

Конспект лекций по дисциплине «Инфокоммуникационные системы и сети»

1. Основные понятия информационных сетей

В настоящее время персональные компьютеры в автономном режиме практически не используются, их, как правило, объединяют в вычислительные или компьютерные сети.

Компьютерная сеть – это совокупность компьютеров и телекоммуникационного оборудования, обеспечивающая информационный обмен компьютеров в сети. Основное назначение компьютерных сетей – обеспечение доступа к распределенным ресурсам.

Телекоммуникации (греч. tele - вдаль, далеко и лат. communicatio - общение) - это передача и прием любой информации (звука, изображения, данных, текста) на расстояние по различным электромагнитным системам (кабельным и оптоволоконным каналам, радиоканалам и другим проводным и беспроводным каналам связи).

Телекоммуникационная сеть - это система технических средств, посредством которой осуществляются телекоммуникации.

К телекоммуникационным сетям относятся:

1. Компьютерные сети (для передачи данных)
2. Телефонные сети (передача голосовой информации)
3. Радиосети (передача голосовой информации - широковещательные услуги)
4. Телевизионные сети (передача голоса и изображения - широковещательные услуги)

Локальная сеть — это сеть, системы которой расположены на небольшом расстоянии друг от друга. Она охватывает небольшое пространство, как правило, одно здание и характеризуется высокими скоростями передачи данных. Каналы такой сети имеют высокое качество и принадлежат одной организации.

Применяются две архитектуры локальных сетей:

1) *архитектура «клиент-сервер»* В ней выделяется один или несколько узлов (их название - серверы), выполняющих в сети управляющие или специальные обслуживающие функции, а остальные узлы (клиенты) являются терминальными, в них работают пользователи.

2) *одноранговая архитектура* предполагает взаимодействие равноправных абонентских систем. Все узлы равноправны; поскольку в общем случае под клиентом понимается объект (устройство или программа), запрашивающий некоторые услуги, а под сервером - объект, предоставляющий эти услуги. Поэтому каждый узел в одноранговых сетях может выполнять функции и клиента, и сервера.

В зависимости от используемых физических средств соединения выделяют:

- *кабельные локальные сети,
- *беспроводные локальные сети.

Коммутируемая локальная сеть (КЛС) — это локальная сеть, состоящая из сегментов, которые с помощью коммутирующего комплекса соединяются в единое целое. Деление локальной сети на сегменты позволяет:

- отключать от сети повреждённые сегменты;
- не пропускать блоки данных в другие сегменты, если они адресованы системе того же сегмента;
- создавать коммуникационную локальную сеть.

Территориальная сеть — это сеть, системы которой расположены в различных географических точках. Она охватывает большое пространство (от района до группы стран). В случае, если она охватывает континенты, то используется название глобальной сети. Характерной особенностью является применение протяжённых широкополосных каналов, большого числа узлов коммутации или спутников связи. Она должна удовлетворять следующим основным требованиям:

- *включать большое число абонентских систем (до нескольких тысяч);
- *покрывать большой географический район;

*обеспечивать ширококешание и доставку сообщений группам и отдельным адресатам;

*иметь высокую пропускную способность (до десятков Гбит/с);

*обладать большой надёжностью в работе;

*гарантировать безопасность данных;

*передать разнообразные виды данных: тексты, звук, изображения.

Глобальная сеть — это сеть, абонентские системы которой расположены в разных странах. Стремление к предоставлению сетевых служб и ресурсов большому числу пользователей привело к объединению территориальных сетей и созданию глобальных сетей. Она является связующим звеном большого числа небольших сетей. Глобальную сеть, состоящую из группы взаимодействующих территориальных сетей, называют также метасетью. Пример: сеть Internet.

Виртуальная сеть — это сеть, характеристики которой в основном определяются её программным обеспечением.

Причины создания виртуальных сетей: ●необходимость создания оперативных изолированных от других пользователей рабочих групп. Рабочая группа — это совокупность пользователей, имеющих общие ресурсы и права использования этих ресурсов. Рабочая группа создаётся в сети для выполнения комплекса задач, определяемых функциональными обязанностями пользователей (разработка проекта, проведение электронного маркетинга и т.д.); ●желание облегчить процедуры перемещения, удаления объектов сети;

2. Топологические модели построения сетей

Все компьютеры в локальной сети соединены линиями связи. Геометрическое расположение линий связи относительно узлов сети и физическое подключение узлов к сети называется физической топологией. В зависимости от топологии различают сети: шинной, кольцевой, звездной, иерархической и произвольной структуры.

Различают физическую и логическую топологию. Логическая и физическая топологии сети независимы друг от друга. Физическая топология - это геометрия построения сети, а логическая топология определяет направления потоков данных между узлами сети и способы передачи данных.

В настоящее время в локальных сетях используются следующие физические топологии:

физическая "шина" (bus);

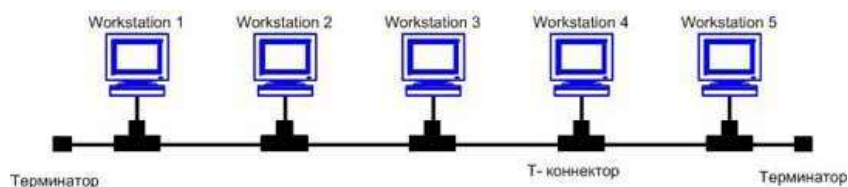
физическая "звезда" (star);

физическое "кольцо" (ring);

физическая "звезда" и логическое "кольцо" (Token Ring).

Шинная топология

Сети с шинной топологией используют линейный моноканал (коаксиальный кабель) передачи данных, на концах которого устанавливаются оконечные сопротивления (терминаторы). Каждый компьютер подключается к коаксиальному кабелю с помощью T-разъема (T - коннектор). Данные от передающего узла сети передаются по шине в обе стороны, отражаясь от оконечных терминаторов. Терминаторы предотвращают отражение сигналов, т.е. используются для гашения сигналов, которые достигают концов канала передачи данных. Таким образом, информация поступает на все узлы, но принимается только тем узлом, которому она предназначена. В топологии логическая шина среда передачи данных используются совместно и одновременно всеми ПК сети, а сигналы от ПК распространяются одновременно во все направления по среде передачи. Так как передача сигналов в топологии физическая шина является широкоэмитальной, т.е. сигналы распространяются одновременно во все направления, то логическая топология данной локальной сети является логической шиной.



Данная топология применяется в локальных сетях с архитектурой Ethernet (классы 10Base-5 и 10Base-2 для толстого и тонкого коаксиального кабеля соответственно).

Преимущества сетей шинной топологии:

- отказ одного из узлов не влияет на работу сети в целом;

- сеть легко настраивать и конфигурировать;

- сеть устойчива к неисправностям отдельных узлов.

Недостатки сетей шинной топологии:

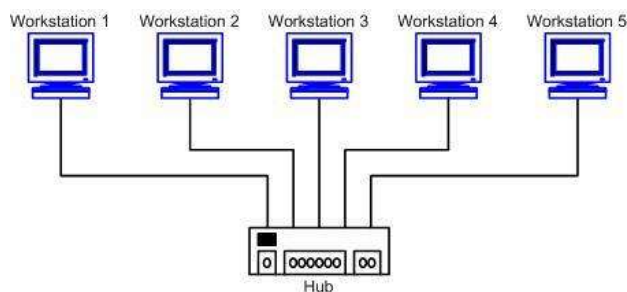
- разрыв кабеля может повлиять на работу всей сети;

- ограниченная длина кабеля и количество рабочих станций;

- трудно определить дефекты соединений

Топология типа “звезда”

В сети построенной по топологии типа “звезда” каждая рабочая станция подсоединяется кабелем (витой парой) к концентратору или хабу (**hub**). Концентратор обеспечивает параллельное соединение ПК и, таким образом, все компьютеры, подключенные к сети, могут общаться друг с другом.



