвечает управляющим пакетом «*Подтверждение*».

В случае, когда пакет данных передан с ошибками, в ответ на него приемник запрашивает повторную передачу. Заканчивается сеанс управляющим пакетом «*Конец*», которым передатчик сообщает о разрыве связи.

Существует множество стандартных протоколов, которые используют как передачу с подтверждением (с гарантированной доставкой пакета), так и передачу без подтверждения (без гарантии доставки пакета). Подробнее о протоколах обмена будет рассказано в следующей главе.

При реальном обмене по сети применяются *многоуровневые протоколы*, каждый из уровней которых предполагает свою структуру пакета (адресацию, управляющую информацию, формат данных и т.д.). Ведь протоколы высоких уровней имеют дело с такими понятиями, как *файл-сервер* или приложение, запрашивающее данные у другого приложения, и вполне могут не иметь представления ни о типе аппаратуры сети, ни о методе управления обменом. Все пакеты более высоких уровней последовательно вкладываются в передаваемый пакет, точнее, в поле данных передаваемого пакета (рис. 3.6). Этот процесс последовательной упаковки данных для передачи называется также ***инкапсуляцией пакетов***.

Каждый следующий вкладываемый пакет может содержать собственную служебную информацию, располагающуюся как до данных (заголовок), так и после них (трейлер), причем ее назначение может быть различным.

Безусловно, доля вспомогательной информации в пакетах при этом возрастает с каждым следующим уровнем, что снижает эффективную скорость передачи данных. Для увеличения этой скорости предпочтительнее, чтобы протоколы обмена были проще, и уровней этих протоколов было меньше. Иначе никакая скорость передачи битов не поможет, и быстрая сеть может передавать файл дольше, чем медленная сеть, которая пользуется более простым протоколом.

Обратный процесс последовательной распаковки данных приемником называется ***декапсуляцией пакетов*** " .

15. MAC-адреса и их структура.

Физический или ***локальный адрес узла***, определяемый технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети – это MAC-адрес сетевого адаптера или порта маршрутизатора.

В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов. Понятно, что столько сетевых адаптеров никогда не будет выпущено.

С тем чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса.

Младшие 24 разряда кода адреса называются OUA (Organizationally Unique Address) – *уникальный адрес*. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, то есть каждый изготовитель может выпустить 16 миллионов сетевых адаптеров.

Следующие 22 разряда кода называются OUI (Organizationally Unique Identifier) – *уникальный идентификатор*. IEEE присваивает один или несколько OUI каждому производителю сетевых адаптеров. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI, это означает, что теоретически может быть зарегистрировано 4 миллиона производителей. Вместе OUA и OUI называются UAA (Universally Administered Address) – универсально управляемый адрес или IEEE-адрес.

Два старших разряда адреса управляющие, они определяют тип адреса, способ интерпретации остальных 46 разрядов. Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46 младшими разрядами. Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это случается довольно редко.

Для широковещательной передачи (то есть передачи всем абонентам сети одновременно) применяется специально выделенный *сетевой адрес*, все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

Данной системы адресов придерживаются такие популярные сети, как Ethernet, Fast Ethernet, Token-Ring, FDDI, 100VG-AnyLAN. Ее недостатки – высокая сложность аппаратуры сетевых адаптеров, а также большая доля служебной информации в передаваемом пакете (адреса источника и приемника вместе требуют уже 96 битов пакета или 12 байт).

Во многих сетевых адаптерах предусмотрен так называемый циркулярный режим. В этом режиме адаптер принимает все пакеты, приходящие к нему, независимо от значения поля адреса приемника. Такой режим используется, например, для проведения диагностики сети, измерения ее производительности, контроля ошибок передачи. При этом один компьютер принимает и контролирует все пакеты, проходящие по сети, но сам ничего не передает. В данном режиме работают сетевые адаптеры мостов и коммутаторы, которые должны обрабатывать перед ретрансляцией все пакеты, приходящие к ним.

16. Семиуровневая модель OSI . Назначение. Взаимодействие уровней модели OSI.

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO (International Standardization Organization) разработала ***базовую модель связи открытых систем OSI*** (Open System Interconnection). Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи. Основными элементами модели являются уровни, прикладные процессы и физические средства соединения. На рис. 3.11 представлена структура базовой модели.

Каждый уровень модели OSI выполняет определенную задачу в процессе передачи данных по сети. Базовая модель является основой для разработки сетевых протоколов. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса области взаимодействия открытых систем.

Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. Если приложение может взять на себя функции некоторых верхних уровней модели OSI, то для обмена данными оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

Взаимодействие:

Модель OSI можно разделить на две различных модели:

– ***горизонтальную модель*** на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;

– ***вертикальную модель*** на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

Каждый уровень компьютера-отправителя взаимодействует с таким же уровнем компьютера-получателя, как будто он связан напрямую. Такая связь называется ***логической*** или ***виртуальной связью***. В действительности взаимодействие осуществляется между смежными уровнями одного компьютера.

Итак, информация на компьютере-отправителе должна пройти через все уровни. Затем она передается по физической среде до компьютера-получателя и опять проходит сквозь все слои, пока не доходит до того же уровня, с которого она была послана на компьютере-отправителе.

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной модели соседние уровни обмениваются данными с использованием интерфейсов прикладных программ *API (*Application Programming Interface).

Перед подачей в сеть данные разбиваются на *пакеты*. При отправке данных пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету добавляется управляющая информация данного уровня (заголовок), которая необходима для успешной передачи данных по сети, как это показано на рис. 3.13, где *Заг* – заголовок пакета, *Кон* – конец пакета.

На принимающей стороне пакет проходит через все уровни в обратном порядке. На каждом уровне протокол этого уровня читает информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, и передает пакет следующему уровню. Когда пакет дойдет до ***Прикладного***уровня, вся управляющая информация будет удалена из пакета, и данные примут свой первоначальный вид.

Каждый уровень модели выполняет свою функцию. Чем выше уровень, тем более сложную задачу он решает. Отдельные уровни модели OSI удобно рассматривать как группы программ, предназначенных для выполнения конкретных функций. Один уровень, к примеру, отвечает за обеспечение преобразования данных из ASCII в EBCDIC и содержит программы, необходимые для выполнения этой задачи.

Каждый уровень обеспечивает сервис для вышестоящего уровня, запрашивая в свою очередь, сервис у нижестоящего уровня. Верхние уровни запрашивают сервис почти одинаково: как правило, это требование маршрутизации каких-то данных из одной сети в другую. Практическая реализация принципов адресации данных возложена на нижние уровни.

Рассматриваемая модель определяет *взаимодействие открытых систем* разных производителей в одной сети. Поэтому она выполняет для них координирующие действия по следующим аспектам:

- взаимодействие прикладных процессов;
- формы представления данных;
- единообразное хранение данных;
- управление сетевыми ресурсами;
- безопасность данных и защита информации;
- диагностика программ и технических средств.

17. Уровни модели OSI: прикладной уровень (Application layer)

Прикладной уровень (Application layer) обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам. В действительности прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети

получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например с помощью протокола электронной почты. Специальные элементы прикладного сервиса обеспечивают сервис для конкретных прикладных программ, таких как программы пересылки файлов и эмуляции терминалов. Если, например программе необходимо переслать файлы, то обязательно будет использован ***протокол передачи, доступа и управления файлами*** FTAM (File Transfer, Access, and Management). В модели OSI прикладная программа, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере), посылает конкретные данные в виде ***дейтаграммы*** (datagram) на прикладной уровень. Одна из основных задач этого уровня – определить, как следует обрабатывать запрос прикладной программы. Другими словами, какой вид должен принять данный запрос.

Единица данных, которой оперирует прикладной уровень, обычно называется ***сообщением*** (message).

Прикладной уровень выполняет следующие функции:

– описание форм и методов взаимодействия прикладных процессов;
– выполнение различных видов работ;
– передача файлов;
– управление заданиями;
– управление системой и т.д.
– идентификация пользователей по их паролям, адресам, электронным подписям;
– определение функционирующих абонентов и возможности доступа к новым прикладным процессам;
– определение достаточности имеющихся ресурсов;
– организация запросов на соединение с другими прикладными процессами;
– передача заявок представительскому уровню на необходимые методы описания информации;
– выбор процедур планируемого диалога процессов;
– управление данными, которыми обмениваются прикладные процессы и синхронизация взаимодействия прикладных процессов;
– определение качества обслуживания (время доставки блоков данных, допустимой частоты ошибок);
– соглашение об исправлении ошибок и определении достоверности данных;
– согласование ограничений, накладываемых на синтаксис (наборы символов, структура данных).

Указанные функции определяют виды сервиса, которые прикладной уровень предоставляет прикладным процессам. Кроме этого, прикладной уровень передает прикладным процессам сервис, предоставляемый физическим, канальным, сетевым, транспортным, сеансовым и представительским уровнями.

На прикладном уровне необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское программное обеспечение.

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу наиболее распространенных протоколов верхних трех уровней относятся:

– FTP (File Transfer Protocol) протокол передачи файлов;
– TFTP (Trivial File Transfer Protocol) простейший протокол пересылки файлов;
– X.400 электронная почта;
– Telnet работа с удаленным терминалом;
– SMTP (Simple Mail Transfer Protocol) простой протокол почтового обмена;

– CMIP (Common Management Information Protocol) общий протокол управления информацией;
– SLIP (Serial Line IP) IP для последовательных линий. Протокол последовательной посимвольной передачи данных;
– SNMP (Simple Network Management Protocol) простой протокол сетевого управления;
– FTAM (File Transfer, Access, and Management) протокол передачи, доступа и управления файлами.

18. Уровни модели OSI: уровень представления данных (Presentation layer)

Уровень представления данных или представительский уровень (Presentation layer) представляет данные, передаваемые между прикладными процессами, в нужной форме.

Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет «понятна» прикладному уровню в другой системе или транспортному уровню той же системы. В случаях необходимости уровень представления в момент передачи информации выполняет преобразование форматов данных в некоторый общий формат представления, а в момент приема, соответственно, выполняет обратное преобразование.

Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. Такая ситуация может возникнуть в ЛВС с не однотипными компьютерами (IBM PC и Macintosh), которым необходимо обмениваться данными. Так, в полях баз данных информация должна быть представлена в виде букв и цифр, а зачастую и в виде графического изображения. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой.

В основу общего представления данных положена единая для всех уровней модели система ASN.1. Эта система служит для описания структуры файлов, а также позволяет решить проблему шифрования данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером такого протокола является протокол ***Secure Socket Layer*** (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Представительный уровень выполняет следующие основные функции:
– генерация запросов на установление сеансов взаимодействия прикладных процессов;
– согласование представления данных между прикладными процессами;
– реализация форм представления данных;
– представление графического материала (чертежей, рисунков, схем);
– засекречивание данных;
– передача запросов на прекращение сеансов.

Протоколы уровня представления данных обычно являются составной частью протоколов трех верхних уровней модели.

19. Уровни модели OSI: сеансовый уровень (Session layer).

Сеансовый уровень (Session layer) – это уровень, определяющий процедуру проведения сеансов между пользователями или прикладными процессами.

Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент, а также предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того чтобы начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

Сеансовый уровень управляет передачей информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. Функции этого уровня состоят в координации связи между двумя прикладными программами, работающими на разных рабочих станциях. Это

происходит в виде хорошо структурированного диалога. В число этих функций входит создание сеанса, управление передачей и приемом пакетов сообщений во время сеанса и завершение сеанса.

На сеансовом уровне определяется, какой будет передача между двумя прикладными процессами:

– ***полудуплексной*** (half duplex; процессы или средства будут передавать и принимать данные по очереди);

– ***дуплексной*** (duplex или full duplex; процессы или средства будут передавать и принимать данные одновременно).

В полудуплексном режиме сеансовый уровень выдает маркер данных тому процессу, который начинает передачу. Когда второму процессу приходит время отвечать, маркер данных передается ему. Сеансовый уровень разрешает передачу только той стороне, которая обладает маркером данных.

Сеансовый уровень обеспечивает выполнение следующих функций:

– установление и завершение на сеансовом уровне соединения между взаимодействующими системами;

– выполнение нормального и срочного обмена данными между прикладными процессами;

– управление взаимодействием прикладных процессов;

– синхронизация сеансовых соединений;

– извещение прикладных процессов об исключительных ситуациях;

– установление в прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки;

– прерывание в нужных случаях прикладного процесса и его корректное возобновление;

– прекращение сеанса без потери данных;

– передача особых сообщений о ходе проведения сеанса.

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью протоколов трех верхних уровней модели.

20. Уровни модели OSI: транспортный уровень (Transport Layer)

Транспортный уровень (Transport Layer) предназначен для передачи пакетов через коммуникационную сеть.

На пути от отправителя к получателю пакеты могут быть *искажены* (появятся *ошибки*) или утеряны. Хотя некоторые приложения имеют собственные средства обработки (обнаружения и/или исправления) ошибок, существуют и такие, которые изначально предполагают реализацию надежного соединения.

Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется.

Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное – способностью к обнаружению и исправлению ошибок передачи, таких как *искажение, потеря* и *дублирование* пакетов.

Транспортный уровень определяет логическую адресацию физических устройств (систем, их частей) в сети. Этот уровень гарантирует доставку информации адресатам и управляет этой доставкой. Его главной задачей является обеспечение эффективных, удобных и надежных форм передачи информации между системами. Когда в процессе обработки находится более одного пакета, транспортный уровень контролирует очередность

прохождения пакетов. Если проходит дубликат принятого ранее пакета, то данный уровень опознает это и игнорирует пакет.
В функции транспортного уровня входят:
- управление передачей по сети и обеспечение целостности пакетов данных;
- обнаружение ошибок, частичная их ликвидация и сообщение о неисправленных ошибках;
- восстановление передачи после отказов и неисправностей;
- укрупнение или разделение пакетов данных;
- предоставление приоритетов при передаче пакетов (нормальная или срочная);
- подтверждение передачи;
- ликвидация пакетов при тупиковых ситуациях в сети.

