Дисклеймер.

Автор не несет ответственности за любой ущерб, причиненный Вам при использовании данного документа. Автор напоминает, что данный документ может содержать ошибки и опечатки, недостоверную и/или непроверенную информацию. Если Вы желаете помочь в развитии проекта или сообщить об ошибке/опечатке/неточности:

GitHub проекта

Автор в ВК

Содержание

1 Введение. История развития компьютерных сетей.

Прародителем современных компьютерных сетей считаются телефонные сети. Еще при первых попытках создать компьютерную сеть, узлы которой были бы отдалены друг от друга на значительное расстояние, использовались телефонные линии, которые, однако, не могли обеспечить должное качество и скорость соединения.

Необходимость в сетях подобного рода возникла еще в 50-х годах прошлого века. Примерно в это время были предприняты первые попытки объединить в сеть несколько удаленных компьютеров. Однако наибольший толчок развитию сетей дало решение министерства обороны США о создании системы раннего оповещения о ракетной атаке со стороны СССР. Так как наблюдательные и радиолокационные пункты были разбросаны по всей стране, возникла необходимость в сети, способной быстро передавать информацию. В 1962 году Джордж Ликлайдер из Массачусетского университета выступает с серией заметок о социальном взаимодействии при помощи компьютерных сетей. В этом же году его приглашают на должнось первого руководителя исследовательского компьютерного проекта при Министерстве обороны США. Реализовывался этот проект на базе DARPA (Defense Advanced Research Projects Agency) — агентства передовых оборонных исследовательских проектов.

Так в конце 1969 года увидела свет первая компьютерная сеть APRANet, состоящая всего из 4-х компьютеров. В основе этой сети лежала идея пакетной коммутации, предложенная еще Полом Бэреном в середине 50-х годов. В течении последующих пяти лет к APRANet были подключены еще несколько сотен компьютеров.

Параллельно развивались другие проекты сетей, однако препятствием между их совместной работой было то, что все они работали по-разному. Встала острая необходимость в едином протоколе, который позволил бы общаться разным компьютерам и сетям совместно. И в 1983 году той же компанией DAPRA был разработан протокол TCP/IP, который был признан стандартным протоколом для построения сетей. Машины APRANet были переведены на него в том же году.

Процесс объединения сетей ускорялся с каждым годом, и появление персональных компьютеров лишь подстегнуло его. Был разработан стандарт OSI, повышалась скорость соединения и в результате мы имеем то, что имеем - Интернет.

2 Деление компьютерных сетей (территориальное, среда передачи данных, архитектура)

По своей природе компьютерные сети подразделяются по территориальному признаку, среде передачи данных и архитектуре. Рассмотрим подробнее все три способа деления.

Территориальное деление подразумевает деление на **глобальные** и **локальные** сети.

1. Примером **глобальной** сети может служить Интернет или сеть мобильной связи стандарта GSM. Отличие глобальной сети от прочих в том, что она охватывает всю Землю. Построение подобной сети — очень ресурсоемкий процесс, требующий объединения усилий большинства стран на Земле.

2. **Локальные** сети же подразумевают охват лишь небольшого участка земной поверхности. Размеры локальных сетей могут быть различны: начиная от локальных сетей, построенных внутри одной квартиры и заканчивая сетями, объединяющими несколь-

ко городов. Локальные сети очень распространены и являются обязательным условием работы крупных и не очень фирм.

По **среде передачи данных** сети делятся на:

1. **Проводные** сети. В сетях такого типа данные передаются посредством использования проводов либо кабелей. Примерами проводных сетей являются телефонная сеть, витая пара, оптоволокно, коаксиал.

2. **Беспроводные** сети. В сетях такого типа данные передаются посредством радиолибо иных волн. Примеры: Wi-Fi, Li-Fi, Bluetooth, спутниковая, сотовая, радиосвязь, инфракрасный порт, NFC.

Архитектура сети — комбинация топологий, методов доступа к среде передачи данных и протоколов, необходимых для создания работоспособной сети. По архитектурному признаку сети могут различаться:

1. Топологией

2. Используемым протоколом

Топология сети — геометрическая форма и физическое расположение компьютеров по отношению к друг другу. По топологии можно выделить:

1. Полносвязные сети (каждый-с-каждым)

2. Неполносвязные сети.

3 Проводные и беспроводные сети

Проводные сети — сети, в которых для передачи данных используются провода, кабели. Примерами проводных сетей являются:

1. Телефонная сеть. Используется витая пара (состоящая из 4 проводков, свитых попарно, а затем эти пары свиты еще раз), либо так называемая «лапша» — два свитых проводка. «Лапша» по определению не является витой парой. Скорость передачи данных по витой паре в телефонных сетях составляет 24 Мбит/с (максимальная скорость для ADSL). В данный момент достаточно широко используется, но постепенно выходит из употребления.

2. Витая пара. Та же самая витая пара, но имеющая от 4 до 8 проводков. Бывает неэкранированная, экранированная и дважды экранированная. Экранированная пара представляет собой заключенную в экран витую пару, дважды экранированная также имеет экран, в который заключены все витые пары. Экран представляет собой тонкую фольгу, которая защищает данные от воздействия помех. Скорость передачи данных до 10 Гбит/с, используется повсеместно.

3. Оптоволокно. Представляет собой кабель из гибкого стекла, покрытого отражающим материалом. Передача данных осуществляется посредством высокочастотных световых вспышек. Скорость передачи данных — гигабайты в секунду. Только начинает свой путь в дома потребителей.

4. Коаксиал. Представляет собой одножильный толстый провод в полиэтиленовой оплетке с экраном. Использовался ранее для построения локальных сетей. Скорость передачи данных составляла до 10 Мбит/с. В настоящий момент вытеснен витой парой.

Беспроводные сети — сети, в которых передача данных осуществляется посредством радиосвязи, световых либо инфракрасных волн, магнитного поля. Виды сетей:

1. WiFi (2,4 ГГц, 5 ГГц). Используются радиоволны. Максимальное расстояние передачи данных, заявленное в спецификации — 300 метров. В условиях зданий — 10-20 метров. Скорость данных — до 300 Мбит/с для 5 ГГц. Распространен повсеместно.