Данные от передающей станции сети передаются через хаб по всем линиям связи всем ПК. Информация поступает на все рабочие станции, но принимается только теми станциями, которым она предназначена. Так как передача сигналов в топологии физическая звезда является

широковещательной, т.е. сигналы от ПК распространяются одновременно во все направления, то логическая топология данной локальной сети является логической шиной.

Данная топология применяется в локальных сетях с архитектурой 10Base-T Ethernet.

Преимущества сетей топологии звезда:

легко подключить новый ПК;

имеется возможность централизованного управления;

сеть устойчива к неисправностям отдельных ПК и к разрывам соединения отдельных ПК.

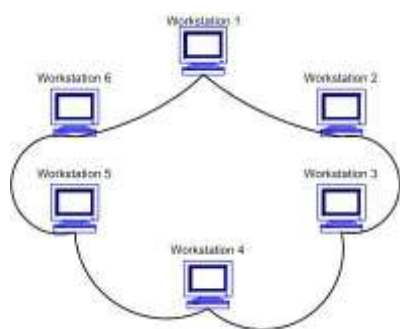
Недостатки сетей топологии звезда:

отказ хаба влияет на работу всей сети;

большой расход кабеля;

Топология “кольцо”

В сети с топологией кольцо все узлы соединены каналами связи в неразрывное кольцо (необязательно окружность), по которому передаются данные. Выход одного ПК соединяется со входом другого ПК. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Данные в кольце всегда движутся в одном и том же направлении.



Принимающая рабочая станция распознает и получает только адресованное ей сообщение. В сети с топологией типа физическое кольцо используется маркерный доступ, который предоставляет станции право на использование кольца в определенном порядке. Логическая топология данной сети - логическое кольцо.

Данную сеть очень легко создавать и настраивать. К основному недостатку сетей топологии кольцо является то, что повреждение линии связи в одном месте или отказ ПК приводит к неработоспособности всей сети.

Как правило, в чистом виде топология “кольцо” не применяется из-за своей ненадёжности, поэтому на практике применяются различные модификации кольцевой топологии.

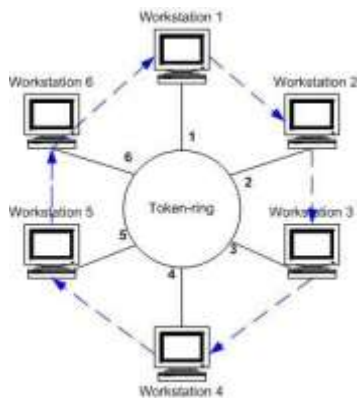
Топология Token Ring

Эта топология основана на топологии "физическое кольцо с подключением типа звезда". В данной топологии все рабочие станции подключаются к центральному концентратору (Token Ring) как в топологии физическая звезда. Центральный концентратор - это интеллектуальное устройство, которое с помощью перемычек обеспечивает последовательное соединение выхода одной станции со входом другой станции.

Другими словами с помощью концентратора каждая станция соединяется только с двумя другими станциями (предыдущей и последующей станциями). Таким образом, рабочие станции связаны петлей кабеля, по которой пакеты данных передаются от одной станции к другой и каждая станция ретранслирует эти посланные пакеты. В каждой рабочей станции имеется для этого приемо-передающее устройство, которое позволяет управлять прохождением данных в сети. Физически такая сеть построена по типу топологии “звезда”.

Концентратор создаёт первичное (основное) и резервное кольца. Если в основном кольце произойдёт обрыв, то его можно обойти, воспользовавшись резервным кольцом, так как используется четырёхжильный кабель. Отказ станции или обрыв линии связи рабочей станции не влечет за собой отказ сети как в топологии кольцо, потому что концентратор отключает

неисправную станцию и замкнет кольцо передачи данных.



В архитектуре Token Ring маркер передаётся от узла к узлу по логическому кольцу, созданному центральным концентратором. Такая маркерная передача осуществляется в фиксированном направлении (направление движения маркера и пакетов данных представлено на рисунке стрелками синего цвета). Станция, обладающая маркером, может отправить данные другой станции.

Для передачи данных рабочие станции должны сначала дождаться прихода свободного маркера. В маркере содержится адрес станции, пославшей этот маркер, а также адрес той станции, которой он предназначен. После этого отправитель передает маркер следующей в сети станции для того, чтобы и та могла отправить свои данные.

Один из узлов сети (обычно для этого используется файл-сервер) создаёт маркер, который отправляется в кольцо сети. Такой узел выступает в качестве активного монитора, который следит за тем, чтобы маркер не был утерян или разрушен.

Преимущества сетей топологии Token Ring:

топология обеспечивает равный доступ ко всем рабочим станциям;

высокая надежность, так как сеть устойчива к неисправностям отдельных станций и к разрывам соединения отдельных станций.

Недостатки сетей топологии Token Ring: большой расход кабеля и соответственно дорогостоящая разводка линий связи.

3. Эталонная модель OSI

Модель OSI была предложена Международной организацией стандартов ISO (International Standards Organization) в 1984 году. С тех пор ее используют (более или менее строго) все производители сетевых продуктов. Как и любая универсальная модель, OSI довольно громоздка, избыточна, и не слишком гибка. Поэтому реальные сетевые средства, предлагаемые различными фирмами, не обязательно придерживаются принятого разделения функций. Однако знакомство с моделью OSI позволяет лучше понять, что же происходит в сети.

Все сетевые функции в модели разделены на 7 уровней (рис. 5.1). При этом вышестоящие уровни выполняют более сложные, глобальные задачи, для чего используют в своих целях нижестоящие уровни, а также управляют ими. Цель нижестоящего уровня – предоставление услуг вышестоящему уровню, причем вышестоящему уровню не важны детали выполнения этих услуг. Нижестоящие уровни выполняют более простые и конкретные функции. В идеале каждый уровень взаимодействует только с теми, которые находятся рядом с ним (выше и ниже него). Верхний уровень соответствует прикладной задаче, работающему в данный момент приложению, нижний – непосредственной передаче сигналов по каналу связи.

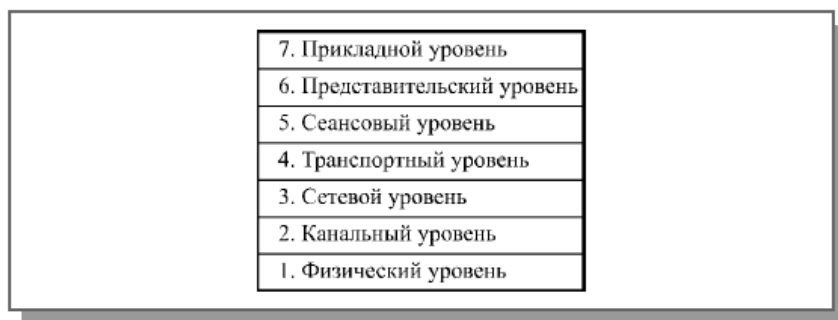


Рис. 5.1 Семь уровней модели OSI

Модель OSI относится не только к локальным сетям, но и к любым сетям связи между компьютерами или другими абонентами. В частности, функции сети Интернет также можно поделить на уровни в соответствии с

моделью OSI. Принципиальные отличия локальных сетей от глобальных, с точки зрения модели OSI, наблюдаются только на нижних уровнях модели.