Начиная с транспортного уровня, все вышележащие протоколы реализуются программными средствами, обычно включаемыми в состав сетевой операционной системы.
Наиболее распространенные протоколы транспортного уровня включают в себя:
- TCP (Transmission Control Protocol) протокол управления передачей стека TCP/IP;
- UDP (User Datagram Protocol) пользовательский протокол дейтаграмм стека TCP/IP;
- NCP (NetWare Core Protocol) базовый протокол сетей NetWare;
- SPX (Sequenced Packet eXchange) упорядоченный обмен пакетами стека Novell;
- TP4 (Transmission Protocol) – протокол передачи класса 4.

21. Уровни модели OSI: сетевой уровень (Network Layer).

Сетевой уровень (Network layer) служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор наиболее быстрого и надежного пути.
Сетевой уровень устанавливает связь в вычислительной сети между двумя системами и обеспечивает прокладку *виртуальных каналов* между ними.
Виртуальный или ***логический канал*** – это такое функционирование компонентов сети, которое создает взаимодействующим компонентам иллюзию прокладки между ними нужного тракта. Кроме этого, сетевой уровень сообщает транспортному уровню о появляющихся ошибках.
Протокол канального уровня обеспечивает доставку данных между любыми узлами только в сети с соответствующей *типовой топологией*. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами.
Таким образом, внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень. При организации доставки пакетов на сетевом уровне используется понятие номер сети. В этом случае ***адрес получателя*** состоит из ***номера сети*** и ***номера компьютера*** в этой сети.
Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.
Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Для того чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач (hops) между сетями, каждый раз, выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет.

На рисунке 3.15 показаны четыре сети, связанные маршрутизаторами. Между узлами *A* и *B* данной сети пролегают два маршрута: первый – через маршрутизаторы 1 и 3, а второй – через маршрутизаторы 1, 2 и 3.

Прокладка наилучшего пути для передачи данных называется ***маршрутизацией***, и ее решение является главной задачей сетевого уровня.

Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени.

Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.

Сетевой уровень модели OSI отвечает за деление пользователей на группы и маршрутизацию пакетов на основе преобразования MAC-адресов в *сетевые адреса*. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

В целом, сетевой уровень выполняет функции:

– создание сетевых соединений и идентификация их портов;

– обнаружение и исправление ошибок, возникающих при передаче через коммуникационную сеть;

– управление потоками пакетов;

– организация (упорядочение) последовательностей пакетов;

– маршрутизация и коммутация;

– сегментирование и объединение пакетов.

На сетевом уровне определяется два вида протоколов. Первый вид относится к определению правил передачи пакетов с данными конечных узлов от узла к маршрутизатору и между маршрутизаторами. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений.

Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

Наиболее часто на сетевом уровне используются протоколы:

– IP (Internet Protocol) протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию;

– IPX (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell;

– X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2);

– CLNP (Connection Less Network Protocol) сетевой протокол без организации соединений.

22. Уровни модели OSI: канальный уровень (Data Link)

Единицей информации ***канального уровня*** (Data Link) является *кадр* (*frame*).

Кадр – это логически организованная структура, в которую можно помещать данные (взаимосвязь *кадра* и *пакета* представлена в разделе 3.1). Задача канального уровня передавать кадры от сетевого уровня к физическому уровню.

На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня является проверка доступности среды

передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок.

Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит, в начало и конец каждого кадра, чтобы отметить его, а также вычисляет *контрольную сумму*, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется *ошибка*.

Задача канального уровня – брать пакеты, поступающие с сетевого уровня и готовить их к передаче, укладывая в кадр соответствующего размера. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать ошибки передачи.

На этом же уровне определяются правила использования физического уровня узлами сети. Электрическое представление данных в ЛВС (биты данных, методы кодирования данных и маркеры) распознаются на этом и только на этом уровне. Здесь обнаруживаются и исправляются (путем требований повторной передачи данных) ошибки.

Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов.

Спецификации IEEE 802.X делят канальный уровень на два подуровня:

– LLC (Logical Link Control) – управление логическим каналом осуществляет логический контроль связи. Подуровень LLC обеспечивает обслуживание сетевого уровня и связан с передачей и приемом пользовательских сообщений.

– MAC (Media Assess Control) – контроль доступа к среде. Подуровень MAC регулирует доступ к разделяемой физической среде (передача маркера или обнаружение коллизий или столкновений) и управляет доступом к каналу связи. Подуровень LLC находится выше подуровня MAC.

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу. При больших размерах передаваемых блоков данных канальный уровень делит их на кадры и передает кадры в виде последовательностей. При получении кадров уровень формирует из них переданные блоки данных. Размер блока данных зависит от способа передачи, качества канала, по которому он передается.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

Канальный уровень может выполнять следующие виды функций:

– организация (установление, управление, расторжение) канальных соединений и идентификация их портов;

– организация и передача кадров;

– обнаружение и исправление ошибок;

– управление потоками данных.

Обеспечение прозрачности логических каналов (передачи по ним данных, закодированных любым способом).

Наиболее часто используемые протоколы на канальном уровне включают:

– HDLC (High Level Data Link Control) протокол управления каналом передачи данных высокого уровня, для последовательных соединений;

– IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x;

– Ethernet сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов;

– Token Ring сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера;
– FDDI (Fiber Distributed Date Interface Station) сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;
– X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов;
– Frame relay сеть, организованная из технологий X25 и ISDN.

23. Уровни модели OSI: физический уровень (Physical Layer).

Физический уровень (Physical Layer) предназначен для сопряжения с физическими средствами соединения.

Физические средства соединения – это совокупность физической среды, аппаратных и программных средств, обеспечивающая передачу сигналов между системами.

Физическая среда – это материальная субстанция, через которую осуществляется передача сигналов. Физическая среда является основой, на которой строятся физические средства соединения. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц.

Физический уровень состоит из *подуровня стыковки* со средой и *подуровня преобразования передачи*. Первый из них обеспечивает сопряжение потока данных с используемым физическим каналом связи. Второй осуществляет преобразования, связанные с применяемыми протоколами.

Физический уровень обеспечивает физический интерфейс с каналом передачи данных, а также описывает процедуры передачи сигналов в канал и получения их из канала. На этом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел. Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

– тип кабелей и разъемов;
– разводку контактов в разъемах;
– схему кодирования сигналов для значений 0 и 1.

Физический уровень выполняет следующие функции:

– установление и разъединение физических соединений;
– передача сигналов в последовательном коде и прием;
– прослушивание, в нужных случаях, каналов;
– идентификация каналов;
– оповещение о появлении неисправностей и отказов.

Оповещение о появлении неисправностей и отказов связано с тем, что на физическом уровне происходит обнаружение определенного класса событий, мешающих нормальной работе сети (столкновение кадров, посланных сразу несколькими системами, обрыв канала, отключение питания, потеря механического контакта и т. д.). Виды сервиса, предоставляемого канальному уровню, определяются протоколами физического уровня. Прослушивание канала необходимо в тех случаях, когда к одному каналу подключается группа систем, но одновременно передавать сигналы разрешается только одной из них. Поэтому прослушивание канала позволяет определить, свободен ли он для передачи. В ряде случаев для более четкого определения структуры физический уровень разбивается на несколько подуровней. Например, физический уровень беспроводной сети делится на три подуровня.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым

адаптером. Повторители являются единственным типом оборудования, которое работает только на физическом уровне.

Выполняется преобразование данных, поступающих от более высокого уровня, в сигналы, передаваемые по кабелю. В глобальных сетях на этом уровне могут использоваться модемы и интерфейс ***RS-232C***. В локальных сетях для преобразования данных применяют сетевые адаптеры, обеспечивающие скоростную передачу данных в цифровой форме. Пример протокола физического уровня – это широко известный интерфейс ***RS-232C/CCITT V.2***, который является наиболее широко распространенной стандартной последовательной связью между компьютерами и периферийными устройствами.

Можно считать этот уровень, отвечающим за аппаратное обеспечение. Физический уровень может обеспечивать как *асинхронную* (последовательную) так и*синхронную* (параллельную) передачу, которая применяется для некоторых мэйнфреймов и мини-компьютеров. На физическом уровне должна быть определена схема кодирования для представления двоичных значений с целью их передачи по каналу связи. Во многих локальных сетях используется манчестерское кодирование.

Примером протокола физического уровня может служить спецификация 100Base-T технологии Ethernet, которая определяет в качестве используемого кабеля*неэкранированную витую пару* категории 5 с волновым сопротивлением 100 Ом, разъем RJ-45, максимальную длину физического сегмента 100 метров, манчестерский код для представления данных на кабеле, и другие характеристики среды и электрических сигналов.

К числу наиболее распространенных спецификаций физического уровня относятся:

– EIA-RS-232-C, CCITT V.24/V.28 – механические/электри-ческие характеристики несбалансированного последовательного интерфейса;

– EIA-RS-422/449, CCITT V.10 – механические, электрические и оптические характеристики сбалансированного последовательного интерфейса;

– Ethernet – сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов;

– Token Ring – сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера.

Модель OSI представляет собой хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, сервисами, предоставляемыми на верхних уровнях, и прочими параметрами.

Иерархически организованная совокупность протоколов, решающих задачу взаимодействия узлов сети, называется ***стеком коммуникационных протоколов***. Протоколы соседних уровней, находящихся в одном узле, взаимодействуют друг с другом также в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть ***интерфейсом***. Интерфейс определяет набор услуг, которые нижележащий уровень предоставляет вышележащему уровню.

24. Спецификации стандартов 802.1 – 802.7

Спецификации института инженеров-электриков и инженеров-электронщиков (Institute of Electrical and Electronics Engineers, IEEE) IEEE 802 определяют стандарты для физических компонентов сети. Эти компоненты – *сетевая карта* (Network Interface Card – NIC) и *сетевой носитель* (network media), которые относятся к физическому и канальному уровням модели OSI. Спецификации IEEE802 определяют механизм доступа адаптера к каналу связи и механизм передачи данных. Стандарты IEEE 802 подразделяют канальный уровень на подуровни:

– Logical Link Control (LLC) – *подуровень управления логической связью*;

– Media; Access Control (MAC) – *подуровень управления доступом к устройствам*.

Существует более двадцати спецификаций IEEE 802.

Стандарт IEEE 802.1 (Internetworking – *объединение сетей*) задает механизмы управления сетью на MAC-уровне. В разделе 802.1 приводятся основные понятия и определения, общие характеристики и требования к локальным сетям, а также поведение маршрутизации на канальном уровне, где логические адреса должны быть преобразованы в их физические адреса и наоборот.

Стандарт IEEE 802.2 (Logical Link Control – *управление логической связью*) определяет функционирование подуровня LLC на канальном уровне модели OSI. LLC обеспечивает интерфейс между методами доступа к среде и сетевым уровнем.

Стандарт IEEE 802.3 (Ethernet Carrier Sense Multiple Access with Collision Detection – *CSMA/CD* LANs Ethernet – *множественный доступ к сетям Ethernet с проверкой несущей и обнаружением конфликтов*) описывает физический уровень и подуровень MAC для сетей, использующих шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов. Прототипом этого метода является метод доступа стандарта Ethernet (10BaseT, 10Base2, 10Base5). Метод доступа CSMA/CD. 802.3 также включает технологии Fast Ethernet (100BaseTx, 100BaseFx, 100BaseFx):

– 100Base-TX – двухпарная витая пара; использует метод MLT-3 для передачи сигналов 5-битовых порций кода 4B/5B по витой паре, а также имеется функция автопереговоров (Auto-negotiation) для выбора режима работы порта.

– 100Base-T4 – четырехпарная витая пара; вместо кодирования 4B/5B в этом методе используется кодирование 8B/6T.

– 100BaseFX – многомодовое оптоволокно. Эта спецификация определяет работу протокола Fast Ethernet по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах на основе хорошо проверенной схемы кодирования и передачи оптических сигналов, использующейся уже на протяжении ряда лет в стандарте FDDI. Как и в стандарте FDDI, каждый узел соединяется с сетью двумя оптическими волокнами, идущими от приемника (Rx) и от передатчика (Tx).

Этот метод доступа используется 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 – MA).

Метод доступа *CSMA/CD* определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети.

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

Стандарт IEEE 802.4 (Token Bus LAN – *локальные сети Token Bus*) определяет метод доступа к шине с передачей маркера, прототип – ArcNet.

При подключении устройств в ArcNet применяют топологию «шина» или «звезда». Адаптеры ArcNet поддерживают метод доступа Token Bus (маркерная шина) и обеспечивают производительность 2,5 Мбит/с. Этот метод предусматривает следующие правила:

– все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);

– в любой момент времени только одна станция в сети обладает таким правом;
– кадр, передаваемый одной станцией, одновременно анализируется всеми остальными станциями сети.

В сетях ArcNet используется асинхронный метод передачи данных (в сетях Ethernet и Token Ring применяется синхронный метод), т.е. передача каждого байта в ArcNet выполняется посылкой ISU (Information Symbol Unit – единица передачи информации), состоящей из трех служебных старт/стоповых битов и восьми битов данных.

Стандарт IEEE 802.5 (Token Ring LAN – *локальные сети Token Ring*) описывает метод доступа к кольцу с передачей маркера, прототип – Token Ring.

Сети стандарта Token Ring, так же как и сети Ethernet, используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему используется алгоритм, основанный на передаче станциями права на использование кольца в определенном порядке. Право на использование кольца передается с помощью маркера, или токена.

Стандарт IEEE 802.6 (Metropolitan Area Network – *городские или муниципальные сети*) описывает рекомендации для региональных сетей.

Стандарт IEEE 802.7 (Broadband Technical Advisory Group – *техническая консультационная группа по широковещательной передаче*) описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

25. Спецификации стандартов 802.8 - 802.12.

Стандарт IEEE 802.8 (Fiber Technical Advisory Group – *техническая консультационная группа по оптоволоконным сетям*) содержит обсуждение использования оптических кабелей в сетях 802.3 – 802.6, а также рекомендации по оптоволоконным сетевым технологиям, носителям, интерфейсу и оборудованию, прототип – сеть *FDDI* (Fiber Distributed Data Interface).