2. LiFi. Используются световые волны. Как следствие, передача возможна лишь в пределах одного помещения. Скорость передачи данных — до 1 Гбит/с.

3. Спутниковая связь. Для передачи данных используются радиоволны. Дорогая в использовании, однако покрывающая почти всю Землю связь. Низкая скорость передачи данных. Примеры технологий: GPS, спутниковый телефон.

4. Инфракрасный порт. Используются высокочастотные инфракрасные импульсы. Передача данных возможна лишь в условиях прямой видимости. Скорость достаточно низкая (Килобиты в секунду).

5. Bluetooth. Используются радиоволны. Средняя скорость передачи данных, но невысокая дальность — до 30 метров.

6. Сотовая связь. Радиоволны. Дальность $\approx 20 - 30$ км. Низкая скорость передачи данных на больших расстояниях, однако возможно ее увеличение при небольших. Примеры: GSM, 3G, 4G.

7. Радиосвязь. На скорость и дальность передачи данных влияют длина волны и ее частота. Используется повсеместно.

8. Фотоэлемент. Вообще непонятная штуковина.

9. NFC. Используется магнитное поле. Дальность передачи данных — до 10 см. Скорость — килобайты в секунду. Используется в метках, бесконтактных картах, проездных, студенческих.

4 Топология сетей.

Сетевая тополо́гия — это конфигурация графа, вершинам которого соответствуют конечные узлы сети (компьютеры) и коммуникационное оборудование (маршрутизаторы), а рёбрам — физические или информационные связи между вершинами.

Топология может быть **полносвязной** (рис. 4.1) — в которой каждый компьютер непосредственно связан со всеми остальными. Однако этот вариант громоздкий и неэффективный, потому что каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров.

Гораздо удобнее использовать неполносвязные топологии. Существует несколько типов такой топологии:

1) Шина (рис. 4.2)**:**

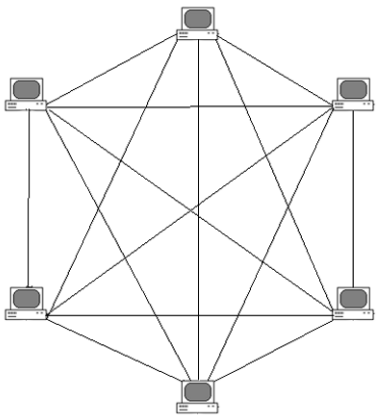

Рис. 4.1:

Топология данного типа, представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

Преимущества сетей шинной топологии:

- расход кабеля существенно уменьшен 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;
- недостаточная надежность сети из-за проблем с разъемами кабеля;
- низкая производительность, обусловлена разделением канала между всеми абонентами.

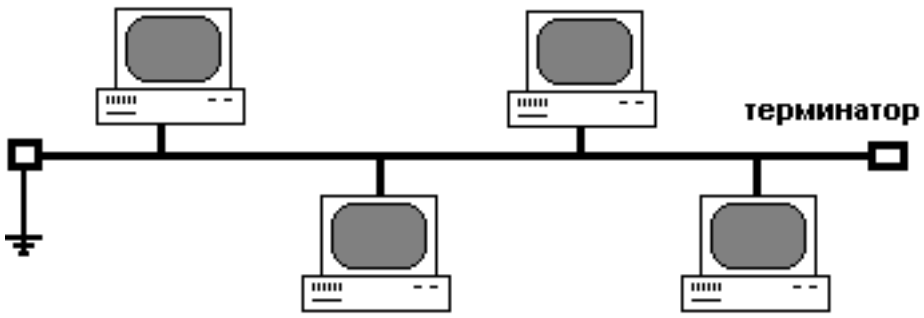

Рис. 4.2:

2) В сети, построенной по топологии типа «**звезда**» (рис. 4.3), каждая рабочая станция подсоединяется кабелем (витой парой) к концентратору или хабу (англ. hub). Концентратор обеспечивает параллельное соединение ПК и, таким образом, все компьютеры, подключенные к сети, могут общаться друг с другом.

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.

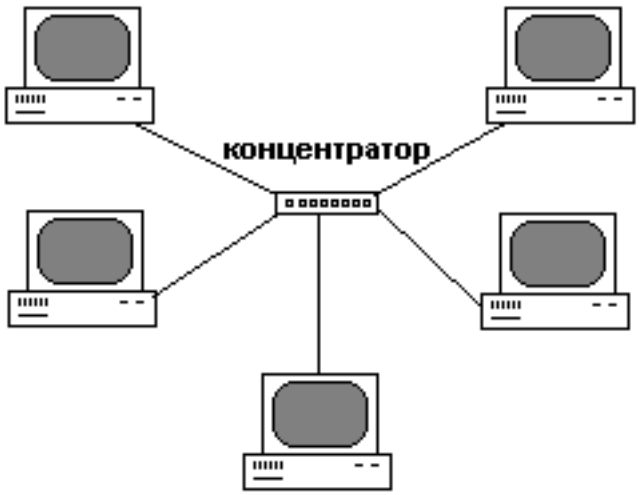

Рис. 4.3:

3) В сети с топологией типа **«кольцо»** (рис. 4.4) 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 относится 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.

4) Дерево — это топология сетей, в которой каждый узел более высокого уровня связан с узлами более низкого уровня звездообразной связью, образуя комбинацию звезд. Также дерево называют иерархической звездой.