4. Беспроводные технологии компьютерных сетей.

Беспроводной связью - это передача информации на расстояние без использования электрических проводников или «проводов». Это расстояние может быть как малой (несколько метров, как в телевизионном дистанционном управлении), так и очень большим (тысячи или даже миллионы километров для телекоммуникаций). Беспроводная связь обычно рассматривается как отрасль телекоммуникаций.

Беспроводная технология в общем используется для оборудования мобильных информационных технологий. В их состав входят мобильные телефоны, наладонники (PDA) и беспроводные сети. Другие примеры *беспроводных технологий* включают устройства глобального позиционирования, устройства дистанционного открывания гаража, беспроводные компьютерные мыши и клавиатуры, спутниковое телевидение и мобильные и радиотелефоны.

Развитие беспроводных технологий

В последние годы направление беспроводных компьютерных сетей и удаленного доступа потерпел бурного развития. Это связано с распространением блокнотных компьютеров, систем поискового вызова (так называемых пейджеров) и появлением систем класса «персональный секретарь» (Personal Digital Assistant (PDA)), расширением функциональных возможностей сотовых телефонов. Такие системы должны обеспечить деловое планирование, расчет времени, хранение документов и поддержание связи с удаленными станциями. Девизом этих систем стало anytime, anywhere, т.е. предоставление услуг связи вне зависимости от места и времени. Кроме того, беспроводные каналы связи актуальны там, где невозможно или дорого прокладку кабельных линий и значительные расстояния. До недавнего времени большинство беспроводных

компьютерных сетей передавала данные со скоростью от 1.2 до 14.0 Кбит / с, зачастую только короткие сообщения (передача файлов больших размеров или длинные сеансы интерактивной работы с базой данных были недоступны). Новые технологии беспроводного передачи оперируют со скоростями в несколько десятков мегабит в секунду.

5. Аппаратные средства построения сетей

Локальные вычислительные сети подразделяются на два кардинально различающихся класса:

- Одноранговые (одноуровневые или Peer to Peer).
- Иерархические (многоуровневые) сети.

Архитектура сети описывает:

- Физическое расположение сетевых устройств.
- Тип используемых адаптеров и кабелей.
- Методы передачи данных по кабелю.

Одноранговая сеть

- Все компьютеры равноправны:
- Нет иерархии среди компьютеров.
- Нет выделенного сервера.
- Как правило, каждый компьютер функционирует и как клиент и

как сервер.

Одноранговую сеть называют так же рабочей группой.

Рабочая группа – это небольшой коллектив, поэтому в одноранговой сети не более 10 компьютеров.

- Все пользователи самостоятельно решают, какие данные на своем компьютере сделать доступными для всех.

- Преимущества:
- Одноранговые сети относительно просты.
- Одноранговые сети дешевле сетей на основе сервера, но требуют

более мощных и дорогих компьютеров.

- Поддержка одноранговых сетей встроена в такие ОС как Windows'95, Windows NT Workstation, OS/2, дополнительного программного обеспечения не требуется.

Иерархическая сеть.

Сервер - специальный компьютер, на котором хранится информация, совместно используемая различными пользователями.

Выделенным называется такой сервер, который функционирует только как сервер.

Сервер оптимизирован для быстрой обработки запросов от сетевых клиентов и для управления защитой файлов и каталогов.

Из-за большого круга выполняемых задач, серверы в больших сетях специализированы.

Преимущества:

- Основным аргументом в пользу сети на основе выделенного сервера является защита данных.
- Благодаря тому, что важная информация сосредоточена на одном или нескольких серверах, нетрудно обеспечить ее регулярное резервное копирование
- Сети на основе сервера могут поддерживать тысячи пользователей.
- Для работы в сети компьютеры пользователей могут быть любых конфигураций, даже самых минимальных.

6. Сетевые протоколы

Протоколы – это набор правил и процедур, регулирующих порядок осуществления некоторой связи. Протоколы реализуются во всех областях деятельности человека, например, дипломатических. В сетевой среде – это правила и технические процедуры, позволяющие нескольким компьютерам общаться друг с другом.

Различают три определяющих свойства протоколов:

1. Каждый протокол предназначен для различных задач и имеет свои преимущества и недостатки.
2. Протоколы работают на разных уровнях модели OSI. Функции протокола определяются уровнем, на котором он работает.
3. Несколько протоколов могут работать совместно. В этом случае они образуют так называемый стек, или набор протоколов. Как сетевые функции

распределяются по всем уровням модели OSI, так и протоколы совместно работают на различных уровнях стека. Например, прикладной уровень протокола TCP/IP соответствует уровню представления модели OSI. В совокупности протоколы определяют полный набор функций и возможностей стека.

Передача данных по сети должна быть разбита на ряд последовательных шагов, каждому из которых соответствует свой протокол. Эти шаги должны выполняться на каждом сетевом компьютере в одной и той же последовательности. На компьютере-отправителе они выполняются сверху вниз, а на компьютере-получателе – снизу вверх.

Компьютер-отправитель в соответствии с протоколом выполняет следующие действия:

- а) разбивает данные на небольшие блоки – пакеты, с которыми может работать протокол;
- б) добавляет к пакетам адресную информацию, чтобы компьютер-получатель мог определить, что эти данные предназначены именно ему;
- в) подготавливает данные к передаче через плату СА по сетевому кабелю.

Компьютер-получатель в соответствии с протоколом выполняет те же действия, но в обратном порядке:

- а) принимает пакеты данных из сетевого кабеля и через плату СА передает пакеты в компьютер;
- б) удаляет из пакета всю служебную информацию, добавленную компьютером-отправителем;
- в) копирует данные из пакета в буфер для их объединения в исходный блок данных;
- г) передает приложению собранный из пакетов блок данных в том формате, который использует это приложение.

И компьютеру-отправителю, и компьютеру-получателю необходимо выполнять каждое действие одинаковым способом, чтобы отправленные данные совпали с полученными.

До середины 80-х гг. большинство ЛВС были изолированными. С развитием ЛВС и увеличением объема передаваемой ими информации они стали компонентами больших сетей. Данные, передаваемые из одной локальной сети в другую по одному из возможных маршрутов, называются *маршрутизированными*, а протоколы, поддерживающие передачу данных между сетями по нескольким маршрутам, – *маршрутизируемыми*. Такие протоколы служат для объединения локальных сетей, поэтому их роль постоянно возрастает.

Модель OSI помогает определить, какие протоколы нужно использовать на каждом ее уровне. Продукты разных производителей, которые соответствуют этой модели, способны вполне корректно взаимодействовать друг с другом. ISO, IEEE, ANSI, ITU (International Telecommunications Union) и другие организации по стандартизации разработали протоколы, соответствующие некоторым уровням модели OSI.

TCP/IP – стандартный промышленный набор протоколов, обеспечивающий связь в неоднородной среде, т.е. между компьютерами разных типов. Совместимость – одно из основных преимуществ TCP/IP, поэтому его поддерживают большинство ЛВС. Кроме того, TCP/IP предоставляет маршрутизируемый протокол для корпоративных сетей и доступ в Интернет. Из-за своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия. У TCP/IP есть два главных недостатка: большой размер и недостаточная скорость работы. Но для современных ОС это не является проблемой (проблема только у DOS-клиентов), а скорость работы сравнима со скоростью работы протокола IPX.