Стандарт FDDI использует оптоволоконный кабель и доступ с применением *маркера*. Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Использование двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят им воспользоваться, должны быть подключены к обоим кольцам. Скорость сети – до 100 Мбит/с. Данная технология позволяет включать до 500 узлов на расстоянии 100 км.

Стандарт IEEE 802.9 (Integrated Voice and Data Network – *интегрированные сети передачи голоса и данных*) задает архитектуру и интерфейсы устройств одновременной передачи данных и голоса по одной линии, а также содержит рекомендации по гибридным сетям, в которых объединяют голосовой трафик и трафик данных в одной и той же сетевой среде.

В ***стандарте IEEE 802.10*** (Network Security – *сетевая безопасность*) рассмотрены вопросы обмена данными, *шифрования* (на основе криптографического преобразования информации), управления сетями и безопасности в сетевых архитектурах, совместимых с моделью OSI.

Стандарт IEEE 802.11 (Wireless Network – *беспроводные сети*) описывает рекомендации по использованию беспроводных сетей.

Стандарт IEEE 802.12 описывает *рекомендации по использованию сетей 100VG* – AnyLAN со скоростью 100 Мб/с и методом доступа по очереди запросов и по приоритету (Demand Priority Queuing – DPQ, Demand Priority Access – DPA).

Технология *100VG* – это комбинация Ethernet и Token-Ring со скоростью передачи 100 Мбит/с, работающая на *неэкранированных витых парах*. В проекте 100Base-VG усовершенствован метод доступа с учетом потребности мультимедийных приложений. В спецификации *100VG* предусматривается поддержка волоконно-оптических кабельных систем. Технология 100VG использует метод доступа – *обработка запросов по*

приоритету (*demand priority access*). В этом случае узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу, а затем разрешает этот запрос в соответствии с приоритетом. Имеется два уровня приоритетов – высокий и низкий.

26. Спецификации стандартов 802.14 - 802.22.

Стандарт IEEE 802.14 определяет *функционирование кабельных модемов*.

Стандарт IEEE 802.15 (PAN – Personal Area Network, *персональные сети*) рассматривает вопросы организации персональных сетей. В настоящее время уже существует несколько спецификаций данного стандарта.

Стандарт IEEE 802.15.1 базируется на спецификациях Bluetooth v1.x. и предназначен для построения так называемых персональных беспроводных сетей (Wireless Personal Area Network, WPAN). Для работы радиоинтерфейса *Bluetooth* используется так называемый нижний (2,45 ГГц) диапазон ISM (industrial, scientific, medical), предназначенный для работы промышленных, научных и медицинских приборов.

Стандарт IEEE 802.15.3 предназначен для *беспроводных частных сетей* и является прямым наследником Bluetooth (частота 2,4 ГГц). IEEE 802.15.3 обеспечивает скорость передачи данных до 55 Мбит/с на расстоянии до 100 метров, одновременно работать в такой сети могут до 245 пользователей. Шифрование данных в сетях IEEE 802.15.3 может осуществлятся по стандарту AES 128.

Стандарт IEEE 802.15.4 (ZigBee) ориентирован, главным образом, на использование в качестве средства связи между автономными приборами и оборудованием.

Стандарт IEEE 802.15.4a (Ultra Wideband, UWB) базируется на технологии сверхширокополосной связи (Ultra Wideband, UWB) основана на передаче множества закодированных импульсов не гармонической формы очень малой мощности и малой длительности в широком диапазоне частот.

Стандарт IEEE 802.16 предназначен для реализации широкополосных каналов в городских сетях (MAN). В отличии от 802.11 он ориентирован для соединения стационарных, а не мобильных объектов. Его задачей является обеспечения сетевого уровня между локальными сетями (IEEE 802.11) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE802.20. Эти стандарты совместно со стандартом IEEE 802.15 и 802.17 образуют взаимосогласованную иерархию протоколов беспроводной связи.

Стандарт IEEE 802.17 называется RPR (Resilient Packet Ring –*адаптивное кольцо для пакетов*), и в отличие от FDDI (а также Token Ring или DQDB) пакеты удаляются из кольца узлом-адресатом, что позволяет осуществлять несколько обменов одновременно.

Стандарт IEEE 802.18 представляет собой требования и рекомендации технической консультативной группы по радиочастотному регулированию – RTAG (*Radio Regulatory Technical Advisory Group*).

Стандарт IEEE 802.19 представляет собой требования и рекомендации технической консультативной группы по сосуществованию – CTAG (*Coexistence Technical Advisory Group*).

Стандарт IEEE 802.20 описывает правила беспроводного мобильного широкополосного доступа MBWA (*Mobile Broadband Wireless Access*) для пакетного интерфейса в беспроводных городских сетях WMAN. Этот стандарт должен поддерживать услуги по передаче данных с IP в качестве транспортного протокола и дополнять стандарт IEEE 802.16 в масштабе WiMAX. Стандарт обеспечит скорость передачи данных более 1 Мбит/с и позволит получить мобильный доступ к данным из движущихся транспортных средств (если скорость их не превышает 250 км/ч). Для беспроводного интерфейса HPI (Highspeed Portable Internet) устанавливаются уровни скорости передачи и безопасности. Быстродействие HPI выше, чем универсальной системы мобильной связи UMTS, которая ориентирована на передачу голоса. Стандарт обеспечивает подключение ПК в небольших

и домашних офисах (SOHO), как альтернативу сетей «последней мили» по медным или оптическим кабелям, использующим технологии DSL.

Стандарт IEEE 802.21 – это стандарт независимой от среды эстафетной передаче соединений – MIHS (*Media Independent Handover Services*).

Стандарт IEEE 802.22 – определяет функционирование беспроводных региональных сетей WRAN (*Wireless Regional Area Network*), использующих для передачи данных телевизионные частотные диапазоны.

27. Понятия протоколов и стеков протоколов. Сетевые протоколы. Транспортные протоколы. Прикладные протоколы.

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется ***стеком протоколов***.

Для каждого уровня определяется набор функций-запросов для взаимодействия с вышележащим уровнем, который называется ***интерфейсом***.

Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются ***протоколами***.

Стеки протоколов разбиваются на три уровня:

– сетевые;
– транспортные;
– прикладные.

Сетевые протоколы предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде. Ниже приведены наиболее популярные сетевые протоколы.

– DDP (Datagram Delivery Protocol, протокол доставки дейтаграмм). *Протокол передачи данных Apple*, используемый в Apple Talk.

– IP (Internet Protocol, протокол Internet). *Протокол стека TCP/IP*, обеспечивающий адресную информацию и информацию о маршрутизации.

– IPX (Internetwork Packet eXchange, межсетевой обмен пакетами) в NWLink. *Протокол Novel NetWare*, используемый для маршрутизации и направления пакетов.

– NetBEUI (NetBIOS Extended User Interface, расширенный пользовательский интерфейс базовой сетевой системы ввода вывода). Разработанный совместно IBM и Microsoft, этот протокол обеспечивает транспортные услуги для NetBIOS.

Транспортные протоколы предоставляют следующие услуги надежной транспортировки данных между компьютерами. Ниже приведены наиболее популярные транспортные протоколы.

– ATP (Apple Talk Protocol, транзакционный протокол Apple Talk) и NBP (Name Binding Protocol, *протокол связывания имен*). Сеансовый и транспортный протоколы Apple Talk.

– NetBIOS (Network Basis Input/Output System, *базовая сетевая система ввода вывода*). NetBIOS устанавливает соединение между компьютерами, а NetBEUIпредоставляет услуги передачи данных для этого соединения.

– SPX (Sequenced Packet eXchange, последовательный обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для обеспечения доставки данных.

– TCP (Transmission Control Protocol, протокол управления передачей). Протокол стека TCP/IP отвечает за надежную доставку данных.

Прикладные протоколы отвечают за взаимодействие приложений. Ниже приведены наиболее популярные прикладные протоколы.

– AFP (Apple Talk File Protocol, файловый протокол Apple Talk). *Протокол удаленного управления файлами Macintosh.*

– FTP (File Transfer Protocol, протокол передачи файлов). *Протокол стека TCP/IP*, используемый для обеспечения услуг по передачи файлов.

– NCP (NetWare Core Protocol, *базовый протокол NetWare*). Оболочка и редиректоры клиента Novel NetWare.

– SNMP (Simple Network Management Protocol, *простой протокол управления сетью*). Протокол стека TCP/IP, используемый для управления и наблюдения за сетевыми устройствами.

– HTTP (Hyper Text Transfer Protocol) – протокол *передачи гипертекста* и другие протоколы.

28. Архитектура стека протоколов Microsoft TCP/IP.

Набор многоуровневых протоколов, или как называют ***стек TCP/IP***, предназначен для использования в различных вариантах сетевого окружения.

Стек TCP/IP с точки зрения системной архитектуры соответствует эталонной модели OSI (Open Systems Interconnection, взаимодействие открытых систем) и позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие.

Стандартная реализация TCP/IP (на примере фирмы Microsoft) соответствует четырехуровневой модели вместо семиуровневой модели

Модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней. В модели используются следующие уровни:

– уровень *Приложения* модели TCP/IP
соответствует *Прикладному*, *Представительскому* и *Сеансовому* уровням модели OSI;

– *Транспортный уровень* модели TCP/IP соответствует аналогичному уровню модели OSI;

– *Межсетевой* уровень модели TCP/IP выполняет те же функции, что и *Сетевой уровень* модели OSI;

– уровень С*етевого интерфейса* модели TCP/IP
соответствует *Канальному* и *Физическому* уровням модели OSI.

29. Стек TCP/IP: уровень Приложения, уровень транспорта

Через уровень *Приложения* модели TCP/IP приложения и службы получают доступ к сети. Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов API: сокеты Windows и NetBIOS.

Интерфейс сокетов Windows, или как его называют *WinSock*, является сетевым программным интерфейсом, предназначенным для облегчения взаимодействия между различными TCP/IP – приложениями и семействами протоколов.

Интерфейс NetBIOS используется для связи между процессами (IPC – Interposes Communications) служб и приложений ОС Windows. NetBIOS выполняет три основных функции:

– определение имен NetBIOS;
– служба дейтаграмм NetBIOS;
– служба сеанса NetBIOS.

Транспортный уровень TCP/IP отвечает за установление и поддержание соединения между двумя узлами. Основные функции уровня:

– подтверждение получения информации;
– управление потоком данных;
– упорядочение и ретрансляция пакетов.

В зависимости от типа службы могут быть использованы два протокола:

– TCP (Transmission Control Protocol – *протокол управления передачей*);
– UDP (User Datagram Protocol – *пользовательский протокол дейтаграмм*).

TCP обычно используют в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные своевременно получены адресатом.

Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют протокол UDP, который является протоколом без установления соединения.

Протокол управления передачей, TCP отвечает за надежную передачу данных от одного узла сети к другому. Он создает сеанс с установлением соединения, иначе говоря, виртуальный канал между машинами. Установление соединения происходит в три шага.

1. Клиент, запрашивающий соединение, отправляет серверу пакет, указывающий номер порта, который клиент желает использовать, а также код (определенное число) ISN (Initial Sequence number).
2. Сервер отвечает пакетом, содержащий ISN сервера, а также ISN клиента, увеличенный на 1.
3. Клиент должен подтвердить установление соединения, вернув ISN сервера, увеличенный на 1.

Трехступенчатое открытие соединения устанавливает номер порта, а также ISN клиента и сервера. Каждый, отправляемый TCP-пакет содержит номера TCP-портов отправителя и получателя, номер фрагмента для сообщений, разбитых на меньшие части, а также контрольную сумму, позволяющую убедиться, что при передачи не произошло ошибок.

В отличие от TCP ***пользовательский протокол дейтаграмм, UDP*** не устанавливает соединения. Протокол UDP предназначен для отправки небольших объемов данных без установки соединения и используется приложениями, которые не нуждаются в подтверждении адресатом их получения. UDP также использует номера портов для определения конкретного процесса по указанному IP адресу. Однако UDP порты отличаются от TCP портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликта между службами.

30. Стек TCP/IP: межсетевой уровень, уровень сетевого интерфейса.

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями. На этом уровне работают маршрутизаторы, которые зависят от используемого протокола и используются для отправки пакетов из одной сети (или ее сегмента) в другую (или другой сегмент сети). В стеке TCP/IP на этом уровне используется протокол IP.

Протокол Интернета, IP обеспечивает обмен дейтаграммами между узлами сети и является протоколом, не устанавливающим соединения и использующим дейтаграммы для отправки данных из одной сети в другую. Данный протокол не ожидает получение подтверждения (ASK, Acknowledgment) отправленных пакетов от узла адресата. Подтверждения, а также повторные отправки пакетов осуществляется протоколами и процессами, работающими на верхних уровнях модели.

К его функциям относится фрагментация дейтаграмм и межсетевая адресация. Протокол IP предоставляет управляющую информацию для сборки фрагментированных дейтаграмм. Главной функцией протокола является межсетевая и глобальная адресация. В зависимости от размера сети, по которой будет маршрутизироваться дейтаграмма или пакет, применяется одна из трех схем адресации.

Протокол IP действует на сетевом уровне модели OSI, поэтому *IP-адреса называются сетевыми*. Они предназначены для передачи сообщений в составных сетях, связывающих подсети, построенные на различных локальных или глобальных сетевых технологиях, например Ethernet или ATM. Однако для непосредственной передачи сообщения в рамках одной подсети вместо IP-адреса нужно использовать локальный (аппаратный) адрес технологии канального уровня, чаще всего MAC-адрес. При этом к IP-пакету добавляются заголовок и концевик кадра канального уровня, в заголовке указываются MAC-адреса источника и приемника кадра.

При формировании кадра канального уровня возникает проблема: каким образом по известному IP-адресу определить соответствующий MAC-адрес. Указанная проблема

решается при помощи протокола ARP (Address Resolution Protocol, протокол разрешения адресов).