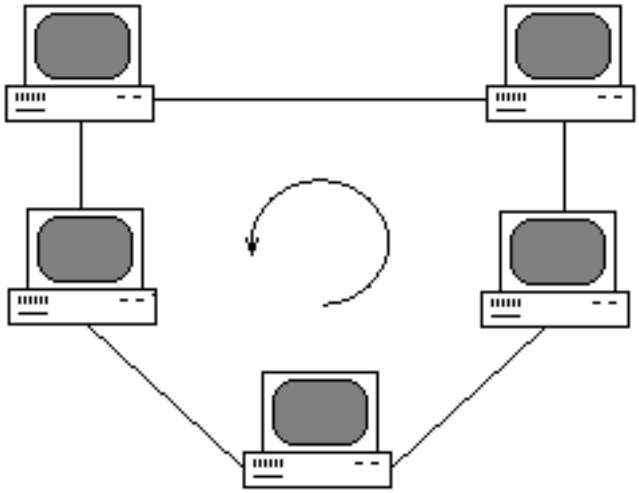

Рис. 4.4:

К достоинствам данной топологии можно отнести то, что сеть с данной топологией легко увеличить и легко её контролировать(поиск обрывов и неисправностей). Недостатками является то, что при выходе из строя родительского узла, выйдут из строя и все его дочерние узлы (выход из строя корня — выход из строя всей сети), и также ограничена пропускная способность (доступ к сети может быть затруднён).

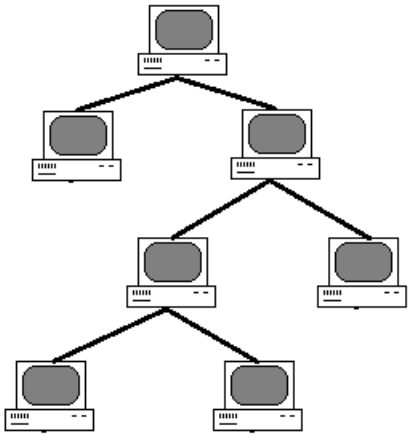

Рис. 4.5:

5 Адресация сетей. MAC, IP. Классовая, безклассовая адресация. Нумерация узлов, сетей. Маска.

Виды глобальных адресов:

- IP-адрес;
- MAC-адрес (6F.1A.48.21.40.FE) — адрес сетевой карты; первые несколько бит — код производителя.

Для того чтобы в процессе обмена информацией компьютеры могли найти друг друга, в сетях существует единая система адресации, основанная на использовании **IP-адреса**.

Каждый компьютер, подключенный к Интернету, имеет свой уникальный 32-битный IP-адрес.

Система IP-адресации учитывает структуру Интернета, то есть то, что Интернет является сетью сетей, а не объединением отдельных компьютеров. IP-адрес содержит адрес сети и адрес компьютера в данной сети.

Для обеспечения максимальной гибкости в процессе распределения IP-адресов, в зависимости от количества компьютеров в сети, адреса разделяются на классы A, B, C, D, E:

A	0	адрес сети 7 бит	адрес узла 24 бит
B	10	адрес сети 14 бит	адрес узла 16 бит
C	110	адрес сети 21 бит	адрес узла 8 бит
D	1110	многоадресная	рассылка
E	1111	зарезервировано	

Подобная адресация называется **классовой**.

Существует также **безклассовая** адресация — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

Маска подсети — битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети (при этом, в отличие от IP-адреса, маска подсети не является частью IP-пакета). Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети 12.34.56.0 с длиной префикса 24 бита.

6 Коммутация каналов и пакетов. Мультиплексирование, демультиплексирование.

Соединение с **коммутацией каналов** — вид телекоммуникационной сети, в которой между двумя узлами сети должно быть установлено соединение (канал), прежде чем они начнут обмен информацией. Это соединение на протяжении всего сеанса обмена информацией может использоваться только указанными двумя узлами. После завершения обмена соединение должно быть соответствующим образом разорвано.

Коммутация пакетов — способ доступа нескольких абонентов к общей сети, при котором информация разделяется на части небольшого размера (так называемые пакеты), которые передаются в сети независимо друг от друга. Узел-приёмник собирает сообщение из пакетов. В таких сетях по одной физической линии связи могут обмениваться данными много узлов.

В информационных технологиях и связи, **мультиплекси́рование** — уплотнение канала, т. е. передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу.

- Мультиплексирование с разделением по частоте предполагает размещение в пределах полосы пропускания канала нескольких каналов с меньшей шириной. Наглядным примером может послужить радиовещание, где в пределах одного канала (радиоэфира) размещено множество радиоканалов на разных частотах (в разных частотных полосах).

- Мультиплексирование с разделением по времени предполагает кадровую передачу данных, при этом переход с каналов меньшей ширины (пропускной способности) на каналы с большей освобождает резерв для передачи в пределах одного кадра большего объёма нескольких кадров меньшего.

Мультиплексирование по времени используется в сетях передачи данных, к примеру, в протоколе Ethernet.

Демультиплексирование — операция, обратная к мультиплексированию.

7 Стандартизация сетей. Многоуровневые модели.

???

8 Эталонная и стандартная модели OSI.

Описывает произвольные виды сетевого взаимодействия между различными узлами.
Эталонная модель OSI состоит из 7 уровней (от нижнего к верхнему):

1. Физический (Технологии ADSL, ISDN, ATM, RS-x, FDDI,);
2. Канальный (Технологии Ethernet, протокол PtPP);
3. Сетевой (Протокол IP);
4. Транспортный (TCP, UDP);
5. Сеансовый (POP);
6. Представительский (POP/SMTP, SNMP, Telnet, HTTP, FTP, DNS);
7. Прикладной (WEB, Email).

Стандартная модель же упрощена и включает в себя всего 4 уровня:

1. Физическо-канальный
2. Сетевой
3. Транспортно-сеансовый
4. Представительско-прикладной

Обработка и передача сообщений.

Имеется некоторое сообщение. При переходе на следующий (нижний) уровень перед ним записывают заголовок, который содержит IP-адреса отправителя и получателя, порты, информацию о протоколах, интерфейсах, типе сообщения и тому подобное. После сообщения добавляется концевик, который содержит служебную информацию для проверки правильности доставки сообщения (контрольные суммы). Для каждого уровня заголовки и концевики свои. Таким образом, физический уровень передает уже гораздо больший пакет. После передачи данных пакет проходит обратную «распаковку». Если целостность пакета нарушена, то то он будет отброшен.