Стек TCP/IP включает и другие протоколы:

- SMTP (Simple Mail Transfer Protocol) – для обмена E-mail;
- FTP (File Transfer Protocol) – для обмена файлами;

- SNMP (Simple Network Management Protocol) – для управления сетью.

TCP/IP разрабатывался специалистами МО США как маршрутизируемый, надежный и функциональный протокол. Он также представляет собой набор протоколов для глобальных вычислительных сетей. Его назначение – обеспечивать взаимодействие между узлами даже в случае ядерной войны. Сейчас ответственность за разработку TCP/IP возложена на сообщество Интернет в целом. Установка и настройка TCP/IP требует знаний и опыта со стороны пользователя, однако применение TCP/IP предоставляет ряд существенных преимуществ.

Протокол TCP/IP в точности не соответствует модели OSI. Вместо семи уровней в нем используется только четыре:

1. Уровень сетевого интерфейса.
2. Межсетевой уровень.
3. Транспортный уровень.
4. Прикладной уровень.

Каждый из них соответствует одному или нескольким уровням модели OSI.

Уровень сетевого интерфейса, относящийся к Физическому и Канальному уровням модели OSI, напрямую взаимодействует с сетью. Он реализует интерфейс между сетевой архитектурой (Ethernet или Token Ring) и Межсетевым уровнем.

Межсетевой уровень, относящийся к Сетевому уровню модели OSI, использует несколько протоколов для маршрутизации и доставки пакетов. Для этого используются маршрутизаторы, которые работают на Сетевом уровне и могут переадресовывать и маршрутизировать пакеты через множество сетей, обмениваясь информацией между отдельными сетями..

Транспортный уровень, соответствующий Транспортному уровню модели OSI, отвечает за установку и поддержание соединения между двумя хостами. Транспортный уровень отвечает также за отправку уведомлений о получении данных, управление потоком, упорядочение пакетов и их

повторную передачу. Transmission Control Protocol (TCP) отвечает за надежную передачу данных между узлами. Это ориентированный на соединение протокол, поэтому он устанавливает сеанс связи между двумя компьютерами прежде, чем начать передачу.

Прикладной уровень, соответствующий Сеансовому, Представительскому и Прикладному уровням модели OSI, соединяет в сети приложения.

7. Сетевые службы

В технической литературе англоязычный термин «server» обычно переводится как «служба», «сервис» или «услуга». Часто эти термины используются как синонимы. В тоже время обычно различают термин «служба»: с одной стороны, и термин «сервис» и «услуга» - с другой. Под службой понимается сетевой компонент, который реализует некоторый набор услуг, который предоставляется данной службой. Таким образом, сервис – это интерфейс между потребителем услуг (например, пользователем) и поставщиком услуг (службой). Реализация сетевых служб реализуется программными средствами, причём все сетевые службы соответствуют архитектуре «клиент-сервер». Пара модулей сетевой операционной системы «клиент-сервер» обеспечивает доступ пользователей к определённому типу ресурсов, например к файлам. В этом случае говорят, что пользователь имеет дело с файловой службой. Обычно сетевая ОС поддерживает несколько видов сетевых служб: файловую службу, службу печати, службу электронной почты, службу удалённого доступа и т.д.

Кроме доступа к аппаратным, программным средствам и данным, сетевые службы решают и другие, более специфические задачи, например, задачи, связанные с распределённой обработкой данных. К таким задачам относится обеспечение синхронизации нескольких копий данных, размещение на разных узлах (служба репликации), или организация

выполнения одной задачи параллельно на нескольких машинах сети (служба вызова удалённых процедур).

Одной из важнейших сетевых служб является DNS – служба – служба определения соответствия доменного имени узла и его IP – адреса. Среди сетевых служб выделяется отдельная группа административных служб, используемых только администратором сети для управления вычислительной сетью, например, служба администрирования пользовательских учётных записей (позволяет администратору вести общую базу данных о пользователях сети), служба мониторинга сети (позволяет анализировать сетевой трафик), служба безопасности (в её функции аутентификация пользователей и процессов) и др.

Как правило, сетевая ОС предоставляет услуги основных сетевых служб, обеспечивающих стандартные функции вычислительно сети. Дополнительные услуги могут предоставляться сетевыми службами, реализуемыми системными сетевыми приложениями или утилитами, работающими под управлением ОС. Например, услуги почтового клиента в ОС семейства Windows предоставляются программой Outlook Express, которая интегрирована в операционную систему.

Одним из главных показателей качества сетевой службы является её удобство, и в первую очередь удобство работ с ней для пользователя. Именно поэтому сетевые службы обеспечиваются специальным интерфейсом, в большинстве случаев интуитивно понятным пользователю.

8. Сетевое оборудование

Оборудование делится на:

- активное
- пассивное
- другое

Активное оборудование требует подачи энергии для генерации сигналов (сетевая карта, повторители, концентраторы, модем).

Пассивное оборудование подачи энергии не требует (кабельная система, соединительные разъемы, коммутационные панели). Устройства бесперебойного питания, устройства кондиционирования воздуха, аксессуары (монтажные стойки, шкафы, кабеле-провода).
Типы оборудования сетей.

1. **Конечные системы.** ES (End Systems). Являются источниками и/или потребителями информации (ПК, сетевые принтеры,...)
2. **Промежуточные системы.** IS (Intermediate Systems). Обеспечивают прохождение информации по сети (концентраторы, маршрутизаторы, модемы, кабельная или беспроводная инфраструктура, соединяющая их).

Сетевой трафик - это поток информации, передаваемый по сети. Трафик кроме полезной информации включает и служебную, необходимую для организации взаимодействия узлов сети. Пропускная способность сети определяется количеством информации, проходящей через линию связи за единицу времени (бит/сек, кбит/сек, Мбит/сек, Гб/сек). Производительность сети применима для активного коммуникационного оборудования. Определяется как общее количество неструктурированной информации, пропускаемой оборудованием за единицу времени (бит/сек).

Открытые и закрытые системы.
Для организации обмена информацией должен быть разработан комплекс программных и аппаратных средств, распределенных по разным устройствам сети. По началу, каждый разработчик и поставщик сетевых средств сам разрабатывал весь комплекс задач с помощью собственного набора протоколов, программ и аппаратуры. Это приводило к несовместимости этих наборов у разных поставщиков. Такие системы назывались закрытыми. При соединении нескольких закрытых систем используются частные решения, которые работают, но ограничивают возможности пользователей, привязывая их к приложениям или к аппаратному обеспечению определенных производителей.

Открытые системы предполагают открытые стандарты, направленные на обеспечение совместимости между различными системами, т.е. задача построения сетей разбита на несколько взаимосвязанных подзадач с определением правил взаимодействия между ними. Стандартизация этих правил позволяет расширить количество разработчиков ПО и АО.

9. Стек протоколов TCP/IP

Стек протоколов TCP/IP представляет собой семейство протоколов, обеспечивающих соединение и совместное использование различных систем. Стек был разработан для работы в разнородных сетях. Протоколы стека отличаются высокой надежностью: они отвечают требованию обеспечения возможности работы узлов сети, уцелевших при ограниченном ядерном нападении. В настоящее время стек протоколов TCP/IP используется как для связи в сети Интернет, так и в локальных сетях.