Протокол управления сообщениями Интернета (ICMP – Internet Control Message Protocol) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол используется для контроля скорости передачи информации между двумя системами. Если маршрутизатор, соединяющий две системы, перегружен трафиком, он может отправить специальное сообщение ICMP – ошибку для уменьшения скорости отправления сообщений.

Узлы локальной сети используют ***протокол управления группами Интернета*** (IGMP – Internet Group Management Protocol), чтобы зарегистрировать себя в группе. Информация о группах содержится на маршрутизаторах локальной сети. Маршрутизаторы используют эту информацию для передачи групповых сообщений.

Групповое сообщение, как и широковещательное, используется для отправки данных сразу нескольким узлам.

NDIS (Network Device Interface Specification) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта.

Уровень сетевого интерфейса:

Этот уровень модели TCP/IP отвечает за распределение IP-дейтаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети, такого как Ethernet, Token Ring или ATM, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

31. Типы адресаций в сетях. Символьная адресация. Протоколы сопоставления адреса ARP и RARP.

Типы адресов: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя)

DNS (Domain Name System) – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet.

Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен – в нем определены DNS-серверы и DNS-клиенты.

DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес. Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет – то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другомуDNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого ***доменным пространством имен***, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены.

Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

- **com** – коммерческие организации (например, microsoft.com);
- **edu** – образовательные (например, mit.edu);
- **gov** – правительственные организации (например, nsf.gov);
- **org** – некоммерческие организации (например, fidonet.org);
- **net** – организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой *домен* на *поддомены* и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от хоста к корню.

Протокол сопоставления адреса, ARP определяет MAC-адреса следующим образом. Осуществляется рассылка всем узлам сети специального кадра, который называется ***ARP-запрос*** (***ARP Request***).

В кадре содержится IP-адрес компьютера, у которого требуется узнать MAC-адрес. Каждый узел сети принимает ARP-запрос и сравнивает IP-адрес из запроса со своим IP-адресом. Если адреса совпадают, узел высылает ***ARP-ответ*** (***ARP Reply***), содержащий требуемый MAC-адрес.

Результаты своей работы протокол ARP сохраняет в специальной таблице, хранящейся в *оперативной памяти*, которая называется ***ARP-кэш***. При необходимости разрешения IP-адреса, протокол ARP сначала ищет IP-адрес в ARP-кэше и только в случае отсутствия нужной записи производит рассылку ARP-запроса.

Записи в ARP-кэше могут быть двух типов: статические и динамические. Статические записи заносятся в кэш администратором при помощи утилиты arp с ключом /s. Динамические записи помещаются в кэш после полученного ARP-ответа и по истечении двух минут удаляются.

Процесс получения по известному IP-адресу MAC-адреса называется ***разрешением IP-адреса***.

Удаление происходит для того, чтобы при перемещении в другую подсеть компьютера с MAC-адресом, занесенным в таблицу, кадры не отправлялись бесполезно в сеть.

Иногда требуется по известному MAC-адресу найти IP-адрес (например, при начале работы компьютеров без жесткого диска, у которых есть MAC-адрес сетевого адаптера и им нужно определить свой IP-адрес). В этом случае используется реверсивный протокол RARP (Reverse ARP).

32. Структура IPv4. Классы IP-адресов.

Использование масок является временным решением проблемы дефицита IP-адресов, так как адресное пространство протокола IP не увеличивается, а количество хостов в Интернете растет с каждым днем. Для принципиального решения проблемы требуется существенное увеличение количества IP-адресов. Для преодоления ограничений IPv4 был разработан ***протокол IP 6-й версии*** – ***IPv6*** (RFC 2373, 2460).

Протокол IP v6 имеет следующие основные особенности:

– длина адреса 128 бит – такая длина обеспечивает примерно 3.4×10^{38} адресов; такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам;

– автоматическая конфигурация – протокол IP v6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP;

- встроенная безопасность – для передачи данных является обязательным использование *протокола защищенной передачи* IPsec (протокол IP v4 также может использовать IPsec, но не обязан этого делать). В настоящее время многие производители сетевого оборудования включают поддержку протокола IP v6 в свои продукты, однако преобладающим остается протокол IPv4. Связано это с тем, что IPv6 обратно несовместим с IPv4 и процесс перехода сопряжен с определенными трудностями.

Существует пять классов IP-адресов: *A, B, C, D* и *E*

За принадлежность к тому или иному классу отвечают первые биты IP-адреса. Целью такого деления являлось создание малого числа больших сетей (***класса A***), умеренного числа средних сетей (***класс B***) и большого числа малых сетей (***класс C***). Если адрес начинается с 0, то сеть относят к *классу A* 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. Сетей класса А немного, зато количество узлов в них может достигать $2^{24} – 2$, то есть 16 777 214 узлов. Если первые два бита адреса равны 10, то сеть относится к *классу B.* 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 $2^{16} – 2$, что составляет 65 534 узлов. Если адрес начинается с последовательности 110, то это сеть *класса C.* 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 $2^8 – 2$, то есть 254 узлами. Адрес, начинающийся с 1110, обозначает особый, ***групповой адрес (***multicast*).* Пакет с таким адресом направляется всем узлам, которым присвоен данный адрес. Адреса *класса E* в настоящее время не используются (зарезервированы для будущих применений).

33. Понятие маски. Правила использование масок. Определение NetworkID и HostID с использованием масок.

Маска подсети (subnet mask) – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны вIP-адресе интерпретироваться как номер сети.
Для стандартных классов сетей маски имеют следующие значения:

– *класс A* – 11111111. 00000000. 00000000. 0000000 (255.0.0.0);

– *класс B* – 11111111.11111111.00000000. 00000000 (255.255.0.0);

– *класс C* – 11111111.11111111.11111111.00000000 (255.255.255.0).

Маска подсети записывается либо в виде, аналогичном записи IP-адреса, например 255.255.255.0, либо совместно с IP-адресом с помощью указания числа единичных разрядов в записи маски, например 192.168.1.1/24, т. е. в маске содержится 24 единицы (255.255.255.0).

При использовании масок можно вообще отказаться от понятия классов.

34. Структурирование сетей с помощью масок.

Часто администраторы сетей испытывают неудобства, из-за того, что количество централизовано выделенных им номеров сетей недостаточно для того, чтобы структурировать сеть надлежащим образом, например, разместить все слабо взаимодействующие компьютеры по разным сетям. В такой ситуации возможны два пути. Первый из них связан с получением от NIC дополнительных номеров сетей. Второй способ, употребляющийся более часто, связан с использованием так называемых *масок,* которые позволяют разделять одну сеть на несколько сетей. Маска - это число, двоичная запись которого содержит единицы в тех разрядах, которые должны интерпретироваться как номер сети.

35. Особые IP-адреса. Понятие частных сетей. Диапазоны частных адресов.

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей.

1. Если первый октет ID сети начинается с 127, такой адрес считается адресом машины-источника пакета. В этом случае пакет не выходит в сеть, а возвращается на компьютер-отправитель. Такие адреса называются ***loopback*** («петля», «замыкание на себя») и используются для проверки функционирования стека TCP/IP.

2. Если все биты IP-адреса равны нулю, адрес обозначает узел-отправитель и используется в некоторых сообщениях ICMP.

3. Если все биты ID сети равны 1, адрес называется ***ограниченным широковещательным*** (limited broadcast), пакеты, направленные по такому адресу рассылаются всем узлам той подсети, в которой находится отправитель пакета.

4. Если все биты ID хоста равны 1, адрес называется ***широковещательным*** (broadcast); пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.

5. Если все биты ID хоста равны 0, адрес считается ***идентификатором подсети*** (subnet ID).

Наличие особых IP-адресов объясняет, почему из диапазона доступных адресов исключаются два адреса – это случаи, когда все биты ID хоста равны 1 или 0. Например, в сети *класса С* не 256, а 254 узлов.

Служба распределения номеров IANA (Internet Assigned Numbers Authority) зарезервировала для частных сетей три блока адресов:

10.0.0.0 – 10.255.255.255 (префикс 10/8)

172.16.0.0 – 172.31.255.255 (префикс 172.16/12)

192.168.0.0 – 192.168.255.255 (префикс 192.168/16)

Будем называть первый блок 24-битовым, второй – 20-битовым, а третий – 16-битовым. Отметим, что первый блок представляет собой ни что иное, как одну сеть класса *A*, второй блок – 16 последовательных сетей класса *B*, а третий блок – 256 последовательных сетей класса *C*.

Любая организация может использовать IP-адреса из этих блоков без согласования с ICANA или Internet-регистраторами. В результате, эти адреса используются во множестве организаций. Таким образом, уникальность адресов сохраняется только в масштабе одной или нескольких организаций, согласованно использующих общий блок адресов. В такой сети каждая рабочая станция может обмениваться информацией с любой другой рабочей станции частной сети.

Если организации требуются уникальные адреса для связи с внешними сетями, такие адреса следует получать обычным путем через регистраторов Internet. Такие адреса никогда не будут входить ни в один из указанных выше блоков частных адресов.

Перед распределением адресов из частного и публичного блоков следует определить, какие из рабочих станций сети должны иметь связь с внешними системами на сетевом уровне. Для таких рабочих станций следует использовать публичные адреса, остальным же – можно присваивать адреса из частных блоков – это не помешает им взаимодействовать со всеми рабочими станция частной сети организации, независимо от того, какие адреса используются (частные или публичные). Однако прямой доступ во внешние сети для рабочих станций с адресами из частного блока невозможен. Для организации их доступа во внешние шлюзы придется использовать прокси-серверы.

Перемещение рабочей станции из частной сети в публичную (и обратное) связано со сменой IP-адреса, соответствующих записей DNS и изменением конфигурационных файлов на других рабочих станций, которые их идентифицируют по IP-адресам. Поскольку частные адреса не имеют глобального значения, маршрутная информация о частных сетях не должна выходить за пределы этих сетей, а пакеты с частными адресами отправителей или получателей не должны передаваться через межсетевые каналы. Предполагается, что маршрутизаторы в публичных сетях (особенно маршрутизаторы провайдеров Internet) будут отбрасывать маршрутную информацию из частных сетей. Если маршрутизатор публичной сети получает такую информацию, ее отбрасывание не должно трактоваться как ошибка протокола маршрутизации.

36. Адресация IPv6. Особенности. Текстовое представление адреса. Типы IPv6 адресов

Использование масок является временным решением проблемы дефицита IP-адресов, так как адресное пространство протокола IP не увеличивается, а количество хостов в Интернете растет с каждым днем. Для принципиального решения проблемы требуется существенное увеличение количества IP-адресов. Для преодоления ограничений IPv4 был разработан ***протокол IP 6-й версии*** – ***IPv6*** (RFC 2373, 2460).

Протокол IP v6 имеет следующие основные особенности:

– длина адреса 128 бит – такая длина обеспечивает примерно 3.4×10^{38} адресов; такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам;

– автоматическая конфигурация – протокол IP v6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP;

– встроенная безопасность – для передачи данных является обязательным использование *протокола защищенной передачи* IPsec (протокол IP v4 также может использовать IPsec, но не обязан этого делать).

В настоящее время многие производители сетевого оборудования включают поддержку протокола IP v6 в свои продукты, однако преобладающим остается протокол IPv4. Связано это с тем, что IPv6 обратно несовместим с IPv4 и процесс перехода сопряжен с определенными трудностями.

37. Кабель типа «витая пара» (twisted pair). Схемы разводки. Кабельные системы Ethernet.

Витой парой (twisted pair) называется кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Кабель типа «витая пара» используется во многих сетевых технологиях, включая Ethernet, ARCNet и IBM Token Ring.

Кабели на витой паре подразделяются на: *неэкранированные* (UTP – Unshielded Twisted Pair) и *экранированные* медные кабели. Последние подразделяются на две разновидности: с экранированием каждой пары и общим экраном (STP – Shielded Twisted Pair) и с одним только общим экраном (FTP – Foiled Twisted Pair). Наличие или отсутствие экрана у кабеля вовсе не означает наличия или отсутствия защиты передаваемых данных, а говорит лишь о различных подходах к подавлению помех. Отсутствие экрана делает неэкранированные кабели более гибкими и устойчивыми к изломам. Кроме того, они не требуют дорогостоящего контура заземления для эксплуатации в нормальном режиме, как экранированные. Неэкранированные кабели идеально подходят для прокладки в помещениях внутри офисов, а экранированные лучше использовать для установки в местах с особыми условиями эксплуатации, например, рядом с очень сильными источниками электромагнитных излучений, которых в офисах обычно нет.

Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю, а экранированные витые пары еще более увеличивают степень помехозащищенности сигналов.

38. Кабели и структурированные кабельные системы. Коаксиальные кабели.

В качестве среды передачи данных используются различные виды кабелей: *коаксиальный*, *кабель на основе экранированной* и *неэкранированной витой пары*, которые относятся к классу электрических, и *оптоволоконный кабель*.

Наиболее популярным видом среды передачи данных на небольшие расстояния (до 100 м) является *неэкранированная витая пара*, которая включена практически во все современные стандарты и технологии локальных сетей и обеспечивает пропускную способность до 100 Мбит/с (на кабелях категории 5) и выше. Также отметим, что *оптоволоконный кабель* применяется как для построения локальных связей, так и для образования магистралей глобальных сетей. Оптоволоконный кабель может обеспечить очень высокую пропускную способность канала (до нескольких десятков Гб/с) и передачу на значительные расстояния (до нескольких десятков километров без промежуточного усиления сигнала).

В качестве среды передачи данных в вычислительных сетях используются также электромагнитные волны различных частот – *КВ* (короткие волны), *УКВ*(ультракороткие волны), *СВЧ* (сверхвысокие частоты). Однако пока в локальных сетях радиосвязь используется только в тех случаях, когда оказывается невозможной прокладка кабеля. Это объясняется недостаточной надежностью и, прежде всего, безопасностью сетевых технологий, построенных на использовании электромагнитного излучения (так называемые *беспроводные сети* – wireless networks). Для построения глобальных каналов этот вид среды передачи данных используется шире – на нем построены спутниковые каналы связи и наземные радиорелейные каналы, работающие в зонах прямой видимости в СВЧ диапазонах.