Порт — идентификатор ID процесса или приложения, для которого предназначается этот пакет.

9 Уровни модели OSI.

Рассмотрим более подробно что делает каждый из уровней модели OSI.

1) Физический. Физический уровень — нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому. Осуществляет передачу электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их приём и преобразование в биты данных в соответствии с методами кодирования цифровых сигналов.

На этом уровне также работают концентраторы, повторители сигнала и медиаконвертеры.

Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п.

2) Канальный уровень предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля за ошибками, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Спецификация IEEE 802 разделяет этот уровень на два подуровня: MAC (англ. media access control) регулирует доступ к разделяемой физической среде, LLC (англ. logical link control) обеспечивает обслуживание сетевого уровня.

На этом уровне работают коммутаторы, мосты и другие устройства. Эти устройства используют адресацию второго уровня (по номеру уровня в модели OSI).

3) Сетевой уровень модели предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.

Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего уровня (по номеру уровня в модели OSI).

4) Транспортный уровень модели предназначен для обеспечения надёжной передачи данных от отправителя к получателю. Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных. Например, UDP ограничивается контролем целостности данных в рамках одной датаграммы и не исключает возможности потери пакета целиком или дублирования пакетов, нарушение порядка получения пакетов данных; TCP обеспечивает надёжную непрерывную передачу данных, исключающую потерю данных или нарушение порядка их поступления или дублирования, может перераспределять данные, разбивая большие порции данных на фрагменты и наоборот, склеивая фрагменты в один пакет.

5) Сеансовый уровень модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

6) Представительский уровень обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или шифрование/дешифрование, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

7) Прикладной уровень — верхний уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью.

10 Система доменных имен.

DNS (англ. Domain Name System — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Система DNS содержит иерархию DNS-серверов, соответствующую иерархии зон. Каждая зона поддерживается как минимум одним авторитетным сервером DNS (от англ. authoritative — авторитетный), на котором расположена информация о домене.

Имя и IP-адрес не тождественны — один IP-адрес может иметь множество имён, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется виртуальный хостинг). Обратное тоже справедливо — одному имени может быть сопоставлено множество IP-адресов: это позволяет создавать балансировку нагрузки.

Для повышения устойчивости системы используется множество серверов, содержащих идентичную информацию, а в протоколе есть средства, позволяющие поддерживать синхронность информации, расположенной на разных серверах. Существует 13 корневых серверов, их адреса практически не изменяются.[1]

Протокол DNS использует для работы TCP- или UDP-порт 53 для ответов на запросы. Традиционно запросы и ответы отправляются в виде одной UDP-датаграммы. TCP используется, когда размер данных ответа превышает 512 байт, и для AXFR-запросов.

11 Маршрутизация сетей. Статическая, динамическая.

Маршрутизация (англ. Routing) — процесс определения маршрута следования информации в сетях связи.

Маршруты могут задаваться административно (статические маршруты), либо вычисляться с помощью алгоритмов маршрутизации, базируясь на информации о топологии и состоянии сети, полученной с помощью протоколов маршрутизации (динамические маршруты).

1) Стати́ческая маршрутиза́ция - вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

При задании статического маршрута указывается:

- Адрес сети (на которую маршрутизируется трафик), маска сети
- Адрес шлюза (узла), который способствует дальнейшей маршрутизации (или подключен к маршрутизируемой сети напрямую)
- (опционально) метрика (иногда именуется также "ценой") маршрута.

При наличии нескольких маршрутов на одну и ту же сеть некоторые маршрутизаторы выбирают маршрут с минимальной метрикой.

Достоинства:

- Лёгкость отладки и конфигурирования в малых сетях.
- Отсутствие дополнительных накладных расходов (из-за отсутствия протоколов маршрутизации)
- Мгновенная готовность (не требуется интервал для конфигурирования/подстройки)
- Низкая нагрузка на процессор маршрутизатора
- Предсказуемость в каждый момент времени

Недостатки:

- Очень плохое масштабирование
- Низкая устойчивость.
- Отсутствие динамического балансирования нагрузки

1) Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации редактируется программно.

Динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных.

12 Электронная почта. Протоколы IMAP, Pop3, SMTP.

Электро́нная по́чта — технология и служба по пересылке и получению электронных сообщений между пользователями компьютерной сети.

Основные компоненты электронной почты:

1. Почтовый клиент.

2. Почтовый сервер.

Почтовые клиенты подразделяются на тонкие и толстые. Тонкие клиенты представляют собой веб-сайт либо API и позволяют управлять почтой используя окно браузера. Толстые клиенты — программы для компьютера, которые скачивают письма в локальное хранилище на компьютере и позволяют работать с ними в режиме оффлайн. Примерами почтовых клиентов могут служить Thunderbird, Outlook (Оутглюк), The Bat.

Почтовые серверы — почтовая программа, которая передает сообщения от одного компьютера к другому. Функции: хранение, отправка и получение сообщений, организация очередей клиентов.

Обычно связка сервер-клиент состоит из следующих компонентов:

- MDA (агент проверки доставки сообщений)
- MTA (агент отправки сообщений)
- MUA (user-agent);

Примеры почтовых серверов:

- SendMail;
- qmail;
- MS Exchange Server;
- Postfix;
- Procmail/MailDrop;
- Exim.

Протоколы передачи почты.

1) SMTP:

В качестве команд этого протокола используется ASCII-text. Для передачи данных используется протокол TCP. Стандартный порт протокола — 25.

Схема посылки почты состоит из 3-х этапов:

1) Приветствие;

2) Пересылка почты;

3) Закрытие сессии;

В процессе выполняются следующие команды:

MAIL FROM — устанавливает обратный адрес.

RCPT TO — устанавливает получателя данного сообщения.

DATA — для отправки сообщений.

2) POP3

POP3 — стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP/IP-соединению.