В основу архитектуры TCP/IP была целенаправленно заложена одноранговая структура. TCP/IP имеет распределенный характер, в отличие от классической "нисходящей" модели обеспечения надежности. В среде с TCP/IP никакого центрального органа нет. Узлы взаимодействуют непосредственно друг с другом, и каждый из них обладает полной информацией о всех доступных сетевых сервисах. Если какой-либо из хост-компьютеров отказывает, ни одна из остальных машин на это не реагирует (если только ей не нужны данные, которые как раз на отказавшем компьютере и находятся).

Приведем список протоколов, входящих в стек TCP/IP:

TCP (Transmission Control Protocol - протокол управления передачей) - базовый транспортный протокол, давший название всему семейству протоколов TCP/IP;

UDP (User Datagram Protocol) - второй по распространенности транспортный протокол семейства TCP/IP;

IP (Internet Protocol) - межсетевой протокол;

ARP (Address Resolution Protocol - протокол разрешения адресов)
- используется для определения соответствия IP-адресов и Ethernet-адресов;

SLIP (Serial Line Internet Protocol) - протокол передачи данных по телефонным линиям;

PPP (Point to Point Protocol) - протокол обмена данными "точка-точка";

RPC (Remote Process Control) - протокол управления удаленными процессами;

TFTP (Trivial File Transfer Protocol) - простой протокол передачи файлов;

DNS (Domain Name System) - протокол обращения к системе доменных имен;

RIP (Routing Information Protocol) - протокол маршрутизации.

10. Методы маршрутизации информационных потоков.

Маршрутизация –*routing*– процесс определения в коммуникационной сети пути, по которому вызов, либо блок данных может достигнуть адресата.

Маршрутизация представляет собой правила выбора очередного узла вычислительной сети на пути движения от источника к адресату. Маршрутизация охватывает все потоки, передаваемые по коммуникационной подсети, но она не оказывает непосредственно влияния на интенсивность поступления потоков в ИС и объемы информации, подлежащий передаче. Маршрутизация имеет дело с сообщениями уже принятыми в сеть.

Все алгоритмы маршрутизации делятся на две группы: стохастические и детерминированные.

Стохастические алгоритмы для принятия решения о маршруте, используют оценки, полученные из наблюдений за прохождением сообщений через узлы, как правило без учета топологии сети передачи данных.

Детерминированные алгоритмы основываются на расчете временных характеристик, например, времени для достижения узлов назначения в идеальных условиях для соответствующей структуры сети условиях.

Существующие алгоритмы маршрутизации классифицируются следующим образом:

- детерминированная маршрутизация (неизменяющейся стратегия без изменения условий в сети);
- локальная адаптивная маршрутизация (принятие решений в зависимости только от локальной информации о работе и загрузке узла);
- распределенная адаптивная маршрутизация (узлы обмениваются информацией между собой и выбор происходит на основе как локальной информации о работе, так и информации о работе всей сети);
- централизованная маршрутизация (все узлы передают информацию центральному узлу, а тот рассылает директивы о том, как управлять работой каждого из них).

Алгоритм маршрутизации, использующий детерминированную стратегию, работает таким образом, чтобы каждый узел мог распознать адрес назначения каждого проходящего через него пакета. По этому адресу в таблице маршрутизации определяется конкретный канал, по которому следует передать пакет данных. В таблице указываются также кратчайшие пути между всеми парами узлов, причем кратчайший путь из любого узла не зависит от того, откуда пакет поступил в данный узел. Для известной нагрузки на сеть, изменяющейся со временем, фиксированные таблицы составляют таким образом, чтобы обеспечить максимальную пропускную способность в различных местах сети.

Выбор маршрута можно сделать зависимым от того, откуда принят пакет. Это в некоторых случаях делает алгоритм более эффективным. Известен метод маршрутизации, заключающийся в детерминированном распределении трафика в узле на пропорциональные части для передачи по двум или более выходящим из этого узла каналам. Однако

детерминированные алгоритмы зачастую неэффективны, поэтому широко применяется адаптивная маршрутизация, при которой принятие решения о выборе производится часто по неполной информации. В этом случае - применяют неоптимальные адаптивные алгоритмы, которые основываются на измерениях времен задержек, длин очереди, интенсивности потоков с учетом информации с близлежащих узлов.

Управление маршрутизацией путем обмена таблицами минимальных задержек. Между узлами характеризуется хорошей способностью к адаптации и к уменьшению задержек. Однако реакция на изменение нагрузок в сетях замедляется.

С точки зрения топологической структуры адаптивная маршрутизация может быть централизованной, локальной и распределенной. При централизованной адаптивной маршрутизации каждый узел сети передает сообщение о своем состоянии (текущее значение о длинах очередей, работоспособность трактов) в центральный узел (ЦУ), который составляет глобальную картину состояния сети. На основе этой информации определяются наилучшие моменты распределения потоков по сети.

Способ сбора информации о состоянии сети и рассылка управляющих директив в сети могут быть синхронными и асинхронными. Если все узлы посылают свои сообщения и получают директивы от ЦУ, то такой способ управления трафиком называется синхронным. При асинхронном управлении маршрутизацией эти действия выполняются о процессе существенных отклонений от нормального режима, когда необходимо внести соответствующие коррективы.

При синхронном способе обмена служебной информацией, представляемой для целей маршрутизации, объем ее может быть слишком большим. При асинхронном он меньше, поскольку ЦУ действует на основе частично устаревшей информации. Если в сети меняются достаточно быстро, то централизованное управление может оказаться неэффективным вследствие запаздывания. Централизация управления может привести к

потере управления по всей сети при выходе ЦУ из строя. Во избежание этого создаются системы гибридной адаптивной маршрутизации. Примером является так называемая дельта-маршрутизация. При этом алгоритме ЦУ следит за общей ситуацией, в то время как всем остальным узлам предоставлена возможность быстро и независимо реагировать на локальные колебания трафика и состоянии компонентов сети. В дельта-алгоритме ЦУ рассылает маршрутные таблицы остальным узлам сети, но эти таблицы используются в сочетании с анализом длин очередей в этом узле.

При нескольких одинаковых по эффективности путях маршрутный алгоритм предоставляет узлу самому решать, по какому из них направить пакет. Но если маршрутная таблица, построенная ЦУ, предусматривает лишь один путь до некоторого адресата, то алгоритм обязывает узел посылать пакеты только по этому пути. Увеличение размеров сетей достигается увеличением числа узлов и объединением сетей. Объединение производится путем создания общих узлов мысленно эти узлы можно разделить на две части, каждая из которых является узлом своей сети. Другой вариант соединения сетей состоит в том, что узлы объединяемых сетей связываются общим трактом. Независимо от способа соединения проблемы маршрутизации оказываются достаточно сложными. Узлы, соединяющие разные сети принято называть шлюзами.

Принцип образования шлюзов позволяет избежать необходимости хранения в каждом узле полного набора маршрутных таблиц. При использовании шлюзов указывают маршрут от узла сети до шлюза, соединяющего одну сеть с другой. Если объединяются не две, а более сетей, может оказаться, что пакет должен пройти промежуточные сети через несколько шлюзов. Имеет смысл в этом случае создать специальный формат, удовлетворяющий требованиям местного протокола.

После упаковки пакетов межсетевой формат маршрутизации в промежуточных сетях между конечными шлюзами может выполняться независимо от межсетевой маршрутизации

Применение таблиц для решения задач маршрутизации при управлении является сложным процессом, требующим больших вычислительных ресурсов. Чтобы устранить этот недостаток были разработаны простейшие алгоритмы маршрутизации без таблиц. Они работают следующим образом.