Очень важно правильно построить фундамент сети – ***кабельную систему***. В последнее время в качестве такой надежной основы все чаще используется структурированная кабельная система.

Структурированная кабельная система (Structured Cabling System – SCS) – это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Преимущества структурированной кабельной системы.

1. ***Универсальность***. Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети.
2. ***Увеличение срока службы***. Срок старения хорошо структурированной кабельной системы может составлять 8–10 лет.

3. ***Уменьшение стоимости добавления новых пользователей и изменения их мест размещения***. Стоимость кабельной системы в основном определяется не стоимостью кабеля, а стоимостью работ по его прокладке.
4. ***Возможность легкого расширения сети***. Структурированная кабельная система является модульной, поэтому ее легко наращивать, позволяя легко и ценой малых затрат переходить на более совершенное оборудование, удовлетворяющее растущим требованиям к системам коммуникаций.
5. ***Обеспечение более эффективного обслуживания***. Структурированная кабельная система облегчает обслуживание и поиск неисправностей.
6. ***Надежность***. Структурированная кабельная система имеет повышенную надежность, поскольку обычно производство всех ее компонентов и техническое сопровождение осуществляется одной фирмой-производителем.

Коаксиальные кабели используются в радио и телевизионной аппаратуре.

Коаксиальные кабели могут передавать данные со скоростью 10 Мбит/с на максимальное расстояние от 185 до 500 метров. Они разделяются на толстые и тонкие в зависимости от толщины.

Кабель Thinnet, известный как кабель RG-58, является наиболее широко используемым физическим носителем данных. Сети при этом не требуют дополнительного оборудования и являются простыми и недорогими. Хотя тонкий коаксиальный кабель (Thin Ethernet) позволяет передачу на меньшее расстояние, чем толстый, но для соединений с тонким кабелем применяются стандартные байонетные разъемы BNC типа СР-50 и ввиду его небольшой стоимости он становится фактически стандартным для офисных ЛВС. Используется в технологии Ethernet 10Base2, описанной ниже.

Толстый коаксиальный кабель (Thick Ethernet) имеет большую степень помехозащищенности, большую механическую прочность, но требует специального приспособления для прокалывания кабеля, чтобы создать ответвления для подключения к ЛВС. Он более дорогой и менее гибкий, чем тонкий. Используется в технологии Ethernet 10Base5, описанной ниже. Сети ARCNet с передачей маркера обычно используют кабель RG-62 A/U.

Рассмотрим основные параметры систем на основе коаксиальных кабелей:

1. Характеристики спецификации 10Base2:
   - тонкий коаксиальный кабель;
   - характеристики кабеля: диаметр 0.2 дюйма, RG-58A/U 50 Ом;
   - приемлемые разъемы – BNC;
   - максимальная длина сегмента – 185 м;
   - минимальное расстояние между узлами – 0.5 м;
   - максимальное число узлов в сегменте – 30.
2. Характеристики спецификации 10Base5:
   - толстый коаксиальный кабель;
   - волновое сопротивление – 50 Ом;
   - максимальная длина сегмента – 500 метров;
   - минимальное расстояние между узлами – 2.5 м;
   - максимальное число узлов в сегменте – 100.

39. Сетевые адаптеры (Network Interface Card). Назначение. Функции сетевых адаптеров. Типы сетевых адаптеров.

Сетевые адаптеры – это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях.

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.

Компьютер, будь то сервер или рабочая станция, подключается к сети с помощью внутренней платы – сетевого адаптера (хотя бывают и внешние сетевые адаптеры, подключаемые к компьютеру через параллельный порт).

Сетевой адаптер вставляется в гнездо *материнской платы*. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов. Сетевые адаптеры преобразуют параллельные коды, используемые внутри компьютера и представленные маломощными сигналами, в последовательный поток мощных сигналов для передачи данных по внешней сети. Сетевые адаптеры должны быть совместимы с кабельной системой сети, внутренней информационной шиной ПК и сетевой операционной системой.

Сетевые адаптеры производят семь основных операций при приеме или передачи сообщения.

1. *Гальваническая развязка* с коаксиальным кабелем или витой парой. Для этой цели используются импульсные трансформаторы. Иногда для развязки используются оптроны.
2. *Прием (передача) данных*. Данные передаются из ОЗУ ПК в адаптер или из адаптера в память ПК через программируемый канал ввода/вывода, канал прямого доступа или разделяемую память.
3. *Буферизация*. Для согласования скоростей пересылки данных в адаптер или из него со скоростью обмена по сети используются буфера. Во время обработки в сетевом адаптере, данные хранятся в буфере. Буфер позволяет адаптеру осуществлять доступ ко всему пакету информации. Использование буферов необходимо для согласования между собой скоростей обработки информации различными компонентами ЛВС.
4. *Формирование пакета*. Сетевой адаптер должен разделить данные на блоки в режиме передачи (или соединить их в режиме приема) данных и оформить в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.
5. *Доступ к каналу связи.* Набор правил, обеспечивающих доступ к среде передачи. Выявление конфликтных ситуаций и контроль состояния сети.
6. *Идентификация своего адреса в принимаемом пакете*. Физический адрес адаптера может определяться установкой переключателей, храниться в специальном регистре или прошиваться в ППЗУ.
7. *Преобразование параллельного кода в последовательный код* при передаче данных, и из последовательного кода в параллельный при приеме. В режиме передачи данные передаются по каналу связи в последовательном коде.
8. *Кодирование и декодирование данных.* На этом этапе должны быть сформированы электрические сигналы, используемые для представления данных. Большинство сетевых адаптеров для этой цели используют *манчестерское кодирование*. Этот метод не требует передачи синхронизирующих сигналов для распознавания единиц и нулей по уровням сигналов, а вместо этого для представления 1 и 0 используется перемена полярности сигнала.
9. *Передача или прием импульсов.* В режиме передачи закодированные электрические импульсы данных передаются в кабель (при приеме импульсы направляются на декодирование).

Сетевые адаптеры вместе с сетевым программным обеспечением способны распознавать и обрабатывать ошибки, которые могут возникнуть из-за электрических помех, коллизий или плохой работы оборудования.

Последние типы сетевых адаптеров поддерживают технологию *Plug and Play*. Если сетевую карту установить в компьютер, то при первой загрузке система определит тип адаптера и запросит для него драйверы.

Некоторые сетевые адаптеры имеют возможность использовать оперативную память ПК в качестве буфера для хранения входящих и исходящих пакетов данных.*Базовый адрес* (Base Memory Address) представляет собой шестнадцатеричное число, которое указывает на адрес в оперативной памяти, где находится этот буфер. Важно выбрать базовый адрес без конфликтов с другими устройствами.

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных – ISA, PCI, PCI-E.

Сетевые адаптеры различаются также по типу принятой в сети технологии – Ethernet, Token Ring, FDDI и т.п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Различные типы сетевых адаптеров отличаются не только методами доступа к среде и протоколами, но еще и следующими параметрами:

- скорость передачи;
- объем буфера для пакета;
- тип шины;
- быстродействие шины;
- совместимость с различными микропроцессорами;
- использование прямого доступа к памяти (DMA);
- адресация портов ввода/вывода и запросов прерывания;
- конструкция разъема.

40. Повторители и концентраторы. Назначение. Особенности использования.

Основная функция ***повторителя*** (repeater), как это следует из его названия, – повторение сигналов, поступающих на его порт. Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети узлами.

Многопортовый повторитель часто называют *концентратором* (concentrator) или *хабом* (hub), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть.

Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть.

Концентратор представляет собой сетевое устройство, действующее на физическом уровне сетевой модели OSI.

Отрезки кабеля, соединяющие два компьютера или какие либо два других сетевых устройства, называются ***физическими сегментами***, поэтому концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической структуризации сети.

Концентратор – устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала.

Так как потоки входных данных в концентраторе больше выходного потока, то главной его задачей является концентрация данных. При этом возможны ситуации, когда число блоков данных, поступающее на входы концентратора, превышает его возможности. Тогда концентратор ликвидирует часть этих блоков.

Ядром концентратора является *процессор*. Для объединения входной информации чаще всего используется *множественный доступ с разделением времени*. Функции, выполняемые концентратором, близки к задачам, возложенным на мультиплексор. Наращиваемые (модульные) концентраторы позволяют выбирать их компоненты, не думая о совместимости с уже используемыми. Современные концентраторы имеют порты для подключения к разнообразным локальным сетям.

Концентратор является активным оборудованием. Он служит центром (шиной) звездообразной конфигурации сети и обеспечивает подключение сетевых устройств. В концентраторе для каждого узла (ПК, принтеры, серверы доступа, телефоны и пр.) должен быть предусмотрен отдельный порт.

Наращиваемые концентраторы представляют собой отдельные модули, которые объединяются при помощи быстродействующей системы связи. Такие концентраторы предоставляют удобный способ поэтапного расширения возможностей и мощности ЛВС.

Концентратор осуществляет электрическую развязку отрезков кабеля до каждого узла, поэтому короткое замыкание на одном из отрезков не выведет из строя всю ЛВС.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – ***логический сегмент***.

Логический сегмент также называют *доменом коллизий*, поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что, какую бы сложную структуру ни образовывали концентраторы, например путем иерархического соединения, все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

Концентраторы поддерживают технологию Plug and Play и не требуют какой-либо установки параметров. Необходимо просто спланировать свою сеть и вставить разъемы в порты концентратора и компьютеров.

41. Мосты. Назначение. Особенности использования.

Мост (bridge) – ретрансляционная система, соединяющая каналы передачи данных. В соответствии с базовой эталонной моделью взаимодействия открытых систем мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы. Мост преобразует физический (1А, 1В) и канальный (2А, 2В) уровни различных типов. Что касается канального процесса, то он объединяет разнотипные каналы передачи данных в один общий.

Мост, а также его быстродействующий аналог – *коммутатор* (switching hub), делят общую среду передачи данных на логические сегменты.

Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

Мосты могут соединять сегменты, использующие разные типы носителей, например 10BaseT, 100BaseT, 1000BaseT (витая пара), 10Base2 (тонкий коаксиальный кабель) и 1000BaseFx (отповолокно). Они могут соединять сети с разными методами доступа к

каналу, например сети Ethernet (метод доступа CSMA/CD) и Token Ring (метод доступа TPMA).

Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает.

По мере развития данного типа оборудования, они стали многопортовыми и получили название *коммутаторов* (switch). Некоторое время оба понятия существовали одновременно, а позднее вместо термина «*мост*» стали применять «*коммутатор*». Далее в этой теме будет использоваться термин «коммутатор» для обозначения этих обеих разновидностей устройств, поскольку все сказанное ниже в равной степени относится и к мостам, и к коммутаторам. Следует отметить, что в последнее время локальные мосты полностью вытеснены коммутаторами.

Нередки случаи, когда необходимо соединить локальные сети, в которых различаются лишь протоколы физического и канального уровней. Протоколы остальных уровней в этих сетях приняты одинаковыми. Такие сети могут быть соединены мостом. Часто мосты наделяются дополнительными функциями. Такие мосты обладают определенным интеллектом (интеллектом в сетях называют действия, выполняемые устройствами) и фильтруют сквозь себя блоки данных, адресованные абонентским системам, расположенным в той же сети. Для этого в памяти каждого моста имеются адреса систем, включенных в каждую из сетей. Блоки, проходящие через интеллектуальный мост, дважды проверяются, на входе и выходе. Это позволяет предотвращать появление ошибок внутри моста.

Мосты не имеют механизмов управления потоками блоков данных. Поэтому может оказаться, что входной поток блоков окажется большим, чем выходной. В этом случае мост не справится с обработкой входного потока, и его буферы могут переполняться. Чтобы этого не произошло, избыточные блоки выбрасываются. Специфические функции выполняет мост в радиосети. Здесь он обеспечивает взаимодействие двух радиоканалов, работающих на разных частотах. Его именуют *ретранслятором*.

Таким образом, мосты оперируют данными на высоком уровне и имеют совершенно определенное назначение. Во-первых, они предназначены для соединения сетевых сегментов, имеющих различные физические среды, например для соединения сегмента с оптоволоконным кабелем и сегмента с коаксиальным кабелем. Мосты также могут быть использованы для связи сегментов, имеющих различные протоколы низкого уровня (физического и канального).

42. Коммутаторы. Назначение. Особенности использования.

Коммутатор (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных (рис. 9.5).

Общая структура коммутатора аналогична стуктуре моста (внешний вид одного из них показан на рис. 9.3), т.е. современные коммутаторы оперируют не только на физическом, но и на канальном уровнях модели OSI.

В коммуникационной сети коммутатор является ретрансляционной системой (система, предназначенная для передачи данных или преобразования протоколов), обладающей свойством прозрачности (т.е. коммутация осуществляется здесь без какой-либо обработки данных). Коммутатор не имеет буферов и не может накапливать данные. Поэтому при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных должны быть одинаковыми. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами. В отличие от других видов ретрансляционных систем, здесь, как правило, не используется программное обеспечение.

Коммутатор может соединять серверы в кластер и служить основой для объединения нескольких рабочих групп. Он направляет пакеты данных между узлами ЛВС. Каждый коммутируемый сегмент получает доступ к каналу передачи данных без конкуренции и

видит только тот трафик, который направляется в его сегмент. Коммутатор должен предоставлять каждому порту возможность соединения с максимальной скоростью без конкуренции со стороны других портов (в отличие от совместно используемого концентратора). Обычно в коммутаторах имеются один или два высокоскоростных порта, а также хорошие инструментальные средства управления. Коммутатором можно заменить маршрутизатор, дополнить им наращиваемый маршрутизатор или использовать коммутатор в качестве основы для соединения нескольких концентраторов. Коммутатор может служить отличным устройством для направления трафика между концентраторами ЛВС рабочей группы и загруженными файл-серверами.