POP поддерживает простые требования «загрузи-и-удали» для доступа к удаленным почтовым ящикам. Хотя большая часть POP-клиентов предоставляет возможность оставить почту на сервере после загрузки, использующие POP клиенты обычно соединяются,

извлекают все письма, сохраняют их на пользовательском компьютере как новые сообщения, удаляют их с сервера, после чего разъединяются.

POP3-сервер прослушивает общеизвестный порт 110.

Доступные сообщения клиента фиксируются при открытии почтового ящика POP-сессией и определяются количеством сообщений для сессии, или, по желанию, с помощью уникального идентификатора, присваиваемого сообщению POP-сервером. Этот уникальный идентификатор является постоянным и уникальным для почтового ящика и позволяет клиенту получить доступ к одному и тому же сообщению в разных POP-сессиях. Почта извлекается и помечается для удаления с помощью номера сообщения. При выходе клиента из сессии помеченные сообщения удаляются из почтового ящика.

Команды POP3:

USER — идентифицирует пользователя с указанным именем;

PASS — указывает пароль для пары клиент-сервер;

QUIT — закрывает TCP соединение;

STAT — возвращает число писем в на сервере;

LIST — запрашивает список сообщений;

RETR — извлекает сообщение с почтового ящика;

DELE — помечает сообщение на удаление;

NOOP (сам NOOB) — сервер возвращает положительный ответ, но не выполняет действий.

LAST — возвращает наибольший размер сообщения из всех, к которым обращались.

RSET — отменяет DELE.

Дополнительные (не входящие в базовую конфигурацию) команды:

APOP — передача на сервер username and password;

UIDL — перенумеровать все сообщения в рамках текущей сессии;

3) IMAP:

IMAP — протокол прикладного уровня для доступа к электронной почте.

Базируется на транспортном протоколе TCP и использует порт 143.

IMAP предоставляет пользователю обширные возможности для работы с почтовыми ящиками, находящимися на центральном сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без постоянной пересылки с сервера и обратно файлов с полным содержанием писем.

Преимущества в сравнении с POP3:

При использовании POP3 клиент подключается к серверу только на промежуток времени, необходимый для загрузки новых сообщений. При использовании IMAP соединение не разрывается, пока пользовательский интерфейс активен, а сообщения загружаются только по требованию клиента. Это позволяет уменьшить время отклика для пользователей, в чьих ящиках имеется много сообщений большого объёма.

Протокол POP требует, чтобы текущий клиент был единственным подключенным к ящику. IMAP позволяет одновременный доступ нескольких клиентов к ящику и предоставляет клиенту возможность отслеживать изменения, вносимые другими клиентами, подключенными одновременно с ним.

Благодаря системе флагов, определенной в IMAP4, клиент может отслеживать состояние сообщения (прочитано, отправлен ответ, удалено и т. д.); данные о флагах хранятся на сервере.

13 Протокол передачи данных TCP, UDP.

TCP — один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных.

В стеке протоколов IP TCP выполняет функции протокола транспортного уровня модели OSI.

Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи.

Когда осуществляется передача от компьютера к компьютеру через Интернет, TCP работает на верхнем уровне между двумя конечными системами, например, браузером и веб-сервером. TCP осуществляет надежную передачу потока байтов от одной программы на некотором компьютере к другой программе на другом компьютере (например, программы для электронной почты, для обмена файлами). TCP контролирует длину сообщения, скорость обмена сообщениями, сетевой трафик.

Пример: Отправитель запрашивает готовность получателя. Затем они устанавливают соединение. Затем происходит передача данных, причем если пакет не был принят, отправитель отправит его еще раз (и так до 16 раз). Затем сессия закрывается.

Структура пакета TCP изображена на рисунке 13.1.

Структура заголовка

Бит	0 — 3	4 — 9	10 — 15	16 — 31
0	Порт источника			Порт назначения
32	Порядковый номер			
64	Номер подтверждения			
96	Длина заголовка	Зарезервировано	Флаги	Размер Окна
128	Контрольная сумма			Указатель важности
160	Опции (необязательное, но используется практически всегда)			
160/192+	Данные			

Рис. 13.1:

UDP — один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных. Протокол был разработан Дэвидом П. Ридом в 1980 году и официально определён в RFC 768.

UDP использует простую модель передачи, без неявных «рукопожатий» для обеспечения надёжности, упорядочивания или целостности данных. Таким образом, UDP предоставляет ненадёжный сервис, и датаграммы могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа. UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении. Чувствительные ко времени приложения часто используют UDP, так как предпочтительнее сбросить пакеты, чем ждать задержавшиеся пакеты, что может оказаться невозможным в системах реального времени. При необходимости исправления ошибок на сетевом уровне интерфейса приложение может задействовать TCP или SCTP, разработанные для этой цели.

Природа UDP как протокола без сохранения состояния также полезна для серверов, отвечающих на небольшие запросы от огромного числа клиентов, например DNS и потоковые мультимедийные приложения вроде IPTV, Voice over IP, протоколы туннелирования IP и многие онлайн-игры.

Структура UDP-пакета изображена на рис. 13.2

Рис. 13.2:

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

14 Протокол файловой передачи данных FTP, протокол HTTP.

FTP — стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). Использует 21-й порт. FTP часто используется для загрузки сетевых страниц и других документов с частного устройства разработки на открытые сервера хостинга.

Протокол построен на архитектуре «клиент-сервер» и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. Пользователи FTP могут пройти аутентификацию, передавая логин и пароль открытым текстом, или же, если это разрешено на сервере, они могут подключиться анонимно. Можно использовать протокол SSH для безопасной передачи, скрывающей (шифрующей) логин и пароль, а также шифрующей содержимое.

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, и даже до TCP/IP, в 1971 году. В первое время он работал поверх протокола NCP. Он и сегодня широко используется для распространения ПО и доступа к удалённым хостам.

Достаточно яркая особенность протокола FTP в том, что он использует множественное (как минимум — двойное) подключение. При этом один канал является управляющим, через который поступают команды серверу и возвращаются его ответы (обычно через TCP-порт 21), а через остальные происходит собственно передача данных, по одному каналу на каждую передачу. Поэтому в рамках одной сессии по протоколу FTP можно передавать одновременно несколько файлов, причём в обоих направлениях. Для каждого канала данных открывается свой TCP порт, номер которого выбирается либо сервером, либо клиентом, в зависимости от режима передачи.