При стохастической маршрутизации пакеты, передаваемые по сети, совершают случайные блуждания и не имеют определенного направления. Они снабжаются счетчиками пройденных узлов и уничтожаются, если их значения превышают установленную величину. При большой скорости операций пакет может быстро прийти в узел назначения. Недостаток метода – отсутствие гарантии, что пакет вообще придет, но преимущества очевидны – полная независимость от информации о состоянии сети и отсутствие таблиц

При лавинной маршрутизации пакет, поступивший в узел, размножается в количестве, равном числу выходных каналов. В этом случае, как и при стохастической маршрутизации, применяется счетчик шагов. При повторном поступлении в узел передача может быть прекращена. Достоинство метода в том, что, по крайней мере, одна копия достигает адресата по кратчайшему пути, причем для управления не требуется таблиц. Однако, могут возникнуть и трудности, связанные с восстановлением процессов.

В большинстве алгоритмов маршрутизации применяются таблицы и фиксированные стратегии распределения потоков, которые затем адаптируются к различным требованиям и условиям, обеспечивающим эффективное управление процессом.

Фиксированная стратегия наиболее проста. Она основывается на готовых таблицах, причем для слабо загруженных сетей и при постоянном трафике можно подобрать наиболее эффективные таблицы маршрутизации. Работа алгоритма в этом случае осуществляется следующим образом. При выходе из строя некоторого промежуточного узла или канала узлы, находящиеся на концах неисправного участка, передают сообщения всем другим и представляют при необходимости таблицы. Чтобы эта информация распространялась как можно быстрее, соответствующим сообщениям

устанавливается высший приоритет. В процессе обработки таблиц реализуется одна из возможных разновидностей фиксированной маршрутизации: использование нескольких путей, разгрузка каналов и создание обходных путей

Алгоритмы фиксированной маршрутизации легко можно приспособить к изменению трафика и перейти к адаптивной маршрутизации. Эти алгоритмы рекомендуется применять при небольших нагрузках и при повреждениях в сетях.

Кроме фиксированного алгоритма для адаптивной маршрутизации применяется маршрутизация по предыдущему опыту, т.е. сначала применяют лавинные и случайные алгоритмы маршрутизации, а по мере получения данных о работе сети и переходе ее в устойчивый режим начинают применять детерминированную стратегию и маршрутизация осуществляется по вновь созданным таблицам. Такая сеть может приспособиться к изменениям, но перенастройка происходит очень медленно

Существует еще один метод адаптивной маршрутизации – метод скорейшей передачи. Каждый узел, получив пакет, пытается как можно скорее его отправить соседнему узлу независимо от того, входит ли канал в кратчайший путь. Каналы упорядочиваются по мере и способности к быстрой доставке. Таблицы строятся аналогично на основе полученных результатов.

Для управления распределением нагрузок, потоков и восстановлением нормальных режимов в масштабах всей сети следует организовать управление маршрутизацией, исходя из требований нормального функционирования каждого отдельного узла. Этот принцип организации определяет одну из разновидностей алгоритмов маршрутизации – локальную адаптивную маршрутизацию

Если узел находится в исправном состоянии, то для принятия решения необходима информация, представляющая собой заранее загруженные в память таблиц, а также сведения о текущем состоянии его выходных каналов

и длинах очередей пакетов. Информация о состоянии других узлов не используется. Алгоритм выбирает маршрут из множества возможных, заданных таблицами, и исходя из характеристик собственного состояния.

Маршрутам присваиваются различные веса: основному маршруту – вес 3, вторичному маршруту – 2, третичному маршруту – 1 и т.д. Устанавливаются зависимости между весами и длинами очередей, причем задается максимальная длина. В каждой очереди также задается определенный вес, зависящий от числа свободных мест до заполнения. Вес очереди складывается с весом маршрута. В процессе маршрутизации делается выбор между первичным и вторичным маршрутом в соответствии с обобщенным значением веса. Если какая-либо из очередей полна, то пакет посылается по другому пути независимо от числа свободных мест в нем.

Локальный адаптивный алгоритм мало увеличивает пропускную способность сети. Он слишком медленно реагирует на увеличение трафика, ведущее к перегрузке. Однако важно то, что сеть оказывается устойчивой.

Распределенная адаптивная маршрутизация учитывает указанные недостатки, обеспечивает минимальное время задержки передаваемого трафика. Каждый узел формирует таблицы маршрутов и передает ко всем узлам назначения с указанием времени передачи к каждому адресату, организует обмен этими таблицами. После обмена таблицами задержек каждый узел приступает к пересчету задержек, учитывая длины собственных очередей к выходным трактам. Эти расчеты показывают, к какому из узлов следует направить пакет, чтобы достичь его с минимальными задержками.

11. Методы коммутации информации

Важное значение в архитектуре открытых сетей играет *коммутация информации*. Ее задачей является прокладка в сетях тактов, необходимых для доставки последовательностей блоков данных абонентским системам-адресатам. Существует несколько методов коммутации информации (рис. 33).



Рис. 33 Методы коммутации информации

Коммутация каналов появилась ранее других в сетях, имеющих большое число каналов. Для этой цели в коммуникационной подсети устанавливается один либо нужное число коммутаторов, именуемых *узлами коммутации каналов*. Каждый из них соединяет нужные пары каналов передачи данных. Благодаря этому создаются *тракты* — последовательности каналов, через которые обеспечивается взаимодействие пар абонентских систем.

При работе в режиме коммутации каналов перед началом взаимодействия необходимо выполнить ряд предварительных процедур связанных с организацией создания тракта.

Метод *коммутации пакетов* не имеет указанных недостатков. Важной его особенностью является одновременное коллективное использование каналов значительным числом абонентских систем. Здесь физические тракты не создаются и ни один канал не отдается в монопольное владение парой абонентских систем. По каждому из каналов по мере поступления передаются блоки данных, посылаемые различными абонентскими системами. Сети с коммутацией пакетов используют вместо одноуровневых коммутаторов (как в предыдущем случае) используют трехуровневые маршрутизаторы. Коммутация пакетов позволяет резко повысить загрузку каналов.

Опыт и расчеты показывают, что экономически выгодно по одним и тем же каналам передавать любую информацию. Как та, которая требует определенного времени доставки, так и та, которая допускает появление

случайных величин запаздывания. В этой связи возникла необходимость создания смешанной коммутации обеспечивающей на базе одного и того же множества канала коммутацию как каналов, так и пакетов.

При *смешанной коммутации* используются уровни и процессы, применяемые как в коммутации каналов так и в коммутации пакетов. При смешанной коммутации имеющиеся каналы отдаются в первую очередь для создания трактов соединяющих абонентские системы. Свободные при этом каналы не простаивают и используются для коммутации пакетов. Естественно, что в рассматриваемом случае в подсети устанавливаются комбинированные узлы, выполняющие роль, как коммутаторов каналов, так и коммутаторов пакетов.

Четвертым типом коммутации информации является *интегральная коммутация*. Она, как и смешанная, предназначена для обеспечения передачи информации с заданным случайным временем доставки блоков данных. Однако интегральная коммутация отличается от смешанной тем, что здесь коммутация каналов и коммутация пакетов осуществляются одновременно в каждом физическом канале.

12. Эволюция моделей и структур информационных сетей.