Коммутатор локальной сети (local area network switch) – устройство, обеспечивающее взаимодействие сегментов одной либо группы локальных сетей.

Коммутатор локальной сети, как и обычный коммутатор, обеспечивает взаимодействие подключенных к нему локальных сетей (рис. 9.6).

В дополнение к основной функции он осуществляет преобразование интерфейсов, если соединяются различные типы сегментов локальной сети. Чаще всего это сети Ethernet, кольцевые сети IBM, сети с оптоволоконным распределенным интерфейсом данных.

В перечень функций, выполняемых коммутатором локальной сети, входят:

- обеспечение сквозной коммутации;
- наличие средств маршрутизации;
- поддержка простого протокола управления сетью;
- имитация моста либо маршрутизатора;
- организация виртуальных сетей;
- скоростная ретрансляция блоков данных.

43. Различие между мостом и коммутатором.

Несмотря на сходство мостов и коммутаторов, ключевая разница между ними состоит в том, что *мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами*. Другими словами, мост передает кадры последовательно, а коммутатор параллельно.

44. Маршрутизаторы. Назначение. Особенности использования. Различия между маршрутизаторами и мостами.

Маршрутизатор (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части.

Каждый маршрутизатор реализует протоколы физического (1А, 1В), канального (2А, 2В) и сетевого (3А, 3В) уровней, как показано на рис.9.7. Специальные сетевые процессы соединяют части коммутатора в единое целое. Физический, канальный и сетевой протоколы в разных сетях различны. Поэтому соединение пар коммуникационных сетей осуществляется через маршрутизаторы, которые осуществляют необходимое преобразование указанных протоколов. Сетевые процессы выполняют взаимодействие соединяемых сетей.

Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных.

Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике и их состоянии. Благодаря этому, выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю. Маршрутизаторы обеспечивают также соединение административно независимых коммуникационных сетей.

Архитектура маршрутизатора также используется при создании узла коммутации пакетов.

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных на сети.

Так как маршрутизаторы работают на сетевом уровне, они могут соединять сети, использующие разную сетевую архитектуру, методы доступа к каналам связи и протоколы.

Маршрутизаторы не обладают такой способностью к анализу сообщений как мосты, но зато могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами.

Мосты принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета.

В «поле зрения» маршрутизаторов находятся только пакеты, адресованные к ним предыдущими маршрутизаторами, в то время как мосты должны обрабатывать все пакеты сообщений в сегменте сети, к которому они подключены.

Тип топологии или протокола уровня доступа к сети не имеет значения для маршрутизаторов, так как они работают на уровень выше, чем мосты (сетевой уровень модели OSI). Маршрутизаторы часто используются для связи между сегментами с одинаковыми протоколами высокого уровня. Наиболее распространенным транспортным протоколом, который используют маршрутизаторы, является IPX фирмы Novell или TCP фирмы Microsoft.

Необходимо запомнить, что для работы маршрутизаторов требуется один и тот же протокол во всех сегментах, с которыми он связан. При связывании сетей с различными протоколами лучше использовать мосты. Для управления загруженностью трафика сегмента сети также можно использовать мосты.

45. Шлюзы. Назначение. Особенности использования.

Шлюз (gateway) – ретрансляционная система, обеспечивающая взаимодействие информационных сетей.

Структура шлюза представлена на рис.9.8.

Шлюз является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней. В свою очередь, наборы протоколов могут опираться на различные типы физических средств соединения.

В тех случаях, когда соединяются информационные сети, то в них часть уровней может иметь одни и те же протоколы. Тогда сети соединяются не при помощи шлюза, а на основе более простых ретрансляционных систем, именуемых маршрутизаторами и мостами.

Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру. Например, шлюз приходится использовать для соединения сети с протоколом TCP/IP и большой ЭВМ со стандартом SNA. Эти две архитектуры не имеют ничего общего, и потому требуется полностью переводить весь поток данных, проходящих между двумя системами.

В качестве шлюза обычно используется выделенный компьютер, на котором запущено программное обеспечение шлюза и производятся преобразования, позволяющие взаимодействовать нескольким системам в сети. Другой функцией шлюзов является преобразование протоколов. При получении сообщения IPX/SPXдля клиента TCP/IP шлюз преобразует сообщения в протокол TCP/IP.

46. Беспроводные технологии: радиосвязь, инфракрасная, связь в микроволновом диапазоне.

Методы *беспроводной технологии* (wireless) передачи данных являются удобным, а иногда незаменимым средством связи. Беспроводные технологии различаются по типам сигнала, частоте (большая частота означает большую скорость передачи) и расстоянию передачи.

Большое значение имеют помехи и стоимость. Можно выделить три основных типа беспроводной технологии:

– радиосвязь;
– связь в микроволновом диапазоне;
– инфракрасная связь.

Передача данных в микроволновом диапазоне (microwaves) использует высокие частоты и применяется как на коротких, так и на больших расстояниях. Главное ограничение заключается в том, чтобы передатчик и приемник были в зоне прямой видимости. Используется в местах, где использование физического носителя затруднено. Передача данных в микроволновом диапазоне при использовании спутников может быть очень дорогой.

Инфракрасные технологии (Infrared transmission), функционируют на очень высоких частотах, приближающихся к частотам видимого света. Они могут быть использованы для установления двусторонней или широковещательной передачи на близких расстояниях. При инфракрасной связи обычно используют светодиоды (LED – Light Emitting Diode) для передачи инфракрасных волн приемнику. Инфракрасная передача ограничена малым расстоянием в прямой зоне видимости и может быть использована в офисных зданиях.

Технологии *радиосвязи* пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Она используется для соединения локальных сетей на больших географических расстояниях. Радиопередача в целом имеет высокую стоимость и чувствительна к электронному и атмосферному наложению, а также подвержена перехватам, поэтому требует шифрования для обеспечения уровня безопасности.

В настоящее время наибольшее распространение получила так называемая Wi-Fi связь, базирующаяся на стандарте IEEE802.11.

Wi-Fi сеть (Wireless Local Area Network – WLAN) – это радиосеть, позволяющая передавать информацию между объектами по радиоволнам (без проводов). Разработкой стандартов в этой области занимается Wi-Fi Alliance.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

– WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
– пользователи мобильных устройств, при подключении к локальным беспроводным сетям, могут легко перемещаться в рамках действующих зон сети;
– скорости современных сетей довольно высоки (до 300 Мб/с), что позволяет их использовать для очень широкого спектра задач;
– с помощью дополнительного оборудования беспроводная сеть может быть успешно соединена с кабельными сетями;
– WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Несмотря на все достоинства, WLAN-сети обладают рядом недостатков, главный из которых – возможность легкого перехвата данных и взлома сети.

47. Сети Wi-Fi. Стандарт IEEE802.11a.

Стандарт ***IEEE 802.11a*** был ратифицирован в 1999 г., но реально начал применяться только с 2001 г. Данный стандарт используется, в основном, в США и Японии. В России и в Европе он не получил широкого распространения.

В соответсвиии со стандартом предполагается использование высокочастотного диапазона (от 5,15 до 5,350 ГГц и от 5,725 до 5,825 ГГц). В США данный диапазон называют диапазоном *нелицензионной национальной информационной инфраструктуры* (Unlicensed National Information Infrastructure, UNII).

По многим параметрам протокол 802.11a мало чем отличается от протокола 802.11g. Передача данных данных осуществляется на скоростях 6 , 9, 12 и 18 Мбит/с.

Последовательность обработки входных данных (битов) в стандарте IEEE 802.11a включает операции *избыточного кодирования* (см. раздел 11.1) и *перемежения*(изменения исходной последовательности) данных.

48. Сети Wi-Fi. Стандарт IEEE802.11b.

Стандарт ***IEEE 802.11b*** является своего рода расширением базового протокола 802.11 и, кроме скоростей 1 и 2 Мбит/с, предусматривает скорости 5,5 и 11 Мбит/с.

В стандарте применяется метод *широкополосной модуляции с прямым расширением спектра* – DSSS (Direct Sequence Spread Spectrum). Весь рабочий диапазон делится на 14 каналов, разнесенных на 25 МГц для исключения взаимных помех. Данные передаются по одному из этих каналов без переключения на другие. Возможно одновременное использование всего 3 каналов. Скорость передачи данных может автоматически меняться в зависимости от уровня помех и расстояния между передатчиком и приемником.

Стандарт IEEE 802.11b обеспечивает максимальную теоретическую скорость передачи 11 Мбит/с, что сравнимо с обычной кабельной сетью 10 Base-T Ethernet. Однако, такая скорость возможна лишь при условии, что в данный момент только одно WLAN-устройство осуществляет передачу. При увеличении числа пользователей полоса пропускания делится на всех и скорость работы падает.

49. Сети Wi-Fi. Стандарт IEEE802.11g.

Стандарт ***802.11g*** окончательно был ратифицирован в июне 2003 г. Он является дальнейшей разработкой спецификации IEEE 802.11b и осуществляет передачу данных в том же частотном диапазоне.

При этом высокая скорость передачи достигается за счет одновременной передачи данных по всем каналам, тогда как скорость передачи в отдельном подканале может быть и невысокой.

При частотном разделении каналов необходимо, чтобы отдельный канал был достаточно узким для минимизации искажения сигнала, но в то же время – достаточно широким для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно расположить частотные подканалы как можно ближе друг к другу, но при этом избежать *межканальной интерференции*, чтобы обеспечить их полную независимость. Частотные каналы, удовлетворяющие вышеперечисленным требованиям, называются *ортогональными*.

Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется ***ортогональным частотным разделением с мультиплексированием*** (OFDM). Одним из ключевых преимуществ метода OFDM является сочетание высокой скорости передачи с эффективным противостоянием многолучевому распространению.

В целом, необходимо отметить, что в результате было достигнута скорость передачи данных 54 Мбит/с (11 Мбит/с у 802.11b), что явилось основным преимуществом этого стандарта. Как и IEEE 802.11b, новая спецификация предусматривает использование диапазона 2,4 ГГц.

Особенностью данного стандарта является совместимость с 802.11b. Например, адаптеры 802.11b могут работать в сетях 802.11g (но при этом не быстрее 11 Мбит/с), а адаптеры 802.11g могут снижать скорость передачи данных до 11 Мбит/с для работы в старых сетях 802.11b.

50. Сети Wi-Fi. Стандарт IEEE802.11n.

Стандарт ***IEEE 802.11n*** основан на *технологии OFDM-MIMO* (Multiple Input Multiple Output). Очень многие реализованные в нем технические детали позаимствованы из стандарта 802.11a, однако в стандарте IEEE 802.11n предусматривается использование как частотного диапазона, принятого для стандарта IEEE 802.11a, так и частотного диапазона, принятого для стандартов IEEE 802.11b/g. То есть устройства, поддерживающие стандарт IEEE 802.11n, могут работать в частотном диапазоне либо 5, либо 2,4 ГГц, причем конкретная реализация зависит от страны. Увеличение скорости передачи в стандарте

IEEE 802.11n достигается, во-первых, благодаря удвоению ширины канала с 20 до 40 МГц, а во-вторых, за счет реализации технологии MIMO.
Технология MIMO (Multiple Input Multiple Output) предполагает применение нескольких передающих и принимающих антенн. По аналогии традиционные системы, то есть системы с одной передающей и одной принимающей антенной, называются SISO (Single Input Single Output).
Теоретически MIMO-система с *n* передающими и *n* принимающими антеннами способна обеспечить пиковую пропускную способность в *n* раз большую, чем системы SISO. Это достигается за счет того, что передатчик разбивает поток данных на независимые последовательности бит и пересылает их одновременно, используя массив антенн. Такая техника передачи называется ***пространственным мультиплексированием***. Отметим, что все антенны передают данные независимо друг от друга в одном и том же частотном диапазоне.
В стандарте IEEE 802.11n предусмотрены как стандартные каналы связи шириной 20 МГц, так и каналы с удвоенной шириной. Однако применение 40-мегагерцевых каналов является опциональной возможностью стандарта, поскольку использование таких каналов может противоречить законодательству некоторых стран.
В протоколе IEEE 802.11n максимальная скорость *сверточного кодирования* равна 5/6, то есть каждые пять входных бит в сверточном кодере превращаются в шесть выходных.

51. Оборудование для сетей Wi-Fi.

Сети Wi-Fi отождествляются с аббревиатурей *WLAN* (Wireless Local Area Network). Для организации *сетей Wi-Fi* (Wireless Fidelity, беспроводное соответствие) необходимы Wi-Fi сетевые карты, точки доступа и антенны. Необходимость в использовании точек доступа отпадает, когда мы говорим об очень малых сетях, размещенных в одном помещении. Использование точек доступа позволяет более гибко настроить сеть, объединить клиентов проводных и беспроводных сетей, а также установить связь с удаленными объектами (внешнее исполнение).
Wi-Fi сетевые карты по сути мало чем отличаются от обычных сетевых карт, за исключением некоторых особенностей настройки. Wi-Fi сетевые карты представлены в трех основных вариантах исполнения – внутренние PCI карты, CARDBUS и USB адаптеры. Также существуют адаптеры в COMPACT FLASH форм-факторе.
Адаптеры различаются по платформе, в которой они используются: PCI – настольный компьютер, CARDBUS – ноутбук, Compact Flash – карманный компьютер, USB – универсален. Принцип построения и настройки сетей – един и не зависит от форм-фактора Wi-Fi адаптера. Необходимо отметить, что тип адаптера влияет лишь на излучаемую мощность передатчика и чувствительность приемника, а также возможность использования внешней антенны.

52. Особенности оптических систем связи (физические, технические).

Волоконно-оптические линии связи - это вид связи, при котором информация передается по оптическим диэлектрическим волноводам, известным под названием "оптическое волокно".
Оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, а также самой перспективной средой для передачи больших потоков информации на значительные расстояния. Основания так считать вытекают из ряда особенностей, присущих оптическим волноводам.