HTTP — протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер», то есть предполагается существование:

- Потребителей (клиентов), которые инициируют соединение и посылают запрос;
- Поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические объекты или что-то абстрактное. Особенностью протокола HTTP является возможность указать в запросе и ответе способ

представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т. д. (в частности, для этого используется HTTP-заголовок). Именно благодаря возможности указанию способа кодирования сообщения, клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым.

HTTP — протокол прикладного уровня; аналогичными ему являются FTP и SMTP. Обмен сообщениями идёт по обыкновенной схеме «запрос-ответ». Для идентификации ресурсов HTTP использует глобальные URI. В отличие от многих других протоколов, HTTP не сохраняет своего состояния. Это означает отсутствие сохранения промежуточного состояния между парами «запрос-ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами (например, «куки» на стороне клиента, «сессии» на стороне сервера). Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

Рис. 14.1:

Свойство	FTP	HTTP
Основан на сессиях работы	Да	Нет
Встроена аутентификация пользователей	Да	Нет
В основном предусмотрен для передачи	Больших двоичных файлов	Небольших текстовых файлов
Модель соединения	Двойное подключение	Одиночное подключение
В основном приспособлен для приёма/передачи	Приёма и передачи	Приёма
Поддерживает текстовый и двоичный режимы передачи	Да	Нет
Поддерживает указание типов передаваемых данных (MIME заголовки)	Нет	Да
Поддерживает операции над файловой системой (mkdir, rm, rename, и т. д.)	Да	Нет

15 Аспекты сетевой безопасности.

Аспекты:

1. Конфиденциальность;
2. Целостность данных;
3. Аутентификация;
4. Доступность.

Конфиденциа́льность — необходимость предотвращения утечки (разглашения) какой-либо информации.

Целостность информации — термин в информатике, означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

В криптографии и информационной безопасности целостность данных— это сохранение данных в том виде, в каком они были созданы. Для проверки целостности данных в криптографии используются хеш-функции, например, MD5. Хэш-функция преобразует последовательность байт произвольного размера в последовательность байт фиксированного размера (число). Если данные изменятся, то и число, генерируемое хеш-функцией, тоже изменится.

Аутентифика́ция — процедура проверки подлинности, например:

- проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;
- подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
- проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Учитывая степень доверия и политику безопасности систем, проводимая проверка подлинности может быть односторонней или взаимной. Обычно она проводится с помощью криптографических способов.

Аутентификацию не следует путать с **авторизацией** (процедурой предоставления субъекту определённых прав) и **идентификацией** (процедурой распознавания субъекта по его идентификатору).

Доступность — состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов

16 Виды сетевых угроз.

1. Сниффинг — прослушка и анализ сетевого трафика.
2. Аутентификация:
   (a) Перехват пароля/ключа;
   (b) Подбор пароля (broot force).
3. Недостаточная аутентификация. Данная уязвимость возникает тогда, когда веб-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной аутентификации.
4. MitM — man-in-the-middle.
5. Лавинные атаки.
   (a) Недостаточное сопротивление автоматизации (атака ботов — DoS). Борьба — Captcha.
   (b) Распределенная лавинная атака (DDoS).
   (c) Флуд.
6. Вирусы, сетевые черви, трояны.
7. Сетевая разведка.
   (a) Скан портов
   (b) Заметание следов
   (c) Инъекции SQL, PHP

(d) Переполнение буфера

(e) Атака на функции форматирования строк

8. Выполнение команд операционной системы.

Защита:

1. Сигнатурный (качественный анализ трафика)
2. Статистический.
3. Гибридный.

Защита от вирусов:

1. Антивирус.
2. Компьютерная гигиена (мойте компьютер перед выходом в интернет, дети).
3. Виртуальная машина (или любая другая песочница).
4. Не подключаться к сети, залить все порты эпоксидкой и выковырять дисковод
5. He-windows.
6. Admin/user.

17 Брандмауэры. Их виды.

Брандмауэр — защита, которая стоит между глобальной и локальной сетью.
Бывают

1. Аппаратными
2. Программными

Типы:

1. Брандмауэр с фильтрацией пакетов.

   Сетевой уровень. Проверяет адрес отправителя и адрес получателя, информацию о приложении или протоколе. Вдобавок следит за портами отправителя и получателя.

   (a) Плюсы:

      i. Недорогой или просто поставляется вместе с антивирусом
      ii. Неплохая скорость.

   (b) Минусы:

      i. Слабая защита.
      ii. Требуется трУЪ настройка.

2. Шлюз сеансового уровня.

   Работает на сеансовом уровне. Следит за квинтированием сеанса связи (логикой пакетов).

(a) Канальные посредники: pipe proxy.

(b) Аппаратные посредники: proxy server.

i. Плюсы:

A. Надежная защита.

ii. Минусы:

A. Скорость меньше.

B. Стоит дороже.

3. Шлюз прикладного уровня.

Этот парниша работает на прикладном уровне. Он может смотреть в пакет, а значит, его можно настроить на фильтрацию определенных команд, в частности, фильтрацию в том числе и служебной или полезной информации. Существуют так называемые посредники прикладного уровня, которые работают каждый с определенными службами (разные посредники для Telnet и FTP, к примеру). Также этот шлюз занимается проблемами аутентификации.

(a) Плюсы:

i. Надежная защита.

(b) Минусы:

i. Большая стоимость

ii. Малая скорость работы

iii. Прозрачность.

4. Брандмауэр экспертного уровня.

А этот чувак вообще крутой и объединяет функции предыдущих брандмауэров. Работает напрямую с опреационной системой, отслеживает сеансы связи, предоставляет посредников, фильтрует.

(a) Плюсы:

i. Максимальная надежность.

(b) Минусы:

i. Максимальная стоимость.

ii. Средняя скорость.

iii. Средняя прозрачность.