Первоначально сети представляли собой нестандартизованные средства взаимодействия автономных компьютеров в нескольких же нестандартизованных вычислительных системах (в настоящее время их называют терминальными сетями). В таких средах прикладное программное обеспечение работало только под управлением единственной операционной системы. Эта операционная система, в свою очередь, могла надежно функционировать только на аппаратных платформах одного и того же производителя.

В период царствования таких цельных систем отдельных изготовителей произошло два события, изменивших ход развития компьютерных технологий. Во-первых, начали появляться первые

примитивные предшественники современных персональных компьютеров (с начала 70-х гг.). Новизна этих устройств заключалась в том, что вся их вычислительная мощность сосредотачивалась непосредственно на рабочем столе. Во-вторых, ученые в исследовательском центре компании Xerox приступили к поискам средств повышения производительности отдельных коллективов. В частности, они начали новый способ совместного использования файлов и данных: рабочими станциями. Как стало известно впоследствии, основной причиной принципиально нового технологического решения оказалась обычная человеческая лень - ученым просто надоело бегать между компьютерами с дискетами.

В результате появилась на свет первая локальная сеть (Local Area Network - LAN), которая получила название "ethernet". Это была примитивная сеть, но рыночный потенциал этой технологии был очевиден и первоначальная версия ethernet, известная сейчас как Ethernet I, была вытеснена улучшенной Ethernet II. Эта версия разработана компаниями Xerox, Digital и Intel, которые совместными усилиями установили "стандарты" для Ethernet II и разработали соответствующие технологии.

Интеллектуальные пользовательские устройства в сочетании с локальными сетями породили новую парадигму — открытые распределенные вычислительные системы.

Интересна история появления первой распределенной сети, впоследствии превратившейся в сеть Internet. В разгар "холодной войны", в конце 60-х гг. по заказу министерства обороны США началась разработка сети, которая должна была связать между собой компьютеры военного ведомства, и в первую очередь компьютеры исследовательских центров, для ускорения научных исследований в интересах обороны. В январе 1969 г. была запущена система, связавшая между собой четыре компьютера в разных концах США (испытания длились 10 мин.). А через год новая информационная сеть, названная ARPANet, уже приступила к работе. С каждым годом ARPANet росла и развивалась. В сеть включались все новые и

новые участники: право доступа в сеть начали требовать сначала все крупные лаборатории, потом - более мелкие, затем - учебные заведения... В 1973 году впервые через сеть оказались соединены компьютеры разных стран: сеть стала международной. В итоге, когда в сеть оказались соединены тысячи компьютеров, стало ясно: необходимо полностью переработать механизм доступа в APRANet. Такой механизм, названный "протоколом TCP/IP" (Transmission Control Protocol/Internet Protocol), был введен в 1983 году.

Рождение протокола TCP/IP, позволяющего пользователям с легкостью подключаться к сети при помощи обыкновенной телефонной линии, совпало с другим событием - разделением APRANet. Военные выделили часть компьютеров в новую сеть, получившую название MILNet, а остальное пространство Сети оставили на усмотрение жаждущей коммуникаций общественности. Так родился Internet.

14 апреля 1998 года история Internet вышла на второй виток: в США состоялся торжественный "запуск" новой сети, получившей название "Internet -2". Создателями новой сети стали крупнейшие учебные заведения, научные и исследовательские учреждения, крупные корпорации США. Скорость передачи информации в Internet-2 просто потрясает воображение, - она превышает более чем в 1000 раз возможности самых быстрых каналов сегодняшней сети. Понятно, что с приходом Internet-2 такие понятия, как "компьютерное телевидение", передача "живого видео" в реальном времени и даже "Internet-кинматограф" переходит из области фантастики в разряд бытовых, привычных явлений.

Базовый функциональный профиль - функциональный профиль, включающий иерархию протоколов только нескольких уровней . Так как базовый функциональный профиль определяется стандартами лишь части уровней области взаимодействия , то он является фундаментом, на котором строится полный функциональный профиль либо коллапсный функциональный профиль . Поэтому базовый функциональный профиль самостоятельного значения не имеет. Пользуются популярностью (рис.313)

базовые функциональные профили, именуемые оптоволоконный распределенный интерфейс данных, распределенная двойная шина с очередями, открытая сетевая обработка данных, базовый функциональный профиль АТМ, сетевая базовая система ввода/вывода.

Коллапсный функциональный профиль - псевдо-полный функциональный профиль, в котором отсутствует один либо несколько уровней.

Коллапсным называют профиль, в котором функции отсутствующих уровней настолько упрощены, что включены в набор задач, выполняемых оставшимися уровнями. Появление коллапсных профилей открыло возможность создания очень простых и быстродействующих локальных сетей. Естественно, что эти преимущества получены за счет резкого упрощения ряда функций области взаимодействия. В этой связи, рассматриваемые профили имеют ограниченные возможности представления данных и организации сеансов. Кроме этого, здесь упрощена передача данных через коммуникационную сеть.

Примером коллапсного профиля является miniMAP, созданный фирмой General Motors.

Рис. 085. Профиль miniMAP.



Его архитектура характеризуется рядом важных особенностей, отличающих ее от Z функционального профиля MAP. Прежде всего, в miniMAP резко ограничены возможности создания разнообразных сетевых

служб . Этот профиль предназначен только для управления такими технологическими процессами , в которых необходимо лишь передавать небольшие порции данных и получать короткие, но быстрые ответы. Подобные процессы используются в сетях считывающих устройств , интеллектуальных датчиков, систем машинного зрения, роботов .

Полный функциональный профиль - функциональный профиль, включающий иерархию протоколов всех семи уровней . Полный функциональный профиль является целостным и законченным продуктом, обеспечивающим прикладные процессы всем набором видов сервиса, предоставляемых областью Взаимодействия Открытых Систем (ВОС). Состоит он из иерархической группы взаимосвязанных функциональных блоков. (рис.167)

Рис. 167. Структура полного профиля.



Базой профиля, как правило, являются выбранные в качестве стандарта территориальные сети и локальные сети. Они определяют физический уровень (1), канальный уровень (2) и сетевой уровень (3). Далее следует общий транспортный протокол, расположенный на транспортном уровне (4). Эти четыре уровня образуют транспортную платформу. В верхней части сеансовый уровень (5), представительный уровень (6) и прикладной уровень (7) создают прикладную платформу. Непосредственно на ней располагаются прикладные процессы.

Полными функциональными профилями являются системная сетевая архитектура, архитектура дискретной сети, функциональный профиль МАР, функциональный профиль ТОР, открытая сетевая архитектура. (рис.313) Во многих странах разработаны правительственные профили взаимодействия открытых систем, также являющиеся полными функциональными профилями.

13. Информационная безопасность в сетях.

Типы угроз в сетях IP-телефонии

Существует несколько основных типов угроз, представляющих опасность в сетях *IP-телефонии*:

1. *Прослушивание.* В момент передачи конфиденциальной информации о пользователях (идентификаторов, паролей) или конфиденциальных данных по незащищенным каналам существует возможность прослушивания и злоупотребления ими в корыстных целях злоумышленником.

2. *Манипулирование данными.* Данные, которые передаются по каналам связи, в принципе можно изменить.

3. *Подмена данных* о пользователе происходит в случае попытки выдачи одного пользователя сети за другого. При этом возникает вероятность несанкционированного доступа к важным функциям системы.