Физические особенности:

1. Широкополосность оптических сигналов, обусловленная чрезвычайно высокой частотой несущей (Fo=10**14 Гц). Это означает, что по оптической линии связи можно передавать информацию со скоростью порядка 10**12 бит/с или Терабит/с. Говоря другими словами, по одному волокну можно передать одновременно 10 миллионов телефонных разговоров и миллион видеосигналов. Скорость передачи

данных может быть увеличена за счет передачи информации сразу в двух направлениях, так как световые волны могут распространяться в одном волокне независимо друг от друга. Кроме того, в оптическом волокне могут распространяться световые сигналы двух разных поляризаций, что позволяет удвоить пропускную способность оптического канала связи. На сегодняшний день предел по плотности передаваемой информации по оптическому волокну не достигнут.

2. Очень малое (по сравнению с другими средами) затухание светового сигнала в волокне. Лучшие образцы российского волокна имеют затухание 0.22 дБ/км на длине волны 1.55 мкм, что позволяет строить линии связи длиной до 100 км без регенерации сигналов. Для сравнения, лучшее волокно Sumitomo на длине волны 1.55 мкм имеет затухание 0.154 дБ/км. В оптических лабораториях США разрабатываются еще более "прозрачные", так называемые фторцирконатные волокна с теоретическим пределом порядка 0,02 дБ/км на длине волны 2.5 мкм. Лабораторные исследования показали, что на основе таких волокон могут быть созданы линии связи с регенерационными участками через 4600 км при скорости передачи порядка 1 Гбит/с.

Технические:

1. Волокно изготовлено из кварца, основу которого составляет двуокись кремния, широко распространенного, а потому недорогого материала, в отличие от меди.
2. Оптические волокна имеют диаметр около 100 мкм., то есть очень компактны и легки, что делает их перспективными для использования в авиации, приборостроении, в кабельной технике.
3. Стеклянные волокна - не металл, при строительстве систем связи автоматически достигается гальваническая развязка сегментов. Применяя особо прочный пластик, на кабельных заводах изготавливают самонесущие подвесные кабели, не содержащие металла и тем самым безопасные в электрическом отношении. Такие кабели можно монтировать на мачтах существующих линий электропередач, как отдельно, так и встроенные в фазовый провод, экономя значительные средства на прокладку кабеля через реки и другие преграды.
4. Системы связи на основе оптических волокон устойчивы к электромагнитным помехам, а передаваемая по световодам информация защищена от несанкционированного доступа. Волоконно-оптические линии связи нельзя подслушать неразрушающим способом. Всякие воздействия на волокно могут быть зарегистрированы методом мониторинга (непрерывного контроля) целостности линии. Теоретически существуют способы обойти защиту путем мониторинга, но затраты на реализацию этих способов будут столь велики, что превзойдут стоимость перехваченной информации.

Существует способ скрытой передачи информации по оптическим линиям связи. При скрытой передаче сигнал от источника излучения модулируется не по амплитуде, как в обычных системах, а по фазе. Затем сигнал смешивается с самим собой, задержанным на некоторое время, большее, чем время когерентности источника излучения.

При таком способе передачи информация не может быть перехвачена амплитудным приемником излучения, так как он зарегистрирует лишь сигнал постоянной интенсивности.

Для обнаружения перехватываемого сигнала понадобится перестраиваемый интерферометр Майкельсона специальной конструкции. Причем, видность интерференционной картины может быть ослаблена как 1:2N, где N - количество сигналов, одновременно передаваемых по оптической системе связи. Можно

распределить передаваемую информацию по множеству сигналов или передавать несколько шумовых сигналов, ухудшая этим условия перехвата информации. Потребуется значительный отбор мощности из волокна, чтобы несанкционированно принять оптический сигнал, а это вмешательство легко зарегистрировать системами мониторинга.

5. Важное свойство оптического волокна - долговечность. Время жизни волокна, то есть сохранение им своих свойств в определенных пределах, превышает 25 лет, что позволяет проложить оптико-волоконный кабель один раз и, по мере необходимости, наращивать пропускную способность канала путем замены приемников и передатчиков на более быстродействующие.

53. Оптический кабель: его разновидности и характеристики.

Многомодовый кабель. Для передачи данных по традиционному для компьютерных сетей многомодовому волоконно-оптическому кабелю стандарт определяет применение излучателей, работающих на двух длинах волн: 1300 и 850 нм. Для *многомодового оптоволокна* стандарт 802.3z определил спецификации l000Base-SX и l000Base-LX.

В первом случае используется длина волны 850 нм (S означает Short Wavelength, короткая волна), а во втором – 1300 нм (L – от Long Wavelength, длинная волна).

Для спецификации l000Base-SX предельная длина оптоволоконного сегмента для кабеля 62,5/125 оставляет 220 м, а для кабеля 50/125 - 500 м.

Одномодовый кабель. Для спецификации l000Base-LX в качестве источника излучения всегда применяется полупроводниковый лазер с длиной волны 1300 нм.

Максимальная длина кабеля для *одномодового волокна* равна 5000 м.

Для присоединения оптоволоконного трансивера к многомодовому кабелю необходимо использовать специальный адаптер.

Твинаксиальный кабель. В качестве среды передачи данных используется высококачественный твинаксиальный кабель (Twinax) с волновым сопротивлением 150 Ом (2x75 Ом). Максимальная длина *твинаксиального сегмента* составляет всего 25 метров, поэтому это решение подходит для оборудования, расположенного в одной комнате.

54. Достоинства и недостатки оптических систем связи.

Недостатки волоконной технологии. При создании линии связи требуются высоконадежные активные элементы, преобразующие электрические сигналы в свет и свет в электрические сигналы. Необходимы также оптические коннекторы (соединители) с малыми оптическими потерями и большим ресурсом на подключение-отключение. Точность изготовления таких элементов линии связи должна соответствовать длине волны излучения, то есть погрешности должны быть порядка доли микрона. Поэтому производство таких компонентов оптических линий связи очень дорогостоящее. Другой недостаток заключается в том, что для монтажа оптических волокон требуется прецизионное (высокоточное), а потому дорогое, технологическое оборудование. Как следствие, при аварии (обрыве) оптического кабеля затраты на восстановление выше, чем при работе с медными кабелями.

Преимущества от применения волоконно-оптических линий связи (ВОЛС) настолько значительны, что, несмотря на перечисленные недостатки оптического волокна, эти линии связи все шире используются для передачи информации.

55. Защита информации. Основные понятия. Виды основных сетевых атак.

Теория защиты информации – система основных идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации.

Следует заметить, что наряду с термином «*защита информации*» применительно к компьютерным сетям широко используется, как правило, в близком значении, термин «*компьютерная безопасность*».

Компьютерная безопасность – одна из основных задач, решаемых любой компьютерной сетью. Проблему безопасности можно рассматривать с разных сторон – злонамеренная порча данных, конфиденциальность информации, несанкционированный доступ, хищения и т. п.

Надежность компьютерной сети – характеристика способности ее аппаратного, программного и программно-аппаратного обеспечения выполнить при определенных условиях требуемые функции в течение определенного периода времени. Повышение надежности основано на принципе предотвращения неисправностей путем снижения интенсивности отказов и сбоев за счет применения электронных схем и компонентов с высокой и сверхвысокой степенью интеграции, снижения уровня помех, облегченных режимов работы схем, обеспечение тепловых режимов их работы, а также за счет совершенствования методов сборки аппаратуры.

Главной целью повышения надежности систем является обеспечение целостности хранимых в них данных.

Отказоустойчивость – это такое свойство вычислительной системы, которое обеспечивает ей как логической машине возможность продолжения действий, заданных программой, после возникновения неисправностей. Введение отказоустойчивости требует избыточного аппаратного и программного обеспечения.

Секретность (***конфиденциальность***) информации – свойство информации быть известной только допущенным и прошедшим авторизацию субъектам системы (пользователям, программам, процессам и др.); статус, предоставленный информации и определяющий требуемую степень ее защиты.

Субъект – активный компонент системы, который может инициировать поток информации или изменить состояние системы.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию (например, страницы, файлы, папки, директории, компьютерные программы, устройства и т. д.).

Доступ – специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

Санкционированный доступ (СД) к информации – это доступ к информации, не нарушающий установленные правила разграничения доступа.

Несанкционированный доступ (НСД) к информации характеризуется нарушением установленных правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Пассивное вторжение (***перехват информации***) характеризуется тем, что нарушитель только наблюдает за прохождением информации по каналу связи, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации.

Активное вторжение характеризуется стремлением нарушителя подменить информацию, передаваемую в сообщении. Он может выборочно модифицировать или добавить правильное или ложное сообщение, удалить, задержать или изменить порядок следования сообщений, а также аннулировать или задержать все сообщения, передаваемые по каналу.

Удаленная атака – информационное разрушающее воздействие на распределенную компьютерную сеть, программно осуществленное по каналам связи.

Интруз – физическое лицо или процесс, которые реализуют неразрешенный, или несанкционированный, доступ к информации, т. е. ***атаку*** на систему.

Авторизация – предоставление субъектам доступа к объектам системы. Доступ к объекту означает доступ к содержащейся в нем информации.

Аутентификация – проверка идентификации пользователя, устройства или другого компонента в системе (обычно для принятия решения о разрешении доступа к ресурсам системы). Частным вариантом аутентификации является установление принадлежности сообщения конкретному автору.

Целостность – состояние данных или компьютерной системы, в которой данные и программы используются установленным способом, обеспечивающим устойчивую работу системы и единство данных.

Безопасная (***защищенная***) ***система*** – система со средствами защиты, которые успешно и эффективно противостоят ***угрозам безопасности*** (возможным действиям, которые прямо или косвенно могут нанести ущерб системе).

Типы атак:

Сниффер пакетов (*sniffer* – в данном случае в смысле фильтрация) – прикладная программа, которая использует сетевую карту, работающую в режиме (promiscuous («не делающий различия») mode), в котором все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки.

Сниффер перехватывает все сетевые пакеты, которые передаются через атакуемый домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. Таким образом, человек, конечный пользователь, оказывается самым слабым звеном системы информационной безопасности, и хакеры, зная это, умело применяют методы социальной инженерии.

Социальная инженерия – это использование хакером психологических приемов «работы» с пользователем. В самом худшем случае хакер, перехватив пароль, получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.

Смягчить угрозу сниффинга пакетов можно с помощью следующих средств:

1. *Аутентификация*. Сильные средства аутентификации являются первым способом защиты от сниффинга пакетов. Под «сильным» мы понимаем такой метод аутентификации, который трудно обойти. Примером такой аутентификации являются *однократные пароли* (OTP – One-Time Passwords).

OTP – это технология *двухфакторной аутентификации*. Типичным примером двухфакторной аутентификации является работа обычного банкомата, который опознает клиента, во-первых, по пластиковой карточке и, во-вторых, по вводимому ПИН-коду. Для аутентификации в системе OTP также требуется ПИН-код и личная карточка. Снифферы, перехватывающие другую информацию (например, сообщения электронной почты), не теряют своей эффективности.

2. *Коммутируемая инфраструктура*. Еще одним способом борьбы со сниффингом пакетов в сетевой среде является создание коммутируемой инфраструктуры. Если, к

примеру, во всей организации используется коммутируемый Ethernet, хакеры могут получить доступ только к трафику, поступающему на тот порт, к которому они подключены. Коммутируемая инфраструктура не ликвидирует угрозу сниффинга, но заметно снижает ее остроту.

3. *Анти-снифферы*. Третий способ борьбы со сниффингом заключается в установке аппаратных или программных средств, распознающих снифферы, работающие в вашей сети. Эти средства не могут полностью ликвидировать угрозу, но, как и многие другие средства сетевой безопасности включаются в общую систему защиты. Так называемые «анти-снифферы» измеряют время реагирования хостов и определяют, не приходится ли хостам обрабатывать «лишний» трафик. Подобного рода средства не могут полностью ликвидировать угрозу сниффинга, но крайне необходимы при построении комплексной системы защиты. Одно из таких средств, поставляемых компанией LOpht Heavy Industries, называется AntiSniff.

3. *Криптография*. Самый эффективный способ борьбы со сниффингом пакетов не предотвращает перехвата и не распознает работу снифферов, но делает эту работу бесполезной. Если канал связи является криптографически защищенным, это значит, что хакер перехватывает не сообщение, а зашифрованный текст. Например, криптография Cisco на сетевом уровне базируется на протоколе *IPSec*. IPSec представляет собой стандартный метод защищенной связи между устройствами с помощью протокола IP. К прочим криптографическим протоколам сетевого управления относятся протоколы *SSH* (Secure Shell) и *SSL* (Secure SocketLayer, см. п.11.6).

IP-спуфинг – это вид атаки, при которой хакер, находящийся внутри организации или за ее пределами выдает себя за санкционированного пользователя.

Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример – атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Если же хакеру удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, хакер получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Полностью устранить угрозу спуфинга практически невозможно, но ее можно ослабить с помощью следующих мер.

1. *Контроль доступа*. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфинга, необходимо настроить контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри защищаемой сети. Заметим, что это помогает бороться с IP-спуфингом, когда санкционированными являются только внутренние адреса. Если санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным.

2. *Фильтрация RFC 2827*. Можно пресечь попытки спуфинга чужих сетей пользователями некоторой сети. Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов данной организации. В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе.

3. *Криптография*. Наиболее эффективный метод борьбы с IP-спуфингом тот же, что и в случае со сниффингом пакетов: необходимо сделать атаку абсолютно неэффективной. IP-спуфинг может функционировать только при условии, что аутентификация происходит на базе IP-адресов.

Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

Атаки DoS, без всякого сомнения, являются наиболее известной формой хакерских атак и одной из самых молодых технологий. Против атак такого типа труднее всего создать стопроцентную защиту. Атаки DoS считаются тривиальными, а от хакера для своей организации они требуют минимум знаний и умений: все необходимое программное обеспечение вместе с описаниями самой технологии совершенно свободно доступно в Интернете. Именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность.

О DoS-атаках широко заговорили после того, как в декабре 1999 г. при помощи этой технологии были успешно атакованы web-узлы таких известных корпораций, как Amazon, Yahoo, CNN, eBay и E-Trade.