18 Пиринговые сети.

Однора́нговая, децентрализо́ванная или пи́ринговая сеть — это оверлейная (то есть являющаяся надстройкой над другой сетью) компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры.

Устройство: В сети присутствует некоторое количество машин, при этом каждая может связаться с любой из других. Каждая из этих машин может посылать запросы другим машинам на предоставление каких-либо ресурсов в пределах этой сети и, таким образом, выступать в роли клиента. Будучи сервером, каждая машина должна быть способной обрабатывать запросы от других машин в сети, отсылать то, что было запрошено. Каждая машина также должна выполнять некоторые вспомогательные и административные функции (например, хранить список других известных машин-«соседей» и поддерживать его актуальность).

Любой член данной сети не гарантирует своё присутствие на постоянной основе. Он может появляться и исчезать в любой момент времени. Но при достижении определённого критического размера сети наступает такой момент, что в сети одновременно существует множество серверов с одинаковыми функциями.

Одна из областей применения технологии одноранговых сетей — это обмен файлами. Пользователи файлообменной сети выкладывают какие-либо файлы в т. н. «расшаренную» директорию, содержимое которой доступно для скачивания другим пользователям. Какой-нибудь другой пользователь сети посылает запрос на поиск какого-либо файла. Программа ищет у клиентов сети файлы, соответствующие запросу, и показывает результат. После этого пользователь может скачать файлы у найденных источников. В современных файлообменных сетях информация загружается сразу с нескольких источников. Её целостность проверяется по контрольным суммам. (Если кто не понял - это торренты).

19 Технология xDSL.

xDSL (англ. digital subscriber line, цифровая абонентская линия) — семейство технологий, позволяющих значительно повысить пропускную способность абонентской линии телефонной сети общего пользования путём использования эффективных линейных кодов и адаптивных методов коррекции искажений линии на основе современных достижений микроэлектроники и методов цифровой обработки сигнала.

Технологии xDSL появились в середине 90-х годов как альтернатива цифровому абонентскому окончанию ISDN.

В аббревиатуре xDSL символ «x» используется для обозначения первого символа в названии конкретной технологии, а DSL обозначает цифровую абонентскую линию DSL (англ. Digital Subscriber Line — цифровая абонентская линия). Технологии xDSL позволяют передавать данные со скоростями, значительно превышающими те скорости, которые доступны даже лучшим аналоговым и цифровым модемам. Эти технологии поддерживают передачу голоса, высокоскоростную передачу данных и видеосигналов, создавая при этом значительные преимущества как для абонентов, так и для провайдеров. Многие технологии xDSL позволяют совмещать высокоскоростную передачу данных и передачу голоса по одной и той же медной паре. Существующие типы технологий xDSL различаются в основном по используемой форме модуляции и скорости передачи данных.

Службы xDSL разрабатывались для достижения определенных целей: они должны работать на существующих телефонных линиях, они не должны мешать работе различной аппаратуры абонента, такой как телефонный аппарат, факс и т. д., скорость работы должна быть выше теоретического предела в 55 Кбит/сек., и наконец, они должны обеспечивать постоянное подключение. Широкое распространение технологий xDSL должно сопровождаться некоторой перестройкой работы поставщиков услуг Интернета и поставщиков услуг телефонных сетей, так как их оборудование теперь должно работать совместно.

К основным типам xDSL относятся ADSL, HDSL, IDSL, MSDSL, PDSL, RADSL, SDSL, SHDSL, UADSL, VDSL. Все эти технологии обеспечивают высокоскоростной цифровой доступ по абонентской телефонной линии. Некоторые технологии xDSL являются оригинальными разработками, другие представляют собой просто теоретические модели, в то время как третьи уже стали широко используемыми стандартами. Основным различием данных технологий являются методы модуляции, используемые для кодирования данных.

20 Протокол DHCP.

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

- Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

- Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.

- Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

21 IP-телефония.

IP-телефони́я — телефонная связь по протоколу IP. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям. Сигнал по каналу связи передаётся в цифровом виде и, как правило, перед передачей преобразовывается (сжимается) с тем, чтобы удалить избыток информации и снизить нагрузку на сеть передачи данных.

IP-телефония является приложением более общей технологии VoIP (англ. Voice over IP) для организации двустороннего общения. Технология VoIP в общем случае подразумевает

все варианты передачи голоса через IP, в том числе не имеющие никакого отношения к телефонии и общению людей. Например, технология VoIP применяется для передачи звука в системах IP-видеонаблюдения, в системах оповещения, при трансляции вебинаров, при просмотре фильмов в режиме онлайн и т. п.

IP-телефония реализует задачи и решения, которые с помощью технологии телефонной сети общего пользования реализовать будет труднее, либо дороже.

Возможность передавать более одного телефонного звонка в рамках высокоскоростного телефонного подключения. Поэтому IP-телефония используется в качестве простого способа для добавления дополнительной телефонной линии дома или в офисе. Свойства, такие как

- конференция,
- переадресация звонка,
- автоматическое повторение номера,
- определение номера звонящего,

предоставляются бесплатно, тогда как в традиционных телекоммуникационных компаниях обычно выставляются в счёт.

- Безопасные звонки, со стандартизованным протоколом (такие как SRTP). Большинство трудностей для включения безопасных телефонных соединений по традиционным телефонным линиям, такие как оцифровка сигнала, передача цифрового сигнала, уже решены в рамках IP-телефонии. Необходимо лишь произвести шифрование сигнала и его идентификацию для существующего потока данных.
- Независимость от месторасположения. Нужно только интернет-соединение для подключения к провайдеру IP-телефонии. Например, операторы центра звонков с помощью IP-телефонов могут работать из любого офиса, где есть в наличии эффективное быстрое и стабильное интернет-подключение.
- Доступна интеграция с другими сервисами через интернет, включая видеозвонок, обмен сообщениями и данными во время разговора, аудиоконференции, управление адресной книгой и получение информации о том, доступны ли для звонка другие абоненты.
- Дополнительные телефонные свойства — такие как маршрутизация звонка, всплывающие окна, альтернативный GSM-роуминг и внедрение IVR — легче и дешевле внедрить и интегрировать. Тот факт, что телефонный звонок находится в той же самой сети передачи данных, что и персональный компьютер пользователя, открывает путь ко многим новым возможностям.