4. *Отказ в обслуживании (denial of service - DoS)* является одной из разновидностей атак нарушителей, в результате которой происходит вывод из строя некоторых узлов или всей сети. Она осуществляется путем переполнения системы ненужным трафиком, на обработку которого уходят все системные ресурсы. Для предотвращения данной угрозы необходимо использовать средство для распознавания подобных атак и ограничения их воздействия на сеть.

Базовыми элементами в области безопасности являются:

аутентификация;

целостность;
активная проверка.

Применение расширенных средств *аутентификации* помогает сохранить в неприкосновенности вашу идентификационную информацию и данные. Такие средства могут основываться на информации, которую *пользователь* знает (*пароль*).

Целостность информации - это способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения). Под *угрозой нарушения целостности* понимается любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что *целостность информации* нарушена. *Целостность* также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения.

И, наконец, *активная проверка* означает проверку правильности реализации элементов технологии безопасности и помогает обнаруживать несанкционированное проникновение в *сеть* и атаки типа DoS. Активная проверка данных действует как система раннего оповещения о различных типах неполадок и, следовательно, позволяет принять упреждающие меры, пока не нанесен серьезный *ущерб*.

14. Методы оценки эффективности информационных сетей.

Эффективность информационной сети — это ее способность достигать поставленную цель в заданных условиях применения и с определенным качеством.

Конкретизируя это понятие, можно сказать, что эффективность информационной сети — это характеристика, отражающая степень соответствия сети своему назначению, техническое совершенство и экономическую целесообразность. Понятие эффективности связано с

получением некоторого полезного результата - эффекта использования информационных сетей. Эффект достигается ценой затрат определенных ресурсов, поэтому эффективность сети часто рассматривается в виде соотношения между эффектом (выигрышем) и затратами.

Показатель эффективности сети — количественная характеристика информационной сети, рассматриваемая применительно к определенным условиям ее функционирования. При оценке эффективности информационной сети необходимо учитывать характеристики трудовой деятельности человека, взаимодействующего с ЭВМ и другими техническими средствами сети. Следовательно, сеть рассматривается как система "человек-машина" (СЧМ).

Показатель эффективности информационной сети определяется процессом ее функционирования, он является функционалом от этого процесса.

15. Территориальные и глобальные сети как средство взаимодействия

При физическом соединении двух или более компьютеров образуется компьютерная сеть. В общем случае, для создания компьютерных сетей необходимо специальное аппаратное обеспечение (сетевое оборудование) и специальное программное обеспечение (сетевые программные средства). Простейшее соединение двух компьютеров для обмена данными называется прямым соединением.

Основной задачей, решаемой при создании компьютерных сетей, является обеспечение совместимости оборудования по электрическим и механическим характеристикам и обеспечение совместимости информационного обеспечения (программ и данных) по системе кодирования и формату данных. Решение этой задачи относится к области стандартизации и основано на так называемой модели OSI (модель взаимодействия открытых систем — Model of Open System Interconnections). (создана на основе

технических предложений Международного института стандартов ISO (International Standards Organization).

Согласно модели ISO/OSI архитектуру компьютерных сетей следует рассматривать на разных уровнях (общее число уровней — до семи). Самый верхний уровень — прикладной. На этом уровне пользователь взаимодействует с вычислительной системой. Самый нижний уровень — физический. Он обеспечивает обмен сигналами между устройствами. Обмен данными в системах связи происходит путем их перемещения с верхнего уровня на нижний, затем транспортировки и, наконец, обратным воспроизведением на компьютере клиента в результате перемещения с нижнего уровня на верхний.

Для обеспечения необходимой совместимости на каждом из семи возможных уровней архитектуры компьютерной сети действуют специальные стандарты, называемые протоколами. Они определяют характер аппаратного взаимодействия компонентов сети (аппаратные протоколы) и характер взаимодействия программ и данных (программные протоколы). Физически функции поддержки протоколов исполняют аппаратные устройства (интерфейсы) и программные средства (программы поддержки протоколов). Программы, выполняющие поддержку протоколов, также называют протоколами.

Так, например, если два компьютера соединены между собой прямым соединением, то на низшем (физическом) уровне протокол их взаимодействия определяют конкретные устройства физического порта (параллельного или последовательного) и механические компоненты (разъемы, кабель и т.п.). На более высоком уровне взаимодействие между компьютерами определяют программные средства, управляющие передачей данных через порты. Для стандартных портов они находятся в базовой системе ввода/вывода (BIOS). На самом высоком уровне протокол взаимодействия обеспечивает операционная система.

В соответствии с используемыми протоколами компьютерные сети принято разделять на локальные (LAN — Local Area Network) и глобальные (WAN — Wide Area Network). Компьютеры локальной сети преимущественно используют единый комплект протоколов для всех участников. По территориальному признаку локальные сети отличаются компактностью. Они могут объединять компьютеры одного помещения, этажа, здания, группы компактно расположенных сооружений. Глобальные сети имеют, как правило, увеличенные географические размеры. Они могут объединять как отдельные компьютеры, так и отдельные локальные сети, в том числе и использующие различные протоколы.

Назначение всех видов компьютерных сетей определяется двумя функциями:

обеспечение совместного использования аппаратных и программных ресурсов сети;

обеспечение совместного доступа к ресурсам данных.

Так, например, все участники локальной сети могут совместно использовать одно общее устройство печати (сетевой принтер) или, например, ресурсы жестких дисков одного выделенного компьютера (файлового сервера). Это же относится и к программному, и к информационному обеспечению. Если в сети имеется специальный компьютер, выделенный для совместного использования участниками сети он называется файловым сервером. Компьютерные сети, в которых нет выделенного сервера, а все локальные компьютеры могут общаться друг с другом на «равных правах» (обычно это небольшие сети), называются одноранговыми.

Группы сотрудников, работающих над одним проектом в рамках локальной сети называются рабочими группами. В рамках одной локальной сети могут работать несколько рабочих групп. У участников рабочих групп могут быть разные права для доступа к общим ресурсам сети. Совокупность приемов разделения и ограничения прав участников компьютерной сети

называется политикой сети. Управление сетевыми политиками (их может быть несколько в одной сети) называется администрированием сети. Лицо, управляющее организацией работы участников локальной компьютерной сети, называется системным администратором.

Создание локальных сетей характерно для отдельных предприятий или отдельных подразделений предприятий. Если предприятие (или отрасль) занимает обширную территорию, то отдельные локальные сети могут объединяться в глобальные сети. В этом случае локальные сети связывают между собой с помощью любых традиционных каналов связи (кабельных, спутниковых, радиорелейных и т. п.). При соблюдении специальных условий для этой цели могут быть использованы даже телефонные каналы, хотя они в наименьшей степени удовлетворяют требованиям цифровой связи.

Для связи между собой нескольких локальных сетей, работающих по разным протоколам, служат специальные средства, называемые шлюзами. Шлюзы могут быть: как аппаратными, так и программными. Например, это может быть специальный компьютер (шлюзовый сервер), а может быть и компьютерная программа. В последнем случае компьютер может выполнять не только функцию шлюза, но и какие-то иные функции, типичные для рабочих станций.

При подключении локальной сети предприятия к глобальной сети важную роль играет понятие сетевой безопасности. В частности, должен быть ограничен доступ в локальную сеть для посторонних лиц извне, а также ограничен выход за пределы локальной сети для сотрудников предприятия, не имеющих соответствующих прав. Для обеспечения сетевой безопасности между локальной и глобальной сетью устанавливают так называемые брандмауэры. Брандмауэром может быть специальный компьютер или компьютерная программа, препятствующая несанкционированному перемещению данных между сетями.