В случае использования некоторых серверных приложений (таких, например, как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol). Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов. Этот тип атак трудно предотвратить, так как для этого требуется координация действий с провайдером. Когда атака этого типа проводится одновременно через множество устройств, речь идет о распределенной атаке DDoS (DDoS – distributed DoS).

Наиболее известными разновидностями атак DoS являются: TCP SYN Flood, Ping of Death, Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K),Trinco, Stacheldracht, Trinity, Smurf, ICMP flood, UDP flood, TCP flood.

Рассмотрим некоторые из них более подробно.

Smurf – ping-запросы ICMP (Internet Control Message Protocol) по адресу направленной широковещательной рассылки. Используемый в пакетах этого запроса фальшивый адрес источника в результате оказывается мишенью атаки. Системы, получившие направленный широковещательный ping-запрос, отвечают на него и «затапливают» сеть, в которой находится сервер-мишень.

ICMP flood – атака, аналогичная Smurf, только без усиления, создаваемого запросами по направленному широковещательному адресу.

UDP flood – отправка на адрес системы-мишени множества пакетов UDP, что приводит к «связыванию» сетевых ресурсов.

TCP flood – отправка на адрес системы-мишени множества TCP-пакетов, что также приводит к «связыванию» сетевых ресурсов.

TCP SYN flood – при проведении такого рода атаки выдается большое количество запросов на инициализацию TCP-соединений с узлом-мишенью, которому, в результате, приходится расходовать все свои ресурсы на то, чтобы отслеживать эти частично открытые соединения.

Угроза атак типа DoS может снижаться тремя способами:

1) *Функции анти-спуфинга.* Правильная конфигурация функций анти-спуфинга на маршрутизаторах и межсетевых экранах помогает снизить риск DoS атак. Эти функции, как минимум, должны включать фильтрацию RFC 2827.

2) *Функции анти-DoS.* Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.

3) *Ограничение объема трафика* (traffic rate limiting). Организация может попросить провайдера ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем некритического трафика, проходящего по сети. Обычным примером является ограничение объемов трафика ICMP, который используется только для диагностических целей. Атаки DDoS часто используют ICMP.

Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.

Хакеры могут проводить парольные атаки с помощью целого ряда методов, таких как *простой перебор* (brute force attack), *троянский конь*, *IP-спуфинг* и*сниффинг пакетов*. Хотя *логин* и *пароль* часто можно получить при помощи IP-спуфинга и сниффинга пакетов, хакеры часто пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название простого перебора. Часто для такой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу).

Еще одна проблема возникает, когда пользователи применяют один и тот же пароль для доступа ко многим системам: корпоративной, персональной и системам Интернет.

Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Одноразовые пароли и/или криптографическая аутентификация могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные выше методы аутентификации.

С точки зрения администратора, существует несколько методов борьбы с подбором паролей. Один из них заключается в использовании средства *L0phtCrack*, которое часто применяют хакеры для подбора паролей в среде Windows NT. Это средство быстро покажет, легко ли подобрать пароль, выбранный пользователем.

Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.

Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа Man-in-the-Middle можно только с помощью криптографии.

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них состоит в использовании хорошо известных слабостей серверного программного обеспечения (sendmail, HTTP, FTP). Используя эти слабости, хакеры могут получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно это бывает не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через *межсетевой экран*. К примеру, хакер, эксплуатирующий известную слабость Web-сервера, часто использует в ходе атаки TCP порт 80. Поскольку Web-сервер предоставляет пользователям Web-страницы, межсетевой экран должен предоставлять доступ к этому порту. С точки зрения межсетевого экрана, атака рассматривается как стандартный трафик для порта 80.

Полностью исключить атаки на уровне приложений невозможно. Хакеры постоянно открывают и публикуют в Интернете все новые уязвимые места прикладных программ.

Самое главное здесь – хорошее системное администрирование. Вот некоторые меры, которые можно предпринять, чтобы снизить уязвимость для атак этого типа:

– чтение лог-файлов операционных систем и сетевых лог-файлов и/или их анализ с помощью специальных аналитических приложений;

– подписка на услуги по рассылке данных о слабых местах прикладных программ;

– использование последних версий операционных систем и приложений и самых последних коррекционных модулей (патчей);

– кроме системного администрирования, необходимо использование *систем распознавания атак* (IDS); существуют две взаимно дополняющие друг друга технологии IDS: первая – *сетевая система IDS* (NIDS), которая отслеживает все пакеты, проходящие через определенный домен; когда система NIDS видит пакет или серию пакетов, совпадающих с сигнатурой известной или вероятной атаки, она генерирует сигнал тревоги и/или прекращает сессию; вторая – *хост-система IDS*(HIDS), защищающая хост с помощью программных агентов; эта система борется только с атаками против одного хоста;

– в своей работе системы IDS пользуются *сигнатурами атак*, которые представляют собой профили конкретных атак или типов атак. Сигнатуры определяют условия, при которых трафик считается хакерским.

Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений.

При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, *эхо-тестирования* (ping sweep) и *сканирования портов*. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде.

Полностью избавиться от сетевой разведки невозможно.

Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера, в сети которого установлена система, проявляющая чрезмерное любопытство.

Злоупотребление доверием – злонамеренное использование отношений доверия, существующих в сети.

Классическим примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети. Другим примером является система, установленная с внешней стороны *межсетевого экрана*, имеющая отношения доверия с системой, установленной с его внутренней стороны. В случае взлома внешней системы, хакер может использовать отношения доверия для проникновения в систему, защищенную межсетевым экраном.

Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны защищенных экраном систем. Отношения доверия должны ограничиваться определенными протоколами и, по возможности, аутентифицироваться не только по IP-адресам, но и по другим параметрам.

Переадресация портов представляет собой разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован.

Представим себе межсетевой экран с тремя интерфейсами, к каждому из которых подключен определенный хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к хосту, установленному с внутренней стороны межсетевого экрана. Хост общего доступа может подключаться и к внутреннему, и к внешнему хосту. Если хакер захватит хост общего доступа, он сможет установить на нем программное средство, перенаправляющее трафик с внешнего хоста прямо на внутренний хост Примером приложения, которое может предоставить такой доступ, является netcat.

Основным способом борьбы с переадресацией портов является использование надежных моделей доверия.

Несанкционированный доступ не может считаться отдельным типом атаки. Большинство сетевых атак проводятся ради получения несанкционированного доступа. Источник таких атак может находиться как внутри сети, так и снаружи.

Способы борьбы с несанкционированным доступом достаточно просты. Главным здесь является сокращение или полная ликвидация возможностей хакера по получению доступа к системе с помощью несанкционированного протокола. В качестве примера можно рассмотреть недопущение хакерского доступа к порту telnetна сервере, который предоставляет Web-услуги внешним пользователям.

Рабочие станции конечных пользователей очень уязвимы для вирусов (компьютерных) и троянских коней.

Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя и способны к самомодификации (мутации).

В качестве примера можно привести вирус, который прописывается в файле command.com (главном интерпретаторе систем Windows) и стирает другие файлы, а также заражает все другие найденные им версии command.com.

«***Троянский конь***» – это не программная вставка, а настоящая программа, которая выглядит как полезное приложение, а на деле выполняет вредную роль.

Примером типичного «троянского коня» является программа, которая выглядит, как простая игра для рабочей станции пользователя. Однако пока пользователь играет в игру, программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу этого пользователя. Все абоненты получают по почте игру, вызывая ее дальнейшее распространение.

Борьба с вирусами и «троянскими конями» ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и, возможно, на уровне сети.

По мере появления новых вирусов и «троянских коней» организация должна устанавливать новые версии антивирусных средств и приложений.

Почтовая бомбардировка или ***бомбардировка электронной почтой*** (mailbombing, мэйлбомбинг) – один из самых старых и примитивных видов интернет-атак. Суть мэйлбомбинга – в засорении почтового ящика «мусорной» корреспонденцией или даже выведении из строя почтового сервера интернет-провайдера.

Для этого применяются специальные программы – *мэйлбомберы*. Они попросту засыпают указанный в качестве мишени почтовый ящик огромным количеством писем, указывая при этом фальшивые данные отправителя – вплоть до IP-адреса. Все, что нужно агрессору, использующему такую программу, – указать e-mailобъекта атаки, число сообщений, написать текст письма, указать фальшивые данные отправителя, если программа этого не делает сама и нажать кнопку «отправить».

56. Классификация средств защиты информации.выше

57. Понятие шифрования. Классические алгоритмы шифрования данных.ниже

58. Стандартные методы шифрования и криптографические системы.

Шифрование данных представляет собой разновидность программных средств защиты информации и имеет особое значение на практике как единственная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки. Понятие «шифрование» часто употребляется в связи с понятием криптографии.

Криптография – изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

Аутентичность информации состоит в подлинности авторства и целостности.

В проблематике современной криптографии можно выделить следующие три типа основных задач:

– обеспечение конфиденциальности;
– создание условий для анонимности (неотслеживаемости);
– обеспечение аутентификации информации и источника сообщения.

Первый тип задач относится к защите информации от несанкционированного доступа по секретному ключу. Доступ к информации (информационным ресурсам) имеют только обладатели ключа. Второй и третий типы задач обязаны своей постановкой массовому применению электронных способов обработки и передачи информации (банковская сфера, электронная коммерция, каналы межличностной коммуникации и др.).

Криптографическое преобразование состоит из двух этапов: прямого и обратного. Прямое преобразование называют *зашифрованием* (в соответствии со стандартом ISO 7492-2, *шифрованием, encrypt*), обратное – *расшифрованием* (*дешифрованием, decrypt*).

С точки зрения криптографии *шифр* или ***криптографическая система*** – совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых *ключом* и *алгоритмом криптографического преобразования*.

Следует различать понятия *ключ* и *пароль*.

Пароль является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

В *симметричных криптосистемах* для зашифрования и для расшифрования используется один и тот же ключ.

В *ассиметричных криптосистемах* используются два ключа – открытый (публичный) и закрытый (секретный, тайный), которые математически связаны друг с другом.

Электронной цифровой подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа, т. е. к криптоатаке.

Удачную *криптоатаку* называют ***взломом***.

Криптосистемы:

Симметричные

Стандартные методы шифрования информации, передаваемой по сетям для повышения степени устойчивости к несанкционированному использованию, реализуют несколько этапов (шагов) шифрования, на каждом из которых используются различные «классические» методы шифрования.

К числу известных *симметричных криптосистем* можно отнести стандарт шифрования США DES, алгоритм IDEA, отечественный ГОСТ28147-89 и др.

Достаточно надежным считается алгоритм *IDEA* (International Data Encryption Algorithm), разработанный в Швейцарии и считающийся блочным шифром. Алгоритм также оперирует 64-битовыми блоками открытого текста. Несомненным достоинством IDEA является то, что его ключ имеет длину 128 бит. Один и тот же алгоритм используется и для зашифрования, и для расшифрования.

В алгоритме IDEA используются следующие математические операции:

– поразрядное сложение по модулю 2 («исключающее ИЛИ»);

– сложение беззнаковых целых по модулю 216 (модуль 65536);

– умножение целых по модулю (216+1) (модуль 65537), рассматриваемых как беззнаковые целые, за исключением того, что блок из 16 нулей рассматривается как 2^{16}.

Все перечисленные операции выполняются над 16-битовыми субблоками. Комбинирование этих операций обеспечивает комплексное преобразование входа, существенно затрудняя криптоанализ IDEA по сравнению с DES, который базируется исключительно на операции «исключающее ИЛИ».

К достоинствам симметричных методов шифрования относится высокая скорость шифрования и дешифрования, к недостаткам – малая степень защиты в случае, если ключ стал доступен третьему лицу.

Ассиметричные

Криптосистема с открытым ключом определяется тремя алгоритмами: *генерации ключей, зашифрования* и *расшифрования*. Алгоритм генерации ключей открыт, и каждый может дать ему на вход строку надлежащей дины и получить пару ключей.

Рассмотрим ассиметричные криптосистемы на примере *алгоритма RSA*. Названный в честь трех изобретателей Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman), этот алгоритм многие годы противостоит многочисленным попыткам криптоаналитического вскрытия.

Безопасность алгоритма основана на трудоемкости разложения на множители больших чисел. Открытый и закрытый ключи являются функциями двух больших простых чисел разрядностью 100 – 200 десятичных цифр. Предполагается, что *восстановление открытого текста по шифртексту и открытому ключу равносильно разложению числа на два больших простых множителя*.

Ключ состоит из тройки больших целых чисел: e, d, n. Пара чисел (*e* и *n*) является не секретной и образует *публичный* (*открытый*) *ключ*. Число *d* является секретным, и пара (*d* и *n*) образует *тайный ключ*, известный только данному пользователю. Проблема верификации пользователей на основе их открытых ключей является одной из важных.

Основные операции алгоритма.

1. Для генерации двух ключей применяются два больших случайных простых числа: *p* и *q*. Для большей крипростойкости алгоритма эти числа должны иметь равную длину.

2. Рассчитывается произведение $n = p \cdot q$ и вычисляется функция $\varphi(n) = (p - 1) \cdot (q - 1)$, которая называется функцией Эйлера и указывает количество положительных целых чисел в интервале от 1 до *N*, которые взаимно просты с *N*.

3. Случайным образом выбирается число *e* такое, что *e* и $\varphi(n)$ являются взаимно простыми числами.

4. С помощью расширенного алгоритма Евклида вычисляется число *d* такое, что $e \cdot d = 1 \bmod \varphi(n)$, другими словами,

$d = e^{-1} \bmod \varphi(n)$.

Подразумевается, что эти шаги выполняет лицо, которое генерирует для себя (или по просьбе другого лица для этого другого лица) соответствующие ключи.

Отметим, что числа *d* и *n* также являются взаимно простыми. Открытый и закрытый ключи составляют вышеуказанные пары чисел: *e* и *n*, *d* и *n* соответственно.

В билетах модель OSI – каждый уровень отдельно

Архитектуры – отдельно каждая

Стек TCP/IP разбит на 2 вопроса