22 Виды сетевых устройств. Их особенности и отличия.

Устройства, подключенные к какому-либо сегменту сети, называют сетевыми устройствами. Их принято подразделять на 2 группы:

Устройства пользователя. В эту группу входят компьютеры, принтеры, сканеры и другие устройства, которые выполняют функции, необходимые непосредственно пользователю сети;

Сетевые устройства. Эти устройства позволяют осуществлять связь с другими сетевыми устройствами или устройствами конечного пользователя. В сети они выполняют специфические функции.

Типы сетевых устройств

1) Сетевые карты

Устройства, которые связывают конечного пользователя с сетью, называются также оконечными узлами или станциями (host). Примером таких устройств является обычный персональный компьютер или рабочая станция. Для работы в сети каждый хост оснащен платой сетевого интерфейса (Network Interface Card — NIC), также называемой сетевым адаптером. Как правило, такие устройства могут функционировать и без компьютерной сети.

2) Повторители (repeater) представляют собой сетевые устройства, функционирующие на первом (физическом) уровне эталонной модели OSI. Для того чтобы понять работу повторителя, необходимо знать, что по мере того, как данные покидают устройство отправителя и выходят в сеть, они преобразуются в электрические или световые импульсы, которые после этого передаются по сетевой передающей среде. Такие импульсы называются сигналами (signals). Когда сигналы покидают передающую станцию, они являются четкими и легко распознаваемыми. Однако чем больше длина кабеля, тем более слабым и менее различимым становится сигнал по мере прохождения по сетевой передающей среде. Целью использования повторителя является регенерация и ресинхронизация сетевых сигналов на битовом уровне, что позволяет передавать их по среде на большее расстояние. Термин повторитель (repeater) первоначально означал отдельный порт "на входе" некоторого устройства и отдельный порт на его "выходе". В настоящее время используются также повторители с несколькими портами. В эталонной модели OSI повторители классифицируются как устройства первого уровня, поскольку они функционируют только на битовом уровне и не просматривают другую содержащуюся в пакете информацию.

3) Концентратор — это один из видов сетевых устройств, которые можно устанавливать на уровне доступа сети Ethernet. На концентраторах есть несколько портов для подключения узлов к сети. Концентраторы — это простые устройства, не оборудованные необходимыми электронными компонентами для передачи сообщений между узлами в сети. Концентратор не в состоянии определить, какому узлу предназначено конкретное сообщение. Он просто принимает электронные сигналы одного порта и воспроизводит (или ретранслирует) то же сообщение для всех остальных портов.

Для отправки и получения сообщений все порты концентратора Ethernet подключаются к одному и тому же каналу. Концентратор называется устройством с общей полосой пропускания, поскольку все узлы в нем работают на одной полосе одного канала.

Концентраторы и повторители имеют похожие характеристики, поэтому концентраторы часто называют многопортовыми повторителями (multiport repeater). Разница между повторителем и концентратором состоит лишь в количестве кабелей, подсоединенных к устройству. В то время как повторитель имеет только два порта, концентратор обычно имеет от 4 до 20 и более портов.

4) Мост (bridge) представляет собой устройство второго уровня, предназначенное для создания двух или более сегментов локальной сети LAN, каждый из которых является отдельным коллизионным доменом. Иными словами, мосты предназначены для более рационального использования полосы пропускания. Целью моста является фильтрация потоков данных в LAN-сети с тем, чтобы локализовать внутрисегментную передачу данных и вместе с тем сохранить возможность связи с другими частями (сегментами) LAN-сети для перенаправления туда потоков данных. Каждое сетевое устройство имеет связанный с

NIC-картой уникальный MAC-адрес. Мост собирает информацию о том, на какой его стороне (порте) находится конкретный MAC-адрес, и принимает решение о пересылке данных на основании соответствующего списка MAC-адресов. Мосты осуществляют фильтрацию потоков данных на основе только MAC-адресов узлов. По этой причине они могут быстро пересылать данные любых протоколов сетевого уровня. На решение о пересылке не влияет тип используемого протокола сетевого уровня, вследствие этого мосты принимают решение только о том, пересылать или не пересылать фрейм, и это решение основывается лишь на MAC-адресе получателя.

5) Коммутаторы используют те же концепции и этапы работы, которые характерны для мостов. В самом простом случае коммутатор можно назвать многопортовым мостом, но в некоторых случаях такое упрощение неправомерно.

Коммутатор Ethernet используется на уровне доступа. Как и концентратор, коммутатор соединяет несколько узлов с сетью. В отличие от концентратора, коммутатор в состоянии передать сообщение конкретному узлу. Когда узел отправляет сообщение другому узлу через коммутатор, тот принимает и декодирует кадры и считывает физический (MAC) адрес сообщения.

6) Маршрутизаторы (router) представляют собой устройства объединенных сетей, которые пересылают пакеты между сетями на основе адресов третьего уровня. Маршрутизаторы способны выбирать наилучший путь в сети для передаваемых данных. Функционируя на третьем уровне, маршрутизатор может принимать решения на основе сетевых адресов вместо использования индивидуальных MAC-адресов второго уровня. Маршрутизаторы также способны соединять между собой сети с различными технологиями второго уровня, такими, как Ethernet, Token Ring и Fiber Distributed Data Interface (FDDI — распределенный интерфейс передачи данных по волоконно»оптическим каналам). Обычно маршрутизаторы также соединяют между собой сети, использующие технологию асинхронной передачи данных ATM (Asynchronous Transfer Mode — ATM) и последовательные соединения. Вследствие своей способности пересылать пакеты на основе информации третьего уровня, маршрутизаторы стали основной магистралью глобальной сети Internet и используют протокол IP.